paloalto
TECHDOCS

Strata Cloud Managerスタートガイド

docs.paloaltonetworks.com

Contact Information

Corporate Headquarters:
Palo Alto Networks
3000 Tannery Way
Santa Clara, CA 95054
www.paloaltonetworks.com/company/contact-support

About the Documentation

- For the most recent version of this guide or for access to related documentation, visit the Technical Documentation portal docs.paloaltonetworks.com.
- To search for a specific topic, go to our search page docs.paloaltonetworks.com/search.html.
- Have feedback or questions for us? Leave a comment on any page in the portal, or write to us at documentation@paloaltonetworks.com.

Copyright

Last Revised

February 5, 2025

Table of Contents

Strata Cloud Managerのご紹介

どこで使用できますか?	何が必要ですか?
• Software NGFW Creditsによって資金提供されたものを含むNGFW • Prisma Access (Managed by Panorama or Strata Cloud Manager) • Prisma SD-WAN	これらの各ライセンスには、Strata Cloud Managerへのアクセスが含まれています。 ❑ Prisma Access ❑ AIOps for NGFW Premium license (use the Strata Cloud Manager app) ❑ Prisma SD-WAN ❑ Strata Cloud Manager Essentials ❑ Strata Cloud Manager Pro → Strata Cloud Managerで利用できる機能は、使用するライセンスによって異なります。

Palo Alto NetworksのStrata Cloud Managerは、ネットワーク セキュリティのデプロイメント全体に対して、AIを活用した統合的な管理と運用を支援します。Strata Cloud Managerを使用すると、Palo Alto Networksのネットワーク セキュリティ インフラストラクチャ全体(NGFWおよびSASE環境)を、単一の合理化されたユーザーインターフェースから簡単に管理できます。すべてのネットワークセキュリティ適用ポイントで、ユーザー、支社サイト、アプリケーション、および脅威を包括的に可視化します。これにより、実用的な洞察、セキュリティの向上、簡単なトラブルシューティングと問題解決が可能になります。

- ネットワークの中断を予測して防止

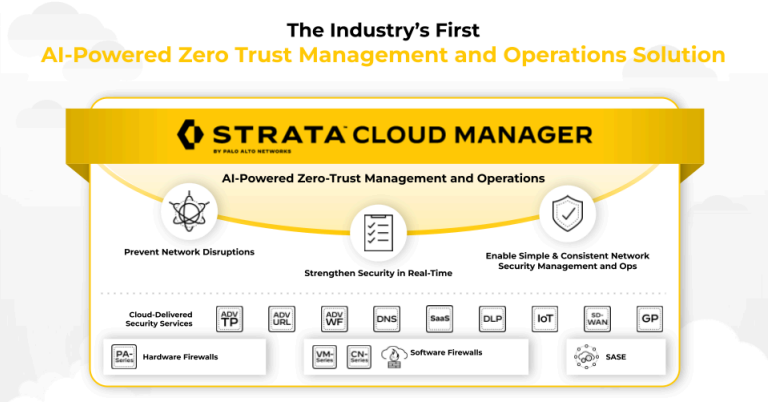
  Strata Cloud Managerは、ネットワークの中断を予測して防止し、問題を迅速に修復することで、お客様とお客様のユーザーが日常業務を継続し、生産性を維持できるようにします。

- リアルタイムのベストプラクティスによるセキュリティの強化

  Strata Cloud Managerは、重要で十分に活用されていないセキュリティ機能を特定し、ニーズに合ったベストプラクティスに基づいてそれらを有効にするようにガイドします。組み込みのベストプラクティスとAIOpsによるインライン修復機能によりセキュリティ体制を強化します。

- シンプルで一貫性のあるネットワークセキュリティの管理と運用

  Strata Cloud Managerは、セキュリティツールを統合して運用と洞察を向上させ、ネットワーク セキュリティ スタック全体にシンプルで一貫した管理エクスペリエンスを採用できるようにします。



Strata Cloud Managerがセキュリティを強化する方法

セキュリティ機能を最大限に活用

- 使用しているセキュリティ機能を確認し、活用できるセキュリティ機能の採用におけるギャップを特定します。 → Feature Adoption (機能の採用)
- セキュリティ サービス サブスクリプションの採用率を確認します。 → CDSS Adoption (CDSSの採用)
- セキュリティ機能がベスト プラクティスにどのように準拠しているか、またはセキュリティ体制を強化するために改善できる点を確認します。→ Built-In Best Practices (組み込みのベストプラクティス)

既存の構成の強化と最適化

使用状況データと自動生成された推奨事項に基づいて、セキュリティ ポリシーをクリーンアップし、合理化します。

- ポリシーで参照されていないオブジェクトと、トラフィックがヒットしないルールをクリーンアップします。これらのオブジェクトとルールは、パフォーマンスを妨害し、ポリシー管理を複雑にする可能性があります。 → Config Clean-Up (設定のクリーンアップ)
- ルールが広すぎると、ネットワークで使用されていないアプリケーションが許可されるため、セキュリティギャップが発生します。Policy Optimizer を使用すると、これらの過度に寛容なルールを、実際に使用しているアプリケーションのみを許可する、より具体的で焦点を絞ったルールに変換できます。 → Policy Optimizer (ポリシーオプティマイザー)

安全な設定のためのリアルタイムガイダンス

- ベストプラクティスガードレールは、セキュリティ ポリシー ルールがベストプラクティスに準拠していることをライブ検証します。 → Live, Inline Best Practice Configuration Checks (ライブのインライン ベスト プラクティス設定チェック)

Strata Cloud Managerがネットワークの中断を予測して防止する方法

包括的な可観測性

- セキュリティインフラストラクチャによってネットワークがどのように安全に保たれているかを把握します。→ Command Center (コマンドセンター)
- ユーザー、ブランチサイト、アプリケーション、ITインフラストラクチャの健康状態とパフォーマンスを、以下から把握します。

  1 つのダッシュボード。→ SASE Health (SASE正常性)ダッシュボード
- デバイスの正常性とパフォーマンスを 1 つのダッシュボードから把握します。→ Device Health (デバイス正常性)ダッシュボード

健全性を予測し、混乱を修復する

自動予測により、潜在的な混乱を防ぎます。問題が検出されると、アクション可能なインサイトが解決を早めます。

- 差し迫った停止の機械支援予測と、修復手順の推奨事項。 → Forecasting and Anomaly Detection (予測と異常検出)
- 推定原因分析により、解決までの時間を短縮します。 → View Probable Causes (考えられる原因の表示)

進化するセキュリティニーズに対応する計画

- 潜在的な容量を事前に特定することで、安定性を向上させます。 →Capacity Analyzer (容量アナライザー)

Strata Cloud Managerがどこでも一貫して機能する仕組み

一貫性のある設定

合理化されたプロセスにより、すべての適用ポイントに一貫したポリシーを適用し、NGFWとSASEのデプロイメントに個別に変更を加える必要がなくなります。

- NGFWとPrisma Accessのモバイルユーザーとリモートネットワークをセットアップしてオンボーディングし、NGFWのソフトウェアアップグレードを計画します。 →Strata Cloud Managerでのワークフロー
- NGFWとPrisma Accessで共有されるセキュリティ ポリシーを設定します。 → NGFWとPrisma Accessの共有管理

柔軟な構成

簡単なフォルダおよびデバイス管理ワークフローにより、大規模な構成管理を簡素化します。

- 構成設定を適用し、ポリシーを環境全体にグローバルに適用したり、組織の特定の部分にターゲット設定とポリシーを適用したりします。 →Configuration Scope (設定範囲)
- ファイアウォールまたはデプロイメント タイプ(Prisma Accessモバイルユーザー、リモートネットワーク、またはサービス接続)を論理的にグループ化して、設定管理を簡素化します。 →Folder Management (フォルダ管理)
- ファイアウォールまたはデプロイメントにすばやくプッシュできる設定をグループ化します。 →Snippets (スニペット)
- デバイスまたはデプロイメント固有の固有の設定値に柔軟に対応できます。 →Variables (変数)

脅威に対する統一的な可視性を実現

- ネットワーク トラフィック、サブスクリプション、ユーザー、アプリケーション、ネットワーク、脅威などを包括的に可視化します。 →Monitoring (モニタリング)
- ネットワーク内で動作しているアプリケーション、IONデバイス、脅威、ユーザー、セキュリティサブスクリプションをインタラクティブに表示します。ダッシュボードは、デプロイメント環境で発生している稼働状態、セキュリティ体制、アクティビティを可視化し、ネットワークのパフォーマンスとセキュリティのギャップを防止または対処するのに役立ちます。 → Dashboards (ダッシュボード)
- ネットワーク トラフィック パターン、帯域幅使用率、セキュリティ サブスクリプション データなどに関するレポートを取得します。レポートは、計画と監視の目的で使用できるネットワークに関する実用的な洞察を提供します。 →Reports (レポート)

Strata Cloud Managerがサポートする製品

どこで使用できますか?	何が必要ですか?
• Software NGFW Creditsによって資金提供されたものを含むNGFW • Prisma Access (Managed by Panorama or Strata Cloud Manager) • Prisma SD-WAN	これらの各ライセンスには、Strata Cloud Managerへのアクセスが含まれています。 ❑ Prisma Access ❑ AIOps for NGFW Premium license (use the Strata Cloud Manager app) ❑ Prisma SD-WAN ❑ Strata Cloud Manager Essentials ❑ Strata Cloud Manager Pro → Strata Cloud Managerで利用できる機能は、使用するライセンスによって異なります。

Strata Cloud Managerは、NGFWとSASEネットワークにAIを活用した統合的な管理と運用を提供しており、利用できるStrata Cloud Manager機能はライセンスによって異なります。ここでは、Strata Cloud ManagerでNGFWやSASEの管理、Strata Cloud Managerのネットワークセキュリティ機能のロック解除を可能にするライセンスについて説明します。→ライセンスの検証方法はこちら

表 **1 :**

Strata Cloud Manager Essentials	Strata Cloud Manager Essentialsは、管理機能とセキュリティ機能を提供しています。これらの機能は、以下の製品とともに無償でご利用いただけます。 • 次世代ファイアウォール(NGFW) • Prisma Access Strata Logging Serviceは、Strata Cloud Manager Essentialsのオプションアドオンとして利用できます。 *Strata Cloud Manager Essentials*と*Strata Cloud Manager Pro*は、以下の機能を持たないカスタマーサポートポータル(CSP)アカウントでアクティベートできます。サイズのストレージを備えた*Strata Logging Service*、*NGFW Free*または*Premium*用の*AIOps*、*Prisma Access*のいずれか。
Strata Cloud Manager Pro	Strata Cloud Manager Proは有料ティアであり、Strata Cloud Manager Essentialsの全機能に加え、運用の健全性強化、ネッ

	トワークの中断防止、リアルタイムのセキュリティ体制強化、ユーザーエクスペリエンスのパフォーマンスを監視するためのAutonomous Digital Experience Management（ADEM）などの高度な機能を備えています。Strata Cloud Manager Proには、1年間のログ保存と無制限のストレージを備えたStrata Logging Serviceが含まれており、デプロイメント環境全体でログの一元管理とシームレスなデータ取得が可能です。Strata Cloud Manager Proでは、以下の製品を購入できます。 • 次世代ファイアウォール(NGFW) • Software NGFW CreditsによるVMシリーズ • Prisma Access
AIOps for NGFW プレミアム	AIOps for NGFW Premiumライセンスを持つNGFWの場合、Strata Cloud ManagerはNGFWの正常性とセキュリティを全体的に把握でき、プロアクティブなチェックを実施してセキュリティギャップを埋めることができます。 • **NGFW (Managed by PAN-OS or Panorama)** → AIOps for NGFW Premium ライセンスを持つPAN-OSおよびPanorama Managed NGFWの場合、Strata Cloud Managerを使用してデプロイメントの正常性とセキュリティ体制を監督します。 • **NGFW (Managed by Strata Cloud Manager)**→AIOps for NGFWライセンスがあれば、Strata Cloud Managerを利用して、**NGFW**のクラウド管理を行うこともできます。 • *Strata Cloud Manager*を使用してCloud Management for NGFWを有効にするには、アカウントチームにお問い合わせください。 • *Strata Cloud Manager*は、*AIOps for NGFW Premium*ライセンスを使用する*NGFW*のみに統合された管理と運用を提供します。*AIOps for NGFW Free*にオンボードされている*NGFW*については、引き続きAIOps for NGFW Freeアプリケーションを使用してください。
Software NGFW Credits	ソフトウェアNGFWクレジットで支援されたVM-Seriesの場合、Strata Cloud ManagerはNGFWのクラウド管理を含むNGFW Premium機能のAIOpsをサポートします。
Prisma Access	Prisma Accessの管理には、Strata Cloud ManagerとPanoramaの2つの方法がありま

	す。Strata Cloud ManagerにはPrisma Accessの可視性機能があり、使用している管理インターフェースに関係なくサポートされています。つまり、Panoramaを使用してPrisma Accessを管理している場合でも、Strata Cloud Managerを使用してPrisma Access環境の包括的なモニタリングを行うことができます。 **Prisma Access (Managed by Strata Cloud Manager)** Prisma Access環境の完全な初期登録、管理、および監視にStrata Cloud Managerを使用します。 これには、Prisma Accessに含まれる クラウド配信型セキュリティサービス の管理と監視にStrata Cloud Managerを使用することも含まれます。 Strata Cloud Managerは、Prisma Access環境に対する包括的な監視、アラート、および可視性を提供します。 • AI搭載自律型DEM • Strata Cloud ManagerでPrisma Accessを監視する • Strata Cloud Managerダッシュボード • Strata Cloud Manager モニタリング • Strata Cloud Manager Reports **Prisma Access (Managed by Panorama)** Panoramaを使用してPrisma Accessを管理している場合は、引き続きPanoramaを使用して環境を管理する必要があります。ただし、Strata Cloud Managerを使用して、Prisma Access環境の包括的な監視、アラート、可視性を実現できます。 • AI搭載自律型DEM • Strata Cloud ManagerでPrisma Accessを監視する • Strata Cloud Managerダッシュボード • Strata Cloud Managerモニタリング • Strata Cloud Manager Reports
AIを活用したADEM	AI搭載ADEMは、Prisma Accessのアドオン ライセンスであり、複雑なIT運用を自動化し、生産性の向上と問題解決までの時間短縮を実現します。Strata Cloud Managerは、すべてのPrisma Accessユーザー（Panorama - Managed Prisma AccessとPrisma Access Cloud Managementの両方）のAI搭載ADEMをサポートしています。

	*Prisma Access*の管理に*Panorama*を使用している場合は、*Panorama*を引き続き使用して環境を管理する必要があり、*Strata Cloud Manager*を使用して*ADEM*の監視を行うことができます。
Prisma SD-WAN	Strata Cloud Manager for Prisma SD-WANを利用する。Prisma SD-WANは、アプリケーション定義の自律型SD-WANを実装したクラウド配信型サービスで、コストや複雑さを増やすことなく、ブランチオフィス、データセンター、大規模キャンパスサイトのセキュリティと接続を支援します。AppFabricは、アプリケーション対応でサイトを安全に接続し、シンブランチ（クラウドからのセキュリティ）ソリューションに、あらゆるWAN、あらゆるクラウドを自由に使用できます。
CDSS（クラウド提供型セキュリティサービス）： • 高度な脅威防御 • 高度な **URL** フィルタリング • アドバンスド **WildFire** • **DNS** セキュリティ • **Enterprise DLP** • **IoT**セキュリティ • **SaaS** セキュリティ	Prisma Accessライセンスまたは**AIOps for NGFW Premium**ライセンスをお持ちの場合は、Strata Cloud Managerを使用してセキュリティ サブスクリプションを管理および監視できます。 Strata Cloud Managerは、セキュリティ サブスクリプションが提供する保護を、エンタープライズトラフィック全体で一貫して提供します。 セキュリティ サブスクリプションで使用できるStrata Cloud Manager機能は、ライセンスによって異なります。また、次のような機能を使用できます。 • セキュリティ サブスクリプションのStrata Cloud Managerダッシュボードとレポート • セキュリティサブスクリプションのStrata Cloud Manager統合管理。Strata Cloud Managerを使用してNGFWやPrisma Access間で共有セキュリティ ポリシーを適用している場合は、セキュリティ サブスクリプションに単一の集中設定を使用できます。

Strata Cloud Managerの概説

どこで使用できますか?	何が必要ですか?
• Software NGFW Creditsによって資金提供されたものを含むNGFW • Prisma Access (Managed by Panorama or Strata Cloud Manager) • Prisma SD-WAN	これらの各ライセンスには、Strata Cloud Managerへのアクセスが含まれています。 ❑ Prisma Access ❑ AIOps for NGFW Premium license (use the Strata Cloud Manager app) ❑ Prisma SD-WAN ❑ Strata Cloud Manager Essentials ❑ Strata Cloud Manager Pro → Strata Cloud Managerで利用できる機能は、使用するライセンスによって異なります。

Strata Cloud Managerについて概説します。Strata Cloud Managerのユーザーインターフェイスでは、ネットワークを包括的に把握でき、NGFWとSASEを管理するための統合されたワークフローを確認できます。シンプルで一貫性のある新しいナビゲーションを使用して、すべてのネットワークデータを操作したり、自動的に表面化される実践につながるインサイトを取得したり、Prisma Access、NGFW、クラウドが提供するセキュリティサービスをまとめて管理および監視したりできます。

左側のナビゲーションバーの各メニューをご覧ください。これらのパスは、Strata Cloud Managerで使用しているPalo Alto Networks製品またはサブスクリプションで標準的に使用されるようになりました。これにより、以下のことが容易になります。

- 新しい機能とサブスクリプションを採用
- 新規ユーザー、デバイス、サイト、またはロケーションのオンボーディング

既存の管理セットアップにそのまま組み込み可能。

重要

*Strata Cloud Manager*で使用できる機能は、お使いのサブスクリプションによって異なります。*Strata Cloud Manager*のドキュメントを参照して、*Strata Cloud Manager*機能のライセンス要件を確認できます。

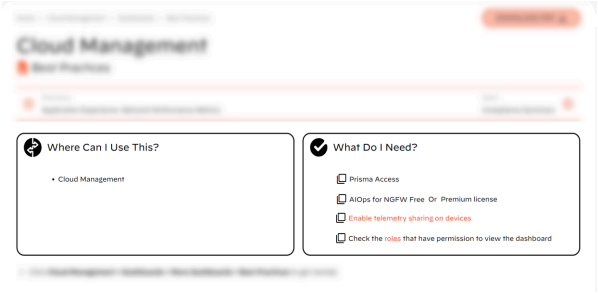
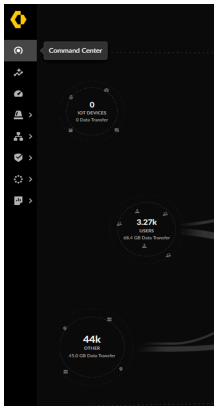
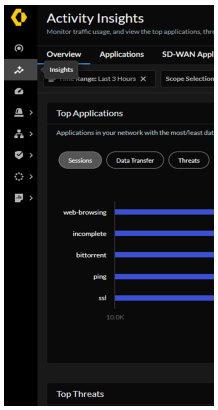
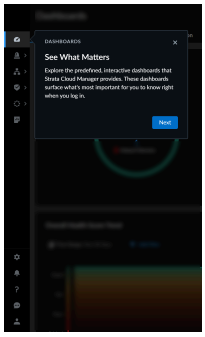
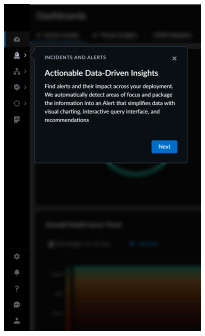
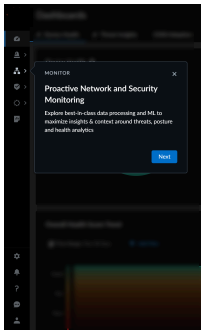
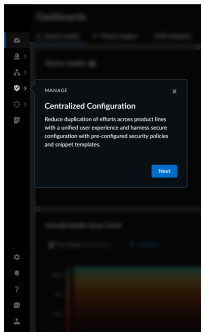
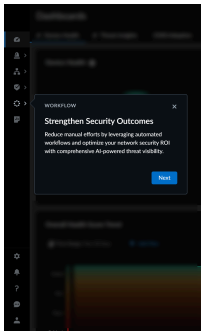
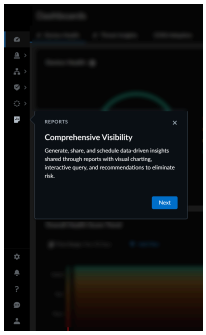
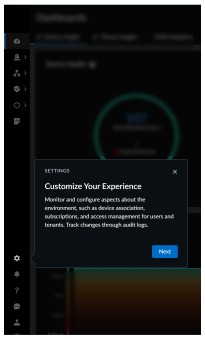


表 **2 :**

指令センター	ネットワークの正常性、セキュリティ、効率性を評価する最初の手段 指令センターは、ネットワークとセキュリティインフラストラクチャの概要を視覚化したものです。4つの異なるビューを提供し、それぞれにトラッキングされたデータ、メトリック、および検証や対話のための実用的なインサイトがあります。 • コマンドセンター:ログ - Strata Cloud Manager	
アクティビティに関するインサイト	統合ネットワークデータ、すべてを**1**か所で Activity Insights(アクティビティに関するインサイト)では、Prisma AccessやNGFWのデプロイメント全体にわたるネットワークアクティビティを詳細に把握できます。Activity Insights(アクティビティに関するインサイト)は、ネットワークトラフィック、アプリケーションの使用状況、脅威、ユーザーアクティビティなどのネットワークデータを1か所に統合します。	

	• インサイト（知見）:アクティビティに関するインサイト	
ダッシュボード	すぐに重要な内容を確認 ダッシュボードは、ログインした瞬間から、自分にとって最も重要な情報が表示されます。各ダッシュボードは、セキュリティ態勢やネットワークの健全性を改善するためにアクションを実行できる領域を強調するように設計されています。 用意されている事前定義済みのインタラクティブなダッシュボードをすべて確認すれば、お気に入りをピン留めできます。 • ダッシュボード:ログ - Strata Cloud Manager	
インシデントとアラート	実践につながるデータドリブンインサイト Strata Cloud Managerは、統合されたインシデントおよびアラートフレームワークを提供します。ネットワーク上のアラートやインシデントを1か所で表示、調査、対処し、関連するアクティビティを調べるためにログにジャンプします。 • インシデントとアラート:ログ - Strata Cloud Manager	
監視	プロアクティブなネットワークとセキュリティの監視 ネットワーク上のあらゆるものの正常性とセキュリティを監視し、IoC検索を使用してネットワーク上のアーティファクトの履歴を調査し、グローバル解析の結果を確認できます。ご利用のサブスクリプションや製品に応じて、以下の監視が可能です。 • NGFW デバイス • Prisma Access • アプリケーション	

	• ユーザー • ブランチサイト • データセンター • ネットワークサービス（GlobalProtectやDNSなど） • Palo Alto Networks サブスクリプション • Prisma Access ロケーション • Prisma SD-WAN • アセット	
管理	設定の一元化 ネットワークセキュリティ製品およびサブスクリプション全体で共有ポリシーを管理します。初日から、事前定義済みのベストプラクティスポリシーと設定、およびインラインのベストプラクティスチェックに基づいて、セキュアな構成を開始できます。 • 管理:NGFW と Prisma のアクセス • 管理:IoT ポリシーの推奨事項 • 管理:Enterprise DLP • 管理:SaaS セキュリティ	
ワークフロー	セキュリティ上の成果の強化 最初にワークフローに移動すると、セキュリティ体制の改善や設定管理の最適化のために実行できる重要な推奨アクションが、**[Discovery (検出)]**ダッシュボードに表示されます。これらのアクションが利用可能になると、すぐに表示されます。引き続き、NGFWとPrisma Accessのモバイルユーザーとリモートネットワークのセットアップとオンボードを行い、NGFWのソフトウェアアップグレードを計画します。 • Prisma Accessのセットアップ • NGFWのセットアップ	

	• Software Upgrade Planner (AIOps用NGFW)	
レポート	包括的な可視性 レポートを通じて共有されるデータ主導のインサイトの生成、共有、スケジュール設定が可能です。ビジュアルなチャート表示、インタラクティブなクエリ、推奨事項により、リスクを排除できます。 • レポート:ログ - Strata Cloud Manager	
設定	オンボーディングとアクティベーションの設定 これらは、新しいユーザー、ライセンス、管理者を追加するとき、あるいはあなた自身がStrata Cloud Managerを使い始めるときに、必ず参照する設定です。 • サブスクリプション • テナント • デバイスの関連付け • IDとアクセス • 監査ログ	

Strata Cloud Managerを起動する

どこで使用できますか?	何が必要ですか?
• Software NGFW Creditsによって資金提供されたものを含むNGFW • Prisma Access (Managed by Panorama or Strata Cloud Manager) • Prisma SD-WAN	これらの各ライセンスには、Strata Cloud Managerへのアクセスが含まれています。 ❑ Prisma Access ❑ AIOps for NGFW Premium license (use the Strata Cloud Manager app) ❑ Prisma SD-WAN ❑ Strata Cloud Manager Essentials ❑ Strata Cloud Manager Pro → Strata Cloud Managerで利用できる機能は、使用するライセンスによって異なります。

Strata Cloud ManagerアプリケーションはPalo Alto Networksハブで利用でき、次のURLで直接アクセスできます。 stratacloudmanager.paloaltonetworks.com。

Prisma Accessライセンス、AIOps for NGFW Premiumライセンス、またはPrisma SD-WANライセンスは、Strata Cloud Managerの統合管理と運用の基本要件です。これらのライセンスを少なくとも1つお持ちの場合は、Strata Cloud Manager にアクセスして、製品を表示したり、管理したりできます。

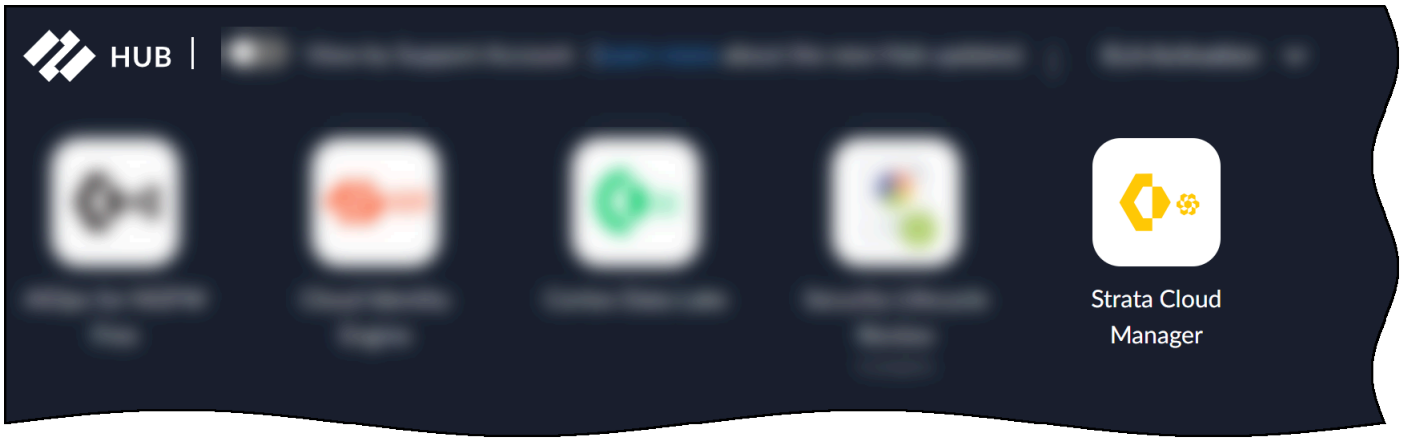
これらのライセンスを複数お持ちの場合は、 Strata Cloud Managerは、これらの製品と対話するための単一のインターフェースと、追加のライセンスまたはアドオンサブスクリプション(Palo Alto Networksのセキュリティサブスクリプションなど)を提供します。 → *Strata Cloud Manager*の統合管理と運用でサポートされている製品とライセンスAA の統合管理と運用でサポートされている製品とライセンスを見るを見る

Strata Cloud Managerの起動はアクセスするには:

- Prisma Access、AIOps for NGFW Premium、または2023年10月以降にPrisma SD-WANを初めて使用する場合は、Strata Cloud Managerをはじめて開始するの仕方を確認してください
- これまでハブ上で個別のスタンドアロンのアプリケーションを使用して製品を管理していた場合、以下が専用の製品アプリからStrata Cloud Managerへ移行するに関する詳細です。

Strata Cloud Managerをはじめて開始する

Prisma Access、 AIOps for NGFW Premium、または Prisma SD-WAN ライセンスをアクティベートすると、Strata Cloud ManagerアプリはPalo Alto Networksハブで利用可能になります 。また次のリンクから直セスアクセスすることも可能です。stratacloudmanager.paloaltonetworks.com



アプリを起動し、Strata Cloud Managerの概説を取得します。製品のオンボードを続行します:

- AIOps for NGFW Premiumを開始する(Cloud Management for NGFWs
- Prisma Accessを開始する
- Prisma SD-WANを開始する

専用の製品アプリからStrata Cloud Managerへ移行する

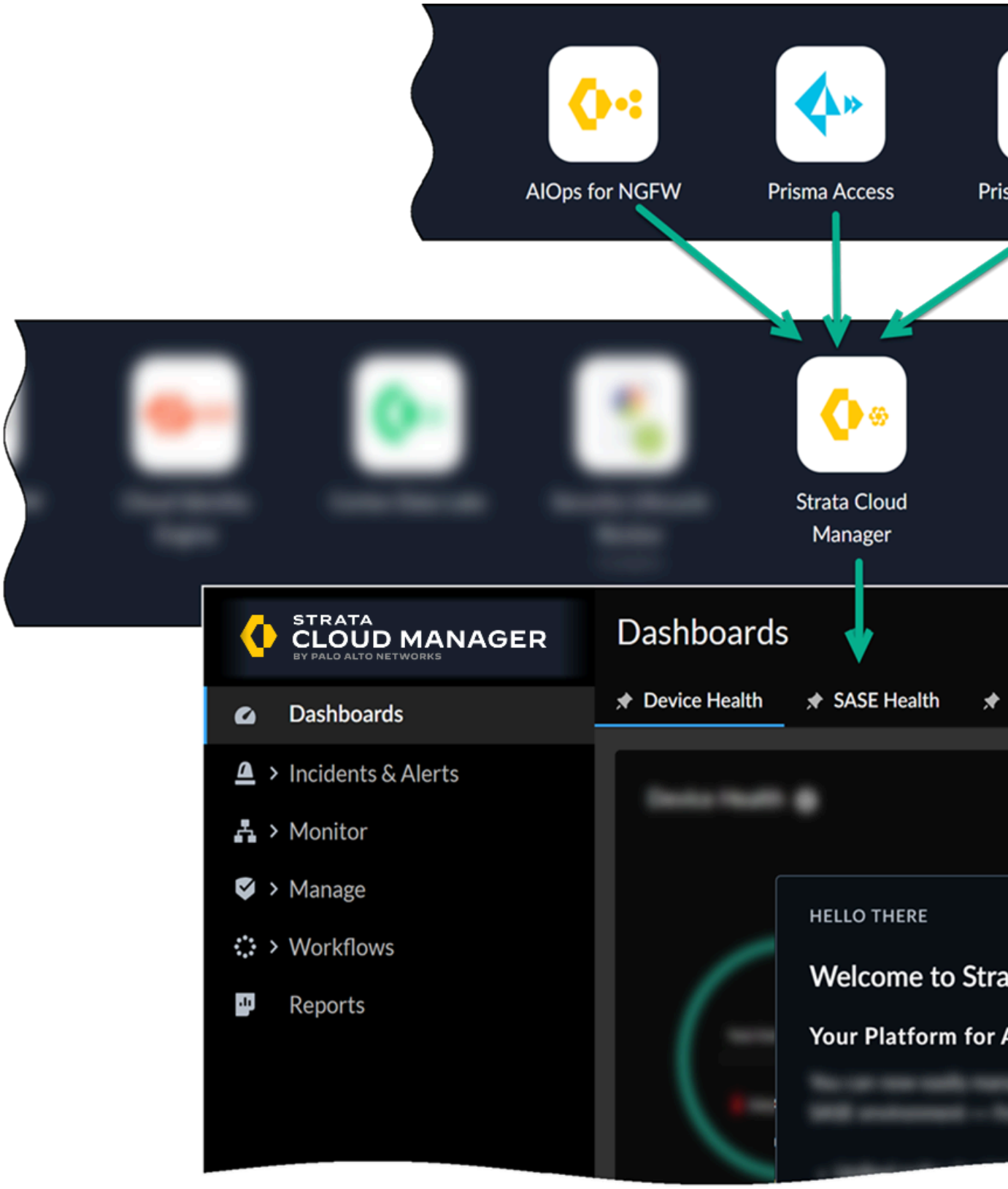
重要

これは、以前にスタンドアロンアプリ(*Prisma Access*アプリ、*AIOps for NGFW Premium*アプリ、*Prisma SD-WAN*アプリ)を使用して製品を管理または操作していた場合にのみ適用されます。これらのアプリは更新されているか、まもなく更新される予定です。これにより*Strata Cloud Manager*統合された管理と運用がご利用いただけます。

製品専用アプリから**Strata Cloud Manager**に移行する際に予想されること:

- Strata Cloud Managerはライセンスサポートに基づく一元的な管理と運用を提供します - ここでは、Strata Cloud Managerで監視または管理を行うことができる製品をご利用いただけます。
- 製品内通知により、アップデートが間もなく行われることを事前にお知らせし、Strata Cloud Managerを提供します。
- 更新はシームレスに行われ、データ、アラート、または資産に影響を与えることはありません。

- アップデート後、ハブ上のStrata Cloud Managerアプリケーションにログインします。Prisma Access、AIOps for NGFW Premium、またはPrisma SD-WANのハブで別々のアプリを使用することはなくなりました。



- 製品アプリケーションは自動的に次のリンクにリダイレクトします:stratacloudmanager.paloaltonetworks.com。これは Strata Cloud Manager の URL です。

  以前に*Strata Cloud Manager*用に更新する複数の製品アプリケーションを使用していた場合、更新された製品アプリケーションはすべて同じ*Strata Cloud Manager*インスタンスにリダイレクトされます。

- Strata Cloud Managerは、ネットワークセキュリティ製品に共通するまったく新しいナビゲーションを提供します。Strata Cloud Managerをご覧になって、新しいナビゲーション体験と機能を探索してください。
- 新しい統合管理インターフェースで製品の以下の機能を見つけてください。
  - AIOps for NGFW:Strata Cloud Managerの機能はどこにありますか?
  - Prisma SD-WAN:Strata Cloud Managerの機能はどこにありますか?
  - Prisma Access Insights:Strata Cloud Managerの機能はどこにありますか?
  - Prisma Access:Strata Cloud Managerの機能はどこにありますか?

Strata Cloud Managerを開始する

どこで使用できますか?	何が必要ですか?
• Software NGFW Creditsによって資金提供されたものを含むNGFW • Prisma Access (Managed by Panorama or Strata Cloud Manager) • Prisma SD-WAN	これらの各ライセンスには、Strata Cloud Managerへのアクセスが含まれています。 ❑ Prisma Access ❑ AIOps for NGFW Premium license (use the Strata Cloud Manager app) ❑ Prisma SD-WAN ❑ Strata Cloud Manager Essentials ❑ Strata Cloud Manager Pro → Strata Cloud Managerで利用できる機能は、使用するライセンスによって異なります。

Strata Cloud Managerは、NGFWとSASEネットワークにAIを活用した統合管理と運用を提供します。Strata Cloud Managerを初めて使うときのチートシートです。

Strata Cloud Managerを使用してPrisma Access、NGFW(NGFW PremiumにはAIOpsが必要)、またはその両方をオンボードで管理する予定の場合、Prisma AccessとNGFWの共有管理を使い始めるために必要な知識が含まれています

❑ (ハブ内

)ライセンスの有効化ライセンスを購入すると、ライセンス認証のリンクが記載されたメールが届きます。リンクをクリックすると、ハブでガイド付きのワークフローが起動します。アクティブ化する各ライセンスのアクティブ化ワークフローに従います。

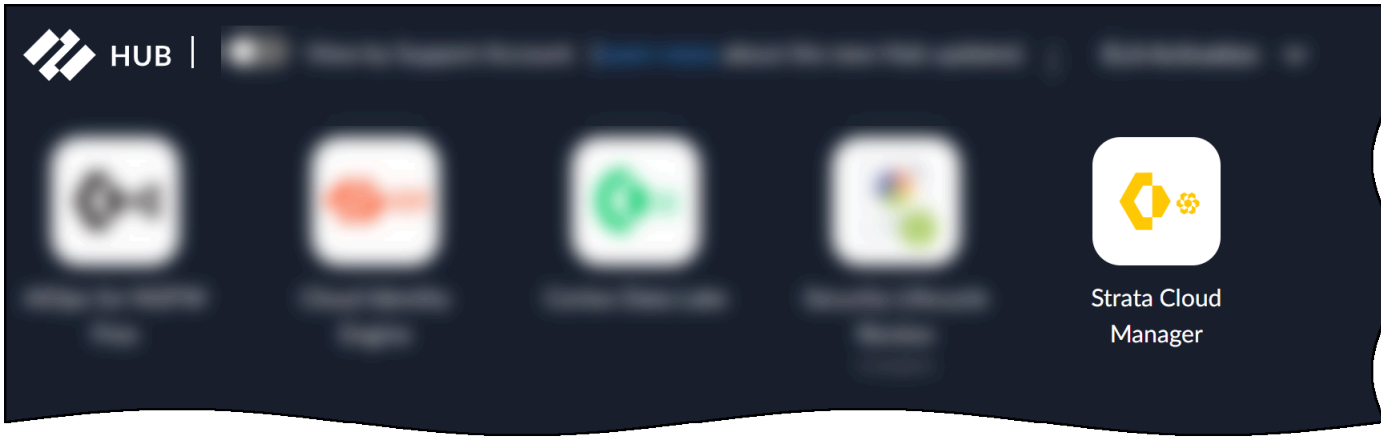
- AIOps for NGFW Premiumライセンス
- Prisma Accessライセンスの有効化
- Prisma SD-WAN

いずれかのライセンスを有効化すると、Strata Cloud Managerが可能になります。これらのライセンスの少なくとも 1 つをアクティブ化した後、追加のライセンスまたはアドオン サブスクリプションのアクティベートを続行します。

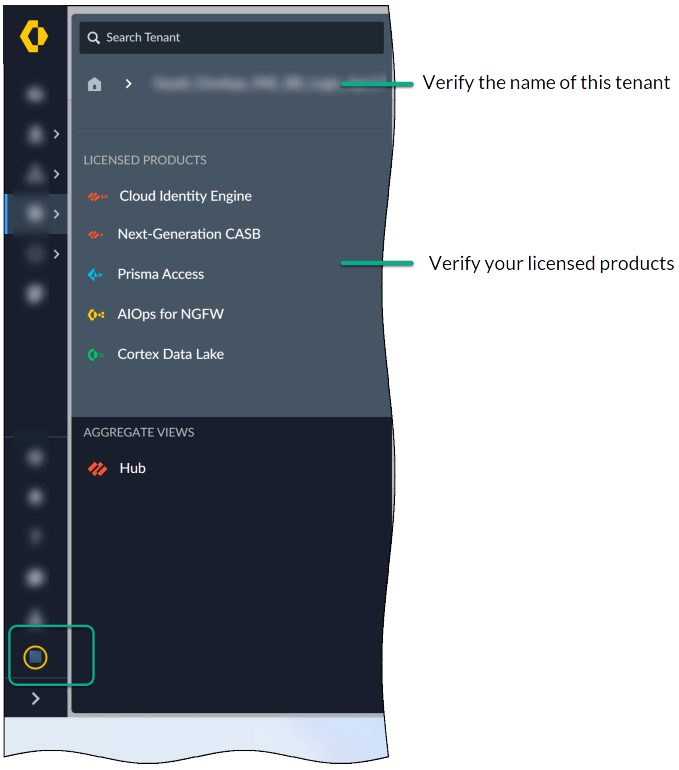
❑ **Strata Cloud Manager**を起動する

Prisma Access、 AIOps for NGFW Premium、または Prisma SD-WAN ライセンスをアクティベートすると、Strata Cloud ManagerアプリはPalo Alto Networksハ

ブで利用可能になります 。また次のリンクから直セスアクセスすることも可能です。stratacloudmanager.paloaltonetworks.com

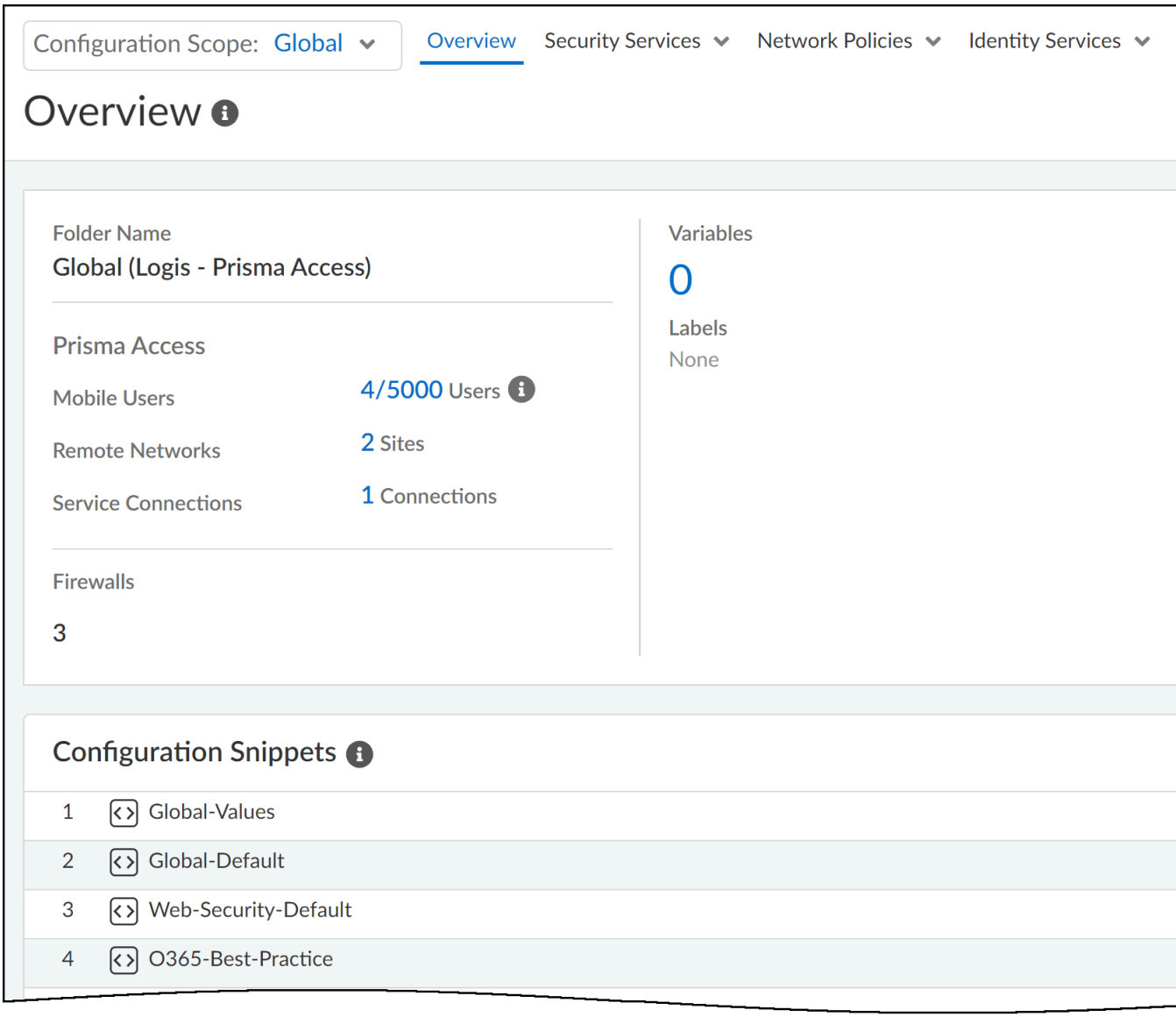


- ライセンスの検証
  - ナビゲーションメニューの下部で、テナントの詳細を選択し、使用しているテナントの名前とライセンス製品を確認します。ここでは、テナントとサブスクリプション管理について詳しく説明します。



  - **[Manage (管理)] > [Configuration (設定)] > [NGFWとPrisma Access]**にアクセスして、Prisma Accessのライセンスステータスと詳細を確認し、他にどのような詳細があるかを確認してください。

    *NGFW*をまだオンボードしていない場合や、*Prisma Access*環境がまだプロビジョニング中の場合は、まだあまりデータが表示されないかもしれません。その場合は、すぐにもう一度確認して、残りの手順をここで完了した後に



- **Strata Cloud Manager**による監視と可視化
  - コマンドセンターを使用して、ネットワークとセキュリティインフラストラクチャを視覚化して確認できます。
  - Activity Insights (アクティビティに関するインサイト)で重要なネットワークデータを確認します。
  - 利用可能なStrata Cloud Managerダッシュボードをご覧ください。多くのダッシュボードでは、スケジュールを設定したり関係者と共有したりできるレポートもサポートしています。
  - Prisma Access環境、Prisma SD-WAN、NGFWを監視します。
  - Prisma Access、NGFW、Prisma SD-WAN全体でインシデントとアラートを確認できます。

- インラインベストプラクティスの推奨事項とワークフロー

  Strata Cloud Managerに直接組み込まれているベストプラクティスガイダンスと自動化の詳細をご覧ください。

- **Strata Cloud Manager**オンボーディング設定

  Strata Cloud Managerは、設定メニューに共通サービスをまとめます。**[Settings (設定)]**に移動して、次の項目を管理します。

  - ロールとアクセス権限:Strata Cloud Managerで使用できるロールと関連するアクセス権限について、詳細をご確認ください。
  - デバイスの関連付け – サポートされているクラウドアプリケーションをデバイスに関連付けます。
  - テナント管理 – テナントによって表されるビジネス組織とユニットの階層を作成および管理します。

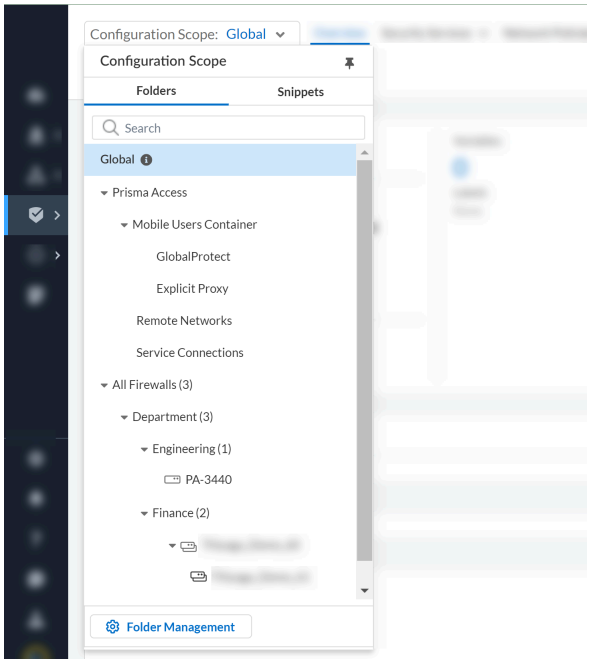
Prisma AccessとNGFWの共有管理

Prisma Access と NGFW の場合、Strata Cloud Managerは共有管理を提供します。NGFWとPrisma Accessのユーザ、リモートネットワーク、およびStrata Cloud Managerへのサービス接続をオンボードして、共通のセキュリティ ポリシーを適用します。

- **NGFW**と**Strata Cloud Manager**への**Prisma**アクセスのオンボード
  - Prisma Accessを設定し、モバイルユーザー、リモートネットワーク、およびサービス接続をオンボードします。
    - Prisma Accessサービスインフラのセットアップ
    - GlobalProtectおよびExplicit Proxy接続を含むPrisma Accessモバイルユーザーのセットアップ
    - Prisma Accessリモートネットワークのセットアップ
    - Prisma Accessサービス接続の設定
  - NGFWのオンボードとセットアップ:
    - NGFWクラウド管理のオンボーディングとセットアップ
- 設定の整理

  Strata Cloud Manager構成設定で作業している場合、現在の管理:設定スコープは常に表示され、表示を切り替えて、より広範な構成またはより細かい構成を管理できます。設定スコー

プでは、ポリシーをグローバルに適用したり、特定のNGFWやPrisma Accessの導入にターゲットを絞った適用を提供したりできます。



Strata Cloud Manager設定の整理を始める方法について、さらに詳しく説明します。

- ワークフロー:フォルダ管理

  設定管理を簡素化するため、フォルダを作成してNGFWを論理的にグループ化しますPrisma Accessフォルダは、デプロイメントタイプに基づいて事前定義されています。Web Security（インターネットやSaaSアプリケーションへのアクセスを管理する管理者向けの簡易管理エクスペリエンス）をフォルダレベルで有効にすることもできます。

- 管理:スニペット

  スニペットを使用して、NGFWやPrisma Accessのデプロイメントにすばやくプッシュできる設定をグループ化できます。

- 管理:変数

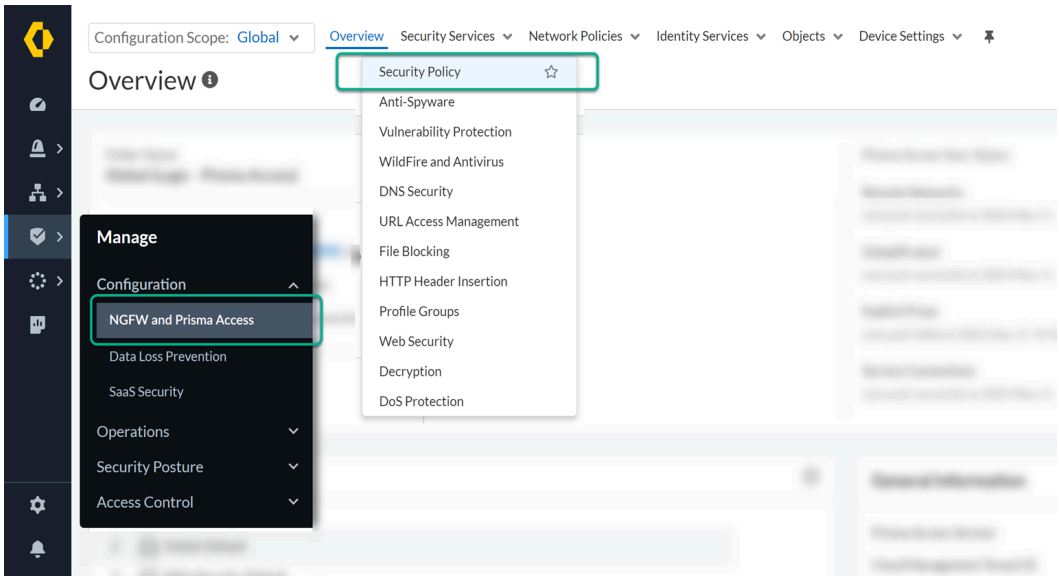
  デバイスまたはデプロイメント固有の設定オブジェクトに対応するために、設定に変数を使用します。

- **NGFW**と**Prisma**アクセスの共有セキュリティポリシー

  Strata Cloud Managerでは、Prisma AccessとNGFWを統合管理できます。お使いのStrata Cloud Managerセキュリティポリシーは共有されており、Prisma AccessとNGFWで

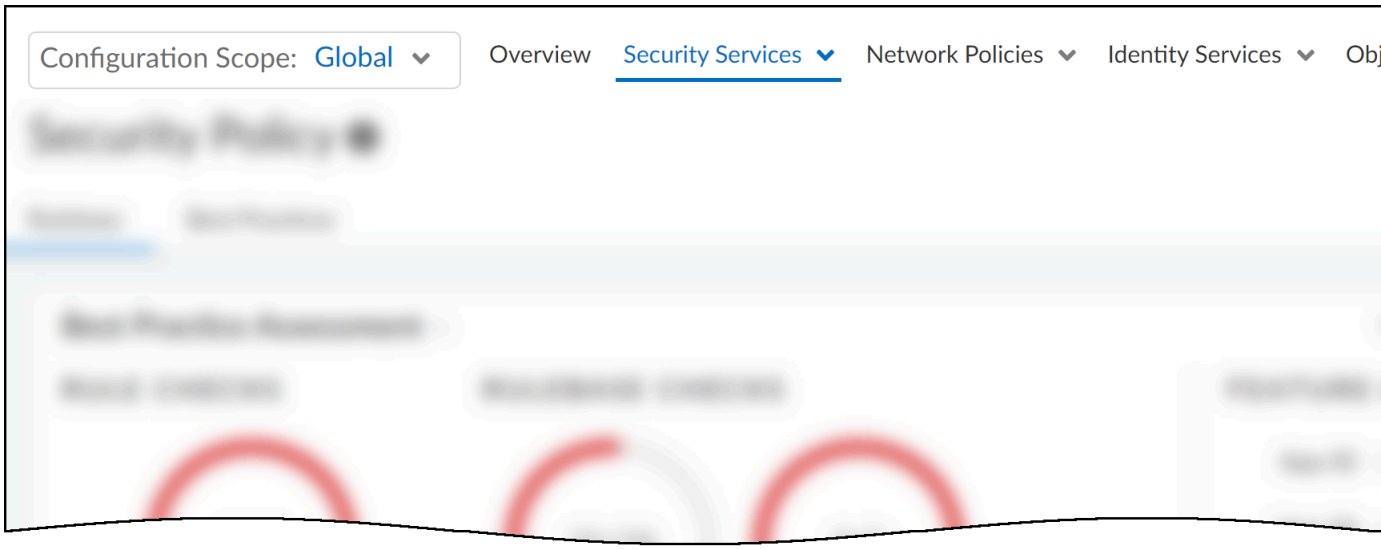
グローバルにポリシーを適用したり、Prisma Accessの導入環境や特定のファイアウォールグループに対して特定の設定を適用したりすることができます。

開始するのは、**[Manage (管理)] > [Configuration (設定)] > [NGFWとPrisma Access]**に進んでください。



- **NGFWとPrisma Access**への設定変更のプッシュ

  お使いのStrata Cloud Manager設定を管理する場合、［**Push Config (設定をプッシュ)**］を選択すると、NGFWとPrisma Accessに構成の変更をプッシュできます。



フォルダに基づいて設定プッシュの範囲を設定するよう求められます。ここでは、次の方法について詳しく説明します。

- 設定変更をプッシュする
- 設定のプッシュのステータスを確認する
- 設定のクリーンアップ方法を見る

Strata Cloud Managerに組み込まれているベストプラクティス

どこで使用できますか?	何が必要ですか?
• Software NGFW Creditsによって資金提供されたものを含むNGFW • Prisma Access (Managed by Panorama or Strata Cloud Manager) • Prisma SD-WAN	これらの各ライセンスには、Strata Cloud Managerへのアクセスが含まれています。 ❑ Prisma Access ❑ AIOps for NGFW Premium license (use the Strata Cloud Manager app) ❑ Prisma SD-WAN ❑ Strata Cloud Manager Essentials ❑ Strata Cloud Manager Pro → Strata Cloud Managerで利用できる機能は、使用するライセンスによって異なります。

Palo Alto Networksのベストプラクティスは、ネットワークインフラストラクチャのコンプライアンスチェックプロセスを効率化することで、可能な限り安全なネットワークを実現するように設計されています。Strata Cloud Managerに直接ベストプラクティスチェックが組み込まれていることから、設定をライブで評価できます。ベストプラクティスに沿ってセキュリティ態勢を引き締めます。Strata Cloud Managerを活用して、Panorama、NGFW、Panorama Managed Prisma Accessのセキュリティ設定をベストプラクティスに照らして評価し、失敗したベストプラクティスのチェックを修復できます。

ベストプラクティスのガイダンスは、セキュリティ体制を強化するだけでなく、環境を効率的に管理し、ユーザーの生産性を最大限に高めることを目的としています。これらのインラインチェックに対して設定を継続的に評価し、セキュリティを向上させる機会を見つけたら、その場でアクションを実行してください。

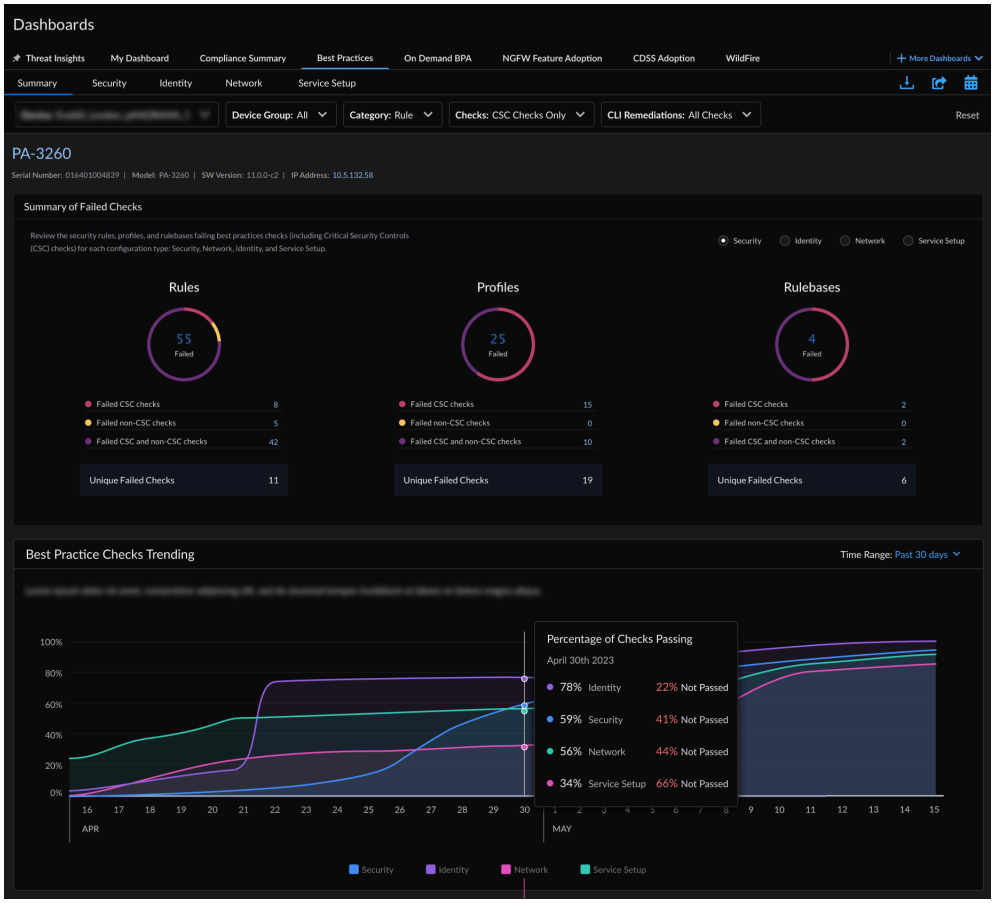
ベストプラクティスの導入とコンプライアンスの可視化

まず、以下の体制に関するダッシュボードを確認することで、セキュリティ態勢全般を迅速に評価できます。

高いレベルで進捗状況を確認し、アクションを起こし始めたいと思われる分野をピンポイントで特定します。

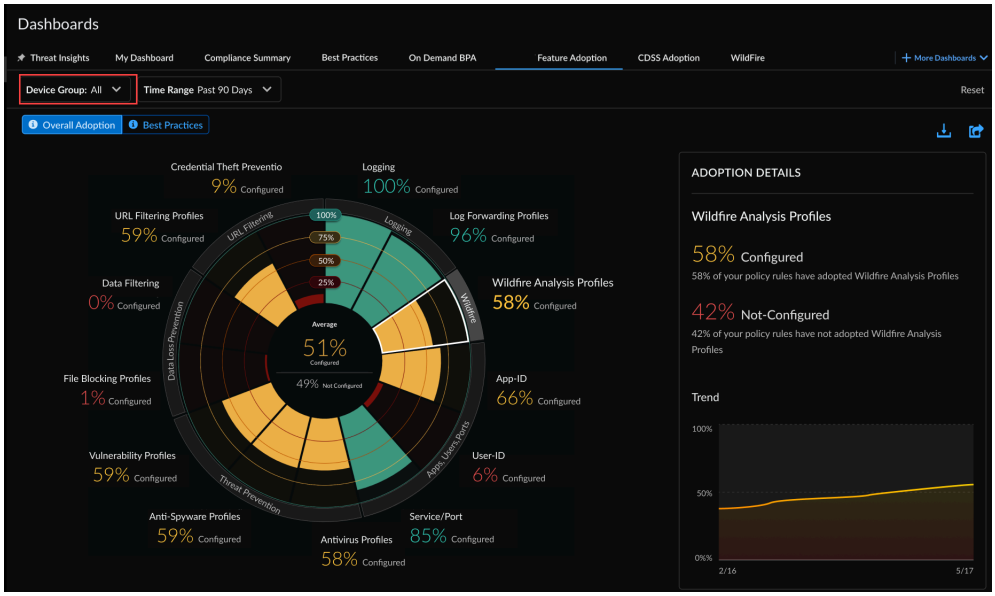
- ダッシュボード:ベストプラクティスダッシュボードで日々のベストプラクティスレポートを確認し、インターネットのセキュリティセンターの重要なセキュリティ管理（CSC）チェックとの対応付けを行うことで、ベストプラクティスのコンプライアンスを向上させるために

変更可能な領域を特定できます。ベストプラクティスレポートをPDFとして共有し、受信トレイに定期的に配信されるようにスケジュールします。

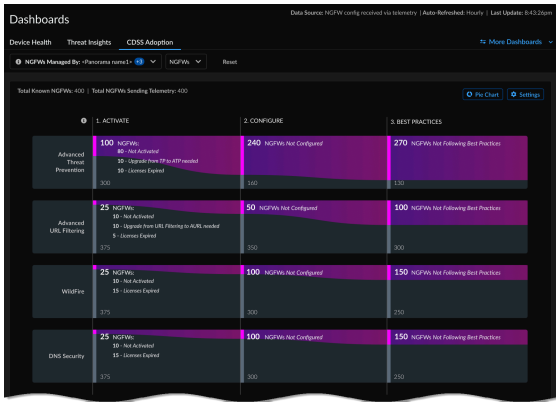


- コンプライアンス概要ダッシュボードを確認することで、インターネット セキュリティ センター (CIS) および 国立標準技術研究所 (NIST) のフレームワークごとにグループ化された、過去12か月までのセキュリティチェックの変更履歴を表示できます。

- ダッシュボード:機能の導入状況を監視し、デプロイメントで使用しているセキュリティ機能や、カバレッジのギャップの可能性を常に把握できます。



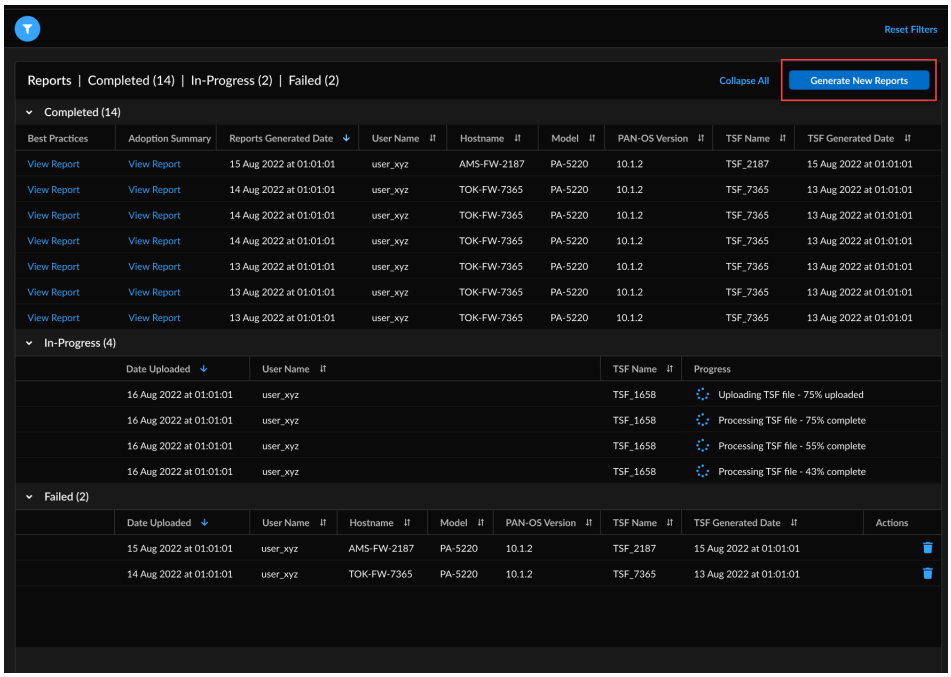
- ダッシュボード:CDSS の採用の監視 - デバイス内のセキュリティサービスまたは機能サブスクリプションとそのライセンス使用状況を表示して、セキュリティギャップを特定し、企業のセキュリティ体制を強化します。



- ダッシュボード:セキュリティ体制インサイトでオンボードされたNGFWデバイスのセキュリティ態勢に基づいて、デプロイメントのセキュリティステータスと傾向を可視化し、インシ

デントの発生時や、セキュリティ設定を詳細に確認する必要がある場合はアラートで通知します。

- バージョン9.1以降を実行している（テレメトリではない）PAN-OSデバイスのBPAレポートを生成し、機能の採用メトリックを含めるようになりました。



セキュリティ態勢を強化するベストプラクティスツール

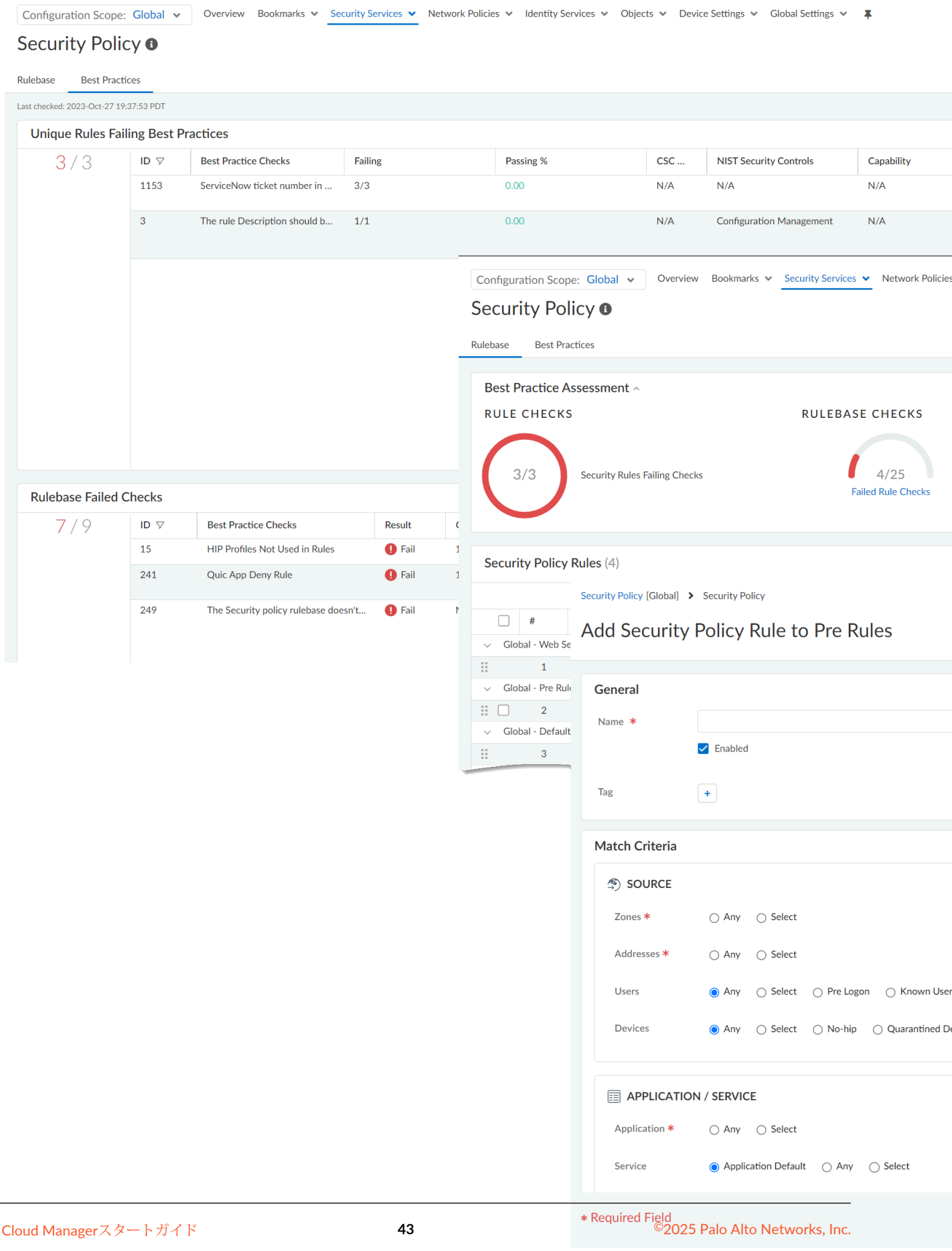
セキュリティ態勢の改善に役立つツール集を見つけることができます。

- デプロイメントのセキュリティ体制チェックをカスタマイズして、管理:セキュリティ体制の設定に関連する推奨事項を最大限に高めます。
- 設定クリーンアップを使用して、未使用の設定オブジェクトとポリシー規則を識別し、削除します。
- ポリシーオプティマイザ設定を構成して、許容しすぎるセキュリティルールを磨き、ネットワークで実際に使用されているアプリケーションのみを許可するように最適化します。

- 独自のコンプライアンスチェックの作成：既存のベスト・プラクティス・チェックをカスタマイズし、組織のビジネス要件により適合するように特別な免除を作成および管理します。
- Policy Analyzer (ポリシーアナライザ)を使用して、セキュリティ ポリシー ルールに対して行う更新は、要件に適合し、エラーや設定ミス（ルールの重複や矛盾を招くような変更）が発生しないようにする必要があります。

ライブ、インラインのベストプラクティス構成チェック

ベストプラクティスのガイダンスは、セキュリティ体制を強化するだけでなく、環境を効率的に管理し、ユーザーの生産性を最大限に高めることを目的としています。これらのインラインチェックに対して設定を継続的に評価し、セキュリティを向上させる機会を見つけたら、その場でアクションを実行してください。



- ベストプラクティススコア

  ベストプラクティススコアは、機能ダッシュボードに表示されます（セキュリティポリシー、復号化、URLアクセス制御など）。これらのスコアにより、ベストプラクティスの進捗状況が一目でわかります。一目で、さらに調査すべき領域や、セキュリティ態勢を改善するためにアクションを起こしたい領域を特定できます。

- ベストプラクティスのフィールドチェック

  フィールドレベルのチェックでは、構成がベストプラクティスと整合していない箇所を正確に確認できます。ベストプラクティスのガイダンスがインラインで提供されるため、すぐに対応できます。

- ベスト プラクティス アセスメント

  ここでは、機能の実装がベストプラクティスとどのように整合しているかを包括的に把握できます。失敗したチェックを調べて、改善できる箇所を確認します（合格したチェックを確認することもできます）。ルールベースのチェックでは、個々のルールの外部で、たとえば複数のルールにまたがって使用されるポリシーオブジェクトに対して実行できる設定変更が強調表示されます。

ベストプラクティスのチェックは以下でご利用いただけます。

- セキュリティ ポリシー ルール ベース

  ルールベースチェックは、セキュリティポリシーがどのように構成および管理されているかを調べます。これには、多くのルールに適用される構成設定も含まれます。

- セキュリティ ルール
- セキュリティ プロファイル
  - アンチスパイウェア
  - 脆弱性防御
  - WildFireおよびアンチウイルス
  - URL アクセス管理
  - DNS セキュリティ
- 認証
- 復号
- グローバルプロテクト

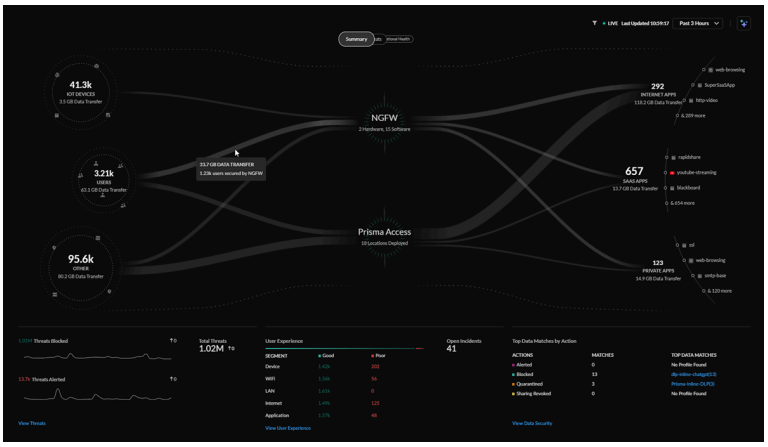
Palo Alto Networksのベストプラクティスの詳細をお求めですか？

ベストプラクティスのホームページでは、ベストプラクティスへの移行と実装に役立つリソースを提供しています。

コマンドセンター:ログ - Strata Cloud Manager

どこで使用できますか?	何が必要ですか?
• Prisma Access (Managed by Panorama or Strata Cloud Manager) • Software NGFW Creditsによって資金提供されたものを含むNGFW • Prisma SD-WAN	これらの各ライセンスには、Strata Cloud Managerへのアクセスが含まれています。 ❑ Prisma Access ❑ AIOps for NGFW Premium license (use the Strata Cloud Manager app) ❑ Strata Cloud Manager Pro ❑ Strata Cloud Manager Essentials ❑ Prisma SD-WAN コマンドセンターにアクセスするために必要なその他のライセンスと前提条件は次のとおりです。 ❑ Strata Logging Service ❑ コマンドセンター で特定のメトリックを表示する特定のライセンス。 ❑ コマンドセンターを表示する権限を持つロール → Strata Cloud Managerで利用できる機能は、使用するライセンスによって異なります。

Strata Cloud Manager Command Centerは、NetSecの新しいホームページです。ネットワークの健全性、セキュリティ、効率性を評価するのに役立つ、インタラクティブなビジュアルサマリーです。コマンドセンターはNetSecプラットフォームの統合ビューを提供し、ソース、アプリケーション、Prisma Accessの導入、NGFW、セキュリティサービスを1ヶ所で包括的に可視化します。



コマンドセンターでは、データを操作したり、ネットワーク上のイベント間の関係を視覚化したりできるため、セキュリティを強化するためにすぐにアクションを実行できます。

コマンドセンターは、新しい Activity Insightsダッシュボード （**Insights (インサイト) > Activity Insights**）と統合されており、オンボードライセンスやサブスクリプションで検出された異常を、実用的なインサイトを通じてハイライトし、その異常を修復するパスを提供します。

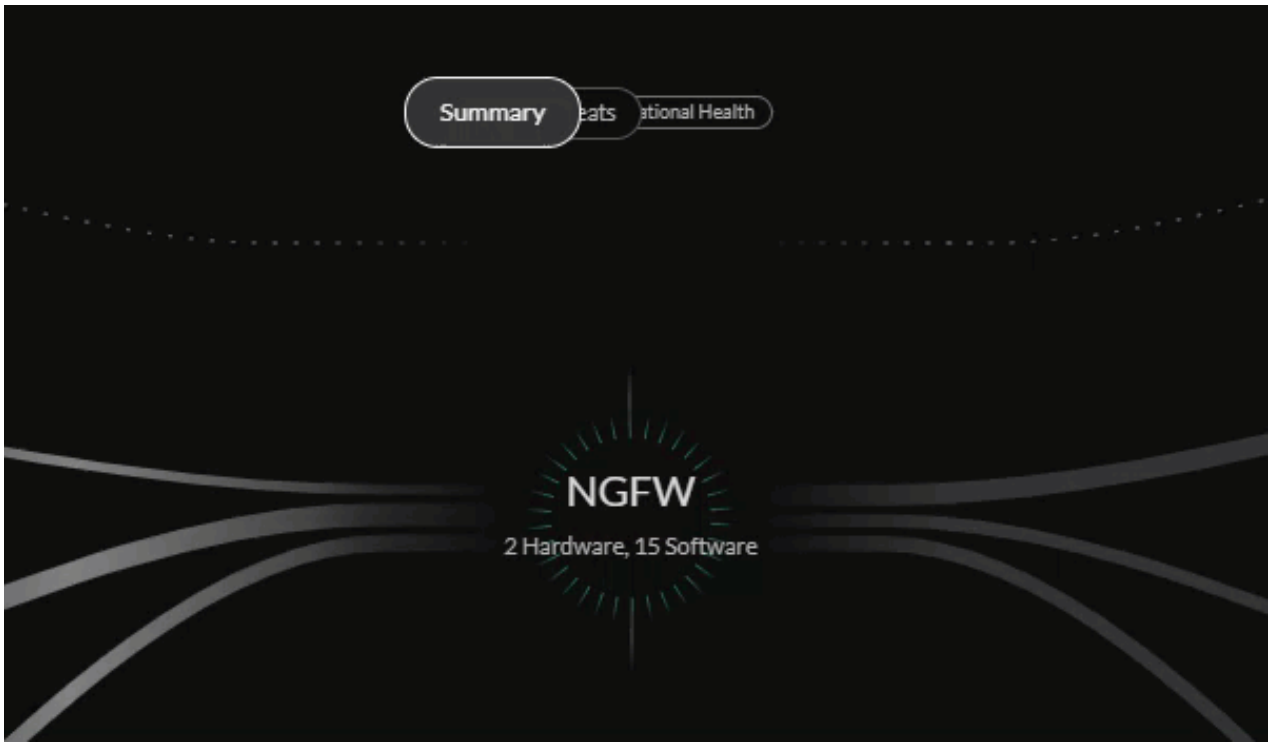
新しいホームページからは、次のことがわかります。

- ソース（ユーザー、IoT、外部ホスト）からアプリケーション（インターネット、SaaS、プライベート）に流れるネットワーク上のすべてのトラフィックを総合的に把握できます。
- ユーザー、デバイス、アプリケーションなどの資産がどのようにアクセスされ、保護されているか。
- コンテキストを含む特定のダッシュボードに移動して、ネットワークに影響を与える問題をより深く理解できます。
- ユーザーが作業中に発生する脅威の種類。

Strata Cloud Managerを起動し、**Command Center (コマンドセンター)**（）をクリックして開始します。

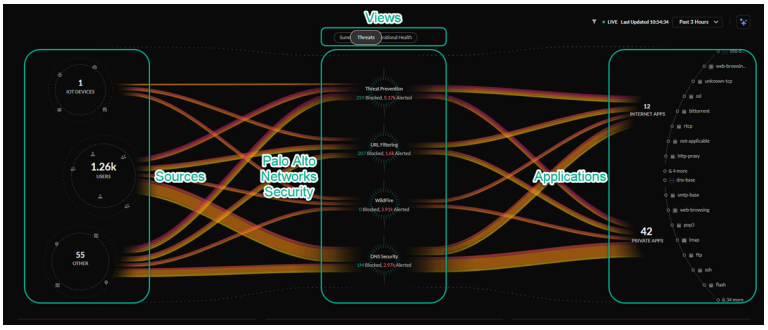
Strata Cloud Manager コマンドセンターと対話する方法

コマンドセンターの各ビューは、ネットワークの健全性とセキュリティを評価するために必要なすべての情報をきれいに分類します。



コマンドセンターのデータは5分ごとに更新され、デフォルトでは過去24時間のデータが表示されます。このデータは、過去1時間、3時間、7日、または30日でフィルタリングすることもできます。

各コマンドセンタービューには、Prisma AccessやNGFW、またはネットワーク上にデプロイされたセキュリティサブスクリプションを介して、ソースからネットワーク上のさまざまなアプリケーションに流れるさまざまな種類のビジュアルデータが表示されます。



Sourcesのバブル（ハイブリッドワーカー、オフィスユーザー、IoTデバイスなど）は左側、Applicationsのバブル（インターネット、SaaSによるアクセス、オンプレミスまたはクラウドでホストされている）は右側にあります。アプリケーションの吹き出しには、各カテゴリで使用頻度の高い上位3つのアプリケーションが表示されます。

送信元は以下が含まれます。

- **IoT**デバイス – 有効なIoTセキュリティライセンスによって検出され、有効になっているデバイス、
- ユーザー – リモートユーザーとブランチユーザー。
- その他 – インターネット上のリソースにアクセスする内部および外部のホスト。

次のようなアプリケーションがあります。

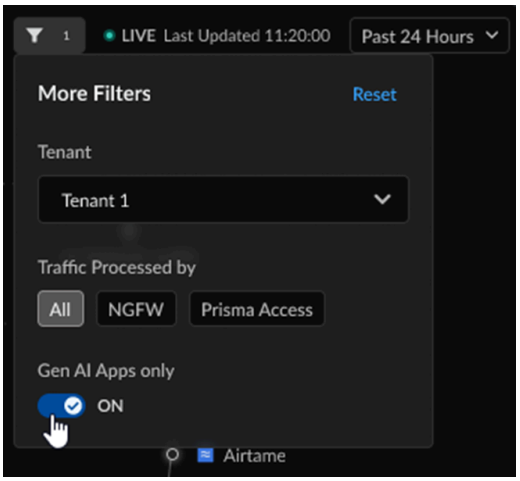
- インターネットアプリ – Webブラウザを使用してアクセスするアプリケーション。
- **SaaS**アプリ – アプリケーションサービスプロバイダが所有および管理するクラウドアプリ。
- プライベートアプリケーション – データセンターでホストされるアプリケーション。

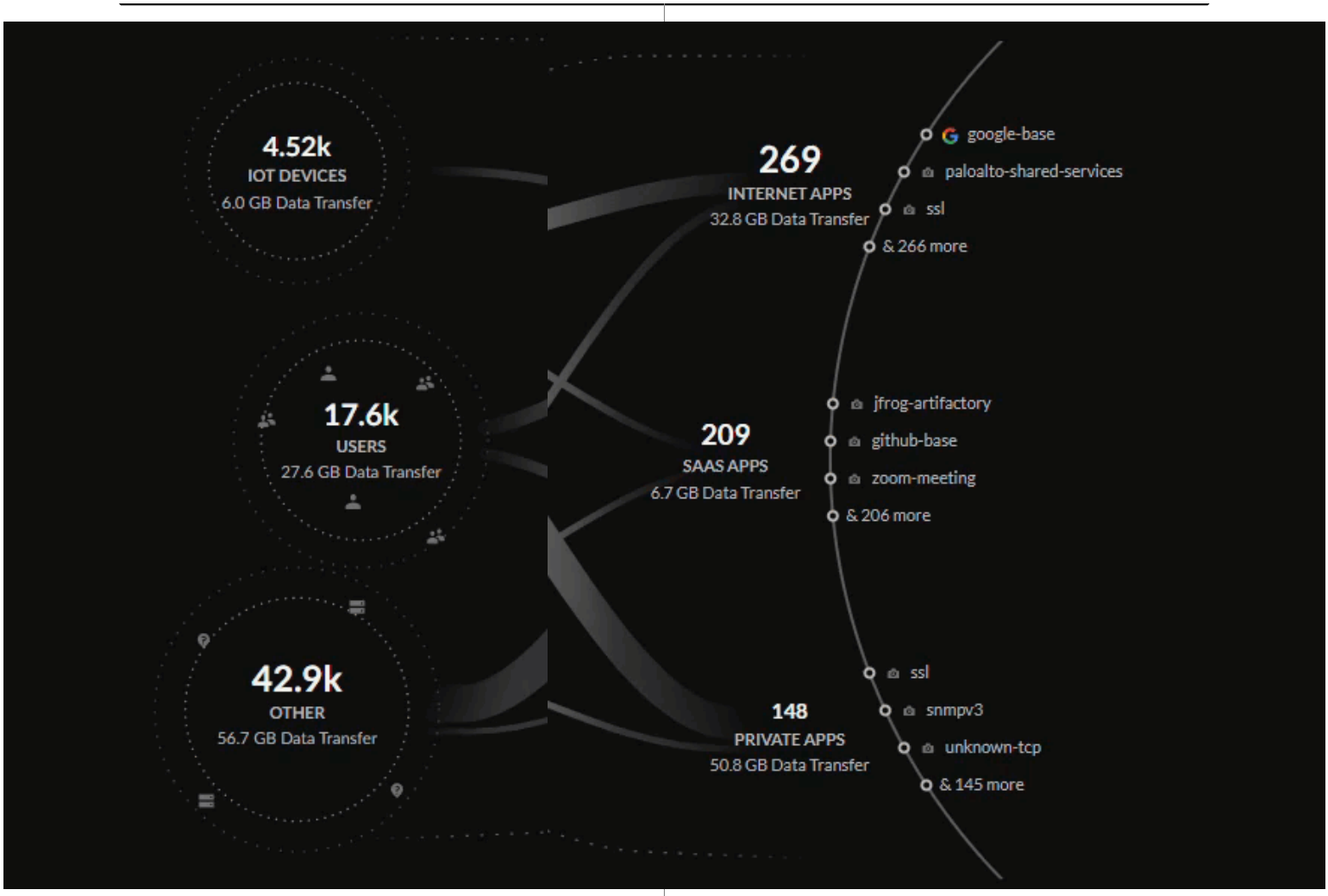
ソース、デプロイメント、またはアプリケーションのバブルをクリックすることで、中央ビューのデータをフィルタリングできます。これにより、選択したバブルに関連して、そのビューの追跡データをより詳細に表示できます。

フィルタ( )を選択すると、コマンドセンタービューのデータをテナントまたは**NGFW**、または**Prisma Access**固有のデータでフィルタリングできます。

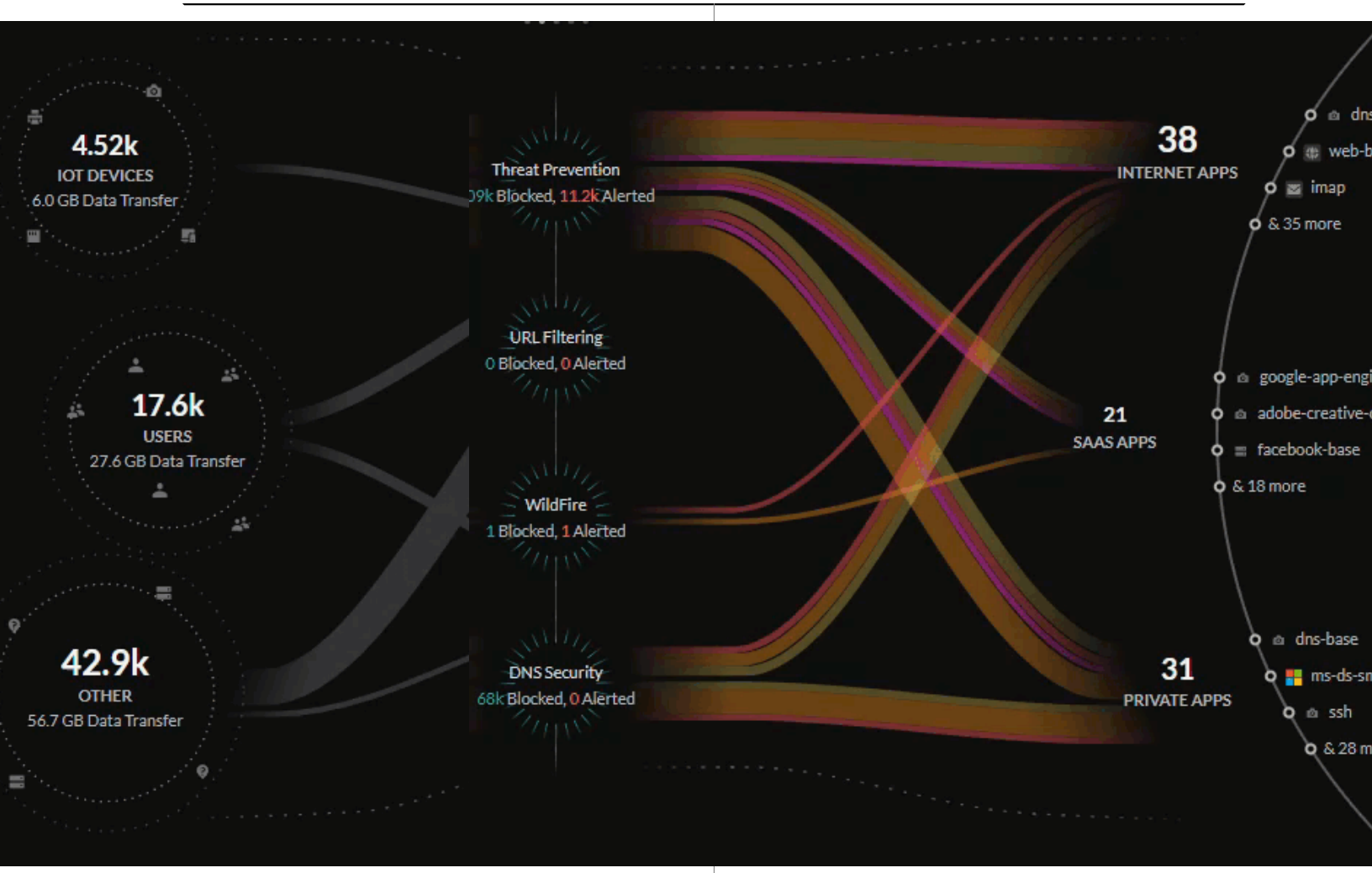
AI Accessライセンスでは、ネットワーク上のユーザーが使用しているGenAIアプリがデータセキュリティにどのような影響を与えているかをより適切に評価するために、**GenAI**アプリのみによってすべてのコマンドセンタービューのトラフィックをフィルタリングできます。

*AI*アクセスセキュリティおよび*AI*アクセスセキュリティのライセンスの詳細については、こちらをクリックしてください。

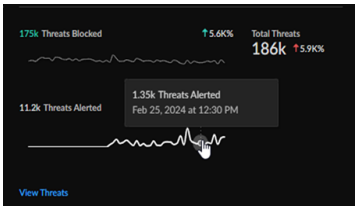




いずれかのビューを表示するときに、行の上にマウスを置くと、ネットワークに関する詳細情報（トラフィックや、ネットワーク上でブロックまたは許可される脅威など）が表示されます。



中央のビジュアルサマリーの下には、アクティベートされたサブスクリプションによって追跡されるいくつかの主要な指標があり、ネットワークに関する実用的なインサイトを提供します。これらの主要な指標は、浮上した指標に関する詳細情報や、考えられる解決策をドリルダウンできる、いくつかの詳細なコンテキストページのいずれかに移動する機能を提供します。



Strata Cloud Managerのコマンドセンタービュー

コマンドセンターには、4つの異なるビューがあり、それぞれに追跡データとメトリックがあり、検証や操作を行うことができます。

- 概要
- 脅威
- 運用状態
- データセキュリティ

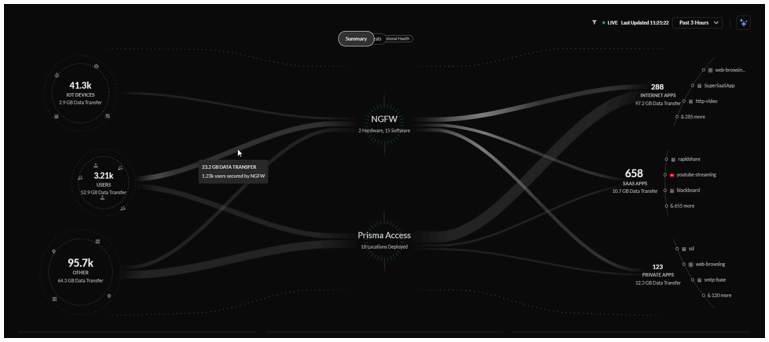
コマンドセンター(概要)

サマリービューには、ユーザー、外部ホスト、IoTデバイス、アプリケーションからのすべてのトラフィックの概要が表示され、他のビューでスポットライトが当たっているネットワーク上の問題や異常の一部のプレビューも表示されます。このビューは、毎日のネットワークの健全性を最初に調べるときに使用できます。

概要ライセンス	• Strata Command Centerを使用するには、Strata Logging Serviceライセンスに付属する次のライセンスのうち少なくとも1つが必要です。
	  ❑ Prisma Accessライセンス
	  ❑ AIOps for NGFW Premiumライセンス
	• またはAIOPs for NGFW FreeライセンスとStrata Logging Serviceライセンス
	• 概要ビューでの追加メトリックに必要なライセンス:
	  ❑ クラウド提供型セキュリティサービス（CDSS）サブスクリプション
	  ❑ Data Securityサブスクリプション
	  ❑ ADEMライセンス
	  ❑ AIアクセスライセンス

中央サマリービュー

中央サマリービューでは、IoTデバイス、ユーザー、インターネットからリソースにアクセスする外部ホスト、インターネットアプリ、SaaSアプリ、ネットワーク上のプライベートアプリの間で転送されているデータを確認できます。



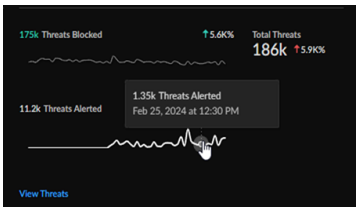
中央サマリービューの線は、ネットワーク上のデータ転送とトラフィックを表します。線の太さは、ソースおよびアプリケーションから転送されるデータ量を表します。

これらのソースがネットワークインフラストラクチャによってどのように保護されているかを確認できます。

- Prisma Access導入
- Strata Logging Serviceインベントリからの次世代ファイアウォール

脅威合計数

［**Total Threats Count (**脅威合計数**)**］ウィジェットでは、ネットワークで検出された脅威の総数、ブロックされた脅威の数、警告された脅威の数、および選択した時間範囲からの脅威の変化を簡単に確認できます。



[アクティビティ インサイト]画面**([Insights (**インサイト**)] > [Activity Insights (**アクティビティに関するインサイト**)] > [Threats (**脅威**)])**をクリックすると、ネットワーク上の脅威の詳細が表示されます。

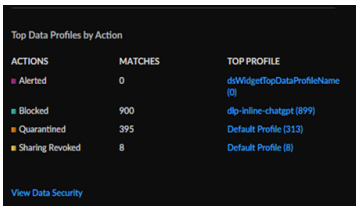
未解決のインシデントとユーザーエクスペリエンス

［**Open Incidents and User Experience ((**オープンインシデントとユーザーエクスペリエンス**)**］ウィジェットでは、オープンインシデントの合計数、ユーザーデバイスからアプリケーションへのサービス配信チェーンの個々のセグメントから、良好または劣化の可能性があるユーザーエクスペリエンスの内訳、選択した時間範囲からのオープンインシデントの変化を確認できます。

アプリケーション エクスペリエンス ダッシュボード**([Dashboards (**ダッシュボード**)] > [Application Experience (**アプリケーションエクスペリエンス**)])**をクリックして、ネットワーク全体の正常性とユーザーエクスペリエンス、およびパフォーマンスメトリクスの詳細な内訳を確認してください。

アクション別上位データプロファイル

［**Top Data Profiles (**上位データプロファイル**)**］ウィジェットでは、定義済みデータ フィルタリング プロファイルの上位、ネットワーク・トラフィックで見つかった一致数、およびそれらのデータ プロファイルに基づいて機密データに対して実行されるアクションを確認できます。

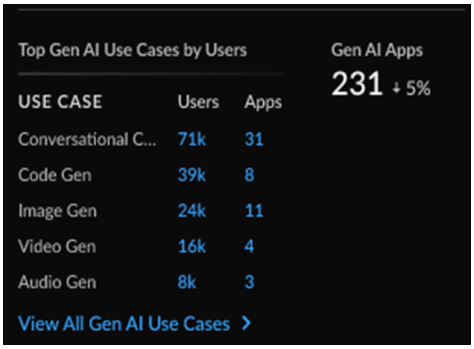


ネットワーク上の機密データのより詳細な内訳については、データセキュリティビュー(**[Command Center (コマンドセンター)] > [Data Security (データセンター)]**)をクリックしてください。

ユーザーとGenAIアプリの主なGenAIユースケース

[Top GenAI Use Cases by User (ユーザー別トップGenAIユースケース)]ウィジェットでは、ネットワーク上のユーザーが利用しているGenAIアプリの上位ユースケース、各ユースケースのユーザー数、各ユースケースに該当するGenAIアプリの量を確認できます。

また、ネットワーク上のGenAIアプリの総数や、時間フィルターに基づいたアプリのシフト率も確認できます。



Activity InsightsのAI Access Securityダッシュボード**(Insights (インサイト) > AI Access)**をクリックすると、ネットワーク上でのGenAIアプリの導入に関する詳細な内訳と、データをより安全に保護するための推奨事項が表示されます。

*AI Access Security*の詳細と、組織がデータセキュリティのリスクを軽減しながら*GenAI*アプリケーションを安全に導入する方法については、こちらをご覧ください。

脅威

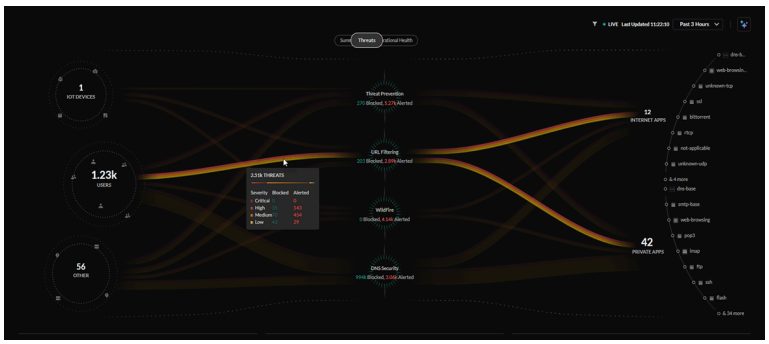
脅威ビューには、ネットワーク上で検査されたトラフィックと、CDSSサブスクリプションによって検出された脅威が表示されます。このビューを使用して、ネットワーク上のブロックおよび警告された脅威を監視したり、警告された脅威をより適切にブロックするためにポリシーの更新が必要なネットワーク領域を調査したりできます。

脅威ライセンス	• 脅威ライセンス(を含む)
	  ❑ Threat Prevention license (脅威防御ライセンス)
	  ❑ URL Filtering license (URLフィルタリングライセンス)
	  ❑ WildFireライセンス
	  ❑ DNS Securityライセンス

Central Threats View (中央脅威ビュー)

[中央脅威］ビューでは、アクティブなクラウド提供セキュリティサービスサブスクリプションによって特定されたネットワーク上のすべての脅威を確認できます。

脅威ビューには、Palo Alto NetworksのCDSSサブスクリプションが、ネットワーク上の潜在的な脅威を監視することでトラフィックをどのように保護しているかが表示されます。コマンドセンターでは、IoTデバイス、ユーザー、アプリケーションの検査トラフィックの割合、および許可または警告された脅威の総数を把握できます。

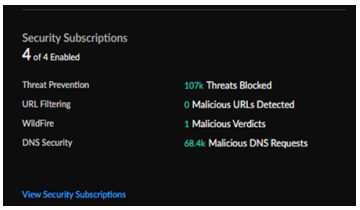


中央の脅威ビューの線は、セキュリティサブスクリプションによって監視されているトラフィックを表し、太さは検出された脅威の量を表し、色は脅威の重大度が重大、高、中、低のいずれかであることを示します。

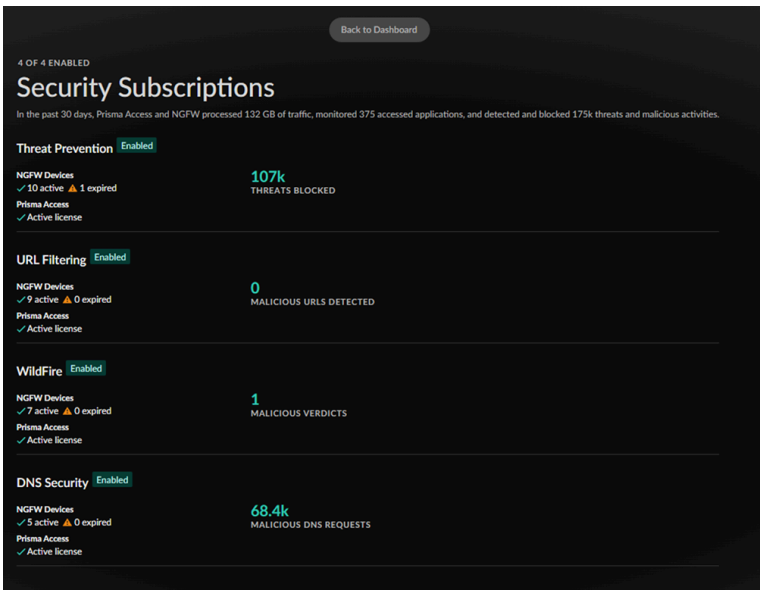
セキュリティ サブスクリプション

［セキュリティサブスクリプション］ウィジェットでは、クラウド提供のセキュリティサブスクリプション、アクティブなサブスクリプション、およびネットワークのセキュリティ保護のスナップショットを確認できます。

サブスクリプション	説明
脅威の防止	脅威の防止は、広範囲に及ぶが洗練されていないコモディティの脅威と、組織化されたサイバー攻撃者によって永続する標的型で高度な脅威の両方からネットワークを保護します
URLフィルタリング	高度なURLフィルタリングは、Webベースの脅威からネットワークとユーザーを保護する包括的なURLフィルタリングソリューションです。
WildFire	クラウドで提供されるWildFireマルウェア分析サービスは、業界最大のグローバルコミュニティのデータと脅威インテリジェンスを使用し、高度な分析を適用して未知の脅威を自動的に特定し、攻撃者の追跡を阻止します
DNSセキュリティ	Palo Alto NetworksのDNSセキュリティサービスを利用すると、DNSトラフィックを自動的にセキュリティで保護します。

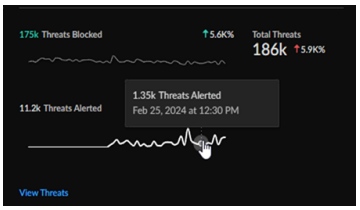


Security Subscriptionsウィジェット(**[Command Center (コマンドセンター)] > [View Security Subscriptions (セキュリティ契約を見る)]**)をクリックすると、NGFWとPrisma Accessの展開に関連するサブスクリプションのステータスの詳細なレポートが表示されます。［**Back to the Dashboard (ダッシュボードに戻る)**］ をクリックして、［**Threats (脅威)**］ ビューに戻ります。



脅威合計数

［**Total Threats Count (**脅威合計数**)**］ウィジェットでは、ネットワークで検出された脅威の総数、ブロックされた脅威の数、警告された脅威の数、および選択した時間範囲からの脅威の変化を簡単に確認できます。



[Activities Insights (アクティビティ インサイト)]**([Insights (**インサイト**)] > [Activity Insights (**アクティビティに関するインサイト**)] > [Threats (**脅威**)])**をクリックすると、ネットワーク上の脅威の詳細が表示されます。

脅威のブロックと警告

［**Blocked and Alerted Threats (**ブロックされた脅威と警告された脅威**)**］ウィジェットでは、ネットワークで検出されている脅威を、カテゴリ、脅威レベル（重大、高、中、低）、および脅威がブロックまたは警告されているかどうかで整理し、トップダウンで表示できます。

ネットワークに影響を与えるすべての脅威の詳細な表 （**[Insights (**インサイト**)] > [Activity Insights (**アクティビティインサイト**)] > [Threats (**脅威**)]**）を参照するには、 こちらをクリックしてください。

運用状態

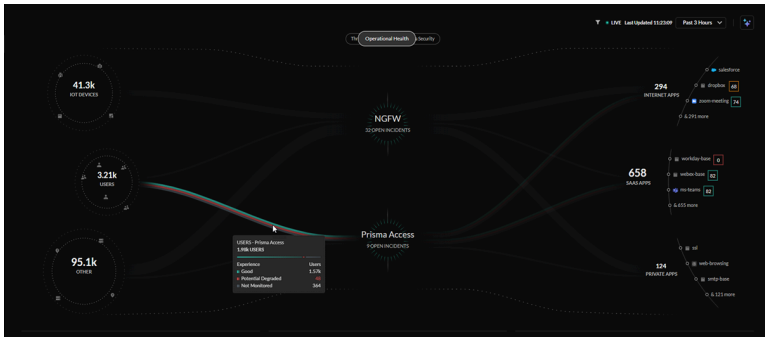
Operational Healthビューには、ネットワーク上のインフラストラクチャの正常性とユーザーエクスペリエンスが表示されます。このビューを使用して、NGFWやPrisma Accessのデプロイメント状況、ネットワーク上のユーザーエクスペリエンスを監視し、各領域の未解決インシデントの重大度を確認できます。

運用状態ライセンス	• 次のようなサブスクリプションの監視: ▫ ADEMオブザーバビリティ ▫ AI搭載ADEM ▫ AIOps for NGFW Premium

Central Operational Healthビュー

［Central Operational Health］ビューでは、インフラストラクチャの正常性とネットワーク上のユーザーエクスペリエンスを確認できます。ユーザーがAutonomous Digital Experience Management（ADEM）ライセンスを持っている場合、このビューで拡張データを受け取ることができます。

Operational Healthビューには、Palo Alto Networks ADEMサブスクリプションが、SASE環境内のすべてのユーザーとアプリケーションにわたるデジタルエクスペリエンスを監視する方法が表示されます。



central Operational Healthビューの線は、ネットワーク上のすべてのユーザを表します。ユーザーはユーザーエクスペリエンススコアによって分類され、線の色は「good」「poor」「監視されていない」の評価を表します。

未解決のインシデントおよびインシデントの重大度別合計

［**Open Health Incidents by Severity (**オープン正常性の重大度別インシデント**)**］ウィジェットでは、ネットワーク上のすべての未解決インシデントを、スコープ（NGFW、Prisma Access、Prisma SD-WAN ） 、 重大度、インシデント数別に表示できます。

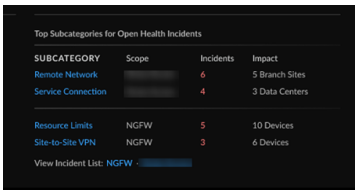
ウィジェットは、選択した期間に基づいて、未解決インシデントの変化率を追跡します。

インシデントとアラートダッシュボードをクリックして、利用可能な各スコープを表示します(**[Incidents and Alerts (インシデントとアラート)] > [Prisma Access / NGFW] > [All Incidents (すべてのインシデント)]**)。

オープンヘルスインシデントの上位サブカテゴリ

[Top Subcategories for Open Health Incidents (オープン正常性インシデントのトップサブカテゴリー)] ウィジェットを使用すると、ネットワーク上のオープンヘルスインシデントの上位サブカテゴリを、範囲、サブカテゴリ、インシデントの量、および影響を受けるもの（データセンター、サイト、デバイスなど）ごとに整理して表示できます。

ウィジェットには、1つのスコープの上位5つのサブカテゴリが表示されます。複数のスコープがある場合は、上位2つのサブカテゴリが表示されます。



インシデントの詳細を確認するには、[Incidents and Alerts(インシデントとアラート)]ダッシュボードをクリックしてください(**Incidents and Alerts (インシデントとアラート) > Prisma Access / NGFW / Prisma SD-WAN**)。

監視対象ユーザーとユーザーエクスペリエンス

［**Open Incidents and User Experience ((オープンインシデントとユーザーエクスペリエンス)**］ウィジェットでは、オープンインシデントの合計数、ユーザーデバイスからアプリケーションへのサービス提供チェーンの個々のセグメントから、良好または劣化の可能性があるユーザーエクスペリエンスの内訳、選択した時間範囲からのオープンインシデントの変化を確認できます。

ネットワーク全体の経験値のより詳細な内訳については、アプリケーション エクスペリエンス ダッシュボード(**[Dashboards (ダッシュボード)] > [Application Experience (アプリケーションエクスペリエンス)]**) をクリックしてください。

ベストプラクティス

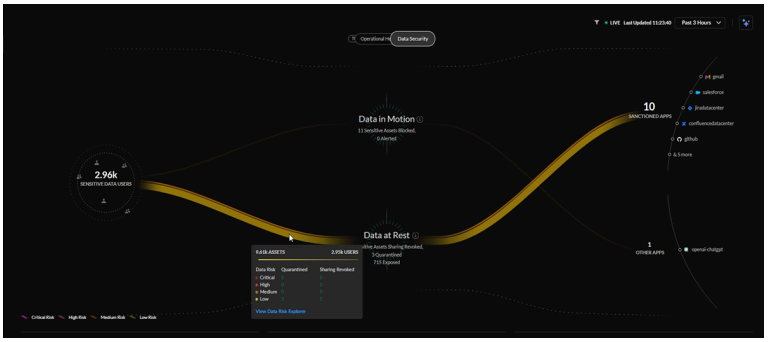
データセキュリティ

データ セキュリティ ビューには、ネットワーク全体および接続されたさまざまな SaaS アプリケーションで検出されたすべての機密データが表示されます。これを使用して、組織内のリスクの高い機密データ フローを監視および識別できます。

データセキュリティライセンス	• データ セキュリティ ライセンスには以下が含まれます: ❑ SaaS セキュリティ ライセンス ❑ データ セキュリティ ライセンス ❑ エンタープライズ DLP ライセンス

中央データセキュリティビュー

中央のデータ セキュリティ ビューでは、ネットワーク全体および接続された SaaS アプリケーション全体の機密性の高い高リスク データ マップが提供されます。コマンド センターでは、組織内の機密データ ユーザー、機密データ アクティビティ (資産のアップロード、ダウンロード、または資産の公開) が検出された特定の承認済み、承認されていない、許容されている、またはタグ付けされていないアプリケーション、および許可、ブロック、隔離、共有取り消し、または公開された資産の数に関する分析情報が提供されます。

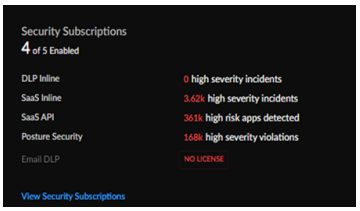


中央のデータ セキュリティ ビューの線は、保存データと移動データのセキュリティ ソリューションを通じて検出された機密データを表します。線の太さはデータの量を表し、色はそのデータがフラグ付けされているか、または重大、高、中、低のリスクとして分類されているかを表します。

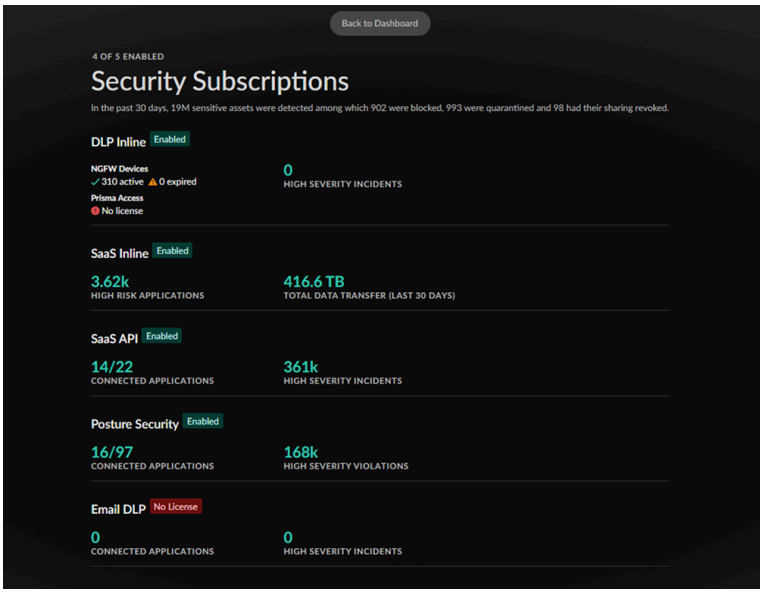
セキュリティ サブスクリプション

セキュリティ サブスクリプション ウィジェットでは、データ セキュリティ サブスクリプション、アクティブなサブスクリプション、およびサブスクリプションによってネットワークがどのように保護されているかのスナップショットを確認できます。

サブスクリプション	説明
DLP インライン	エンタープライズ DLP は、教師あり機械学習アルゴリズムを使用して機密文書をカテゴリに分類し、漏洩、データ損失、データ流出を防ぐクラウドベースのサービスです。
SaaS インライン	SaaS InlineソリューションはStrata Logging Serviceと連携し、ネットワーク上で使用されているすべてのSaaSアプリケーションを検出する。
SaaS API	SaaS API は、クラウド アプリの API を使用して承認された SaaS アプリケーションに直接接続し、アプリケーション内でのデータ分類、共有または権限の可視性、脅威の検出を提供できるクラウドベースのサービスです。
姿勢セキュリティ	SaaS セキュリティ ポスチャ管理 (SSPM) は、継続的な監視を通じて、承認された SaaS アプリケーション内の誤った設定を検出し、修正するのに役立ちます。
Email DLP (電子メールDLP)	Email DLPは、AI/MLを活用したデータ検出により機密情報を含むメールの流出を防ぐ Enterprise DLP(エンタープライズDLP)のアドオンです。



[Security Subscriptions (セキュリティ サブスクリプション)] ウィジェット **(コマンド センター > セキュリティ サブスクリプションの表示)** をクリックすると、NGFW および Prisma Access の展開に関連するサブスクリプションのステータスの詳細なレポートが表示されます。**[Back to the Dashboard (ダッシュボードに戻る)]** をクリックして、 **[Data Security (データ セキュリティ)]** ビューに戻ります。



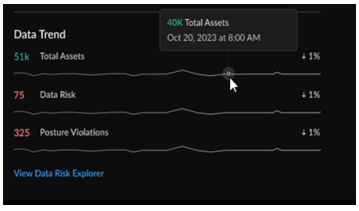
トップデータプロファイル

Top Data Profiles (トップ データ プロファイル**)** ウィジェットには、検査されたすべての機密データで検出されたトップ データ プロファイル、データ プロファイルの重大度、および移動中のデータと保存中のデータでインライン検出された資産一致の数が表示されます。

[Data Loss Prevention (データ損失防止**)]** ダッシュボード **(Manage (**管理**) > Configuration (**設定**) > Data Loss Prevention (**データ損失防止**))** をクリックして、すべての定義済みデータ プロファイルを確認し、カスタム データ プロファイルを追加します。

データトレンド

データ トレンド ウィジェットには、データ セキュリティ サブスクリプションによって監視されている機密データのトレンドが、総資産、データ リスク、およびポスチャ違反の変化率別に表示されています。



データ リスク ダッシュボード **(Manage (**管理**) > Configuration (**設定**) > Data Loss Prevention (**データ損失防止**) > Data Risk (**データリスク**))** をクリックして、全体的なデータ リスク スコアを理解し、組織のデータ セキュリティ体制を改善するための実用的な推奨事項を確認します。

インサイト（知見）:アクティビティに関するインサイト

どこで使用できますか?	何が必要ですか?
• Prisma Access (Managed by Panorama or Strata Cloud Manager) • Software NGFW Creditsによって資金提供されたものを含むNGFW • Prisma SD-WAN	これらの各ライセンスには、Strata Cloud Managerへのアクセスが含まれています。 ❑ Prisma Access ❑ AIOps for NGFW Premium license (use the Strata Cloud Manager app) ❑ Prisma SD-WAN ❑ Strata Cloud Manager Essentials ❑ Strata Cloud Manager Pro Activity Insightsの特定のビューにアクセスするために必要なその他のライセンスと前提条件は次のとおりです。 ❑ Strata Logging Service ❑ クラウド提供セキュリティサービス (CDSS) ❑ ADEM Observability (ADEMの可観測性) ❑ WAN Clarity Reporting (WAN クラリティレポート) ❑ ダッシュボード を表示する権限を持つロール → Strata Cloud Managerで利用できる機能は、使用するライセンスによって異なります。

Activity Insights(アクティビティに関するインサイト)では、Prisma AccessやNGFWのデプロイメント全体にわたるネットワークアクティビティを詳細に把握できます。このビューは、ネットワークトラフィック、アプリケーションの使用状況、脅威、ユーザーアクティビティなどのネットワークデータを1か所に統合します。Activity Insightsは、可視化、監視、レポート作成の機能を提供し、タスクを簡単に実行できます。Strata Cloud Manager Command Centerでフォーカスが必要な領域を特定したら、コンテキストリンクを使用してActivity Insightsまたはその他のダッシュボードに移動し、さらに分析します。

Activity Insightsには高度なフィルタ機能があり、導入環境にとって重要なセキュリティ面に集中できます。Activity Insightsの高度なレポート機能を使用すると、［Overview (概要)］タブのデータからレポートをダウンロード、共有、スケジュールできます。レポー

トでは、ダッシュボードで適用されたフィルタごとにデータが別々に表示されます。または、**Strata Cloud Manager** > [レポート]メニューからActivity Insightsとダッシュボードのレポートをスケジュールすることもできます。

Strata Cloud Managerを起動し、**[Insights (インサイト)]**（  ）をクリックして開始します。

Activity Insightsでは何が表示されますか。

Activity Insightsは、Prisma AccessおよびNGFW環境に導入されたStrata Logging Serviceテナントごとの集計データを表示します。特定のデプロイメントに対してデータをフィルタリングできます。Activity Insightsにはさまざまなタブがあります。これらの各タブでは、アプリケーション、ユーザ、脅威、URL、ネットワーク使用状況に関連するネットワークデータを統合的に表示できます。

- 概要 - アプリケーション、脅威、ユーザ、URL、セッションのデータと、選択した時間範囲内に含まれるアクティビティの最大数を表示します。このビューを手早く見ることで、ネットワーク内の不正行為をすばやく特定し、さらに掘り下げて調査が必要なアクティビティを検証できます。
- アプリケーション - データ転送、アプリケーションリスク、アプリケーションエクスペリエンスを監視するADEM機能など、ネットワーク内のすべてのアプリケーション使用状況の概要。
- **SD-WANアプリケーション** - Prisma SD-WANアプリケーションのパフォーマンスを、時間範囲の正常性スコア、トランザクション統計、帯域幅使用率メトリックの詳細とともに表示します。
- 脅威 - Palo Alto Networksのセキュリティサービスが検出し、ネットワーク内でブロックしたすべての脅威の総合的なビューを提供します。
- ユーザー - ユーザーエクスペリエンスを監視するADEMの機能を含む、ユーザーのトラフィックとアクティビティに関するより深い洞察を提供します。
- **URL** - ネットワークでアクセスされたURL、そのうちの何件が悪意のあるものであるか、URLにアクセスしているユーザーとアプリケーション、ネットワーク内のURLを許可するルール、セキュリティサービスによる強制が表示されます。
- ルール - ユーザやアプリケーションによって生成されるトラフィックを許可するセキュリティポリシールール、トラフィックセッションで検出された脅威、ルールに影響を与えるURLに関するインサイトを提供します。
- リージョン - アプリケーション、ユーザ、脅威、およびURLに関連するネットワークトラフィックの詳細を示します。

管理画面のデータはどのように利用できますか？

ここを見つけることで 助けになる

- 監視するアプリケーションを特定し、スコアの低いアプリケーションのユーザーエクスペリエンスを向上させ、認可されていない危険なアプリケーションを制御します。
- 展開に最も関連性の高い脅威を表示し、調査のために脅威のコンテキストを取得します。
- ログからの発見事項に基づいてセキュリティポリシールールとトラフィックルールを絞り込み、セキュリティギャップを解消します。

- ユーザーのアクティビティを監視して潜在的な脅威を検出および阻止し、機密情報の悪用を防止します。

アクティビティに関するインサイト:概要

どこで使用できますか?	何が必要ですか?
• Prisma Access (Managed by Panorama or Strata Cloud Manager) • Software NGFW Creditsによって資金提供されたものを含むNGFW • Prisma SD-WAN	これらの各ライセンスには、Strata Cloud Managerへのアクセスが含まれています。 ❑ Prisma Access ❑ AIOps for NGFW Premium license (use the Strata Cloud Manager app) ❑ Prisma SD-WAN ❑ Strata Cloud Manager Essentials ❑ Strata Cloud Manager Pro Activity Insightsの特定のビューにアクセスするために必要なその他のライセンスと前提条件は次のとおりです。 ❑ Strata Logging Service ❑ クラウド提供セキュリティサービス (CDSS) ❑ ADEM Observability (ADEMの可観測性) ❑ WAN Clarity Reporting (WAN クラリティレポート) ❑ ダッシュボード を表示する権限を持つロール → Strata Cloud Managerで利用できる機能は、使用するライセンスによって異なります。

選択した期間、ネットワーク内で最も多く見られたアプリケーション、脅威、ユーザ、URL、およびルールの概要を表示します。このビューを手早く見ることで、ネットワーク内の不正行為をすばやく特定し、さらに掘り下げて調査が必要なアクティビティを検証できます。[Overview (概要)]ビューには、次の項目が含まれます。

- セッション数、データ転送数、検出された脅威、アクセスされたURL、アプリケーションにアクセスしたユーザ数の観点から、ネットワーク内で最大のアクティビティを持つアプリケーションおよびアプリケーションカテゴリの上位5つ。アプリケーションの詳細を参照するには、**[View all Applications (すべてのアプリケーションを表示)]**をクリックします。

- セッション、ユーザ、およびアプリケーションに最も影響を与えている上位5つの脅威と脅威カテゴリ。セッション、ユーザ、およびアプリケーションの詳細をそれぞれログビューア、ユーザタブ、アプリケーションタブで表示します。

- ブロック、許可、警告されたセッションのネットワークトラフィックの傾向、データ転送量、および最も多くのトラフィックを生成しているユーザ。

- トラフィックセッション数の多い上位5ユーザー、データ転送量、トラフィックで見つかった脅威、アクセスされたURL、監視対象アプリケーションのユーザーエクスペリエンススコア。
- セッション、ユーザー、URLにアクセスするアプリケーションの詳細とともに、最もアクセスされたURL。

- 導入環境に設定されているセキュリティ ポリシー・ルールのうち、最も影響を受ける上位5つのルール。ルールに一致するトラフィックに関係するセッション、ユーザー、URL、脅威、データ転送、アプリケーションを知るためのフィルタが用意されています。

フィルタを使用して、環境に注目し、関連するデータポイントを表示できます。これらのフィルタはダッシュボードのすべてのタブで使用できます。

フィルタ

Activity Insightsには高度なフィルタ機能があり、導入環境にとって重要なセキュリティ面に集中できます。使用できるフィルタは次のとおりです。

- 時間範囲 - 指定した期間のデータを表示する
- スコープの選択 - 導入環境に固有のデータ:Prisma Access、NGFW
- サブテナント - データが表示されるプリズマアクセスインスタンス
- ユーザー名 - 個々のユーザーが関与するアクティビティの表示
- アプリケーション - 特定のアプリケーションに関するネットワークイベント
- アプリケーションタイプ - アプリケーションのタイプ (SaaS、インターネット、プライベート)
- 脅威カテゴリ - 特定のカテゴリの脅威のデータ
- 脅威処理 - 許可またはブロックされた脅威に固有のビュー
- **URL**リスクレベル - 特定のリスクレベルを持つURLに関するデータ。高、中、低
- **URL**カテゴリ - URLカテゴリに基づいてデータをフィルタリング
- ソースの場所 - 特定の場所から発信されたアクティビティの表示
- デスティネーションロケーション - 特定の地域を対象としたアクティビティの表示
- **URL** - アクセスされた特定のURLに関連するアクティビティ。

- **SaaS**アプリケーション - 特定のSaaSアプリケーションに関するデータ
- 認可済みアプリケーション - 認可済みまたは認可されていないアプリケーションのみのデータを表示する
- ポートタイプ - 標準ポートまたは非標準ポートを通過するアプリケーションからのトラフィックをソートします。
- プロトコル - 特定のTCP、UDP、またはHTTPポートを使用するトラフィックを参照
- ソースタイプ - 特定のデバイス、ユーザー、またはその他から生成されたアクティビティを表示します。

レポート

アイコンの1つである**[Overview (概要)]**タブの[]をクリックすると、**[Overview (概要)]**タブのデータからレポートをダウンロード、共有、スケジュールできます。**Strata Cloud Manager** > **[Reports (レポート)]**メニューからレポートをスケジュールすることもできます。アイコンをクリックし、**[Type (種類)]**ドロップダウンから[Activity Insights (アクティビティに関するインサイト)]-[Summary (概要)]を選択します。

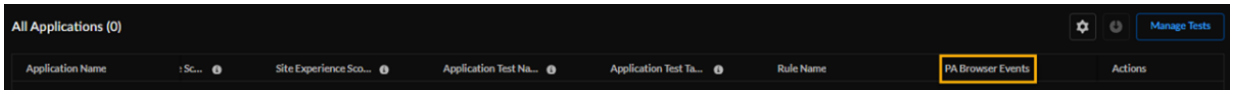
アクティビティに関するインサイト:アプリケーション

どこで使用できますか?	何が必要ですか?
• Prisma Access （*Strata Cloud Manager*または*Panorama*の設定管理付き） • NGFW （*Strata Cloud Manager*または*Panorama*の設定管理付き）	Activity Insightsを使用するには、これらのライセンスのうち少なくとも1つが必要です: ❑ Prisma Access ❑ AIOps for NGFW Free (use the AIOps for NGFW Free app)またはAIOps for NGFW Premium license (use the Strata Cloud Manager app) 。Activity Insights:[アプリケーション]タブを表示するために必要なその他のライセンスは次のとおりです。 ❑ Strata Logging Service ❑ ADEM Observabilityは、追加のPrisma Access機能のロックを解除します。

Prisma AccessとNGFWのセットアップ内のアプリケーション、アプリケーションを使用しているユーザー、リスクスコア、各アプリケーションのユーザーエクスペリエンスを監視し、リスクの高いアプリケーションがもたらすセキュリティへの影響を把握します。アプリケーションの使用状況に関する調査結果は、リスクが高い未許可アプリケーションを制御するセキュリティポリシーを調整する際に役立ちます。**[Activity Insights (アクティビティに関するインサイト)] > [Applications (アプリケーション)]**をクリックして、次の情報を表示します。

- リスクスコア別アプリケーション - 組織で実行されているアプリケーションの総数と、良好、普通、および劣悪なアプリケーション数。アプリケーションは、アプリケーションのエクスペリエンス スコアに基づいて、Good、Fair、Poorに分類されます。
- アプリケーションデータ転送 - 選択した時間帯にNGFWおよびPrisma Accessファイアウォール経由でダウンロードおよびアップロードされたデータの合計。アプリケーションカテゴリから発信され、デバイス（データセンターまたはファイアウォール）から宛先を通過するデータ転送を表示するようにフィルタリングできます。
- すべてのアプリケーション - このウィジェットを使用して、監視対象のPrisma Accessアプリケーションと、そのアプリケーション上で実行されている合成テスト、およびNGFW環境で実行されているアプリケーションを確認できます。テーブルには、各アプリケーションの正常性を示すエクスペリエンス スコアも表示されます。Prisma Access Browserを契約している

場合は、**PA Browser Events**の列が表示されます。イベント数を選択すると、Prisma Access Browser管理ページにリダイレクトされます。



表のデータをcsv形式でダウンロードできます（Prisma Accessアプリケーションのみ）。［**Manage Tests (テストの管理)**］ボタンをクリックすると、［Application Tests (アプリケーションテスト)］テーブルにすべてのPrisma Accessアプリケーションに設定されているすべての合成テストが表示されます。アプリケーションを監視するテストを作成する場合は、[ユーザーエクスペリエンス]列の下の**[App to view Health (正常性を監視するアプリ)]**をクリックします。

- アプリケーションの詳細 - アプリケーションの一般的な詳細と、アプリケーションのアクティビティおよびアプリケーションエクスペリエンスに関する詳細を表示します。
  - ［**Activity (アクティビティ)**］タブには、アプリケーション内で確認された脅威の総数、アプリケーションにアクセスしたユーザの総数、アプリケーションを通じて転送されたデータ、PAブラウザデータイベント、PAブラウザアクセスイベントが表示されます。

    次の画像は、**PA Browser Access Events (PAブラウザデータイベント)**と**PA Browser Access Events (PAブラウザアクセスイベント)**に関するApplication Details (アプリケーションの詳細)を示しています。デフォルトのビューには、すべてのイベントとブロックされたイベントの**Aggregate (集計)**が表示されます。または、**Event Type (イベントタイプ)**と**Count (カウント)**ごとの**Breakdown (内訳)**を表示するように選択することもできます。

  - **[Experience (エクスペリエンス)]**タブには、アプリケーションエクスペリエンススコア、選択した時間帯のスコア傾向、およびネットワークパフォーマンスメトリックが表示されます。

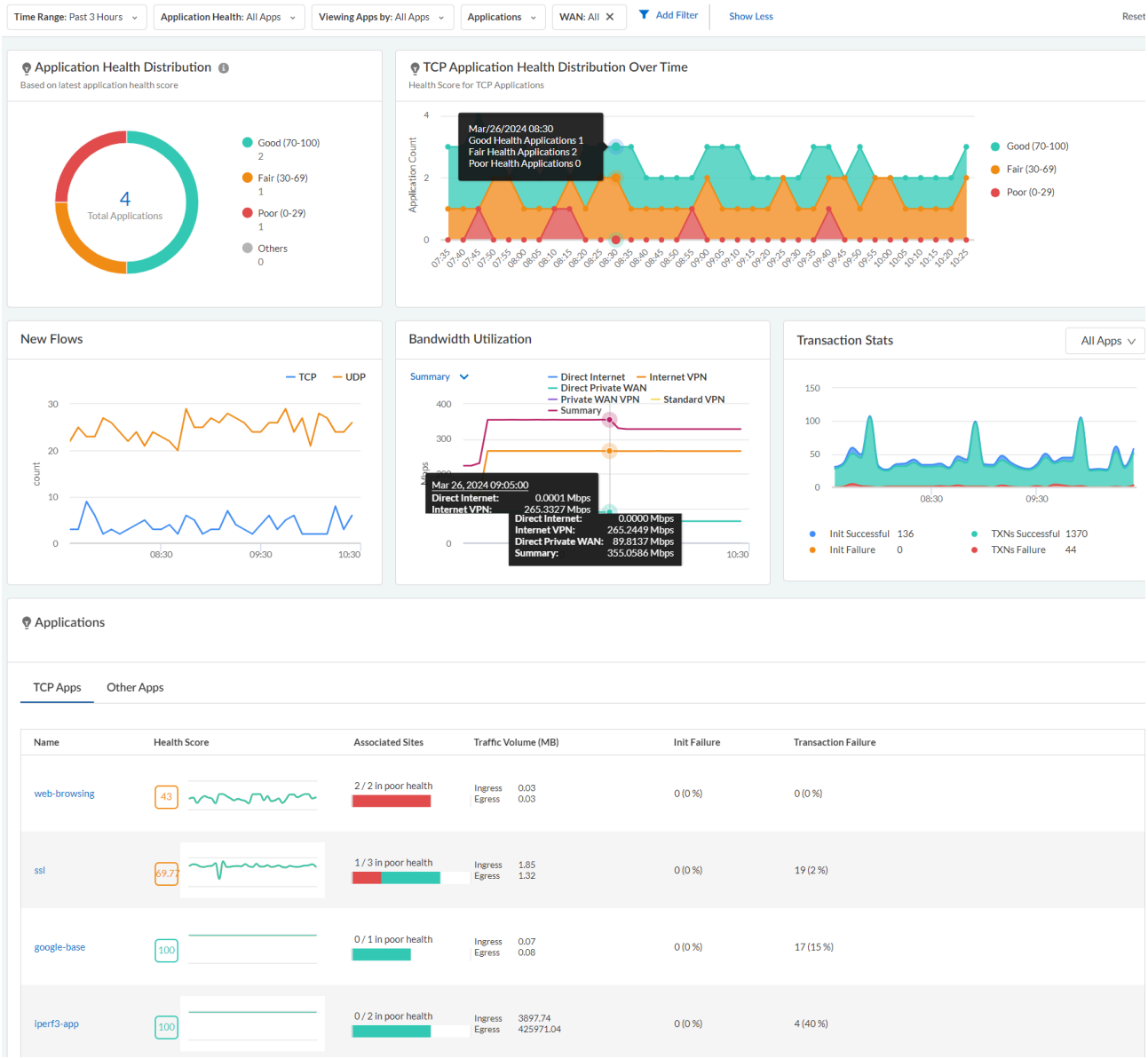
アプリがコンテナアプリの場合、表示される統計はコンテナ内のすべてのアプリケーションのロールアップです。例えば、*gmail*はコンテナアプリです（*gmail*には*App-ID*はありません）。*gmail-posting*、*gmail-downloading*、*gmail-uploading*などのアプリケーションをグループ化します。このコンテナアプリに設定されたリスクスコアは、含まれるアプリケーションに対して見つかった最も高いリスクスコアです。他のすべてのメトリックは、含まれるアプリケーションに対して見つかった値を合計して計算されます。

レポート - このビューのデータをカバーするレポートは生成できません。ただし、**Application Usage (**アプリケーションの使用状況**)**レポートを使用して、ネットワーク内のアプリケーションの使用状況データを表示できます。レポートをスケジュールするには、**[Strata Cloud Manager > Reports (**レポート**)]**メニューから アイコンをクリックし、**[Type (**種類**)]**ドロップダウンから[アプリケーションの使用状況]を選択します。

Activity Insights (アクティビティに関するインサイト):SD-WANアプリケーション

どこで使用できますか?	何が必要ですか?
• Prisma SD-WAN	❑ Prisma SD-WANライセンス ❑ 特定のウィジェットを表示するためのWAN Clarity Reportingライセンス

Prisma SD-WANでパフォーマンスが悪い上位アプリケーションを見る。すべての低品質アプリケーションの稼働状態スコア、稼働状態スコアに基づくテナントの低品質アプリケーションのリスト、および低品質アプリケーションの過去3時間の平均稼働状態スコアを5分間隔で確認できます。



- アプリケーション正常性ディストリビューション（WAN Clarityライセンスが必要）：特定のテナントのGood、Fair、Poorアプリケーションのディストリビューション。
- 経時的なアプリケーション正常性ディストリビューション（WAN Clarityライセンスが必要）：一定期間におけるGood、Fair、PoorのTCPアプリケーションの正常性ディストリビューション。時系列グラフは、選択した期間に基づいて計算され、更新されます。たとえば、サポートされている期間は1時間、3時間、1日、7日、30日、90日で、間隔はそれぞれ1分、5分、1時間、1日です。
- 新しいフロー:特定のアプリケーション、特定のアプリケーションセット、または指定された期間のすべてのアプリケーションの新しいTCPフローおよびUDPフローを表示します。TCPフローは、最初のSYNパケットを確認すると新しいフローと見なされます。UDPフローは、いずれかの方向で最初のUDPパケットを検出すると、新しいフローと見なされます。フローとは、送信元と宛先のIP、送信元と宛先のポート、およびプロトコルによって識別される両方向のパケットのシーケンスです。

- 帯域幅使用状況：帯域幅使用状況チャートは、ネットワーク内のトレイルで利用されている帯域幅の量を表示します。チャートを使用して、アプリケーションのパフォーマンスを妨げる可能性のあるネットワーク内のWAN輻輳を特定します。これは、帯域幅スパイク、特定のサイトで消費された総帯域幅、およびアプリケーションを視覚的に表したもので、アップロードがイングレス方向かイグレス方向かを示します。帯域幅使用率チャートにカーソルを移動すると、アプリケーションまたはタイムスタンプで帯域幅使用率をより詳細に表示できます。通常、アプリケーションは帯域幅の使用率の高い順にリストされます。
- トランザクション統計:TCPフローに関するトランザクション統計情報を提供します。この統計情報には、特定のアプリケーションまたはすべてのアプリケーション、特定のパスまたはすべてのパス、およびすべての正常性イベントの開始/トランザクションの成功と失敗が含まれます。
- アプリケーション:名前、アプリケーションプロファイル、正常性スコア、影響を受けたサイト、トラフィック量、初期/障害、トランザクション/障害など、すべてのアプリケーションの詳細が一覧表示されます。アプリケーション名をクリックすると、新しいページで個々のアプリの詳細を確認できます。

Activity Insights (アクティビティに関するインサイト):脅威

どこで使用できますか?	何が必要ですか?
• Prisma Access （*Strata Cloud Manager*または*Panorama*の設定管理付き） • NGFW （*Strata Cloud Manager*または*Panorama*の設定管理付き）	Activity Insights を使用するには、次のライセンスのうち少なくとも1つが必要です。 ❑ Prisma Access ❑ AIOps for NGFW Free (use the AIOps for NGFW Free app)又はAIOps for NGFW Premium license (use the Strata Cloud Manager app) ❑ Strata Cloud Manager Essentials ❑ Strata Cloud Manager Pro Activity Insightsを表示するために必要なその他のライセンス:[Threats (脅威)]タブ: ❑ Strata Logging Service ❑ CDSSライセンス ❑ ADEM Observabilityにより追加のPrisma Access機能のロックが解除されます

ネットワークで見られる脅威のアクティビティとさまざまな種類の脅威の全体像を把握します。このタブには、Prisma AccessおよびNGFWのデプロイメントで確認された脅威セッションの合計数、選択した期間の脅威カテゴリと脅威の重大度に基づく数値の内訳が表示されます。脅威に関連付けられたセキュリティ成果物 (ファイル ハッシュ、URL、ドメイン、またはIPアドレス (IPv4またはIPv6))を検索して、Palo Alto Networksの脅威インテリジェンス分析とサードパーティの分析結果を知ることができます。

ネットワーク内の固有の脅威について、次の詳細を確認します。

- **Threat Name (脅威名)** - 脅威シグネチャ名。時間範囲内のすべての脅威セッションを含む、脅威に関する最新のThreat Vault情報を検索するために使用します。
- 脅威**ID**- 一意の脅威シグネチャID。脅威IDを使用して、このシグネチャに関するPalo Alto Networks脅威データベースの最新情報を検索します。
- 脅威のカテゴリとサブカテゴリ-ザ - 脅威の種類は脅威のシグネチャ(ウイルス対策、スパイウェア(C2)、および脆弱性)に基づきます。
- ライセンス - 脅威を検出したPalo Alto Networksのセキュリティサービス。

- 重大度 - 脅威の重大度は、脆弱性が悪用される容易さ、脆弱性への影響、脆弱な製品の普及度、脆弱性の影響などに基づいて決定されます。重大度は次のように分類されます。
  - Critical(重大) - 脆弱性が非常に広く展開されているソフトウェアのデフォルトインストールに影響を及ぼし、エクスプロイトによってルートが侵害される可能性がある場合。エクスプロイトコード(システムコード、方法、概念実証(POC))の悪用方法に関する情報は広く利用可能で、簡単に悪用できます。攻撃者は、特別な認証資格情報や個々の被害者に関する知識を必要としません。
  - 重大度がCritical(重大)に変わる可能性があるものの、軽減要因が存在する脅威。たとえば、悪用するのが困難であったり、上位の特権が与えられることがなかったり、被害サーバー数が多くなかったりする場合です。
  - [medium (中)]: 影響が最小限に抑えられる小さな脅威。たとえば、標的に侵入することのないDoS攻撃や、攻撃者が被害サーバーと同じLAN上に存在する必要があり、標準以外の設定や隠れたアプリケーションにのみ影響するか、アクセスがごく限られている悪用などです。
  - 低 - 組織のインフラストラクチャにほとんど影響を与えない警告レベルの脅威。通常、ローカルまたは物理的なシステムへのアクセスが必要であり、被害者のプライバシーやDoS の問題、情報漏洩などが発生することがあります。
  - [informational (情報)]: 直ちに脅威とはならなくても、存在する可能性がある深層の問題に注意を引くために報告される、疑わしいイベント。
- セッション数の合計 - 脅威が検出されたセッションの数。脅威名をクリックすると、指定した時間範囲内の関連するすべての脅威セッションが表示されます。脅威セッションテーブルには、Palo Alto Networkセキュリティサービスが脅威を検出した時間、脅威の影響を受けたユーザー、ルール、アプリケーション、デバイス、脅威に対して実行されたアクション(許可またはブロック)など、脅威に関するコンテキストが表示されます。
- 合計ユーザー数 - 脅威にさらされたユーザーの数。
- 許可された脅威とブロックされた脅威- 脅威に適用されたアクションを確認して、アクションがネットワーク上で誤検出をトリガーしていないことを確認します。
- アクション - ログビューアで脅威のログ履歴を調査します。

レポート - このビューのデータをカバーするレポートは生成できません。

Activity Insights (アクティビティに関するインサイト):Users

どこで使用できますか?	何が必要ですか?
• Prisma Access （*Strata Cloud Manager*または*Panorama*の設定管理付き） • NGFW （*Strata Cloud Manager*または*Panorama*の設定管理付き）	Activity Insights を使用するには、次のライセンスのうち少なくとも1つが必要です。 ❑ Prisma Access ❑ AIOps for NGFW Free (use the AIOps for NGFW Free app)又はAIOps for NGFW Premium license (use the Strata Cloud Manager app) ❑ Strata Cloud Manager Essentials ❑ Strata Cloud Manager Pro Activity Insightsを表示するために必要なその他のライセンス:ユーザータブは次のとおりです。 ❑ Strata Logging Service ❑ [Advanced URL Filteringライセンス] ❑ [Cloud Identity Engineライセンス] ❑ [Advanced Threat Preventionライセンス] ❑ ADEM ObservabilityでPrisma Accessの追加機能がアンロックされます

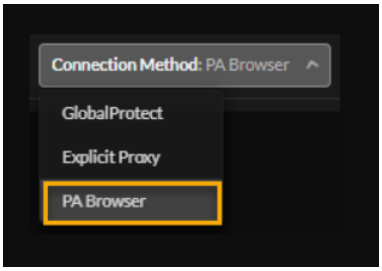
Prisma AccessおよびNGFW環境でのユーザーアクティビティを監視します。Prisma AccessおよびNGFWセキュリティサービスに接続するユーザーのデータは、デバイスのGlobalProtectアプリケーションを介して、またはデバイスのWebブラウザを介してExplicit Proxyを介して表示できます。ユーザーアクティビティを監視することで、潜在的な脅威の検出と阻止、機密情報の悪用の保護、セキュリティギャップを埋めるためのセキュリティポリシールールの調整に役立ちます。

ユーザーデータは、次の条件に基づいてフィルタリングできます。

- デプロイメント(Prisma Access、NGFW)
- 接続方法とバージョン(GlobalProtect、Explicit Proxy、Prisma Access Browser)
- username
- デバイス名
- トラフィックの発信場所とPrisma Accessの場所
- ユーザーがアクセスするアプリケーションとユーザーエクスペリエンススコアフィルタ

以下の詳細をこちらからご覧いただけます。

- 接続/アクティブユーザー - 現在接続中のGlobalProtect、Explicit Proxy Mobile Users、Prisma Access Browserに関する集計データを監視します。



  データがフェッチされた時点、またはタイムスタンプに示されたとおりにネットワークに接続しているユーザー数を表示します。ユーザー別またはユーザーデバイス別のトレンドを表示できます。番号を選択すると、すべての接続ユーザとそのすべてのデバイスに関する詳細が、[**Connected Users (**接続済みユーザー**) | Connected User Devices ()**接続済みユーザーデバイス]テーブルに表示されます。

  動的特権アクセスのデータを、「ユーザー別またはユーザーデバイス別のトレンド表示」、「接続ユーザー|接続ユーザーデバイス」、「シアター別プロジェクト配信」で表示します。

- **Monitored Users (**監視対象ユーザ**)** - ADEMで監視されているユーザまたはユーザデバイスの総数と、その平均ユーザエクスペリエンスを表示します。これは、ADEMで監視されているすべてのユーザについて集計されたエクスペリエンススコアです。番号をクリックすると、ユーザーエクスペリエンスに関連するユーザーアクティビティの詳細が表示されます。
- **Risky Users (**危険なユーザー**)** - 脅威の影響を受けたユーザー数を表示します。上矢印または下矢印は、この時間範囲と以前の時間範囲を比較して、接続されているデバイス数の差をパーセントで判断します。[View More Details for GlobalProtect Versions (GlobalProtectバージョンの詳細を表示)]または[IP Pool Utilization (IPプール使用率)]を選択すると、環境内のリスクのあるユーザーに関する詳細が表示されます。
- **GlobalProtect Version Details (GlobalProtect**バージョンの詳細**)**には、デバイスにインストールされているGlobalProtectのバージョンが表示されます。各バージョンで接続しているユーザー数を確認できます。データを使用して、GlobalProtectアプリの最新バージョンへの準拠を強制します。「ディストリビューション傾向」の線にカーソルを合わせると、その時点で接続しているユーザーのIPアドレスが表示されます。
- その時点での接続ユーザー数に基づく、異なるIPプール割り当てシアター別の**IP**プール利用率を参照してください。グラフ上のIPプール使用率のパーセンテージは、すべてのサブネットで使用できるすべてのIPプールブロックのうち、使用されているIPプールブロックの数です。IPプールバーが任意のリージョンの最大容量に近づいたら、サブネットを追加してプロアクティブなアクションを実行できます。
- ［ユーザー］テーブルには、時間範囲中にログインしたユーザーに関する情報が表示されます。ユーザー名をクリックすると、個々のユーザーの閲覧パターン（最も頻繁にアクセス

されるサイト、データ転送先のサイト、高リスクサイトへのアクセス試行）を可視化できます。

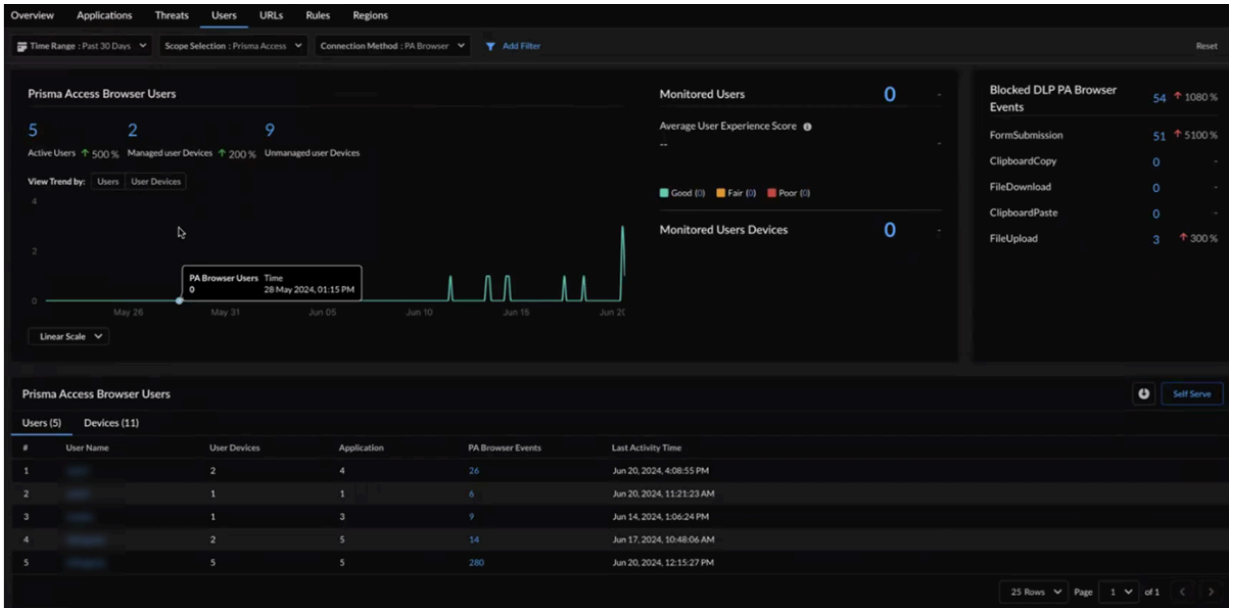
- 脅威
  - 閲覧概要 - ユーザーが最も多くのデータ転送を行ったサイトの種類と、ユーザーによるサイト訪問回数を示す数値を参照してください。
  - **Top 10 Most Visited URL Categories (**最もアクセス数が多い**URL**カテゴリ上位**10** 件**)** - データ転送に基づいて、ユーザーのトップURLカテゴリを表示します。URLカテゴリごとの、アクセスされたユニークURL数も確認できます。
  - **URL**閲覧概要 - ユーザーがアクセスした一意のURLのうち、悪意のあるURLや危険性の高いURLへのアクセスに注意してください。これらのサイトは、ネットワークを脅威、データ損失、コンプライアンス違反の危険にさらす可能性があります。これらのサイトへのアクセス数が想定よりも多い場合は、想定に近付くようにセキュリティポリシールールを調整してください。
  - 上位**10URL** - ユーザーが最も頻繁にアクセスするサイトのリスクレベルを確認します。リスクの高いURLは、ネットワークを脅威にさらす可能性が高いため、監視する必要があります。
  - **(**リスク別ブロック**URL** - ユーザーが最も頻繁にアクセスしようとしたブロックされたURLです。URLフィルタリングログを確認し、アクションを変更するためにセキュリティポリシールールを調整する必要があるかどうかを確認します。
  - 重大な脅威 - ユーザに対して検出された脅威の合計と、脅威の重大度に基づいた数値を表示します。他のユーザーと数を比較します。数値が異常に高い場合は、セキュリティポリシールールを調整します。
  - 上位重大脅威:ユーザーが最も頻繁に検出する脅威です。
- 接続性：特定の期間にユーザーがログインしているデバイスの傾向と、すべてのユーザーログインおよびログアウトイベントのデバイス接続の詳細を表示します。
- エクスペリエンス - デバイスのユーザーエクスペリエンスデータ、監視対象の各アプリケーションのエクスペリエンススコアとトレンド、および個々のデバイスに対する監視対象ユーザーとアプリケーションのパフォーマンスメトリックを提供します。

- Prisma Access Browser - **Prisma Access Browser**接続方法を選択すると、Prisma Access Browserのユーザーに関する情報が表示されます。

  Prisma Access Browserユーザーアクティビティ傾向グラフには、選択した時間範囲フィルタのある時点でアクティブになっているユーザー数が表示されます。Prisma Access接続エージェント（管理対象デバイス）がインストールされている場合と、エージェント（管理対象外）ユーザーがインストールされていない場合の、これらのアクティブユーザーのデバイスの内訳を示しています。

  Prisma Access Browserは、ブラウザのユーザーのアクションを優れた可視性で示し、企業のデータ資産に関するユーザーのデバイスでのアクションが企業のDLPポリシーによって許可されているかブロックされているかを示します。［**Blocked DLP PA Browser Events (**ブロッ

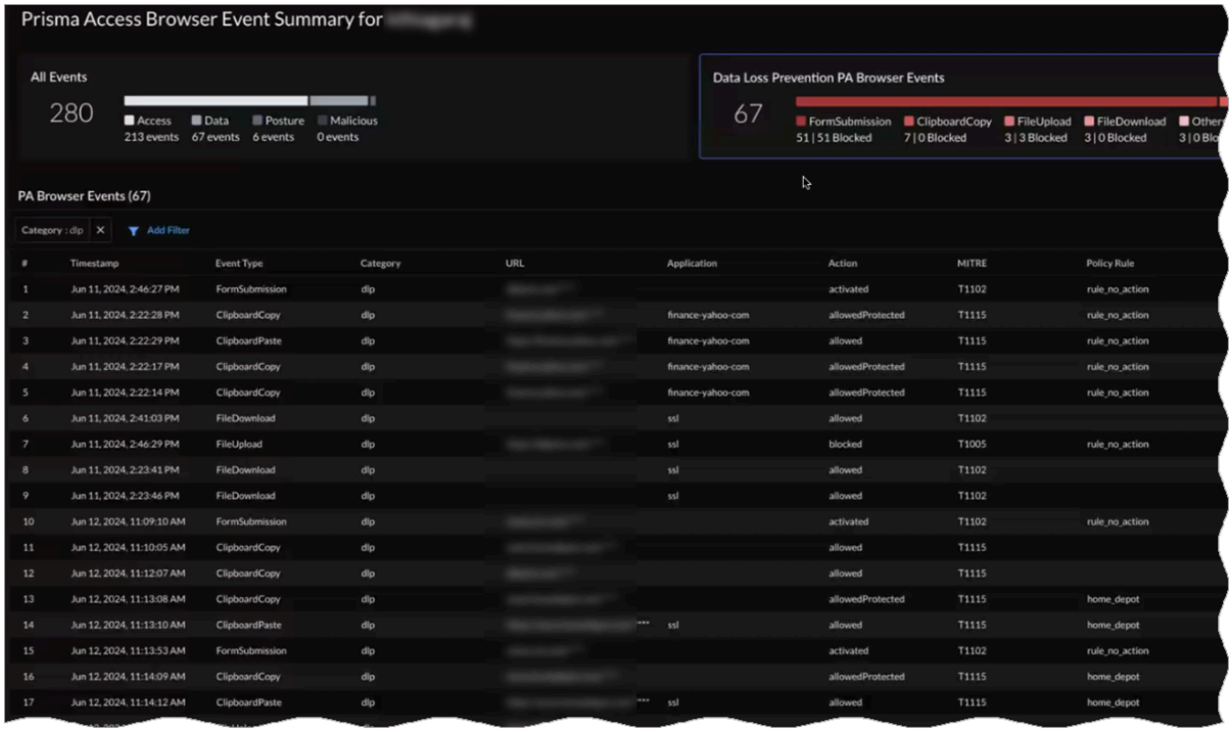
クされたDLP PAブラウザイベント)］ウィジェットには、ポリシーによってブロックされているブラウザ上で実行されたユーザーアクションを示すイベントが表示されます。



［**Prisma Access Browser Users (Prisma Access Browserユーザー)**］テーブルには、Prisma Access Browserを介してアプリケーションにアクセスするアクティブユーザーのリストが表示されます。任意のユーザー名をクリックすると、**[ユーザー詳細] > [アクティビティ]**ページでこのユーザーのアクティビティページが表示されます。

[Prisma Access Browserイベント概要]には、選択した時間間隔でユーザーがブラウザを介して実行したすべてのブラウザアクションが一覧表示されます。［**PA Browser Events (PAブラウザイベント)**］テーブルのデフォルト・ビューには、ポリシーによって許可されているかブロックされているかに関係なく、すべてのDLPブラウザイベントのリストが表示されます。適切なイベントカテゴリを選択することにより、ビューを**Access Events (アクセスイベント)**、**Posture Events (体制イベント)**、**[Malicious Events (悪意あるイベント)]**などの他のイベントカテゴリに切り替えることができます。各イベントカテゴリでは、イベントタイプの内訳のほか、ブラウザイベントがいつ実行されたかを示すタイムスタンプ、アクセスされたア

プリケーションURLに関する情報、アプリケーション名、関連するMITRE攻撃ノートを表示できます。

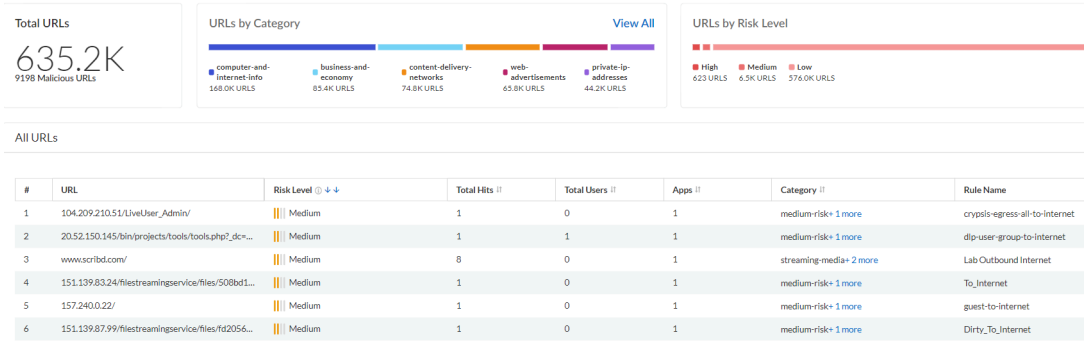


レポート - このビューのデータをカバーするレポートは生成できません。ただし、ユーザアクティビティレポートを使用して、ネットワーク内のユーザに固有のアクティビティを表示できます。**Strata Cloud Manager** > [レポート]メニューからレポートをスケジュールするには、アイコンをクリックし、**[Type (種類)]**ドロップダウンから[ユーザー]を選択します。

Activity Insights (アクティビティに関するインサイト):URL

どこで使用できますか?	何が必要ですか?
• Prisma Access （*Strata Cloud Manager*または*Panorama*の設定管理付き） • NGFW （*Strata Cloud Manager*または*Panorama*の設定管理付き）	Activity Insights を使用するには、次のライセンスのうち少なくとも1つが必要です。 ❑ Prisma Access ❑ AIOps for NGFW Free (use the AIOps for NGFW Free app)又はAIOps for NGFW Premium license (use the Strata Cloud Manager app) ❑ Strata Cloud Manager Essentials ❑ Strata Cloud Manager Pro Activity Insightsを表示するために必要なその他のライセンス:URLタブは次のとおりです。 ❑ Strata Logging Service ❑ Advanced URL Filteringライセンス

このビューは、高度なURLフィルタリングサービスが検出したPrisma AccessおよびNGFW展開内のURLアクティビティをまとめたものです。指定した期間にネットワーク内で検出されたURLの総数や、URLカテゴリ別、リスクレベル別の内訳を可視化できます。フィルタリングオプションを使用して、ダッシュボードのビューをフィルタリングします。



ここでから

- へのデータを使用して、アクセスの多いURLカテゴリ、URLカテゴリ付きの一意のURL、グローバル解析結果とともにネットワーク内のURL履歴を識別します。URLフィルタリングサービスによってフィルタリングされた悪意のあるURLに基づいて、これらのURLカテゴリは、ネットワークを悪意ある搾取的なコンテンツに晒す可能性があります。これらのURLカテゴリをブロックするのがベストプラクティスです。

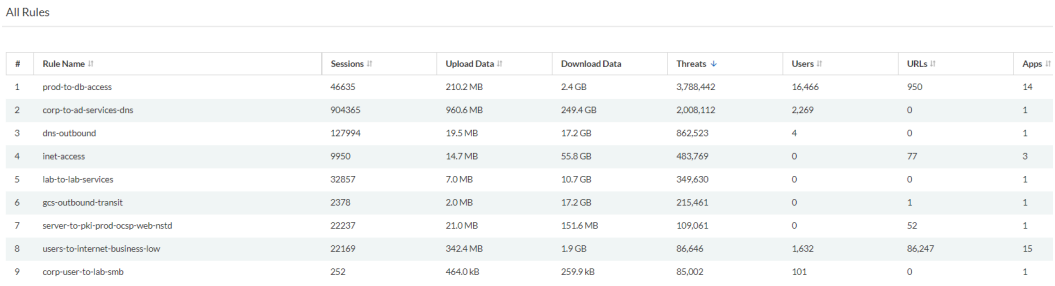
- リスクの高いURL、ユーザー、アプリケーション、ルールへの影響を確認します。リスクの高いURLサイトに悪意は確認されていません。ただし、それでもネットワークが脅威にさらされる可能性があります（悪意はないが、防弾ISPによってホストされているサイトは、リスクの高いサイトの例です）。徹底した復号化とセキュリティポリシールールでこれらのサイトを対象にすることを検討してください。

レポート - このビューのデータをカバーするレポートは生成できません。

Activity Insights (アクティビティに関するインサイト):ルール

どこで使用できますか?	何が必要ですか?
• Prisma Access （*Strata Cloud Manager*または*Panorama*の設定管理付き） • NGFW （*Strata Cloud Manager*または*Panorama*の設定管理付き）	Activity Insights を使用するには、次のライセンスのうち少なくとも1つが必要です。 ❑ Prisma Access ❑ AIOps for NGFW Free (use the AIOps for NGFW Free app)又はAIOps for NGFW Premium license (use the Strata Cloud Manager app) ❑ Strata Cloud Manager Essentials ❑ Strata Cloud Manager Pro Activity Insightsを表示するために必要なその他のライセンス:［Rules (ルール)］タブは次のとおりです。 ❑ Strata Logging Service

ネットワーク内のすべてのトラフィックに一致するセキュリティポリシールールを表示します。セキュリティポリシールールは、送信元および宛先のIPアドレス、アプリケーション、ユーザー、サービスなどのトラフィック属性に基づいて、セッションをブロックするか許可するかが決定されます。ネットワークを通過するすべてのトラフィックはセッションと照合され、各セッションはセキュリティ ポリシールールと照合されます。セッションが一致すると、セキュリティポリシールールが適用されます。


All Rules

#	Rule Name	Sessions	Upload Data	Download Data	Threats	Users	URLs	Apps
1	prod-to-db-access	46635	210.2 MB	2.4 GB	3,788,442	16,466	950	14
2	corp-to-ad-services-dns	904365	960.6 MB	249.4 GB	2,008,112	2,269	0	1
3	dns-outbound	127994	19.5 MB	17.2 GB	862,523	4	0	1
4	inet-access	9950	14.7 MB	55.8 GB	483,769	0	77	3
5	lab-to-lab-services	32857	7.0 MB	10.7 GB	349,630	0	0	1
6	gcs-outbound-transit	2378	2.0 MB	17.2 GB	215,461	0	1	1
7	server-to-pki-prod-ocsp-web-nstd	22237	21.0 MB	151.6 MB	109,061	0	52	1
8	users-to-internet-business-low	22169	342.4 MB	1.9 GB	86,646	1,632	86,247	15
9	corp-user-to-lab-smb	252	464.0 kB	259.9 kB	85,002	101	0	1

ダッシュボードには、セキュリティポリシールールに一致するネットワークイベントの次の詳細が表示されます。

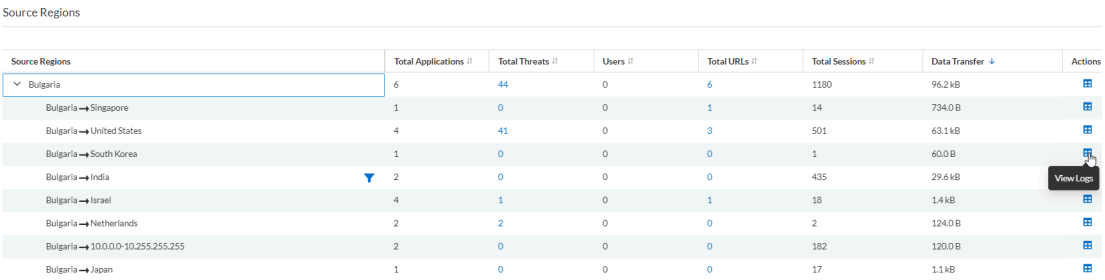
トラフィックセッション、データ転送、セッションで検出された脅威、影響を受けたユーザー、閲覧したURL、アクセスしたアプリケーション。トラフィック・セッションに最も一致するルールを確認し、それらのセッションを分析してルールが過度に許容されていないかを理解し、必要に応じてルールを最適化します。

レポート - このビューのデータをカバーするレポートは生成できません。

Activity Insights (アクティビティに関するインサイト):リージョン

どこで使用できますか?	何が必要ですか?
• Prisma Access （*Strata Cloud Manager*または*Panorama*の設定管理付き） • NGFW （*Strata Cloud Manager*または*Panorama*の設定管理付き）	Activity Insights を使用するには、次のライセンスのうち少なくとも1つが必要です。 ❑ Prisma Access ❑ AIOps for NGFW Free (use the AIOps for NGFW Free app)又はAIOps for NGFW Premium license (use the Strata Cloud Manager app) ❑ Strata Cloud Manager Essentials ❑ Strata Cloud Manager Pro Activity Insightsを表示するために必要なその他のライセンス:[リージョン] タブは次のとおりです。 ❑ Strata Logging Service

これらは、ネットワーク内でトラフィックが発生したリージョンです。このビューには、脅威、ユーザー、URL、ネットワーク セッション、およびこれらの場所から発生したデータ転送に関する情報が表示されます。また、ドリルダウンして、トラフィックのターゲット位置を把握することもできます。セッション用のトラフィックログを表示するには[Actions (アクション)]をクリックします。このデータを使用して、ネットワークに侵入しようとする脅威の標的となる領域を特定し、絞り込むことができます。ルールを最適化する (これは対象リージョンに適用されます)



特定の送信元と宛先のリージョンとの間のトラフィックを絞り込むためのフィルタリングオプションがあります。その他のフィルタリングオプションには、次のものがあります。

- 特定のデプロイメントで見られるトラフィック (Prisma Access、NGFW)
- 認可されたアプリケーションまたは認可されていないアプリケーションとの間のトラフィック
- 特定のポートとプロトコルを使用するトラフィック

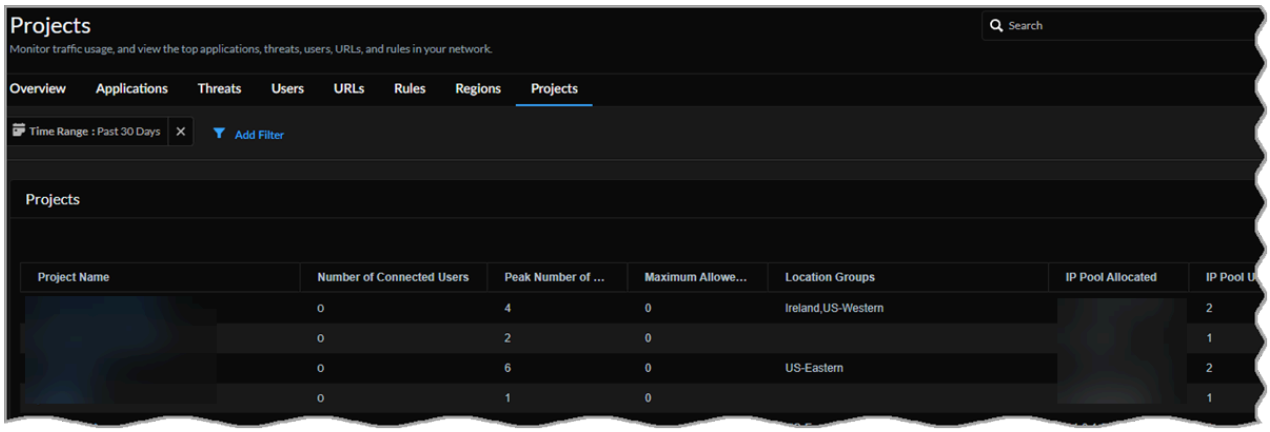
- 特定の脅威タイプ、脅威カテゴリ、URL、URLカテゴリを含むトラフィック

レポート - このビューのデータをカバーするレポートは生成できません。ただし、ネットワーク使用状況レポートを使用して、ネットワーク・トラフィックの詳細を把握することができます。レポートをスケジュールするには、**Strata Cloud Manager** > レポートメニューで、アイコンをクリックし、**[Type (種類)]**ドロップダウンで[Network Usage (ネットワーク使用量)]を選択します。

Activity Insights (アクティビティに関するインサイト):プロジェクト

どこで使用できますか?	何が必要ですか?
• Prisma Access （*Strata Cloud Manager*または*Panorama*の設定管理付き） • NGFW （*Strata Cloud Manager*または*Panorama*の設定管理付き）	Activity Insights (アクティビティインサイト)を使用するには、次のライセンスのうち少なくとも 1 つが必要です。 ❑ Prisma Access ❑ AIOps for NGFW Free (use the AIOps for NGFW Free app)または AIOps for NGFW Premium license (use the Strata Cloud Manager app) ❑ Strata Cloud Manager Essentials ❑ Strata Cloud Manager Pro

Strata Cloud Manager を使用してダイナミック権限アクセスプロジェクトのアクティビティを監視することで、Prisma Access Agentのデプロイメントを可視化できます。



- プロジェクト表には、動的権限アクセスユーザーがPrisma Accessを使用してアクセスするプロジェクトの概要が表示されます。プロジェクトの名前を選択すると、その詳細ページが表示されます。

- プロジェクトの詳細ページには以下の項目が表示されます。
  - 概要 – このプロジェクトで選択した期間における最大許容ユーザー数とピークユーザー数が表示されます。
  - **IP**プール使用率 – 使用中のIPの数と、このプロジェクトのプールでまだ使用可能なIPの数が表示されます。
  - 接続ユーザ - 選択した時間範囲に接続しているユーザのグラフを表示します。
  - ロケーショングループ別の接続ユーザー – 所属するPrisma Accessロケーショングループ別のユーザー数が表示されます。

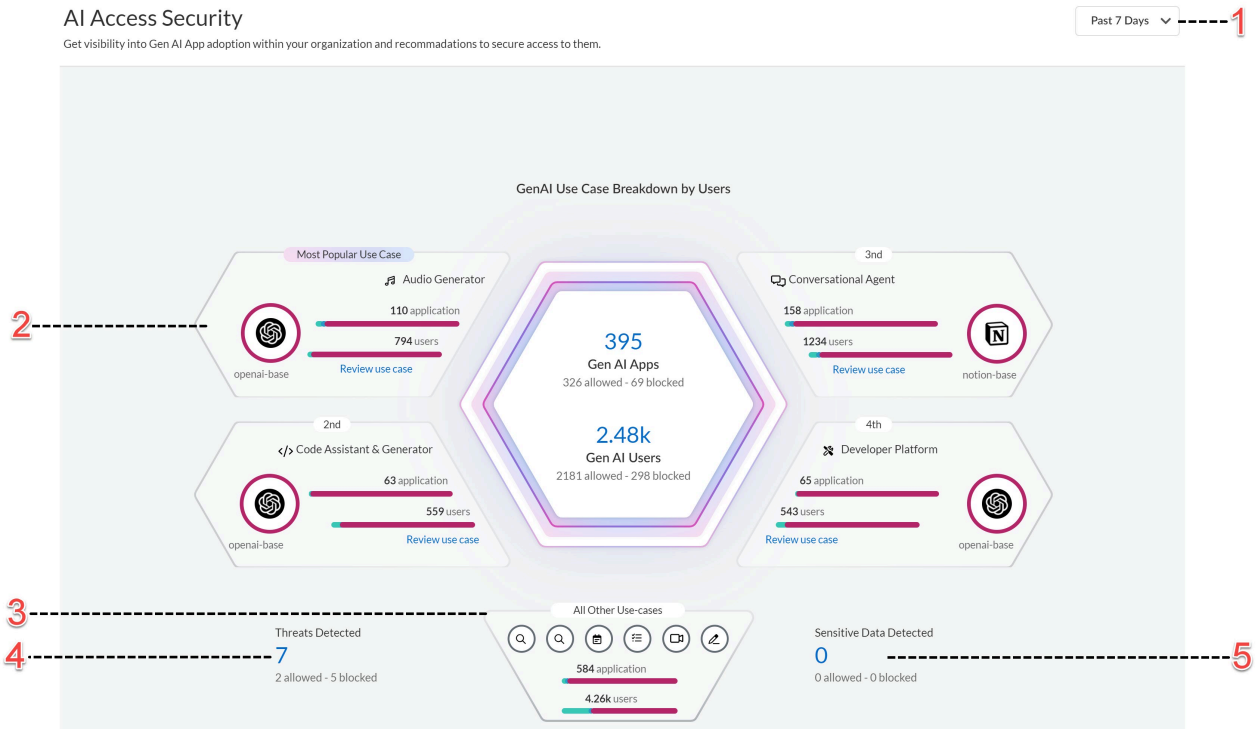
インサイト（知見）:AIアクセス

どこで使用できますか?	何が必要ですか?
• Prisma Access （*Strata Cloud Manager*または*Panorama*の設定管理付き） • NGFW （*Strata Cloud Manager*または*Panorama*の設定管理付き）	以下のいずれかのライセン ❑ ス：ライセンスAI Access Security ❑ CASB-PAライセンス ❑ CASB-Xライセンス AIアクセスセキュリティに対応したライセンスの詳細については、 こちらをクリックしてください。

GenAI（生成AI）アプリケーションは、ユーザーのプロンプトに応じてテキスト、画像、動画などのデータを生成し、ユーザーのデータ入力に基づいて継続的に学習できるAIアプリケーションです。その利用は驚異的な勢いで増えており、ビジネスの無限のチャンスを提供しています。しかし、GenAIアプリケーションが競合的に改善するという性質は、企業やセキュリティ管理者に新たな危険をもたらします。従業員が機密データや専有データをGenAIアプリに流出させないようにするにはどうすればいいのでしょうか？

Palo Alto Networksは、GenAIアプリケーションを組織全体で安全に導入できるように、AIアクセスセキュリティを導入しています。

AI Access Security Insights (AIアクセス セキュリティに関するインサイト)ダッシュボードを使用して、ネットワーク上のGenAIアプリケーションの使用状況をフィルタリングします。AI Access Security Insightsのダッシュボードでは、どのGenAIアプリが誰によって使用されているかを理解するのに役立つ詳細な情報を確認できます。



*GenAI*アプリケーションから機密データを保護する方法の詳細については、こちらをクリックしてください。

インサイト（知見）:AI Runtime Security (AIランタイム セキュリティ)

どこで使用できますか?	何が必要ですか?
• Prisma Access （*Strata Cloud Manager*または*Panorama*の設定管理付き） • NGFW （*Strata Cloud Manager*または*Panorama*の設定管理付き）	☐ AIランタイムセキュリティライセンスの有効化 ☐ AIランタイムセキュリティセットアップの前提条件 ☐ SCMでクラウドアカウントを登録して有効化する

Palo Alto Networks AI Runtime Securityは、AIを活用したリアルタイムのセキュリティを活用することで、組織のクラウドネットワークアーキテクチャをAI固有および従来型のネットワーク攻撃から保護する、目的に特化した集中型セキュリティソリューションです。次世代のAIモデル、AIアプリケーション、AIデータセットを、プロンプトインジェクション、機密データ漏洩、セキュアでない出力（マルウェアやURLなど）、モデルDoS攻撃などのネットワークの脅威から保護します。

AI Runtime Security Insights (AIランタイム セキュリティ インサイト)ダッシュボードを使用して、クラウドネットワークの攻撃対象領域を把握し、悪意のある脅威からクラウド資産を防御します。

*AI*および*AI*以外のネットワークトラフィックフローを潜在的な攻撃から保護する方法の詳細については、こちらをクリックしてください。

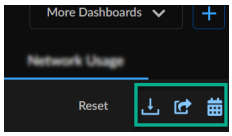
ダッシュボード:ログ - Strata Cloud Manager

どこで使用できますか?	何が必要ですか?
• Prisma Access (Managed by Panorama or Strata Cloud Manager) • Software NGFW Creditsによって資金提供されたものを含むNGFW • Prisma SD-WAN	これらの各ライセンスには、Strata Cloud Managerへのアクセスが含まれています。 ❑ Prisma Access ❑ AIOps for NGFW Premium license (use the Strata Cloud Manager app) ❑ Strata Cloud Manager Essentials ❑ Strata Cloud Manager Pro ❑ Prisma SD-WAN 特定のダッシュボードにアクセスするために必要なその他のライセンスと前提条件は次のとおりです。 ❑ クラウド配信型セキュリティサービス (CDSS) ❑ ADEM Observability (ADEMの可観測性) ❑ ダッシュボード を表示する権限を持つロール → Strata Cloud Managerで利用できる機能は、使用するライセンスによって異なります。

Strata Cloud Managerは、ネットワーク内の作業中のアプリケーション、IONデバイス、脅威、ユーザー、およびセキュリティサブスクリプションを包括的に把握できる一連の対話型ダッシュボードを提供します。ダッシュボードは、デプロイメント環境で発生している稼働状態、セキュリティ体制、アクティビティを可視化し、ネットワークのパフォーマンスとセキュリティのギャップを防止または対処するのに役立ちます。ダッシュボードのサポートは、Palo Alto Networks製品とクラウド管理でサポートされるサブスクリプション全体に拡張され、Traps、Cortex XDR、Prisma SaaS、Proofpointなどの他のソースからも提供されます。よく目にするデータは、契約によって異なります。各ダッシュボードトピックを確認すると、そのダッシュボードのライセンス要件、ロール権限が表示するデータに影響を与える可能性があるかどうか、および各サブスクリプションがロック解除するさまざまなタイプのデータについて知ることができます。

ダッシュボードには、左側のナビゲーションペインの[ダッシュボード]メニューからアクセスできます。SASE Healthのダッシュボードは、デフォルトではランディングページに固定されて

います。**[More Dashboards (**その他のダッシュボード**)]**をクリックし、ダッシュボード名の横にあるチェックボックスをオンまたはオフにして、ダッシュボードをダッシュボードランディングページに固定または固定解除します。**[Build My Dashboard (**マイダッシュボードの構築**)]**オプションを使用して、独自のダッシュボードを構築することもできます。ダッシュボードの一部には、オフラインで共有できるレポートをダウンロードして共有したり、定期的な更新をスケジュールできるオプションもあります。レポートがダッシュボードでサポートされているかどうかを確認するには、次のアイコンを確認します。



Cloud Identity Engineとの統合

ダッシュボードを最大限に活用するには、Cloud Identity Engine（Directory Sync）を設定することをお勧めします。Cloud Identity Engineは、Palo Alto Networksが提供する無料のアプリです。他のアプリからActive Directory情報に読み取り専用でアクセスでき、以下のことが可能になります。

- ユーザーアクティビティデータの取得 - クラウドアイデンティティエンジンにより、レポートを実行するユーザーを指定できます。
- Cloud Identity Engineのセットアップにより、簡単かつ安全に他のメンバーとレポートを共有できるため、スケジュールされたレポートに受信者を簡単に追加できます。レポートの受信者はCloud Identity Engineと照合され、一致するものが見つからなかった場合は、サポートアカウントに関連付けられているメールアドレスドメインと照合して、追加の妥当性確認手順を実行します。これらのチェックにより、レポートが組織の外部に送信されないようにします。

統合アプリは同じリージョンにデプロイする必要があります。Cloud Identity EngineとPrisma AccessまたはDirectory Syncを統合するには、いつでもハブに移動できます。#Palo Alto Networksのアプリを統合する

ダッシュボードのサポート

製品のダッシュボードサポートの一部は、*Strata Cloud Manager*への移行を保留しています。

機能	サポート対象				ライセンスおよびその他の要件	集計データの範囲
	Prisma Access(クラウドマネージド)	**Prisma Access (Panoramaマネージド)**	**AIOps for N**	**Prisma SASE Multitenant Platform**		
	• Prisma Access (Managed by Strata Cloud Manager)とPrisma Access (Managed by Panorama)のドキュメント		• AIOps for NGFWのドキュメント	• Prisma SASE Multitenant Platformのドキュメント		
佐瀬健康	あり	あり	あり		• ADEMの可観測性 • AIを活用したADEM	
ベストプラクティス	あり	いいえ	PAN-OS バージョン:10.0以降	あり	[AIOps for NGFW専用]デバイスでのテレメトリ共有を有効にする	• Prisma Access (Manage ナントあたり • AIOps for NGFW:NGF 位/AIOps for NGFWインスタンスに関連付けられたPanorama単位
コンプライアンス概要	いいえ	なし	あり	いいえ	【AIOps for NGFW専用】デバイス内でのテレメトリ共有を有効にする	AIOps for NGFW: NGFW/ PanoramaごとにAIOps for NGFWイン

機能	サポート対象				ライセンスおよびその他の要件	集計データの範囲
	Prisma Access(クラウドマネージド)	Prisma Access (Panoramaマネージド)	AIOps for NG	Prisma SASE Multitenant Platform		
						スタンスに関連付け
オンデマンド BPA	いいえ	なし	あり	いいえ	TSF	AIOps for NGFW: NGFW/PanoramaごとにAIOps for NGFWインスタンスに関連付け
エグゼクティブ概要	あり	あり	あり	あり	• Strata Logging Serviceライセンス • 脅威防止ライセンス • URLフィルタリングライセンス • WildFireライセンス • エンタープライズDLPライセンス	Strata Logging Serviceテナントあたり
WildFire	あり	なし	あり	あり**	WildFireライセンス	TSG(テナント サービス グループ)単位
DNS セキュリティ	あり	あり	あり	あり**	DNSセキュリティライセンス	TSG(テナント サービス グループ)単位

機能	サポート対象				ライセンスおよびその他の要件	集計データの範囲
	Prisma Access(クラウドマネージド)	Prisma Access (Panoramaマネージド)	AIOps for N(	Prisma SASE Multitenant Platform		
ログビューアー	あり	あり	あり	あり	Strata Logging Serviceライセンス	Strata Logging Serviceテナントあたり
IOC検索	あり	なし	あり	あり**	検索でトレンドグラフを表示するための要件: • DNSライセンス • WildFireライセンス • Strata Logging Serviceライセンス • URLフィルタリング	
ダウンロード/共有/スケジュール	あり	あり	あり	あり		この表のそれぞれの機能欄を参照
SaaS セキュリティ	あり	なし	いいえ	いいえ	• Saas Securityライセンス • Strata Logging Service	Prisma Accessテナントあたり
DLP インシデント	あり	なし	いいえ	いいえ	エンタープライズDLPライセンス	Prisma Accessテナントあたり

機能	サポート対象				ライセンスおよびその他の要件	集計データの範囲
	Prisma Access(クラウドマネージド)	Prisma Access (Panoramaマネージド)	AIOps for NG	Prisma SASE Multitenant Platform		
デバイスの健全性	いいえ	なし	あり	いいえ	• [AIOps for NGFW専用]デバイスでのテレメトリ共有を有効にする	AIOps for NGFW:NGFW単位/AIOps for NGFWインスタンスに関連付けられたPanorama単位
セキュリティ体制インサイト	いいえ	なし	あり	いいえ		AIOps for NGFW:NGFW単位/AIOps for NGFWインスタンスに関連付けられたPanorama単位
高度な脅威防御	いいえ	なし	あり	いいえ	• 脅威防御または高度な脅威防御ライセンス • Strata Logging Service	Strata Logging Serviceテナントあたり
IoTセキュリティ	あり	あり	あり	いいえ	IoT Securityライセンス	IoT Securityテナントあたり
Prisma SD-WAN	いいえ	いいえ	なし	あり	Prisma SD-WANライセンス	Prisma SD-WANテナントあたり
PAN-OS CVE	いいえ	あり	あり		【AIOps for NGFW専用】デバイス内でのテレメトリ共有を有効にする	• AIOps for NGFW: NGFW/Panoramaごとに AIOps for NGFWイ

機能	サポート対象				ライセンスおよびその他の要件	集計データの範囲
	Prisma Access(クラウドマネージド)	Prisma Access (Panoramaマネージド)	AIOps for N(	Prisma SASE Multitenant Platform		
						ンスタンスに関連付け • APIアクセスを利用したCVEのPSIRTデータベース
CDSS の採用	あり	あり	あり		【AIOps for NGFW専用】デバイス内でのテレメトリ共有を有効にする	AIOps for NGFW: NGFW/PanoramaごとにAIOps for NGFWインスタンスに関連付け
機能の導入状況	いいえ	あり	あり		【AIOps for NGFW専用】デバイス内でのテレメトリ共有を有効にする	AIOps for NGFW: NGFW/PanoramaごとにAIOps for NGFWインスタンスに関連付け

Prisma Access (Panoramaマネージド)* -

- 米州以外の地域でホストされているStrata Logging Serviceを持つPrisma Access（Panorama管理）ユーザーの場合、Prisma Accessが米州以外のリージョンのStrata Logging Serviceからデータを読み取り、処理することを許可する同意を提供する必要があります。ダッシュボードホームページのプライバシー通知を確認して同意すると、同意が得られ、ダッシュボードとログをさらに表示できます。アプリ管理者、インスタンス管理者、アカウント管理者のみがプライバシー通知を表示して承諾できます。
- Prisma Access（Panoramaマネージド）マルチテナント環境では、ダッシュボードはサポートされません。

はい* - Prisma AccessとPAN-OSのすべてのバージョンがサポートされていることを意味します。

はい** - マルチテナントプラットフォームでは、テナントはTSG(テナントサービスグループ)として識別され、TSG IDで割り当てられます。CSP（カスタマーサポートポータル）ごとに1つまたは複数のテナントを関連付けることができます。ダッシュボードに表示されるデータは、次のシナリオによって異なります。

- ダッシュボードにアクセスするアプリはTSGに対応し、SASEプラットフォームまたはハブ上のテナントビューを介してアクセスする必要があります。
- ハブでCommon Servicesを使用してテナントにデバイスを関連付けています。
- テナントがCSPと1対1または多対1のマッピングを行っているかどうかを確認します。
  - テナントがCSPと1対1でマッピングしている場合、すべてのソースにわたるダッシュボードデータを表示できます（たとえば、WildFireダッシュボードでは、Palo Alto Networksファイアウォール、Prisma Access、Traps、Cortex XDR、Prisma SaaS、Proofpoint、手動アップロードのサンプルにまたがるデータが表示されます）。
  - CSPごとに複数のテナントが関連付けられている場合、ダッシュボードには、特定のテナントに関連付けられたPrisma Access、Palo Alto Networksファイアウォール、Panoramaアプライアンスのデータのみが表示され、他のソースからのデータは表示されません。

AIOps for NGFW* - AIOps for NGFWで利用できるダッシュボードは、Freeライセンスまたはライセンス階層の有無によって異なります。

ダッシュボード:カスタムダッシュボードの作成

どこで使用できますか?	何が必要ですか?
• Prisma Access (Managed by Panorama or Strata Cloud Manager) • Software NGFW Creditsによって資金提供されたものを含むNGFW • Prisma SD-WAN	これらの各ライセンスには、Strata Cloud Managerへのアクセスが含まれています。 ❑ Prisma Access ❑ AIOps for NGFW Premium license (use the Strata Cloud Manager app) ❑ Strata Cloud Manager Essentials ❑ Strata Cloud Manager Pro ❑ Prisma SD-WAN その他のライセンスと可視性に必要な前提条件は次のとおりです。 ❑ ダッシュボードの特定のウィジェットのロックを解除するライセンス ❑ ダッシュボードを表示する権限を持つロール → Strata Cloud Managerで利用できる機能は、使用するライセンスによって異なります。

デフォルトのダッシュボードとは別に、カスタムダッシュボードを作成して、ウィジェットを使用してネットワークで関心のある領域を可視化できます。ウィジェットは、ダッシュボードを作成するために使用されるコンポーネントです。ウィジェットは、ウィジェットライブラリに分類されて保存されます。[ダッシュボード > +]をクリックし、ドロップダウンリストからカテゴリを選択してウィジェットを表示します。ウィジェットライブラリで使用できるウィジェットは、セキュリティサービスのサブスクリプションによって異なります。たとえば、AIOps for NGFW PremiumとAdvanced WildFireのライセンスを持っている場合、WildFireカテゴリの下にあるすべてのウィジェットを表示して使用してダッシュボードを作成できます。

ダッシュボードの作成に使用できるウィジェットカテゴリです。これらのカテゴリのウィジェットにアクセスし、ウィジェットについて知るためのライセンス要件については、以下のリンクを参照してください。

- ダッシュボード:高度な脅威防御
- ダッシュボード:DNS セキュリティ
- ダッシュボード:WildFire

ダッシュボードを作成する

カスタムダッシュボードには最大10個のウィジェットを追加でき、ユーザーごとに10個のカスタムダッシュボードを作成できます。ダッシュボードとウィジェットはいつでもカスタマイズできます。ウィジェットタイル、説明、フィルタの表示/非表示、レイアウト、ダッシュボード名、説明などのダッシュボード設定をカスタマイズできます。また、ダッシュボードにフィルタを含めることもできます。

STEP 1 | [ダッシュボード > +]をクリックします。

STEP 2 | ダッシュボードの名前を入力します。

STEP 3 | [Widget Library (ウィジェットライブラリ)]ドロップダウンからウィジェットカテゴリを選択します。

STEP 4 | ウィジェットをダッシュボードに追加する - ウィジェットの上にマウスを置くと、ウィジェットの詳細が表示されます。ウィジェットをダッシュボードキャンバスにドラッグ＆ドロップします。

ダッシュボードキャンバスに、別のウィジェットカテゴリから同じ種類または異なる種類のウィジェットを追加できます。

STEP 5 | **Sample Data (サンプルデータ)**ビューと**Real Data (リアルデータ)**ビューを切り替えて、ダッシュボードウィジェットの外観を確認します。サンプルデータは、ダッシュボードがどのように見えるか、どのような種類の情報を見ることができるかを視覚化するのに役立ちます。**[Real Data (リアルデータ)]**オプションを使用して、デプロイメントの実データを表示します。

STEP 6 | （任意）エディタビューでダッシュボードをカスタマイズできます。

- ダッシュボードでウィジェットを並べ替える - ウィジェットを選択し、キャンバス内の必要な場所にドラッグ＆ドロップします。
- ウィジェットの編集 - 各ウィジェットの右上にある編集アイコンを使用してウィジェットの設定を編集します。使用できる設定はウィジェットによって異なり、すべてのウィジェットで同じではありません。たとえば、ウィジェット名、説明、オプションを編集して、評決、アクションなどのウィジェット内のデータをフィルタリングおよびソートできます。

  ウィジェットの設定は、エディタビューで編集することも、ダッシュボードを保存した後に編集することもできます。

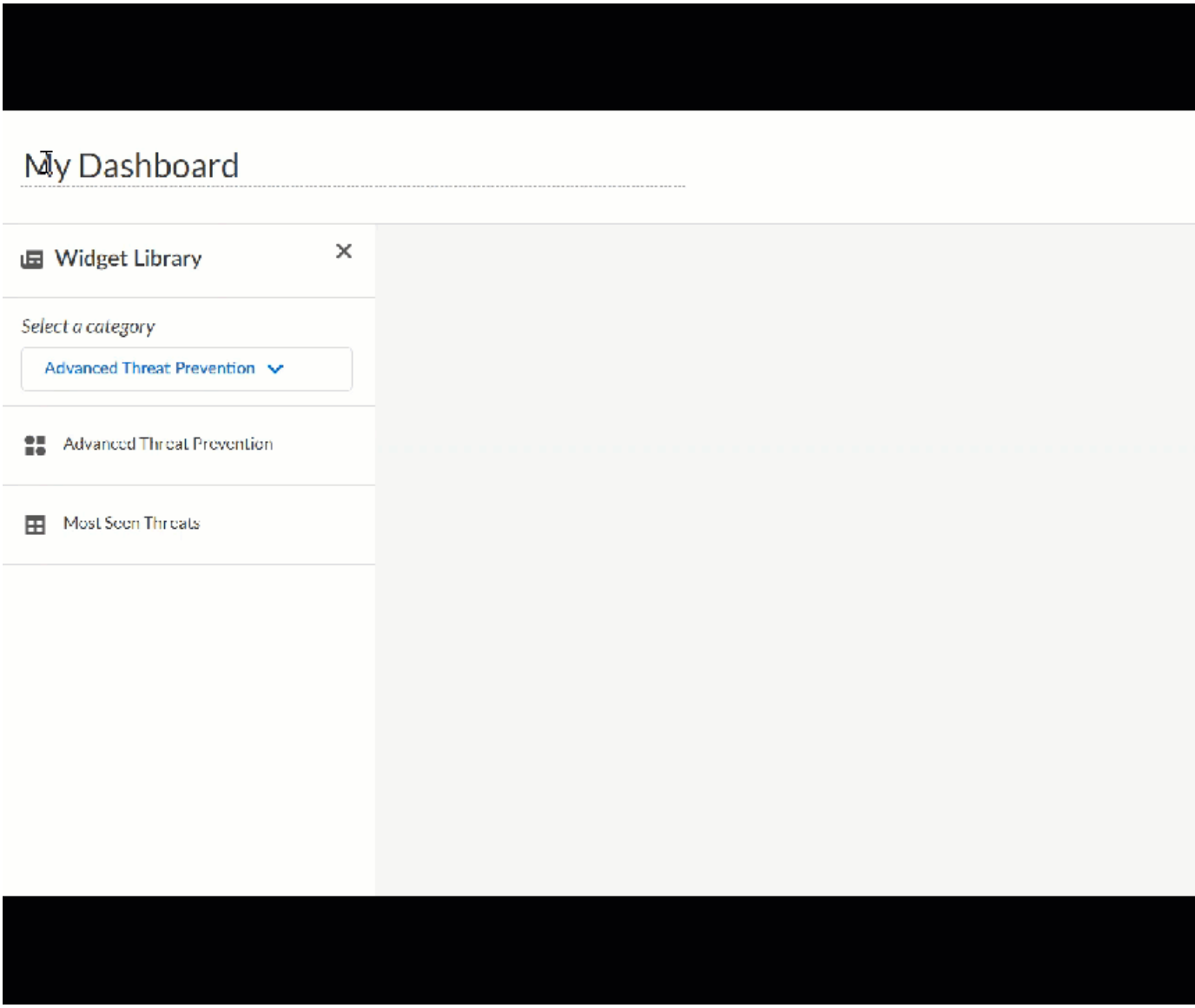
STEP 7 | ダッシュボードを保存し、ページ上部の**[Go to see dashboard (ダッシュボードを見る)]**をクリックしてダッシュボードを開きます。

STEP 8 | （任意）ダッシュボードを保存した後、次の操作を実行できます。

- ダッシュボードデータを表示する時間範囲を変更します。

  ダッシュボードを保存した後にのみ、時刻を変更できます。エディタビューでは、時間範囲はデフォルトで24時間です。

- 編集または削除アイコンを使用して、カスタムダッシュボードを変更または削除します。



ダッシュボード:デバイスの健全性

どこで使用できますか?	何が必要ですか?
• Software NGFW Creditsによって資金提供されたものを含むNGFW	☐ Strata Cloud Manager Essentials ☐ AIOps for NGFW Premium または Strata Cloud Manager Pro → Strata Cloud Managerで利用できる機能は、使用するライセンスによって異なります。

- **[Dashboards (ダッシュボード)] > [Device Health (デバイスの正常性)]**をクリックして開始します。

このダッシュボードには何が表示されますか?

ダッシュボードには、テナントにオンボードされ、テレメトリ データも送信しているすべてのファイアウォールの集計データが表示されます。

[Device Health (デバイスの正常性)］ダッシュボードには、オンボードされたNGFWの正常性スコアに基づいて、デプロイメントの累積的な正常性ステータスとパフォーマンスが表示されます。デバイスの正常性は、正常性スコアの重大度（0～100）と、それに対応する正常性グレード（良好、普通、不良、重大）によって決定されます。稼働状態スコアは、未解決のアラートの優先度、数量、種類、ステータスに基づいて計算されます。

ダッシュボードのデータはどのように利用できますか？

このダッシュボードは、次のことに役立ちます。

- 稼働状態スコアの履歴データを見ることで、ある期間に行った導入の改善点を把握できます。
- デプロイメントで注意が必要なデバイスを絞り込み、問題を解決するために問題の優先順位を付けます。

レポート機能（レポートのダウンロード、共有、スケジュール）は、このダッシュボードではサポートされていません。

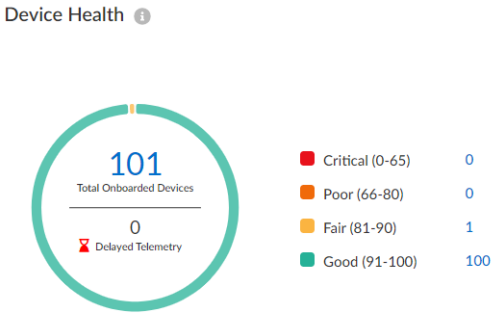
デバイス正常性ダッシュボード:デバイス正常性スコア

どこで使用できますか?	何が必要ですか?
• Software NGFW Creditsによって資金提供されたものを含むNGFW	☐ Strata Cloud Manager Essentials ☐ AIOps for NGFW Premium または Strata Cloud Manager Pro → Strata Cloud Managerで利用できる機能は、使用するライセンスによって異なります。

- **[Dashboards (ダッシュボード)]** > **[Device Health (デバイスの正常性)]** をクリックしてダッシュボードを表示します。

ダッシュボードウィジェットには、次の情報が表示されます。

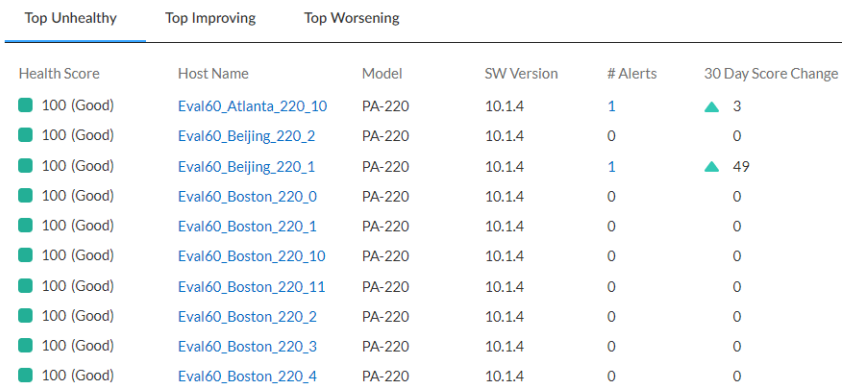
- オンボードされたNGFWの合計数。
- 12時間以上テレメトリデータを送信していないデバイスの数。
- デプロイメント内のオンボード デバイスの正常性スコアの重大度。番号のリンクをクリックすると、デバイスの詳細、デバイスの正常性統計、および注意が必要なデバイスのアラートを確認できます。



デバイス正常性ダッシュボード:デバイスの統計情報

どこで使用できますか?	何が必要ですか?
• Software NGFW Creditsによって資金提供されたものを含むNGFW	❑ Strata Cloud Manager Essentials ❑ AIOps for NGFW Premium または Strata Cloud Manager Pro → Strata Cloud Managerで利用できる機能は、使用するライセンスによって異なります。

- **[Dashboards (ダッシュボード)]** > **[Device Health (デバイスの正常性)]** をクリックしてダッシュボードを表示します。



トップの異常

デプロイメント中で正常性とパフォーマンスの問題が最も多いデバイスは、これらのデバイスです。ドリルダウンして、デバイスの詳細とデバイス上のアラートを表示することもできます。重要なアラートを修正して、稼働状態スコアとデプロイメントの稼働状態を改善します。

トップの改善

デバイスの現在の稼働状態スコアと比較して、稼働状態スコアが改善された上位10台のデバイスを30日間にわたって表示します。

トップの悪化

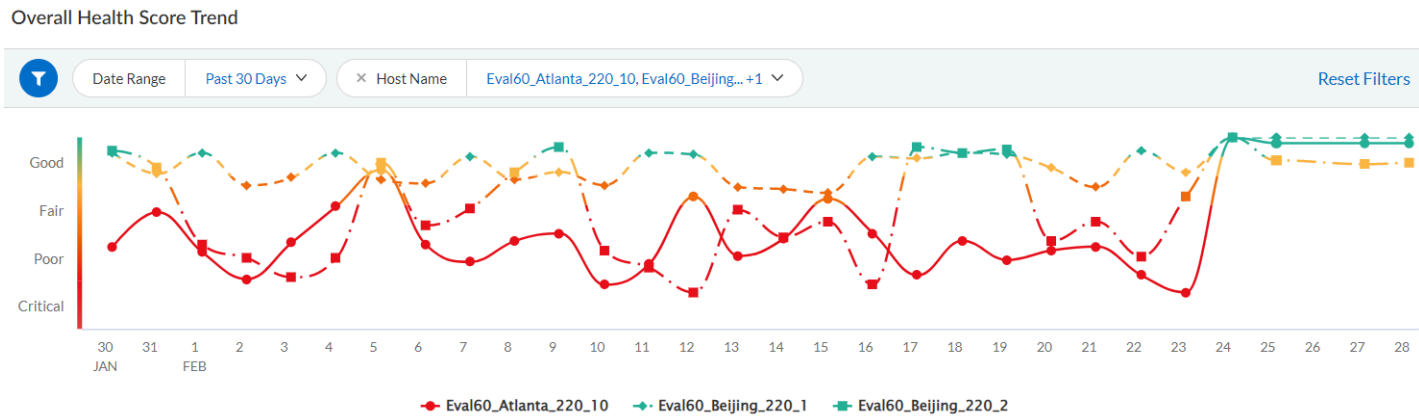
30日間の時間範囲でデバイスの状態を確認します。これらは、デバイスの現在のヘルススコアと比較してヘルススコアが低下した上位10のデバイスです。

デバイス正常性ダッシュボード:スコアトレンド

どこで使用できますか?	何が必要ですか?
• Software NGFW Creditsによって資金提供されたものを含むNGFW	❑ Strata Cloud Manager Essentials

どこで使用できますか?	何が必要ですか?
	❑ AIOps for NGFW Premium または Strata Cloud Manager Pro → Strata Cloud Managerで利用できる機能は、使用するライセンスによって異なります。

- **[Dashboards (ダッシュボード)] > [Device Health (デバイスの正常性)]** をクリックしてダッシュボードを表示します。



期間チャートには、選択した期間におけるデプロイメントの正常性の傾向が表示されます。トリガーポイントにカーソルを合わせると、ヘルススコアの重大度に貢献しているデバイスを確認できます。ホスト名、モデル、またはソフトウェアバージョンでフィルタリングされた1つ以上のデバイスの傾向を表示できます。

ダッシュボード:エグゼクティブ概要

どこで使用できますか?	何が必要ですか?
• Prisma Access (Managed by Panorama or Strata Cloud Manager) • Software NGFW Creditsによって資金提供されたものを含むNGFW • Prisma SD-WAN	これらの各ライセンスには、Strata Cloud Managerへのアクセスが含まれています。 ❑ Prisma Access ❑ AIOps for NGFW Premium license (use the Strata Cloud Manager app) ❑ Strata Cloud Manager Essentials ❑ Strata Cloud Manager Pro ❑ Prisma SD-WAN その他のライセンスと可視性に必要な前提条件は次のとおりです。 ❑ ダッシュボードの特定のウィジェットのロックを解除するライセンス ❑ ダッシュボードを表示する権限を持つロール → Strata Cloud Managerで利用できる機能は、使用するライセンスによって異なります。

- **Strata Cloud Manager** > **[Dashboards (ダッシュボード)]** > **[More Dashboards (その他のダッシュボード)]** > **[Executive Summary (エグゼクティブサマリー)]**をクリックして、作業を開始します。

このダッシュボードには何が表示されますか?

ダッシュボードには*Strata Logging Service*テナント毎の集計データが表示されます。

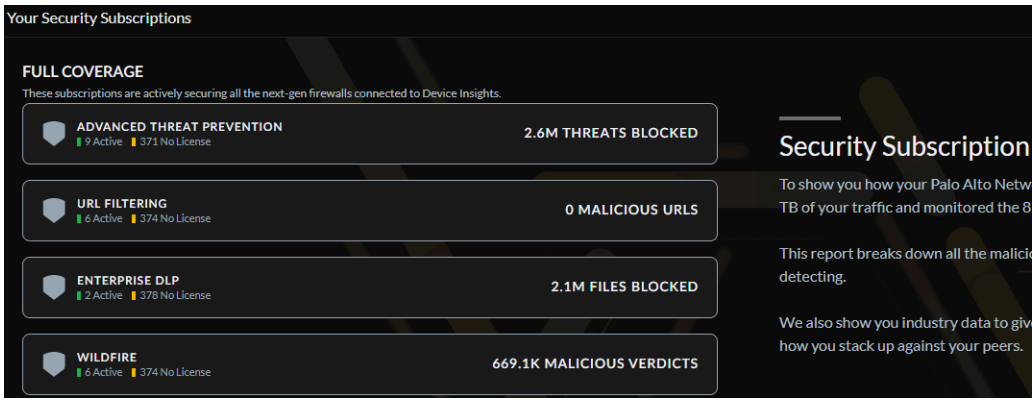
エグゼクティブサマリーダッシュボードは、Palo Alto Networksのセキュリティサブスクリプションがどのように保護を行うかを示しています。このレポートでは、これらのサブスクリプションが検出しているネットワーク内の悪意のあるアクティビティが分類されます。**WildFire**、高度な脅威防御、高度な**URL**フィルタリングおよびエンタープライズ**DLP**。ダッシュボードには、これらの各サービスのデータがセキュリティサービスのダッシュボードへのリンクとともに表示され、さらに詳しく調査できます。

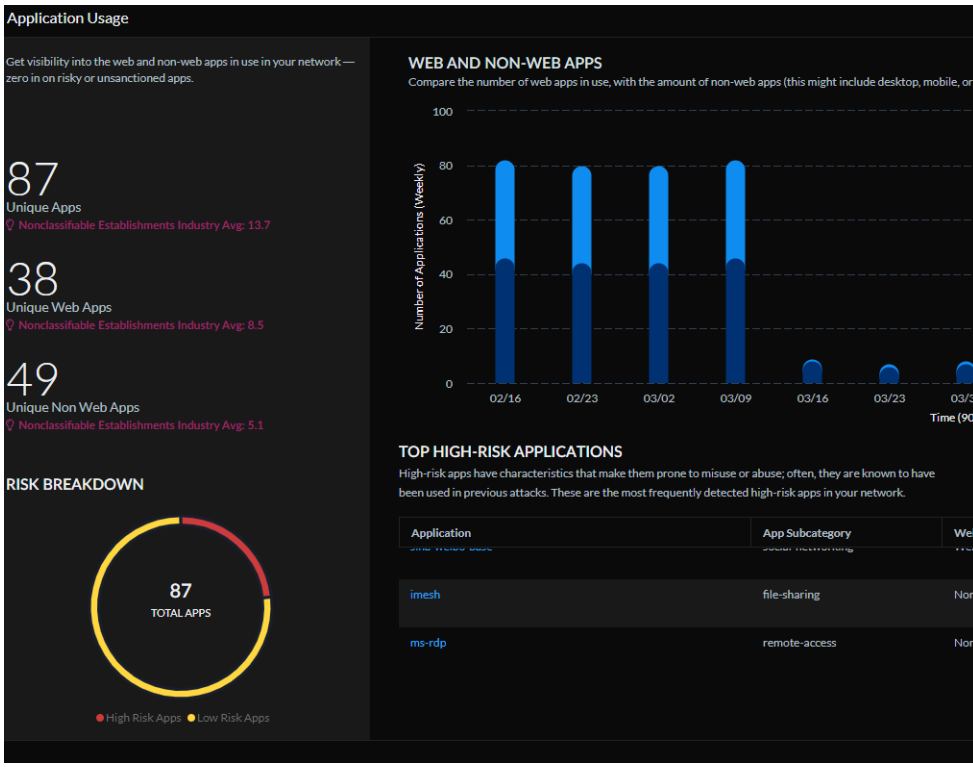
このダッシュボードはレポートをサポートしています。ダッシュボードの右上にあるアイコンは、このダッシュボードでレポートがサポートされていることを示します。このダッシュボードに表示されるデータを含むレポートを共有、ダウンロード、スケジュール設定できます。

ダッシュボードのデータをどのように活用できますか?

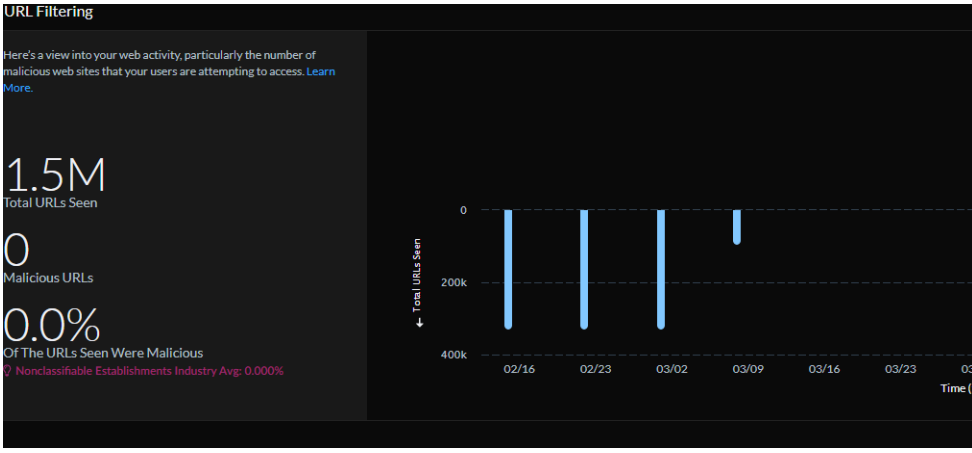
- アクティブなPalo Alto Networksサブスクリプションが検出しているすべての悪意のあるアクティビティを確認します。セキュリティギャップを埋めるために、サブスクリプション設定またはセキュリティルール設定を調整する必要があるかどうかを確認します。
- 業界データを示し、直面している脅威のランドスケープと、同業他社とどのように競合するかを示します。

ダッシュボードには、以下のデータが表示されます。

エグゼクティブサマリーダッシュボード:セキュリティサブスクリプション	このレポートでは、サブスクリプションが検知し、防止している悪意のあるアクティビティの数値を確認できます。 • 高リスクアプリケーション • 深刻な脅威（エクスプロイト、マルウェア、およびC2) • 悪意のあるウェブアクティビティ • ファイルベースの脅威(見たことのない脅威を含む) • データの損失 

エグゼクティブサマリーダッシュボード:アプリケーションの使用状況	リスクの高いアプリケーションのトラフィック ログを確認し、セキュリティ体制を強化する方法を確認します。 
エグゼクティブサマリーダッシュボード:高度な脅威防御 *Advanced Threat Prevention*(高度な脅威防御)ライセンスが必要です。	ほとんどの脅威を許可するセキュリティポリシールールを調べます。このルールを確認して、より厳格な脅威適用を有効にできる場所を確認してください。もっと詳しく知る。
エグゼクティブサマリーダッシュボード:**URL** フィルタリング 高度なURLフィルタリングのライセンスが必要です。	これがあなたのネットワーク内の悪意のあるウェブ活動の実態です。特にあなたのユーザーがアクセスしよ

うとしている悪意のあるウェブサイトの数をご覧くださ



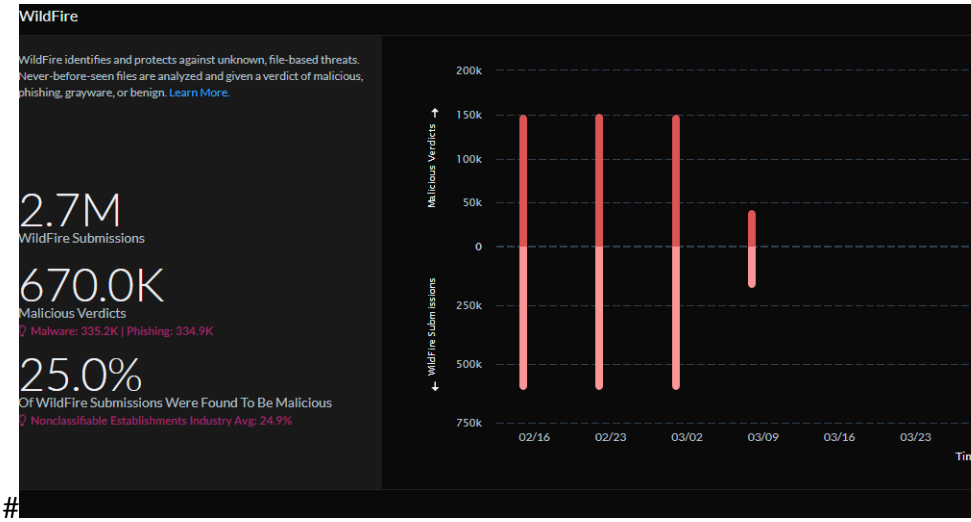
い。

エグゼクティブサマリーダッシュボード:**WildFire**

高度な*WildFire*ライセンスが必要です。

このダッシュボードのピアデータにより、業界の脅威の状況と、セキュリティカバレッジが類似組織と比較してどのようになっているかを確認できます。この業界データは、利用していないサブスクリプションについても表示され、セキュリティギャップを埋めるためにカバレッジを拡大できる場所があるかどうかを確認できます。

このダッシュボードが提供するデータの種類を拡大したものです。ここでは、WildFireがネットワークと業界を保護するために行っている作業を確認できます。詳細はこち



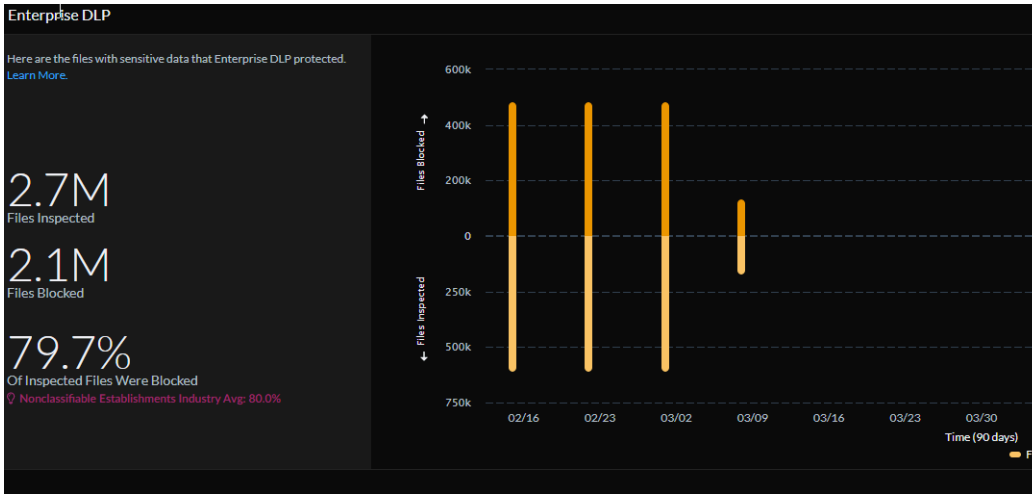
ら。#

エグゼクティブサマリーダッシュボード:**Enterprise DLP**

*Enterprise DLP*ライセンスが必要です。

Palo Alto Networks Enterprise DLPサービスがデータセキュリティ基準を徹底してデータを保護する方法をご覧ください。ダッシュボードでは、ほとんどのアップロードがDLPによってブロックされているアプリケーションと、ネットワーク内でDLPによってブロックされているファイルの総数を確認できます。また、このデータを使用して同業他社と比較し、セキュリティ対策基準のベンチマークを作成することもできます。

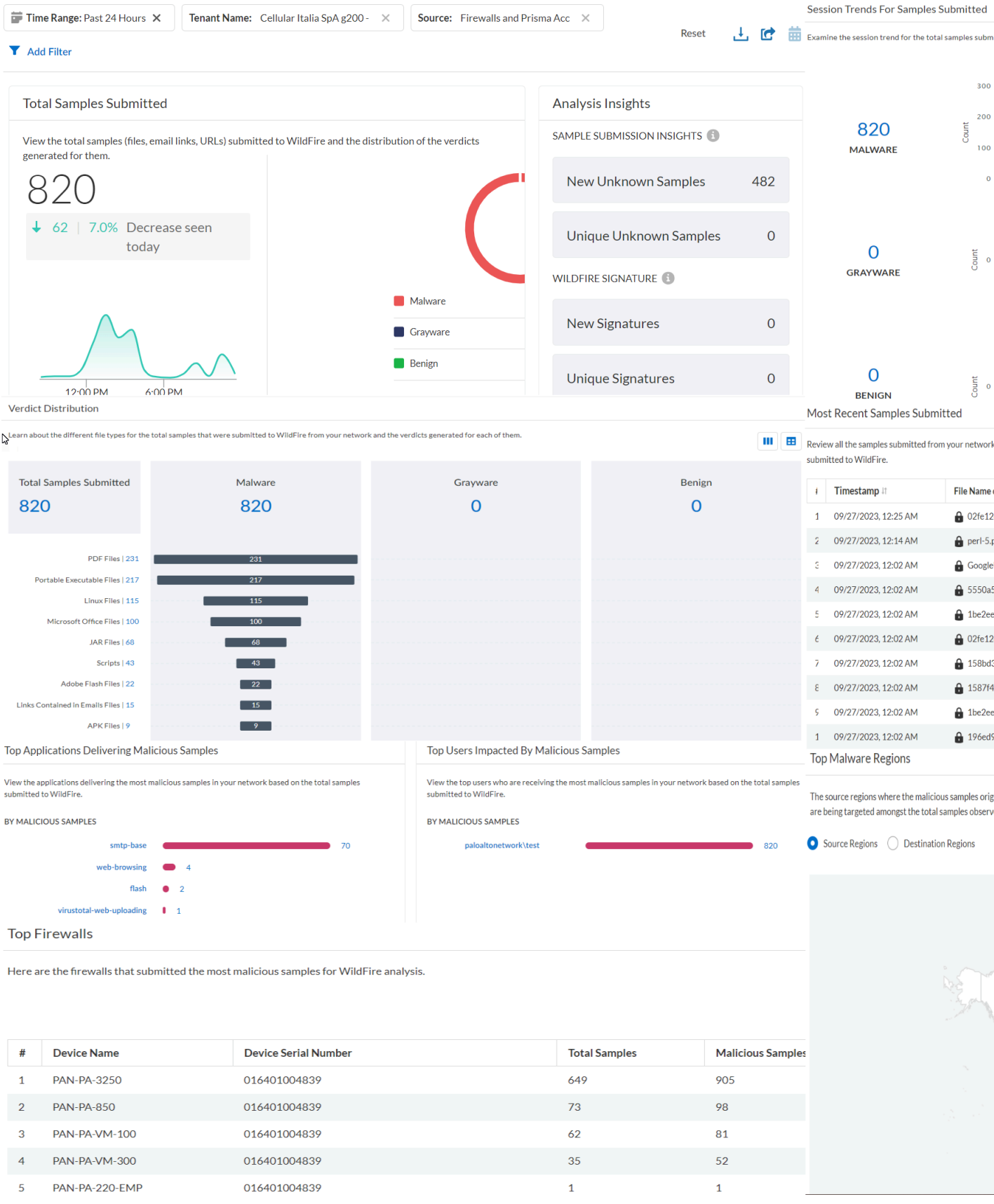
アプリケーションと送信元のユーザー名を確認して、DLPインシデントの発生元をより深く理解し、管理します。



ダッシュボード:WildFire

どこで使用できますか?	何が必要ですか?
• Prisma Access (Managed by Panorama or Strata Cloud Manager) • Software NGFW Creditsによって資金提供されたものを含むNGFW	これらの各ライセンスには、Strata Cloud Managerへのアクセスが含まれています。 ❑ Prisma Access ❑ AIOps for NGFW Premium license (use the Strata Cloud Manager app) ❑ Strata Cloud Manager Essentials ❑ Strata Cloud Manager Pro その他のライセンスと可視性に必要な前提条件は次のとおりです。 ❑ ダッシュボードを表示する権限を持つロール ❑ Advanced WildFire → Strata Cloud Managerで利用できる機能は、使用するライセンスによって異なります。

- 開始するには、**Strata Cloud Manager** > **[Dashboards (ダッシュボード)]** > **[More Dashboards (その他のダッシュボード)]** > **[WildFire]**をクリックします。



#	Device Name	Device Serial Number	Total Samples	Malicious Samples
1	PAN-PA-3250	016401004839	649	905
2	PAN-PA-850	016401004839	73	98
3	PAN-PA-VM-100	016401004839	62	81
4	PAN-PA-VM-300	016401004839	35	52
5	PAN-PA-220-EMP	016401004839	1	1

このダッシュボードには何が表示されますか？

ダッシュボードにはテナント サービス グループ（*TSG*）毎の集計データが表示されます。ダッシュボードには、テナントが カスタマー サポート ポータル アカウントと 1 対 1 でマッピング されている場合、テナントに 関連付けられている *Prisma Access*、*Palo Alto Networks*ファイアウォール、および*Panorama*アプライアンス全体のデータが表示されます。カスタマー サポート ポータルごとに複数のテナントが関連付けられている場合、ダッシュボードには他の送信元からのデータは表示されません。

WildFireダッシュボードには、ファイルや実行可能ファイルに隠されたまったく新しいマルウェアからWildFireがどのように保護しているかが表示されます。このダッシュボードは レポートをサポートしています。ダッシュボードの右上にあるアイコンは、このダッシュボードでレポートがサポートされていることを示します。このダッシュボードに表示されるデータを含むレポートを共有、ダウンロード、スケジュール設定できます。

ダッシュボードのデータはどのように利用できますか？

このダッシュボードを使用して、

- （AIOps for NGFW Premiumライセンスが必要)WildFire の送信を監視し、分析のためにWildFireクラウドに送信された WildFire サンプルの詳細を取得できます。
- 対象ユーザー、ファイルを配信したアプリケーション、分析のためにサンプルを送信したファイアウォール、およびファイルのコマンド アンド コントロール アクティビティに関係するすべてのURLの詳細を表示できます。
- （AIOps for NGFW Premiumライセンスが必要) を取得して、 WildFire ログ と分析レポートを表示し、レポートに基づいてデプロイメントの WildFire 設定 を調整します。

WildFireダッシュボード：フィルタ

どこで使用できますか?	何が必要ですか?
• Prisma Access (Managed by Panorama or Strata Cloud Manager) • Software NGFW Creditsによって資金提供されたものを含むNGFW	これらの各ライセンスには、Strata Cloud Managerへのアクセスが含まれています。 ☐ Prisma Access ☐ AIOps for NGFW Premium license (use the Strata Cloud Manager app) ☐ Strata Cloud Manager Essentials ☐ Strata Cloud Manager Pro その他のライセンスと可視性に必要な前提条件は次のとおりです。 ☐ ダッシュボードを表示する権限を持つロール

どこで使用できますか?	何が必要ですか?
	❑ Advanced WildFire → Strata Cloud Managerで利用できる機能は、使用するライセンスによって異なります。

WildFireダッシュボードには、ダッシュボードから特定のデータを絞り込むためのこれらのフィルターオプションが用意されています。

- **[Time range (時間範囲)]**-過去**24**時間、過去**7**日間、過去**30**日間、またはカスタム時間範囲から選択して、特定の期間のデータを表示します。
- テナント名-ダッシュボードデータが表示されるテナント。
- 送信元 - ダッシュボードデータの範囲は、Prisma AccessおよびPalo Alto Networksのファイアウォールから取得されます。
- サンプル - パブリックまたはプライベートオプションから選択すると、Wildfireパブリック クラウドまたはプライベートクラウド環境から送信されたデータが表示されます。
- 評決 - WildFire分析で良性、マルウェア、またはグレイウェアとして識別されたサンプルを表示します。
- アクション - [許可]または[ブロック]オプションから選択すると、ポリシー ルールによって許可またはブロックされているWildFireサンプルが表示されます。
- ファイルタイプ - WildFireで分析したサンプルのファイルタイプに基づいてデータを表示します。WildFire解析でサポートされているファイルタイプについてご確認ください。
- ファイルハッシュ - WildFireで分析されたファイルハッシュのデータを表示します。以下に、分析されるファイルごとにWildFireによって生成されるハッシュ バージョンの一覧を示します。
  - **SHA-1** – ファイルのSHA-1値が表示されます。
  - **SHA-256** – ファイルのSHA-256値が表示されます。
  - **MD5** – ファイルの MD5 情報を表示します。
- アプリ名 - アプリケーションから配信されるサンプルに基づいてデータをフィルタリングします。
- 発信元リージョン - 特定の場所から送信されたサンプルを表示するためのフィルター。
- 宛先地域 - 特定の場所で受信されたサンプルを表示するフィルタ。
- ユーザー名 - ネットワーク内のサンプルの配信対象となるユーザのデータをフィルタリングするためのユーザ名を入力します。
- デバイスのシリアルナンバー - WildFire分析のためにサンプルを送信したデバイスのデータをフィルタリングします。

WildFireダッシュボード：送信済みの総サンプル数

どこで使用できますか?	何が必要ですか?
• Prisma Access (Managed by Panorama or Strata Cloud Manager) • Software NGFW Creditsによって資金提供されたものを含むNGFW	これらの各ライセンスには、Strata Cloud Managerへのアクセスが含まれています。 ❑ Prisma Access ❑ AIOps for NGFW Premium license (use the Strata Cloud Manager app) ❑ Strata Cloud Manager Essentials ❑ Strata Cloud Manager Pro その他のライセンスと可視性に必要な前提条件は次のとおりです。 ❑ ダッシュボードを表示する権限を持つロール ❑ Advanced WildFire → Strata Cloud Managerで利用できる機能は、使用するライセンスによって異なります。

- ダッシュボードを表示するには、**[Dashboards (ダッシュボード)]** > **[More Dashboards (その他のダッシュボード)]** > **[WildFire]**をクリックします。

選択した期間にWildFire分析のために提出されたサンプルの総数。ウィジェットには、各送信元から送信されたサンプルの数と、サンプルに対して生成された評決が表示されます。ウィジェットには、WildFire分析のために提出されたサンプルの急増も表示されます。マルウェアサンプルの急増を調査し、ネットワークへの脅威の影響を軽減するために対策を講じます。

WildFireダッシュボード：解析インサイト

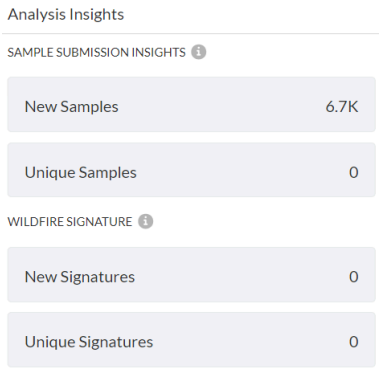
どこで使用できますか?	何が必要ですか?
• Prisma Access (Managed by Panorama or Strata Cloud Manager) • Software NGFW Creditsによって資金提供されたものを含むNGFW	これらの各ライセンスには、Strata Cloud Managerへのアクセスが含まれています。 ❑ Prisma Access ❑ AIOps for NGFW Premium license (use the Strata Cloud Manager app) ❑ Strata Cloud Manager Essentials ❑ Strata Cloud Manager Pro

どこで使用できますか?	何が必要ですか?
	その他のライセンスと可視性に必要な前提条件は次のとおりです。 □ ダッシュボードを表示する権限を持つロール □ Advanced WildFire → Strata Cloud Managerで利用できる機能は、使用するライセンスによって異なります。

- ダッシュボードを表示するには、**[Dashboards (ダッシュボード)]** > **[More Dashboards (その他のダッシュボード)]** > **[WildFire]**をクリックします。

ネットワークから送信された固有のWildFireサンプルと生成されたシグネチャに関するインサイトが得られます。データを使用して、選択した期間にネットワークでのみ確認された新しい脅威と、生成されたシグネチャによってネットワークが保護されている回数を把握することができます。

- 固有の不明サンプル - ネットワークからWildFireに送信されたサンプルのうち、ネットワーク内でのみ見られ、以前はWildFireに知られておらず、他のパブリックフィードやプライベートフィードでは利用できないサンプルの数。
- 新しい不明のサンプル - ネットワークからWildFireに送信された新しいサンプルのうち、WildFireにとって以前は未知であったものの数（明確なsha256付き）。
- 固有シグネチャ - 環境に固有のサンプルから生成されたシグネチャの数。
- 新しいシグネチャ - アップロードしたすべてのサンプルからWildFireによって作成された新しいシグネチャの数。



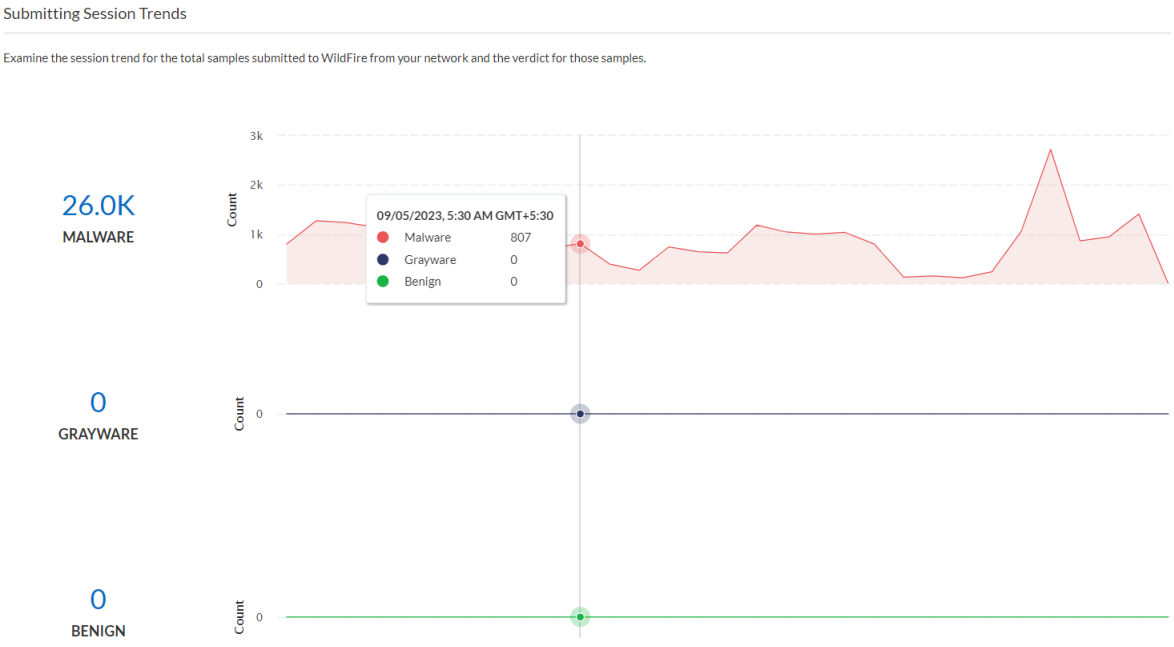
WildFireダッシュボード：送信されたサンプルのセッション傾向

どこで使用できますか?	何が必要ですか?
• Prisma Access (Managed by Panorama or Strata Cloud Manager)	これらの各ライセンスには、Strata Cloud Managerへのアクセスが含まれています。

どこで使用できますか?	何が必要ですか?
• Software NGFW Creditsによって資金提供されたものを含むNGFW	❑ Prisma Access ❑ AIOps for NGFW Premium license (use the Strata Cloud Manager app) ❑ Strata Cloud Manager Essentials ❑ Strata Cloud Manager Pro その他のライセンスと可視性に必要な前提条件は次のとおりです。 ❑ ダッシュボードを表示する権限を持つロール ❑ Advanced WildFire → Strata Cloud Managerで利用できる機能は、使用するライセンスによって異なります。

- ダッシュボードを表示するには、**[Dashboards (ダッシュボード)]** > **[More Dashboards (その他のダッシュボード)]** > **[WildFire]**をクリックします。

ネットワークからWildFireに送信済みの総サンプル数と、それらのサンプルの評決に関するセッションの傾向を調べます。これらのサンプルに対して IOC 検索を実行すると、ネットワーク内のサンプルの履歴とサンプルのグローバルな分析結果を知ることができます。



WildFireダッシュボード：判定の配布

どこで使用できますか?	何が必要ですか?
• Prisma Access (Managed by Panorama or Strata Cloud Manager) • Software NGFW Creditsによって資金提供されたものを含むNGFW	これらの各ライセンスには、Strata Cloud Managerへのアクセスが含まれています。 ❑ Prisma Access ❑ AIOps for NGFW Premium license (use the Strata Cloud Manager app) ❑ Strata Cloud Manager Essentials ❑ Strata Cloud Manager Pro その他のライセンスと可視性に必要な前提条件は次のとおりです。 ❑ ダッシュボードを表示する権限を持つロール ❑ Advanced WildFire → Strata Cloud Managerで利用できる機能は、使用するライセンスによって異なります。

- ダッシュボードを表示するには、**[Dashboards (ダッシュボード)]** > **[More Dashboards (その他のダッシュボード)]** > **[WildFire]**をクリックします。

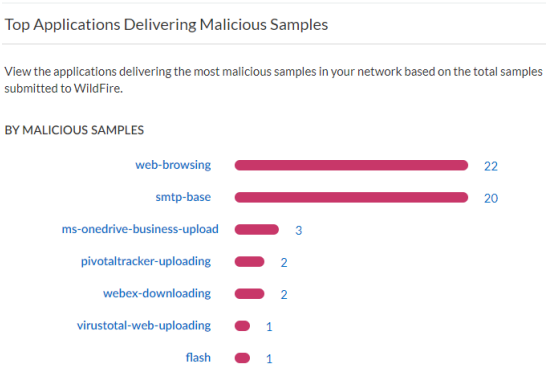
WildFireがネットワークで初めて検出したNET新規サンプルの判定について詳しく調査します。マルウェアが隠れていることが最も多いサンプルタイプに焦点を当てます。リンクをクリックすると、サンプルの詳細を知ることができます。

WildFireダッシュボード：悪意のあるサンプルを配信する上位のアプリケーション

どこで使用できますか?	何が必要ですか?
• Prisma Access (Managed by Panorama or Strata Cloud Manager) • Software NGFW Creditsによって資金提供されたものを含むNGFW	これらの各ライセンスには、Strata Cloud Managerへのアクセスが含まれています。 ❑ Prisma Access ❑ AIOps for NGFW Premium license (use the Strata Cloud Manager app) ❑ Strata Cloud Manager Essentials ❑ Strata Cloud Manager Pro その他のライセンスと可視性に必要な前提条件は次のとおりです。 ❑ ダッシュボードを表示する権限を持つロール ❑ Advanced WildFire → Strata Cloud Managerで利用できる機能は、使用するライセンスによって異なります。

- ダッシュボードを表示するには、**[Dashboards (ダッシュボード)]** > **[More Dashboards (その他のダッシュボード)]** > **[WildFire]**をクリックします。

ネットワークで最も悪意のあるサンプルを配信したアプリケーションの詳細を確認します。悪意のあるサンプル数をクリックすると、サンプルの詳細が表示されます。

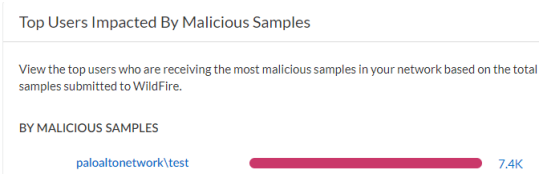


WildFireダッシュボード：悪意のあるサンプルによって影響を受けたトップユーザー

どこで使用できますか?	何が必要ですか?
• Prisma Access (Managed by Panorama or Strata Cloud Manager) • Software NGFW Creditsによって資金提供されたものを含むNGFW	これらの各ライセンスには、Strata Cloud Managerへのアクセスが含まれています。 ❑ Prisma Access ❑ AIOps for NGFW Premium license (use the Strata Cloud Manager app) ❑ Strata Cloud Manager Essentials ❑ Strata Cloud Manager Pro その他のライセンスと可視性に必要な前提条件は次のとおりです。 ❑ ダッシュボードを表示する権限を持つロール ❑ Advanced WildFire → Strata Cloud Managerで利用できる機能は、使用するライセンスによって異なります。

- ダッシュボードを表示するには、**[Dashboards (ダッシュボード)]** > **[More Dashboards (その他のダッシュボード)]** > **[WildFire]**をクリックします。

これは、ネットワーク内で悪意のあるサンプルの配信に最も頻繁に使用されるユーザーアカウントを示しています。ユーザー名をクリックして、ユーザー アクティビティ パターンを調査します。

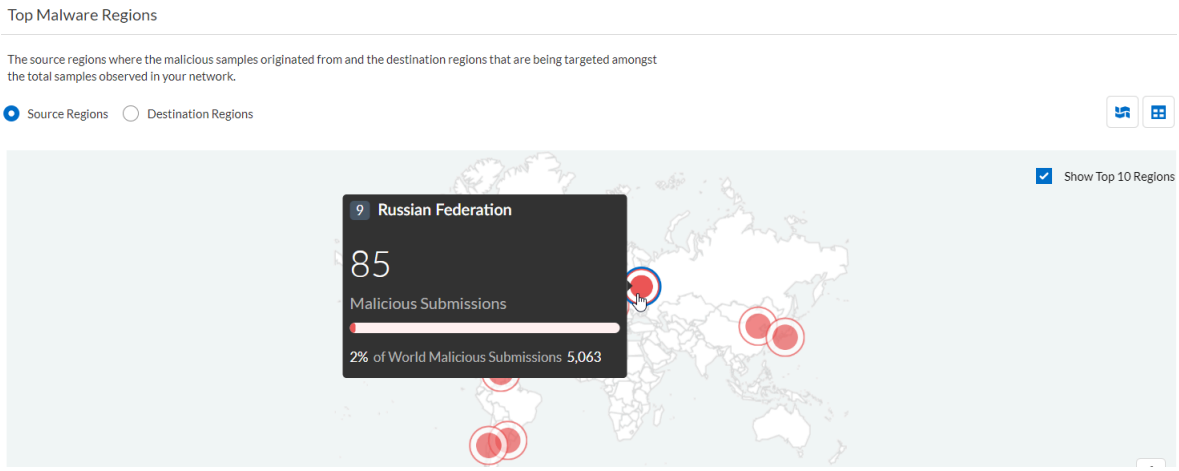


WildFireダッシュボード：上位のマルウェア領域

どこで使用できますか?	何が必要ですか?
• Prisma Access (Managed by Panorama or Strata Cloud Manager) • Software NGFW Creditsによって資金提供されたものを含むNGFW	これらの各ライセンスには、Strata Cloud Managerへのアクセスが含まれています。 ❑ Prisma Access ❑ AIOps for NGFW Premium license (use the Strata Cloud Manager app) ❑ Strata Cloud Manager Essentials ❑ Strata Cloud Manager Pro その他のライセンスと可視性に必要な前提条件は次のとおりです。 ❑ ダッシュボードを表示する権限を持つロール ❑ Advanced WildFire → Strata Cloud Managerで利用できる機能は、使用するライセンスによって異なります。

- ダッシュボードを表示するには、**[Dashboards (ダッシュボード)]** > **[More Dashboards (その他のダッシュボード)]** > **[WildFire]**をクリックします。

悪意のあるサンプルの発信元またはネットワーク内で配信された場所を確認します。送信元と宛先のリージョンのサンプル数をマップまたは表形式で表示できます。マルウェアの標的となる地域やマルウェア攻撃の種類を絞り込む際に使用します。



WildFireダッシュボード：トップファイアウォール

どこで使用できますか?	何が必要ですか?
• Software NGFW Creditsによって資金提供されたものを含むNGFW	これらの各ライセンスには、Strata Cloud Managerへのアクセスが含まれています。 ❑ AIOps for NGFW Premium license (use the Strata Cloud Manager app) ❑ Strata Cloud Manager Essentials ❑ Strata Cloud Manager Pro その他のライセンスと可視性に必要な前提条件は次のとおりです。 ❑ ダッシュボードを表示する権限を持つロール ❑ Advanced WildFire → Strata Cloud Managerで利用できる機能は、使用するライセンスによって異なります。

- ダッシュボードを表示するには、**[Dashboards (ダッシュボード)]** > **[More Dashboards (その他のダッシュボード)]** > **[WildFire]**をクリックします。

WildFire分析対象として最も悪意のあるサンプルを送信したファイアウォールを表示します。これらのファイアウォールを見直して、影響を受けるエンドポイントを追跡し、ポリシー ルールを再設定して脅威を軽減し、悪意のあるファイルをソースで封じ込めます。

Top Firewalls

Here are the firewalls that submitted the most malicious samples for WildFire analysis.

#	Device Name	Device Serial Number	Total Samples	Malicious Samples
1	PAN-PA-3250	016401004839	4866	6947
2	PAN-PA-5220-AC	016401004839	1168	1715
3	PAN-PA-VM-300	016401004839	619	1054
4	PAN-PA-VM-100	016401004839	673	1017
5	PAN-PA-850	016401004839	39	56
6	PAN-PA-VM-500-E60	016401004839	5	6
7	PAN-PA-220-EMP	016401004839	3	5
8	PAN-PA-5260-AC	016401004839	1	1

ダッシュボード:DNS セキュリティ

どこで使用できますか?	何が必要ですか?
• Prisma Access (Managed by Panorama or Strata Cloud Manager) • Software NGFW Creditsによって資金提供されたものを含むNGFW	これらの各ライセンスには、Strata Cloud Managerへのアクセスが含まれています。 ❑ Prisma Access ❑ AIOps for NGFW Premium license (use the Strata Cloud Manager app) ❑ Strata Cloud Manager Essentials ❑ Strata Cloud Manager Pro その他のライセンスと可視性に必要な前提条件は次のとおりです。 ❑ ダッシュボードを表示する権限を持つロール ❑ DNSセキュリティまたは高度なDNSセキュリティ → Strata Cloud Managerで利用できる機能は、使用するライセンスによって異なります。

- **Strata Cloud Manager** > **[Dashboards (ダッシュボード)]** > **[More Dashboards (その他のダッシュボード)]** > **[DNS Security (DNSセキュリティ)]**をクリックして、作業を開始します。

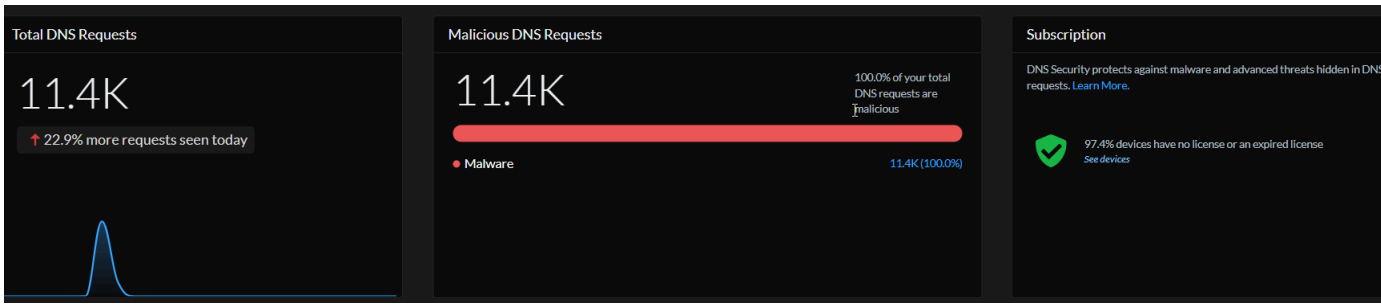
このダッシュボードには何が表示されますか?

ダッシュボードにはテナント サービス グループ（*TSG*）毎の集計データが表示されます。ダッシュボードには、*Prisma Access*、*Palo Alto Networks*のファイアウォール、テナントに関連付けられた*Panorama*アプライアンスのデータが表示されます。

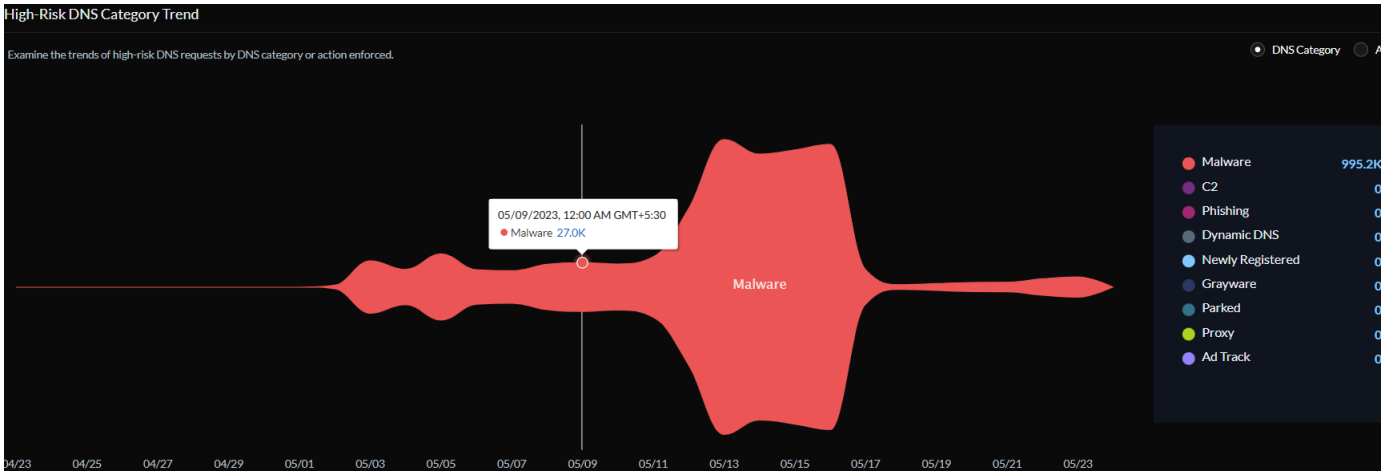
新しい DNS Security ダッシュボードでは、DNS Security サブスクリプションが DNS を使用する高度な脅威やマルウェアからどのように保護されているかを確認できます。ダッシュボードに表示される情報は、時間範囲、実行したアクション、ドメイン、リゾルバIP、DNSカテゴリでフィルタリングすることもできます。ダッシュボードにデータが表示されるソースとテナント名は、[テナント名]フィルタと[ソース]フィルタに表示されます。表示内容:DNSリクエスト統計と傾向

- **[Total DNS Requests (DNS**リクエスト総数**)]** - DNS Securityによって処理されたDNSリクエストの総数が表示されます。折れ線グラフは、ユーザが定義した時間範囲に基づいてDNS要求の数を示します。カスタム時間範囲を指定すると、それに応じて折れ線グラフが更新されます。

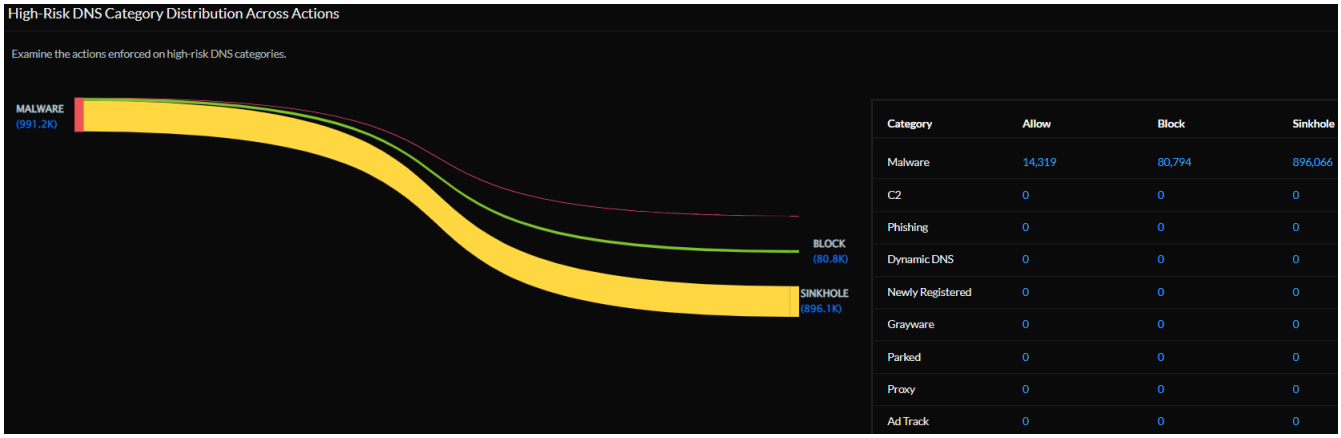
- ［**Malicious DNS Requests (**悪意のある**DNS**リクエスト**)**］ - 悪意ある DNS 要求として分類された DNS 要求を積み上げ棒グラフで表示します。番号リンクをクリックすると、DNSリクエストの詳細が表示されます。
- サブスクリプション - DNSセキュリティサブスクリプションが有効なネットワーク内のデバイスの数が表示されます。DNSセキュリティが搭載されていない、または契約が経過するデバイスの割合も、完全なリストへのリンクとともに表示されます。



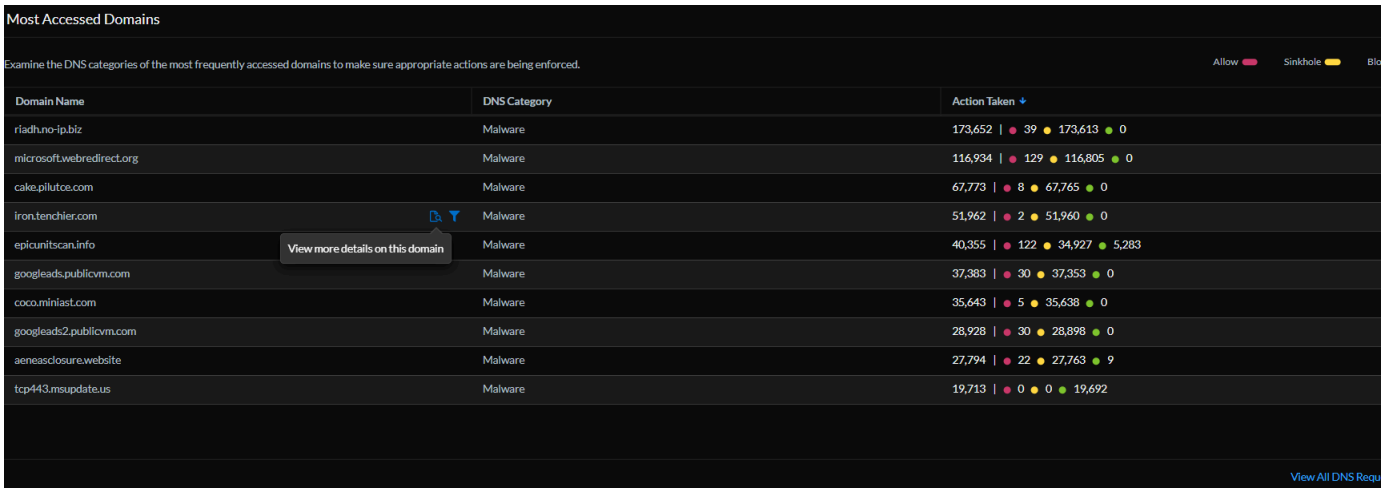
- 高リスク**DNS**カテゴリ傾向 - DNSカテゴリ別、またはDNSカテゴリに対して行われたアクション別に、高リスクDNS要求の傾向を調べます。特定のフローにカーソルを合わせると、ポップアップが開き、実行された要求の数やアクションの種類が表示されます。



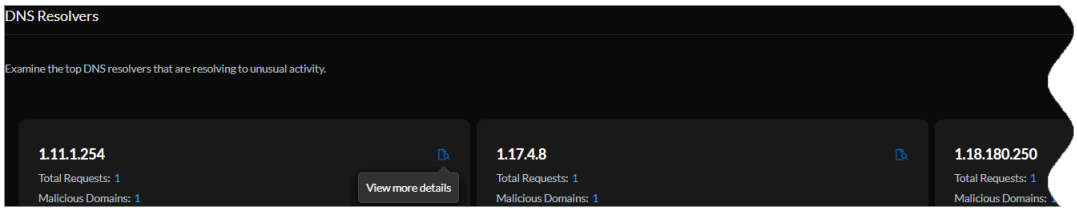
- アクション全体にわたるハイリスク**DNS**カテゴリの分散 - ファイアウォールが特定のハイリスクDNSカテゴリに対して行っているアクションを調べます。



- 最もアクセスの多いドメイン - DNSカテゴリと実行されたアクションとともに、ネットワークから最もよく要求されるドメインの上位10のリストを提供します。ドメインの詳細と関連するログを表示できます。アクセスされたドメインの完全なリストを表示するには、**[View All DNS Request (すべてのDNS要求を表示)]**を選択します。



- **DNS**リソルバー - ネットワーク内の悪意のある疑わしいDNS解決アクティビティを監視します。悪意のあるドメインに解決される上位のDNSリゾルバーと、不審なほど数の少ないDNS要求を解決しているリゾルバーを表示します。検索アイコンをクリックすると、アーティファクト（IPアドレス）の詳細が表示されます。ネットワーク内のアーティファクトの履歴とグローバル解析結果を表示できます。



- ユーザが悪意のあるドメインを訪問する - 悪意のあるURLのホスト名またはドメインを解決しようとしているネットワーク上ホストを調べます。

- **(Advanced DNS Security ライセンスが必要)** ハイジャックされたドメイン - 高度なDNSSecurity によって決定されたハイジャックされたドメインの一覧を提供します。エントリごとに、送信元IPに基づいた分類理由とトラフィック ヒット数があります。

Hijacked Domains

Hijacked	Hits
xyz.test-ipv4-wildcard.hijacking.testpanw.com	117
www.test-ipv4-wildcard.hijacking.testpanw.com	118
www.test-cname-rrname-sub-wc.hijacking.testpanw.com	353
test.test-ipv4-wildcard.hijacking.testpanw.com	118
test-ipv6.hijacking.testpanw.com	469
test-ipv4.hijacking.testpanw.com	472
test-cname-rrname.hijacking.testpanw.com	234
test-cname-rrname-wc.hijacking.testpanw.com	117
qpwc.test-ipv4-wildcard.hijacking.testpanw.com	118

- **(Advanced DNS Security ライセンスが必要)** 設定ミスドメイン - ユーザーが指定したパブリック相対親ドメインに関連付けられた解決不能ドメインのリストを提供します。エントリごとに、設定ミスの理由と、送信元IPに基づくトラフィック ヒット数があります。

Misconfigured Domains

Misconfigured Domains	Misconfigured Reasons	Hits
demo.test-dnsmisconfig-zone-dangling.testpanw.com	test-dnsmisconfig-zone-dangling.testpanw.com:A:1.2.3.4 the IP 1.2.3.4 is allocatable	117
adns-demo.test-dnsmisconfig-zone-dangling.testpanw...	test-dnsmisconfig-zone-dangling.testpanw.com:A:1.2.3.4 the IP 1.2.3.4 is allocatable	117
abc.test-dnsmisconfig-zone-dangling.testpanw.com	test-dnsmisconfig-zone-dangling.testpanw.com:A:1.2.3.4 the IP 1.2.3.4 is allocatable	589
123demo.test-dnsmisconfig-zone-dangling.testpanw.c...	test-dnsmisconfig-zone-dangling.testpanw.com:A:1.2.3.4 the IP 1.2.3.4 is allocatable	0
123.test-dnsmisconfig-zone-dangling.testpanw.com	test-dnsmisconfig-zone-dangling.testpanw.com:A:1.2.3.4 the IP 1.2.3.4 is allocatable	471

このダッシュボードはレポートをサポートしています。ダッシュボードの右上にあるアイコンは、このダッシュボードでレポートがサポートされていることを示します。このダッシュボードに表示されるデータを含むレポートを共有、ダウンロード、スケジュール設定できます。

ダッシュボードのデータをどのように活用できますか?

このダッシュボードでは以下が実行可能です。

- DNSリクエストの処理方法と分類方法を調べる
- DNSベースの脅威に関する洞察を得る
- 高度なDNSセキュリティで乗っ取られたドメインや誤って設定されたドメインからのDNSリクエストを検出する

ダッシュボード:AI Runtime Security (AIランタイムセキュリティ)

Strata Cloud Manager（SCM）のコマンドセンター ダッシュボードでは、ポッド、モデル、アプリ、VM、名前空間など、クラスタとVMにデプロイされたクラウドワークロードを統合ビューで確認できます。

どこで使用できますか?	何が必要ですか?
• AIランタイムセキュリティ	☐ AIランタイムセキュリティライセンスの有効化 ☐ AIランタイムセキュリティセットアップの前提条件 ☐ オンボードとSCMでのクラウドアカウントの有効化

クラウドのリソースを見る

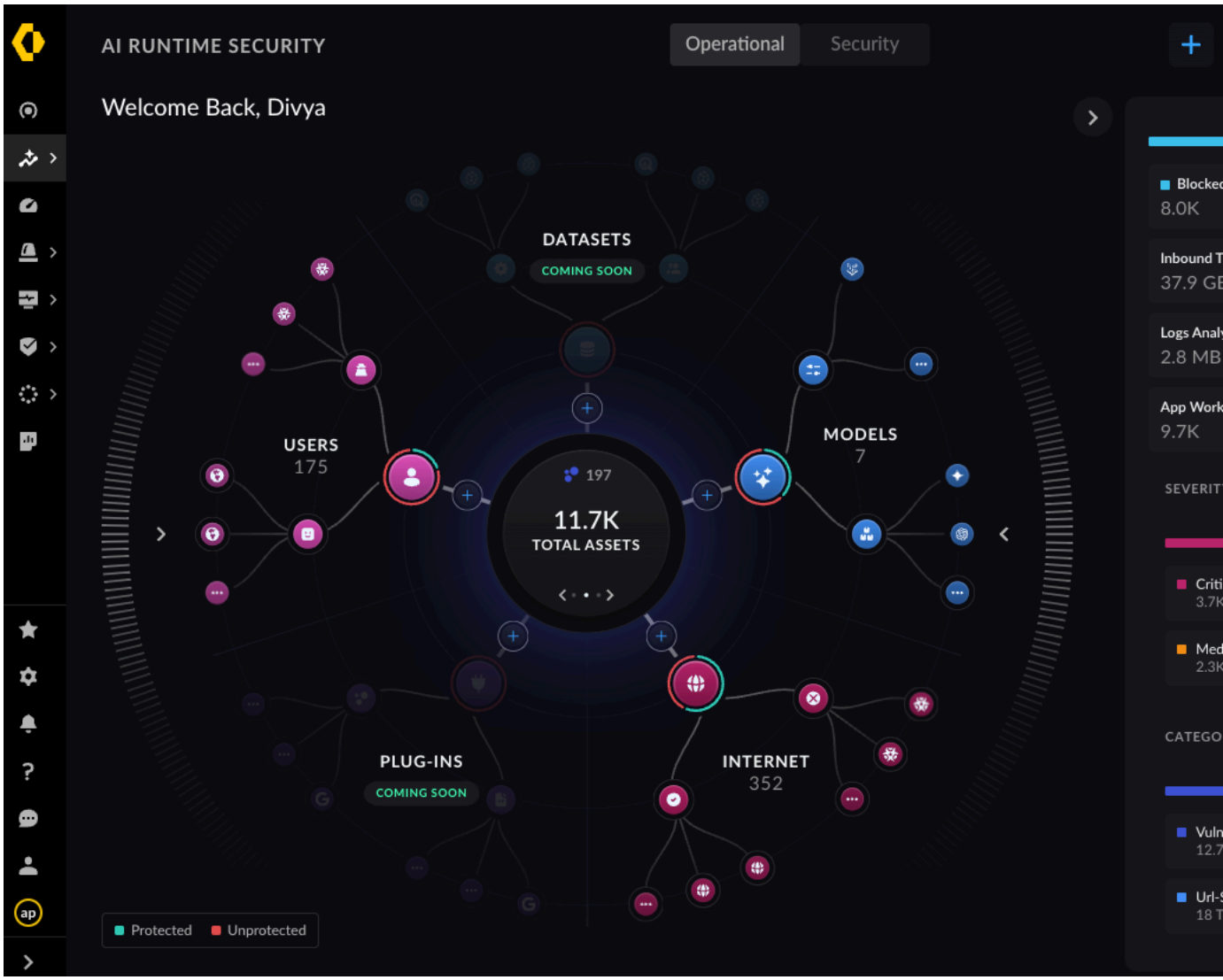
SCMでクラウドアカウントを正常にオンボーディングし、サービスアカウントをアクティブ化すると、SCMダッシュボードでは、クラウドワークロードの資産検出がリアルタイムで統合されます。

SCMの［インサイト］→［AIランタイムセキュリティ］の［クラウドアプリケーションコマンドセンター］では、オンボーディングされたクラウドアカウント内のすべてのクラウド資産を検出するための実用的なインサイトが表示されます。

SCMダッシュボードの資産検出は、オペレーションビューとセキュリティビューに分類されます。

検出では、脆弱性の検出、URLセキュリティ、プロンプトインジェクションなどの脅威の緊急度とリスクカテゴリに基づいて、脅威の内訳が表示されます。

1. ［オペレーション］ビューは、次の項目を集約したビューです。
   1. クラウド環境で発見された資産の総数と内訳
   2. トラフィックフロー - AIランタイムセキュリティインスタンスによる保護と非保護
   3. アプリケーション ワークロード（コンテナ、サーバーレス機能、VM）
   4. 照会されるAIモデル
   5. インターネットにアクセスするユーザーアプリケーション
   6. 外部アプリケーションからアクセスされるアプリケーション・ユーザー
   7. インバウンドおよびアウトバウンドのトラフィック統計



2. セキュリティビューでの:
    1. （「+」アイコン）AI Runtime Securityインスタンスを追加して、操作ビューで識別される保護されていないネットワークトラフィックを保護できます

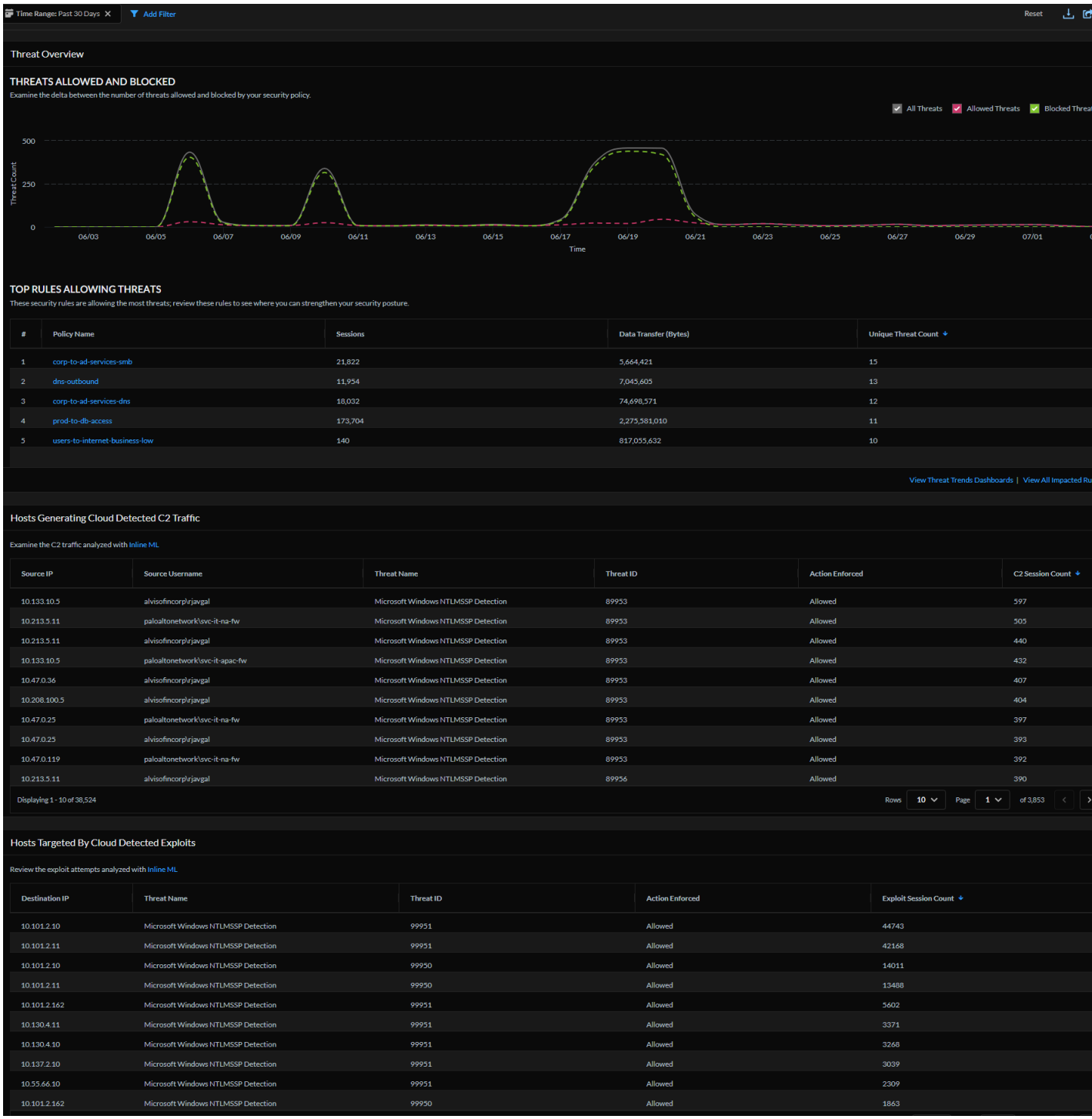
       。
    2. AIランタイムセキュリティインスタンスの保護がすでに存在する場合は、利用可能なAIランタイムセキュリティインスタンスを介して保護されていないトラフィックをリダイレクトします。

次に、ユーザーアプリ、AIモデル、インターネット間の危険なネットワークフローパスを検出します。クラウドネットワークアーキテクチャを監視および防御するには、「AIトラフィックネットワークリスク分析」と「AI Runtime Securityインスタンスのデプロイメント」を参照してください。

ダッシュボード:高度な脅威防御

どこで使用できますか?	何が必要ですか?
• Prisma Access (Managed by Panorama or Strata Cloud Manager) • Software NGFW Creditsによって資金提供されたものを含むNGFW	これらの各ライセンスには、Strata Cloud Managerへのアクセスが含まれています。 ❑ Prisma Access ❑ AIOps for NGFW Premium license (use the Strata Cloud Manager app) ❑ Strata Cloud Manager Essentials ❑ Strata Cloud Manager Pro その他のライセンスと可視性に必要な前提条件は次のとおりです。 ❑ ダッシュボードを表示する権限を持つロール ❑ 脅威防御または高度な脅威防御 → Strata Cloud Managerで利用できる機能は、使用するライセンスによって異なります。

- **Strata Cloud Manager** > **[Dashboards (**ダッシュボード**)]** > **[More Dashboards (**その他のダッシュボード**)]** > **[Advanced Threat Prevention**（高度な脅威防御）**]**をクリックして開始します。



このダッシュボードには何が表示されますか?

ダッシュボードには*Strata Logging Service*テナント毎の集計データが表示されます。

Advanced Threat Prevention（高度な脅威防御）ダッシュボードは、ネットワークで検出された脅威に関する洞察を提供し、セキュリティ体制を強化する機会を特定します。脅威は、インライ

ン クラウド分析モデルと、さまざまなPalo Alto Networksサービスから収集された悪意のあるトラフィック データから生成された脅威シグネチャを使用して検出されます。このダッシュボードには、許可およびブロックされた脅威のタイムライン ビューと、クラウドで検出されたC2トラフィックを生成するホストとクラウドで検出されたエクスプロイトのターゲットとなるホストのリストが表示されます。

このダッシュボードはレポートをサポートしています。ダッシュボードの右上にあるアイコンは、このダッシュボードでレポートがサポートされていることを示します。このダッシュボードに表示されるデータを含むレポートを共有、ダウンロード、スケジュール設定できます。

ダッシュボードのデータをどのように活用できますか?

ダッシュボードは以下の用途にご活用いただけます。

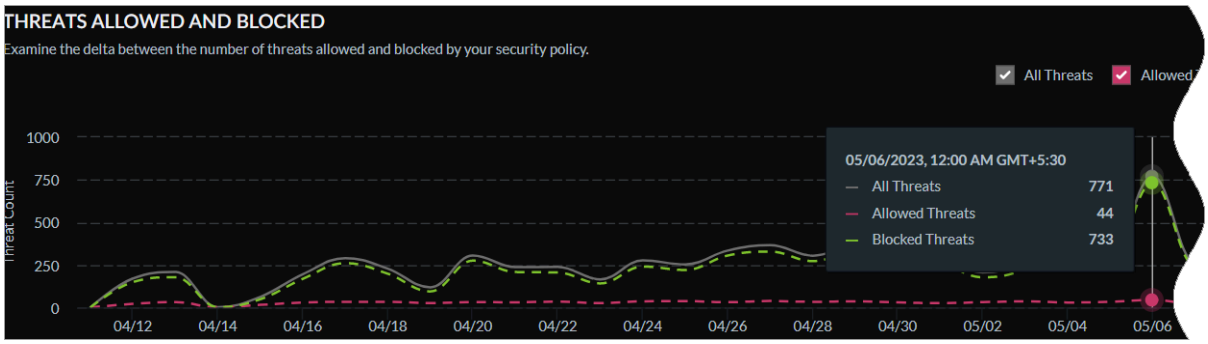
- ネットワーク トラフィックの脅威を可視化する
- 脅威セッションを分析してポリシー ルールの精度を向上させる
- インライン クラウド分析によって検出されたリアルタイムの脅威を把握する
- ログとクラウド レポートから脅威に関するコンテキストを取得し、このデータを使用してインシデント対応プロセスを改善する

Advanced Threat Prevention（高度な脅威防御）ダッシュボード:脅威概要

どこで使用できますか?	何が必要ですか?
• Prisma Access (Managed by Panorama or Strata Cloud Manager) • Software NGFW Creditsによって資金提供されたものを含むNGFW	これらの各ライセンスには、Strata Cloud Managerへのアクセスが含まれています。 ❑ Prisma Access ❑ AIOps for NGFW Premium license (use the Strata Cloud Manager app) ❑ Strata Cloud Manager Essentials ❑ Strata Cloud Manager Pro その他のライセンスと可視性に必要な前提条件は次のとおりです。 ❑ ダッシュボードを表示する権限を持つロール ❑ 脅威防御または高度な脅威防御 → Strata Cloud Managerで利用できる機能は、使用するライセンスによって異なります。

- **Strata Cloud Manager** > **[Dashboards (**ダッシュボード**)]** > **[More Dashboards (**その他のダッシュボード**)]** > **[Advanced Threat Prevention**（高度な脅威防御）**]**をクリックしてダッシュボードを表示します。

セキュリティルールで許可されている脅威とブロックされている脅威のデルタを比較します。

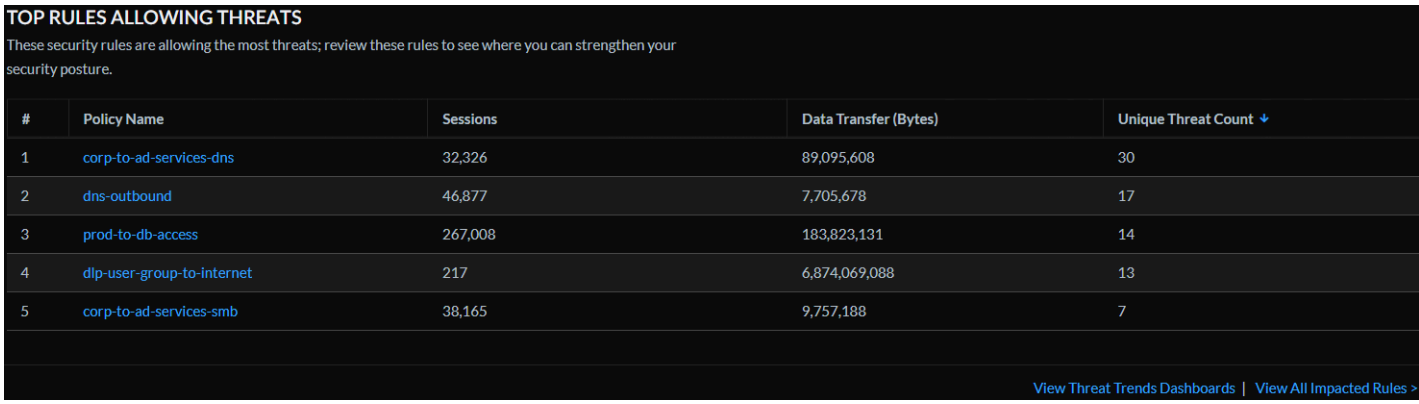


Advanced Threat Prevention（高度な脅威防御）ダッシュボード:脅威が許可されるトップルール

どこで使用できますか?	何が必要ですか?
• Prisma Access (Managed by Panorama or Strata Cloud Manager) • Software NGFW Creditsによって資金提供されたものを含むNGFW	これらの各ライセンスには、Strata Cloud Managerへのアクセスが含まれています。 ❑ Prisma Access ❑ AIOps for NGFW Premium license (use the Strata Cloud Manager app) ❑ Strata Cloud Manager Essentials ❑ Strata Cloud Manager Pro その他のライセンスと可視性に必要な前提条件は次のとおりです。 ❑ ダッシュボードを表示する権限を持つロール ❑ 脅威防御または高度な脅威防御 → Strata Cloud Managerで利用できる機能は、使用するライセンスによって異なります。

- **Strata Cloud Manager** > **[Dashboards (**ダッシュボード**)]** > **[More Dashboards (**その他のダッシュボード**)]** > **[Advanced Threat Prevention**（高度な脅威防御）**]**をクリックしてダッシュボードを表示します。

セキュリティポリシールールに一致した脅威セッションを調べ、セキュリティ態勢を強化するためにポリシー ルールを変更する必要があるかどうかを確認します。Activity Insightsで脅威と照合ルールをさらに分析できます。



列	詳説
ポリシー名	対応する脅威を許可しているセキュリティポリシールール。
セッション	セキュリティポリシールールに一致した脅威セッションの数。
データ転送 (バイト)	セキュリティ ポリシー ルールに一致するセッションを流れたデータ量。
固有脅威数	セキュリティ ポリシー ルールに一致した脅威の数。

Advanced Threat Prevention（高度な脅威防御）ダッシュボード:クラウドを生成するホストが検出した C2 トラフィック

どこで使用できますか?	何が必要ですか?
• Prisma Access (Managed by Panorama or Strata Cloud Manager) • Software NGFW Creditsによって資金提供されたものを含むNGFW	これらの各ライセンスには、Strata Cloud Managerへのアクセスが含まれています。 ❑ Prisma Access ❑ AIOps for NGFW Premium license (use the Strata Cloud Manager app) ❑ Strata Cloud Manager Essentials ❑ Strata Cloud Manager Pro その他のライセンスと可視性に必要な前提条件は次のとおりです。 ❑ ダッシュボードを表示する権限を持つロール ❑ 脅威防御または高度な脅威防御

どこで使用できますか?	何が必要ですか?
	→ Strata Cloud Managerで利用できる機能は、使用するライセンスによって異なります。

- **Strata Cloud Manager** > **[Dashboards (**ダッシュボード**)]** > **[More Dashboards (**その他のダッシュボード**)]** > **[Advanced Threat Prevention**（高度な脅威防御）**]**をクリックしてダッシュボードを表示します。

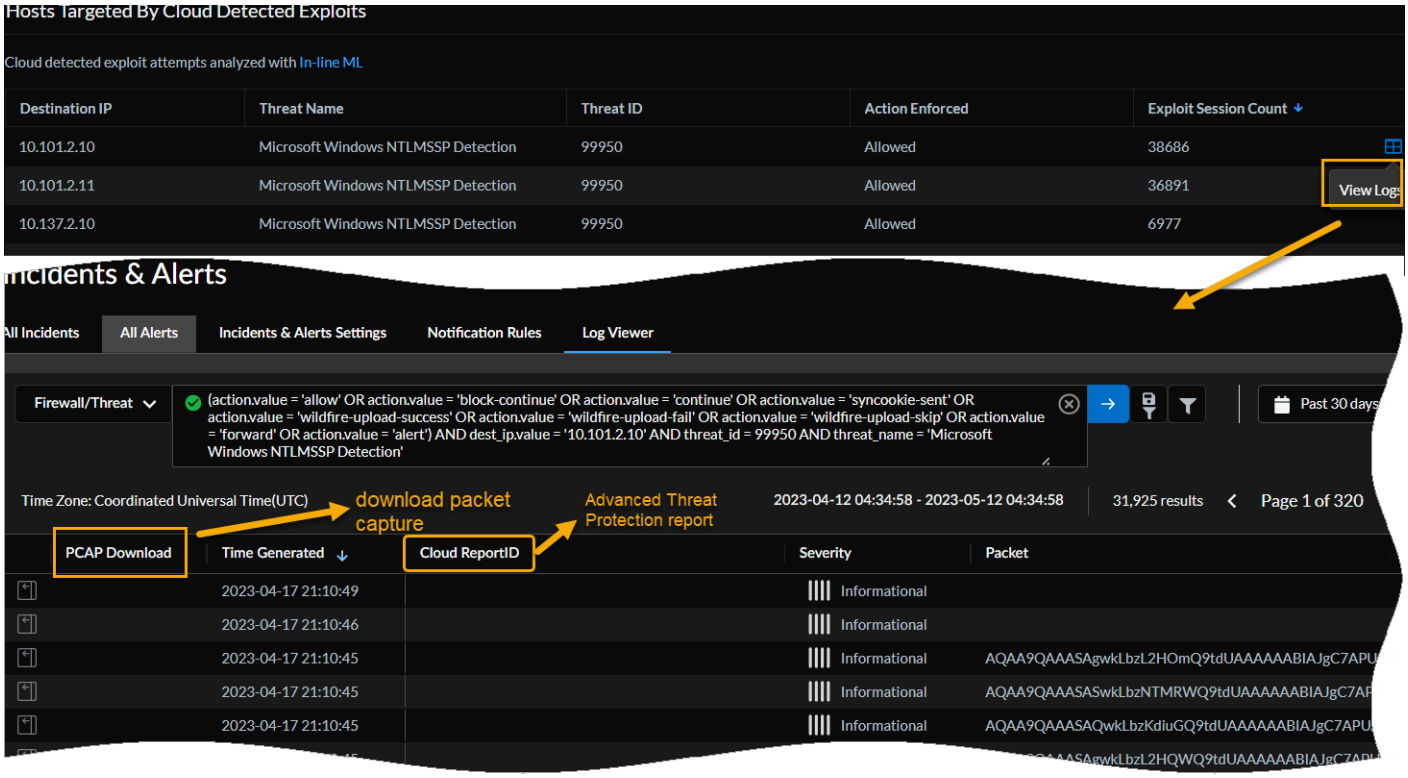
C2(コマンド/コントロール）トラフィックの生成を担当する送信元IPおよびユーザを調べます。Advanced Threat Prevention(高度な脅威防御)は、クラウドベースのエンジンとインライン クラウド分析を使用して、未知のC2や脆弱性のトラフィックを検出および分析します。発信元IPの横にある検索アイコンをクリックして、発信元IPに関連する使用パターンを確認します。[Log Viewer (ログビューア)]へのコンテキストリンクは、脅威セッションの分析、パケットキャプチャおよびクラウドレポートのダウンロード、追加のコンテキストの取得、Palo Alto Networksの脅威分析データの活用、インシデント対応プロセスの改善に役立ちます。

Advanced Threat Prevention（高度な脅威防御）ダッシュボード:クラウドが検出したエクスプロイトの標的となったホスト

どこで使用できますか?	何が必要ですか?
• Prisma Access (Managed by Panorama or Strata Cloud Manager) • Software NGFW Creditsによって資金提供されたものを含むNGFW	これらの各ライセンスには、Strata Cloud Managerへのアクセスが含まれています。 ❑ Prisma Access ❑ AIOps for NGFW Premium license (use the Strata Cloud Manager app) ❑ Strata Cloud Manager Essentials ❑ Strata Cloud Manager Pro その他のライセンスと可視性に必要な前提条件は次のとおりです。 ❑ ダッシュボードを表示する権限を持つロール ❑ 脅威防御または高度な脅威防御 → Strata Cloud Managerで利用できる機能は、使用するライセンスによって異なります。

- **Strata Cloud Manager** > **[Dashboards (**ダッシュボード**)]** > **[More Dashboards (**その他のダッシュボード**)]** > **[Advanced Threat Prevention**（高度な脅威防御）**]**をクリックしてダッシュボードを表示します。

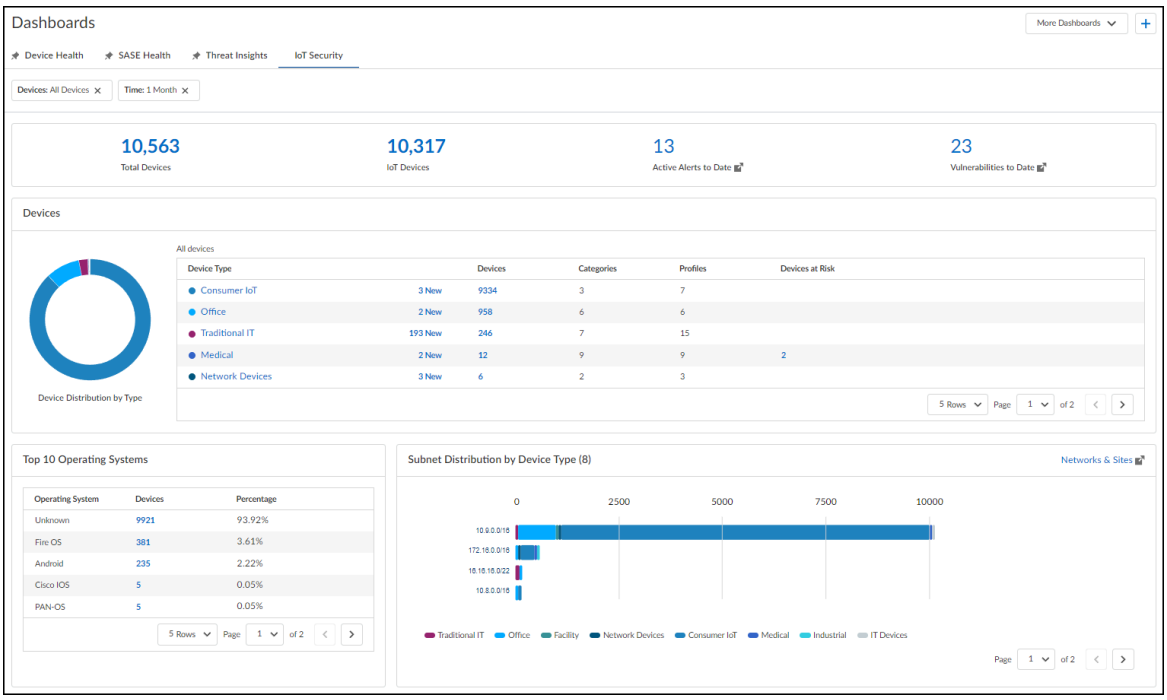
これらは、脆弱性の悪用の標的となるIPです。Advanced Threat Prevention(高度な脅威防御)は、クラウドベースのエンジンとインラインクラウド分析を使用して、トラフィックを検出および分析します。宛先IPアドレスにカーソルを合わせて検索アイコンをクリックすると、宛先IPに関する利用パターンを確認できます。ログを表示して、脅威の周囲のコンテキストを取得します。ログからクラウドレポートとパケットキャプチャをダウンロードして、追加のコンテキストを取得し、Palo Alto Networksの脅威分析データと脅威インテリジェンスを使用してインシデント応答プロセスを改善できます。



ダッシュボード:IoTセキュリティ

どこで使用できますか?	何が必要ですか?
• Prisma Access (Managed by Panorama or Strata Cloud Manager) • Software NGFW Creditsによって資金提供されたものを含むNGFW	これらの各ライセンスには、Strata Cloud Managerへのアクセスが含まれています。 ❑ Prisma Access ❑ AIOps for NGFW Premium license (use the Strata Cloud Manager app) ❑ Strata Cloud Manager Essentials ❑ Strata Cloud Manager Pro その他のライセンスと可視性に必要な前提条件は次のとおりです。 ❑ ダッシュボードを表示する権限を持つロール ❑ IoTセキュリティ → Strata Cloud Managerで利用できる機能は、使用するライセンスによって異なります。

[Dashboards (ダッシュボード)] > [More Dashboards (その他のダッシュボード)] > [IoT Security (IoTセキュリティ)]をクリックして、作業を開始します。



このダッシュボードには何が表示されますか?

IoT Securityのダッシュボードには、ネットワーク上のデバイスに関する情報、デバイスプロファイルとオペレーティングシステム、およびサブネット間のデバイスタイプ別の配信方法が表示されます。高度なIoTセキュリティ製品（エンタープライズ IoT Security プラス、インダストリアルIoT Securityまたはメディカル IoT Security）の場合、IoT Securityダッシュボードには、現在までにアクティブなアラートの総数と、現在までの脆弱性が追加表示されます。

青色で書式設定されたテキストは対話式です。クリックするとどうなるか:

- 概要（一番上）：**[Total Devices (デバイス合計)]**および**[IoT Devices (IoTデバイス)]** は、**[Monitor (モニター)] > Assets (アセット)]** ページにリンクし、すべてのデバイスまたはすべてのIoTデバイスのインベントリを表示するフィルタを適用します。「現在までにアクティブなアラート」と「現在までにアクティブな脆弱性」の青色のテキストは、IoT Securityポータルで対応するページを開きます。（アラートや脆弱性がない場合、番号は0でリンクはありません）
- デバイス – チャートのセクションまたは［デバイスタイプ］列のエントリをクリックすると、選択したタイプ内のデバイスカテゴリが拡大表示され、そこから選択したカテゴリ内のデバイスプロファイルが表示されます。グラフ内に戻るか、表の上にあるパンくずリストをクリックすると、デバイスのより広範な分類にズームアウトされます。

  [危険にさらされているデバイス]列と[デバイス]列の数字は、[資産 > 監視]ページにリンクしています。Strata Cloud Managerは自動的にフィルタを適用して、選択した列と行に一致するデバイスを表示します。表示されている現在のレベルに応じて、[デバイスタイプ]、[カテゴリ名]、[プロファイル名]のいずれかになります。

  > *IoT Security*がネットワーク上で検出した新しいデバイスの数が表示されることがあります。これらの数値は、デバイス列の数字の左に表示されます。*IoT Security*は、ダッシュボードの上部にある時間フィルタ内にネットワーク上で最初に検出されたデバイスを「新規」と見なします。

- 上位10のオペレーティングシステム – [デバイス]列の数字は、選択したOSを搭載したデバイスのみを表示するフィルタが適用された[資産 > 監視]ページにリンクしています。
- ［デバイスタイプ別サブネット配信］ – サブネットのバーにカーソルを合わせると、デバイスタイプごとにグループ化されたデバイスの数がサブネット内に表示されます。この情報は、無関係なデバイスタイプが同一サブネット内に混在しすぎていないかを判断するのに役立ちます。たとえば、施設、産業、および消費者向けのIoTデバイスが1つのサブネットに表示される場合、各タイプのデバイスを個別のサブネットにセグメント化したい場合があります。**[Networks & Sites (ネットワークとサイト)]**をクリックすると新しいブラウザウィンドウが起動し、IoTセキュリティポータルの[ネットワーク] > [ネットワークサイトと > ネットワーク]が開きます。

このダッシュボードのデータはどのように利用できますか？

このダッシュボードのデータを使用して、ネットワーク上のデバイスについて学習します。

フィルタ(ページ上部)

- ダッシュボードに表示されるデータをデバイスの種類と期間（過去1年、1か月、1週間、1日、または1時間）でフィルタリングして、関心のあるデバイスに関するデータを表示することができます。

概要(ダッシュボードの上部全体)

- デバイスタイプと時間フィルタによって判断された、ネットワークでアクティブになったデバイスの総数を確認できます。
- アクティブなデバイスの総数のうち、具体的にIoTデバイスは何台かを確認できます。
- 現在までに検出されたアクティブなアラートや脆弱性の数を見ることで、デバイスが動作するセキュリティの展望について把握できます。

デバイス

- さまざまなデバイス タイプの中でデバイスの数を学び、ドリル ダウンしてさまざまなデバイス カテゴリの中で、そしてさまざまなデバイス プロファイルの中でデバイスの数を学びます。デバイス分類の細かさが増している各レベルで、重要なリスク デバイスの数と、そのデバイスがどのようなデバイスであるかを確認します。

上位**10**のオペレーティングシステム

- OSのIoT Securityが検出されたすべてのデバイスの中で、最も一般的なオペレーティングシステムの上位10位、各オペレーティングシステムを使用しているデバイスの数、およびその割合を確認します。

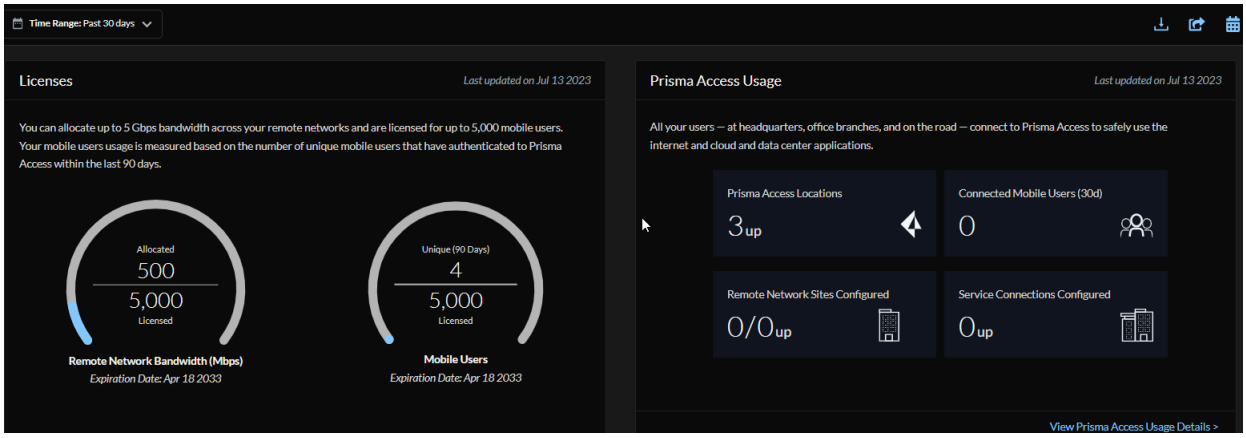
デバイスタイプ別のサブネット配信

- さまざまなデバイスタイプがネットワーク全体のサブネットにどのように分散されているかを確認します。同じサブネット内にデバイスタイプが多数混在している場合は、それらを独自の別々のサブネットにセグメント化することを検討してください。

ダッシュボード:Prisma Access

どこで使用できますか?	何が必要ですか?
• Prisma Access (Managed by Panorama or Strata Cloud Manager)	以下のいずれかです。 ❑ Prisma Accessライセンス ❑ Strata Cloud Manager Pro → Strata Cloud Managerで利用できる機能は、使用するライセンスによって異なります。

- 開始するには、**Strata Cloud Manager** > **[Dashboards (ダッシュボード)]** > **[More Dashboards (その他のダッシュボード)]** > **[Prisma Access]**をクリックします。



このダッシュボードには何が表示されますか？

ライセンスで利用できる機能の活用方法を理解し、ご利用のPrisma Access環境の正常性とパフォーマンスを全体的に把握します。

Prisma Access Usageのデータには、次のものがあります。

- Prisma Accessの使用状況の概要–ライセンス、Prisma Accessの場所、モバイルユーザー容量および/または帯域幅使用率
- モバイルユーザーとリモートネットワーク向けのPrisma Accessの上位ロケーション
- リモートネットワークおよびサービス接続サイトの全体的な帯域幅消費、および最も消費の多いリモートネットワークおよびサービス接続サイトの
- 最も影響を受けたトンネルを含むトンネル切断の傾向

ダッシュボードには、*Prisma Access*テナントごとの集計データが表示されます。

このダッシュボードはレポートをサポートしています。ダッシュボードの右上にある  アイコンは、このダッシュボードでレポートがサポートされていることを示します。このダッシュボードに表示されるデータを含むレポートを共有、ダウンロード、スケジュール設定できます。

ダッシュボードのデータをどのように活用できますか?

このダッシュボードは、ネットワーク内のPrisma Accessの使用状況を可視化し、ダッシュボードのデータに基づいて構成設定を調整するのにご使用いただけます。

ダッシュボード:アプリケーションエクスペリエンス

どこで使用できますか?	何が必要ですか?
• Prisma Access （*Strata Cloud Manager*または*Panorama*の設定管理付き）	❑ Prisma Accessライセンス ❑ 監視対象アプリケーションのデータを表示するADEM Observabilityライセンス ❑ Remote Networksライセンス *(*リモートサイトのエクスペリエンスデータを見るために必要*)*

- **Strata Cloud Manager** > **[**ダッシュボード**]** > **[**その他のダッシュボード**]** > **[**アプリケーションエクスペリエンス**]**をクリックして開始します。

このダッシュボードには何が表示されますか？

このダッシュボードに表示されるデータは変更され、選択したカード（［モバイルユーザーエクスペリエンス］または［リモートサイトエクスペリエンス］）に対応します。AI-Powered ADEMを初めて使用する場合は、まず組織全体で使用中のアプリケーションを調査し、この情報を使用して、どのアプリケーション用のアプリテストを作成するかを特定するとよいでしょう。さらに、アプリケーションの問題を報告しているユーザーやリモートサイトがある場合は、このダッシュボードが問題の切り分けを開始するのに適しています。アプリケーションの使用状況のデータは、Prisma Accessを通過する実ユーザートラフィックから取得されます。モバイルユーザおよびリモートサイトからのトラフィックが含まれます。

フィルタを追加して結果を絞り込み、特定のアプリケーション、導入タイプ、エクスペリエンススコア、モバイルユーザー、グループ、またはプリズマアクセスの場所のデータのみを表示できます。アプリケーションの個々のエクスペリエンススコアと、既存のパフォーマンス問題によって影響を受けているユーザ数およびリモートサイト数を表示します。

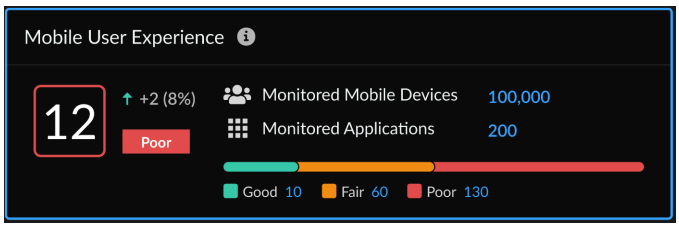
ダッシュボードのデータをどのように活用できますか?

ネットワーク上で実行されているアプリケーションを調査し、監視するアプリケーションを決定したら、アプリテストを作成できます。アプリテストを作成する際は、複数のユーザーやサイトを対象としたアプリテストを作成することもできますが、テストの数は個々のユーザーやIONデバイスごとに実行されたアプリテストの数に基づいています（たとえば、Slack向けのアプリテストがあり、1,000ユーザーを対象とした場合、これは1000テストとしてライセンスにカウントされます）。

アプリケーション エクスペリエンス ダッシュボード:モバイル ユーザー エクスペリエンスカード

どこで使用できますか?	何が必要ですか?
• Prisma Access （*Strata Cloud Manager*または*Panorama*の設定管理付き）	❑ Prisma Accessライセンス ❑ 監視対象アプリケーションのデータを表示するADEM Observabilityライセンス

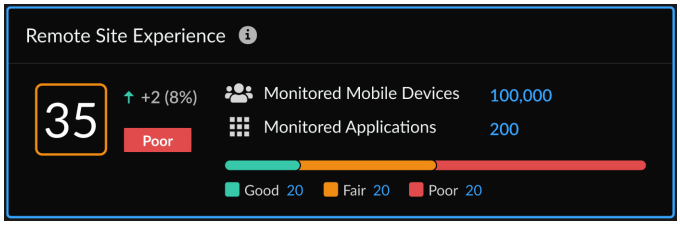
このウィジェットには、監視対象のすべてのアプリケーションのすべてのモバイル ユーザーのアプリケーション セグメント スコアの平均が表示されます。また、ユーザーデバイス数別に、良好、普通、劣悪なエクスペリエンスの内訳も表示されます。パフォーマンスが正常または低下しているユーザーをドリルダウンして調査を開始できます。このカードのエクスペリエンス スコアは、ユーザーにとっての全体的なデジタルエクスペリエンスの指標となります。ADEMは、モバイルユーザーごとに監視するアプリケーションごとに、アプリケーションの可用性、DNS解決時間、TCP接続時間、SSL接続時間、HTTPレイテンシの5つの重要なメトリックに基づいてスコアを計算します。アプリケーションが可用性テストに失敗した場合（アプリケーションが使用できない場合）、エクスペリエンス スコアは0になります。アプリケーションが到達可能な場合は、残りの4つのメトリックのみが計算されます。上記のメトリック（アプリケーションの到達可能性以外）はそれぞれ重み付けとベースラインの下限および上限しきい値が異なり、それらの重み付けの合計は100になります。これらの個々のメトリックスコアの合計によって、ユーザーのアプリケーション エクスペリエンス スコアが決まります。各アプリケーションのすべてのテストサンプル結果の平均が、ユーザーのエクスペリエンス スコアを決定します。



アプリケーション エクスペリエンス ダッシュボード:リモート サイト エクスペリエンス カード

どこで使用できますか?	何が必要ですか?
• Prisma Access （*Strata Cloud Manager*または*Panorama*の設定管理付き）	❑ Prisma Accessライセンス ❑ 監視対象アプリケーションのデータを表示するADEM Observabilityライセンス ❑ Remote Networksライセンス

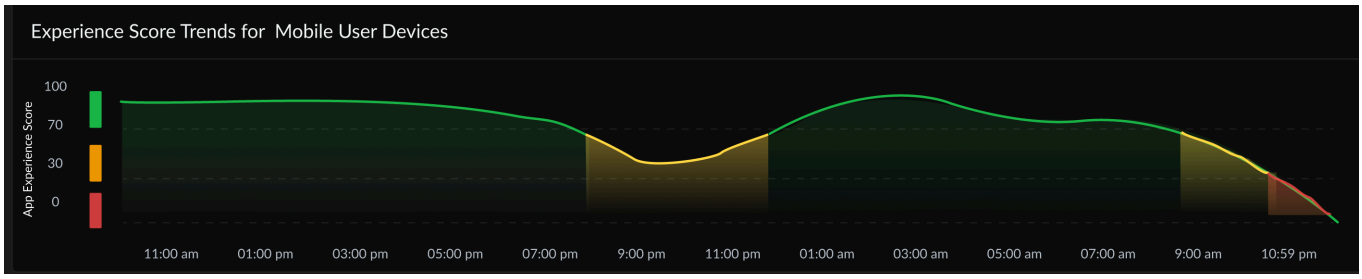
リモート サイト エクスペリエンス スコアは、すべてのアクティブなWAN経路上の監視対象アプリケーションの平均スコアです。そのリモートサイトについて監視されている個々のアプリケーションから収集されたすべてのテストサンプル結果の平均です。リモートサイトまたはブランチの全体的な経験スコア(色分けされた四角で囲まれている)を確認できます。これは、そのサイト用に監視されているすべてのアプリケーションのアクティブな経路で収集されたすべてのテストサンプルの経験スコアの平均です。各バックアップ経路のエクスペリエンス スコアは、リモートサイトおよびアプリケーションごとに個別に計算され、利用可能になりますが、リモートサイトのエクスペリエンス スコアの計算には、バックアップ経路のエクスペリエンス スコアは考慮されません。「fair」または「poor」の横の数字をクリックすると、パフォーマンスが「Faor」または「Poor」になっているサイトをドリルダウンできます。



アプリケーション エクスペリエンス ダッシュボード:エクスペリエンススコアのトレンド

どこで使用できますか?	何が必要ですか?
• Prisma Access （*Strata Cloud Manager*または*Panorama*の設定管理付き）	❑ Prisma Accessライセンス ❑ 監視対象アプリケーションのデータを表示するADEM Observabilityライセンス

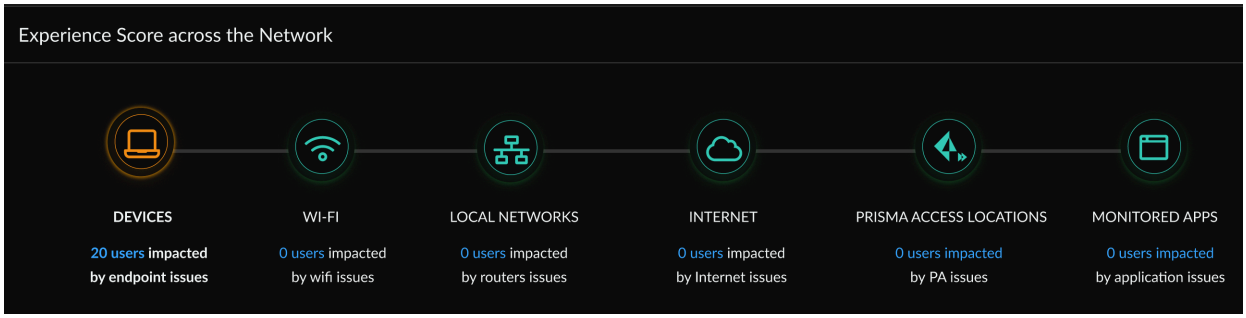
このウィジェットには、すべてのモバイルユーザーの平均モバイルユーザーエクスペリエンスの時系列グラフが表示されます。エクスペリエンススコアは、選択した時間範囲に設定された間隔で計算および表示されます。Y軸はスコア範囲に基づいて色分けされ、エクスペリエンススコアの質がわかります（赤 = Poor、黄 = Fair、緑 = Good）。トレンドラインにマウスカーソルを合わせると、カーソルが置かれた時点のエクスペリエンススコアが表示されます。



アプリケーション エクスペリエンス ダッシュボード:ネットワーク全体でのエクスペリエンススコア

どこで使用できますか?	何が必要ですか?
• Prisma Access （*Strata Cloud Manager*または*Panorama*の設定管理付き）	❑ Prisma Accessライセンス ❑ 監視対象アプリケーションのデータを表示するADEM Observabilityライセンス

エンドポイント(モバイルユーザー向け)またはブランチオフィス(リモートサイト)からアプリケーションまで、組織内で問題を引き起こしている可能性のあるネットワークのセグメントを特定します。エンドポイントやPrisma SD-WANのリモートサイトからアプリケーションまで、組織内のどのセグメントが問題を引き起こしているかを確認できます。ISPやコンピュートロケーションの停止、SaaSアプリの停止など、組織内のデジタル体験に影響を与えているセグメントと、その影響下にあるユーザーやサイトの正確な数を確認できます。アイコンは色分けされており、すべてのモバイルユーザーのセグメント正常性スコアの平均に基づいています。緑のアイコンは「Good」（スコアが70以上）、黄色は「Fair」（スコアが30～70）、赤色は「Poor」（スコア<30）を表します。



デバイス - デバイスの正常性指標(CPU/メモリ/ディスク容量/ディスクキュー/バッテリ)

Wi-Fi - WIFIメトリクス（信号品質、Tx、Rx、SSID、BSSID、チャネル）

ローカルネットワーク:ネットワーク パフォーマンス メトリック(遅延/損失/ジッタ)

インターネット - ネットワークパフォーマンスメトリック（遅延/損失/ジッタ） デバイスがインターネットセグメントであるGlobalProtectに接続されていない場合、ネットワークパフォーマンスメトリックはアプリケーションセグメントに対して実行されたTCP PINGテストと同じになります。

Prisma Access Locations - ネットワークパフォーマンスメトリック(Latency/Loss/Jitter)デバイスがGlobalProtectに接続されていない場合、このセグメントのテストは実行されません。

監視対象アプリ - ネットワークパフォーマンス指標(レイテンシ/損失/ジッタ) アプリケーションパフォーマンス指標(可用性、DNSルックアップ、TCP接続、SSL接続、HTTPレイテンシ、最初のバイトまでの時間、最後のバイトまでの時間、データ転送)

アプリケーション エクスペリエンス ダッシュボード:アプリケーション エクスペリエンス スコアのグローバル ディストリビューション

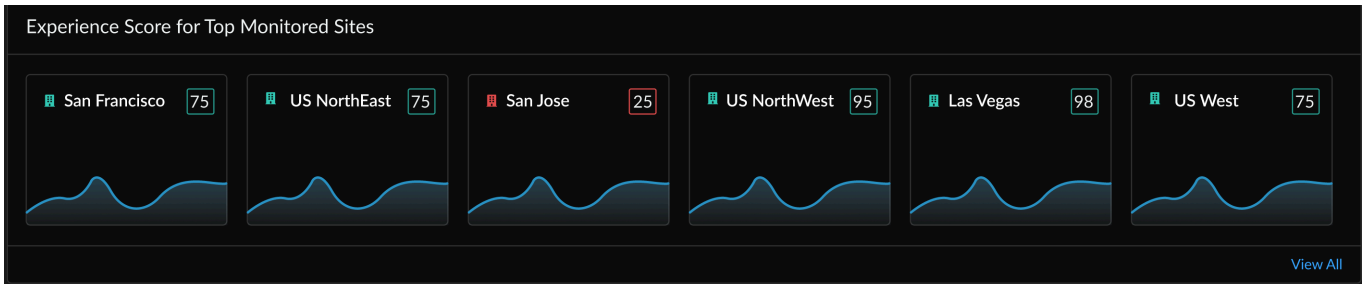
どこで使用できますか?	何が必要ですか?
• Prisma Access （*Strata Cloud Manager*または*Panorama*の設定管理付き）	❑ Prisma Accessライセンス ❑ 監視対象アプリケーションのデータを表示するADEM Observabilityライセンス

選択したカードに応じて、このウィジェットのマップ ビューには、監視対象のモバイル ユーザーとアプリケーションの合計数、または特定のPrisma Accessロケーションで監視対象のリモート サイトとアプリケーションの合計数に基づいて、Prisma Accessロケーションのエクスペリエンスが表示されます。Prisma Accessの場所には、円が表示されている特定のPrisma Accessの場所に接続されているすべての監視対象モバイル ユーザーとリモート サイトのアプリケーション セグメント スコアのステータスを表すために色分けされた円が付けられています。マウス カーソルを円の上に置くと、その場所のエクスペリエンス スコア、監視対象のモバイル ユーザー デバイスまたはリモート サイトの合計数、およびその場所で監視されているアプリの合計数が表示されます。地理的に非常に近い複数の場所は、数字が入った1つの円で表されます。数字は、そのエリアにグループ化された場所の数を示します。どの場所がグループ化されているかを正確に確認するには、地図を拡大します。

アプリケーション エクスペリエンス ダッシュボード:上位のモニタリング対象サイトのエクスペリエンス スコア

どこで使用できますか?	何が必要ですか?
• Prisma Access （*Strata Cloud Manager*または*Panorama*の設定管理付き）	❑ Prisma Accessライセンス ❑ 監視対象アプリケーションのデータを表示するADEM Observabilityライセンス

このウィジェットは、アプリケーションごとに1枚のカードを表示し、スコアの高いサイトを表示します。このウィジェットは、選択した時間範囲のリモートサイトの経験スコアの傾向を表示します。トレンドラインの上にマウスカーソルを置くと、その時点の経験値が表示されます。

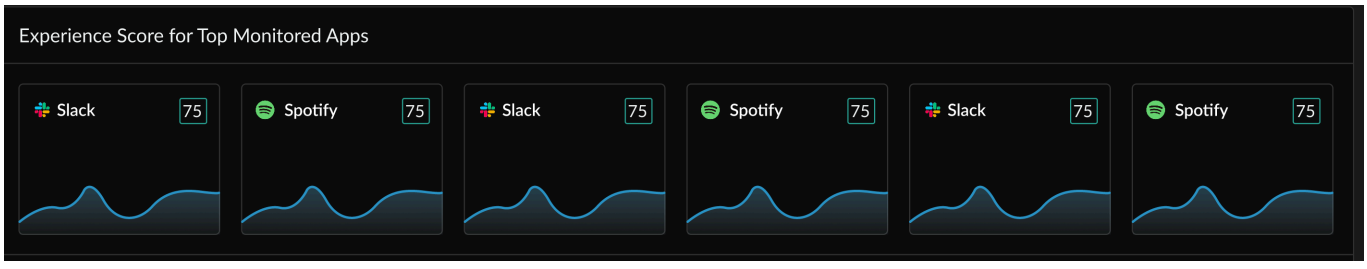


アプリケーション エクスペリエンス ダッシュボード:上位のモニタリング対象アプリケーションのエクスペリエンススコア

どこで使用できますか?	何が必要ですか?
• Prisma Access （*Strata Cloud Manager*または*Panorama*の設定管理付き）	❑ Prisma Accessライセンス ❑ 監視対象アプリケーションのデータを表示するADEM Observabilityライセンス

各アプリケーションカードには、リモートサイト上の特定のアプリケーションについて、監視対象のすべてのモバイルユーザーの平均アプリケーションセグメントスコア（四角で囲まれた数値）が表示されます。エクスペリエンス スコアは、すべての監視対象アプリケーションのアプリエクスペリエンス スコアの平均として計算されます。エクスペリエンス スコアは、アプリケーションのアクティブパスのエンドツーエンドのエクスペリエンスを示します。これは、特定のアプリケーションのみを対象に、アクティブパスで収集されたすべてのテストサンプルの平均です。トレンドラインには、選択した時間枠の 5 分間のすべてのAPMデータサンプルの平均が表示されます。

監視しているアプリケーションの数と、監視されているアクティブパスとバックアップパスの数を確認できます。各アプリケーションカードには、影響を受けるパスの数が表示されます。アプリケーションカードをクリックすると、その特定のアプリケーションのメトリックが表示されます。

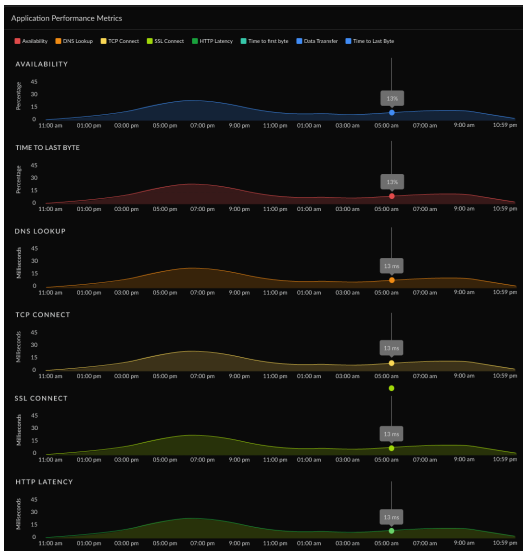


アプリケーション エクスペリエンス ダッシュボード:アプリケーションパフォーマンスメトリック

どこで使用できますか?	何が必要ですか?
• Prisma Access （*Strata Cloud Manager*または*Panorama*の設定管理付き）	❑ Prisma Accessライセンス ❑ 監視対象アプリケーションのデータを表示するADEM Observabilityライセンス

Autonomous DEMはTCP pingとCurlを使用して、エンドツーエンドのアプリケーションパフォーマンスを決定します。

メトリック	詳説
価格と提供開始時期	**Time Range (**時間範囲**)**中のアプリケーションの可用性（パーセント単位）。
DNS検索	DNS解決時間。
TCP接続	TCP接続の確立に要する時間。
SSL接続	SSL接続の確立に要する時間。
HTTP遅延	HTTP接続の確立に要する時間。
最初のバイトまでの時間	DNS Lookup (DNSルックアップ)、TCP Connect (TCP接続)、SSL Connect (SSL接続)、HTTP Latency (HTTP 遅延)の時間の合計が Time to First Byte (最初のバイトまでの時間)となります。
データ転送	データ全体が転送されるのに要する合計時間。
最後のバイトまでの時間	最初のバイトまでの時間+データ転送時間。

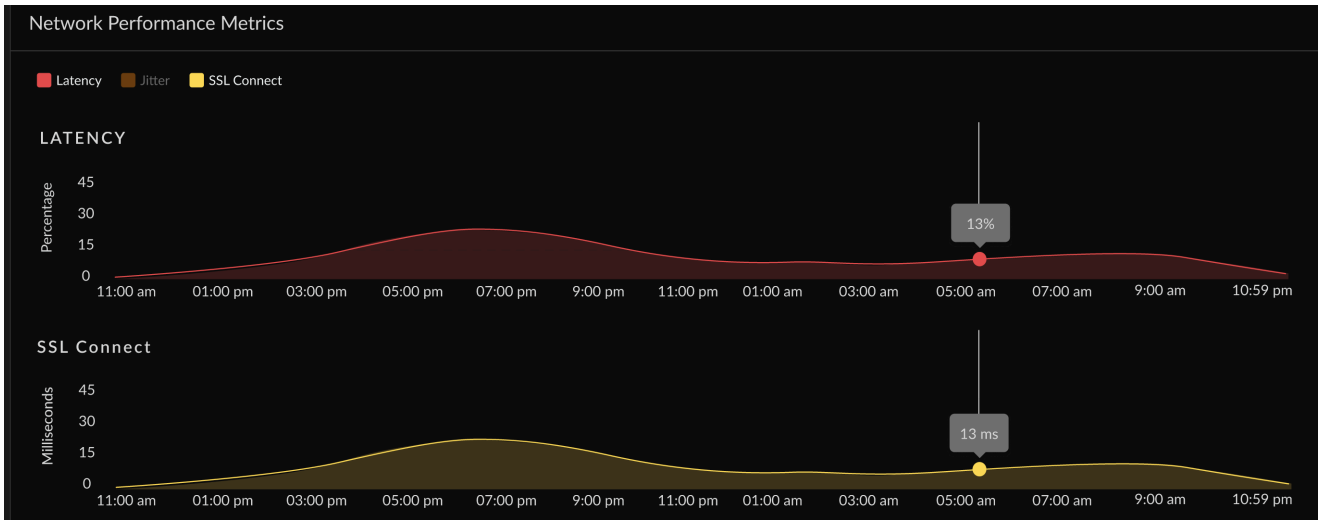


アプリケーション エクスペリエンス ダッシュボード:ネットワークパフォーマンスメトリック

どこで使用できますか?	何が必要ですか?
• Prisma Access （*Strata Cloud Manager*または*Panorama*の設定管理付き）	❑ Prisma Accessライセンス ❑ 監視対象アプリケーションのデータを表示するADEM Observabilityライセンス

ADEMはICMP pingを使用して、各セグメントのネットワークパフォーマンスを判断します。

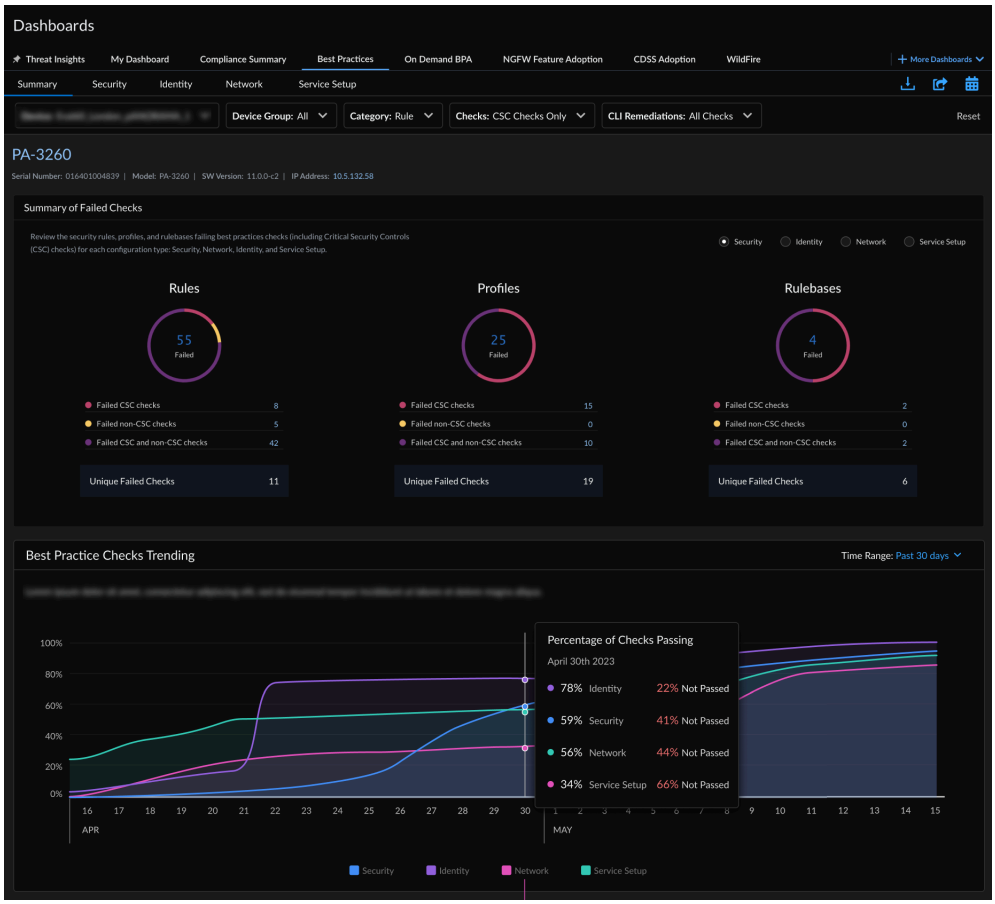
メトリック	詳説
価格と提供開始時期	**Time Range (期間)**中のネットワーク可用性メトリック。
ネットワークの遅延	ネットワーク上でのデータ転送にかかる時間。
パケットの損失	データ送信中のパケットの損失。
ジッター	**Time Range (期間)**中の遅延の変化。



ダッシュボード:ベストプラクティス

どこで使用できますか?	何が必要ですか?
• Prisma Access (Managed by Panorama or Strata Cloud Manager) • Software NGFW Creditsによって資金提供されたものを含むNGFW	これらの各ライセンスには、Strata Cloud Managerへのアクセスが含まれています。 ❑ Prisma Access ❑ AIOps for NGFW Premium ❑ Strata Cloud Manager Essentials ❑ Strata Cloud Manager Pro → Strata Cloud Managerで利用できる機能は、使用するライセンスによって異なります。

- **Strata Cloud Manager** > **[Dashboards (**ダッシュボード**)]** > **[More Dashboards (**その他のダッシュボード**)]** > **[Best Practices (**ベストプラクティス**)]**をクリックして、作業を開始します。



このダッシュボードには何が表示されますか？

ダッシュボードには、テナントに関連付けられている*Prisma Access*および*NGFW/Panorama*ごとに集計されたデータが表示されます。

ベスト プラクティス ダッシュボードは、Palo Alto Networksのベスト プラクティス ガイダンスに照らしてセキュリティ体制を測定します。ベストプラクティスには、インターネットセキュリティセンターの重要なセキュリティ管理 (CSC) のチェックが含まれます。CSCチェックは他のベスト プラクティス チェックとは別に呼び出されるため、CSCコンプライアンスに準拠するための更新を簡単に選択して優先順位を付けることができます。

ベスト プラクティス ダッシュボードは5つのセクションに分かれています。

- 概要

  構成タイプ (セキュリティ、ネットワーク、ID、およびサービス セットアップ) 全体にわたってデバイスのすべての失敗したチェックの包括的なビューを提供し、BPAチェックの履歴トレンド チャートを表示し、主要な機能領域におけるベスト プラクティスの採用率を評価します。

- セキュリティ

  選択したデバイスと場所のベスト プラクティスとCSCチェックに失敗したルール、ルールベース、またはプロファイルを表示します。利用可能な場合、CLI修復により、ポリシー ルールの問題を解決できます。CLI修正は、オンデマンドBPAレポートを生成するときにアップロードしたTSFデータを使用して生成されます。

  - ルールベース

    ポリシーがどのように構成されているか、および多くのルールに適用される構成設定がベスト プラクティス (CSC チェックを含む) に準拠しているかどうかを確認します。

  - ルール

    ベスト プラクティスとCSCチェックに失敗したルールを表示します。失敗したチェックを修正するための迅速なアクションをどこで実行できるかを確認してください。ルールはセッション数に基づいて並べ替えられるため、トラフィックに最も影響を与えているルールを確認して更新することから始めることができます。

  - プロファイル

    CSCチェックなどのベスト プラクティスに対してプロファイルがどのように適合しているかを示します。プロファイルは、セキュリティルールまたは復号化ルールに一致するトラフィックの高度な検査を実行します。

- **ID**

  デバイスの認証強制設定 (認証ルール、認証プロファイル、認証ポータル) がベスト プラクティスを満たし、CSCチェックに準拠しているかどうかを示します。

- ネットワーク

  アプリケーションのオーバーライド ルールとネットワーク設定がベスト プラクティスおよびCSCチェックに準拠しているかどうかを確認します。

- サービスのセットアップ

  デバイスで有効にしたサブスクリプションがベスト プラクティスおよびCSCチェックとどのように一致しているかを確認します。ここで、WildFireのセットアップ、GlobalProtectポータル、GlobalProtectゲートウェイの構成を確認し、失敗したチェックを修正できます。

このダッシュボードはレポートをサポートしています。ダッシュボードの右上にある  アイコンは、このダッシュボードでレポートがサポートされていることを示します。このダッシュボードに表示されるデータを含むレポートを共有、ダウンロード、スケジュール設定できます。

管理画面のデータはどのように利用できますか？

ベスト プラクティス ガイダンスはセキュリティ体制の強化を目的としていますが、このレポートの調査結果は、環境をより効果的に管理するために変更を加えることができる領域を特定するのにも役立ちます。

ダッシュボード:コンプライアンス概要

どこで使用できますか?	何が必要ですか?
• Software NGFW Creditsによって資金提供されたものを含むNGFW	☐ AIOps for NGFW Premium または Strata Cloud Manager Pro → Strata Cloud Managerで利用できる機能は、使用するライセンスによって異なります。

インターネット セキュリティ センター (CIS) および 国立標準技術研究所 (NIST) のフレームワークごとにグループ化された、過去12か月までのセキュリティチェックの変更履歴を表示できます。各フレームワークごとに、コントロールのリストと、各コントロールの現在および平均順守率、ベストプラクティスチェックの合計数、失敗したチェックの数が表示されます。

チャートとリストを操作し、コントロールとその履歴統計の関係を確認します。個々のコントロールと関連するチェックの詳細を表示し、ベストプラクティスのチェックを選択して、チェックでエラーとなっているファイアウォール構成を表示します。

CIS(重要なセキュリティコントロール)フレームワークは、既知のサイバー攻撃経路から組織とそのデータを保護するための、優先順位の高い一連の推奨アクションとベストプラクティスです。CISコントロールの基本および基礎となる16種類のうち、11種類のチェック概要を表示できます。

- CSC 3:継続的な脆弱性管理
- CSC 4:管理者権限の制御された使用
- CSC 6:監査ログの保守、モニタリング、および分析
- CSC 7:メールと Web ブラウザの保護
- CSC 8:マルウェア防御
- CSC 9:ネットワーク ポート、プロトコル、およびサービスの制限と制御
- CSC 11:ファイアウォール、ルーター、スイッチなどネットワークデバイスの安全な設定
- CSC 12:境界防御
- CSC 13:データ保護
- CSC 14:Need to Knowに基づいて制御されているアクセス
- CSC 16:アカウントのモニタリングと制御

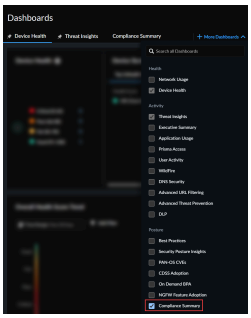
NISTサイバーセキュリティフレームワーク **SP 800-53** コントロールのフレームワークは、連邦政府機関やその他の組織が情報システムのセキュリティとプライバシーの管理を実装し、維持管理するためのガイダンスです。NISTコントロールの8つのファミリーのチェック概要を表示できます。

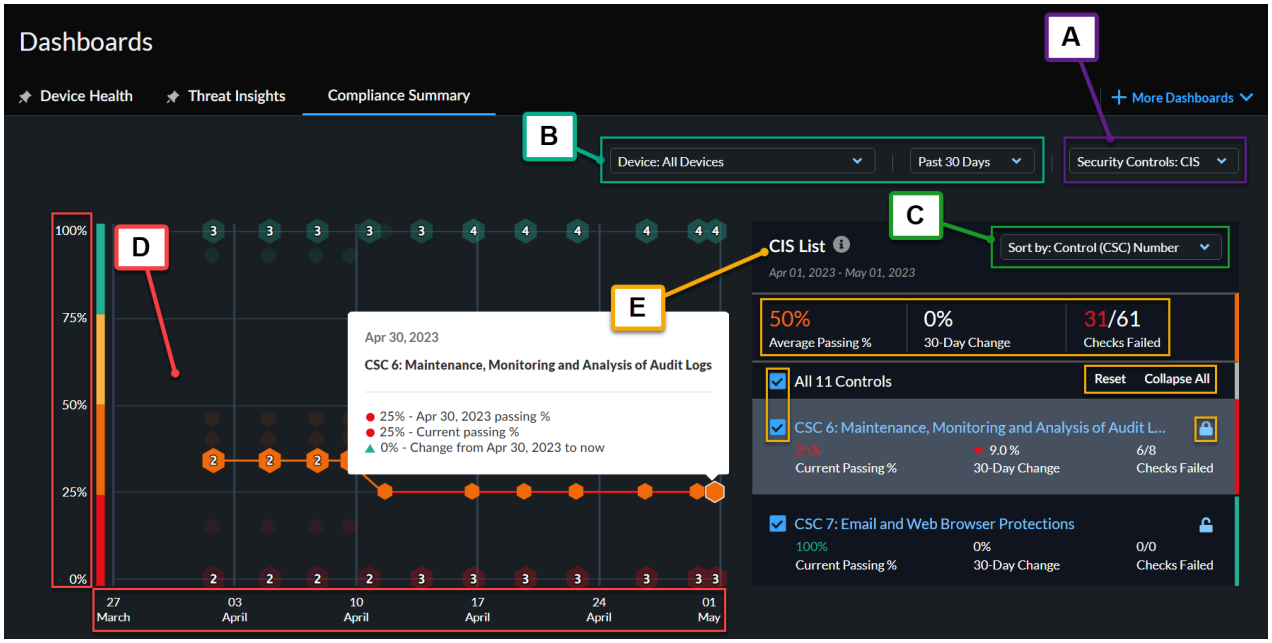
- SC:アクセス制御
- AU:監査と説明責任

- CM:設定の管理
- CP:緊急時対応計画
- IA:識別と認証
- RA:リスク アセスメント
- SC:システムと通信の保護
- SI:システムと情報の完全性

[Compliance Summary Dashboard (コンプライアンス概要ダッシュボード)]にアクセスするには、**[Dashboards (ダッシュボード)]**に移動し、**[Compliance Summary (コンプライアンス概要)]**タブを選択します。

タブの選択肢の中に***[Compliance Summary (コンプライアンス概要)]***が表示されない場合は、［***More Dashboards (その他のダッシュボード)***］を選択し、［***Posture (体制)***］の下に表示された選択肢から［コンプライアンス概要］のチェックボックスをオンにします。





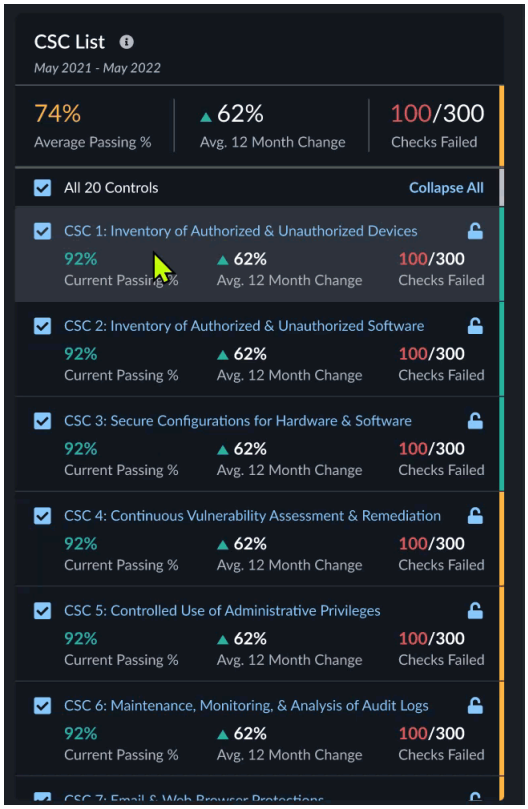
A)セキュリティコントロールセレクター	CISまたはNISTコントロールの選択

B)フィルタ基準：	• デバイス
	• タイム フレーム
	  • 過去7日間
	  • 過去30日間
	  • 過去 90 日間
	  • 過去6ヶ月
	  • 過去 12 か月

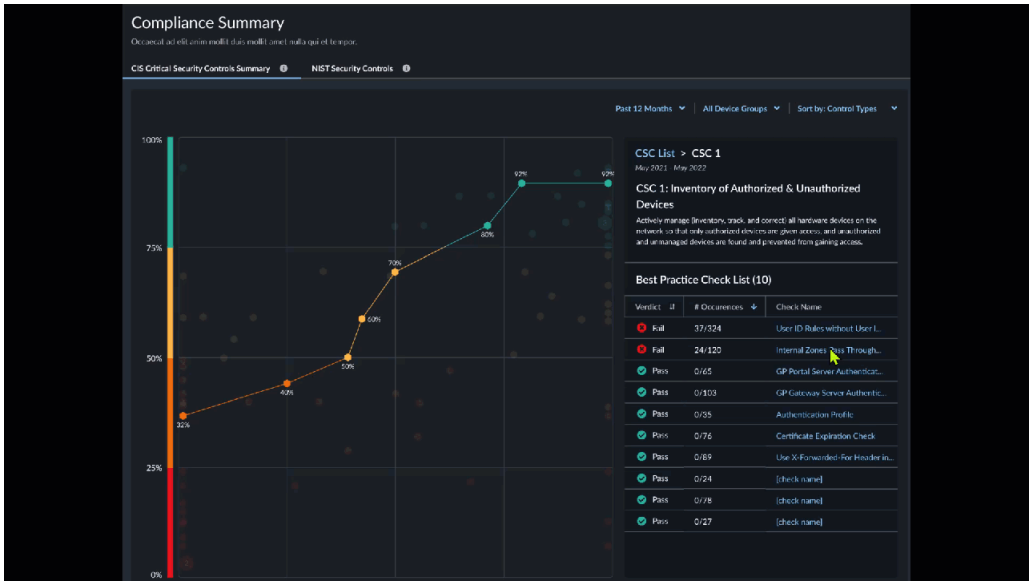
C)ソート基準：	• コントロール (CSC) 番号 • 現在の合格率 % • % 変更 • 失敗したチェック数
D)折れ線グラフ	• 合格率(%) - 指定されたチェックタイプの合格率を表示します。 • タイムライン - 特定のチェックタイプについて、パーセンテージがいつ測定されたかを表示します。

E)チェックリスト	• 統計
	  • 平均合格率（%）- 合格チェックの平均の割合を表示します。
	  • 12ヶ月の変化 - 12ヶ月の期間での変化を示します。
	  • Checks Failed (失敗したチェック数)：失敗したチェックの数を表示します。
	• 選択したコントロール - チェックマークを付けると、折れ線グラフ上にコントロールが表示されます。
	• リセット - すべてのロックを削除します。
	• すべて折りたたむ/すべて展開する - 一覧の統計を表示/非表示にします。
	• 折れ線グラフのロック - 折れ線グラフ上でロックされたチェックを可視状態に保ちます。

- リスト上のコントロールを選択すると、そのコントロールに含まれるベストプラクティスチェックが表示されます。



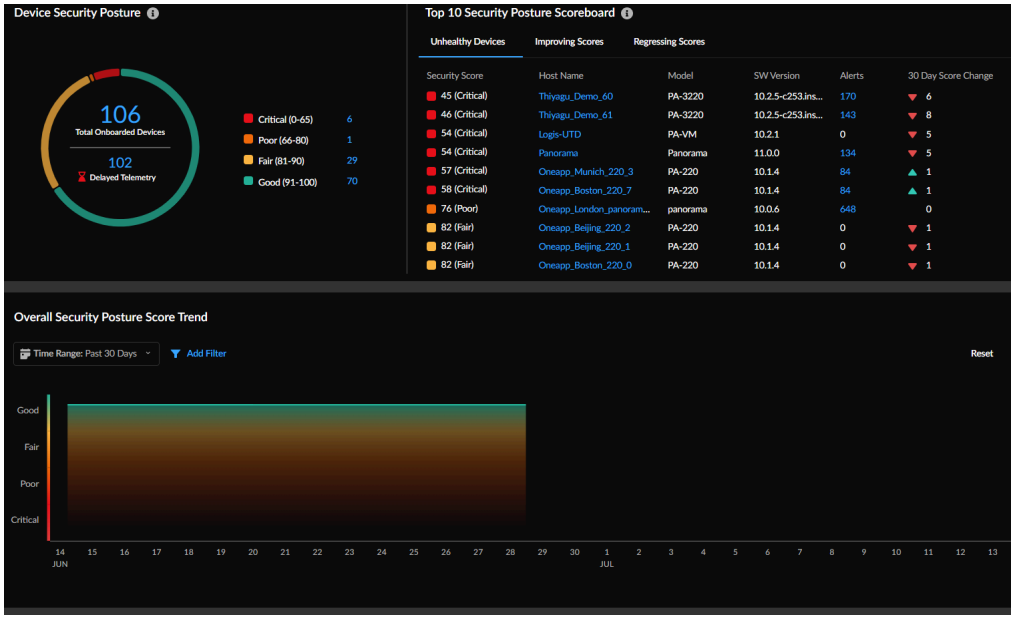
- ベストプラクティスチェックを選択して、チェックでエラーになっているファイアウォール構成を表示します。



ダッシュボード:セキュリティ体制インサイト

どこで使用できますか?	何が必要ですか?
• Software NGFW Creditsによって資金提供されたものを含むNGFW	☐ Strata Cloud Manager Essentials ☐ AIOps for NGFW Premium または Strata Cloud Manager Pro → Strata Cloud Managerで利用できる機能は、使用するライセンスによって異なります。

- 開始するには、**Strata Cloud Manager** > **[Dashboards (ダッシュボード)]** > **[More Dashboard (その他のダッシュボード)]** > **[Security Posture Insights (セキュリティ体制インサイト)]** をクリックします。



このダッシュボードには何が表示されますか？

ダッシュボードには、テナントに関連付けられているすべてのファイアウォールの集計データが表示され、テレメトリデータも送信されています。

オンボードのNGFWデバイスのセキュリティ体制に基づいて、デプロイメントのセキュリティステータスと傾向を可視化できます。セキュリティスコアの重大度（0～100）と、それに対応するセキュリティグレード（良好、普通、不良、重大）によって、デバイスのセキュリティ体制が決定されます。セキュリティスコアは、未解決のアラートの優先度、数量、種類、ステータスに基づいて計算されます。

ダッシュボードのデータはどのように利用できますか？

このダッシュボードを使用して、次の操作を行うことができます。

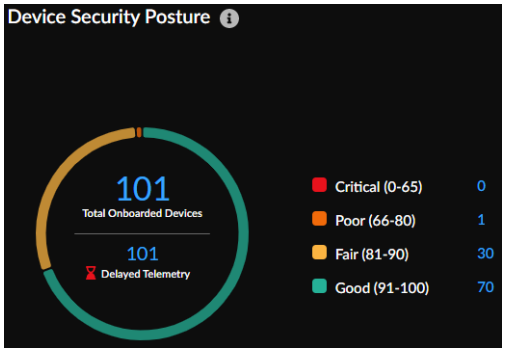
- デプロイメントのセキュリティ体制に影響を与える問題の傾向を把握できます。
- セキュリティスコアの履歴データを見ることで、デプロイメント環境で行われたセキュリティの改善点を把握できます。
- セキュリティ態勢を改善できる機会のあるデバイスを絞り込み、解決すべき課題に優先順位をつける。

レポート機能（レポートのダウンロード、共有、スケジュール）は、このダッシュボードではサポートされていません。

セキュリティ体制インサイトダッシュボード:デバイスのセキュリティ体制

どこで使用できますか?	何が必要ですか?
• Software NGFW Creditsによって資金提供されたものを含むNGFW	☐ Strata Cloud Manager Essentials ☐ AIOps for NGFW Premium または Strata Cloud Manager Pro → Strata Cloud Managerで利用できる機能は、使用するライセンスによって異なります。

- ダッシュボードを表示するには、**Strata Cloud Manager** > **[Dashboards (ダッシュボード)]** > **[More Dashboard (その他のダッシュボード)]** > **[Security Posture Insights (セキュリティ体制インサイト)]** をクリックします。



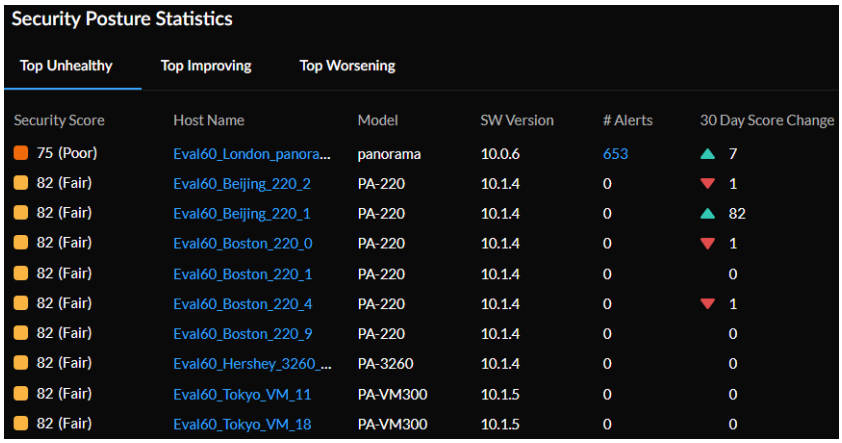
ダッシュボードウィジェットには、次の情報が表示されます。

- オンボードされた NGFW の合計数。
- 12 時間以上テレメトリ データを送信していないデバイスの数。
- デプロイメント内のオンボード デバイスのセキュリティ スコアの優先度。番号リンクをクリックすると、デバイスの詳細とセキュリティ統計を知ることができます。

セキュリティ体制インサイトダッシュボード:セキュリティ体制の統計

どこで使用できますか?	何が必要ですか?
• Software NGFW Creditsによって資金提供されたものを含むNGFW	❑ Strata Cloud Manager Essentials ❑ AIOps for NGFW Premium または Strata Cloud Manager Pro → Strata Cloud Managerで利用できる機能は、使用するライセンスによって異なります。

- ダッシュボードを表示するには、**Strata Cloud Manager** > **[Dashboards (ダッシュボード)]** > **[More Dashboard (その他のダッシュボード)]** > **[Security Posture Insights (セキュリティ体制インサイト)]** をクリックします。



トップの異常

これらは、導入環境のセキュリティ体制に最も影響を与える上位10台のデバイスです。ドリルダウンして、デバイスの詳細とデバイス上のアラートを表示します。デバイス上のクリティカルアラートの修復手順を実行して、セキュリティ体制を改善します。

トップの改善

30 日間にわたってセキュリティ体制スコアが向上した上位 10 台のデバイスを、デバイスの現在のセキュリティスコアと比較して表示します。

トップの悪化

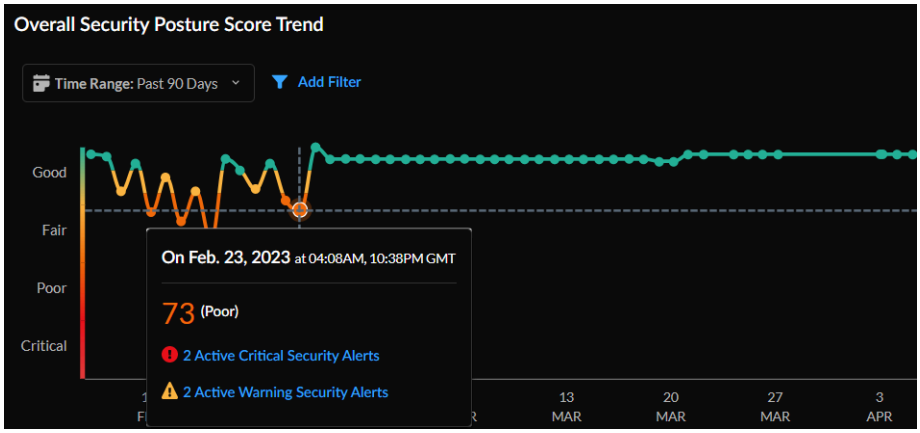
これらは、デバイスの現在のセキュリティスコアと比較してセキュリティ体制スコアが低くなったデバイスです。これらのデバイスのアラートを確認し、優先順位を付けて修正します。

セキュリティ体制インサイトダッシュボード:スコアトレンド

どこで使用できますか?	何が必要ですか?
• Software NGFW Creditsによって資金提供されたものを含むNGFW	☐ Strata Cloud Manager Essentials ☐ AIOps for NGFW Premium または Strata Cloud Manager Pro → Strata Cloud Managerで利用できる機能は、使用するライセンスによって異なります。

- ダッシュボードを表示するには、**Strata Cloud Manager** > **[Dashboards (ダッシュボード)]** > **[More Dashboard (その他のダッシュボード)]** > **[Security Posture Insights (セキュリティ体制インサイト)]** をクリックします。

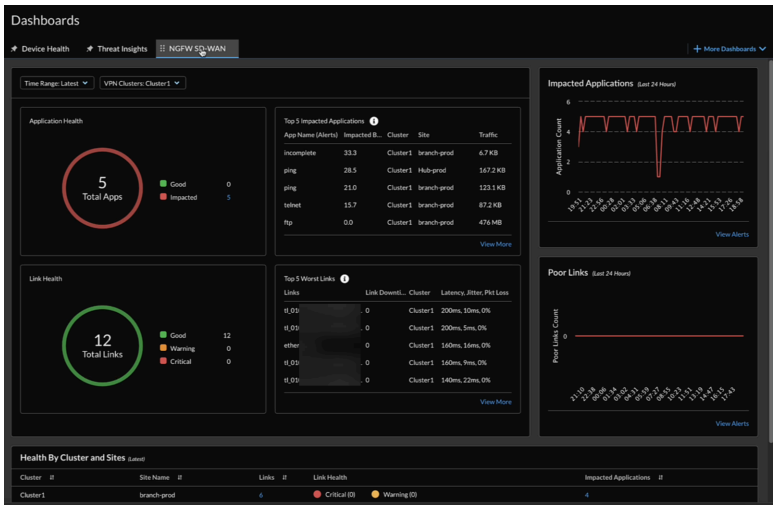
グラフには、選択した期間におけるデプロイメント環境のセキュリティ体制の傾向が表示されます。トリガーポイントにカーソルを合わせると、セキュリティ体制の傾向に関係しているデバイスとアクティブなアラートを確認できます。ホスト名、モデル、またはソフトウェアバージョンでフィルタリングされた1つ以上のデバイスの傾向を表示できます。



ダッシュボード:NGFW SD-WAN

どこで使用できますか?	何が必要ですか?
• Software NGFW Creditsによって資金提供されたものを含むNGFW	☐ AIOps for NGFW Premium または Strata Cloud Manager Pro → Strata Cloud Managerで利用できる機能は、使用するライセンスによって異なります。

- **[Dashboards (ダッシュボード)] [More Dashboards (その他のダッシュボード)] [NGFW SD-WAN]**をクリックして、作業を開始します。



このダッシュボードを利用するには、パロアルトネットワークスの次世代ファイアウォールのStrata Cloud Managerで Software-Defined Wide Area Network (SD-WAN) をセットアップします。

このダッシュボードには何が表示されますか？

NGFW SD-WANダッシュボードには、SD-WANを備えたクラウドマネージドファイアウォールのリンクとアプリケーショントラフィックのパフォーマンスメトリックが表示されます。

ダッシュボードのデータはどのように利用できますか？

このダッシュボードは、次のことに役立ちます。

- VPNクラスタ内のアプリケーションとリンクのパフォーマンスメトリックを可視化し、すべてのVPNクラスタのサマリー情報を表示することで、問題をトラブルシューティングできます。
- ドリルダウンして、影響を受けるサイト、アプリケーション、およびリンクに問題を切り分ける。

- 問題のあるリンクやアプリケーションを調査して、修正するための実行可能なアラートをあげる。MLを活用した異常検知、正規性バンド、予測により、データ駆動型のしきい値に基づいて実用的なアラートが生成され、トレンドに関するインサイトを得ることができます。

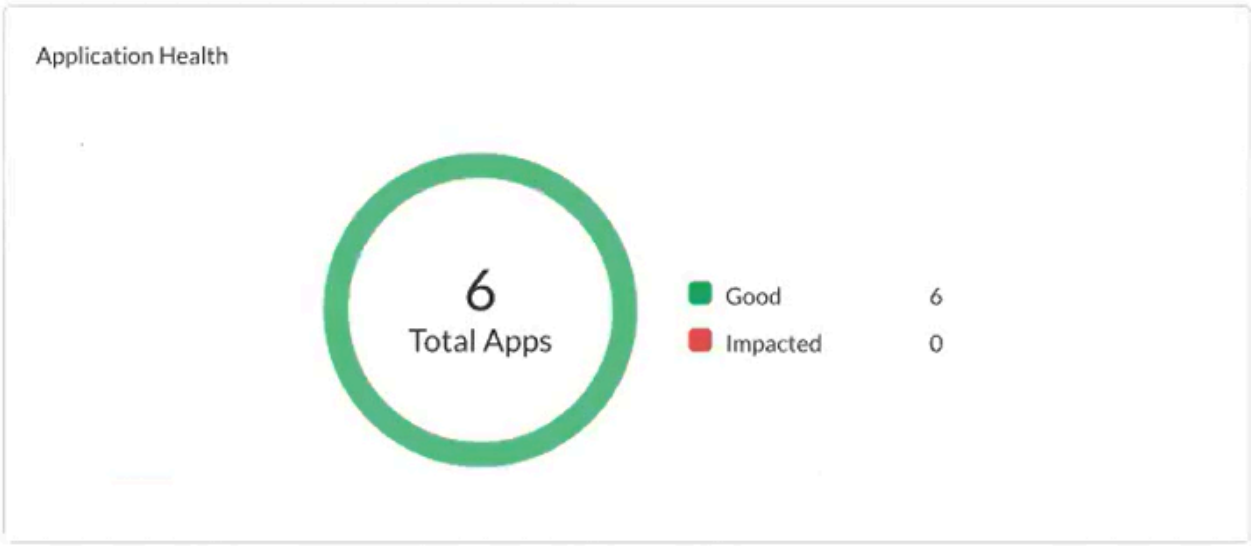
NGFWのSD-WANダッシュボードを監視する方法を紹介する動画です。

NGFW SD-WANダッシュボード:アプリケーションの健全性

どこで使用できますか?	何が必要ですか?
• Software NGFW Creditsによって資金提供されたものを含むNGFW	☐ AIOps for NGFW Premium または Strata Cloud Manager Pro → Strata Cloud Managerで利用できる機能は、使用するライセンスによって異なります。

ダッシュボードには、以下が表示されます。

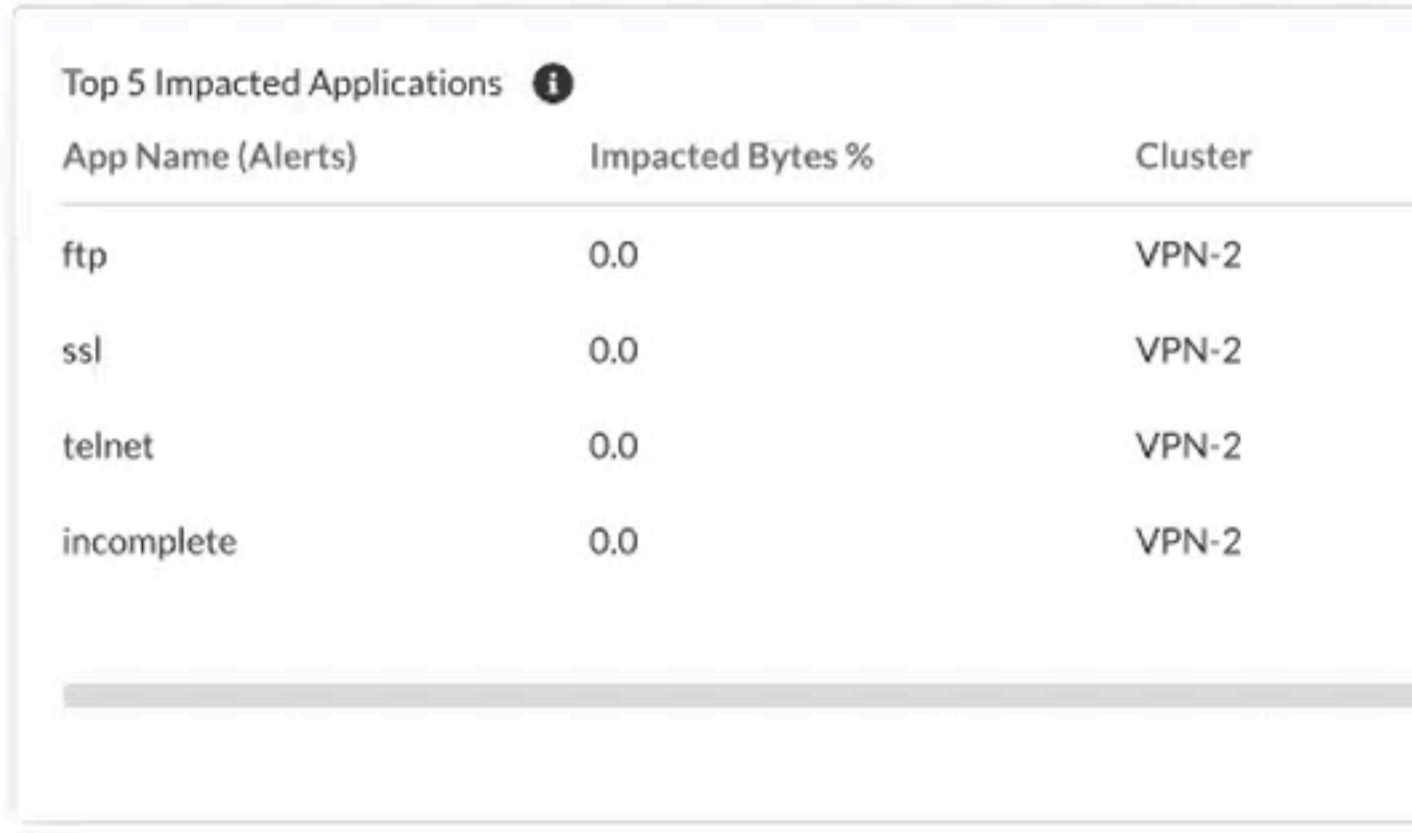
- 選択した期間とVPNクラスタのアプリケーションの合計数。
- 影響を受けたアプリケーションの数 (VPNクラスタ内の1つまたは複数のアプリケーションで、ファイアウォールが選択できるパスのリストにあるパス品質プロファイルで指定されたしきい値を満たすジッター、遅延、またはパケットロスのパフォーマンスを持つパスが1つもない場合がこれに該当)。
- 正常性に問題がないアプリケーション、つまり、ジッター、遅延、またはパケット損失のパフォーマンスの問題が発生していない VPN クラスタ内のアプリケーションの数。



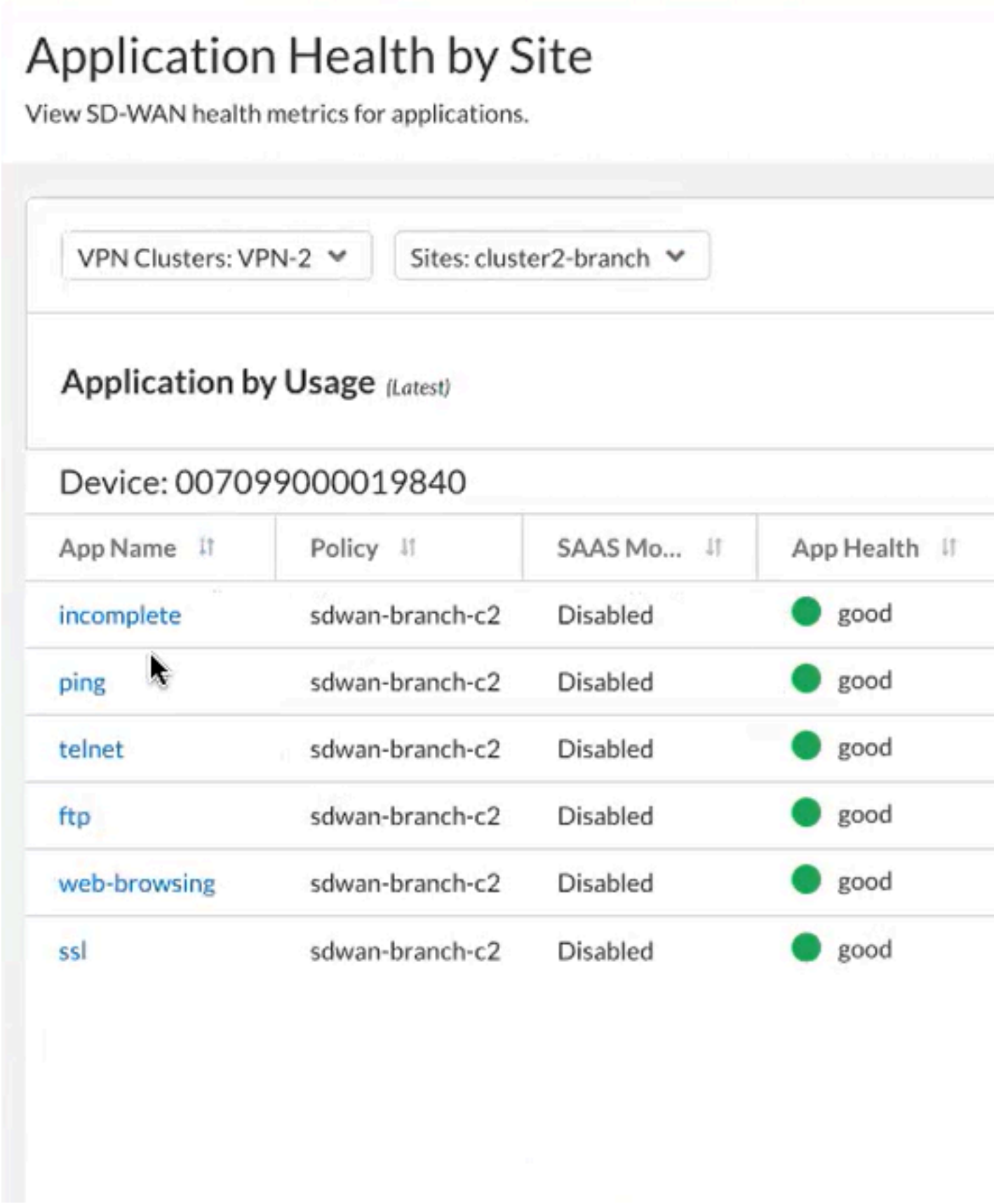
NGFW SD-WANダッシュボード:影響を受ける上位アプリケーション

どこで使用できますか?	何が必要ですか?
• Software NGFW Creditsによって資金提供されたものを含むNGFW	☐ AIOps for NGFW Premium または Strata Cloud Manager Pro → Strata Cloud Managerで利用できる機能は、使用するライセンスによって異なります。

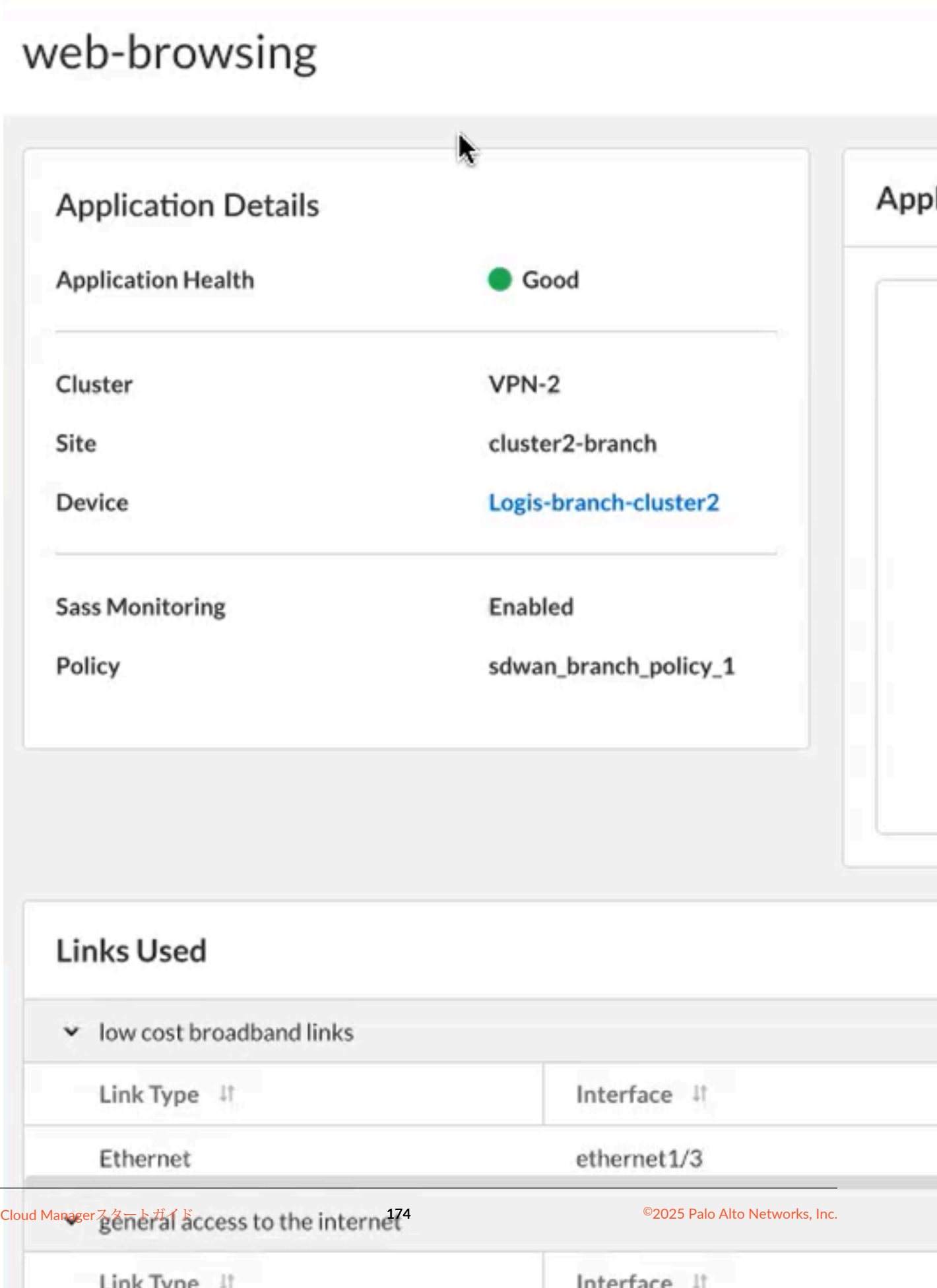
選択した期間と VPN クラスターについて、Strata Cloud Managerは、トラフィックの合計バイト数に対する影響を受けたパーセンテージの計算値に基づいて、影響を受けたアプリケーションの上位 5 本を表示します。計算したパーセンテージが高いほど、アプリケーションへの影響が大きいことを示します。



[View More (詳細を表示)]をクリックして、影響を受けるすべてのアプリケーションを確認します。



さらに、アプリケーションをクリックすると、トラフィックや使用されているリンクなどの詳細が表示されます。使用済みリンクをクリックして詳細を表示することもできます。



NGFW SD-WANダッシュボード:影響を受けるアプリケーション

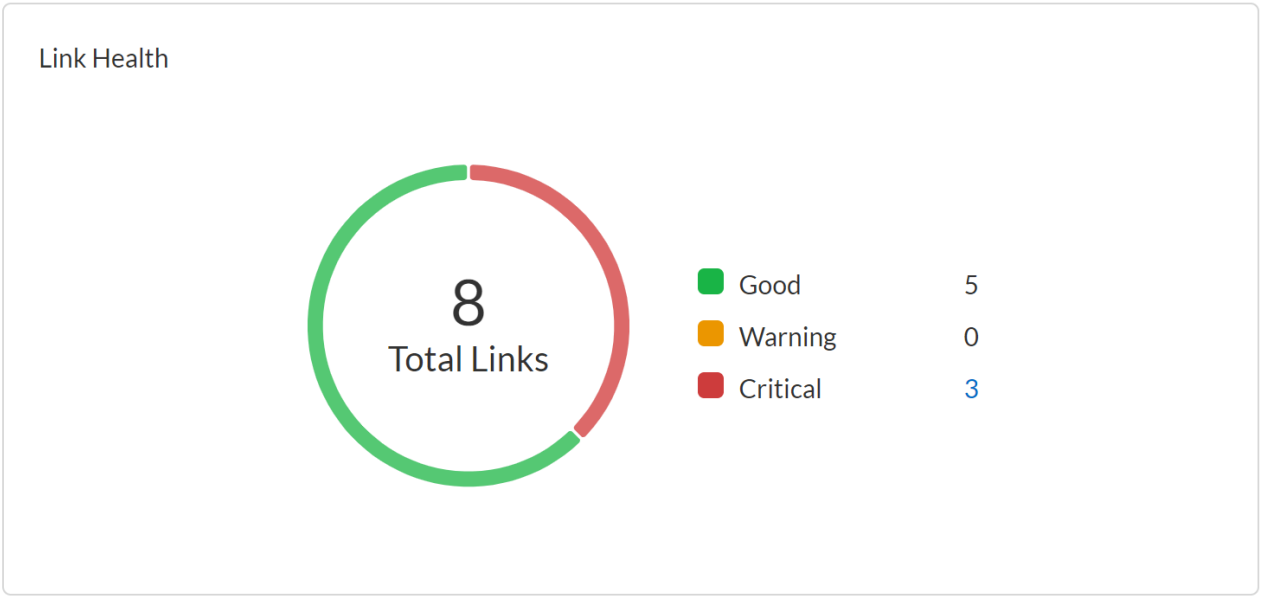
どこで使用できますか?	何が必要ですか?
• Software NGFW Creditsによって資金提供されたものを含むNGFW	❑ AIOps for NGFW Premium または Strata Cloud Manager Pro → Strata Cloud Managerで利用できる機能は、使用するライセンスによって異なります。

- グラフは、過去24時間の影響を受けたアプリケーションを示す傾向を示しています。傾向を示すラインにカーソルを合わせると、特定の時点で影響を受けたアプリケーションが表示されます。
- アラートの表示 をクリックすることで、影響を受けたアプリケーションによって発生した関連アラートを表示できます。

NGFW SD-WANダッシュボード:Link Health (リンクの正常性)

どこで使用できますか?	何が必要ですか?
• Software NGFW Creditsによって資金提供されたものを含むNGFW	❑ AIOps for NGFW Premium または Strata Cloud Manager Pro → Strata Cloud Managerで利用できる機能は、使用するライセンスによって異なります。

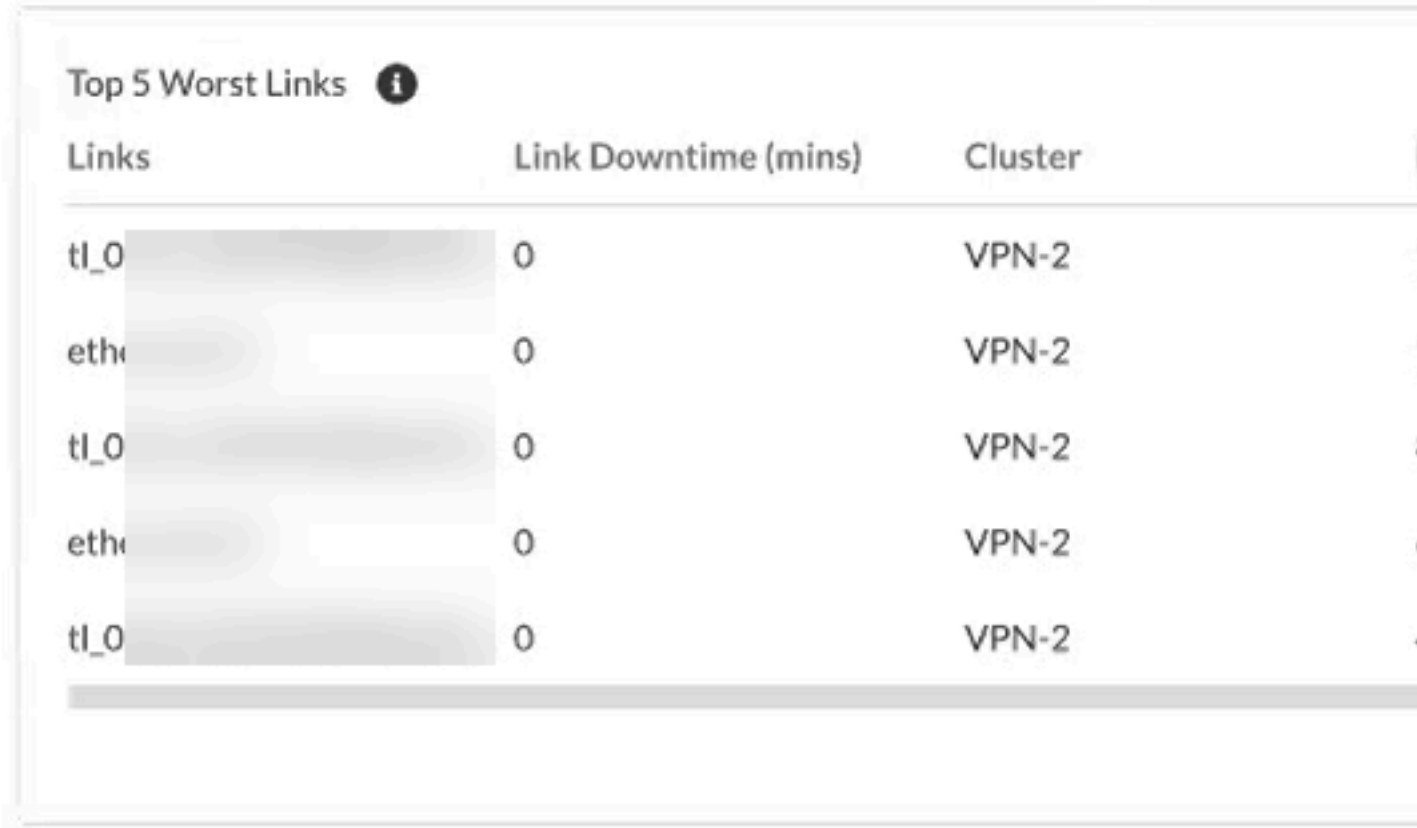
- 選択した期間とVPNクラスタのリンクの合計数。
- [Critical (重大)]、[Warning (警告)]、[Good (良好)]に分類されたリンクの数。
- ［**Critical (重大)**］の数字リンクをクリックすると、SD-WANリンクのパフォーマンスが原因で発生したアラートが表示されます。



NGFW SD-WANダッシュボード:上位ワーストリンク

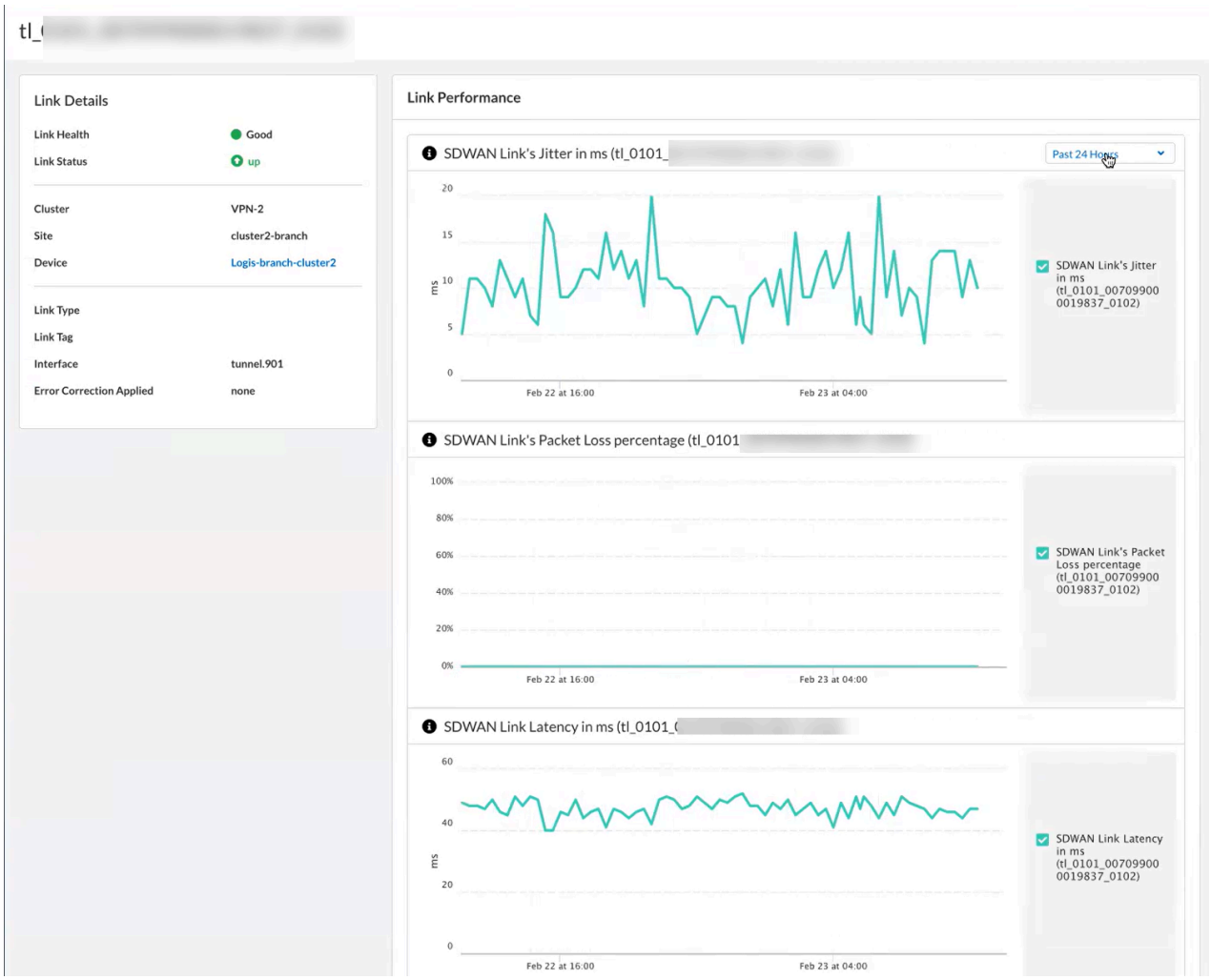
どこで使用できますか?	何が必要ですか?
• Software NGFW Creditsによって資金提供されたものを含むNGFW	☐ AIOps for NGFW Premium または Strata Cloud Manager Pro → Strata Cloud Managerで利用できる機能は、使用するライセンスによって異なります。

選択した期間とVPNクラスターに対して、Strata Cloud Managerは、インターフェースメトリクス (トンネルのダウンタイム、遅延、ジッター、パケットロス) の平均計算値を基に、上位5件のワーストリンクを表示します。リンクは、トンネルのダウンタイム、遅延、パケットロス、およびジッターの優先順位に基づいてランク付けされます。計算された平均値が高いほど、リンクの品質が低いことになります。



[View More (詳細を表示)]をクリックすると、影響を受けているすべてのリンクを確認できます。

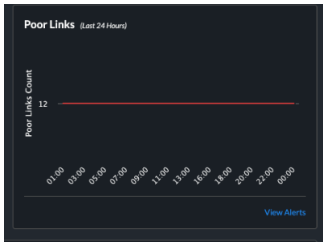
さらに、リンクをクリックすると、リンクパフォーマンスに基づいたチャートを含む詳細が表示されます。



NGFW SD-WANダッシュボード:貧弱なリンク

どこで使用できますか?	何が必要ですか?
• Software NGFW Creditsによって資金提供されたものを含むNGFW	☐ AIOps for NGFW Premium または Strata Cloud Manager Pro → Strata Cloud Managerで利用できる機能は、使用するライセンスによって異なります。

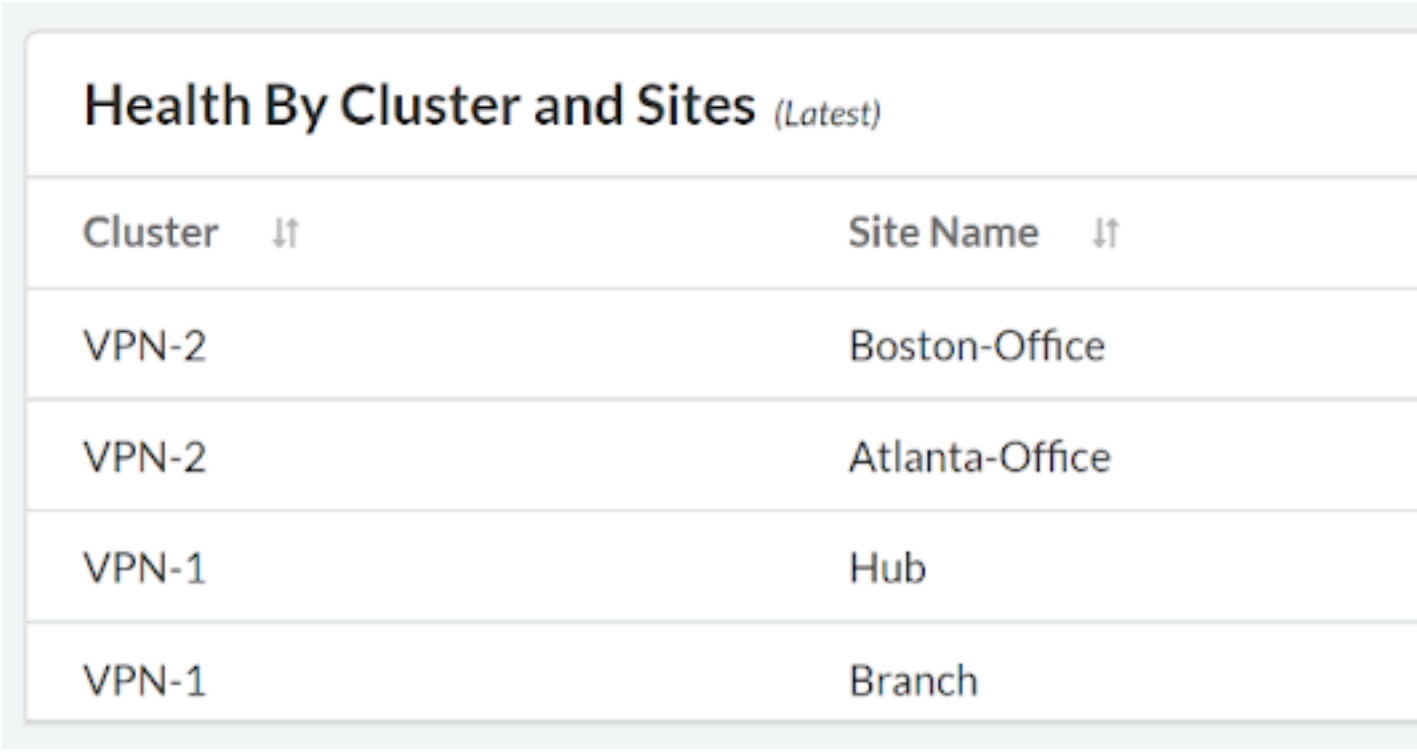
- チャートは、過去24時間に検出された脆弱なリンクの傾向を示しています。トレンドラインの上にカーソルを置くと、特定の時点での不良リンクが表示されます。
- **[View Alerts (アラートの表示)]**をクリックすると、リンクの脆弱さが原因で発生した関連するアラートが表示されます。



NGFW SD-WANダッシュボード:クラスタ別とサイト別のヘルス

どこで使用できますか?	何が必要ですか?
• Software NGFW Creditsによって資金提供されたものを含むNGFW	☐ AIOps for NGFW Premium または Strata Cloud Manager Pro → Strata Cloud Managerで利用できる機能は、使用するライセンスによって異なります。

各サイトのリンク数、正常性、影響を受けたアプリケーションを表示します。



これらの列の下の数字リンクをクリックすると、その列に関する詳細が表示されます。

ダッシュボード:Prisma SD-WAN

どこで使用できますか?	何が必要ですか?
• Prisma SD-WAN	❑ Prisma SD-WANライセンス その他のライセンスと可視性に必要な前提条件は次のとおりです。 ❑ ダッシュボードの特定のウィジェットのロックを解除するライセンス ❑ 予測分析のためのWANクラリティ ❑ ダッシュボードを表示する権限を持つロール → Strata Cloud Managerで利用できる機能は、使用するライセンスによって異なります。

このダッシュボードには何が表示されますか？

Dashboard (ダッシュボード)には、Prisma SD-WANのネットワーク、デバイス、アプリケーションのメトリックが、概要レベルとグラフィカルに表示されます。さらに、次の情報が表示されます。

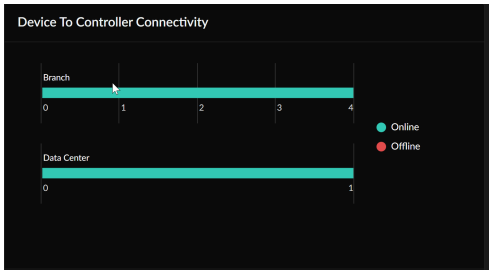
- ブランチオフィスおよびデータセンターデバイスとコントローラの接続ステータス。
- 入口および出口トラフィックのアプリケーション使用率データ。
- 過去1週間のテナント全体のすべての支店サイトの基本的なネットワークインサイトとレポート。
- 生成されたインシデント数別の上位ブランチサイトおよびデータセンターサイトに関する情報。
- MOSスコア、パケット損失、ジッター、遅延などのサイト全体のリンク品質メトリック。
- 過去3ヶ月から6ヶ月の情報に基づく、サイトレベルでの容量使用率の予測。

Prisma SD-WANダッシュボード:デバイスとコントローラの接続

どこで使用できますか?	何が必要ですか?
• Prisma SD-WAN	❑ Prisma SD-WANライセンス その他のライセンスと可視性に必要な前提条件は次のとおりです。 ❑ ダッシュボードの特定のウィジェットのロックを解除するライセンス

どこで使用できますか?	何が必要ですか?
	❑ 予測分析のためのWANクラリティ ❑ ダッシュボードを表示する権限を持つロール → Strata Cloud Managerで利用できる機能は、使用するライセンスによって異なります。

デバイスからコントローラーへの接続ウィジェットには、ブランチおよびデータセンターのPrisma SD-WANコントローラーに接続されたオンラインおよびオフラインのIONデバイスの数が表示されます。このインタラクティブなグラフを使用すると、対応する支店とデータセンターの請求対象デバイスのオンラインまたはオフラインのステータスを表示できます。

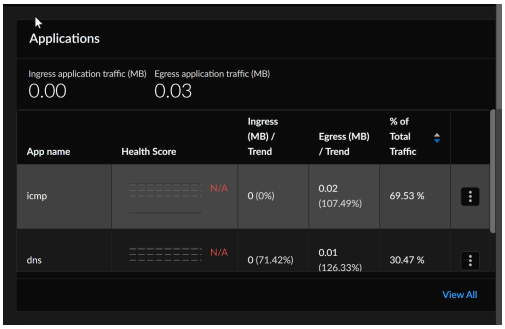


インタラクティブグラフの **[Branch (バッチ)]** または**[Data Center (データセンター)]**をクリックすると、要求されたデバイスと要求されていないデバイスの名前、ステータス、インストールされているソフトウェアバージョン、最後のアクティビティ、およびデバイスの冗長ステータスが表示されます。

Prisma SD-WANダッシュボード:アプリケーション [applications]

どこで使用できますか?	何が必要ですか?
• Prisma SD-WAN	❑ Prisma SD-WANライセンス その他のライセンスと可視性に必要な前提条件は次のとおりです。 ❑ ダッシュボードの特定のウィジェットのロックを解除するライセンス ❑ 予測分析のためのWANクラリティ ❑ ダッシュボードを表示する権限を持つロール → Strata Cloud Managerで利用できる機能は、使用するライセンスによって異なります。

［Applications (アプリケーション)］ウィジェットには、選択した時間範囲におけるサイトのアプリケーション使用率に関する情報が表示されます。時間範囲のアプリケーション入口および出口トラフィックの合計が表示されます。他のトラフィックとともに、トラフィック量上位10件のアプリケーションが表示されます。［**View All (すべて表示)**］をクリックすると、選択した時間帯のアプリケーション稼働状況分布、TCPアプリケーション稼働状況分布（経時的）、新しいフロー、帯域幅使用率、トランザクション統計が、上位のアプリケーションとともに表示されます。ドリルダウンすると、ダッシュボードで選択した時間範囲のサイトごとのアプリケーションのパフォーマンスとメトリックを表示できます。

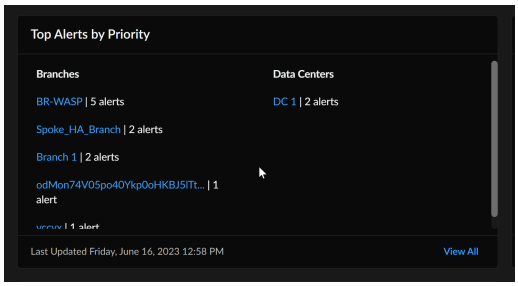


初期状態ではすべてのTCPアプリケーションのメトリックが表示されますが、上位10のTCPアプリケーションのいずれかを選択して、特定の上位アプリケーションに絞り込むことができます。

Prisma SD-WAN ダッシュボード:優先度別の上位アラート

どこで使用できますか?	何が必要ですか?
• Prisma SD-WAN	❑ Prisma SD-WANライセンス その他のライセンスと可視性に必要な前提条件は次のとおりです。 ❑ ダッシュボードの特定のウィジェットのロックを解除するライセンス ❑ 予測分析のためのWANクラリティ ❑ ダッシュボードを表示する権限を持つロール → Strata Cloud Managerで利用できる機能は、使用するライセンスによって異なります。

優先度別の上位アラートウィジェットには、優先度別の上位5つのアラートが表示されます。選択した時間範囲で生成されたアラートの数によって、上位のブランチサイトとデータセンターサイトの情報を確認できます。ドリルダウンして、選択した時間範囲のサイトごとのアラート情報を表示できます。



[View All (すべて表示)] をクリックすると、アラートに関する次の情報が表示されます。

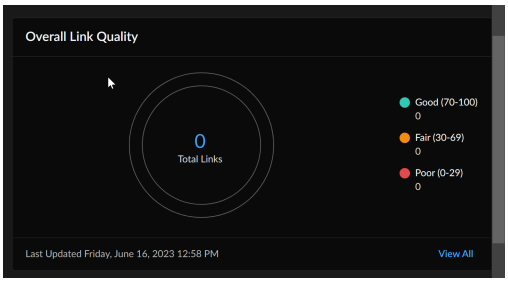
- アラートが作成された日時。
- インシデントの名前。
- 影響を受ける主なオブジェクト。
- アラートの重大度。
- アラートの優先順位。

省略記号をクリックしてアラートのトラブルシューティングを行います。

Prisma SD-WANダッシュボード:全体的なリンク品質

どこで使用できますか?	何が必要ですか?
• Prisma SD-WAN	❑ Prisma SD-WANライセンス その他のライセンスと可視性に必要な前提条件は次のとおりです。 ❑ ダッシュボードの特定のウィジェットのロックを解除するライセンス ❑ 予測分析のためのWANクラリティ ❑ ダッシュボードを表示する権限を持つロール → Strata Cloud Managerで利用できる機能は、使用するライセンスによって異なります。

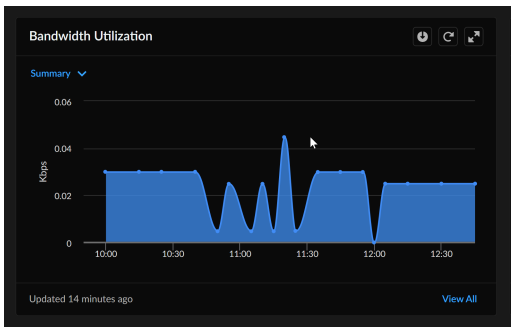
[Overall Link Quality (全体的なリンク品質)] ウィジェットは、選択した時間範囲におけるすべてのサイトのリンクの現在の状態の全体的なスナップショットを提供します。ドリルダウンして、リンク パフォーマンス、リンク パケット ロス、リンク ジッター、およびリンクジッターを表示することができ、[Link Quality Metrics (リンク品質指標)]ダッシュボードでより詳細に表示したい情報を分析できます。



Prisma SD-WANダッシュボード:帯域幅使用状況

どこで使用できますか?	何が必要ですか?
• Prisma SD-WAN	❑ Prisma SD-WANライセンス その他のライセンスと可視性に必要な前提条件は次のとおりです。 ❑ ダッシュボードの特定のウィジェットのロックを解除するライセンス ❑ 予測分析のためのWANクラリティ ❑ ダッシュボードを表示する権限を持つロール → Strata Cloud Managerで利用できる機能は、使用するライセンスによって異なります。

[Bandwidth Utilization (帯域幅使用率)]ウィジェットには、ネットワーク内のトレイルで利用されている帯域幅の量が表示されます。これは、帯域幅スパイク、特定のサイトで消費された総帯域幅、およびアプリケーションを視覚的に表したもので、アップロードが入口方向か出口方向か(またはその両方に該当するのか)を示します。



Bandwidth Utilization (帯域幅使用率)チャートにカーソルを移動すると、アプリケーションまたはタイムスタンプで帯域幅使用率をより詳細に表示できます。通常、アプリケーションは帯域幅の使用率の高い順にリストされます。チャートには、時間の経過とともに消費される帯域幅が表示されます。1Hビューは1分ごとの細かいデータを提供し、1D写真は5分ごとのデータを示して

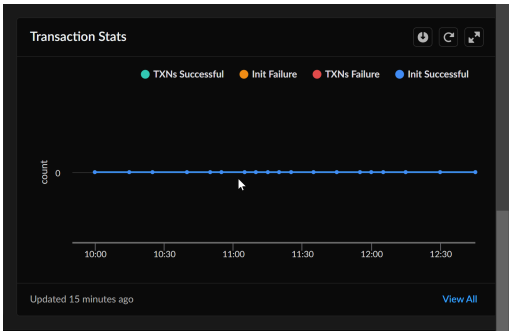
います。1次元チャートデータは、各サンプルの平均が5分以上です。使用率が5分を超えて持続する場合は、対応するピーク使用率を両方のチャートで確認できます。

ウィジェットからダウンロードオプションを使用して、PDF、CSV、XLS、PNGのいずれかの形式で帯域幅使用率チャートをダウンロードすることができます。

Prisma SD-WAN ダッシュボード:トランザクション統計

どこで使用できますか?	何が必要ですか?
• Prisma SD-WAN	☐ Prisma SD-WANライセンス その他のライセンスと可視性に必要な前提条件は次のとおりです。 ☐ ダッシュボードの特定のウィジェットのロックを解除するライセンス ☐ 予測分析のためのWANクラリティ ☐ ダッシュボードを表示する権限を持つロール → Strata Cloud Managerで利用できる機能は、使用するライセンスによって異なります。

[Transaction Stats (トランザクション統計)]ウィジェットには、TCPフローに関するトランザクション統計を表示します。特定のアプリケーションまたはすべてのアプリケーション、特定のパスまたはすべてのパス、すべての正常性イベントに関する開始/トランザクションの成功と失敗が表示されます。ネットワークパス上で実行されるネットワークおよびアプリケーションのパフォーマンスと可用性を測定します。Prisma SD-WANは、指定されたパス上の各リクエストについて、開始トランザクションとデータ転送トランザクションのトランザクションエラー率をリアルタイムで監視します。



［Transaction Stats (トランザクション統計)］チャートから、帯域幅使用率またはパス別にアプリケーションのリストを表示します。成功したトランザクションを除外して、トランザクションの失敗の統計をきめ細かく表示できます。チャートには、次のカテゴリのトランザクションの成功または失敗の数が表示されます。

- **Init Sucessful**：スリーウェイハンドシェイクを正常に完了しました。

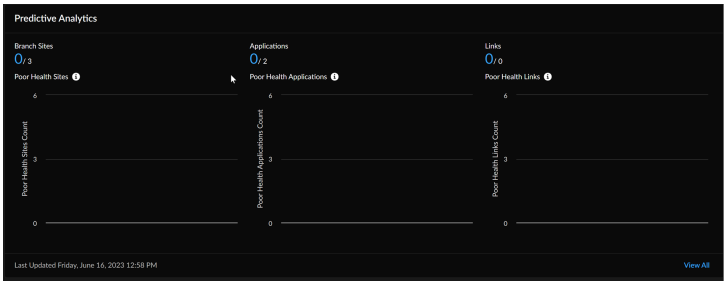
- **TXNs Sucessful**：3ウェイハンドシェイク完了後、データの転送に成功しました。
- **Init Failure**:スリーウェイハンドシェイクを完了できませんでした。障害の原因としては、ファイアウォールの設定ミス、アプリケーションサーバの問題、ネットワークアクセス制御リストの設定ミス、WANネットワークプロバイダの問題などが考えられます。
- **TXNs Failure**：スリーウェイハンドシェイクの完了後、データの転送が失敗しました。障害の原因としては、ファイアウォールの設定ミス、アプリケーションサーバの問題、ネットワークアクセス制御リストの設定ミス、WANネットワークプロバイダの問題などが考えられます。

ウィジェットからダウンロードオプションを使用して、PDF、CSV、XLS、PNGのいずれかの形式で帯域幅使用率チャートをダウンロードすることができます。

Prisma SD-WANダッシュボード:予測分析

どこで使用できますか?	何が必要ですか?
• Prisma SD-WAN	☐ Prisma SD-WANライセンス その他のライセンスと可視性に必要な前提条件は次のとおりです。 ☐ ダッシュボードの特定のウィジェットのロックを解除するライセンス ☐ 予測分析のためのWANクラリティ ☐ ダッシュボードを表示する権限を持つロール → Strata Cloud Managerで利用できる機能は、使用するライセンスによって異なります。

Predictive Analytics (予測分析) ウィジェットは、サイトとアプリケーションの正常性に関する洞察とプロアクティブな監視を提供し、重大な問題を特定してより迅速にトラブルシューティングすることで、サービス レベルを向上させます。重要なサイト、リンク、アプリケーションを識別し、AI/MLヘルススコアに基づいてテナント レベルでそれらを **Good**、**Fair**、**Poor** に分類します。ウィジェットには、過去3～6ヶ月の情報に基づいてブランチ サイト レベルでの容量使用率を予測する機能が含まれています。



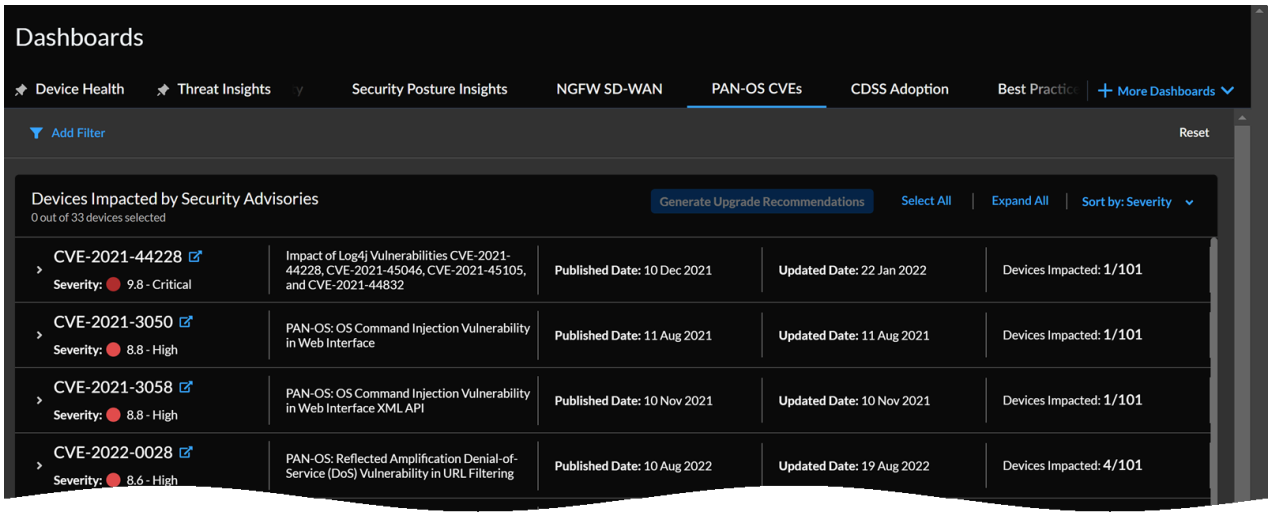
メトリックを表示するデフォルトの時間範囲は3時間ですが、必要な情報の範囲に応じて、より短い期間またはより長い期間に調整できます。過去28日間に帯域幅使用率が増加した上位10のサイトに関する洞察を得られます。28日間の予測が利用できない場合はいつでも7日間の予測を表示し、将来の支店の容量使用率を予測できます。

[View All (すべて表示)] をクリックすると、ブランチ サイト、アプリケーション、リンク、ネットワーク インサイト、過去30日間のトラフィック量の増加が見られた上位サイト、サイト容量の予測と異常に関するインサイトが得られます。

ダッシュボード:PAN-OS CVE

どこで使用できますか?	何が必要ですか?
• Software NGFW Creditsによって資金提供されたものを含むNGFW	❑ Strata Cloud Manager Essentials ❑ AIOps for NGFW Premium または Strata Cloud Manager Pro → Strata Cloud Managerで利用できる機能は、使用するライセンスによって異なります。

- **[Dashboards (ダッシュボード)]** [More Dashboards (その他のダッシュボード)] [PAN-OS CVEs]をクリックして、作業を開始します。



このダッシュボードには何が表示されますか？

ダッシュボードには、テナントにオンボードされ、テレメトリ データも送信しているすべてのファイアウォールと*Panorama*の集計データが表示されます。さらに、*NGFW PSIRT*の*CVEs*のデータベースのテレメトリデータも表示されます。

PAN-OS CVEsダッシュボードでは、デバイスで有効になっている機能に基づいて、特定の脆弱性の影響を受けるデバイスの数が表示されます。Strata Cloud Managerは、有効になっている機能を分析し、CVEの影響を受けるデバイスを特定します。

影響を受けるデバイスの脆弱性を把握したら、アップグレード推奨機能を使用してパッチ適用を計画できます。CVEを展開し、脆弱性を修正するためにアップグレードするファイアウォールを選択して、**[Generate Upgrade Recommendations (アップグレード推奨事項の作成)]**をクリックします。［NGFW - Upgrade Recommendations (アップグレード推奨事項)］ にリダイレクトされ、生成されたレポートが表示されます。

ここでは、デバイスに影響を与える脆弱性を評価し、脆弱性を修正するためのアップグレードの推奨事項を生成する方法を示します。

ダッシュボードのデータはどのように利用できますか？

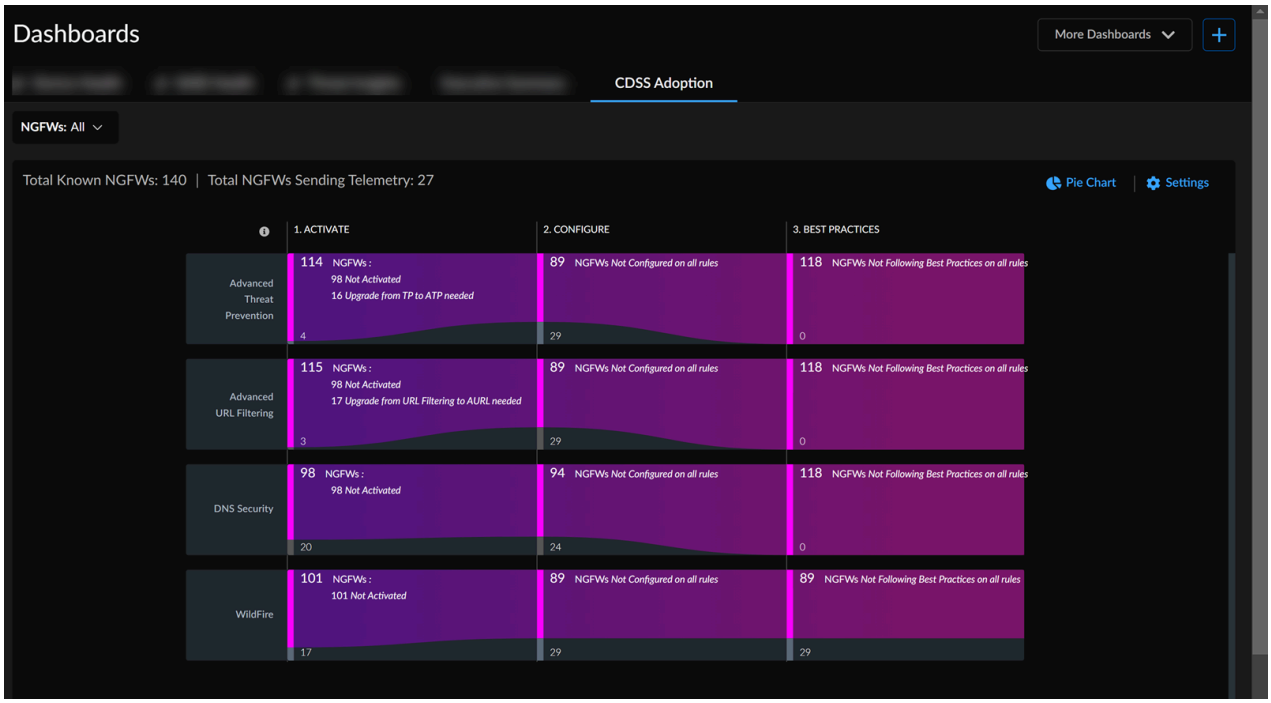
このダッシュボードは、次のことに役立ちます。

- 脆弱性を緩和するためにアップグレードするデバイスを決定します。
- CVEを更新すると、ホスト名、モデル、シリアルナンバー、SWバージョン、最後のテレメトリアップデートなど、影響を受けるデバイスの詳細が表示されます。
- CVEをフィルタリングし、**[Severity (重要度)]**または**[Devices Impacted (影響を受けるデバイス)]**でさらにソートします。
- CVEに関連付けられているアドバイザリをクリックして表示する。

ダッシュボード:CDSS の採用

どこで使用できますか?	何が必要ですか?
• Software NGFW Creditsによって資金提供されたものを含むNGFW	☐ Strata Cloud Manager Essentials ☐ AIOps for NGFW Premium または Strata Cloud Manager Pro → Strata Cloud Managerで利用できる機能は、使用するライセンスによって異なります。

- 開始するには、**[Dashboards (ダッシュボード)]** > **[Posture (体制)]** > **[CDSS Adoption (CDSS採用)]** をクリックします。



このダッシュボードには何が表示されますか?

- ダッシュボードには、テナントにオンボードされ、テレメトリ データも送信しているすべてのファイアウォールの集計データが表示されます。
- 現在、このダッシュボードは、次の4つのセキュリティサブスクリプションのみをサポートしています。高度な脅威防御、高度な*URL*フィルタリング、*DNS*セキュリティ、*Wildfire*。

CDSS 採用 ダッシュボードには、推奨されるクラウド配信セキュリティ サービス(CDSS)サブスクリプションとデバイスでのその使用状況が表示されます。これにより、セキュリティ ギャップを特定し、企業のセキュリティ体制を強化するのに役立ちます。このページに移動すると、NGFWでゾーンの役割を確認または更新するように求めるポップアップが表示され、セキュリティサービスの推奨事項を正確に取得できます。このポップアップウィンドウのリンクをたどると、ゾーンをロールにマップできます。

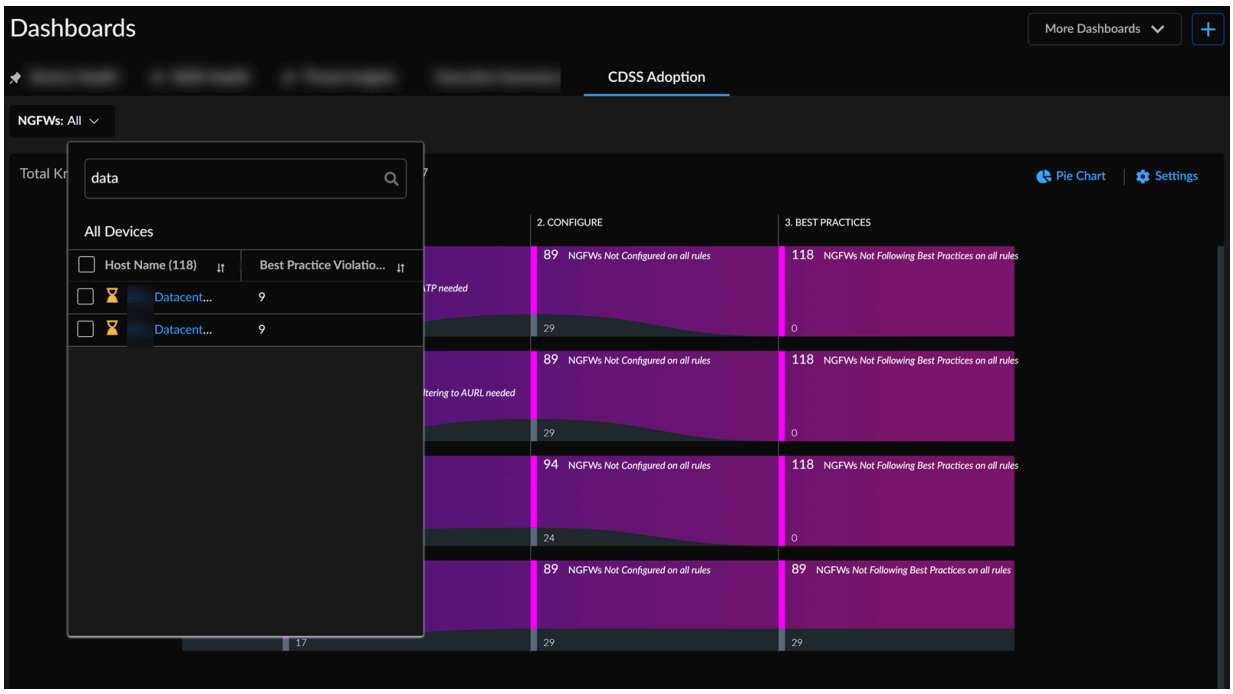
CDSS採用ダッシュボードを使用してセキュリティ サブスクリプションを監視する方法を紹介するビデオを次に示します。

管理画面のデータはどのように利用できますか？

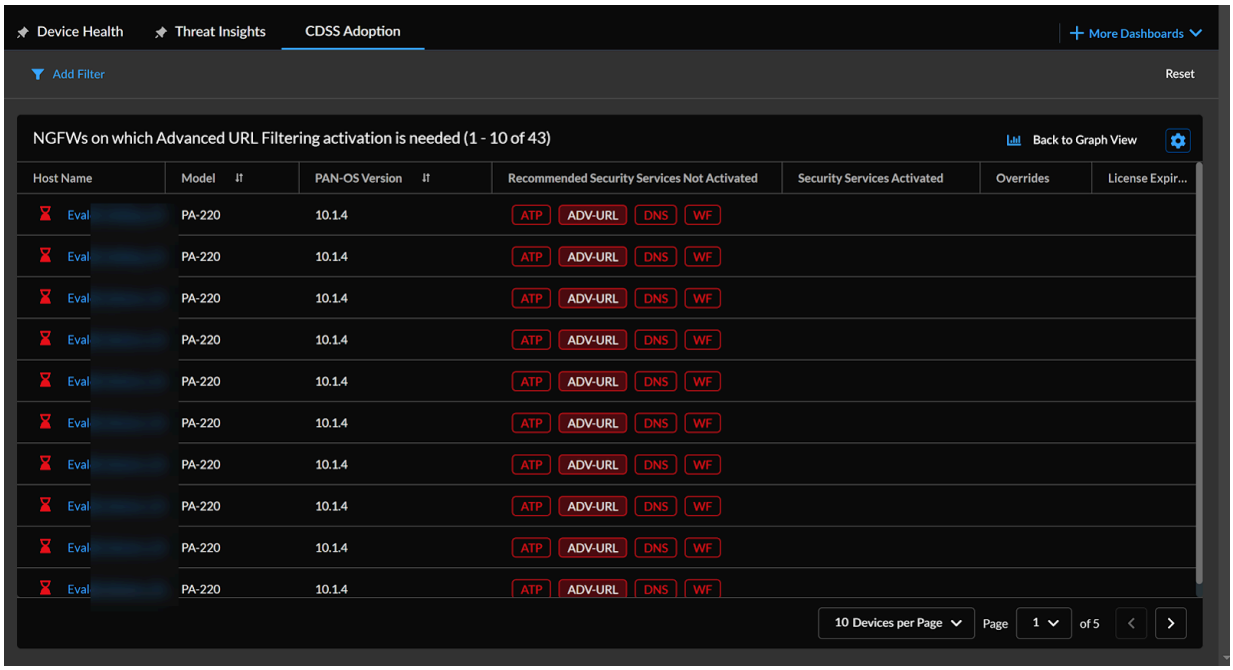
このダッシュボードは次のことに役立ちます。

- 概要ページの上部には、AIOps for NGFWインスタンスで既知のNGFW の合計数とテレメトリを送信しているNGFWの数が表示されます。CDSSの導入は、アクティベーション、設定、ベストプラクティスの遵守を通じて進行します。各サブスクリプションの進行状況を追跡するには、チャート内の数字をクリックするだけで、この過程で更新が必要なデバイスのリストが表示されます。デバイスでセキュリティ サブスクリプション ライセンスを使用するには、ライセンスをアクティブ化してから、それに応じてサービスまたは機能を設定する必要があります。

  特定のNGFWのセキュリティ サービス データに焦点を当てるには、それに基づいてグラフをフィルターします。このドロップダウン リストでは、デバイスのベスト プラクティス違反も表示できます。

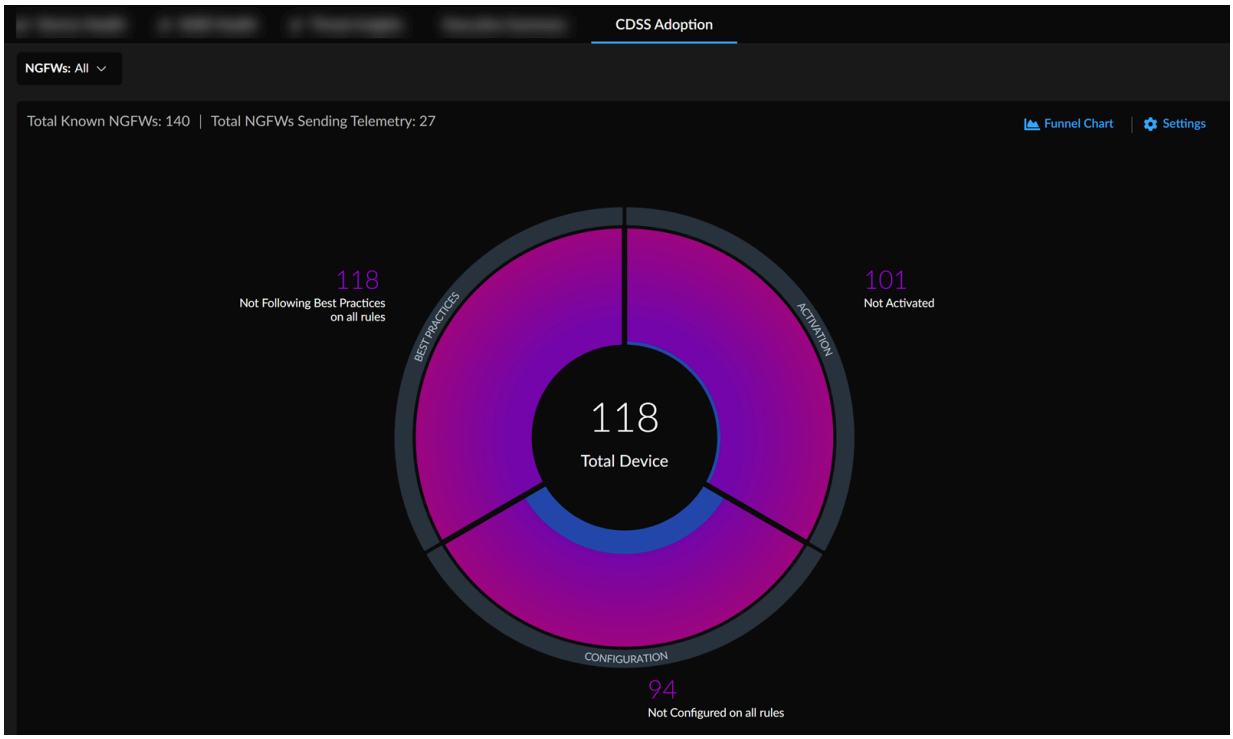


- **ACTIVATE**、**CONFIGURE**、または **BEST PRACTICES**のいずれかの値をクリックすると、詳細が表形式で表示されます。

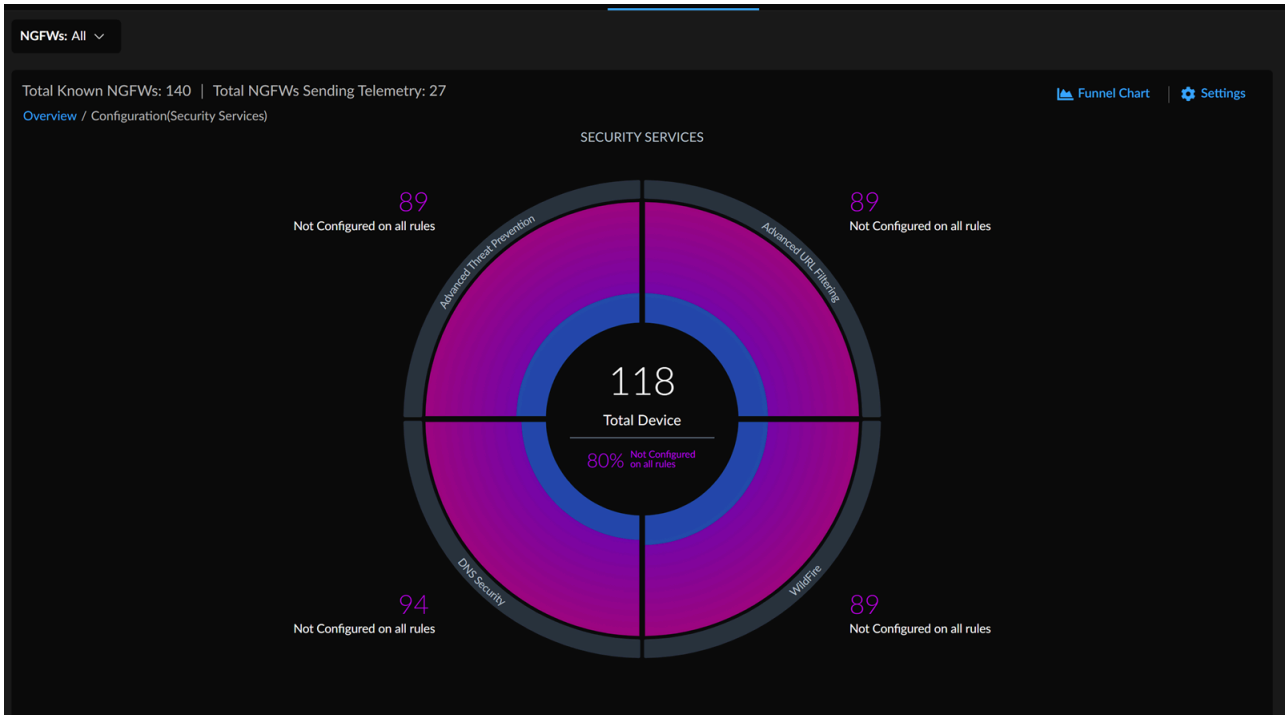


この例では、NGFW用のAIOpsは、NGFW用のAdvanced Threat Protection (ATP)、ドメイン ネーム システム(DNS)、WildFire(WF)セキュリティ サービスとともに、高度なURLフィルタリング(ADV-URL) をアクティブ化することを推奨しています。**[Back to Graph View (**グラフビューに戻る**)]** をクリックすると、概要ページに移動できます。

- 同じセキュリティ ポスチャ データを円グラフ形式で表示することもできます。円グラフアイコンをクリックすると、推奨されるセキュリティ サービスに関する情報が円グラフ形式で表示されます。



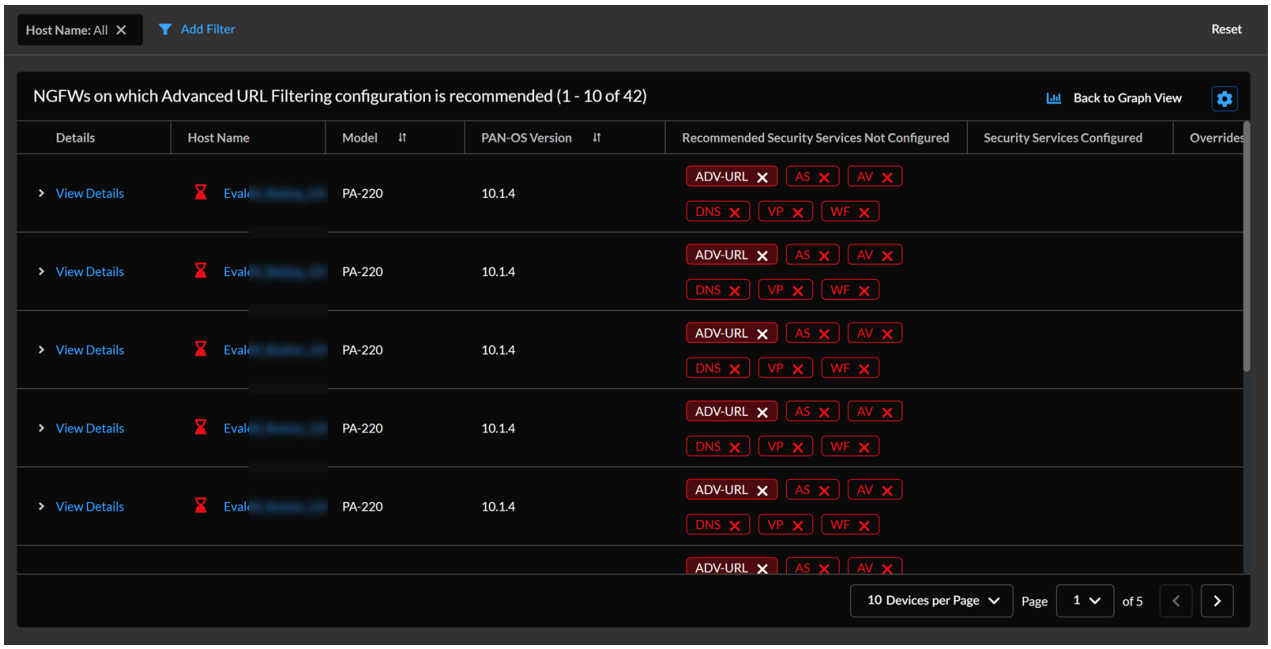
- 円グラフのセクションをクリックすると、個々のセキュリティ サービスに関する情報を表示できます。



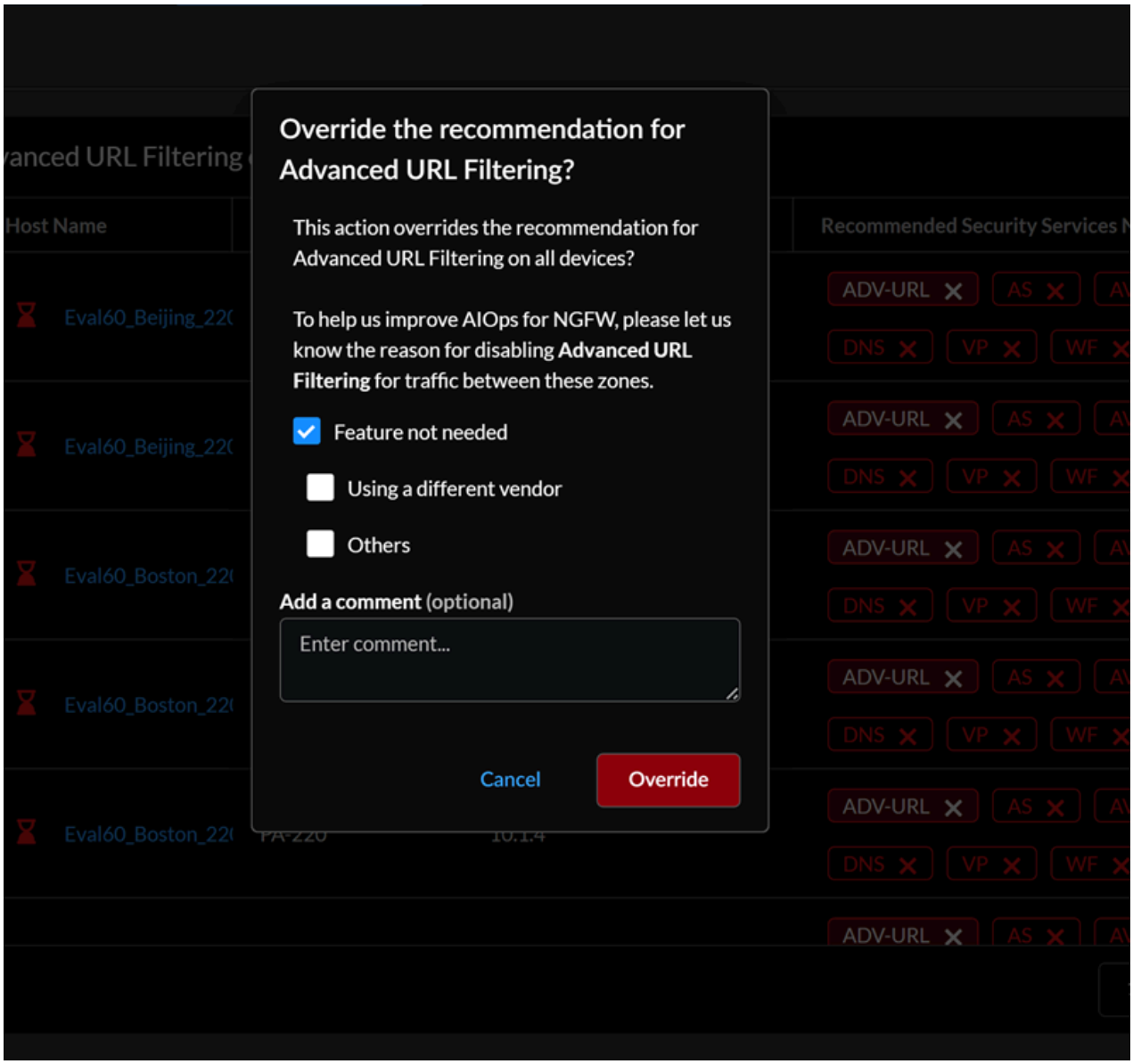
この例では、DNSセキュリティが構成されていない NGFW を表示するには、円グラフの **DNS**セキュリティ セクションの上にある値をクリックするか、円グラフの **DNS**セキュリティ セクションをクリックします。

推奨セキュリティ サービスをオーバーライドする

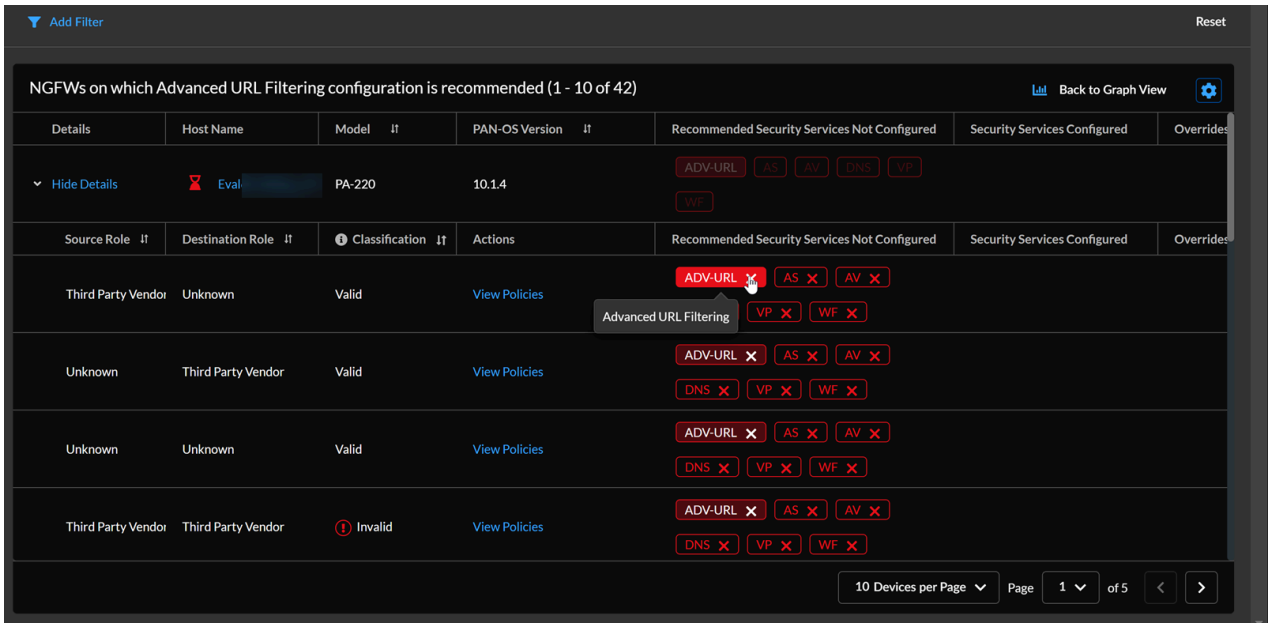
何らかの理由で推奨されるセキュリティサービスが必要ない場合は、それを上書きできます。**[CONFIGURE]**の下の値をクリックすると、表形式で詳細が表示され、推奨されるセキュリティ サービスをオーバーライドできます。



この例では、NGFW用のAIOpsは、デバイスの他のセキュリティ サービスとともに、高度なURLフィルタリング(ADV-URL)の構成を推奨しています。NGFWデバイスとその下のすべてのゾーンのADV-URLセキュリティ サービスをキャンセルできます。

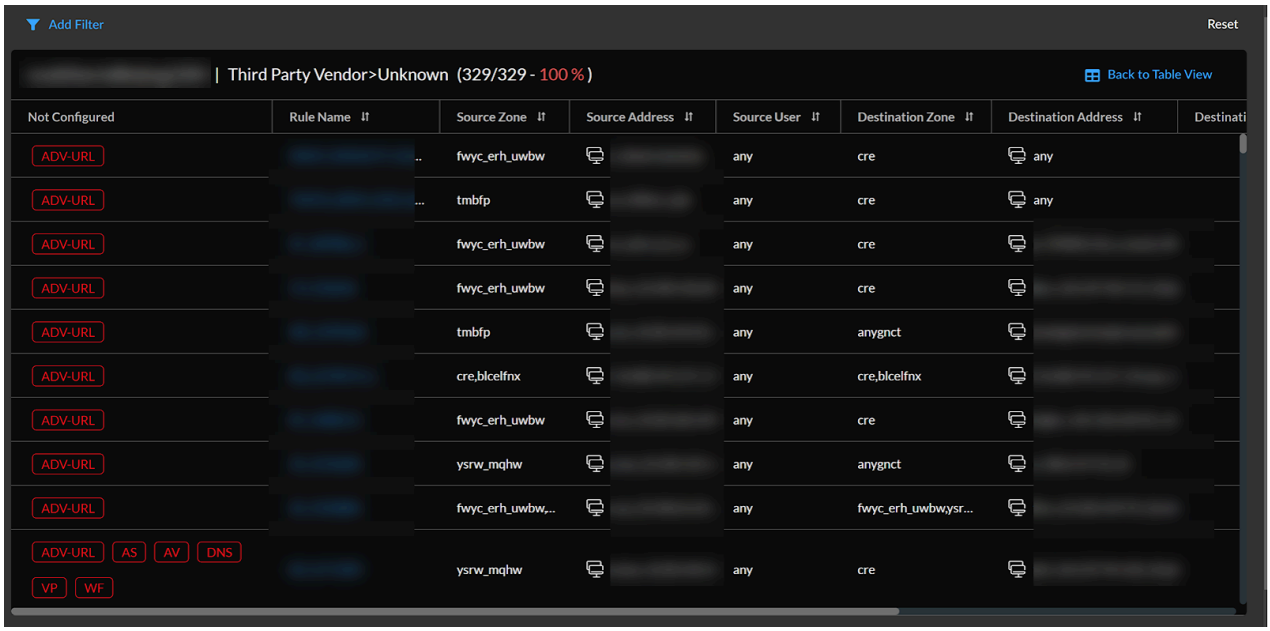


推奨されるセキュリティ サービスをゾーン レベルでオーバーライドすることもできます。NGFW の詳細を表示して 、ソースと宛先のロール、ポリシー、および推奨されるセキュリティ サービスを表示します。



この例では、ソース ロールの**ADV-URL**セキュリティ サービスを **Third Party Vendor**として、宛先ロールのADV-URLセキュリティ サービスを**Unknown**としてオーバーライドできます。また、**[Overrides (オーバーライド)]** 列のセキュリティ サービスをクリックして、オーバーライドされた推奨事項を復元することもできます。

ロールに関連付けられた ポリシーを表示 できます。ルールを選択すると、アプリを終了せずに詳細が表示されます。



セキュリティ サービスを表形式で表示するには **[Back to Table View (表ビューに戻る)]** をクリックします。

ダッシュボード:機能の導入状況

どこで使用できますか?	何が必要ですか?
• Software NGFW Creditsによって資金提供されたものを含むNGFW	☐ Strata Cloud Manager Essentials ☐ AIOps for NGFW Premium または Strata Cloud Manager Pro → Strata Cloud Managerで利用できる機能は、使用するライセンスによって異なります。

- 開始するには、**[Dashboards (ダッシュボード)]** > **[Feature Adoption (機能の導入状況)]** をクリックします。

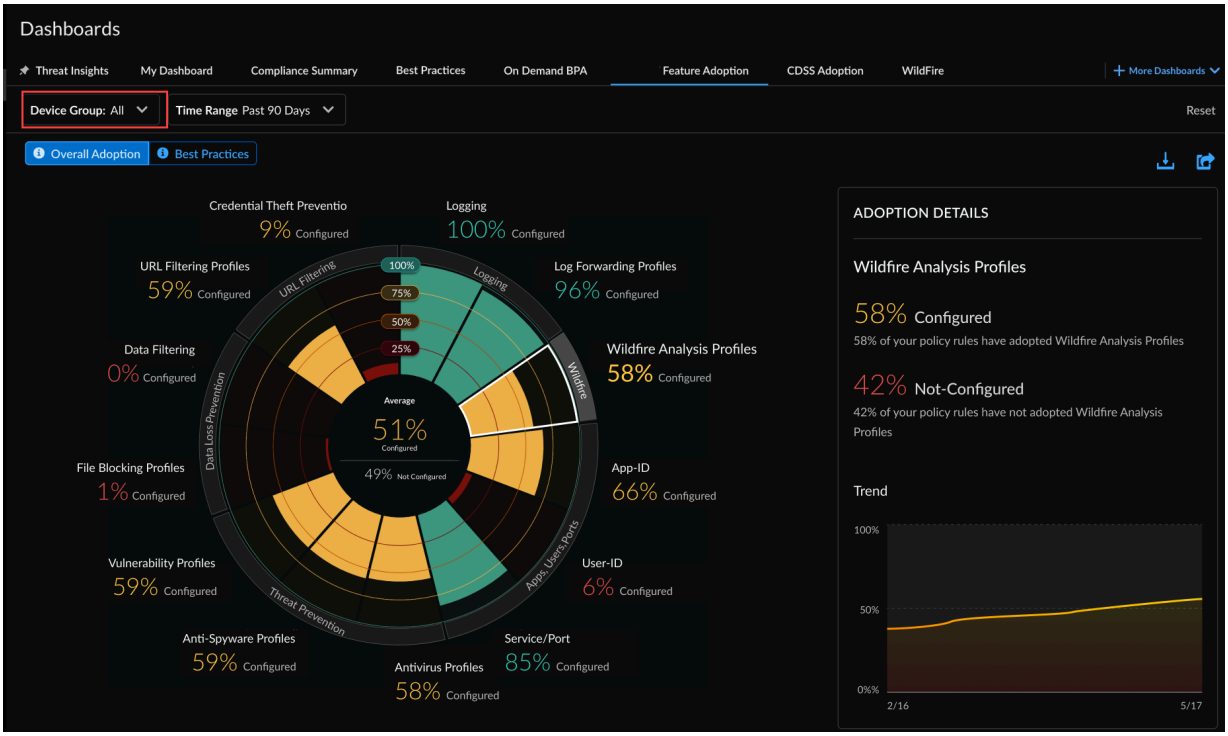
このダッシュボードには何が表示されますか?

ダッシュボードには、テナントにオンボードされ、テレメトリ データも送信しているすべてのファイアウォールの集計データが表示されます。

機能導入ダッシュボードには、デプロイメント環境で使用しているセキュリティ機能が表示されます。この機能を使用して、導入状況のギャップを特定できます。これにより、Palo Alto Networksのセキュリティ サブスクリプションとファイアウォール機能を最大限に活用することができます。

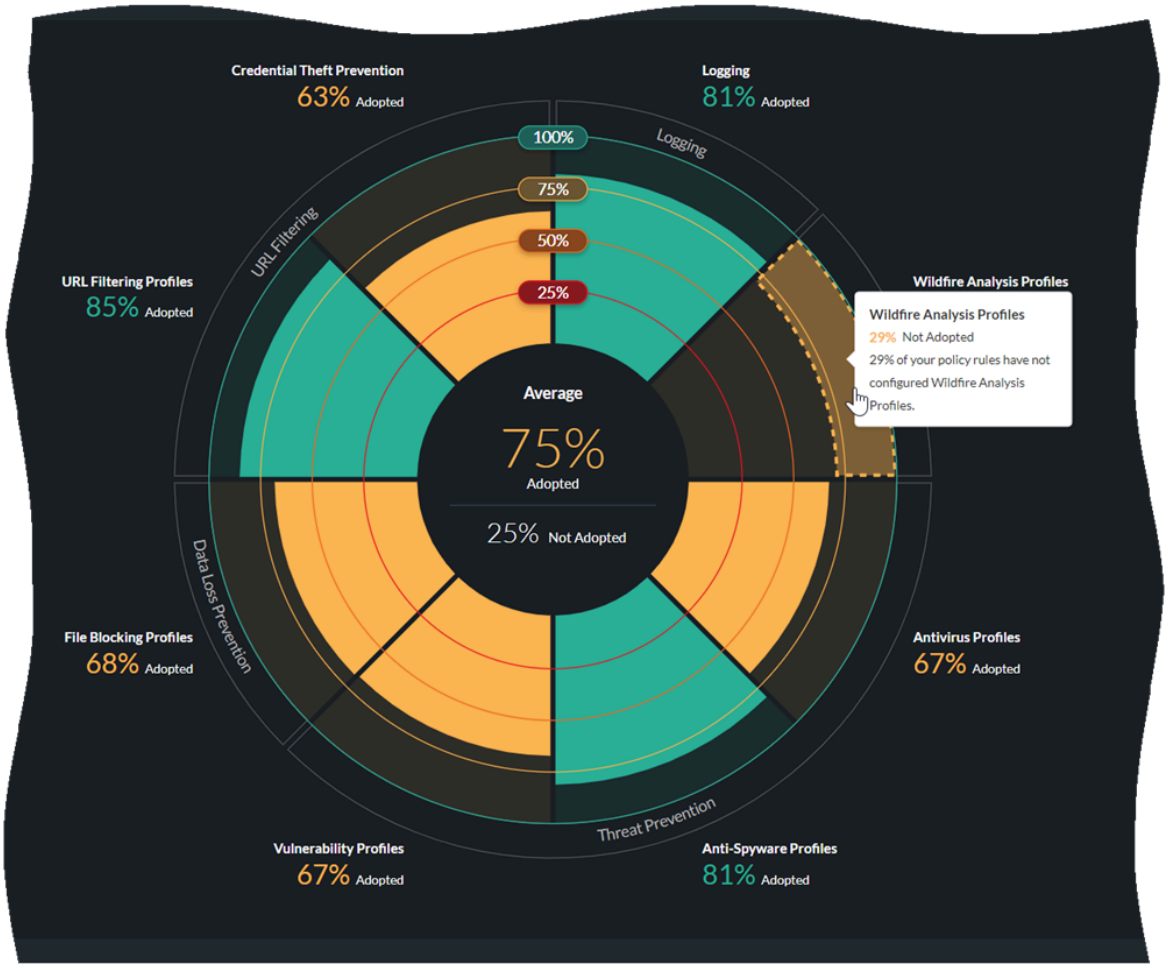
このダッシュボードの使い方

特定のファイアウォールセットの機能の導入に焦点を当てるには、Panorama管理対象デバイスを含むデバイス グループに基づいてチャートをフィルタリングできます。過去の導入状況の傾向チャートも見ることができます。

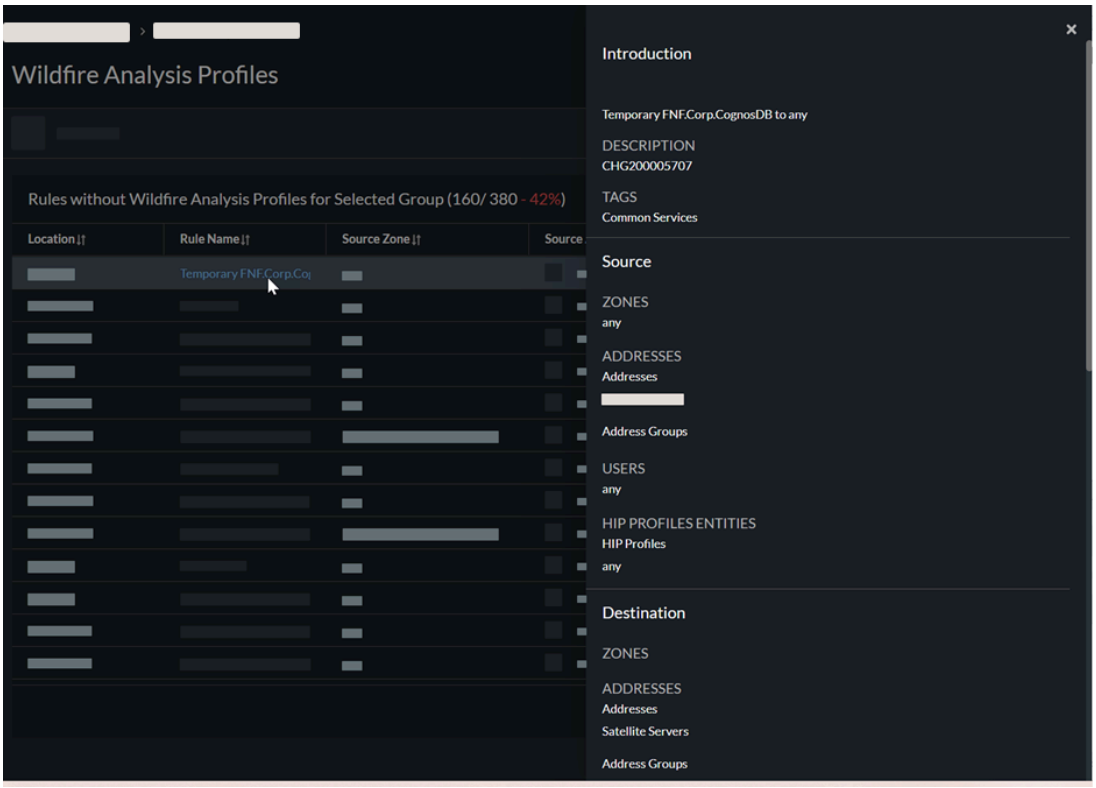


- *TSF*を使用してオンデマンド*BPA*レポートを生成すると、*TSF*の採用情報が*[Feature Adoption (*機能の導入状況*)]*ダッシュボードに反映されます。*(PAN-OS 9.1*以上*TSF)*
- 採用データを*.csv*形式でエクスポートし、*Microsoft Excel*などのサードパーティ製アプリケーションで使用できます

チャート上の機能のセクションを選択すると、その機能がないポリシー ルールが表示されます。



ルールを選択すると、アプリを終了せずに詳細が表示されます。

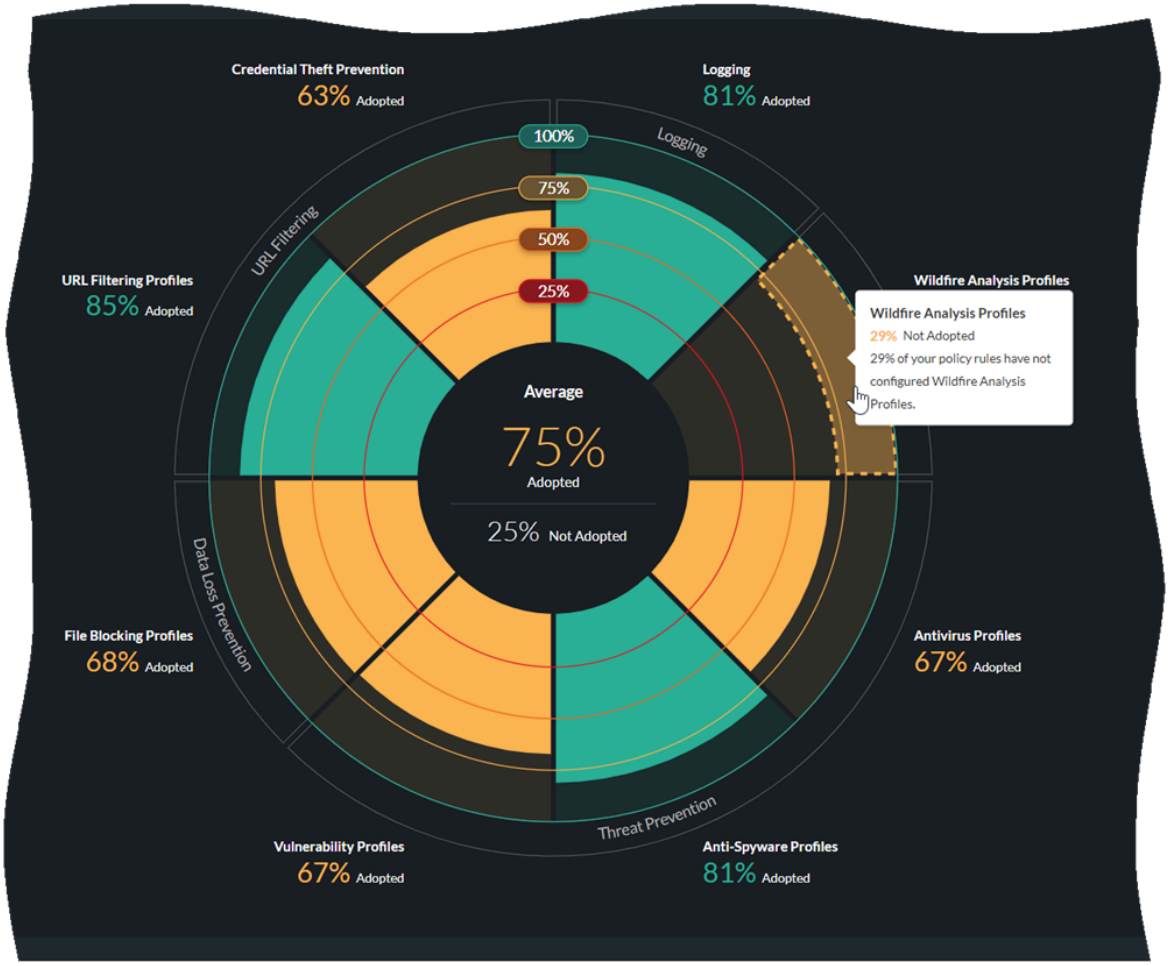


導入状況におけるギャップを特定する

このダッシュボードは、ユーザーのセキュリティポリシーがどの点で強いが、どこにセキュリティポリシー機能適用のギャップがあるか－したがって改善の努力をすべきかを示してくれます。トラフィックの可視性を最大化し攻撃に対する最大の保護を実現するには、セキュリティ機能適用の目標を設定し、ベストプラクティス ベースラインとして以下の推奨事項を適用します。ベースラインと対比して現在の体制を評価し、セキュリティ機能導入におけるギャップを認識します。

Adoption Summary（導入状況のサマリー）により、セキュリティ機能の適用を改善できるデバイス、ゾーンおよび領域を特定することが容易になります。適用情報は、Device Group（デバイスグループ）、Serial Number & Vsys（シリアル番号とVSYS）、Zones（ゾーン）、Areas of Architecture（アーキテクチャのエリア）、Tags（タグ）、Rule Details（ルール詳細）、およびZone Mappings（ゾーンマッピング）別に確認できます。デバイスグループでフィルタリングして範囲を狭め、ギャップを特定します。

[Dashboard (ダッシュボード**)]** > **[Feature Adoption (**機能の導入状況**)]**で**[Overall Adoption (**導入状況全体**)]**を選択すると、以下の機能の採用率を確認できます。[ベストプラクティス]を選択すると、Palo Alto Networksのベストプラクティスに準拠したこれらの機能の導入率を確認できます。この情報をギャップ判定基準に使います。実際の適用率が推奨値に合致しない場合は、ギャップを埋めるよう計画します：



- WildFire分析、アンチウィルス、アンチスパイウェア、脆弱性防御およびファイルブロッキングのプロファイルを、100%を目標として、またはほぼ100%の適用率を狙って、トラフィックを許可するすべてのルールに適用します。プロファイルを許可ルールに適用しない場合は、適用しないことを業務上正当化できることを確認する必要があります。

  セキュリティプロファイルをすべての許可ルールについて設定することにより、ファイアウォールは、アプリケーションやサービス/ポートに関係なく、復号化されたトラフィックについて脅威があるかないかを検査することができます。設定を更新した後は、テレメトリ以外のデバイスのBPAを実行して、進捗状況を測定し、セキュリティ プロファイルがアタッチされていない新しいルールを見つけます。

  *WildFire*プロファイルは、*WildFire*ライセンスがなくてもルールに適用できます。*PE*ファイルについては適用が限定されますが、それでも、未知の悪意あるファイルの可視性は保証されます。

- アンチスパイウェアプロファイルでは、危殆化された内部ホストが悪意あるまたはカスタムドメインにDNSクエリを送信するのを防止し、危殆化された可能性のあるホストを特定し追跡し、DNSチェックでのギャップを防止するために、DNS Sinkhole（シンクホール）をすべてのルールに適用します。DNS Sinkholeを有効化することにより、ネットワークの利用に支障を与えることなくネットワークが保護されますので、これは直ちに有効化でき、また有効化すべきです。

- URL フィルタリングおよび認証情報盗難（フィッシング）保護をすべてのインターネット向けトラフィックに適用します。

Adoption Summary（導入状況のサマリー）のApplication & User Control （アプリケーション & ユーザー制御）で、以下の機能の導入率をチェックします。推奨事項をギャップ判定基準に使います。実際の適用率が推奨値に合致しない場合は、ギャップを埋めるよう計画します：

- App-IDを、できるだけ100%に近いルールに適用します。User-IDを、ユーザープレゼンスをもつ送信元ゾーンおよびアドレス範囲を有するすべてのルールに適用します（ユーザーソースのないゾーンもあります。例えば、データセンター・ゾーンは、サーバーでありますが、ユーザーではありません）。App-IDおよびUser-IDを活用して、適切なユーザーが認可（そして許容）されたアプリケーションへのアクセスを許可されるよう、ポリシーを生成します。悪意のあるまたは望まないアプリケーションを指名してブロックします。
- サービス/ポート適用率目標を100%またはほぼ100%に設定します。業務上それなりの理由がない限り、非標準ポートにアプリケーションを許可してはなりません。

Adoption Summary（導入状況のサマリー）のLogging （ロギング）で、以下の機能の導入率をチェックします。推奨事項をギャップ判定基準に使います。実際の適用率が推奨値に合致しない場合は、ギャップを埋めるよう計画します：

- ロギングおよびログ転送の適用率目標を100%またはほぼ100%に設定します。
- すべてのゾーンにつき、ゾーン プロテクション プロファイルを設定します。

サマリー：

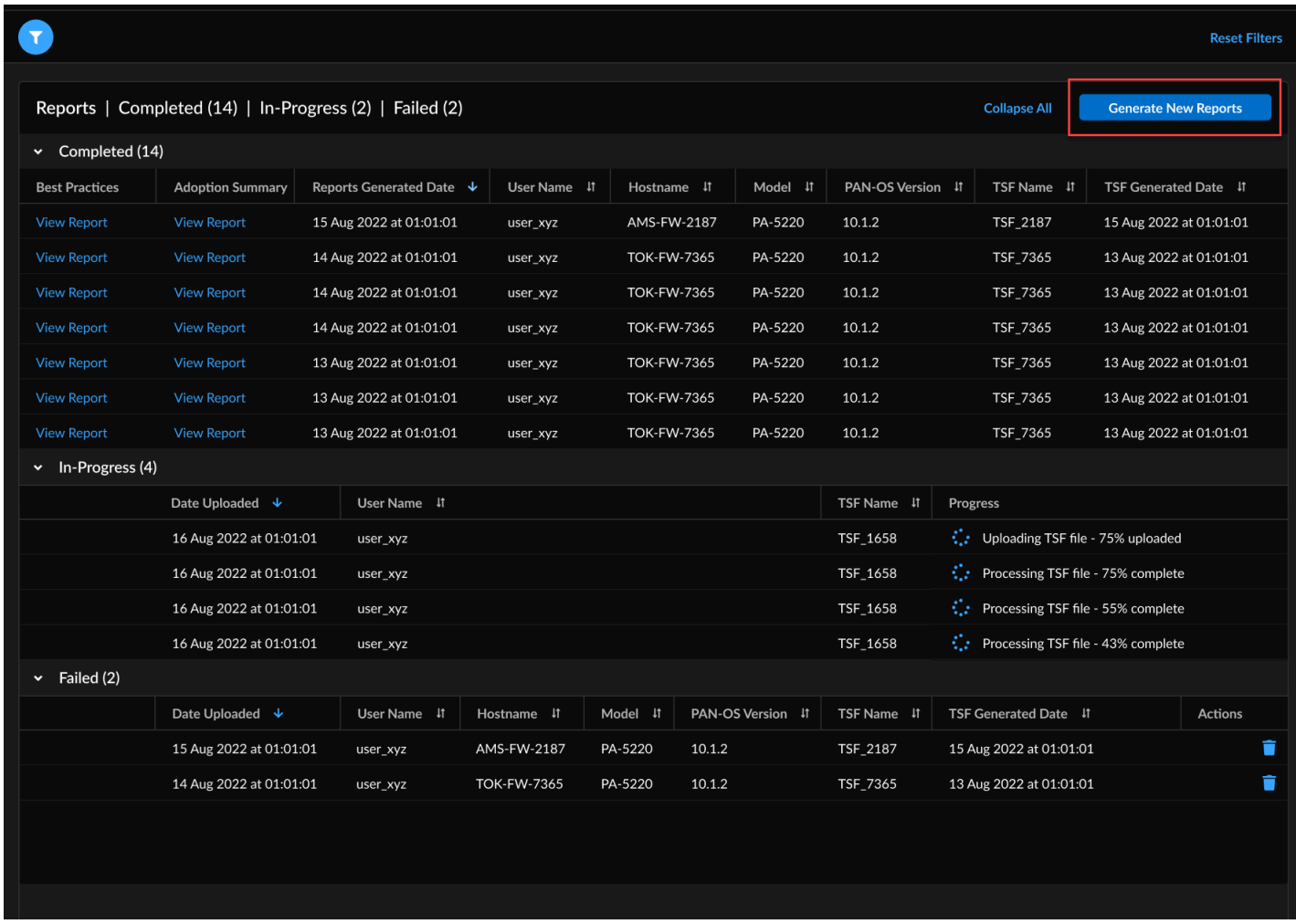
機能	適用目標
WildFire	セキュリティポリシーの適用率はできるだけ100%に
Antivirus（アンチウイルス）	セキュリティポリシーの適用率はできるだけ100%に
アンチスパイウェア	セキュリティポリシーの適用率はできるだけ100%に
脆弱性が	セキュリティポリシーの適用率はできるだけ100%に
ファイル ブロッキング	セキュリティポリシーの適用率はできるだけ100%に
URL フィルタリングおよび認証情報盗難	すべてのインターネット向けトラフィック
App-ID	セキュリティポリシーの適用率はできるだけ100%に
User-ID	ユーザープレゼンスをもつ送信元ゾーンおよびアドレス範囲を有するすべてのルール
サービス/ポート	セキュリティポリシーの適用率はできるだけ100%に
ﾛｷﾞﾝｸﾞ	セキュリティポリシーの適用率はできるだけ100%に

機能	適用目標
ログ転送	セキュリティポリシーの適用率はできるだけ100%に
ゾーン プロテクション	すべてのゾーン

ダッシュボード:オンデマンド BPA

どこで使用できますか?	何が必要ですか?
• Software NGFW Creditsによって資金提供されたものを含むNGFW	❑ Strata Cloud Manager Essentials ❑ AIOps for NGFW Premium または Strata Cloud Manager Pro → Strata Cloud Managerで利用できる機能は、使用するライセンスによって異なります。

- **[Dashboards (ダッシュボード)]** > **[On Demand BPA (オンデマンド BPA)]** にアクセスして開始します。



このダッシュボードには何が表示されますか？

ダッシュボードには、アップロードされたデバイスの*TSF*ファイルに基づいて、ベストプラクティス評価（*BPA*）レポートが表示されます。

ベストプラクティス評価（BPA）と機能導入の概要をStrata Cloud Managerから直接実行できるようになりました。テクニカルサポートファイル（TSF）をアップロードするだけです。テレメトリデータを送信していないデバイスや、AIOps for NGFWにオンボードされていないデバイスのオンデマンドBPAレポートを生成できます。

ダッシュボードのデータはどのように利用できますか？

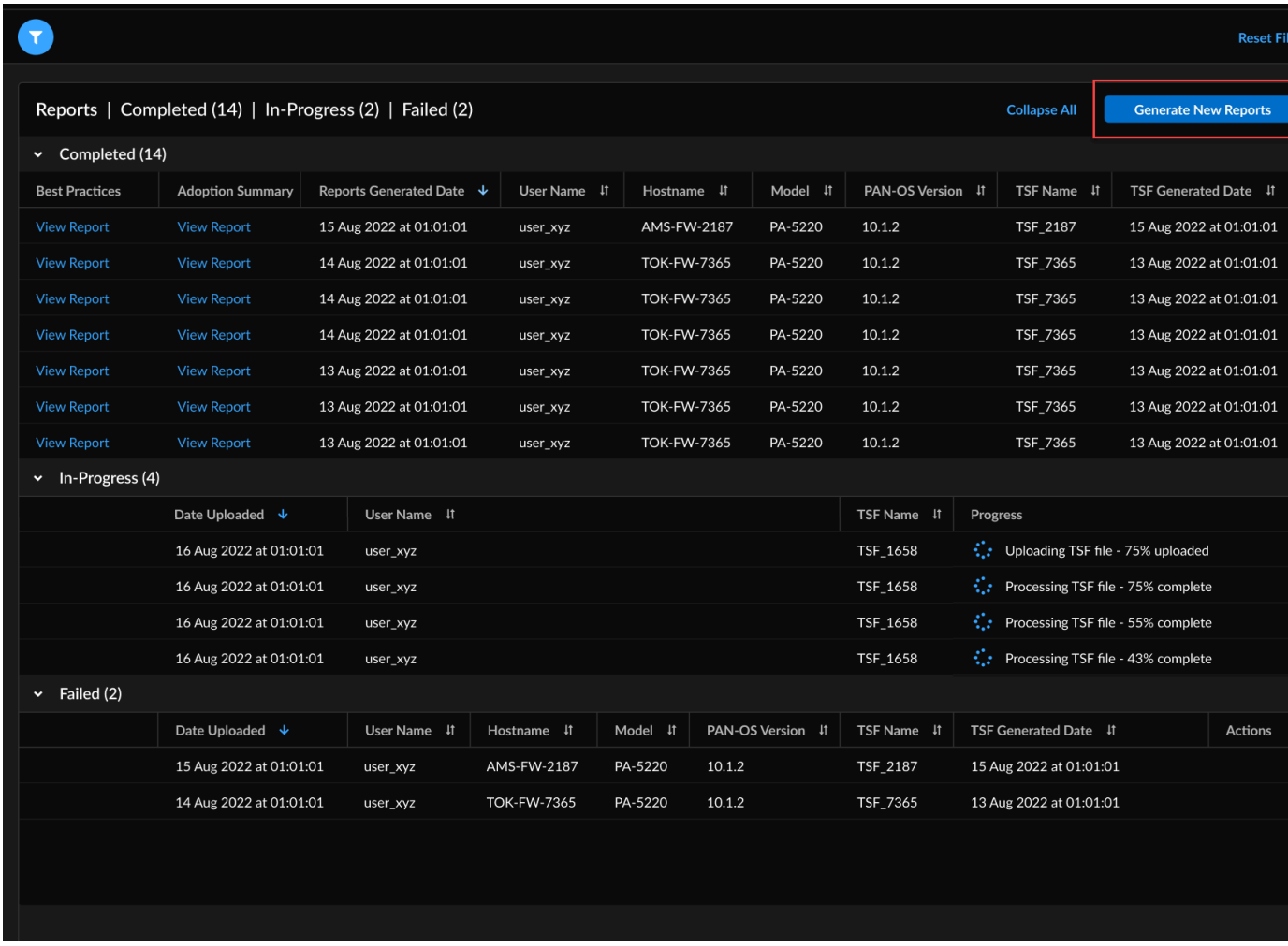
BPAは、Palo Alto Networksのベストプラクティスに照らしてセキュリティ態勢を評価し、デバイスの改善に優先順位を付けます。セキュリティ ベストプラクティスは、既知および未知の脅威を予防し、攻撃可能範囲を縮小し、トラフィックの可視性を提供するために、自社のネットワーク上にどのようなアプリケーション、ユーザーおよびコンテンツが存在するかを知り、それらを管理することができます。さらにベストプラクティスには、インターネットセキュリティセンターの重要なセキュリティ管理 (CSC) のチェックが含まれます。セキュリティ体制を強化し、改善を実施するためのベストプラクティスガイダンスをご覧ください。

オンデマンドBPAレポートの生成

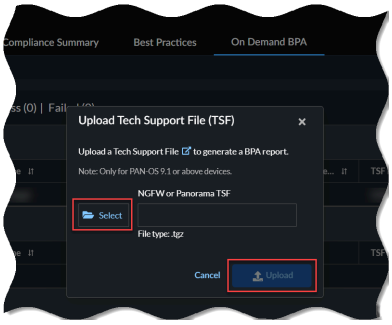
オンデマンドでBPAレポートを生成する手順は、次のとおりです。

STEP 1 | **[Dashboards (ダッシュボード)]** > **[On Demand BPA (オンデマンド BPA)]**に移動します。

STEP 2 | 新しい**BPA**レポートを生成。



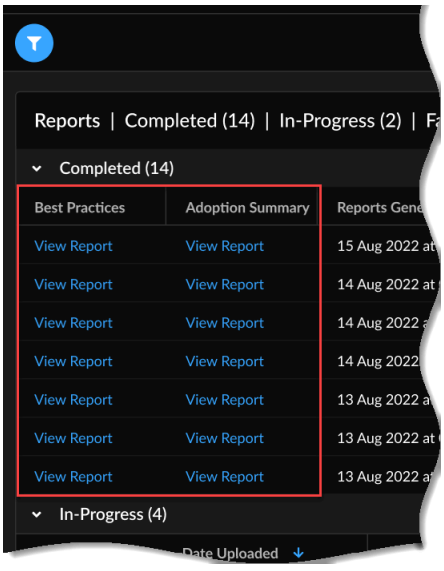
STEP 3 | **TSF**を選択し、**TSF**ファイルをアップロードします。



アップロード時間は、.tgzファイルのサイズとインターネット速度によって異なります。ファイルサイズが大きい場合、ファイルのアップロードに数分かかることがあります。**[In-Progress (**実行中**)]**を展開し、TSFファイルのステータスを表示します。

- オンデマンド*BPA*は、*.tgz*ファイル形式のテクニカルサポートファイル（*TSF*）のみをサポートしています。
- オンデマンド*BPA*は、*PAN-OS*バージョン*9.1*以上を搭載したデバイスからの*TSF*をサポートし、レポート生成を実現します。
- *Palo Alto Networks*のデータキャプチャ、処理、テレメトリストレージについては、[Trust Center (トラストセンター)]の[AIOps for NGFW Privacy (NGFWプライバシー用のAIOps)]を参照してください。

STEP 4 | 結果を見るには**[Completed (**完了**)]**の下にある**[View Report (**レポートを表示**)]**をしてください。



ダッシュボード:佐瀬健康

どこで使用できますか?	何が必要ですか?
• Prisma Access (Managed by Panorama or Strata Cloud Manager)	• 以下のいずれかです。 ❑ Prisma AccessとADEMの可観測性 ❑ Strata Cloud Manager Pro • ダッシュボードを表示する権限を持つロール → Strata Cloud Managerで利用できる機能は、使用するライセンスによって異なります。

このダッシュボードには何が表示されますか？

このダッシュボードには、現在Prisma Accessに接続されているモバイルユーザー、リモートサイト、およびアプリケーション（AI-Powered ADEMライセンスを購入している場合）の全体的な状態が表示されます。丸内の数字は、現在、そのサイトが表示されるPrisma Access Locationから接続しているユーザー数またはサイトの数を表します。ドットは、単一のユーザーまたはサイトを表します。地図上で背景が青色になっている箇所は、その地域に表示されている数字が予測または予測であることを示しています。

このダッシュボードに表示されているデータを、次のフィルタで1つ以上フィルタリングします

- 期間
- Prisma Access ロケーション
- 送信元の場所

ダッシュボードのデータをどう使うか？

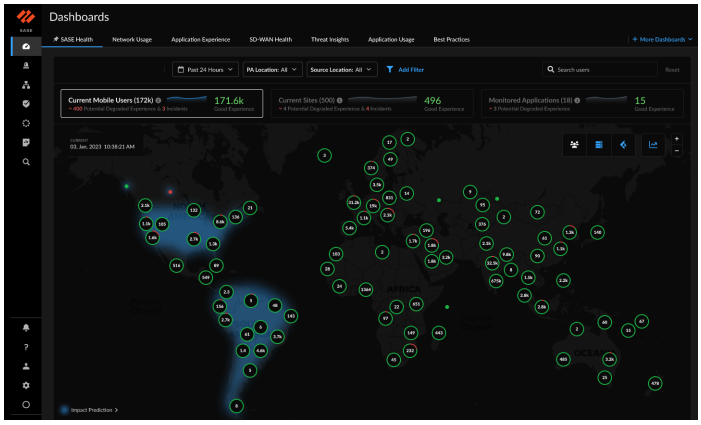
ダッシュボードを使用して、Prisma Accessに接続されているモバイルユーザーとリモートサイトの数を、マップ上の位置ごとに分類して、概要と全体的な正常性を確認できます。このダッシュボードでも、全体的な正常性を確認できます。

SASE正常性ダッシュボード:現在のモバイルユーザー - マップビュー

どこで使用できますか?	何が必要ですか?
• Prisma Access (Managed by Panorama or Strata Cloud Manager)	• 以下のいずれかです。 ❑ Prisma AccessとADEMの可観測性 ❑ Strata Cloud Manager Pro

どこで使用できますか?	何が必要ですか?
	• ダッシュボードを表示する権限を持つロール → Strata Cloud Managerで利用できる機能は、使用するライセンスによって異なります。

[SASE Health (SASE正常性)]ダッシュボードの**[Current Mobile Users (現在のモバイルユーザー)]**タブには、すべての場所のモバイルユーザーエクスペリエンスの内訳が表示されます。丸内の数字は、現在GlobalProtectを使用してPrisma Accessに接続しているモバイルユーザーの数に対応しています。ドットは単一のモバイルユーザーを表します。緑色の丸またはドットは、ユーザー エクスペリエンス スコアが良好であることを示します。同様に、赤色の場合はエクスペリエンス スコアが低下していることを示します。劣化したエクスペリエンス スコアは、FairスコアとPoorスコアを合わせたものになります。**[Current Mobile Users (現在のモバイルユーザー)]**の右側の折れ線グラフには、選択した**[Time Range (期間)]**におけるすべてのモバイルユーザーの平均エクスペリエンススコアの傾向が表示されます。



[Potential Degraded Experience (機能低下の可能性のあるユーザーエクスペリエンス)]または**[インシデント]**の横の数字（つまり、ユーザーエクスペリエンスに機能低下の可能性のあるユーザー数）をクリックすると、左側に開いたペインに劣化したエクスペリエンスの詳細が表示されます。

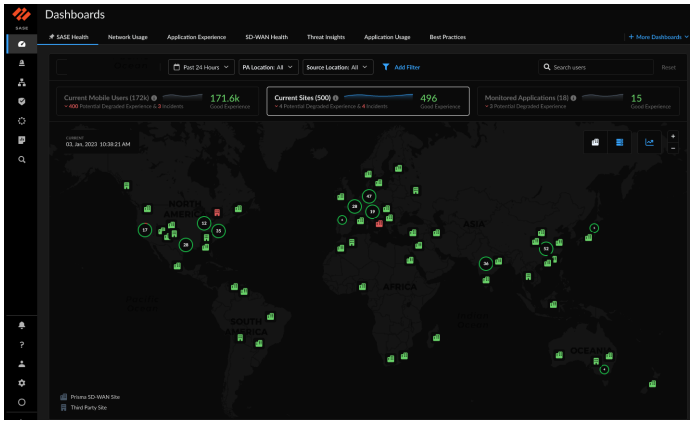
SASE正常性ダッシュボード:現在のサイト - マップビュー

どこで使用できますか?	何が必要ですか?

• Prisma Access (Managed by Panorama or Strata Cloud Manager)	• 以下のいずれかです。
	  ❑ Prisma AccessとADEMの可観測性
	  ❑ Strata Cloud Manager Pro
	• ダッシュボードを表示する権限を持つロール

どこで使用できますか?	何が必要ですか?
	→ Strata Cloud Managerで利用できる機能は、使用するライセンスによって異なります。

このダッシュボードには、世界中のPrisma Access Locationsに接続している設定済みサイトの数が表示されます。括弧内の数字は接続サイトの合計数、カード内の右の数字はGoodエクスペリエンス スコアがアップしているサイトの数です。何らかの理由で経験値が取得できないサイトは、接続サイト数の計算時に除外されません。青い折れ線グラフは、全サイトの平均エクスペリエンススコアの経時的推移を示しています。「Current Sites (現在のサイト)」の下には、すべてのサイトのインシデント数とともに、エクスペリエンススコアが「低下（Poor）」したサイトの数が表示されます。インシデントは、次のカテゴリの1つ以上に分類されます。インフラストラクチャ、ネットワークサービス、データセンター、およびサードパーティサイト（データセンターがダウン）。

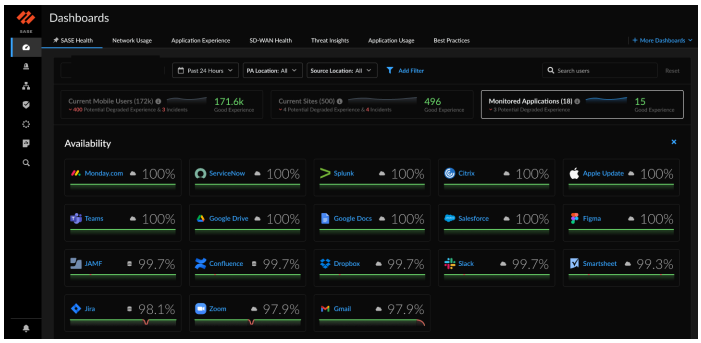


SASE正常性ダッシュボード:監視対象のアプリケーション

どこで使用できますか?	何が必要ですか?
• Prisma Access (Managed by Panorama or Strata Cloud Manager)	• 以下のいずれかです。 ❑ Prisma AccessとADEMの可観測性 ❑ Strata Cloud Manager Pro • ダッシュボードを表示する権限を持つロール → Strata Cloud Managerで利用できる機能は、使用するライセンスによって異なります。

SASE Health (SASE正常性)ダッシュボードの**[Monitored Applications (監視対象のアプリケーション)]**タブで、アプリケーションの可用性の指標を参照してください。このダッシュボードには、ADEMを通じて監視されているアプリケーションの数と、それらのアプリケーションのうち

スコアが低下しているアプリケーションの数が表示されます。この数は、モバイルユーザーとリモートサイトの両方のアプリケーションエクスペリエンスを考慮しています。アプリケーションのエクスペリエンススコアが「Poor」または「Fair」のアプリケーションは、パフォーマンスが低下しているエクスペリエンスと見なされます。また、フィルタを使用して選択した時間帯のアプリケーションの可用性も確認できます。



アプリケーション名の右側の数字は、［**Time Range (時間範囲)**]内のアプリケーションが使用可能であった時間の割合を示します。

監視:ログ - Strata Cloud Manager

どこで使用できますか?	何が必要ですか?
• Prisma Access (Managed by Panorama or Strata Cloud Manager) • Software NGFW Creditsによって資金提供されたものを含むNGFW • Prisma SD-WAN	これらの各ライセンスには、Strata Cloud Managerへのアクセスが含まれています。 ❑ Prisma Access ❑ AIOps for NGFW Premium license (use the Strata Cloud Manager app) ❑ Strata Cloud Manager Essentials ❑ Strata Cloud Manager Pro ❑ Prisma SD-WAN その他のライセンスと可視性に必要な前提条件は次のとおりです。 ❑ ADEM Observability (ADEMの観測可能性) ❑ Autonomous DEM for Remote Networks (リモートネットワーク用自律型DEM) ❑ AI-Powered ADEM (AI搭載ADEM) ❑ WAN Clarity Reporting (WANクラリティレポート) ❑ ダッシュボードを表示する権限を持つロール → Strata Cloud Managerで利用できる機能は、使用するライセンスによって異なります。

ネットワークトラフィック全体、およびStrata Cloud Managerで管理している製品やサブスクリプションを包括的に可視化できます。Prisma Accessでは、リモートネットワーク、アプリケーション、NGFWデバイス、モバイルユーザーの正常性や接続状態を保護することができます。Strata Cloud Managerは、一般的なネットワークサービスのパフォーマンス、サブスクリプションライセンスの利用詳細、接続の問題の分析に使用するツールを管理する機能も提供しています。Prisma SD-WANユーザーは、Prisma SD-WANアプリケーション、IONデバイス、データセンターなどの正常性や接続状況も、すべて1か所で監視できます。

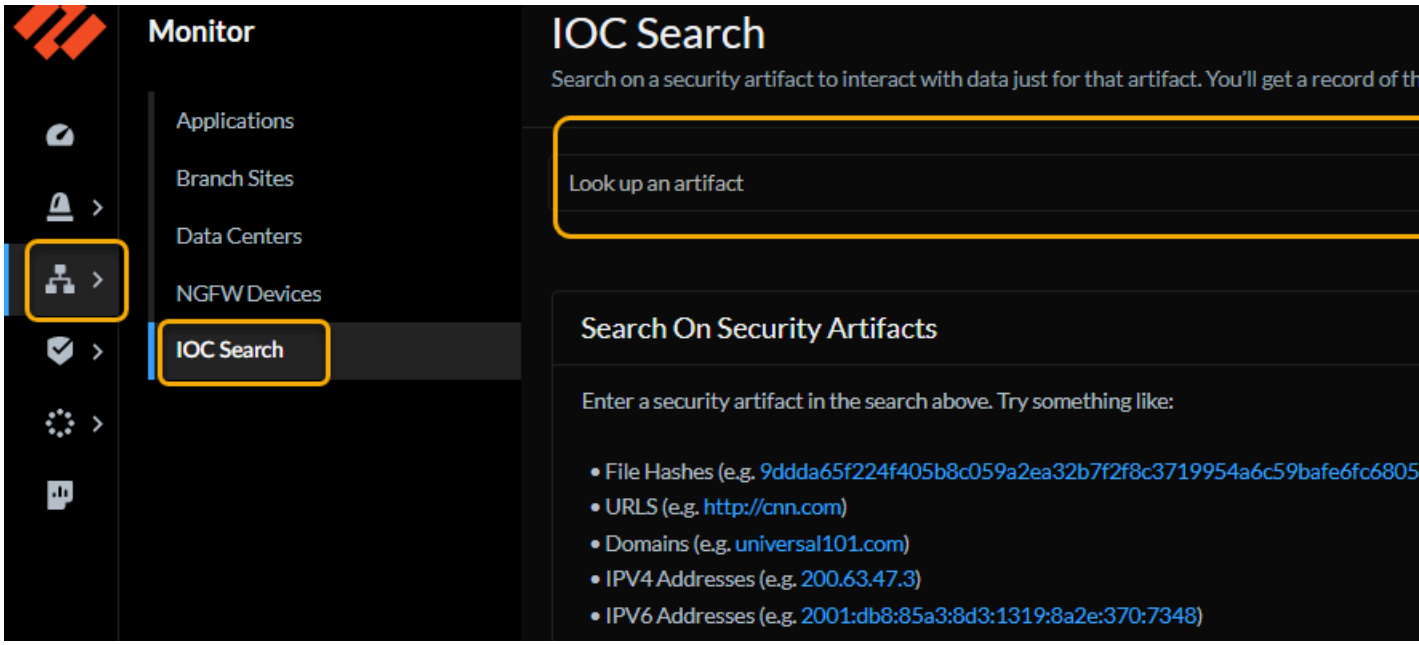
監視:IOC検索

どこで使用できますか?	何が必要ですか?
• Prisma Access (Managed by Panorama or Strata Cloud Manager) • Software NGFW Creditsによって資金提供されたものを含むNGFW • Prisma SD-WAN	これらの各ライセンスには、Strata Cloud Managerへのアクセスが含まれています。 ❑ Prisma Access ❑ AIOps for NGFW Premium license (use the Strata Cloud Manager app) ❑ Strata Cloud Manager Essentials ❑ Strata Cloud Manager Pro ❑ Prisma SD-WAN その他のライセンスと可視性に必要な前提条件は次のとおりです。 ❑ ADEM Observability (ADEMの観測可能性) ❑ Autonomous DEM for Remote Networks (リモートネットワーク用自律型DEM) ❑ AI-Powered ADEM (AI搭載ADEM) ❑ WAN Clarity Reporting (WANクラリティレポート) ❑ ダッシュボードを表示する権限を持つロール → Strata Cloud Managerで利用できる機能は、使用するライセンスによって異なります。

セキュリティ アーティファクトを検索して、そのアーティファクトに関するデータのみを操作することができます。検索結果には次のものがあります。

- アーティファクトの履歴とネットワーク内でのアクティビティ。ネットワーク内でアーティファクトがどの程度普及しているかを評価し、同業他社と比較します。
- Palo Alto Networksは、Palo Alto Networksが処理および分析するすべてのトラフィックの分析に基づいて、アーティファクトに関する脅威インテリジェンスを提供します。
- アーティファクトに関するサードパーティの分析結果を統合。

[Monitor (監視)] > [IOC Search (IOCサーチ)]をクリックして開始します。

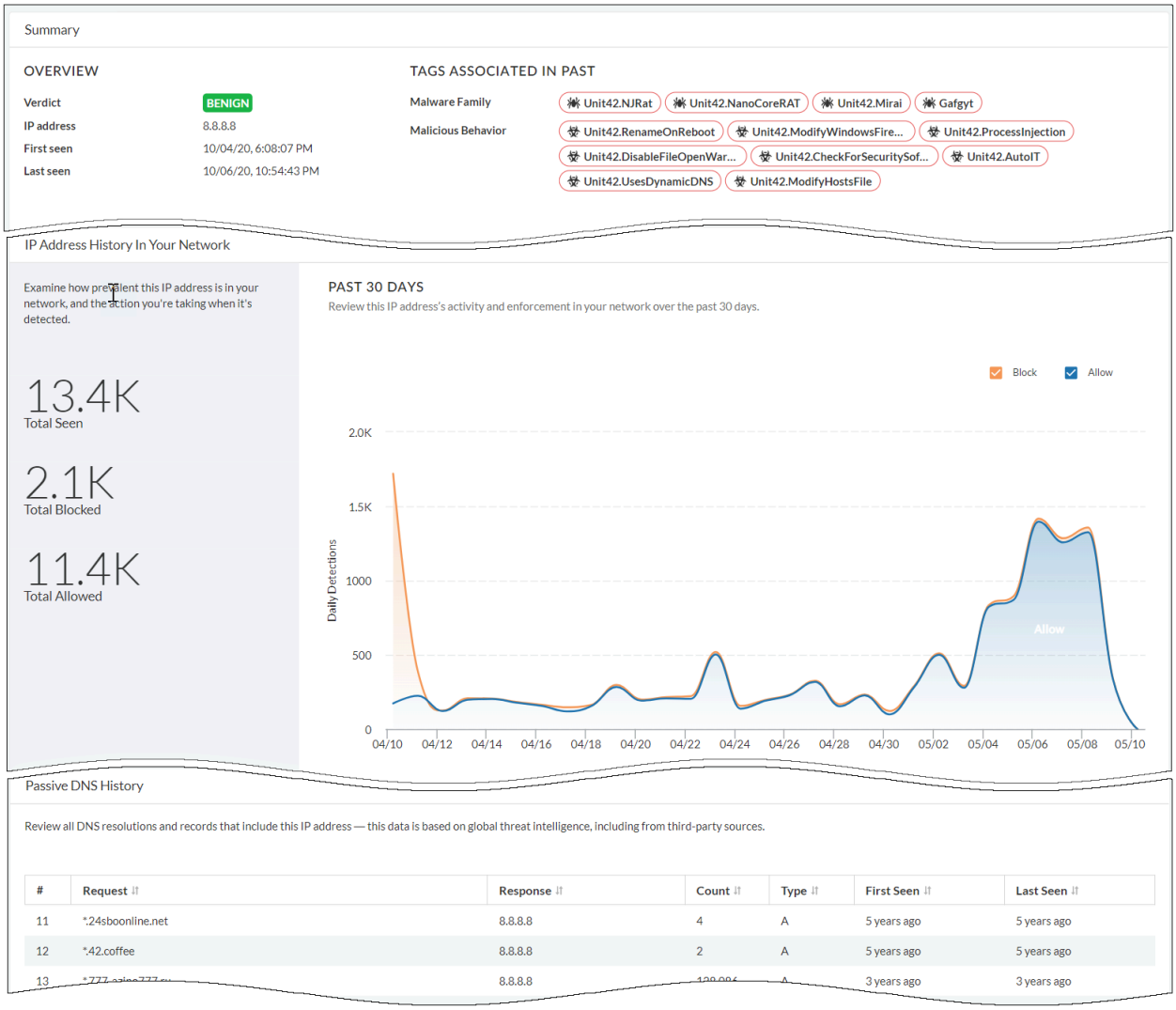


まず、ファイルハッシュ、**URL**、ドメイン、**IP**アドレス（IPv4またはIPv6）のいずれかの種類のアーティファクトを検索します。

IP アドレス

IPアドレスを探して、ネットワーク内のIPアドレスアクティビティに関連する脅威情報を分析できます。検索結果には次のデータが表示されます。

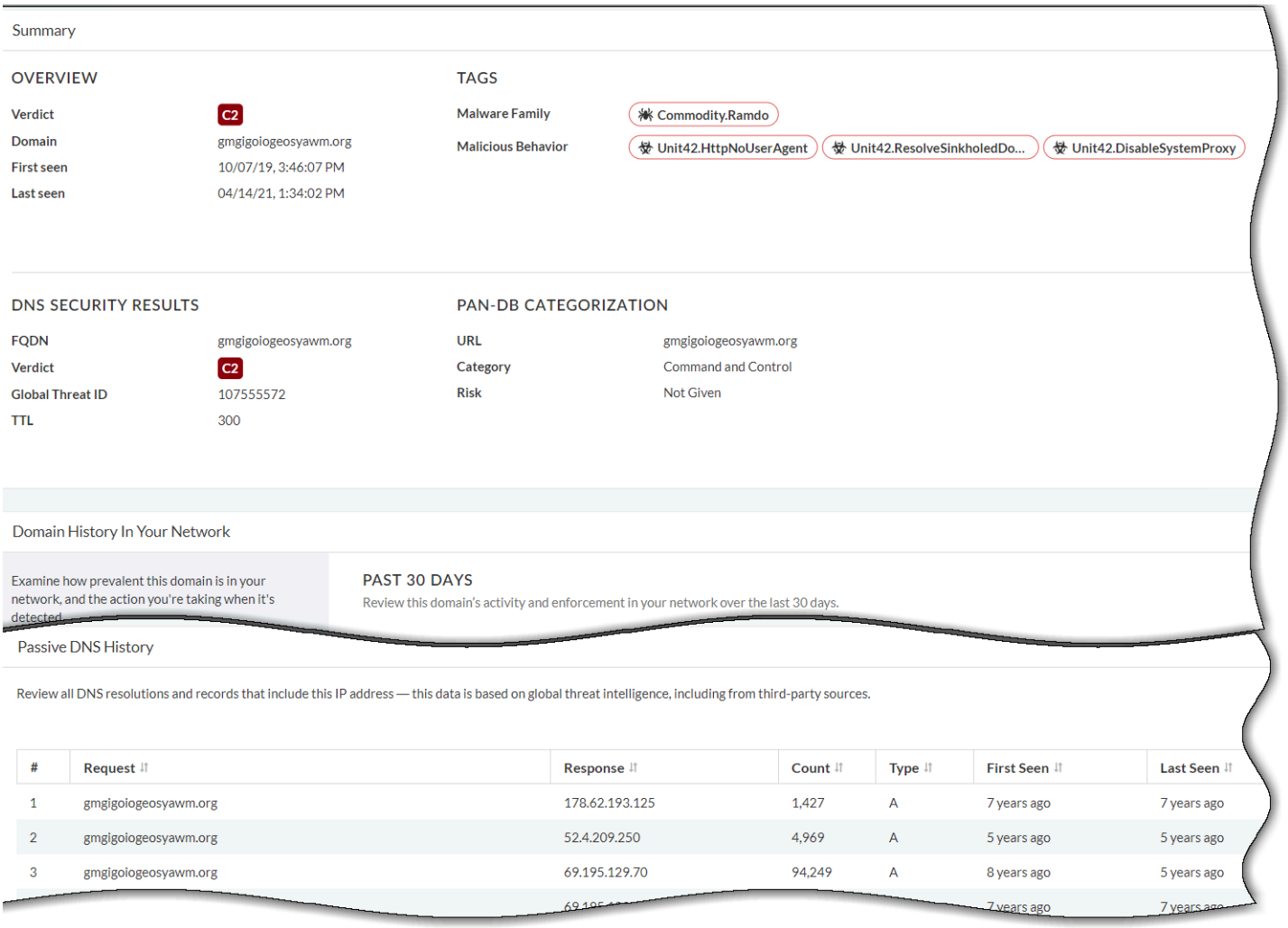
- 過去30日間にネットワーク内でIPアドレスが検出された合計回数。
- IPアドレスに対して実行されたアクション（許可またはブロック）をグラフィカルに表示します。
- Palo Alto Networksの脅威インテリジェンスとサードパーティの送信元に基づくIPアドレスを含むDNSリクエストのリスト。



ドメイン

ネットワーク内のドメインに関連付けられているアクティビティの概要を表示します。検索結果には次のものがあります。

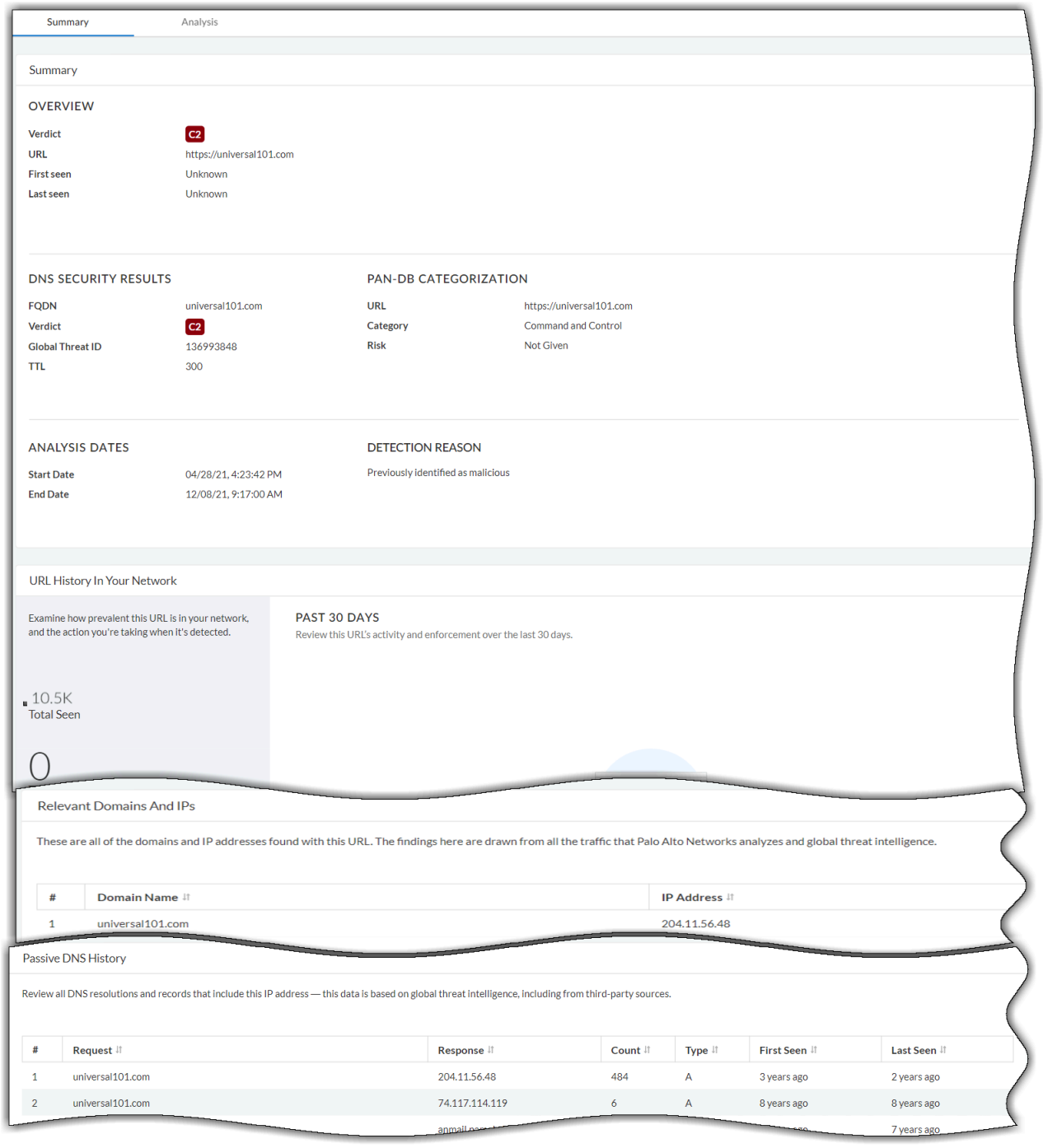
- WildFireのサンプル分析に基づくネットワーク内のドメインの分類。
- 過去30日間にドメインに関連付けられたアクティビティの合計数。
- 各アクティビティに適用された強制をグラフ形式で表示します。
- WildFireの分析から得られた情報で、ドメインに対する評決の割り当てに使用されたデータをサポートします。
- このドメインのインスタンスを含むすべてのWildFire提出物から収集されたDNSアクティビティ。



URL

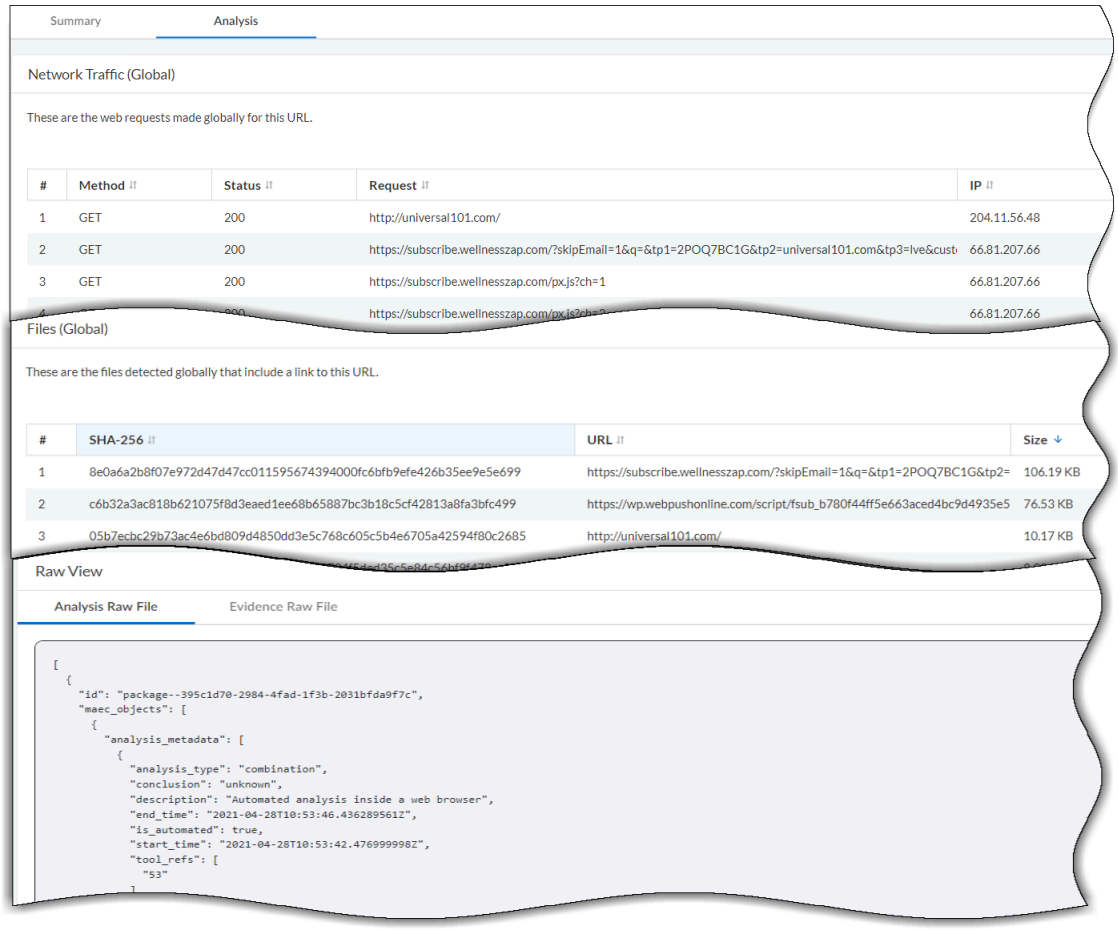
Palo Alto Networksが分析するすべてのトラフィックにおけるURLのアクティビティについて知ることができます。検索結果には次のものがあります。

Summary (要約) - URLのネットワーク内でのアクティビティの要約を確認します。データには次のものが含まれます。URLとPAN-DB分類に関するDNSセキュリティ調査結果。



Screenshot (スクリーン)ショット - URLアーティファクトで検索したときにウェブサイトのスナップショットを表示します。

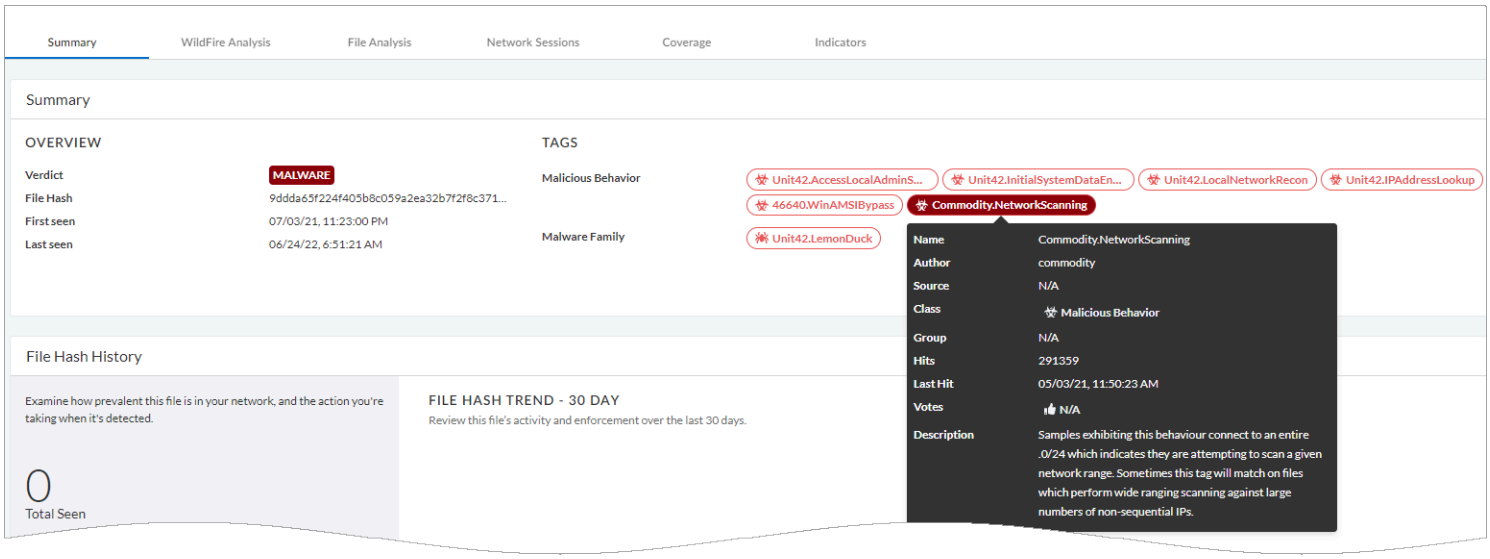
Analysis (分析) - このURLに対してグローバルに行われた要求、およびこのURLで検出されたファイルを含むファイル分析データを参照してください。ファイルハッシュ値またはファイルビューを使用して詳細を知ることができます。



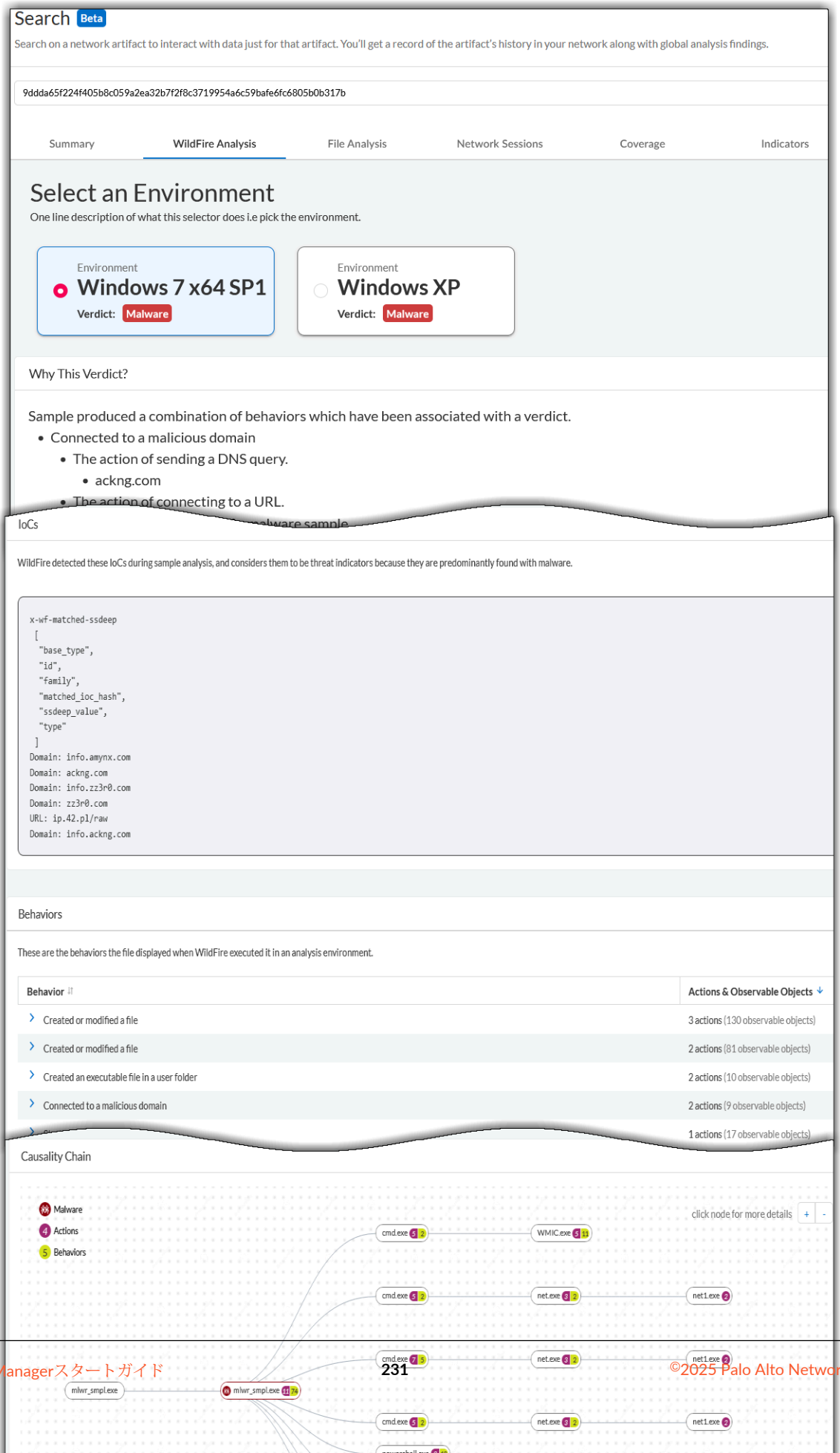
ファイルハッシュ

ファイルハッシュ検索は、ファイルのアクティビティ、ファイルプロパティの分析、WildFireサンプル分析の詳細を要約します。検索結果をドリルダウンすると、次のデータを確認できます。

Summary (概要) - ファイルハッシュ評決とネットワーク内でのファイルのアクティビティの履歴を表示します。タグ名をクリックするとタグの詳細が表示されます。タグは、ファイルが脅威ファミリー、キャンペーン、またはアクターの一部であるかどうかを理解するのに役立ちます。



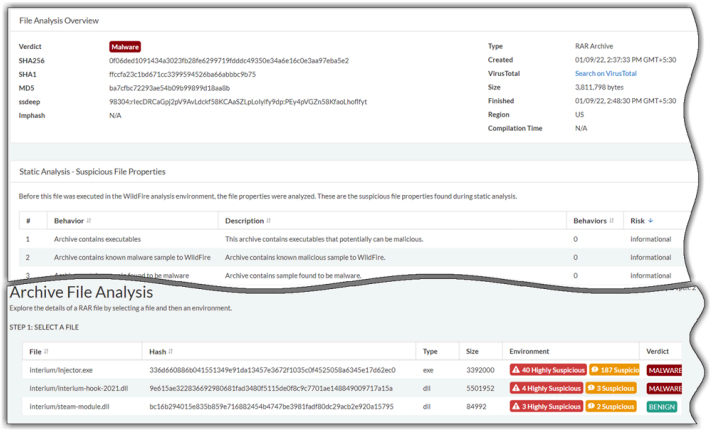
WildFire Analysis (WildFire分析) - WildFire分析中にサンプル（ファイル）がどのように動作したかを評価します。サンプル評決、サンプル分析中に検出された脅威指標、分析環境でサンプルを処理中の動作に関する情報を表示できます。WildFireのサンプル分析中にキャプチャされたさまざまなプロセスマイルストーンのスクリーンショットを表示することもできます。



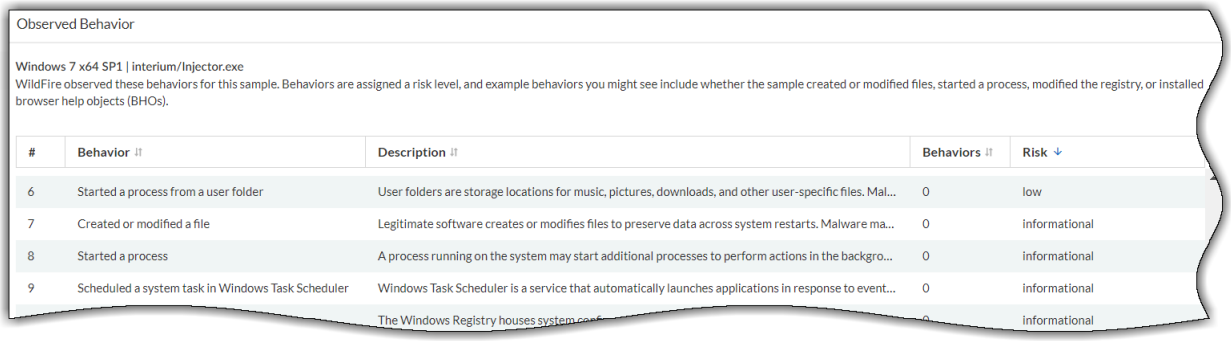
File Analysis (ファイル分析) - WildFire分析環境でサンプル（ファイル）の実行前と実行後の分析を比較します。

Overview (概要) - サンプルの評決はここで確認してください。評決の分類が間違っている場合は、評決の変更をリクエストします。Palo Alto Networksの脅威チームはサンプルについてさらに調査し、誤りが見つかった場合は判決を更新します。

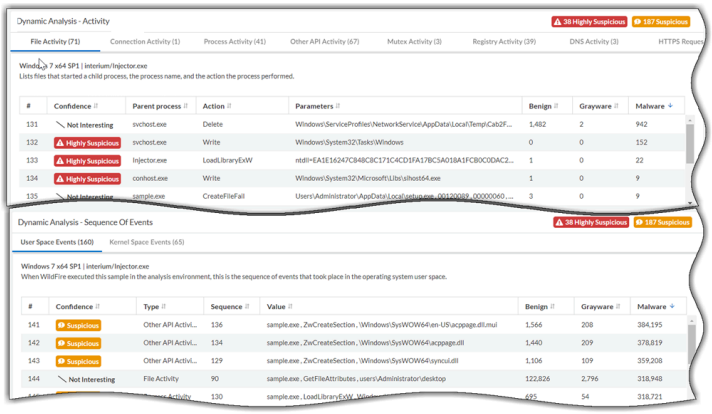
Static Analysis (静的解析) - 静的解析は、WildFire解析環境でファイルが実行される前に、特定のファイルの内容を調べます。検索では、スタティック分析で検出された疑わしいファイルプロパティも表示されます。検索結果はファイルの種類によって異なります。このスクリーンショットは、アーカイブファイルの静的解析を示しています。



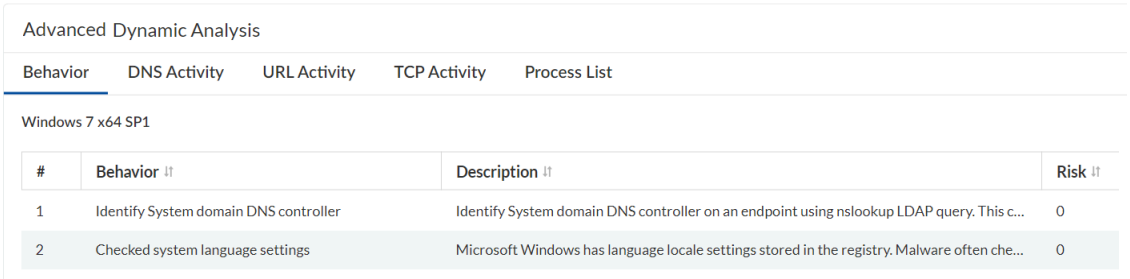
Observed Behavior (観察行動) - 特定の環境におけるサンプルのWildFire行動分析を確認します。



Dynamic Analysis (動的解析) - ファイルを詳細に検査し、侵害されたネットワークの追加情報やインジケータを抽出します。関係するプロセスアクティビティ、およびファイル実行中にシステムで発生した一連のイベントを確認できます。

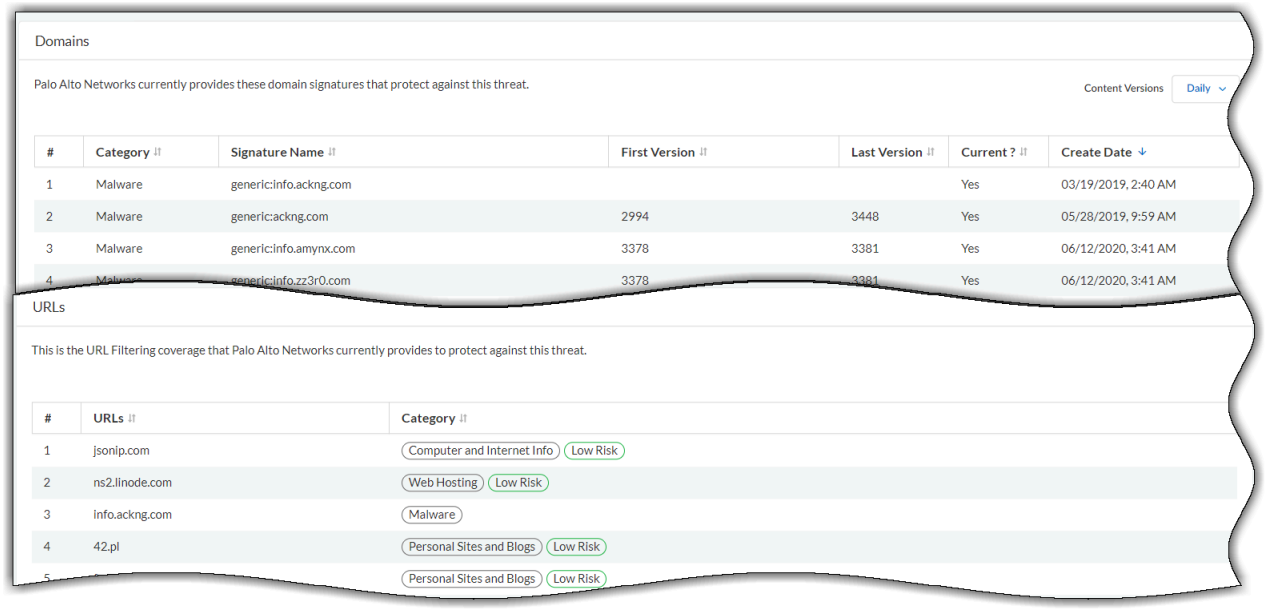


Advanced Dynamic Analysis (高度な動的解析) - 高度に回避されたマルウェアの脅威を検出して防止するクラウドベースのエンジンである、高度なWildFire技術（インテリジェントな実行時メモリ解析、ハイパーバイザーの動的解析、依存関係エミュレーションなど）で解析されたサンプルの分析結果を表示します。観察された動作を表示し、この情報を実行後の分析に使用できます。



Network Sessions (ネットワークセッション) - サンプルのネットワークセッションについて学習します。このデータを使用して、脅威のコンテキストの詳細、影響を受けるホストとクライアント、およびマルウェアの配信に使用されるアプリケーションを知ることができます。

Coverage (カバレッジ) - 脅威に対する保護レベルを評価するために、サンプルのシグネチャカバレッジをチェックします。サンプルのダウンロード元ドメインにタグ付けされたシグニチャと、サンプルがアクセスする URL を表示できます。



Indicators (インジケータ) - 設定されたネットワークの指標となるアーティファクトを表示します。インジケータは、ドメイン、IPアドレス、URL、ユーザーエージェントヘッダー、相互除外オブジェクトなどのアーティファクトタイプに基づいて分類されます。危険性の高いアーティファクトは、Suspicious (疑わしい)またはHighly Suspicious (非常に疑わしい)と分類されます。

Domain

2 Highly Suspicious 4 Suspicious 4 Interesting

These domains - seen when this sample was executed in the WildFire analysis environment - are predominantly found with malware, and can indicate a compromised network.

#	Confidence	Indicator	Matching Indicators	Benign	Grayware	Malware
1	Highly Suspicious	info.ackng.com		0	0	234
2	Highly Suspicious	42.pl		97	5	499
3	Suspicious	ns3.epik.com		555	43	28,611
					44	28,595

IPv4

1 Highly Suspicious 2 Suspicious

These IP addresses - seen when this sample was executed in the WildFire analysis environment - are predominantly found with malware, and can indicate a compromised network.

#	Confidence	Indicator	Matching Indicators	Benign	Grayware	Malware
1	Highly Suspicious	88.214.207.96		30	1	277
2	Suspicious	127.0.0.1		273,674	891,030	7,528,431
					8	562

URL

1 Highly Suspicious 4 Interesting

These URLs - seen when this sample was executed in the WildFire analysis environment - are predominantly found with malware, and can indicate a compromised network.

#	Confidence	Indicator	Matching Indicators	Benign	Grayware	Malware
1	Highly Suspicious	/e.png?id=		0	0	233
2	Suspicious	ip.42.pl/raw		104	7	507
3	Interesting	zz3r0.com/e.png?id=GVZ823834177364.GVZ823834177364.local&ma...		--	--	--
					--	--

User Agent

1 Suspicious

These user agent headers - seen for HTTP requests that were sent when this sample was executed in the WildFire analysis environment - are predominantly found with malware, and can indicate a compromised network.

#	Confidence	Indicator	Matching Indicators	Benign	Grayware	Malware
1	Suspicious	Python-urllib/2.7		5,162	26,246	54,432

Mutex

5 Interesting

A mutex (mutual exclusion object) allows programs to share the same resource, though the resource cannot be used by more than one program simultaneously. These mutexes are predominantly found with malware, and can indicate a compromised network.

#	Confidence	Indicator	Matching Indicators	Benign	Grayware	Malware
1	Interesting	testmutex_{D0E858DF-985E-4907-B7FB-8D732C3FC3B9}		1	0	0
2	Interesting	Local\c:!users!jgs9ctxe4sno!appdata!roaming!microsoft!windows!cookies!		--	--	--
					--	--

監視:支店サイト

どこで使用できますか?	何が必要ですか?
• Prisma Access (Managed by Panorama or Strata Cloud Manager) • Software NGFW Creditsによって資金提供されたものを含むNGFW • Prisma SD-WAN	これらの各ライセンスには、Strata Cloud Managerへのアクセスが含まれています。 ❑ Prisma Access ❑ AIOps for NGFW Premium license (use the Strata Cloud Manager app) ❑ Strata Cloud Manager Essentials ❑ Strata Cloud Manager Pro ❑ Prisma SD-WAN その他のライセンスと可視性に必要な前提条件は次のとおりです。 ❑ ADEM Observability (ADEMの観測可能性) ❑ Autonomous DEM for Remote Networks (リモートネットワーク用自律型DEM) ❑ AI-Powered ADEM (AI搭載ADEM) ❑ WAN Clarity Reporting (WANクラリティレポート) ❑ ダッシュボードを表示する権限を持つロール → Strata Cloud Managerで利用できる機能は、使用するライセンスによって異なります。

支店サイト:**Prisma Access**

[Monitor (監視)] > **[Branch Sites (支店サイト)]** > **[Prisma Access]** 選択すると、 リモートネットワークの健全性と接続性、およびさまざまなPrisma Access場所に配置されたすべてのリモートネットワークの使用状況が表示されます。リアルタイムの接続ステータスと帯域幅消費の詳細、およびその他のデプロイメントの詳細が表示されます。モバイル ユーザー、支社、小売店はリモート ネットワークに接続します。リモート ネットワークとモバイル ユーザーに設定されているトンネルの健全性も表示できます。

表示されるウィジェットに加えて、 Prisma Accessライセンスの場合、このダッシュボードにはサイトエクスペリエンススコアと Prisma SD-WAN支店サイトの詳細ページは、 ADEM ObservabilityまたはAI-Powered ADEMライセンス。

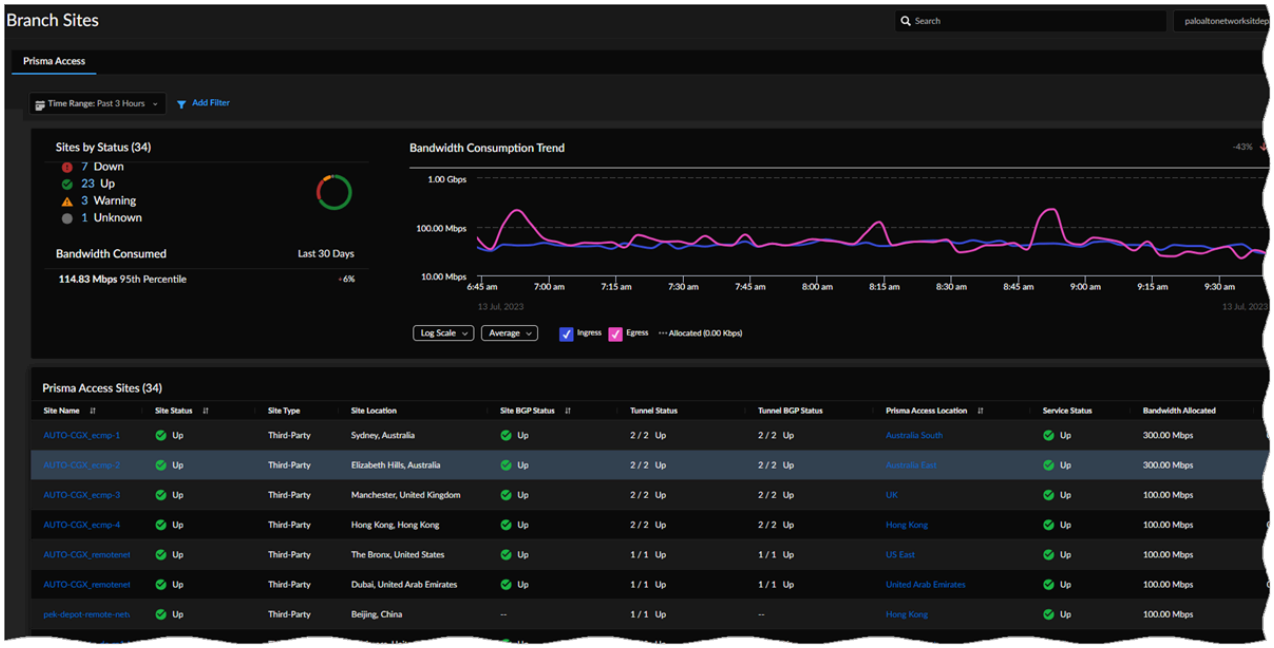
支店サイト:**Prisma SD-WAN**

[Monitor (監視)] > **[Branch Sites (支店サイト)]** > **[Prisma SD-WAN]**選択して、Prisma SD-WANで支店サイトをセットアップします。支店サイトには、Prisma SD-WANのワイド エリア ネットワークにあるブランチ オフィスが含まれる。ION デバイスが特定のサイトに到着する前または到着した後に、 支店サイトをセットアップ できます。Prisma SD-WANの支社サイトからは、次のようなビューを確認できます:

- 支社サイトの **[Map (マップ)]** ビューには、支社サイトデバイスからコントローラへの接続ステータスと、サイトのアラーム ステータスが表示されます。
- **[List (リスト)]** ビューには、選択した **[Time Range (時間範囲)]** 内にアクティブだったサイトの数と、支店サイトの全体的な正常性メトリクスが表示されます。
- **[Activity (アクティビティ)]** ビューには、主要なアプリケーション分析、最新のサイト ヘルス スコア、および時間の経過に伴うサイト の正常性に関する分布が表示されます。
- Prisma Access
- Prisma SD-WAN

支店サイト:

[Branch Sites (支店サイト)] > **[Prisma Access]**選択すると、 リモートネットワークの正常性と接続性、およびさまざまなPrisma Access場所に配置されたすべてのリモートネットワークの使用状況が表示されます。



リアルタイムの接続ステータスと帯域幅消費の詳細、およびその他のデプロイメントの詳細が表示されます。モバイル ユーザー、支社、小売店はリモート ネットワークに接続します。リモート ネットワークとモバイル ユーザーに設定されているトンネルの正常性も表示できます。これらのウィジェットの詳細については、「View and Monitor Branch Sites (ブランチサイトの表示と監視)」を参照してください。

次の作業を行えます。

- ステータス別にリモートネットワークのサイトを確認できます。

- リモートネットワークの帯域幅消費の傾向を確認できます。
- Prisma Accessサイトを表示し、任意のサイトを選択すると、さらに詳細が表示されます。
- サイト内の各SPNの帯域幅消費の詳細を表示するには、「**IPSec Termination Node Utilization Details (IPSec終端ノード使用状況)**」を開きます。
- サイトのトンネルデータとトンネルの傾向を表示します。
- サイトのステータス、正常性、接続性、および利用情報を表示します。

支店サイト(Prisma SD-WAN)

ION デバイスが特定のサイトに到着する前または到着した後に、 支店サイトをセットアップ できます。Prisma SD-WANの支社サイトからは、次のようなビューを確認できます:

- 支社サイトの**[Map (マップ)]**ビューには、支社サイトデバイスからコントローラへの接続ステータスと、サイトのアラーム ステータスが表示されます。ブランチサイトを選択すると、次の情報が表示されます。
  - サイトの概要:分析とトラブルシューティングに使用します。
  - 構成:サイトとデバイス設定に使用します。
  - オーバーレイ接続：すべてのVPNオーバーレイ接続のステータスを表示するために使用されます

  。
- **[List (リスト)]**ビューには、選択した**[Time Range (時間範囲)]**内にアクティブだったサイトの数と、支店サイトの全体的な正常性メトリクスが表示されます。低品質サイトの平均スコアは、低品質と特定されたサイトのすべての低品質サンプルの平均です。時系列グラフは、選択した期間に基づいて計算され、更新されます。たとえば、サポートされている期間は1時間、3時間、24時間、7日、30日、90日で、間隔はそれぞれ1分、5分、1時間、1日です。
  - サイト接続性の正常性分布:最新のサイト接続性の正常性分布に基づいて、特定のテナントの「Good」、「Fair」、「Poor」サイトの分布をグラフ化します。
  - サイト接続性の正常性の経時的分布:デバイスソフトウェア5.6.1以上を実行している正常性スコアの時系列グラフ。
  - サイト アプリケーション エクスペリエンス スコア:サイト アプリケーション エクスペリエンス スコア:
  - **PRISMA SD-WAN**支店サイト:ブランチサイトのサイト正常性、サイト接続性の正常性、回線の正常性、セキュアファブリック正常性、およびしきい値のキャパシティの近さを表示します。サイト予測、アラームステータス、およびADEMステータスで支店サイトをさらに掘り下げてフィルタリングできます。

- **[Activity (アクティビティ)]**ビューには、主要なアプリケーション分析、最新のサイト正常性スコア、および時間の経過に伴うサイトの正常性に関する分布が表示されます。これらには次のものが含まれます。
  - サイト正常性分布: 最新のサイト正常性スコアに基づいて、特定のテナントの「Good」、「Fair」、「Poor」サイトの分布グラフを表示します。
  - サイト正常性の時系列分布：ブランチサイトの正常性スコアに基づいて、特定のテナントのサイト正常性の時系列グラフを表示します。
  - 帯域幅使用率：サイトおよびWANパス上の各アプリケーションの帯域幅使用率を、ネットワークで最も帯域幅を消費する上位10アプリケーションのデータとともに表示します。
  - トランザクション統計：TCPフローに関するトランザクション統計を表示します。特定のアプリケーションまたはすべてのアプリケーション、特定のパスまたはすべてのパス、すべての正常性イベントに関する開始/トランザクションの成功と失敗が表示されます。
  - 新しいフロー：アプリケーション、特定のアプリケーションセット、または指定された期間のすべてのアプリケーションの新しいTCPおよびUDPフローを表示します。
  - 同時フロー：ネットワーク上でアクティブな接続数をアプリケーション別に把握できます。

監視:データセンター

どこで使用できますか?	何が必要ですか?
• Prisma Access (Managed by Panorama or Strata Cloud Manager) • Software NGFW Creditsによって資金提供されたものを含むNGFW • Prisma SD-WAN	これらの各ライセンスには、Strata Cloud Managerへのアクセスが含まれています。 ❑ Prisma Access ❑ AIOps for NGFW Premium license (use the Strata Cloud Manager app) ❑ Strata Cloud Manager Essentials ❑ Strata Cloud Manager Pro ❑ Prisma SD-WAN その他のライセンスと可視性に必要な前提条件は次のとおりです。 ❑ ADEM Observability (ADEMの観測可能性) ❑ Autonomous DEM for Remote Networks (リモートネットワーク用自律型DEM) ❑ AI-Powered ADEM (AI搭載ADEM) ❑ WAN Clarity Reporting (WANクラリティレポート) ❑ ダッシュボードを表示する権限を持つロール → Strata Cloud Managerで利用できる機能は、使用するライセンスによって異なります。

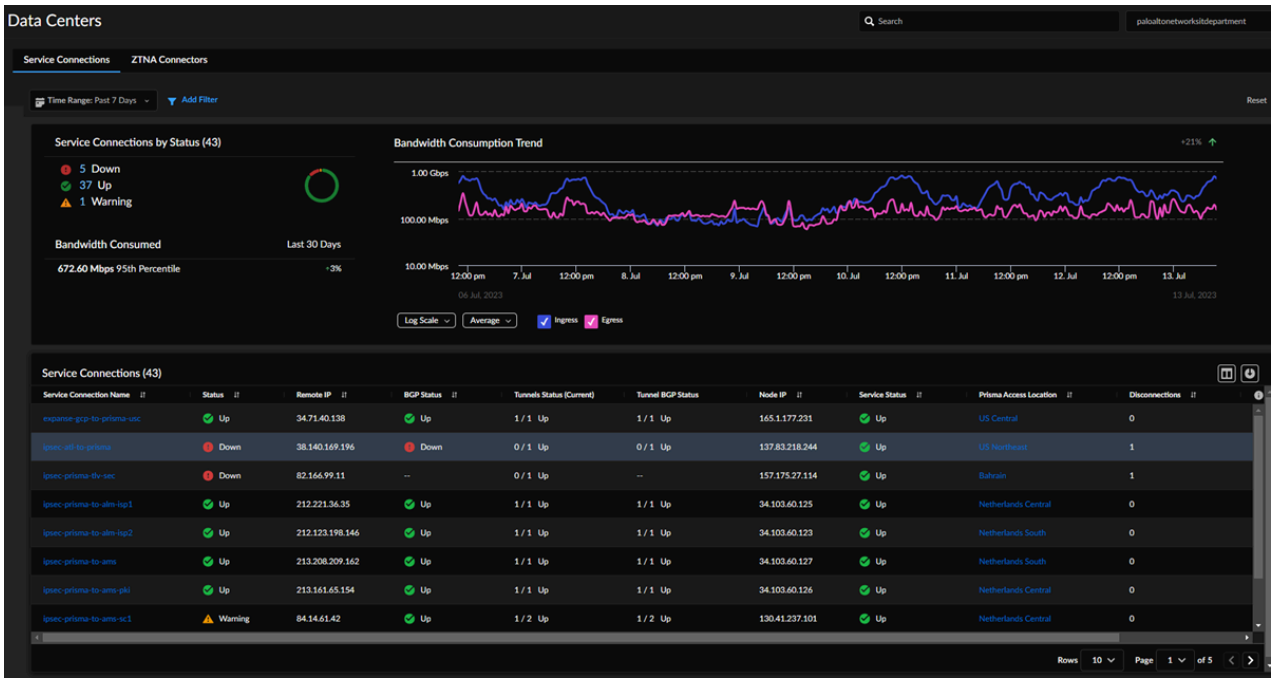
サービス接続、ZTNAコネクター、サイト接続が、Prisma SD-WANデータセンターでどのように機能しているかを監視します。**Monitor (監視) > Prisma Access > Data Centers (データセンター) > Service Connections (サービス接続)** または **ZTNA Connectors (ZTNAコネクタ)** タブを選択し、Prisma Accessで、サービス接続と ZTNA コネクタの接続性とステータスを表示します。

Prisma SD-WANデータセンターごと に **[Monitor (監視)] > [Data Centers (監視)] > [Prisma SD-WAN]**を選択して、サイトの接続情報とVPNオーバーレイ接続のステータスを表示します。

- サービスコネクション
- ZTNA コネクタ
- Prisma SD-WAN

サービスコネクション

[Monitor (監視)] > **[Data Centers (データセンター)]** > **[Service Connections (サービスコネクション)]**を選択して開始します。



サービスコネクションの集計データだけでなく、個々のサービスコネクションに関する情報も表示できます。サービスコネクションにより、モバイルユーザーとリモートネットワークの両方が可能になります。サービスコネクションは、企業リソースへのアクセスを提供するだけでなく、モバイルユーザーが支店ロケーションに到達できるようにします。これらのウィジェットの詳細については、「*Prisma Access Administration Guide (Prisma Access*管理ガイド*)*」の「View and Monitor Data Centers (データセンターの表示と監視)」を参照してください。

- 時間範囲を選択すると、ステータス別のサービスコネクションとその帯域幅消費の傾向が表示されます。
- すべてのサービスコネクションの正常性ステータスを表示します。
- すべてのサービスコネクションの帯域幅消費傾向を表示します。
- ステータス、リモートIPアドレス、BGPステータス、現在のトンネルステータス、その他のデータなど、サービスコネクションに関するデータを表示します。任意のサービスコネクションを選択すると、その詳細が表示されます。

ZTNA コネクタ

[Monitor (監視)] > **[Data Centers (データセンター)]** > **[ZTNA Connectors (ZTNA コネクタ)]**を選択して、使用を開始します。

ゼロ トラスト ネットワーク アクセス (ZTNA) コネクタは、すべてのアプリケーションのプライベート アプリケーション アクセスを簡素化します。環境内のZTNAコネクタVMは、プライベート アプリケーションとPrisma Accessとの間に自動的にトンネルを形成します。設定されているすべてのZTNAコネクタの概要を表示します。これには、コネクタに関連付けられているア

プリケーションターゲット、その平均帯域幅と中央値、およびステータス（アップ、部分アップ、またはダウン）が含まれます。これらのウィジェットの詳細については、「*Prisma Access Administration Guide (Prisma Access*管理ガイド*)*」の「View and Monitor Data Centers (データセンターの表示と監視)」を参照してください。

次の作業を行えます。

- ZTNAコネクタグループの正常性とステータスを表示する。
- 個々のZTNAコネクタの正常性とステータスを表示します。

データセンター（Prisma SD-WAN）

Prisma SD-WAN サイトには、広域ネットワークに配置する データセンター が含まれます。エンタープライズ アプリケーションとサービスをデータセンターでホストできます。データセンターの作成の一環として、デフォルトのドメインとポリシー セットを選択し、WANネットワーク、回線カテゴリ、回線ラベル、回線仕様をセットアップできます。Prisma SD-WAN データセンター 画面には、データセンター名、ION デバイス、およびサイトの開いているアラームを含むデータセンターのリストが表示されます。

データセンターの場合は、次のようになります。

- サイトの接続情報、 デプロイメントモード、WAN マルチキャスト ピア グループ プロファイル、 インターネットおよびプライベート WAN 回線、およびIP プレフィックスを表示する**[Configuration (**設定**)]**タブ。また、 ユーザー エージェントを設定し 、データセンターの クラスター設定 の詳細を表示することもできます。
- 「**Overlay Connections (**オーバーレイ接続**)**」 タブには、すべての VPN オーバーレイ接続のステータスが表示されます。各サイトの接続は、VPNオーバーレイ接続のステータスに基づいて計算されます。

監視:Network Services（ネットワーク サービス）

どこで使用できますか?	何が必要ですか?
• Prisma Access (Managed by Panorama or Strata Cloud Manager) • Software NGFW Creditsによって資金提供されたものを含むNGFW • Prisma SD-WAN	これらの各ライセンスには、Strata Cloud Managerへのアクセスが含まれています。 ❑ Prisma Access ❑ AIOps for NGFW Premium license (use the Strata Cloud Manager app) ❑ Strata Cloud Manager Essentials ❑ Strata Cloud Manager Pro ❑ Prisma SD-WAN その他のライセンスと可視性に必要な前提条件は次のとおりです。 ❑ ADEM Observability (ADEMの観測可能性) ❑ Autonomous DEM for Remote Networks (リモートネットワーク用自律型DEM) ❑ AI-Powered ADEM (AI搭載ADEM) ❑ WAN Clarity Reporting (WANクラリティレポート) ❑ ダッシュボードを表示する権限を持つロール → Strata Cloud Managerで利用できる機能は、使用するライセンスによって異なります。

[Monitor (監視)] > [Network Services (ネットワークサービス)] ページから、アプリケーションにアクセスするユーザ エクスペリエンスに影響を与える一般的なネットワーク サービスのパフォーマンスを表示できます。**[GlobalProtect Authentication (GlobalProtect認証)]** タブを選択すると、さまざまな場所のGlobalProtectの認証の成功数または失敗数が表示されます。ネットワークサービスを選択します：**DNS**は、Prisma AccessDNSプロキシに関してテナント全体で受信されたDNSプロキシの要求と応答を表示します。

- グローバルプロテクト認証チェック
- DNS

グローバルプロテクト認証チェック

開始するには、**[Monitor (監視)] > [Network Services (ネットワークサービス)] > [GlobalProtect Authentication (GlobalProtect認証)]** を選択します。

[Insights (インサイト)]では、アプリケーションにアクセスする際のユーザーエクスペリエンスに影響する一般的なネットワークサービスのパフォーマンスを確認できます。ネットワークサービスには、GlobalProtect認証の成功数と失敗数のレポートが含まれ、モバイルユーザーがPrisma Accessに接続できるかどうかの指標となります。以下を表示できます。

- さまざまな場所でのGlobalProtectの認証成功回数について具体的に説明します。
- GlobalProtectの認証失敗数は、場所によって異なります。
- さまざまな場所でのGlobalProtectの認証タイムアウトエラー。

これらのウィジェットの詳細については、「View and Monitor Network Services (ネットワークサービスの表示と監視)」を参照してください。

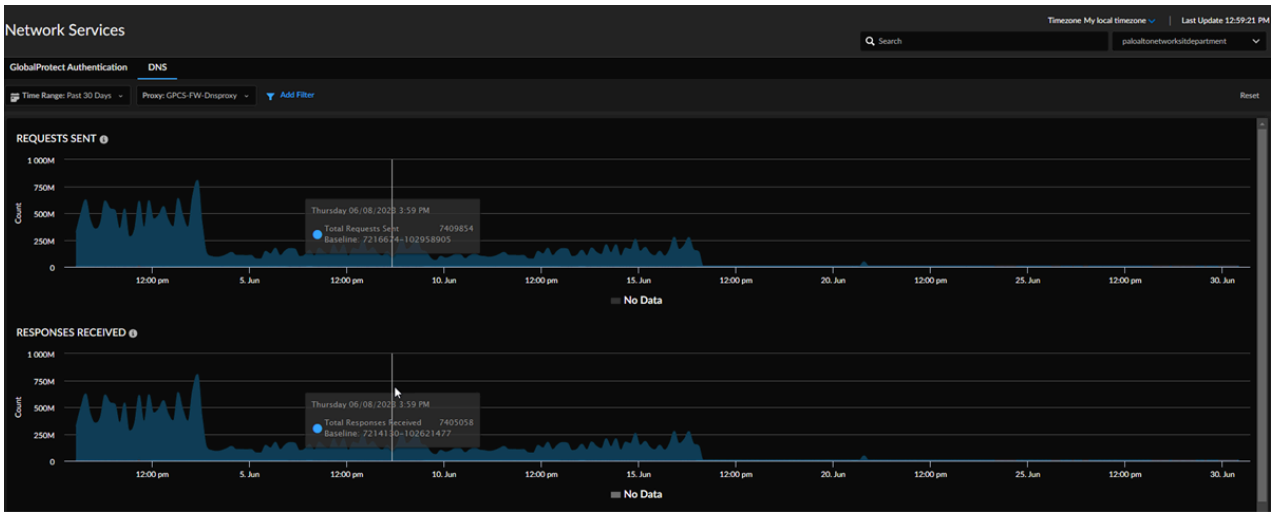
DNS

[Monitor (監視)] > **[Network Services (ネットワーク サービス)]** > **[DNS]**を選択して開始します。

Network Services（ネットワーク サービス）**DNS**はDNSプロキシの要求と応答を表示します。次のフィルタを使用することができます:

- 期間
- **DNS**プロキシ名

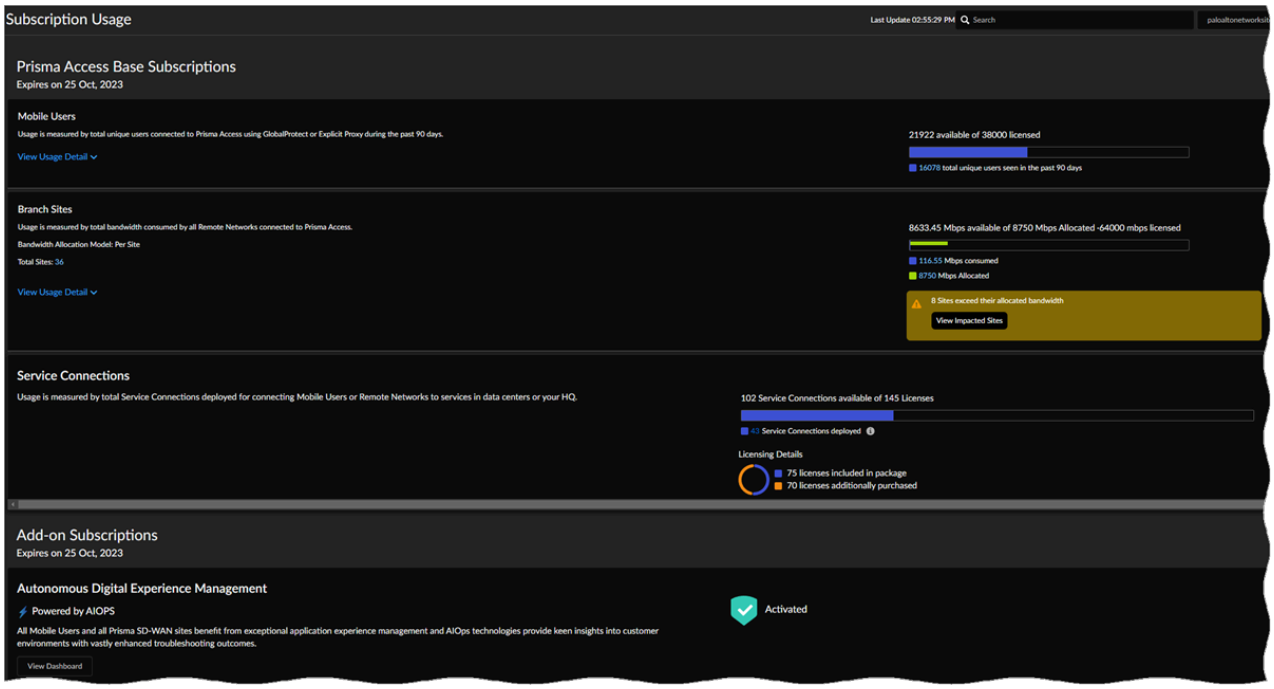
DNSプロキシフィルタの値は過去30日間に関連し、ロード時に自動的に選択されます（つまり、明示的なプロキシデータがない場合は、明示的なプロキシフィルタは存在しません）。詳細については、「ネットワークサービスの表示と監視」を参照してください。



監視:サブスクリプションの使用法

どこで使用できますか?	何が必要ですか?
• Prisma Access （*Strata Cloud Manager*または*Panorama*の設定管理付き）	❑ Prisma Accessライセンス ❑ 特定の機能のロックを解除するためのAI-Powered ADEM。

[Monitor (監視)] > **[Subscription Usage (サブスクリプションの使用状況)]**を選択すると、接続しているユニークユーザーの合計数、リモートネットワークユーザーが消費する帯域幅、展開されているサービス接続の合計数、アドオンサブスクリプションの詳細など、**Prisma Access Base** サブスクリプションの使用に関する詳細が表示されます。



- モバイルユーザー:これまでに利用したユニークなモバイルユーザーライセンス数を表示します。ライセンスは過去90日間のPrisma Accessログインデータに基づいているため、ウィジェットには過去90日間にPrisma Accessに接続したユニークモバイルユーザーが消費したライセンスの合計数が表示されます。過去90日間に1回以上Prisma Accessにログインしたユーザーが、1つのモバイルユーザーライセンスの消費に貢献します。
- 支店サイト:Prisma Accessに接続されているすべてのリモートネットワークで消費される帯域幅の合計使用量を確認できます。Mbps単位で、割り当てた帯域幅と消費した帯域幅を表示します。Prisma Accessに接続されているすべてのリモート・ネットワークで消費された帯域幅の合計で使用量が表示されます。
- サブスクリプションの使用方法:これまでに利用したサービス接続ライセンス数を確認できます。

このページの「アドオンサブスクリプション」セクションを参照して、モバイルユーザーおよびリモートネットワーク用の自律型デジタルエクスペリエンス管理ライセンスなど、購入した追加ライセンスを確認してください。購入したライセンスの総数と、これまでに利用していないライセンス数を確認できます。モバイルユーザー監視用アプリケーションテストの表示 - モバイルユーザー用に作成できる残りのアプリケーションテストの数。アプリケーション テストは、監視対象のモバイル ユーザーの数により決定され、モバイル ユーザーごとに最大10個のアプリ テストが許可されます

詳細については、「サブスクリプション使用状況の表示と監視」を参照してください。

監視:IONデバイス

どこで使用できますか?	何が必要ですか?
• Prisma SD-WAN	☐ Prisma SD-WANライセンス

Prisma SD-WANのIONデバイスを使用すると、MPLS、LTE、インターネットリンクなどの異なるWANネットワークを、高性能でハイブリッドな単一のWAN(ワイドエリアネットワーク)にまとめることができます。

[Device List (デバイスリスト)]画面には、IONデバイスのソフトウェアバージョンやステータスなど、Prisma SD-WANデバイスのリストに関する情報が表示され、デバイスのソフトウェアバージョンのアップグレードやデバイスの設定を行うことができます。

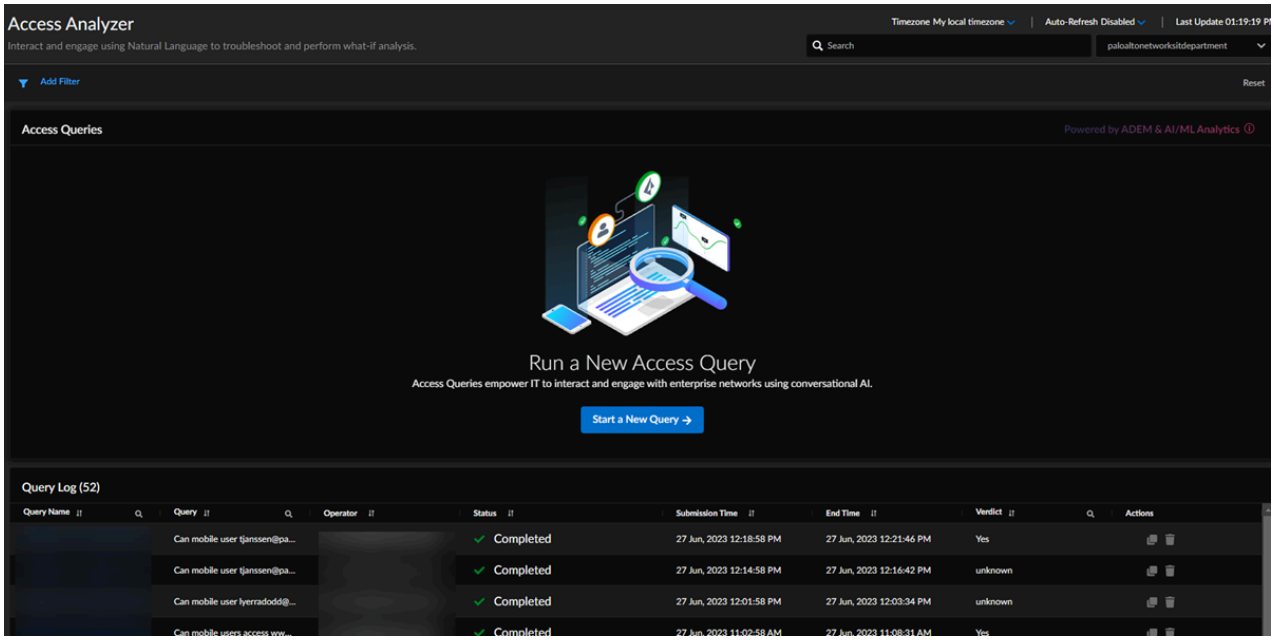
エンティティ	詳説
デバイス名	IONデバイスに設定されている名前を表示します。
デバイス情報	IONデバイスの種類とシリアナンバーを表示します。
software	デバイスの現在のソフトウェアバージョンを表示します。［**Upgrade (アップグレード)**］をクリックして、デバイスソフトウェアのバージョンを変更します。
最終アクティビティ	IONデバイスが最後に設定およびアップグレードされた日時に関する情報を表示します。
状態	IONデバイスの現在の状態を表示します。
冗長性	ION デバイスが高可用性（HA）構成の一部である場合に表示されます。
アクション	省略符号メニューからIONデバイスの設定を選択できます。

［**Device Activity (デバイスアクティビティ)**］画面には、過去24時間のサイトのさまざまなデバイス アクティビティ レポートが表示されます。

監視:アクセスアナライザー

どこで使用できますか?	何が必要ですか?
• Prisma Access （*Strata Cloud Manager*または*Panorama*の設定管理付き）	❑ Prisma Accessライセンス ❑ AI-Powered ADEMライセンス

新しいアクセスアナライザクエリを開始し、既存のクエリのテーブルを表示するには、**{Monitor (監視)} > [Access Analyzer (アクセスアナライザー)]** を選択します。



アクセスアナライザは、SASE環境を自動的に監視します。SASE環境におけるアクセスと接続の問題を分析するコンテキスト トラブルシューティングとwhat-if解析のための会話型AIツールを提供します。

次の作業を行えます。

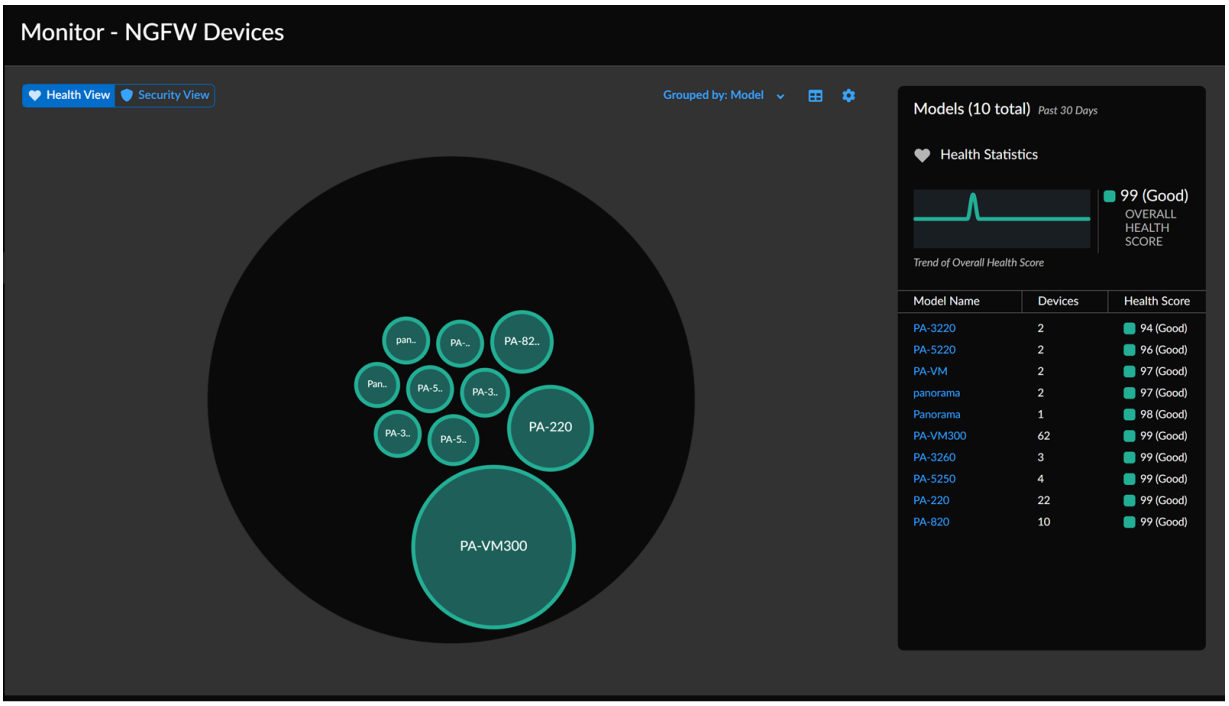
- Access Analyzerで自然言語クエリを作成する方法について説明します。
- 新しいアクセスアナライザクエリを開始します。
- 既存のクエリのリストを表示し、テーブルから任意のクエリを選択すると、さらに詳細が表示されます。

監視:NGFW デバイス

どこで使用できますか?	何が必要ですか?
• NGFW （*Strata Cloud Manager*または*Panorama*の設定管理付き）	❑ AIOps for NGFW Free (use the AIOps for NGFW Free ap または AIOps for NGFW Premium license (use the Strata Cloud ❑ Software NGFW Credits （*VM-Series*ソフトウェア*NGFW*の場合）

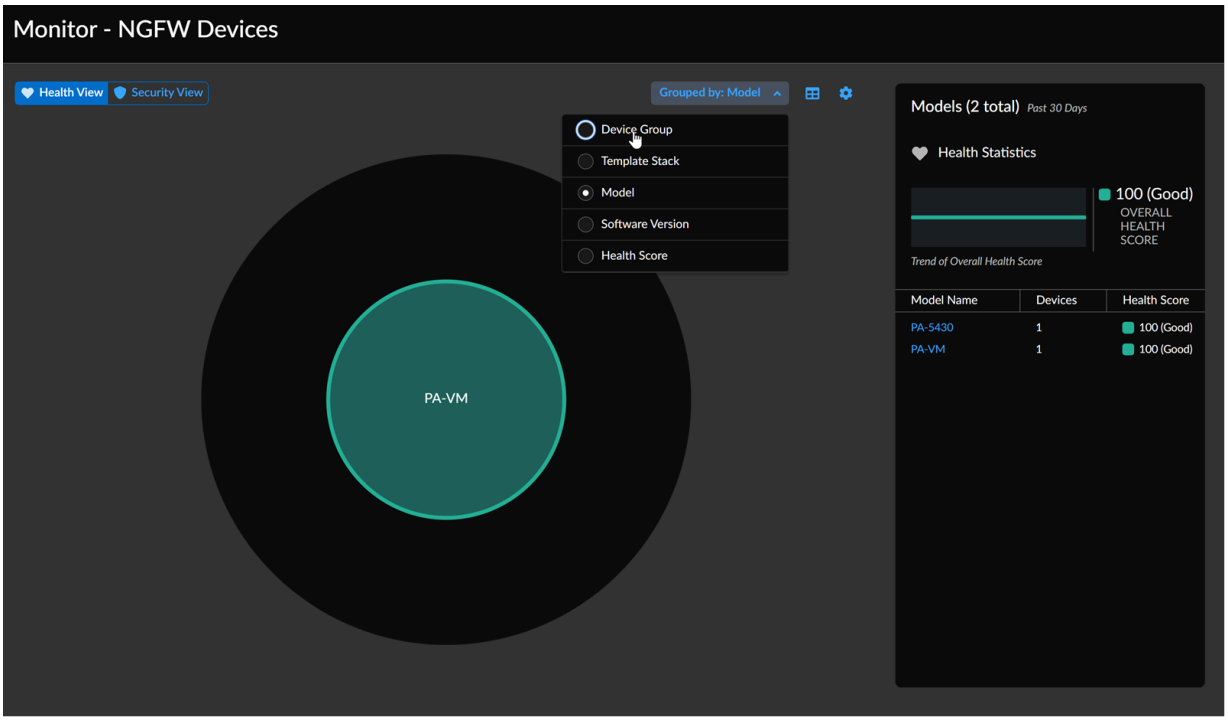
[Monitor (監視)] > [NGFW Devices (NGFWデバイス)]では、デプロイメント内のデバイスを色分けしてインタラクティブに表示できるため、管理と調査を簡単かつ直感的に行うことができます。

STEP 1 | **[Monitor (監視)] > [NGFW Devices (NGFWデバイス)]**を選択します。



STEP 2 | **[Health (正常性)]** または **[Security (セキュリティ)]**を選択します。

STEP 3 | 視覚化を グループ化する属性を選択します。



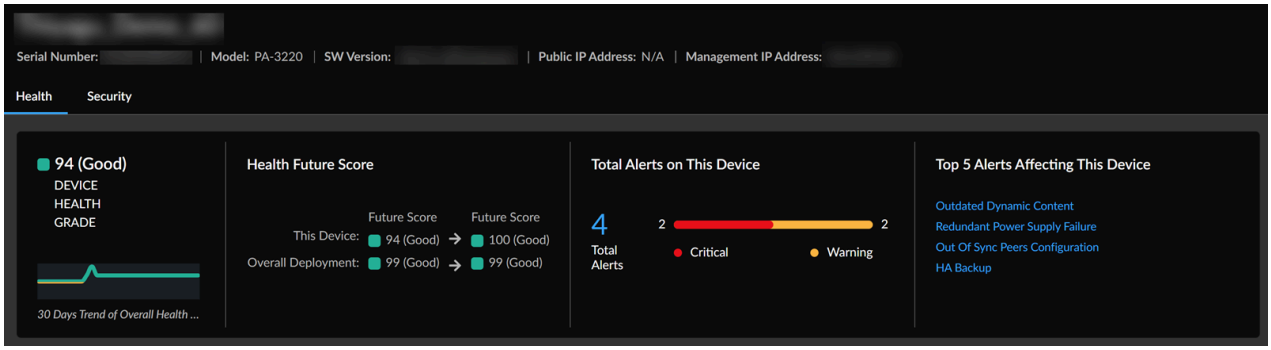
[Device Group (デバイス グループ)] と *[Template Stack (テンプレート スタック)]*のグループ化オプションは、*Panorama*がデバイス テレメトリを送信する*Panorama*管理のデプロイメントでのみ使用できます。

STEP 4 | グループを選択すると、そのグループ内のデバイスが表示され、デバイスを選択すると、そのデバイスに関する一般情報が表示されます。

デバイスの詳細を知りたい場合は、そのデバイスを選択してください。

デバイスの詳細を表示

NGFW デバイス の視覚化からデバイスを選択するか、アプリケーション内の他の場所からリンクをたどることで、正常性グレード、メトリック、接続など、ファイアウォールまたはPanoramaアプライアンスに関する特定の詳細を表示できます。



デバイスヘルスグレード

デバイスの現在の健康等級と、過去30<x>日間の履歴を示すチャート。健康状態の評価は、「Good (良好)」、「Fair (普通)」、「Poor (不良)」、「Critical (危険)」のいずれかになります。

修復後の健全性グレード

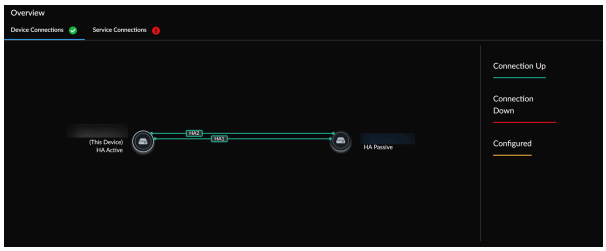
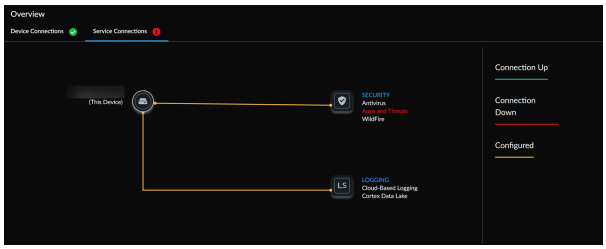
未解決のアラートに対処した後のデバイスの健全性グレード。このタイルには、アラートを閉じた後の全体的なデプロイメントの健全性も表示されます。

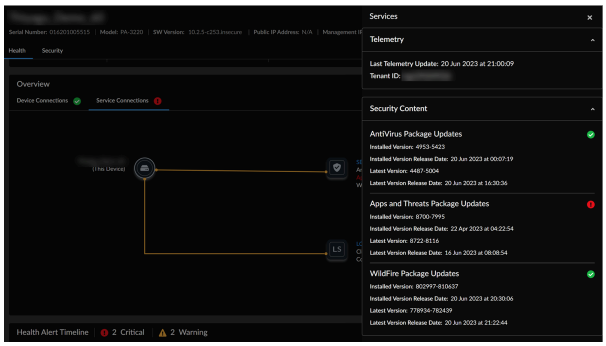
合計アラート数

デバイス上の未解決アラートの合計数。

トップ**5**アラート

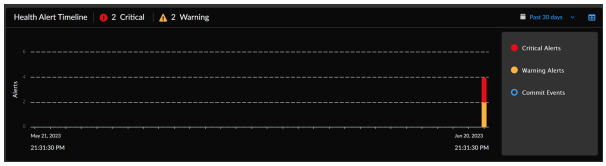
過去30日間にこのデバイスで最も頻繁に発生したアラート5件。

概要 > デバイス接続 現在表示しているデバイスに接続されている他のデバイス。詳細を表示するにはデバイスを選択します。	
概要 > サービス接続 デバイスに統合されているすべてのセキュリティおよびログ記録サービスの概要。サービスを選択して詳細を表示します。	



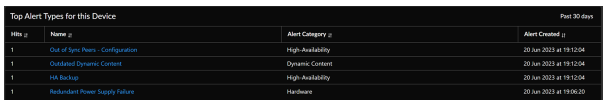
アラートのタイムライン

デバイスアラートとコミットイベントのタイムライン。アラートは、Critical (重大)、Warning (警告)、またはCommit Events (コミット イベント)として分類されます。アラート データを表形式で表示するには切り替えます。



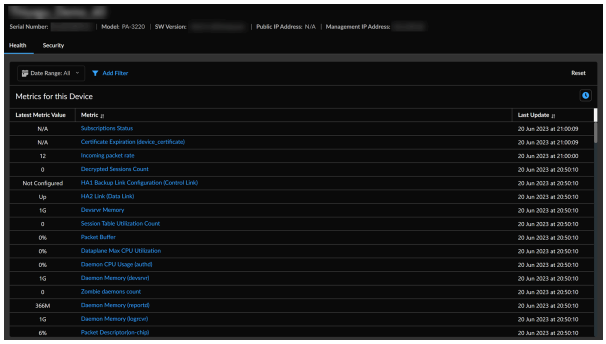
このデバイスのトップアラートタイプ

過去30日間に最も多く発生したアラート。アラートの詳細を表示するには、アラートを選択します。



アプリケーション使用率トップ**10**

ファイアウォール上で最も多くのデータを使用する10個のアプリケーション。

このデバイスのメトリック HAリンク データを含む、デバイスに対して実行されるセキュリティ チェックで収集されたすべての健全性メトリックのリスト。 詳細を表示するにはメトリックを選択します。	

監視:容量アナライザー

どこで使用できますか?	何が必要ですか?
• NGFW	☐ AIOps for NGFW Premium または Strata Cloud Manager Pro → Strata Cloud Managerで利用できる機能は、使用するライセンスによって異なります。

Capacity Analyzerを使用すると、モデルタイプに基づいてメトリクスの使用状況を追跡して、デバイスのリソース容量を分析および監視できます。Capacity Analyzer (容量アナライザー)には次の利点があります。

- 既存のメトリック使用率と、最大限度までの未使用メトリック容量の包括的な理解。
- ハードウェアプラットフォームに関するメトリックの使用状況を1つのビューで示し、詳細のドリルダウンを支援するヒートマップの視覚化。
- お客様固有のニーズに基づいて、より大容量のファイアウォールへのアップグレードを計画する機能。

*VM*シリーズのファイアウォールでは、***Capacity Analyzer (***容量アナライザー*)***機能はサポートされていません。

容量アナライザー機能の使い方を動画でご紹介します。

Capacity Analyzerは、最大容量に近づいたリソースの消費を予測してアラートを発生させるのに役立つアラートをサポートするように拡張されています。Capacity Analyzerのアラートは、潜在的な容量ボトルネックを特定するために3か月前に生成されます。これにより、NGFW容量が最大使用率に達する前に構成クリーンアップまたはアップサイズを計画し、システムの安定性を維持できます。サポートされている容量アラートの一覧については、「Premium Health Alerts (プレミアム正常性アラート)」を参照してください。

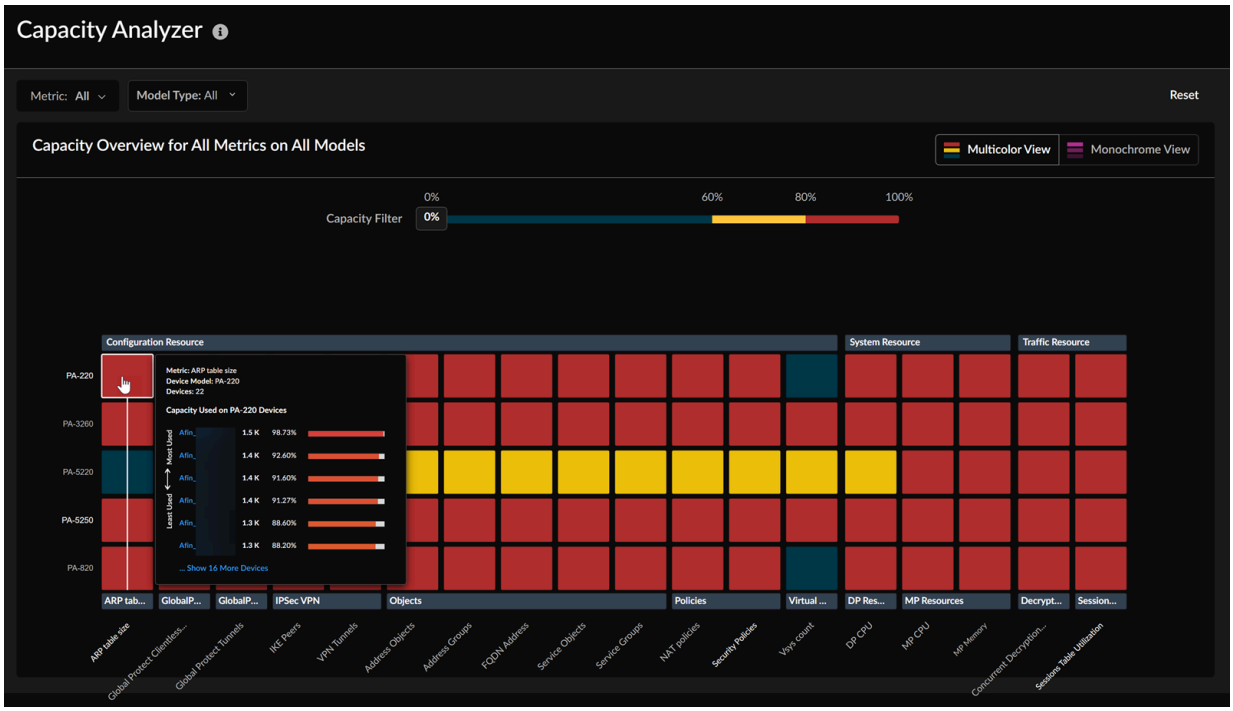
容量アナライザーは、次のタイプに基づいてメトリックをグループ化します。

- NATポリシーやアドレスオブジェクトなどの設定リソースメトリック。
- CPU、メモリ、ディスク、ログなどのシステム運用リソースのメトリック。
- 復号化使用率やセッションテーブル使用率などのトラフィックリソースメトリック。

ヒートマップには、各デバイスのメトリックの使用状況が表示されます。濃い色は使用率が高く、明るい色は使用率が低いことを示します。デフォルトでは、マルチカラービューが選択されています。同様にモノクロ表示に切り替えることができます。

キャパシティアナライザヒートマップを使用してメトリックの使用に関する情報を取得するさまざまな方法は次のとおりです。

- デバイスのメトリックブロックにカーソルを置くと、次の詳細を表示するツールチップが表示されます。
  - メトリックの名前
  - デバイスのモデルとデバイスのリスト
  - デバイス容量の範囲



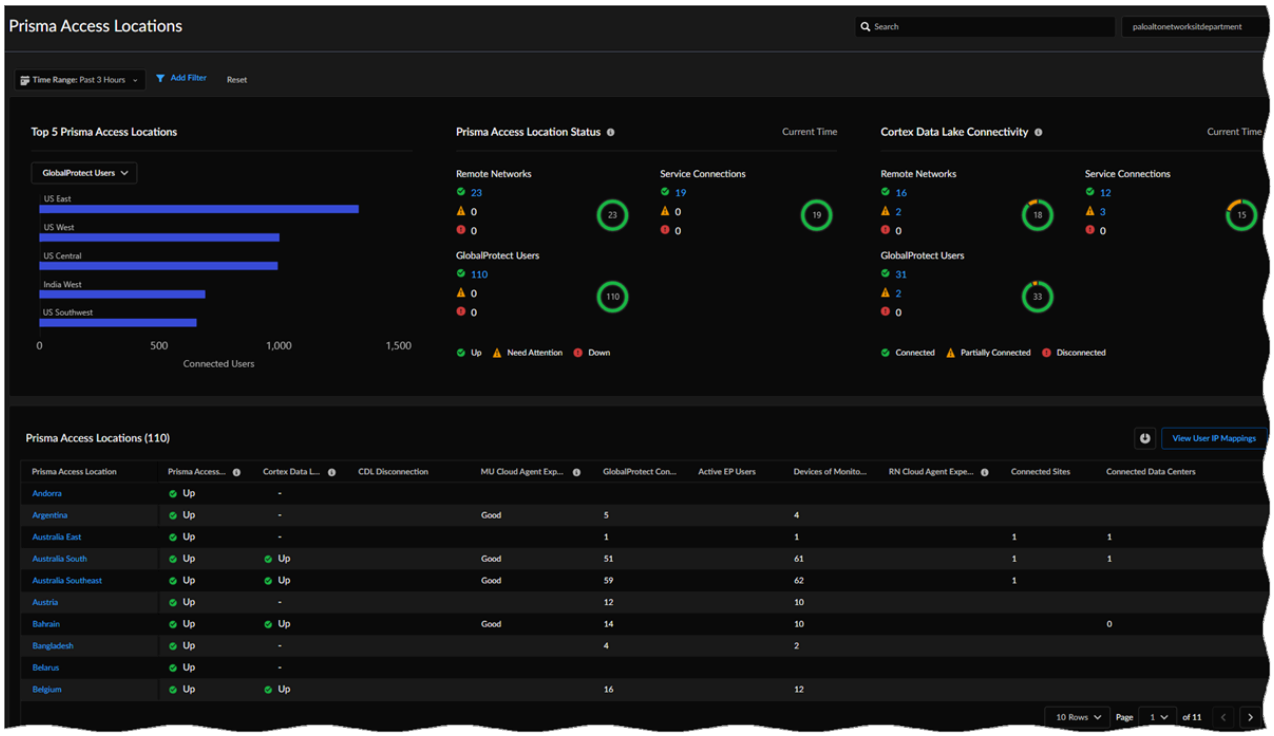
- 次の属性を使用してデータをフィルタリングします。
  - [メトリック] - メトリック名を使用して表示または検索するメトリックを1つ以上選択します。
  - モデル - 1つ以上のデバイスモデルを選択するか、モデル名を使用して検索します。
  - 容量 - 容量フィルタの目盛りで容量を選択します。

容量アナライザーのヒートマップの使用方法の詳細については、「メトリック容量の分析」を参照してください。

監視:Prisma Access ロケーション

どこで使用できますか?	何が必要ですか?
• Prisma Access （*Strata Cloud Manager*または*Panorama*の設定管理付き）	❑ Prisma Accessライセンス これはPrisma Access Insightsの機能です。

開始するには、**[Monitor (監視)] > [Prisma Access Locations (Prisma Accessロケーション)]** を選択します。ここから、リモート ネットワークとモバイル ユーザーのすべての Prisma Access ロケーションの正常性を表示します。これらのウィジェットの詳細については、「*Prisma Access Administration Guide (Prisma Access*管理ガイド*)*」の「View and Monitor Prisma Access Locations (Prisma Accessロケーションの表示と監視)」を参照してください。

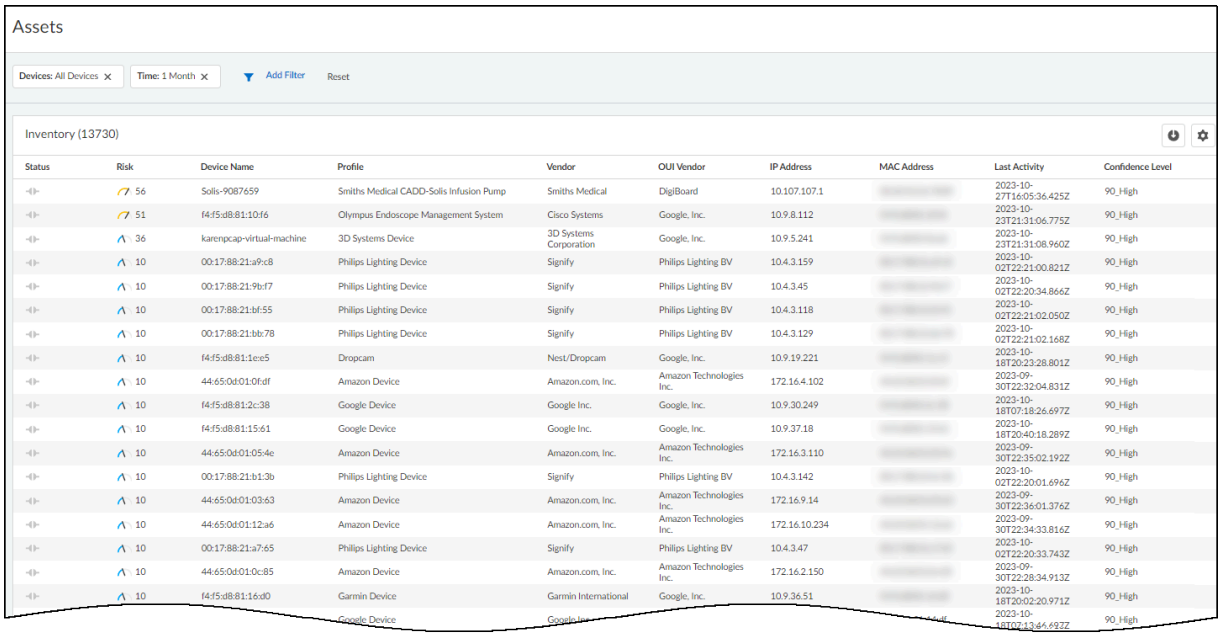


- 消費された合計帯域幅に基づいて、リモート ネットワーク、サービス接続、GlobalProtect モバイル ユーザー、または明示的なプロキシ モバイル ユーザーの上位 5 つの Prisma アクセスの場所を確認します。
- Prisma Access ロケーションのステータスを表示します。
- Strata Logging Service接続性を表示します。
- すべてのPrisma Accessロケーションを一覧表示するPrisma Accessロケーション テーブルを表示し、個々のPrisma Accessロケーションを名前で選択して詳細を表示します。

監視:アセット

どこで使用できますか?	何が必要ですか?
• NGFW （*Strata Cloud Manager*または*Panorama*の設定管理付き）	❑ IoT Securityサブスクリプション ❑ Software NGFW Credits （*VM-Series*ソフトウェア*NGFW*の場合）

まず、**[Monitor (監視)] > [Assets (アセット)]**を選択します。ここでは、ネットワーク上のIoT、OT、ITデバイスの動的に管理されたインベントリを確認できます。インベントリには、IPアドレスとMACアドレス、プロファイル、ベンダー、モデル、OS、および（高度なIoTセキュリティ製品の場合は）デバイスレベルのリスクスコアなど、各デバイスの多数の属性が表示されます。



このインベントリのデータを使用して、ネットワーク上の資産について学習します。

- IoT、OT、ITデバイスなど、ネットワーク上で検出されたデバイスの動的生成および最新のインベントリを表示します。
- IoTダッシュボードには、デバイスの種類が大まかに表示されますが、アセットインベントリでは、個々のデバイスを探索して詳細を確認し、セキュリティ態勢を評価できます。
- ダッシュボードに表示されるデータを、サイト、デバイスタイプ、期間、および1つ以上のデバイス属性でフィルタリングして、関心のあるデバイスに関するデータを表示します。
- 列の表示と非表示を切り替えて、重要なデバイス属性を表示します。100以上の属性カラムがあり、その中から選択できます。

- 現在アクティブなページに表示されているデータをCSV形式のファイルとしてダウンロードし、レポートに含めたり、今後の参照に利用できます。ファイルには、ダウンロード時に表示されていたデバイスとデバイス属性が含まれています。

インシデントとアラート:ログ - Strata Cloud Manager

どこで使用できますか?	何が必要ですか?
• Prisma Access (Managed by Panorama or Strata Cloud Manager) • Software NGFW Creditsによって資金提供されたものを含むNGFW • Prisma SD-WAN	これらの各ライセンスには、Strata Cloud Managerへのアクセスが含まれています。 ❑ Prisma Access ❑ AIOps for NGFW Premium license (use the Strata Cloud Manager app) ❑ Prisma SD-WAN ❑ Strata Cloud Manager Essentials ❑ Strata Cloud Manager Pro その他のライセンスと可視性に必要な前提条件は次のとおりです。 ❑ ダッシュボードを表示する権限を持つロール → Strata Cloud Managerで利用できる機能は、使用するライセンスによって異なります。

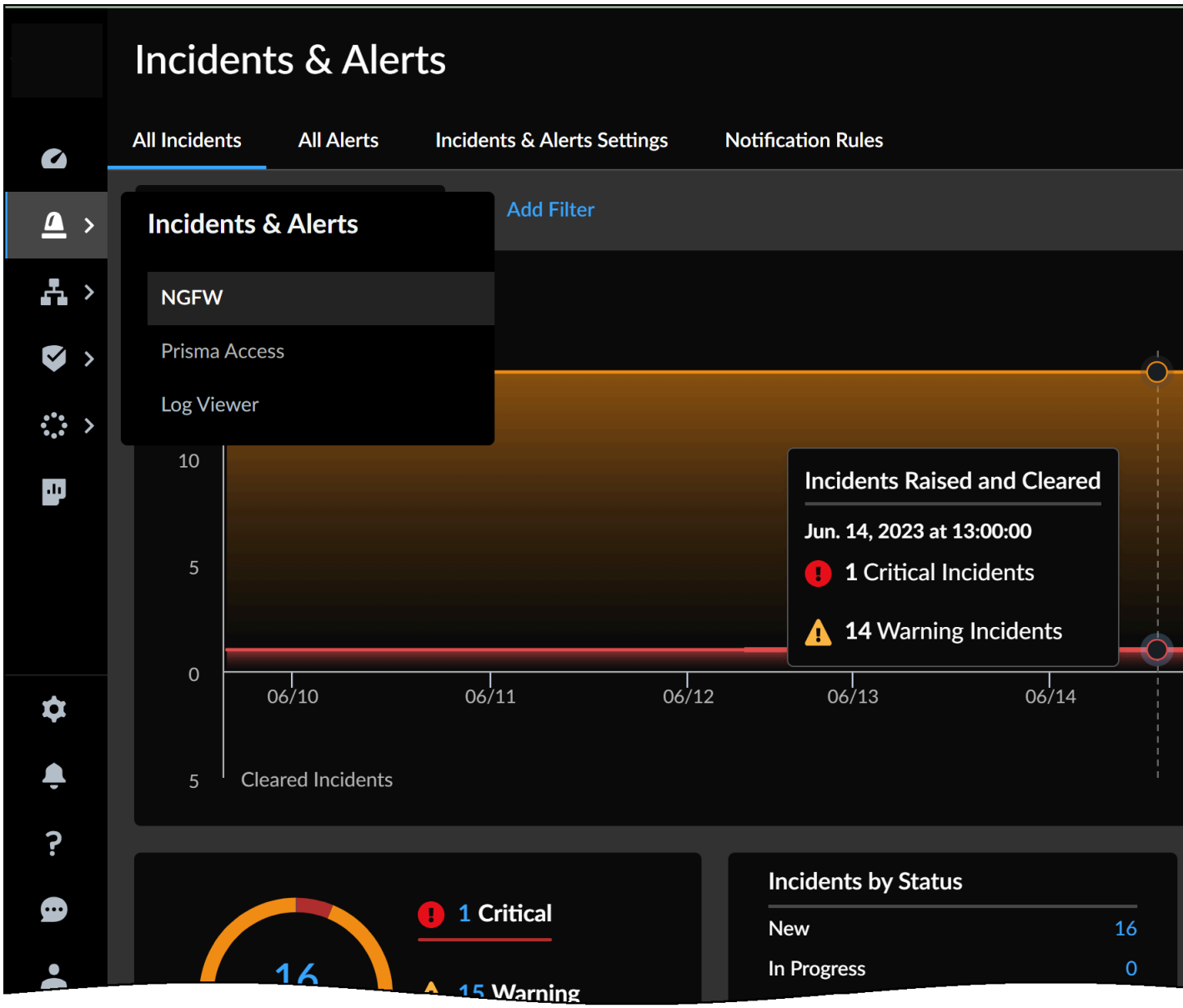
Strata Cloud Managerは、Palo Alto Networks製品およびサブスクリプションが企業内で検出するインシデントとアラートを相互にやり取りし、調査するための共通のフレームワークを提供します。

- インシデントとアラート:NGFW
- インシデントとアラート:Prisma Access
- インシデントとアラート:Prisma SD-WAN

デバイスとデプロイメントの継続的な正常性を維持し、業務の中断を回避するために、インシデントとアラートの各ページで次のことを行います。

- ネットワーク全体のインシデントとアラートを表示し、ドリルダウンして調査できます。
- インシデント通知とアラート通知をトリガーするルールの作成と確認。

インシデントとアラート、およびインシデントとアラート:ログ ビューアー間を移動して、インシデントとアラートをトリガーしている、またはインシデントとアラートに関連付けられているネットワーク上のアクティビティを調査できます。



インシデントとアラート:NGFW

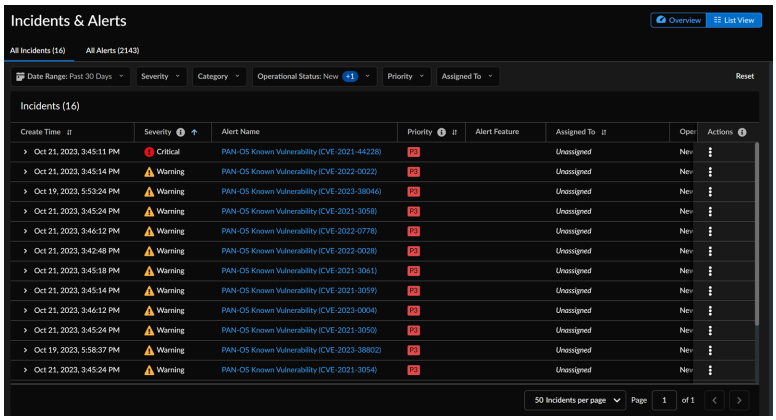
どこで使用できますか?	何が必要ですか?
• Software NGFW Creditsによって資金提供されたものを含むNGFW	❑ 次のいずれかのライセンス: ❑ AIOps for NGFW Free (use the AIOps for NGFW Free app)またはAIOps for NGFW Premium license (use the Strata Cloud Manager app) ❑ Strata Cloud Manager Essentials ❑ Strata Cloud Manager Pro

アプリケーションは、デバイスの継続的な正常性を管理し、業務を中断するインシデントを回避するために、ファイアウォールのデプロイメントで検出された1つ以上の問題に基づいてインシデントとアラートを生成します。**[Incidents & Alerts (**インシデントとアラート**)]** > **[NGFW]**を使用すると、NGFW全体にわたるインシデントとアラートを単一のビューで確認できます。

[NGFW Incidents & Alerts (NGFW インシデントとアラート**)]** を使って起動する方法は以下の通りです。

- インシデントにより、脆弱性に関する情報が提供されます。それらを調査し、必要に応じて予防処置を取ることができます。

  [Incidents & Alerts (インシデントとアラート**)]** > **[NGFW]** > **[All Incidents (**すべてのインシデント**)]**に移動して、ネットワーク全体のインシデントを表示し、インシデントとやり取りします。



- アラートは、対処する必要がある特定の問題（ファイアウォール機能の低下または喪失）を示します。アラートは、複数のイベント間の相関や集約に基づいて生成することもできま

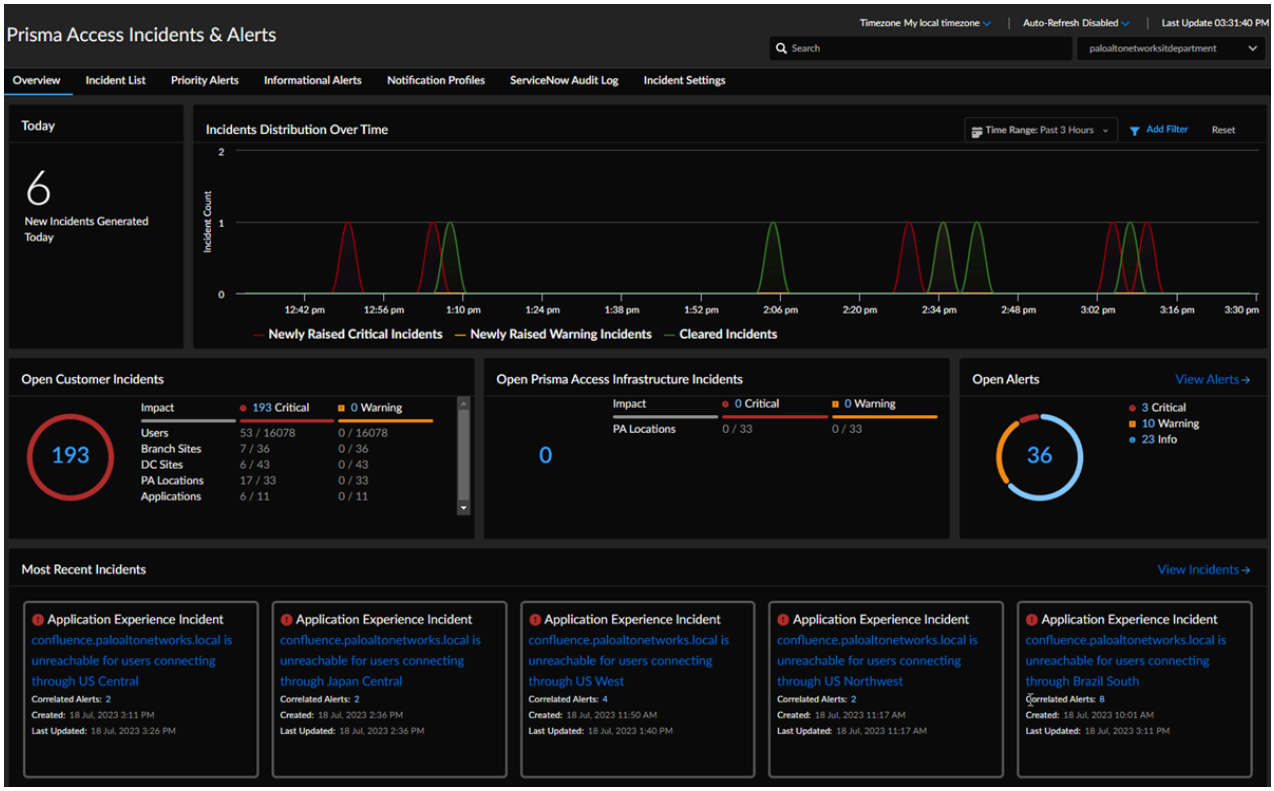
す。このようにイベントを1つのアラートに集約することで、トリアージ、チーム間でのアラートハンドオフの効率化、重要情報の一元化、通知の疲労軽減などを実現します。

[Incidents & Alerts (インシデントとアラート**)]** > **[NGFW]** > **[All Incidents (**すべてのインシデント**)]** に移動して、ネットワーク全体のアラートを表示し、インシデントとやり取りします。

インシデントとアラート:Prisma Access

どこで使用できますか?	何が必要ですか?
• Prisma Access （*Strata Cloud Manager*または*Panorama*の設定管理付き）	❑ AI-Powered ADEMライセンス ❑ ADEM Observabilityライセンス ❑ Prisma Accessライセンス

[Incidents & Alerts (インシデントとアラート)] > **[Prisma Access Incidents & Alerts (Prisma Accessインシデントとアラート)]**を選択して開始します。環境で使用できるインシデントとアラートは、ライセンスによって異なります。



概要を見る

Prisma Access環境に関連するインシデントとアラートのOverview (概要)情報を参照してください。環境で使用できるインシデントとアラートは、ライセンスによって異なります。

すべてのインシデントを見る

[Incident List (インシデントリスト)]を表示します。環境内のすべてのインシデントが表示されます。**[Add Filter (フィルターを追加)]** ドロップダウンを使用して、表のカラムで ［Incidents

(インシデント)] を選択します（複数のカラムでフィルタリングできます）。表内から任意の**[Incident (インシデント)]**を選択すると、インシデントの詳細情報が表示されます。

優先アラートの表示

Prisma Access環境のステータスを示す[Priority Alerts (優先アラート)]を参照してください。

情報アラートの表示

[Informational Alerts (情報アラート)]の表示。今後のソフトウェアアップグレードと、実行中または完了したアップグレードのステータスを通知します。

通知プロファイル

[Notification Profiles (通知プロファイル)]から、**Notification Subscriptions (**通知サブスクリプション**)**に関する情報の表示や、**[Notification Profile (**通知プロファイル**)]**の新規作成または既存の変更を行うことができます。

ServiceNow 監査ログ

ServiceNowを使用している場合は、ServiceNowの各インシデント**ID**を示すServiceNow監査ログを確認できます。また、インシデントごとに実行されるServiceNowの操作（作成、更新、削除など）も表示されます。

インシデント設定

[Incident Settings (インシデント設定)]から、受信するインシデントをインシデントカテゴリとインシデントコードでカスタマイズできます。

コード別のインシデントとアラート

インシデントとアラートをコードID別に表示し、それらが説明する問題と問題点を把握して、修正方法を見つけます。インシデントとアラートはライセンス別に分類されます。

- AIを活用したADEMインシデント
- ADEMインシデント
- Prisma Accessインシデント
- 優先アラート
- 情報アラート

インシデントとアラートについては、「インシデントとアラートのリファレンスガイド」を参照してください。

ServiceNowとの連携については 、「*Integrations Guide (*統合ガイド*)*」の「ServiceNowとPrisma Accessの統合」を参照してください。

インシデントとアラート:Prisma SD-WAN

どこで使用できますか?	何が必要ですか?
• Prisma SD-WAN	☐ Prisma SD-WANライセンス

Prisma SD-WANは、システムがシステム定義または顧客が定義したしきい値に達した場合、またはシステムに障害が発生した場合にインシデントとアラートを生成します。これらのインシデントとアラートを使用して、システムをトラブルシューティングします。

[Incidents and Alerts (インシデントとアラート)] > **[Prisma SD-WAN]**を選択すると、Strata Cloud Manager内のインシデントとアラートが表示されます。

Prisma SD-WANのインシデントやアラートをナビゲートするには、以下のタブを使用します。

- 概要
- インシデント
- アラート
- 設定

概要

Prisma SD-WANでインシデントやアラートとそのカテゴリを表示します。**[Overview (概要)]**タブがデフォルトのビューです。

次の情報を表示する上位インシデントとアラートを表示します。

インシデントの種類	インシデントのカテゴリを表示します。
詳説	インシデントの説明を表示します。
重要度	インシデントの重大度を表示します。
優先順位	インシデントの優先度を表示します。
相関アラート	このインシデントで集計されたインシデント数を表示します。
ステータス	インシデントのステータスを表示します。
作成済	システムによってインシデントが発生した時刻が表示されます。
最終更新	システムによってインシデントが最後に更新された日時が表示されます。

インシデント

インシデントとは、システムの障害を示すものです。インシデントの発生とクリアは、重大度によって異なります。

- 重大 – ネットワークの全体または一部がダウンしており、迅速な対応が必要です。
- 警告 – ネットワークに影響を与えるため、早急な対応が必要です。
- 情報 – ネットワークは機能が低下しており、すぐに注意する必要があります。

アラート

アラートは、ネットワークの障害を示す場合とそうでない場合があります。システムがシステム定義またはカスタマー定義のしきい値に達するとアラートが発生します。

設定

[Settings (設定)]タブを使用して、設定された指定された分類とアクション属性に基づいてイベントコード抑制を管理するインシデントポリシーを作成します。インシデントポリシー ルールを使用して、スケジュールされた期間中に発生したインシデントを抑制またはエスカレーションできます。さらに、システム生成インシデントのデフォルト優先度を、ビジネス要件により近い優先度レベルに変更することもできます。

インシデントとアラート:ログ ビューアー

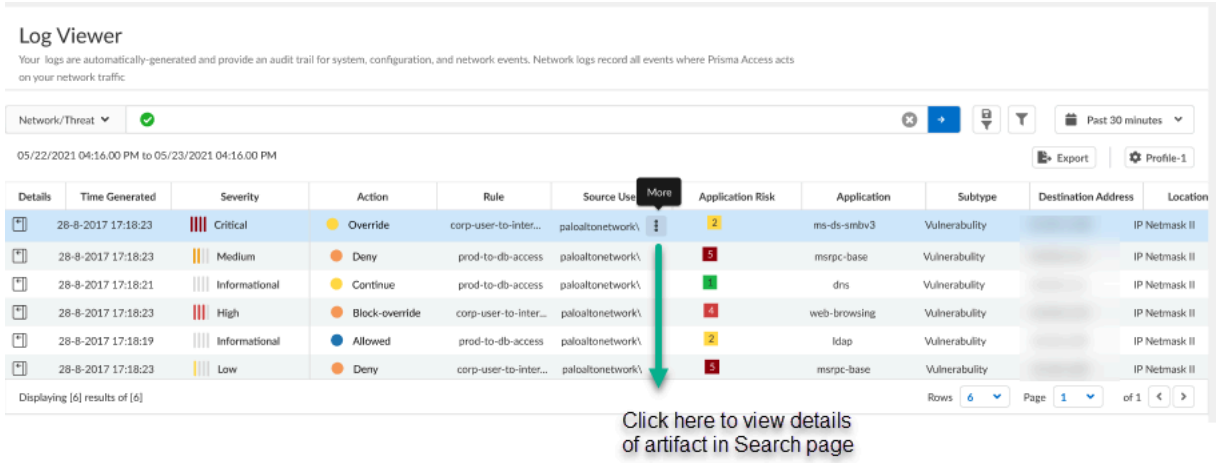
どこで使用できますか?	何が必要ですか?
• Prisma Access （*Strata Cloud Manager*または*Panorama*の設定管理付き） • Software NGFW Creditsによって資金提供されたものを含むNGFW	❑ これらの各ライセンスには、Strata Cloud Managerへのアクセスが含まれています。 ❑ Prisma Access ❑ AIOps for NGFW Premium license (use the Strata Cloud Manager app) または AIOps for NGFW Free (use the AIOps for NGFW Free app) ❑ Strata Cloud Manager Essentials ❑ Strata Cloud Manager Pro ❑ ダッシュボードを表示する権限を持つロール

ログビューアはExplore の機能を提供します。ログビューアでは、保存されているログを表示したり操作したりできます。 Strata Logging Service。

Log Viewer (ログビューア**)**では、システム、設定、およびネットワークイベントの監査証跡を実施できます。ダッシュボードからログに移動して詳細を取得し、調査結果を調査します。クエリフィールドと時間範囲の設定により、関心のある特定のログを絞り込むことができます。

- クエリの作成方法の詳細
- ログビューアの新機能については、 Strata Logging Serviceリリースノートをご覧ください。

ログ ビューアは、 ログのアクションと重大度を強調表示し、セッションがどのように実施されているかを理解するのに役立ちます。検索 ページでログのセキュリティ アーティファクトの詳細を表示することもできます。



* 次のログ タイプとログ フィールドの詳細は、検索で表示できます。

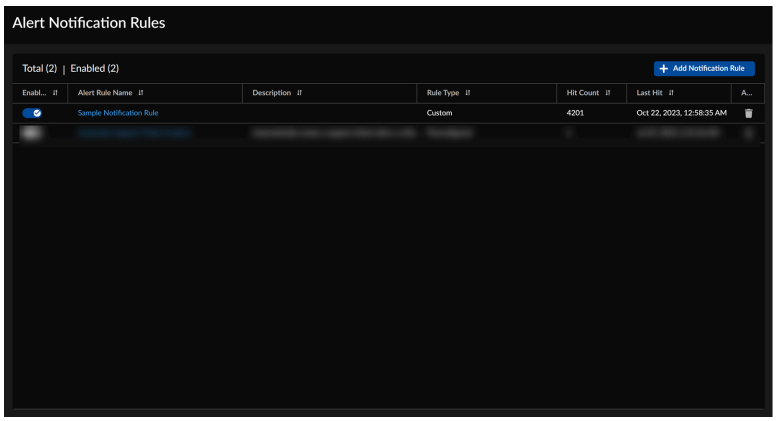
ログ タイプ	列名
トラフィック、脅威、URL、ファイル	• 送信元アドレス • 宛先アドレス • NAT送信元 • NAT宛先
脅威、ファイル	ファイルハッシュ
URL	• URL • URLドメイン
DNS セキュリティ	• 送信元アドレス • 宛先アドレス • ドメイン • FQDN

インシデントとアラートの設定

どこで使用できますか?	何が必要ですか?
• Software NGFW Creditsによって資金提供されたものを含むNGFW	❑ AIOps for NGFW Free (use the AIOps for NGFW Free app) または AIOps for NGFW Premium license (use the Strata Cloud Manager app) ❑ Strata Cloud Manager Essentials ❑ Strata Cloud Manager Pro

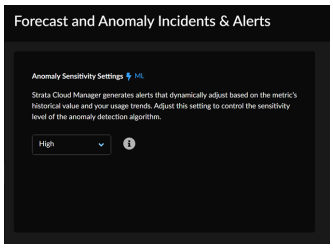
- 通知をトリガーするアラート、通知の受信方法、受信頻度など、通知の環境設定を定義し、通知ルールを作成します。

  [Incidents & Alerts (インシデントとアラート)] > **[Incident & Alert Settings (インシデントとアラート設定)]** > **[Notification Rules (通知ルール)]**に移動して、通知をトリガーするルールを表示および追加します。



- Strata Cloud Managerは、メトリックの履歴値と利用傾向に基づいて動的に調整するアラートとインシデントを生成します。この設定を調整して、異常検知アルゴリズムの感度レベルを制御できます。

  [Incidents & Alerts (インシデントとアラート)] > **[Incident & Alert Settings (インシデントとアラート設定)]** > **[Anomaly Sensitivity (異常感度)]**に移動して、異常検出アルゴリズムの感度レベルを設定します。

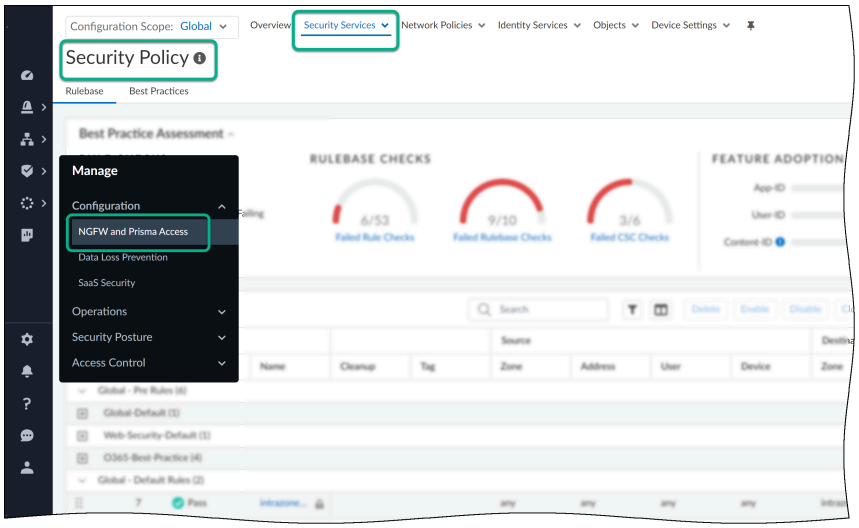


管理:NGFW と Prisma のアクセス

どこで使用できますか?	何が必要ですか?
• Prisma Access (Managed by Panorama or Strata Cloud Manager) • Software NGFW Creditsによって資金提供されたものを含むNGFW	これらの各ライセンスには、Strata Cloud Managerへのアクセスが含まれています。 ❑ Prisma Access ❑ AIOps for NGFW Premium ❑ Strata Cloud Manager Essentials ❑ Strata Cloud Manager Pro → Strata Cloud Managerで利用できる機能は、使用するライセンスによって異なります。

Strata Cloud Managerを使用すると、NGFWおよびPrisma Access全体で共有セキュリティポリシーを設定できます。開始するには、次の手順を実行します。

- ❑ Prismaアクセス、NGFW、またはその両方をStrata Cloud Managerでセットアップします。
- ❑ 同様の設定が必要なNGFWをグループ化するフォルダをセットアップします。Prisma Accessフォルダは事前定義されており、モバイルユーザー、リモートネットワーク、サービス接続といったデプロイメント タイプに基づいて対象設定を行うことができます。
- ❑ 作業する管理:設定スコープを設定します。NGFWとPrisma Access環境の両方でグローバルに適用される設定を構成したり、フォルダに基づいて特定のNGFWまたはPrisma Accessのデプロイメントに設定をターゲットすることもできます。
- ❑ 管理:スニペットを使用して、NGFW またはデプロイメントのセットの共通基本設定を標準化します。スニペットを使用することで、新しいデバイス、ユーザー、またはロケーションを、既知の良好な設定で迅速にオンボードすることができ、新しいデバイスのオンボードに必要な時間を短縮できます。
- ❑ **[Manage (管理)] > [Configuration (設定)] > [NGFWとPrisma Access]**からセキュリティ ポリシーの作成を開始し、前述の管理機能を使用してNGFWとPrisma Access間で共有します。



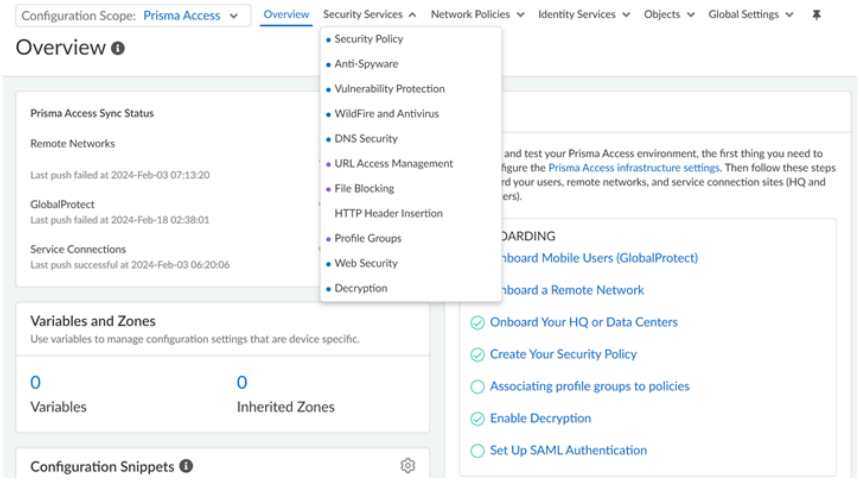
管理:設定スコープ

どこで使用できますか?	何が必要ですか?
• Prisma Access (Managed by Panorama or Strata Cloud Manager) • Software NGFW Creditsによって資金提供されたものを含むNGFW	これらの各ライセンスには、Strata Cloud Managerへのアクセスが含まれています。 ❑ Prisma Access ❑ AIOps for NGFW Premium ❑ Strata Cloud Manager Essentials ❑ Strata Cloud Manager Pro → Strata Cloud Managerで利用できる機能は、使用するライセンスによって異なります。

Strata Cloud Managerを使用すると、環境全体に構成設定を適用してポリシーをグローバルに適用することも、組織 の特定の部分に設定とポリシーを適用することもできる。お使いのStrata Cloud Manager設定管理では、現在の 設定スコープ が常に表示され、ビューを切り替えることで、より広範囲またはより詳細な構成を管理できます。

特定の構成スコープに適用可能な構成要素と、それらが共通の構成スコープから継承されたものか、システムによって生成されたものかを明確にすることができます。色分けされた構成インジケーターは、構成がどこから継承されているかを理解するのに役立つだけでなく、オブジェクトタイプを視覚的に区別して簡単にスキャンすることができます。

- 灰色の点は継承された設定を示します
- 紫色の点は定義済みの設定を示します
- 青色の点はオブジェクトが現在の設定スコープ内に存在することを示します



グローバル 構成設定を使用すると、すべてのネットワーク トラフィックに適用されるポリシー要件を簡単に管理および適用できます。あるいは、ポリシーと構成設定を、適切なデプロイメントの種類にターゲットを絞ることもできます。

- **Prisma Access**
  - モバイル ユーザー コンテナ– 設定はすべてのモバイル ユーザー接続タイプに適用されます。GlobalProtect と Explicit Proxy、または各接続タイプに個別に適用します。
  - リモート ネットワーク– 設定はリモート ネットワーク サイト (支社、小売店など) に適用されます。
  - サービス接続– 設定はサービス接続サイト (HQ およびデータ センター) に適用されます。
- すべてのファイアウォール – 設定はすべての NGFW に適用されるか、共有または特定の構成設定やポリシーの適用を必要とする NGFW をグループ化した特定のフォルダーに適用されます。

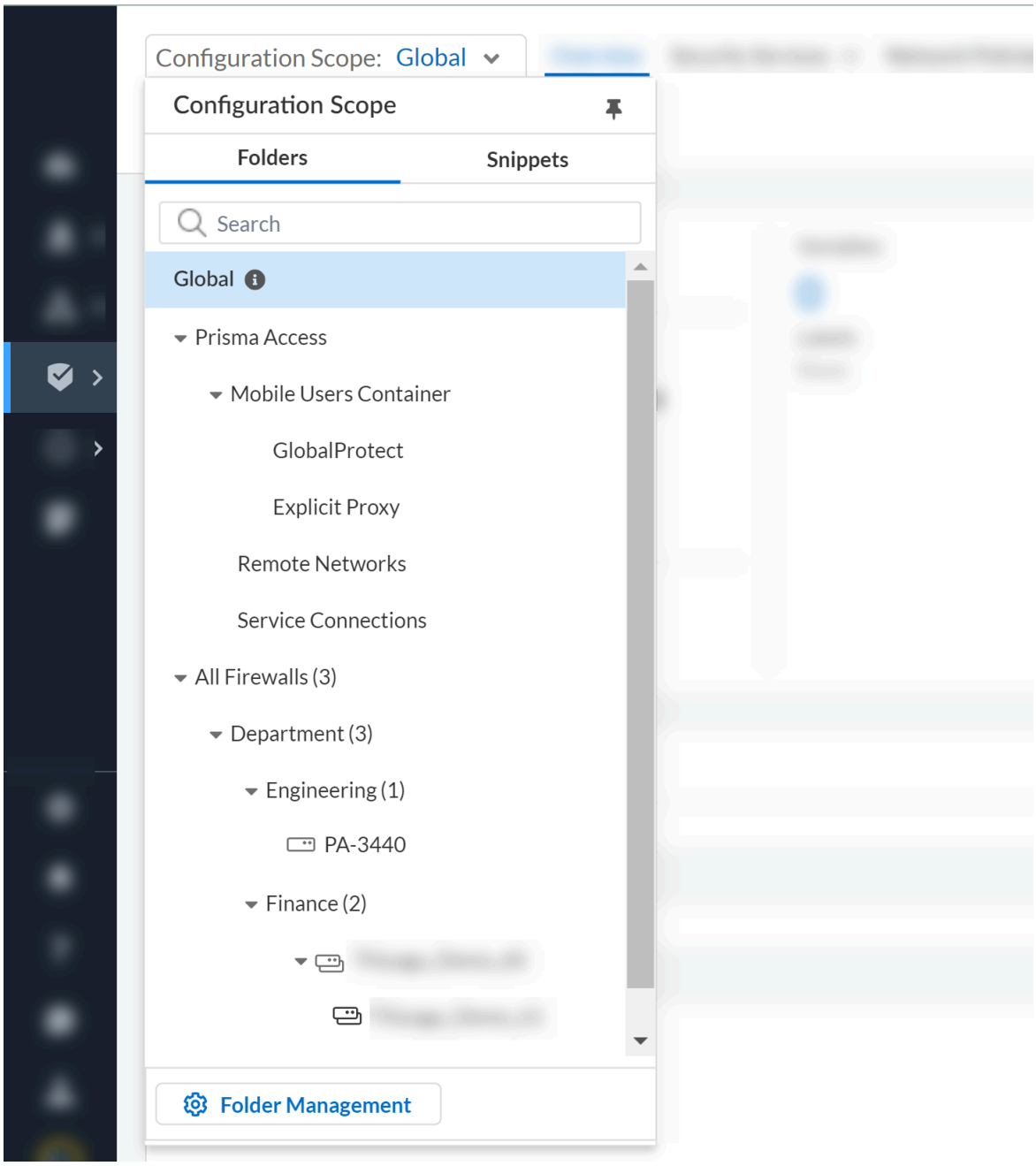
詳細については以下をご覧ください。

- ワークフロー:フォルダ管理

  フォルダーを使用してデバイスとデプロイメントタイプを論理的にグループ化し、設定管理を簡素化します。
- 管理:スニペット

  スニペットを使用して設定をグループ化し、ファイアウォールまたはデプロイメントにすばやくプッシュできます。
- 管理:変数

  デバイスまたはデプロイメント固有の設定オブジェクトに対応するために、設定に変数を使用します。



管理:スニペット

どこで使用できますか?	何が必要ですか?
• Prisma Access (Managed by Panorama or Strata Cloud Manager) • Software NGFW Creditsによって資金提供されたものを含むNGFW	これらの各ライセンスには、Strata Cloud Managerへのアクセスが含まれています。 ❑ Prisma Access ❑ AIOps for NGFW Premium ❑ Strata Cloud Manager Essentials

どこで使用できますか?	何が必要ですか?
	❑ Strata Cloud Manager Pro → Strata Cloud Managerで利用できる機能は、使用するライセンスによって異なります。

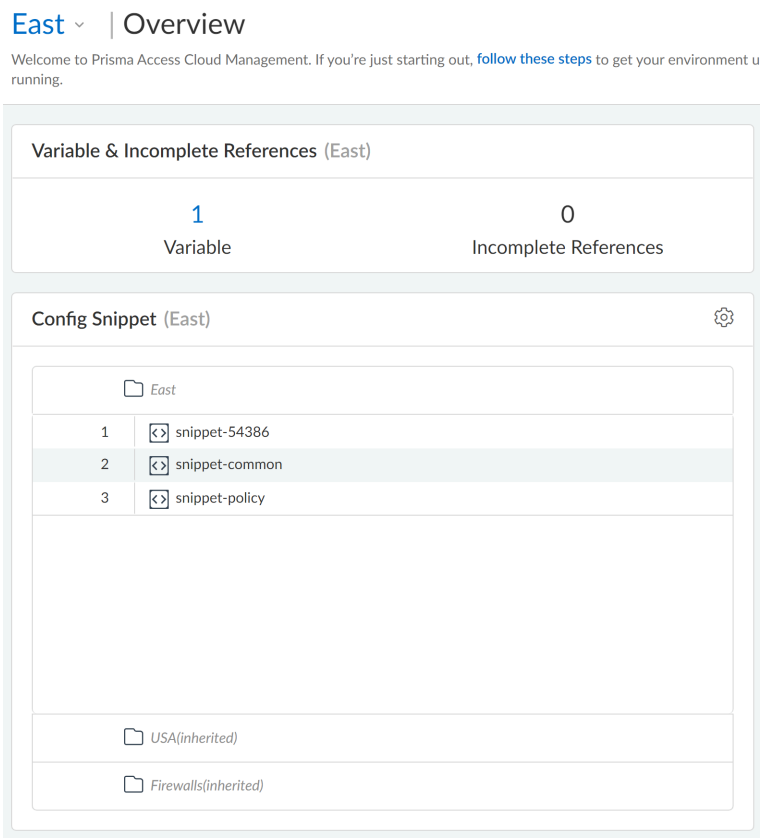
スニペットを使用して設定をグループ化し、ファイアウォールまたはデプロイメントにすばやくプッシュできます。

スニペットは、フォルダー、デプロイメント、またはデバイスに関連付けることができる設定オブジェクトであり、階層や設定オブジェクトのグループには収まりません。スニペットを使用すると、一連のファイアウォールやデプロイメントの共通の基本設定を標準化できます。これにより、既知の良好な設定で新しいデバイスをすばやくオンボーディングでき、新しいデバイスのオンボーディングに必要な時間を短縮できます。たとえば、リモートの支社に新しいファイアウォールを導入できます。必要なネットワークとポリシー ルールの設定をすべて含むスニペットのセットを、新しいファイアウォールが属するフォルダに関連付けることができます。これにより、リモートブランチオフィスを保護するためのファイアウォールのセットアップに必要な時間が短縮されます。

オブジェクト値が競合する場合、スニペットの関連付けはトップダウン優先になります。名前が重複したルールは許可されず、任意のフォルダーで同じ名前のスニペットを作成するとき、または同じ名前のスニペットが既に関連付けられている場合はスニペットをフォルダーに関連付けるときに検証が失敗します。

つまり、最初と最後に関連付けられたスニペットの値が同じオブジェクトで異なる場合、最初のスニペットの値がデバイスまたはデプロイメントに継承されます。さらに、スニペットから継承されたすべての設定は、子フォルダー、デプロイメント、またはデバイスレベルでオーバーライドできます。

フォルダ階層内では、スニペットを任意のフォルダ階層内で一度だけ関連付けることができます。つまり、スニペットをフォルダーとその下にネストされているフォルダーの両方に関連付けることはできません。ただし、同じスニペットを別のフォルダーまたは別のフォルダーにネストされたフォルダーに関連付けることができます。フォルダー階層内のフォルダーに既に関連付けられているスニペットはグレー表示され、該当する場合は複数回使用できません。



スニペットにおけるクロススコープ構成の参照性

この機能により、グローバルスコープにアタッチされている一般的な構成やオブジェクトを参照して、Prisma AccessやNGFWファイアウォールにプッシュすることができます。グローバルスコープ内のこれらの共有オブジェクトと設定は、すべてのスニペットで使用できます。グローバルスコープに関連付けられたスニペットは、グローバルスニペットと見なされます。グローバルスコープにアタッチされたこれらのスニペット内で定義されたオブジェクトは、設定内のどのスニペットでも参照できます。

たとえば、Global Variableという名前のスニペットを作成して変数を統合し、グローバルスコープにアタッチできます。これにより、設定内の他のすべてのスニペットを簡単に参照して利用できるようになります。同様に、アクセスポリシー ルール、脅威防御プロファイル、ゾーン、アドレス、および標準ネットワークセグメントを表すその他のオブジェクトのカスタムURLカテゴリを効果的に管理できます。

スニペットを作成する

スニペットを作成してフォルダー、デプロイメント、またはデバイスに関連付けて、共通の基本設定をデバイスのグループに適用します。必要な数だけスニペットをフォルダー、デプロイメント、またはデバイスに関連付けることができます。

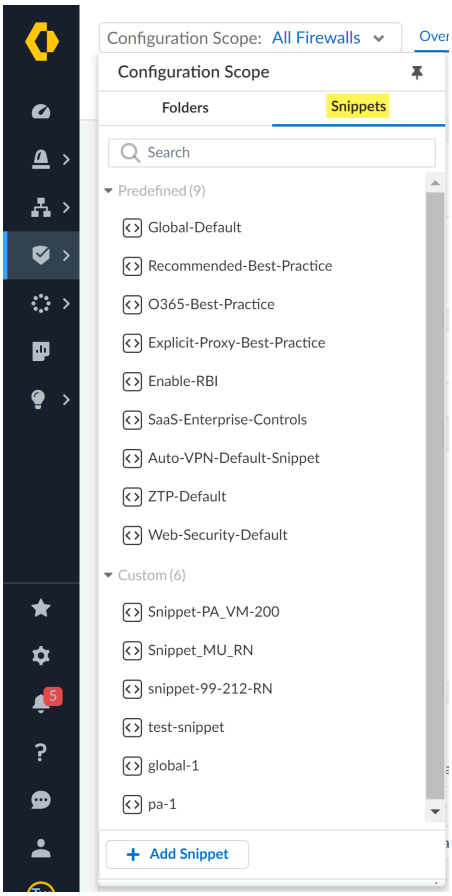
スニペットは、作成後いつでも変更して任意のフォルダー、デプロイメント、またはデバイスに再関連付けることができます。

使用されなくなったカスタムスニペットは削除できます。

STEP 1 | Strata Cloud Managerにログインします。

STEP 2 | **[Manage (管理)]** > **[Configuration (設定)]** > **[NGFWとPrisma Access]** > **[Overview (概要)]**を選択し、設定スコープを展開して**[Snippets (スニペット)]**を表示します。

STEP 3 | スニペットを追加します。

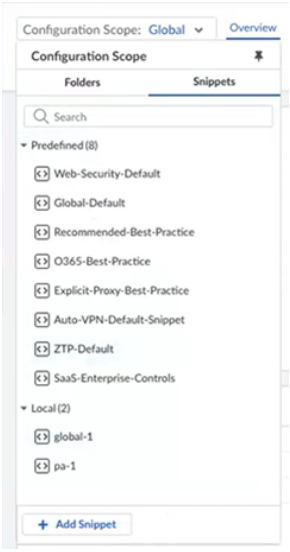


STEP 4 | スニペットを作成します。

1. スニペットに分かりやすい名前を付けます。
2. （任意）スニペットの**Description**（説明）を入力します。
3. （任意）必要に応じて、1つ以上の**Labels (**ラベル**)**を割り当てます。

   既存のラベルを選択するか、作成したいラベルを入力して新しいラベルを作成できます。
4. **Create**（作成）を選択します。

   新しく作成されたスニペットは、ローカルスニペットに分類されて一覧表示されます。スニペットが公開されると、「公開済みスニペット」に移動されます。



STEP 5 | スニペット設定を作成します。

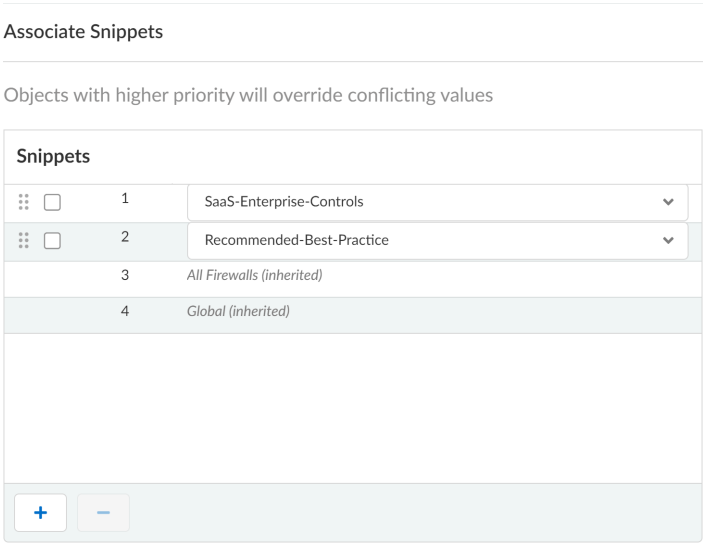
これで、スニペットの設定スコープになりました。スニペットスコープ内で作成したすべての設定は、スニペットに対してのみ適用されます。

スニペットスコープでは、スニペットの概要を確認してスニペットに関する詳細情報を確認できます。これには、変数の数、スニペットの作成と最終更新に関する情報、スニペットが関連付けられているすべてのフォルダー、デプロイメント、デバイスのリストなどの情報が含まれます。

STEP 6 | スニペットを関連付けます。

1. **[Manage (管理)] > [Configuration (設定)] > [NGFWとPrisma Access] > [Overview (概要)]**を選択し、設定スコープを展開して**[Config Tree (設定ツリー)]**を表示します。
2. スニペットを関連付けるフォルダー、デプロイメント、またはデバイスを選択します。
3. 設定スニペットを編集します。
4. 関連付けたいスニペットを追加し、必要に応じて並べ替えます。

   スニペットをグローバルスコープに関連付けると、そのスニペットは設定内の他のすべてのスニペットで参照可能になり、使用できるようになります。すべてのスニペットは、グローバルフォルダに添付されたスニペット内のオブジェクトを参照できます。
5. 閉じる。



STEP 7 | **Push Config (設定をプッシュする)** を使用して設定の変更をネットワークにプッシュします。

スニペットを変更

スニペットの設定、詳細、および関連付けを変更します。

フォルダー、デプロイメント、またはデバイスに関連付けられなくなったカスタムスニペットは削除できます。

STEP 1 | Strata Cloud Managerにログインします。

STEP 2 | **[Manage (管理)] > [Configuration (設定)] > [NGFWとPrisma Access] > [Overview (概要)]**を選択し、設定スコープを展開して**[Snippets (スニペット)]**を表示します。

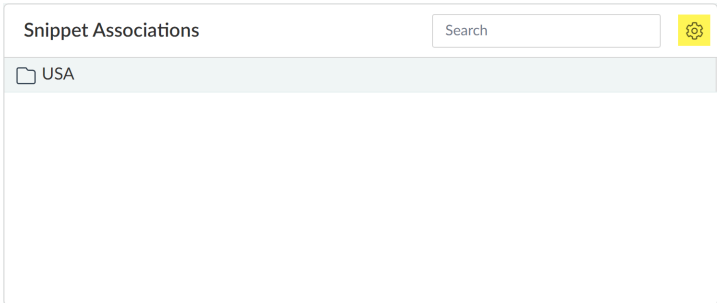
STEP 3 | 変更するスニペットを選択します。

スニペットを選択すると、スニペットの概要にリダイレクトされます。

STEP 4 | (任意) スニペットを編集して、名前や説明を変更したり、追加のラベルを変更または割り当てたりします。**Pause Update (更新をプッシュ)** を有効または無効にして、設定の相違点を確認し、変更を受け入れることを決定します。

STEP 5 | **Snippet Associations (**スニペット アソシエーション**)**を編集して、スニペットを別のフォルダー、デプロイメント、またはデバイスに再関連付けたり、スニペットを追加のフォルダー、デプロイメント、またはデバイスに関連付けたりします。

スニペット再関連付け画面を終了して変更を適用します。



STEP 6 | 必要に応じてスニペット設定を変更します。

STEP 7 | 構成をプッシュします。

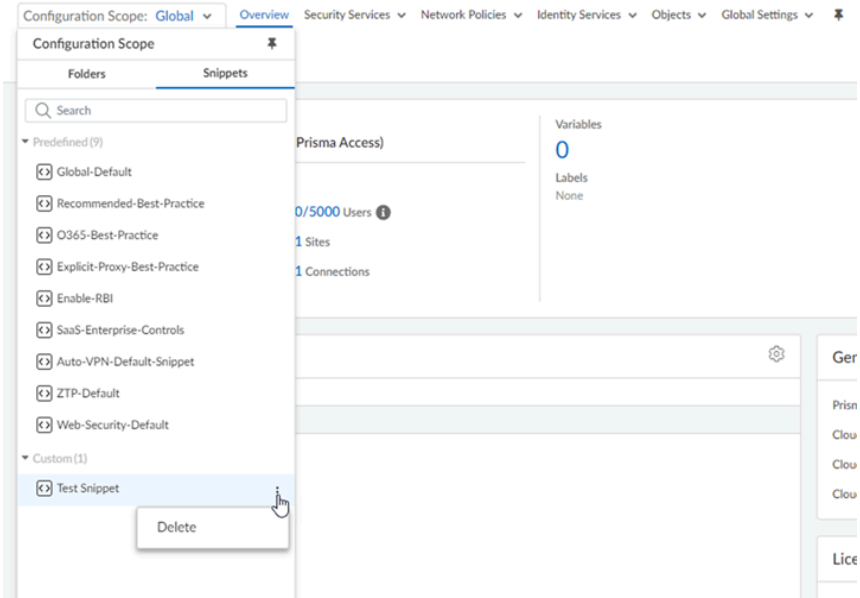
スニペットを削除する

カスタムスニペットを削除して、設定を整理しておいてください。スニペットは、削除する前にファイアウォール、フォルダー、またはデプロイメントとの関連付けを解除する必要があります。事前定義済みのスニペットの削除はサポートされていません。

STEP 1 | Strata Cloud Managerにログインします。

STEP 2 | **[Manage (**管理**)] > [Configuration (**設定**)] > [NGFW**と**Prisma Access] > [Overview (**概要**)]**を選択し、設定スコープを展開して**[Snippets (**スニペット**)]**を表示します。

STEP 3 | 削除するカスタムスニペットの縦の3つの点をクリックします。



STEP 4 | スニペットを削除します。

現在フォルダー、デプロイメント、またはデバイスに関連付けられているスニペットは削除できません。削除する前に、まず***Snippet Associations (***スニペットアソシエーション**)**を編集して既存の関連付けをすべて削除します。

スニペットを複製する

既存のスニペットを新しいスニペットのテンプレートとして使用する場合は、簡単に複製できるので、新しいオブジェクトを設定する必要はありません。

複製されたスニペットはデバイス、フォルダー、デプロイメントに関連付けられていないため、設定を開始する前に関連付けを解除しなくても自由にカスタマイズできます。

STEP 1 | Strata Cloud Managerにログインします。

STEP 2 | **[Manage (管理)]** > **[Configuration (設定)]** > **[NGFW**と**Prisma Access]** > **[Overview (概要)]**を選択し、設定スコープを展開して**[Snippets (**スニペット**)]**を表示します。

STEP 3 | クローンしたいカスタムスニペットの縦に3つ並んだ点をクリックします。

STEP 4 | スニペットを複製します。

1. (任意) 複製したスニペットに新しい名前を付けます。

スニペット設定の共有

この機能は、マルチテナント環境を含むすべてのテナント間で共通の設定を共有するためのユニークで柔軟な方法を提供します。さまざまな設定をスニペットとして保存および管理し、顧客アカウントのテナント間で簡単に共有できます。この機能により、さまざまなテナント環境にわたる共有設定の管理において、かなりの柔軟性と制御が可能になります。

さらに、この機能は、テナント間の一般的なシナリオの設定管理の一元化と、マルチビジネスユニットセットアップ内のグローバル設定の監視をサポートします。

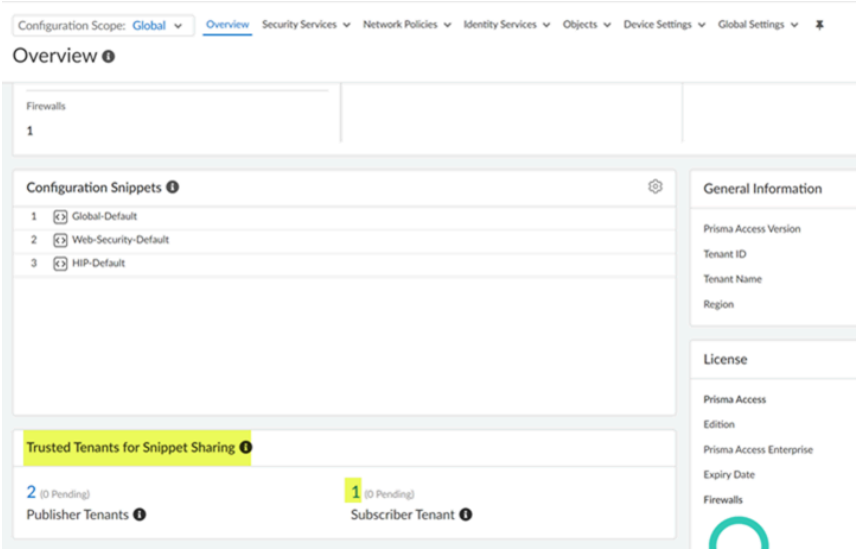
このフレームワークでは、パブリッシャーテナントはサブスクライバーテナントとスニペットを共有し、サブスクライバーテナントはパブリッシャーテナントからスニペットを受け取ります。

STEP 1 | Strata Cloud Managerにログインします。

STEP 2 | パブリッシャーテナントで、**[Manage (管理)]** > **[Configuration (設定)]** > **[FGFW**と**Prisma Access]** > **[Overview (概要)]** を選択し、**[Global (**グローバル**)]**構成スコープを選択します。

STEP 3 | テナント間の信頼の確立:サブスクライバーテナントとパブリッシャーテナント間の接続を確立して、スニペットを共有できるようにします。

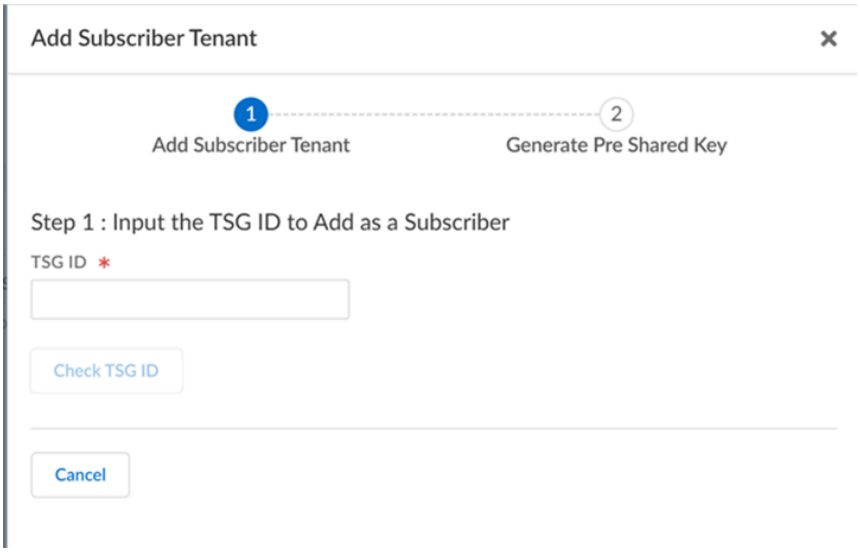
1. **[Trusted Tenants for Snippet Sharing (**スニペット共有のための信頼できるテナント**)]** の下の **[Subscriber Tenant (**サブスクライバーテナント**)]** をクリックします。



2. サブスクライバーテナントを追加します。

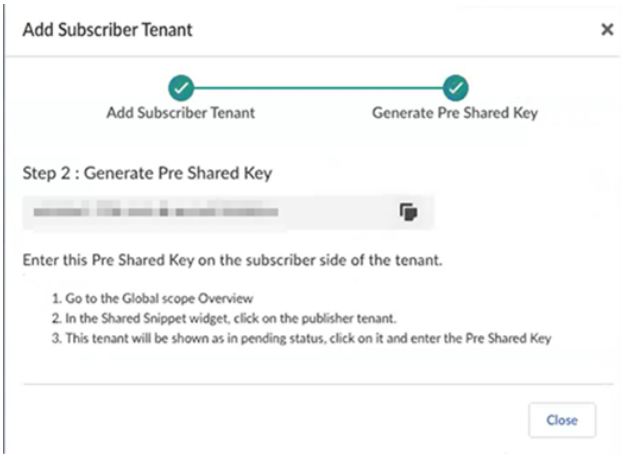
3. サブスクライバーテナントとして追加する**TSG ID**を入力し、**TSG ID**を確認します。これにより、ランダムに生成されたTSG攻撃やシリアル化されたTSGベースの攻撃を確実に防ぐことができます。

   検証が成功すると、TSD IDが検証されたことを示す確認メッセージが表示されます。



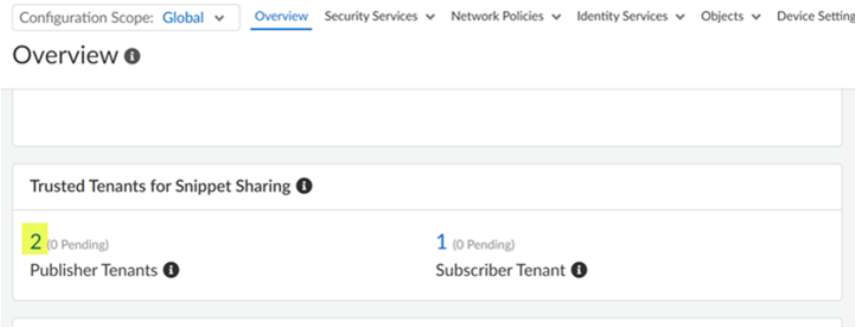
4. **[Next (**次へ**)]:**事前共有キーを生成します。

生成された PSK をコピーします。このPSKは、ステップ4でパブリッシャテナントを検証するときに入力します。



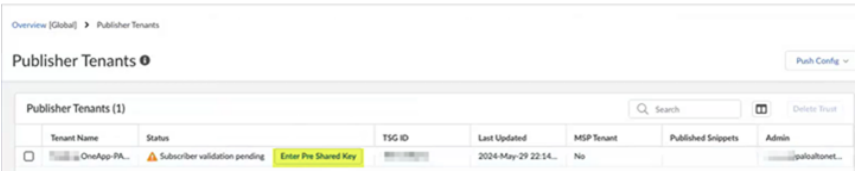
STEP 4 | サブスクライバー テナントに移動し、**[Manage (管理)]** > **[Configuration (設定)]** > **[NGFWとPrisma Access]** > **[Overview (概要)]**を選択し、設定スコープを**[Snippets (スニペット)]**に設定します。

1. **[Trusted Tenants for Snippet Sharing (スニペット共有用の信頼できるテナント)]**の **[Publisher Tenants (パブリッシャーテナント)]** ステータスが **[Pending (保留中)]** と表示されます。



2. **[Publisher Tenants (パブリッシャーテナント)]** をクリックし、前のステップで生成された事前共有キーを入力して、サブスクライバーテナントを検証します。

   検証が成功すると、テナントが信頼できることを確認するメッセージが表示され、サブスクライバーテナントとパブリッシャーテナント間の信頼が確立されます。



STEP 5 | スニペットをサブスクライバーテナントに公開します。

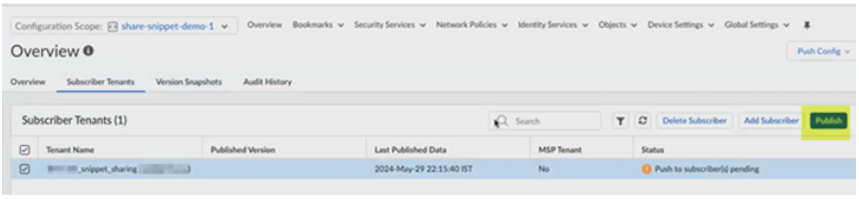
1. スニペットを作成してフォルダに関連付けます。

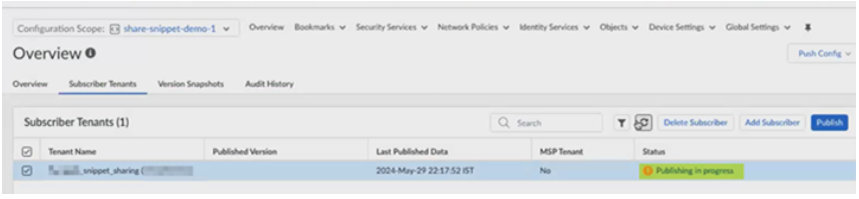
   新しく作成されたスニペットは、ローカルスニペットに表示されます。

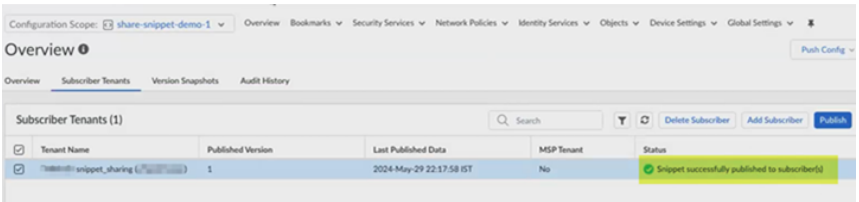
   - **[Overview (概要)]**タブには、名前、説明、作成時間（スニペットがサブスクライバー側に読み込まれた日時）、最終更新時間、ラベルの詳細などのスニペットの詳細が表示されます。
   - **[Subscriber Tenants (サブスクライバーテナント)]** タブには、テナント名、テナントで公開されているバージョン、最終公開日、および公開ステータスが表示されます。
     - 設定の変更を確認するには、**[Published Version (公開バージョン)]**をクリックします。
     - スニペットをテナントに公開する前に、サブスクライバーを追加して保存します。
   - バージョンスナップショットには、スニペット設定の履歴が表示されます。この画面では、設定スナップショットを候補設定と比較したり、候補としてバージョンスナップショットを保存または以前の設定スナップショットをロードできます。バージョン番号をクリックすると、設定の違いが表示されます。
   - 監査履歴には、管理者が開始したすべてのアクションの監査記録が表示されます。公開されたバージョン番号、加えられた変更、変更の所有者、変更の日時、変更の詳細などの詳細が記録されます。

2. **[Subscriber Tenant (サブスクライバーテナント)]** タブで、テナント名を選択し、**[Publish (公開)]** を選択します。

   これにより、パブリッシュリクエストがサブスクライバーテナントに送信されます。ステータス列には、「スニペットがサブスクライバーに正常に公開されました」と表示され、スニペットは「公開済みスニペット」に表示されます。







STEP 6 | サブスクライバーテナントで確認します。

1. **Overview (概要) > Configuration Scope (設定スニペット) > Snippets (スニペット)**に移動し、「サブスクリプション済みスニペット」でスニペットを選択します。

   パブリッシャーテナントの名前、説明、TSG ID、スニペットの作成時間、最終更新時間、ラベル、更新の一時停止の詳細などの詳細を表示するスニペット概要にリダイレクトされます。

STEP 7 | トラストを削除します。

フォルダまたはファイアウォールに関連付けられているサブスクライブされたスニペットは複製のみ可能で、削除することはできません。

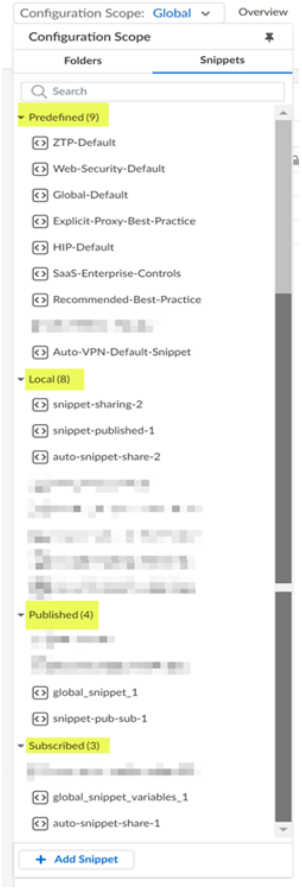
1. サブスクライバーまたはパブリッシャーテナントに移動します。
2. **[Trusted Tenants for Snippet Sharing (スニペット共有のための信頼できるテナント)]** の下の **[Subscriber Tenant (サブスクライバーテナント)]** をクリックします。
3. **[Tenant Name (テナント名)]**を選択し、**[Delete Trust (信頼を削除)]** を選択します。

トラストを削除すると、スニペットはファイアウォールまたはフォルダに関連付けられなくなり、ローカルスニペットになります。

スニペット分類

- 事前定義済みすべてのStrata Cloud Managerユーザーは、これらのスニペットにアクセスして、ベストプラクティス設定で新しいファイアウォールとデプロイメントをすばやくセットアップできます。
- ローカルこれらの編集可能なスニペットはテナント内で作成され、他のサブスクライバーテナントと共有することはできません。
- 公開済:信頼できるサブスクライバーテナントは、これらの共有スニペットにアクセスできますが、複製や編集はできません。

- 登録済みパブリッシャーテナントによって共有されるこれらのスニペットは、ユーザーが複製することはできますが、編集することはできません。



管理:変数

どこで使用できますか?	何が必要ですか?
• Prisma Access (Managed by Panorama or Strata Cloud Manager) • Software NGFW Creditsによって資金提供されたものを含むNGFW	これらの各ライセンスには、Strata Cloud Managerへのアクセスが含まれています。 ❑ Prisma Access ❑ AIOps for NGFW Premium ❑ Strata Cloud Manager Essentials ❑ Strata Cloud Manager Pro → Strata Cloud Managerで利用できる機能は、使用するライセンスによって異なります。

デバイスまたはデプロイメント固有の設定オブジェクトに対応するために、設定に変数を使用します。

変数は、設定を標準化すると同時に、デバイスやデプロイメント環境固有の固有の設定値に柔軟に対応できる高度なツールです。変数を使用すると、管理する必要のあるスニペットの数を減らしながら、必要に応じてファイアウォールやデプロイメント固有の設定値を維持できます。

たとえば、複数のネストされたフォルダに関連付けたい設定のスニペットがあり、各ネストされたフォルダには地理的な場所に固有のファイアウォールのセットが含まれているとします。このスニペットでは、特定のIP範囲のみのビジネス クリティカル システムへのアクセスを制限するポリシー ルールを設定しました。このシナリオでは、ネストされた各フォルダーに固有のIPアドレス範囲ごとに変数を作成し、その変数を継承されたスニペット設定で使用できます。これにより、デバイスまたはデプロイメント固有の設定値に対応するためのスニペットを減らしながら、設定変更を管理およびプッシュできます。

変数は、フォルダー、デプロイメント、またはファイアウォールレベルで作成できます。フォルダーの変数を作成すると、その変数はフォルダーの下にネストされているすべてのフォルダーに継承されます。フォルダーの設定スコープで変数が競合する場合、ファイアウォールまたはデプロイメントは、ネストされたフォルダーを含むフォルダーの変数値を継承します。ただし、継承された変数は、ネストされたフォルダー、デプロイメント、またはファイアウォールレベルでオーバーライドできます。

次のタイプの変数がサポートされています。

変数タイプ	詳説
AS 番号	BGP設定で使用する自律型システム番号。
数	アクションをトリガーするために発生する必要があるイベントの数。
デバイス**ID**	アクティブ/アクティブ高可用性 (HA) 設定でデバイス優先度値を割り当てるために使用するデバイス ID。
デバイス優先度	デバイス優先度は、アクティブ/パッシブ高可用性 (HA) 設定においてどのファイアウォールがアクティブな役割を果たすべきかを示すものです。
最大保証帯域 出口側	サービス品質（QoS）プロファイル設定で使用する出口最大値。
FQDN	完全修飾ドメイン名。
Group-ID	高可用性グループID。
IP ネットマスク	静的IPアドレスまたはネットワークアドレス。
IP範囲	IPアドレス範囲。例：**`192.168.1.10-192.168.1.20`**。
IP ワイルドカード	類似のIPアドレスを許可または拒否するIPワイルドカードマスク。 例：`10.0.0.5/255.255.0.255` 。

変数タイプ	詳説
Link Tag (リンクタグ**)**	SD-WAN設定で使用するリンクタグ。
パーセント	**0**から**99**の間のパーセンテージ。
ポート	送信元または宛先ポート。
QoSプロファイル	QoS設定で使用するためのQoSプロファイル。
レート	アクションをトリガーするしきい値を指定するレート。たとえば、DoSプロテクション プロファイルのアラームレート。
ルーター**ID**	ロジカルルーターにBorder Gateway Protocol (ボーダ ゲートウェイ プロトコル -BGP) を設定する場合のルーター ID。
タイマー	アクションをトリガーするしきい値を設定するための秒単位のタイマー。
ゾーン	セキュリティ ゾーン。

変数を作成する

変数がサポートされている場合は、変数をインラインで作成することもできます。

STEP 1 | Strata Cloud Managerにログインします。

STEP 2 | **[Manage (管理)]** > **[Configuration (設定)]** > **[NGFW**と**Prisma Access]** > **[Overview (概要)]** を選択し、変数を作成する設定スコープを選択します。

フォルダーで、変数を作成するフォルダーまたはデバイスを選択します。

スニペットで、変数を作成する特定のスニペットを選択します。

STEP 3 | [Variables (変数)]セクションで、表示されている変数カウントをクリックします。

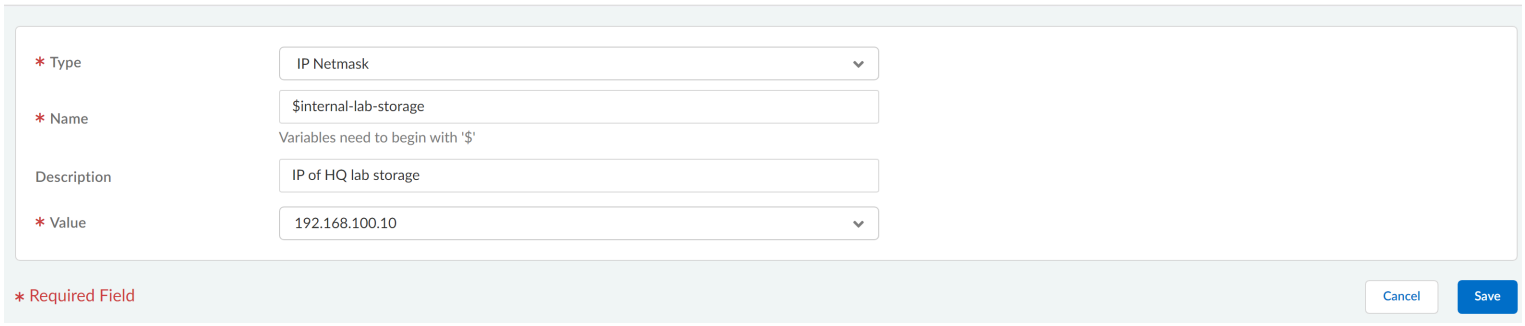
STEP 4 | 変数を追加します。

STEP 5 | 変数を作成します。

この例では、重要な内部リソースのアドレスオブジェクトとして使用する IP ネットマスク変数が作成されます。

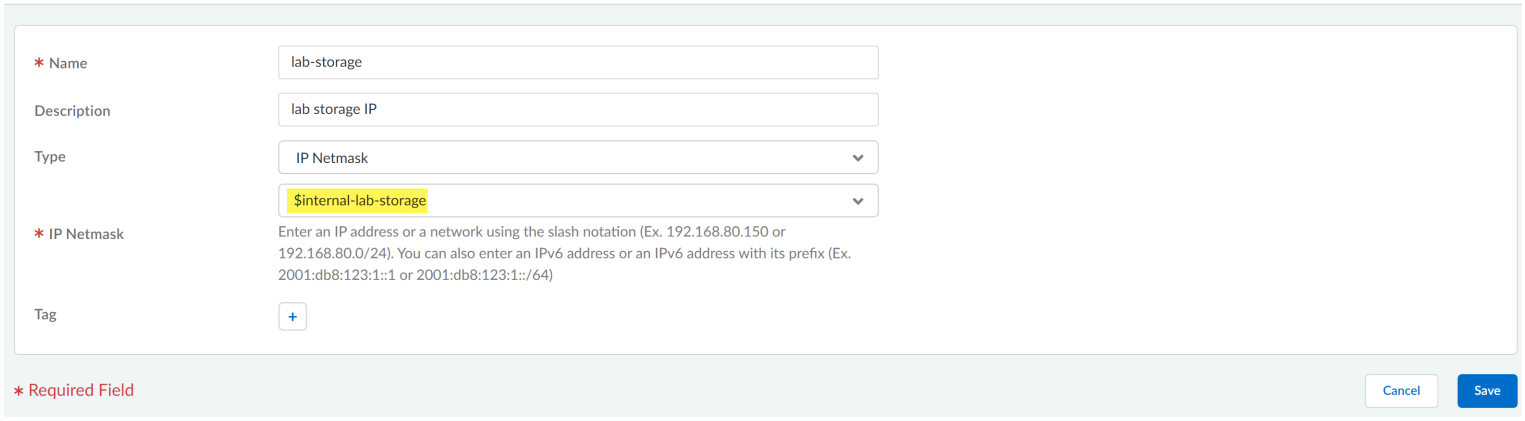
1. 変数タイプを選択します。
2. 変数に分かりやすい名前を付けます。

   すべての変数名は **$** で始まる必要があります。
3. （任意）変数の説明を入力します。
4. 変数 **Value (値)** を入力します。
5. **Save**（保存）を選択します。



STEP 6 | 変数を設定に追加します。

この例では、前のステップで作成した **$internal-lab-storage** 変数がアドレスオブジェクト設定に追加されます。



STEP 7 | **Push Config (構成をプッシュ)**します。

変数をインポートする

どこで使用できますか?	何が必要ですか?
• Strata Cloud Manager	❑ AIOps for NGFW Premiumライセンス ❑ Prisma Accessライセンス

CSVファイルを使用して変数をStrata Cloud Managerにインポートします。変数のインポートは、ファイアウォールによってフォルダー階層から継承された複数の変数、またはファイアウォールの設定スコープですでに設定されている複数の変数を、新しいファイアウォール固有の値で上書きするように設計されています。

変数は、フォルダー階層から既に継承されているか、変数のインポートを使用して上書きするようにファイアウォールの設定スコープで設定されている必要があります。変数をインポートしてまったく新しい変数を作成することはサポートされていません。

STEP 1 | Strata Cloud Managerにログインします。

STEP 2 | **[Manage (管理)]** > **[Configuration (設定)]** > **[NGFW and Prisma Access (NGFWとPrisma Access)]** > **[Overview (概要)]**を選択します。

STEP 3 | [Variables (変数)]セクションで、表示されている変数カウントをクリックします。

STEP 4 | **[CSV** エクスポート/インポート**]** > **[**エクスポート**]** を選択して、上書きする変数をエクスポートします。

Palo Alto Networksでは、最初に上書きしたい変数をエクスポートすることを推奨しています。これにより、Strata Cloud Managerにアップロードするcsvファイルが適切にフォーマットされていることが保証されます。これにより、ターゲットフォルダとファイアウォールの変数が正しく割り当てられるため、インポート処理も迅速になります。

STEP 5 | エクスポートされたCSVファイルの変数を変更します。

インポート用にCSVファイルを変更するときは、次の点を考慮してください。

- エクスポートされたCSVファイルの変更は、メモ帳などのシンプルなテキストエディタのみがサポートされています。
- # は、変数がフォルダー階層で作成され、ファイアウォールに継承されることを示します。

  # を削除すると、継承された変数値をファイアウォール固有の値でオーバーライドできます。

  ファイアウォール設定スコープでの変数値の上書きのみがサポートされているため、#が付加された変数値はインポート時にStrata Cloud Managerによって無視されます。
- -NA- は、変数がファイアウォール設定に存在しないことを示します。これは、変数がファイアウォールが属するフォルダ階層の外部で作成されたことを意味します。

  変数値を -NA- に変更することはサポートされていません。 Strata Cloud Manager は -NA- に変更された変数値を無視します。

  -NA- の値を持つ変数にファイアウォール固有の値を割り当てることは、その変数がファイアウォールの設定スコープに存在しないためサポートされていません。変数インポート

を使用して変数を上書きするには、変数をファイアウォールがフォルダ階層から継承するか、ファイアウォールの設定スコープで設定する必要があります。

- 変数値がNone#またはNoneの場合は、変数**Value**を **None**として変数が作成されたことを意味します。

  任意の変数値を「None」に変更すると、値は削除できますが、変数は削除できません。

- ファイアウォールの設定スコープで作成された変数の場合、変数値を削除して空白のままにすると、変数が削除されます。

  フォルダー階層で作成され、ファイアウォールによって継承された変数の場合、変数値を削除して空白のままにすると、変数値はフォルダー階層から継承された値に戻ります。

1. エクスポートしたCSVファイルを見つけて開きます。エクスポートされたCSVファイルの形式は次のとおりです。

   ```
   <cloud-management-tenant-name> - Prisma Access_<export-date>_variables
   ```

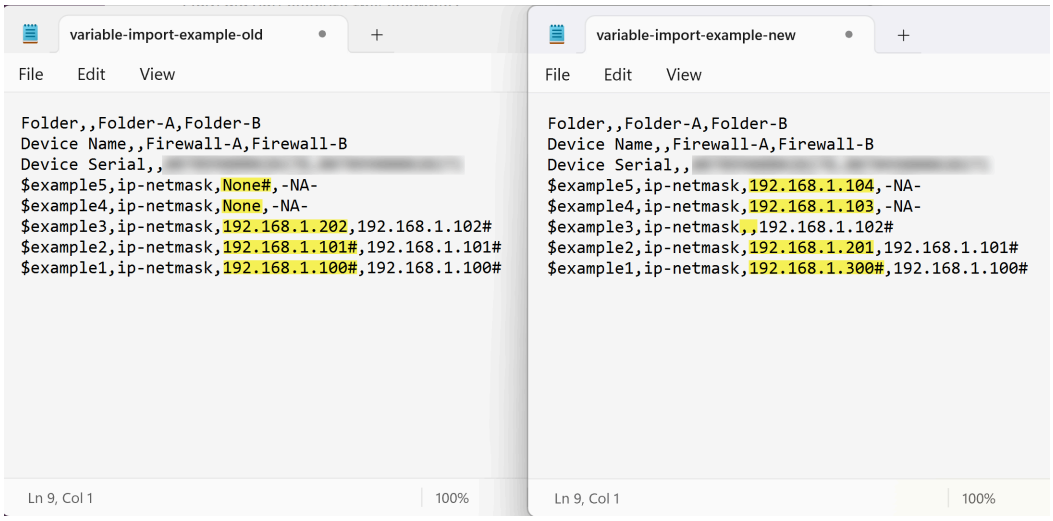
2. 必要に応じて変数を変更します。

   > *Palo Alto Networks*では、フォルダ名、デバイス名、またはデバイスのシリアルナンバーを変更することは推奨していません。これにより、インポートが失敗する可能性があります。

   以下の例では、`Firewall-A` 選択スコープの変数値を次のように変更しました。これは、変数のインポートを使用して 1 回の操作で複数の変数を変更する方法を示しています。

   - `$example1` – 継承されたNone#値をファイアウォール固有の値で上書きします。
   - `$example2` –ファイアウォール固有のNone値をファイアウォール固有の値で上書きします。
   - `$example3` – 変数がファイアウォールの設定スコープで作成された場合、値が空になると変数が削除されます。

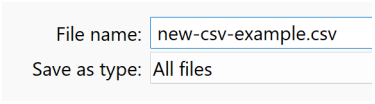
     変数がフォルダ階層から継承され、ファイアウォールの設定スコープで上書きされた場合、値が空の場合、フォルダ階層から継承された変数値が復元されます。
   - `$example4` – 継承された `192.168.1.101` の値をファイアウォール固有の値で上書きします。
   - `$example5` – 変数の変更例 Strata Cloud Managerは#が付加されたままなので無視します。



STEP 6 | 変更を保存します。

[File (ファイル)] > [Save (保存)]を選択して、CSVファイルに加えた変更を保存します。

または、**[File (ファイル)] > [Save As(名前を付けて保存)]** を選択して、変更を新しいCSVファイルに保存します。新しい CSV ファイルを作成するには、ファイル拡張子として**.csv**を含める必要があります。



STEP 7 | CSV ファイルをStrata Cloud Managerにインポートします。

1. **[Manage (管理)] > [Configuration (設定)] > [Overview (概要)]**を選択します。
2. [Variables (変数)]セクションで、表示されている変数カウントをクリックします。
3. **[CSV Export/Import (CSV エクスポート/インポート)] > [Import (インポート)]**を選択します。
4. ファイル を選択し、変更した変数を含むCSV ファイルを選択します。
5. インポート。

変数をエクスポート

フォルダとファイアウォールの設定変数をCSV形式でローカルデバイスにエクスポートします。変数のエクスポートは、複数のファイアウォールにまたがる多数の変数を上書きする場合に便利です。

フォルダーレベルでインターフェースを設定するときに作成されたインターフェース変数のエクスポートはサポートされていません。

STEP 1 | Strata Cloud Managerにログインします。

STEP 2 | **[Manage (管理)] > [NGFW and Prisma Access (NGFWとPrisma Access)] > [Configuration (設定)] > [Overview (概要)]**を選択します。

STEP 3 | [Variables (変数)]セクションで、表示されている変数カウントをクリックします。

STEP 4 | **[CSV Export/Import (CSV** エクスポート/インポート**)]** > **[Import (**インポート**)]**を選択します。

STEP 5 | エクスポートする変数を含むフォルダとファイアウォールを選択し、**[Next (**次へ**)]** をクリックします。

*Strata Cloud Manager*で作成されたすべての変数をエクスポートする場合は、***[All Firewalls (***すべてのファイアウォール***)]***を選択します。

STEP 6 | エクスポートする変数を1つ以上選択します。

STEP 7 | (任意) 選択した変数をプレビューして追加の詳細を表示します。

変数プレビューから、変数名、変数が作成された設定スコープ、変数値などの情報を表示できます。

[Cance (キャンセル**)]** をクリックして次のステップに進むか、ローカルデバイスに**[Download CSV (CSV**をダウンロード**)]** を実施します。

STEP 8 | 選択した変数をCSV形式でエクスポートします。

CSVがエクスポートされ、デバイスにローカルにダウンロードされます。エクスポートされたCSVファイルの形式は次のとおりです。

```
<cloud-management-tenant-name> - Prisma Access_<export-
date>_variables
```


管理:概要

どこで使用できますか?	何が必要ですか?
• Prisma Access (Managed by Panorama or Strata Cloud Manager) • Software NGFW Creditsによって資金提供されたものを含むNGFW	これらの各ライセンスには、Strata Cloud Managerへのアクセスが含まれています。 ❑ Prisma Access ❑ AIOps for NGFW Premium ❑ Strata Cloud Manager Essentials ❑ Strata Cloud Manager Pro → Strata Cloud Managerで利用できる機能は、使用するライセンスによって異なります。

概要ページは、NGFW および Prisma Access の初回セットアップと日常の構成管理 (**[Manage (管理)]** > **[Configuration (設定)]** > **[NGFWとPrisma Access]** > **[Overview (概要)]**) の両方の出発点として考えてください。

- グローバル
- Prisma Access
- Strata Cloud Manager

グローバル

どこで使用できますか?	何が必要ですか?
• Prisma Access (Managed by Strata Cloud Manager) • NGFW (Managed by Strata Cloud Manager) • NGFW (Managed by PAN-OS or Panorama) • VM-Series, funded with Software NGFW Credits	❑ AIOps for NGFW Premium license (use the Strata Cloud Manager app) ❑ Prisma Accessライセンス

グローバル設定スコープを選択すると、次の詳細を表示できます。

- 作成したグローバルフォルダとその変数
- 設定が競合するファイアウォール
- ファイアウォールの同期ステータスとファイアウォールの接続ステータス
- 一般情報

- 設定スニペット
- ライセンス
- スニペット共有用の信頼できるテナント
- 設定バージョン スナップショット

設定の概要(Prisma Access)

どこで使用できますか?	何が必要ですか?
• Prisma Access (Managed by Strata Cloud Manager)	❑ Prisma Accessライセンス

Prisma Accessを使い始めたばかりの場合:

- 基本チェックリストでは、Prisma Accessの立ち上げと運用方法について説明しています。ここでタスクと手順を実行して基本的なセットアップから開始し、その後、環境をテストしてデプロイメント環境を構築します。
- これはポリシーフォルダと設定フォルダの仕組みです。
- Prisma Accessに設定変更をプッシュする方法をご紹介します。

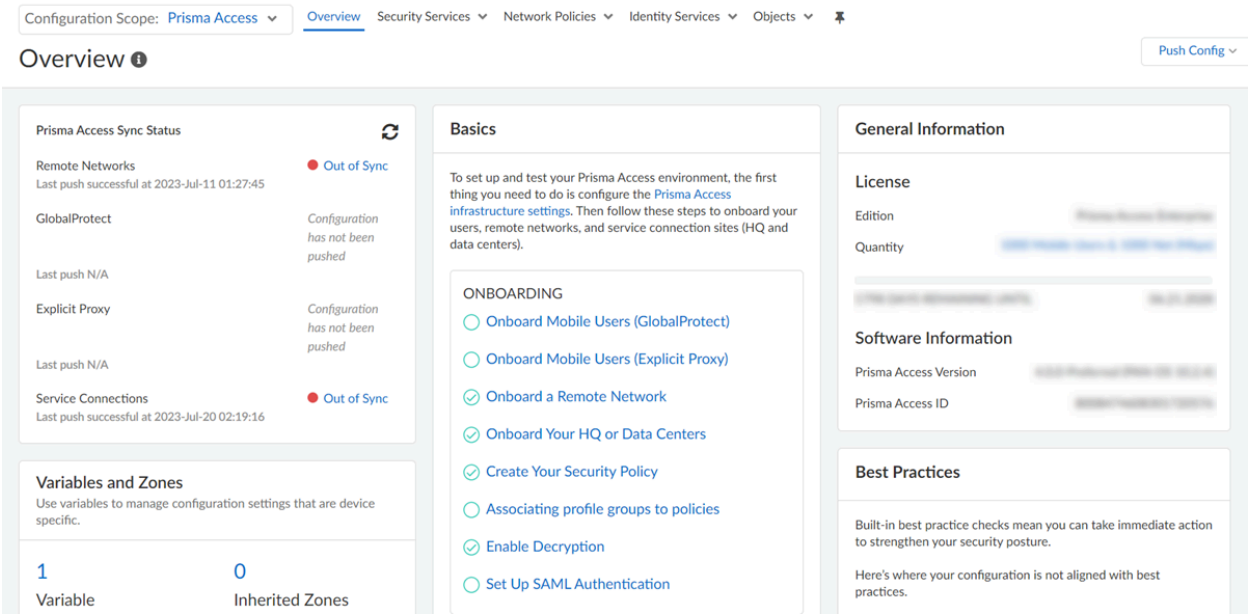
Prisma Access環境の詳細について:

- ライセンスの詳細を確認して、Prisma Accessサブスクリプションの内容を確認してください。
- **About (**詳細**)**パネルには、Prisma Access環境のソフトウェアとテナント情報が表示されます。

日常的な設定管理について:

- 設定状況が一目でわかる
- 設定スニペットを使用して、Prisma Accessデプロイメントセットの共通基本設定を標準化
- 設定スナップショットの検索：設定バージョンを比較し、以前のバージョンをリストア（またはロード）して、トラフィックフローやセキュリティに意図しない影響を与える設定プッシュから復旧
- 使用していないオブジェクトやルールをクリーンアップし、使用していないアプリケーションを許可することでセキュリティギャップをもたらしているルールを厳格化することで、設定を最適化
- セキュリティ体制強化につながる設定変更が可能な領域を特定

- また、Prisma Accessのライセンスとその内容についての詳細もご覧いただけます。

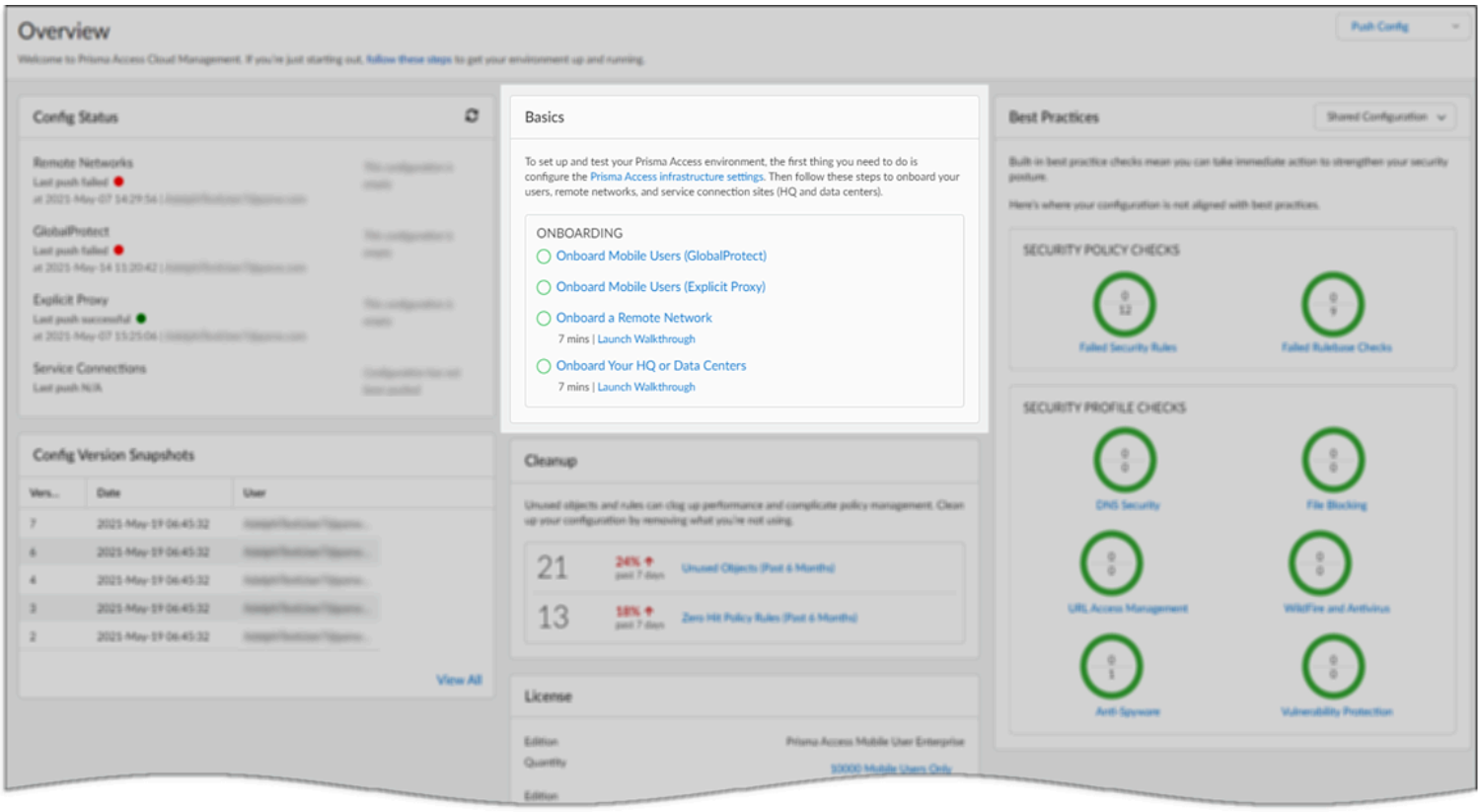


基本的なセットアップが完了したら、環境のテストとデプロイメント環境の構築を開始できます。

基本

Prisma Accessの設定 基本ガイドでは、Prisma Accessの立ち上げと運用について説明します。ここでの作業を完了して、基本的なセットアップを開始します。この作業は、環境のテストや導入環境の構築に使用できます。

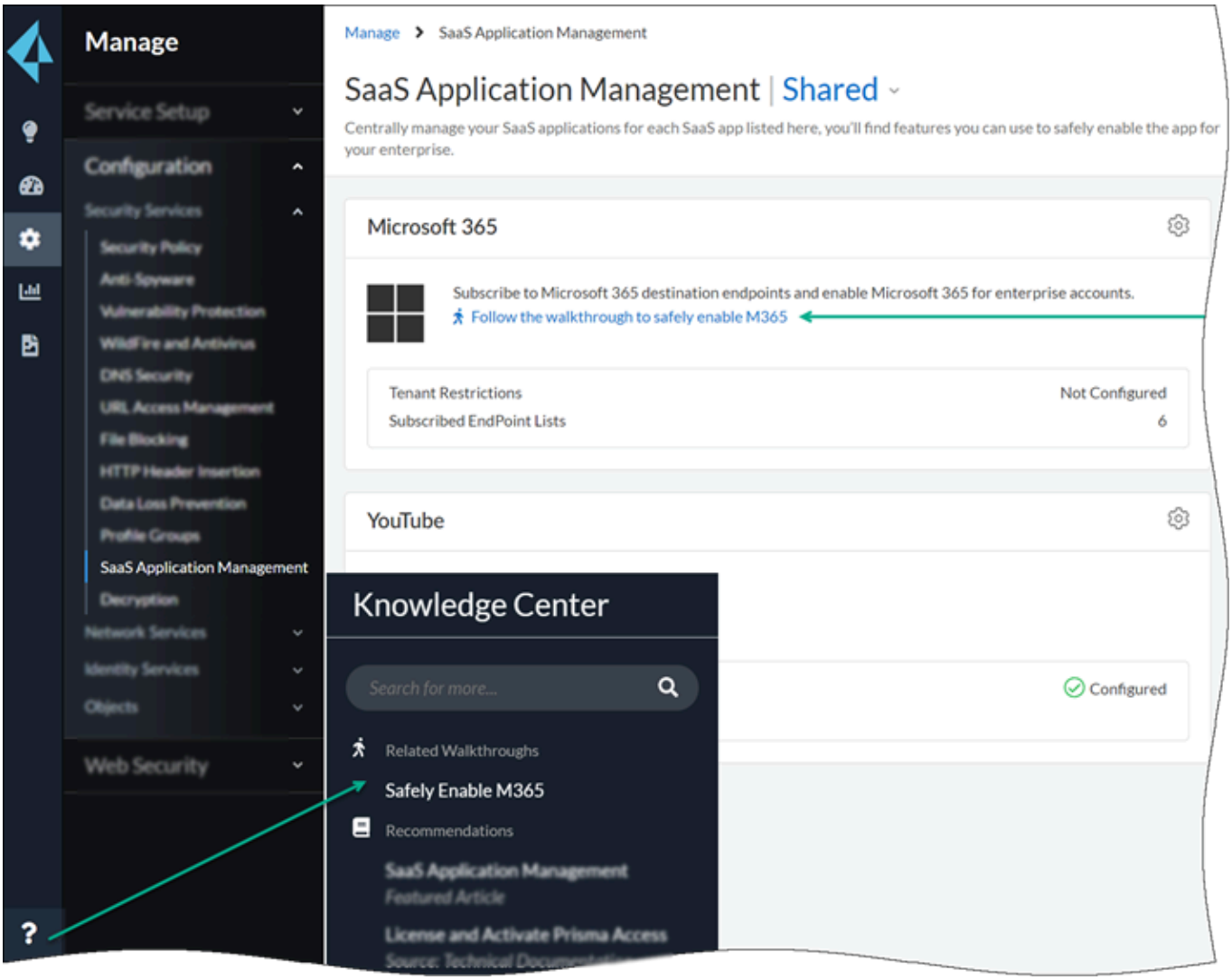
各タスクは、関連する設定を設定するページにリンクします。設定が完了すると、このリストのタスクが完了と表示されます。そのため、進捗状況が一目で把握でき、新人研修の段階であれば特に便利です。

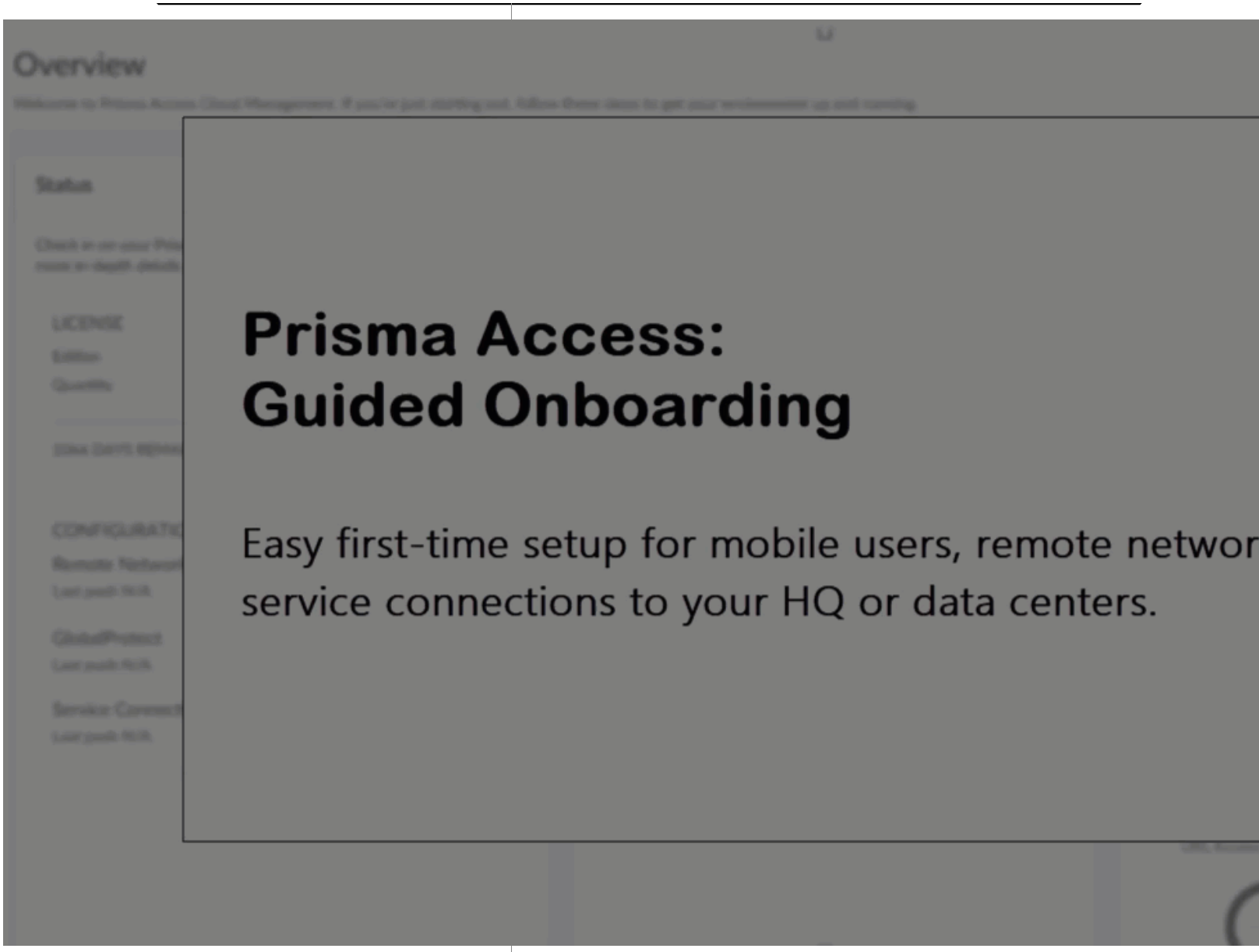


ウォークスルー

いくつかの To-Do には、環境を稼働させるために必要な基本的な手順を順を追って説明する手順も含まれています。

オンボーディングのウォークスルーは**[Overview (概要)]**ダッシュボードで確認できます。をクリックしてヘルプに移動し、現在表示しているページで利用可能なウォークスルーがあるかどうかを確認し、ページ上で直接起動できるウォークスルーに目を光らせてください。





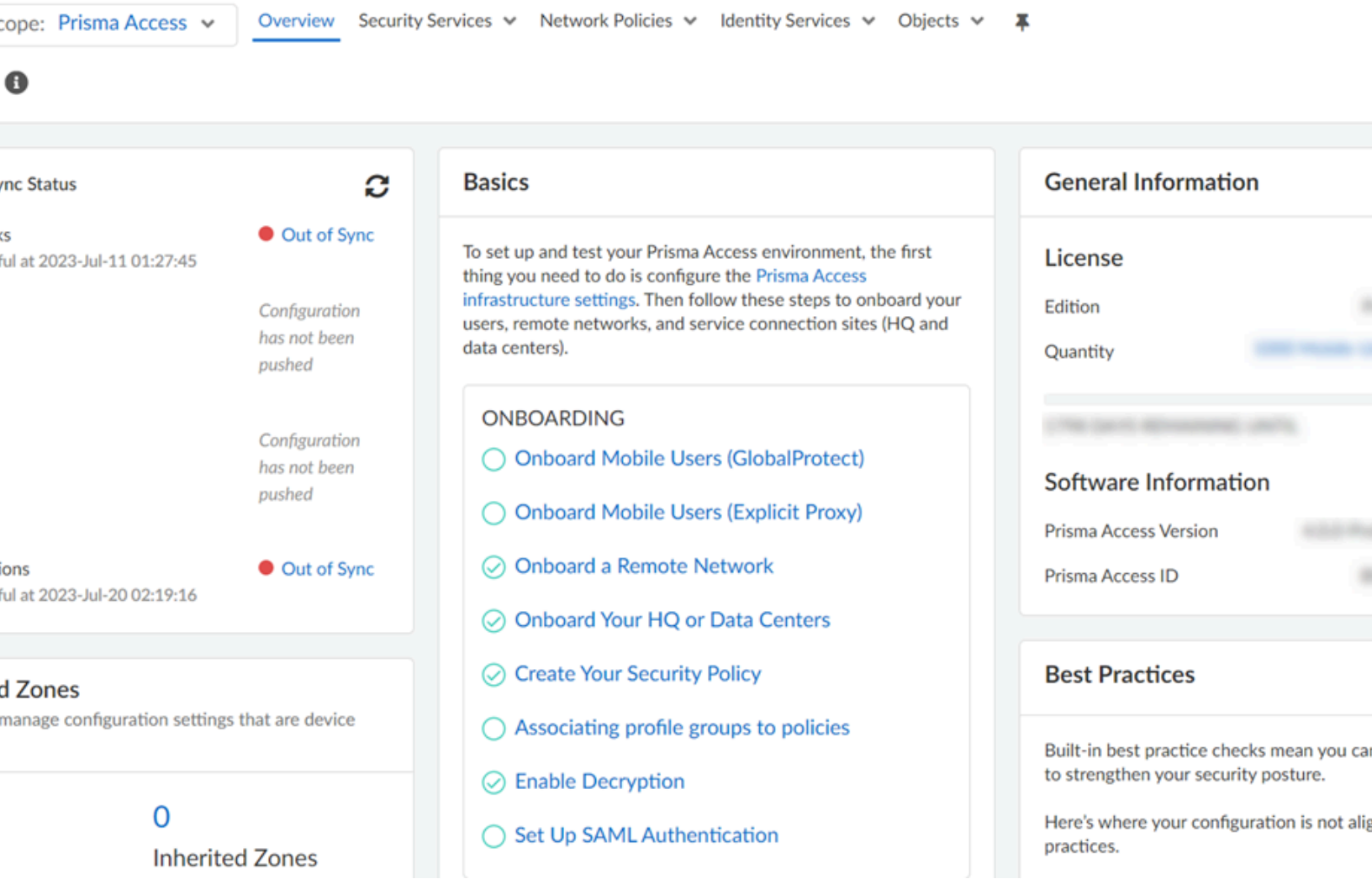
Prisma Access の同期ステータス

概要ページでは、Prisma Access設定のステータスをすばやく確認できます。予期しないものが表示された場合は、ドリルダウンして影響を受ける設定を特定します。表示される可能性のあるステータスは次のとおりです。

- 設定がプッシュされていない – これまでのところ、Prisma Access にプッシュされた設定はありません。
- この設定は空です – ユーザーがPrisma Accessに空の設定をプッシュしました。この場合、設定はすでに設定されていたので、Prisma Accessへのプッシュは設定を削除することだったかもしれません。**[Push Config (設定をプッシュ)]** > **[Jobs (ジョブ)]**に移動して、最近の変更を確認します。

- 同期されていない – ユーザがプリズマアクセスに設定をプッシュしましたが、プッシュに関連するエラーまたは警告があります。これは設定の問題か、Prisma Accessへのプッシュに関連する問題かもしれません。
- 同期中 – Prisma Access への最新の設定プッシュは正常に実行され、エラーはありません。

予期しないものが表示された場合は、ステータスをクリックすると、モバイルユーザー（GlobalProtectまたは明示的なプロキシ接続）、リモートネットワーク、またはサービス接続のいずれかがある場所を示すマップビューが開きます。そうすれば、確認が必要な設定や更新が必要な箇所を特定できます。



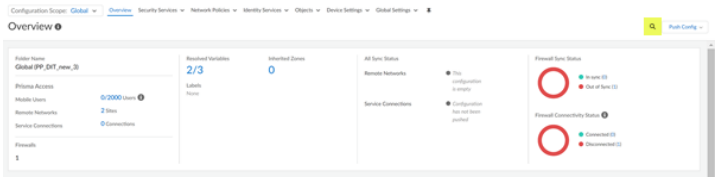
設定検索を使用したグローバル検索

Config Searchでは、IPアドレス、オブジェクト名、参照オブジェクト、重複オブジェクト、ポリシー名、ポリシー規則、特定のCVEの対象となるポリシー、規則UUID、定義済みスニペット、アプリケーション名など、特定の文字列に対する特定の設定オブジェクトと設定を検索し、オブジェクトが使用されているすべての参照のリストを取得できます。

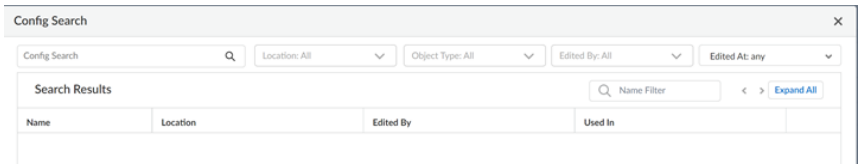
1. 設定検索を起動するには、Webインターフェイスの右上にある**[Push Config (設定のプッシュ)]**の横にある

   アイコンをクリックします。**[Config Search (設定検索)]**は、**[Manage (管理)]**のすべてのページから利用できます。

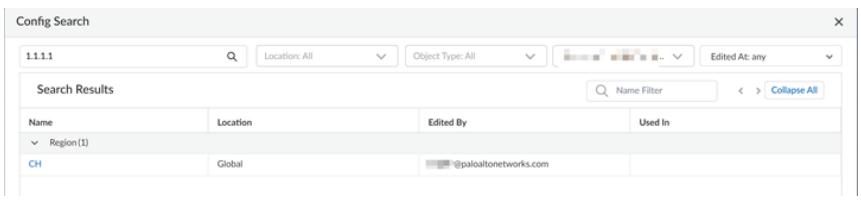
2. **[Config Search (設定検索)]**画面では、**[Config String (設定文字列)]**、**[Location (場所)]**、**[Object Type (オブジェクトタイプ)]**、**[Edited By (編集者)]**、または**[Edited At (編集箇所)]**の各フィールドを使用して検索できます。

   検索のヒント:

   - 完全に一致するフレーズを検索するには、フレーズを引用符で囲みます。
   - 検索語に含まれるスペースは、AND演算子として処理されます。たとえば、「corp policy」を検索すると、検索結果には設定に corp と policy の両方があるインスタンスが表示されます。
   - 以前の検索を再実行するには、[検索の設定]アイコンをクリックします。最新の50件の検索が表示されます。リストの項目をクリックすると、その検索が再実行されます。検索履歴リストは、管理者アカウントごとに固有のものです。
   - [Config Search (設定検索)]は検索可能なフィールドごとに利用できます。たとえば、次のオブジェクトタイプでセキュリティポリシーを検索することができます。タグ、ゾーン、アドレス、ユーザー、HIP プロファイル、アプリケーション、UUID、およびサービス。
   - 場所はフォルダとスニペットでグループ化されています。複数の場所を選択して検索できます。場所を選択しない場合、デフォルトですべての場所が選択されます。
   - オブジェクトタイプが選択されていない場合、すべてが選択されます。

3. 検索結果は分類され、Strata Cloud Manager 内の設定場所へのリンクが提供されるため、検索した文字列のすべての出現と参照箇所を簡単に見つけることができます。

設定の概要(Strata Cloud Manager)

どこで使用できますか?	何が必要ですか?
• NGFW (Managed by Strata Cloud Manager) • NGFW (Managed by PAN-OS or Panorama) • VM-Series, funded with Software NGFW Credits	❑ AIOps for NGFW Premium license (use the Strata Cloud Manager app)

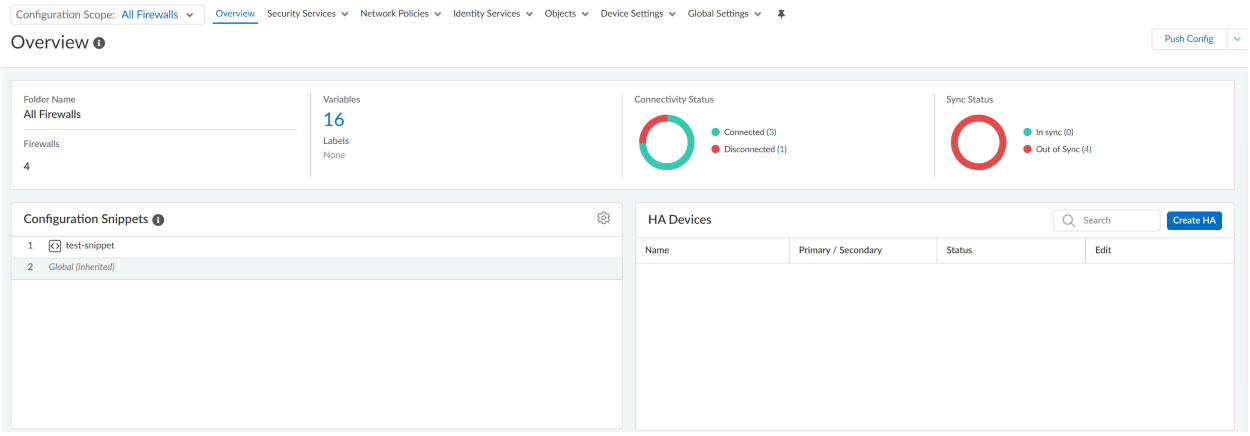
NGFWのクラウド管理を始めたばかりの場合:

- これはポリシーフォルダと設定フォルダの仕組みです。
- 設定変更をファイアウォールにプッシュする方法をご紹介します。

日常的な設定管理の場合:

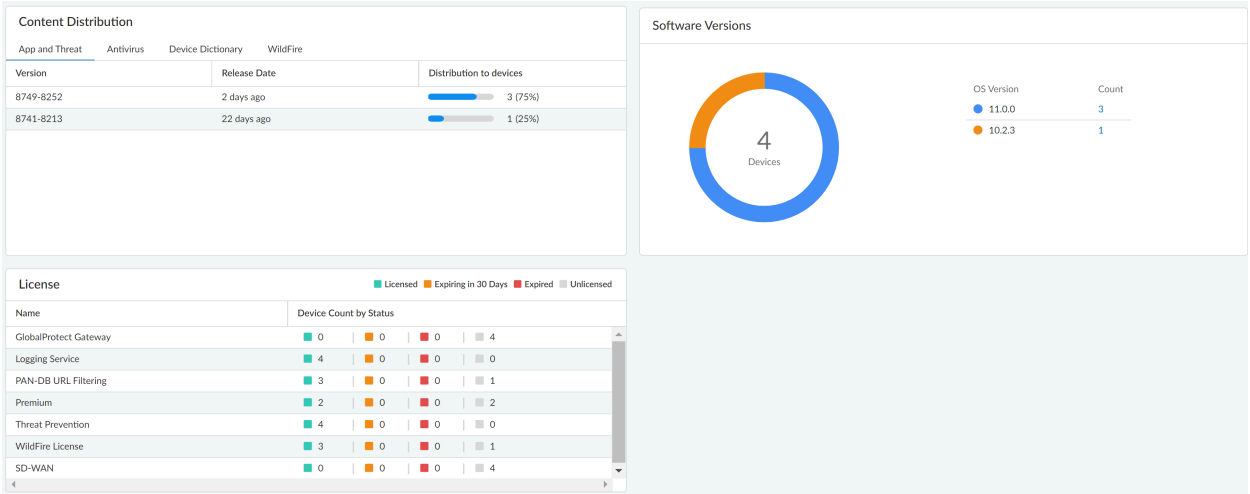
- 現在のフォルダ名、フォルダに追加されたファイアウォールの数、フォルダ用に作成された変数の数の概要が一目でわかります。
- ローカル設定を管理するための集中管理ファイアウォールと個別のファイアウォールを切り替えることなく、ローカルファイアウォール設定を可視化および制御できます。
  - 「設定競合のあるファイアウォール」には、競合のあるファイアウォールの数が表示されます。番号をクリックすると、ファイアウォールの競合とその位置が表示されます。任意のファイアウォールをクリックして、デバイスレベルの競合を確認します。
  - 設定が競合するオブジェクトは、ファイアウォールごとの競合の数を示します。番号をクリックすると、特定のファイアウォールの競合オブジェクトとそのタイプが表示されます。オブジェクトをクリックすると、コンフリクトの詳細が表示されます。
- 設定スニペットを使用して、管理対象ファイアウォールのセットの共通基本設定を標準化します。
- 高可用性（HA）設定でマネージドファイアウォールを設定し、冗長性を提供してビジネス継続性を確保します。
- 管理対象ファイアウォールのStrata Cloud Managerへの接続ステータスを確認します。

- Strata Cloud Managerと管理対象ファイアウォールの現在の実行コンフィギュレーション間の設定の同期ステータスを確認します。



管理対象ファイアウォールの詳細について:

- コンテンツ配信とソフトウェアバージョンの詳細を確認して、管理対象のファイアウォールで実行されている動的コンテンツ更新とPAN-OSソフトウェアのバージョンを確認します。
- ライセンスの詳細を確認して、管理対象のファイアウォールでアクティブになっているライセンスを確認します。



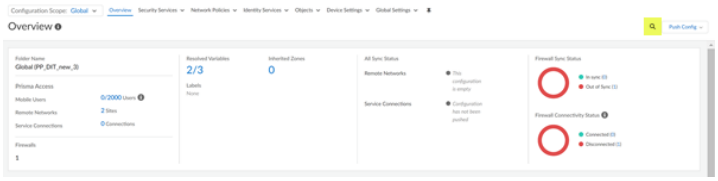
設定検索を使用したグローバル検索

Config Searchでは、IPアドレス、オブジェクト名、参照オブジェクト、重複オブジェクト、ポリシー名、ポリシー規則、特定のCVEの対象となるポリシー、規則UUID、定義済みスニペット、アプリケーション名など、特定の文字列に対する設定オブジェクトと設定を検索し、オブジェクトが使用されているすべての参照のリストを検索できます。

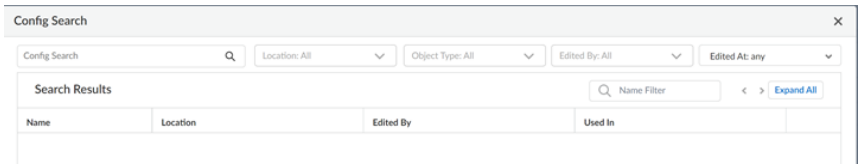
1. 設定検索を起動するには、Webインターフェイスの右上にある**[Push Config (設定のプッシュ)]**の横にある

   アイコンをクリックします。**[Config Search (設定検索)]**は、**[Manage (管理)]**のすべてのページから利用できます。

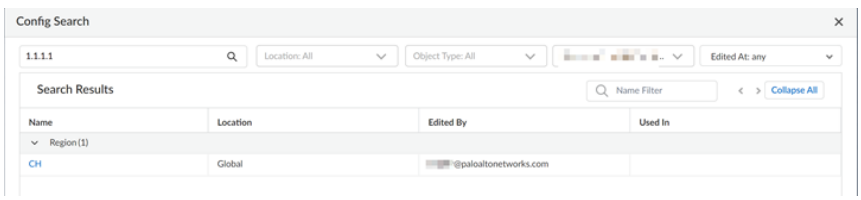
2. **[Config Search (設定検索)]**画面では、**[Config String (設定文字列)]**、**[Location (場所)]**、**[Object Type (オブジェクトタイプ)]**、**[Edited By (編集者)]**、または**[Edited At (編集箇所)]**の各フィールドを使用して検索できます。

   検索のヒント:

   - 完全に一致するフレーズを検索するには、フレーズを引用符で囲みます。
   - 検索語に含まれるスペースは、AND演算子として処理されます。たとえば、「corp policy」を検索すると、検索結果には設定に corp と policy の両方があるインスタンスが表示されます。
   - 以前の検索を再実行するには、[検索の設定]アイコンをクリックします。最新の50件の検索が表示されます。リストの項目をクリックすると、その検索が再実行されます。検索履歴リストは、管理者アカウントごとに固有のものです。
   - [Config Search (設定検索)]は検索可能なフィールドごとに利用できます。たとえば、次のオブジェクトタイプでセキュリティポリシーを検索することができます。タグ、ゾーン、アドレス、ユーザー、HIP プロファイル、アプリケーション、UUID、およびサービス。
   - 場所はフォルダとスニペットでグループ化されています。複数の場所を選択して検索できます。場所を選択しない場合、デフォルトですべての場所が選択されます。
   - オブジェクトタイプが選択されていない場合、すべてが選択されます。

3. 検索結果は分類され、Strata Cloud Manager 内の設定場所へのリンクが提供されるため、検索した文字列のすべての出現と参照箇所を簡単に見つけることができます。

管理:セキュリティ サービス

どこで使用できますか?	何が必要ですか?
• Prisma Access (Managed by Panorama or Strata Cloud Manager) • Software NGFW Creditsによって資金提供されたものを含むNGFW	これらの各ライセンスには、Strata Cloud Managerへのアクセスが含まれています。 ❑ Prisma Access ❑ AIOps for NGFW Premium ❑ Strata Cloud Manager Essentials ❑ Strata Cloud Manager Pro → Strata Cloud Managerで利用できる機能は、使用するライセンスによって異なります。

セキュリティ サービスを管理し、ネットワーク、システム、ユーザーを保護します。

[Manage (管理)] > [Configuration (設定)] > [NGFWとPrisma Access] > [Security Services (セキュリティサービス)]に移動します。

セキュリティ サービスを使用すると、次のことが可能になります。

- 管理:セキュリティ ポリシーを使用して Prisma Access トラフィックを強制する方法を定義します。
- 暗号化されたトラフィックに潜む脅威を管理:復号で阻止します。

管理:セキュリティ ポリシー

どこで使用できますか?	何が必要ですか?
• Prisma Access (Managed by Panorama or Strata Cloud Manager) • Software NGFW Creditsによって資金提供されたものを含むNGFW	これらの各ライセンスには、Strata Cloud Managerへのアクセスが含まれています。 ❑ Prisma Access ❑ AIOps for NGFW Premium ❑ Strata Cloud Manager Essentials ❑ Strata Cloud Manager Pro → Strata Cloud Managerで利用できる機能は、使用するライセンスによって異なります。

セキュリティ ポリシーは、Prisma Access およびNGFWのデプロイメントでトラフィックをどのように強制するかを定義する場所です。Strata Cloud Manager環境をパススルーするすべてのト

ラフィックはセキュリティ ポリシーに照らして評価され、複数のルールが上から下の順に適用されます。

セキュリティポリシーをセットアップするには、**[Manage (管理)]** > **[Configuration (設定)]** > **[NGFWとPrisma Access]** > **[Security Services (セキュリティ サービス)]** > **[Security Policy (セキュリティ ポリシー)]** に移動します。

セキュリティ ポリシーを開始する

ここでは、セキュリティ ポリシーを機能させるために今すぐできることをいくつか紹介します。

- セキュリティ ポリシー ルールの作成 – セキュリティポリシーを使用すると、ルールを適用し、アクションを実行できます。また、必要に応じて、全般的または個別の指定を行うことができます。
- ルールベース内のルールの追跡 – ルールベース内の各ルールに自動的に番号を振ります。ルールを移動させたり順序を変えたりすると、新しい順序に基づいて番号が変化します。
- ポリシールールのベストプラクティスの適用 – ルールを作成あるいは変更する際、ルールの説明、タグ、監査コメントを必須にして、ポリシー ルールベースを確実に正しく整理・グループ化することで、重要なルールの履歴を監査目的で維持することができるようになります。
- テストポリシー規則 – ポリシーアナライザのチェックポリシー ルールを使用します。
- セキュリティ プロファイルのアクティベート – セキュリティ プロファイルは、セキュリティポリシーでアプリケーションまたはカテゴリが許可された後に適用され、トラフィックをスキャンします。
- セキュリティ プロファイル グループの作成 – セキュリティ プロファイル グループは、セキュリティ プロファイルのセットとして、1 つの単位として処理でき、セキュリティ ポリシーに簡単に追加できます。
- ファイル ブロックのセットアップ – ブロックまたはモニターする特定のファイルタイプを識別できます。
- データ フィルタリング プロファイルの作成 – 機密情報がネットワークを離れることがないようにすることができます。
- Webセキュリティの管理 – インターネットおよびSaaSアプリケーションへのアクセス（一般的なブラウジング）を制御します。

管理:復号

どこで使用できますか?	何が必要ですか?
• Prisma Access (Managed by Panorama or Strata Cloud Manager) • Software NGFW Creditsによって資金提供されたものを含むNGFW	これらの各ライセンスには、Strata Cloud Managerへのアクセスが含まれています。 ❑ Prisma Access ❑ AIOps for NGFW Premium ❑ Strata Cloud Manager Essentials

どこで使用できますか?	何が必要ですか?
	❑ Strata Cloud Manager Pro → Strata Cloud Managerで利用できる機能は、使用するライセンスによって異なります。

復号化を有効にして、暗号化されたトラフィックに隠された脅威を阻止します。最初に必要な操作は、復号証明書のインポートだけです。それ以外は、ベストプラクティス設定が事前に組み込まれており、それをそのまま使用できます。

トラフィックの復号化の詳細については、こちらを参照してください。

[Manage (管理)] > [Configuration (設定)] > [NGFWとPrisma Access] > [Security Services (セキュリティサービス)] > [Decryption (復号化)]に移動します。

復号の概要

SSL（Secure Sockets Layer）および SSH（Secure Shell）暗号化プロトコルは、2 つのエンティティ間（Web サーバーとクライアントなど）のトラフィックを安全に保護します。SSL および SSH はトラフィックをカプセル化し、データを暗号化します。これにより、データを復号化するキーとデバイス間の信頼を確立する証明書を持つクライアントとサーバー以外のエンティティにとって、データは意味のないものになります。次の目的で SSL および SSH トラフィックを復号化します：

- 暗号化されたトラフィックに隠れたマルウェアがネットワークに侵入するのを防ぎます。例えば、SSL 暗号化を使用するウェブサイトに攻撃者が侵入するとします。従業員がそのウェブサイトにアクセスし、知らないうちにエクスプロイトやマルウェアをダウンロードします。その後、マルウェアは感染した従業員のエンドポイントを使ってネットワーク内を横方向に移動し、他のシステムに侵入します。
- センシティブな情報がネットワークの外部に流出するのを防ぎます。
- 安全なネットワーク上で適切なアプリケーションが実行されていることを確認する。
- トラフィックを選択的に復号化します。例えば、金銭あるいはヘルスケアを扱うトラフィックを復号化から除外する復号化ポリシーおよびプロファイルを作成します。

*SSH*プロキシの復号化は*Strata Cloud Manager*ではサポートされていません。

復号ポリシー

Strata Cloud Managerには、次の2種類の復号化ポリシールールが用意されています。アウトバウンドSSLトラフィックを制御するSSL転送プロキシ、インバウンドSSLトラフィックを制御するSSLインバウンド インスペクション。

SSL 転送プロキシ

外部サイトに送信される SSL トラフィックを復号化するようにファイアウォールを設定すると、ファイアウォールはフォワード プロキシとして機能します。SSL フォワード プロキシ復号ポリシーを使用すると、内部ユーザーから Web への SSL/TLS トラフィックを復号化および検査

できます。SSL フォワード プロキシ復号化はトラフィックを復号化し、ファイアウォールが復号化プロファイル、セキュリティ ポリシー、プロファイルをトラフィックに適用できるようにすることで、SSL で暗号化されたトラフィックに隠れたマルウェアが企業ネットワークに侵入するのを防ぎます。

SSL インバウンド インスペクション

SSL インバウンド インスペクションを使用すると、クライアントからターゲットのネットワークサーバー（証明書があり、証明書をファイアウォールにインポートできる任意のサーバー）へのインバウンド SSL/TLS トラフィックを復号化および検査し、疑わしいセッションをブロックします。たとえば、悪意のある人物が Web サーバーの既知の脆弱性を悪用しようとしているとします。インバウンド SSL/TLS 復号化により、トラフィックの可視性が実現し、ファイアウォールが脅威に積極的に対処できるようになります。

復号プロファイル

復号化プロファイルをポリシールールに付与し、サーバー証明書、サポートされていないモード、エラーのチェックなど、細かなアクセス設定をトラフィックに適用できます。

SSLフォワードプロキシプロファイル

SSLフォワード プロキシの復号化プロファイルは、プロファイルを付与するフォワードプロキシ復号化ポリシーで定義されている、アウトバウンド SSL/TLS トラフィックのサーバー検証、セッション モード チェック、およびエラーチェックを制御します。

SSLインバウンド検査プロファイル

SSL インバウンド インスペクション復号プロファイルは、プロファイルを付与するインバウンド インスペクション復号化ポリシーで定義されている、インバウンド SSL/TLS トラフィックのセッション モード チェックおよびエラーチェックを制御します。

復号化なしのプロファイル

復号化プロファイルなしは、復号化しないことを選択したトラフィックのサーバ検証チェックを実行します。復号化から除外するトラフィックを定義する「復号化なし」復号化ポリシーに復号化なしのプロファイルをアタッチします。（サイトが証明書のピンニングや相互認証などの技術的な理由で復号化を妨げる場合、トラフィックの復号化を除外するためにポリシーを使用しないでください。代わりに、ホスト名を復号化除外リストに追加します）

復号化のヒント

- ベストプラクティスのポリシールールを出発点として復号化ポリシーを構築

  トラフィックを復号化するルールと、機密コンテンツを復号化から除外するルールは、URLカテゴリに基づいて構築されます。
- 機密コンテンツを復号化から除外する

  ビジネス、法律、規制上の理由から、機密コンテンツを復号化から除外します。
  - 事前定義された復号除外 — Palo Alto Networksは、この除外リストを維持し、定期的に更新します。このリストは、復号化に指定したすべてのトラフィックにグローバルおよびデ

フォルトで適用されます。リストエントリは、ビジネスニーズに合う場合は無効にすることができます。

- カスタム除外 – サイトまたはアプリケーションを復号化からグローバルに除外します。
- ポリシーベースの除外 – URLカテゴリと外部動的リストを使用して、ターゲットを絞ったポリシーベースの復号化ルールを作成します。復号化ポリシー規則のアクションを復号化なしに設定して、一致するトラフィックを復号化から除外します。

復号化除外は常にポリシールールの先頭に配置し、最初に適用するようにしてください。

- 復号化設定をグローバルに適用できる部分と、特定の場所を対象とする部分を考慮する
  - Strata Cloud Manager復号化ポリシーは、すべてのNGFWとPrisma Accessロケーションにグローバルに適用されます。

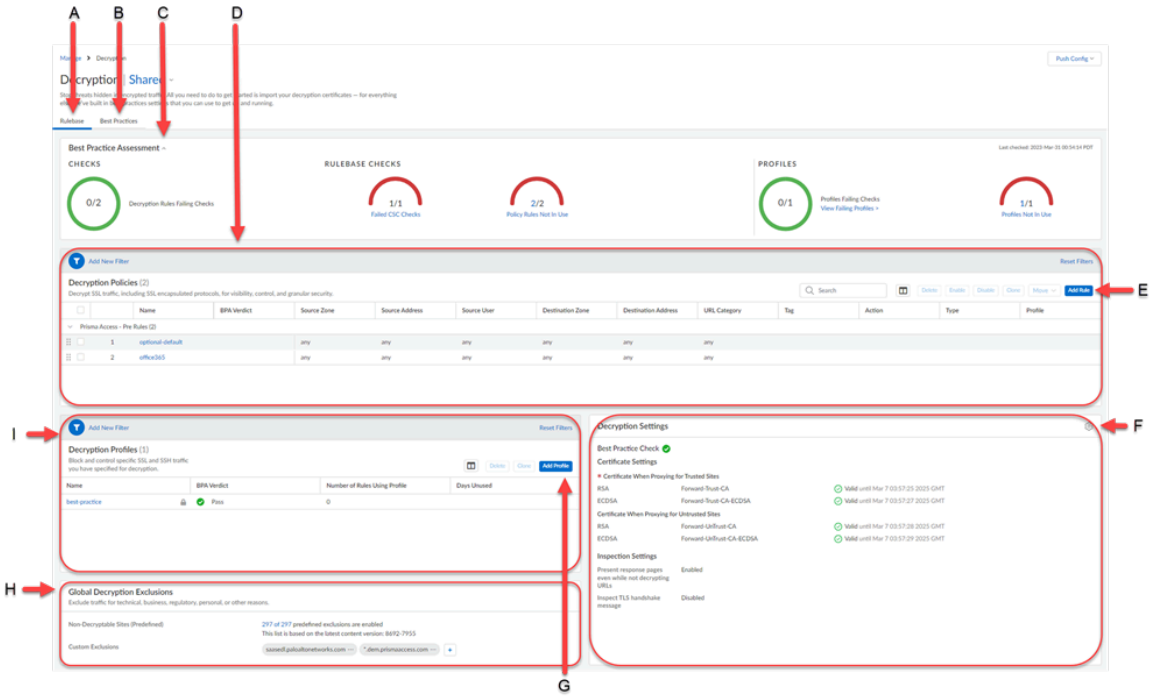
    管理 > 設定 > **NGFW** と **Prisma** のアクセス > セキュリティ サービス > 復号
  - 各タイプの復号化ポリシーに移動して、特定のファイアウォール、モバイルユーザーの場所、リモートネットワークサイト、またはサービス接続を対象とするポリシールールを作成する

    管理 > 設定 > **NGFW** と **Prisma** のアクセス > 設定スコープ > グローバル/ファイアウォール/モバイルユーザー/リモートネットワーク/サービス接続
- ルールの順序が重要です

  復号ポリシールールは上から下へ適用されます。復号化ポリシールールのリストの先頭に、最初に適用するルールを配置します。グローバルルール（プレルール）が最初に適用され、モバイルユーザ、リモートネットワーク、およびサービス接続に固有のルールの前に常にリストされます。

一目でわかる復号

[Decryption (復号化)]画面は、復号ポリシーとプロファイルを設定し、ベストプラクティス評価を表示する場所です。



A）ルールベース – ルールベース チェックは、多くのルール全体に適用される構成設定など、セキュリティ ポリシーがどのように構成および管理されているかを調べます。

B）ベストプラクティス – ここでは、機能の実装がベストプラクティスとどのように整合しているかを包括的に確認できます。失敗したチェックを調べて、改善できる箇所を確認します（合格したチェックを確認することもできます）。

C）ベストプラクティス評価 – ベストプラクティススコアが復号化ダッシュボードに表示されます。これらのスコアにより、ベストプラクティスの進捗状況が一目でわかります。一目で、さらに調査すべき領域や、セキュリティ態勢を改善するためにアクションを起こしたい領域を特定できます。

D）復号化ポリシー – オンボード復号化ポリシーのリスト。ポリシー設定、ポリシータイプ（*SSL*フォワードプロキシ、*SSL*インバウンドインスペクション、または*SSH*プロキシ）、ポリシーアクション（復号化または復号化なし）、およびBPA評決を確認します。

E）ルールの追加 – 新しい復号化ポリシーを追加および設定します。

F）復号化設定 – 証明書と復号化の設定にアクセスします。証明書のインポートとエクスポート。

G）プロファイル追加 – 新しい復号プロファイルを追加および設定します。

H）グローバル復号化除外 – 復号化から除外されるアプリケーション。

I）復号化プロファイル – オンボード復号化プロファイルのリスト。プロファイル設定、プロファイルを使用したポリシー、およびBPA評決を確認します。

管理:ネットワークポリシー

どこで使用できますか?	何が必要ですか?
• Prisma Access (Managed by Panorama or Strata Cloud Manager) • Software NGFW Creditsによって資金提供されたものを含むNGFW	これらの各ライセンスには、Strata Cloud Managerへのアクセスが含まれています。 ❑ Prisma Access ❑ AIOps for NGFW Premium ❑ Strata Cloud Manager Essentials ❑ Strata Cloud Manager Pro → Strata Cloud Managerで利用できる機能は、使用するライセンスによって異なります。

さまざまな種類のネットワーク ポリシーを作成して、ネットワークを脅威や中断から保護できます。ネットワーク リソースの割り当てを最適化し、ネットワーク ポリシーを管理してトラフィックの優先順位を付け、アプリケーションの分類を構成するのに役立ちます。

ルールは上から下に評価され、トラフィックが定義されたルール基準に一致すると、後続のルールは評価されません。可能な限り最適な一致条件を適用するには、より一般的なポリシー ルールよりも、より具体的なポリシー ルールを優先する必要があります。ルールのログ記録が有効になっている場合、ポリシー ルールに一致するトラフィックのログが生成されます。ログ記録オプションはルールごとに設定可能です。

ベストプラクティス ポリシー ルールはほとんどのポリシー タイプで利用可能であり、迅速かつ安全に開始するのに役立ちます。これらのルールは、常に最低限のセキュリティ レベルを確保できるように編集することはできませんが、ポリシーをカスタマイズするための基盤として使用したい場合は、複製することができます。

開始するのは、 **[Manage (管理)] > [Configuration (設定)] > [NGFWとPrisma Access] > [Network Policies (ネットワーク ポリシー)]**に進んでください。

ネットワーク ポリシーを使用すると、次のことが可能になります。

- 管理:QoSを使用して業務に最も重要なトラフィックを優先する。
- 管理:アプリケーション オーバーライドを使用してPrisma Accessがアプリケーションを分類する方法を管理する。

管理:QoS

どこで使用できますか?	何が必要ですか?
• Prisma Access (Managed by Panorama or Strata Cloud Manager)	以下のいずれかです。 ❑ Prisma Accessライセンス

どこで使用できますか?	何が必要ですか?
	❑ Strata Cloud Manager Pro → Strata Cloud Managerで利用できる機能は、使用するライセンスによって異なります。

Quality of Service (クオリティ オブ サービス - QoS)を使用すると、ビジネス クリティカルなトラフィックや、低遅延を必要とするアプリケーション (VoIP やビデオ アプリケーションなど) を優先できます。QoS ポリシー ルールを追加または編集するには、**[Manage (管理)]** > **[Configuration (設定)]** > **[NGFWとPrisma Access]** > **[Network Policies (ネットワークポリシー)]** > **[QoS]**に移動します。

QoS ポリシー ルール

優先処理または帯域幅制限を必要とするトラフィックを識別するためのクオリティ オブ サービス (QoS) ポリシー ルール。QoSルールを使用すると、限られたネットワーク容量でも優先度の高いアプリケーションとトラフィックを確実に実行できます。DSCP (Differentiated Services Code Points) を使用してトラフィックの QoS 処理を設定できます。これらのコードポイントは、トラフィックに対して（たとえば）高優先度またはベストエフォート配信を要求するために使用できるパケット ヘッダー値です。Prisma Accessは、着信トラフィックに対してDSCP値を適用し、セッション トラフィックがファイアウォールから出るときにセッションにDSCP値をマークします。これは、セッションのすべてのインバウンドとアウトバウンド トラフィックが継続的なQoS処理を受けていることを意味します。次のコードポイントを使用してトラフィックQoS処理を設定できます。

- **:**迅速な転送 **(EF)**- トラフィックに対して低損失、低遅延、保証された帯域幅を要求するために使用されます。

  コードポイント値がEFのパケットは、通常、優先順位が最も高く、保証された配信です。
- 確実な転送 **(AF)**– アプリケーションの信頼性の高い配信を提供するために使用されます。

  AF コードポイントを持つパケットは、トラフィックがベスト エフォート サービスが提供するよりも高い優先度の処理を受けることを要求していることを示します。EF コードポイントを持つパケットは、AF コードポイントを持つパケットよりも優先されます。
- クラス セレクタ **(CS)** -IP優先順位フィールドを使用して優先トラフィックをマークするネットワークIPアドレスとの下位互換性を提供するために使用されます。
- **IP** 優先順位 **(ToS)** –優先トラフィックをマークするためにレガシー ネットワークIPアドレスによって使用されます。
- カスタム コードポイント- コードポイント名とバイナリ値を入力して、トラフィックに一致するカスタム コードポイントを作成します。

  たとえば、Voice over IP (ボイス オーバー インターネット プロトコル - VoIP)などの音声通信を優先するQoSポリシー ルールを作成して、一貫したパケット転送を確保できます。これにより、音声通信の一貫性が確保されます。

管理:アプリケーション オーバーライド

どこで使用できますか?	何が必要ですか?
• Prisma Access (Managed by Panorama or Strata Cloud Manager) • Software NGFW Creditsによって資金提供されたものを含むNGFW	これらの各ライセンスには、Strata Cloud Managerへのアクセスが含まれています。 ❑ Prisma Access ❑ AIOps for NGFW Premium ❑ Strata Cloud Manager Essentials ❑ Strata Cloud Manager Pro → Strata Cloud Managerで利用できる機能は、使用するライセンスによって異なります。

アプリケーション オーバーライド ポリシーを作成し、アプリケーションをレイヤ7検査にApp-IDを使用する代わりに、高速パスレイヤ4検査を使用して処理するように指定します。これにより、セキュリティ適用ノードはセッションを通常のステートフル検査として処理し、アプリケーションの処理時間を節約できます。既知のIPアドレス間でカスタム アプリケーションのトラフィック検査を行わない場合に、アプリケーション上書きポリシー規則を作成できます。たとえば、非標準ポートにカスタムアプリケーションがあり、そのアプリケーションにアクセスするユーザが制裁を受けることがわかっていて、その両方が信頼ゾーンにある場合、カスタムアプリケーションにアクセスする信頼できるユーザのアプリケーション検査要件を上書きできます。

Prisma Accessによるアプリケーションの分類方法を変更するには 、**[Manage (管理)]** > **[Configuration (設定)]** > **[NGFWとPrisma Access]** > **[Network Policies (ネットワークポリシー)]** > **[Application Override (アプリケーション オーバーライド)]**に進み、アプリケーションのオーバーライド ポリシー ルールを作成します。

アプリケーション オーバーライドに関するヒント

アプリケーション オーバーライド ポリシー ルールを作成すると、App-IDが展開のトラフィックを分類し、そのアプリケーション識別情報に基づいて脅威検査を実行することを制限していると考えてください。社内の独自アプリケーションをサポートするうえで、Strata Cloud Managerがレイヤ7検査を実行し、アプリケーショントラフィックをスキャンして脅威を検出するように、アプリケーションシグネチャを含むカスタムアプリケーションを（アプリケーションオーバーライドルールの代わりに）作成することを検討する価値があります。カスタムアプリケーションを作成するには、**[Manage (管理)]** > **[Configuration (設定)]** > **[NGFWとPrisma Access]** > **[Objects (オブジェクト)]** > **[Applications (アプリケーション)]**に進みます。

アプリケーションオーバーライドポリシー

以下のセクションを使用して、アプリケーション オーバーライド ルールを設定します。

- **[Source (送信元)]**
  - **[Zones (ゾーン)]**–**[Add (追加)]** [source zones (送信元ゾーン)]
  - ［**Addresses (アドレス)**］ – 送信元アドレス、アドレス グループ、またはリージョンを追加し、設定を指定します。
- **[Destination (宛先)]**
  - **[Zones (ゾーン)]**：宛先ゾーンを選択するために追加します。
  - ［**Addresses (アドレス)**］ – 送信元アドレス、アドレス グループ、またはリージョンを追加し、設定を指定します。
- **[Application (アプリケーション)]**
  - **[Application (アプリケーション)]** – 前述のルール基準に一致するトラフィック フローのオーバーライド アプリケーションを選択します。カスタム アプリケーションをオーバーライドするときに実行される脅威検査はありません。この例外は、脅威検査をサポートする事前に定義されたアプリケーションにオーバーライドする場合です。

    新しいアプリケーションを定義するには、**[Manage (管理)]** > **[Configuration (設定)]** > **[NGFWとPrisma Access]** > **[Objects (オブジェクト)]** > **[Applications (アプリケーション)]**に進みます。
- **Protocol (プロトコル)**
  - **Protocol (プロトコル)**–アプリケーション オーバーライドを許可するプロトコル (**TCP**または**UDP**) を選択します。
  - **Port (ポート)**–指定した宛先アドレスのポート番号 (0 ～ 65535) またはポート番号の範囲 (ポート 1 ～ ポート 2) を入力します。複数のポートまたはポートの範囲はコンマで区切ります。

管理:ポリシー ベース フォワーディング

どこで使用できますか?	何が必要ですか?
• Prisma Access (Managed by Panorama or Strata Cloud Manager) • Software NGFW Creditsによって資金提供されたものを含むNGFW	これらの各ライセンスには、Strata Cloud Managerへのアクセスが含まれています。 ❑ Prisma Access ❑ AIOps for NGFW Premium ❑ Strata Cloud Manager Essentials ❑ Strata Cloud Manager Pro → Strata Cloud Managerで利用できる機能は、使用するライセンスによって異なります。

ポリシー ベース転送(PB)Fルールを使用すると、ルーティング テーブルに指定されたネクストホップからの代替経路を選択させることができます。これは通常、セキュリティまたはパフォーマンス上の理由で出力インターフェースを指定するときに使用します。

開始するのは、 **[Manage (管理)]** > **[Configuration (設定)]** > **[NGFWとPrisma Access]** > **[Network Policies (ネットワーク ポリシー)]** > **[Policy Based Forwarding (ポリシーベース転送)]**に進んでください。

Policy-Based Forwarding (ポリシー ベース転送) ルールを使用して、トラフィックを特定の出力インターフェースに向けることで、そのトラフィックのデフォルトのパスをオーバーライドできます。ポリシーベース転送ルールを作成する前に、IPv4アドレスのセットがIPv6アドレスのセットのサブセットとして扱われることを理解してください。

ポリシーベースの転送ルールを設定するには、次のセクションを参照してください。

- **[Source (送信元)]**
  - **[Zones (ゾーン)]**–**[Add (追加)]** [source zones (送信元ゾーン)]
  - ［**Interface (インターフェース)**］–送信元インターフェイスを追加します。
  - ［**Addresses (アドレス)**］ – 送信元アドレス、アドレス グループ、またはリージョンを追加し、設定を指定します。
  - ［**Users (ユーザー)**］：ポリシーを適用するユーザおよびユーザ グループを追加します。
- **[Destination (宛先)**
  - **Addresses (アドれすぅ)**］：送信元アドレス、アドレス グループ、またはリージョンを追加し、設定を指定します。
- **[Application and Services (アプリケーションとサービス)]**
  - **[Application Entiities (アプリケーションエンティティ)]**–代替パスでルーティングするアプリケーションを選択します。

    つまり、アプリケーションを確認できる十分な情報をファイアウォールが取得する前に、ポリシーベース転送ルールが適用される可能性があります。このため、アプリケーション固有のルールをポリシーベース転送で使用することはお勧めできません。可能な限り、サービスオブジェクトを使用してください。

    カスタム アプリケーション、アプリケーション フィルター、アプリケーション グループはポリシーベース転送ルールで使用できません。
  - **[Service Entities (サービス エンティティ)]**–代替パスでルーティングするサービスおよびサービス グループを選択します。

- ［**Forwarding (転送)**
  - **Action (アクション)]** – パケット照合時に実行するアクションは、次のいずれかから選択できます。
    - **Forward (転送)**–パケットを特定の**Egress Interface (出力インターフェース)** に向けます。
    - **Discard (破棄)** –パケットを廃棄します。
    - **No PBF (PBF なし)**–ルールに定義された送信元、宛先、アプリケーション、またはサービスの条件に一致するパケットを除外します。一致するパケットは、PBFの代わりにルート テーブルを使用します。
  - ［**Egress Interface (出力インターフェース)**］–ポリシーベース転送ルールに一致するトラフィックの転送先のネットワーク情報を選択します。
  - ［**Next Hop (ネクストホップ)**
    - **IP Address (IPアドレス)**］–一致するパケットを転送するIPアドレスを入力するか、IPネットマスク タイプのアドレス オブジェクトを選択します。
    - **[FQDN]**–一致するパケットを転送するFQDNを入力します（または、タイプFQDNのアドレス オブジェクトを選択するか作成します）。
    - **None (なし)**–ネクストホップがないということは、パケットの宛先IPアドレスがネクストホップとして使用されていることを意味します。宛先 IP アドレスが出力インターフェースと同じサブネットに存在しない場合、転送はエラーになります。
  - **[Monitor (監視)]**–モニタリングを有効にして、IPアドレスが指定されていない場合にターゲットIPアドレスまたは Next Hop (ネクストホップ) IPアドレスとの接続を確認します。

管理:NAT

どこで使用できますか?	何が必要ですか?
• Prisma Access (Managed by Panorama or Strata Cloud Manager) • Software NGFW Creditsによって資金提供されたものを含むNGFW	これらの各ライセンスには、Strata Cloud Managerへのアクセスが含まれています。 ❑ Prisma Access ❑ AIOps for NGFW Premium ❑ Strata Cloud Manager Essentials ❑ Strata Cloud Manager Pro → Strata Cloud Managerで利用できる機能は、使用するライセンスによって異なります。

NAT では、ルーティングできないプライベート IPv4 アドレスをグローバルにルーティングできる 1 つ以上の IPv4 アドレスに変換するため、組織のルーティング可能な IP アドレスを節約できます。NATを使用すれば、公開アドレスにアクセスする必要があるホストの真のIPアドレスを非公開にし、ポート転送によってトラフィックを管理できるようになります。また、NATにより同

一の IP サブネットのネットワークが相互通信できるようにして、ネットワーク設計の課題を解決できます。

少なくとも、パケットの送信元ゾーンと宛先ゾーンを照合する NATポリシールールを設定します。ゾーンの他に、パケットの宛先インターフェイス、送信元アドレス、宛先アドレス、およびサービスに基づいて、照合基準を設定できます。複数の NAT ルールを設定できます。

開始するのは、 **[Manage (管理)] > [Configuration (設定)] > [NGFWとPrisma Access] > [Network Services (ネットワーク サービス)] > NAT**に進んでください。

接続の問題をトラブルシューティングします。ルーティングとトンネルの状態を集約的に把握し、詳細をドリルダウンして異常や問題のある構成を見つけます。

管理:SD-WAN

どこで使用できますか?	何が必要ですか?
• SD-WAN	❑ SD-WANライセンス

SD-WAN ポリシー ルールは、アプリケーションおよび/またはサービス、またトラフィック分散プロファイルを指定し、ファイアウォールが既存のセッションに属さず、その他のすべての基準に合致する着信パケットの優先パスを選択する方法を決定します。この基準には、送信元と宛先のゾーン、送信元と宛先の IP アドレス、送信元ユーザー等があります。SD-WAN ポリシールールでは、遅延、ジッター、およびパケット損失のしきい値のパス品質プロファイルも指定できます。いずれかのしきい値の超過があると、ファイアウォールはアプリケーションおよび/またはサービスに新たなパスを選択します。

SD-WANポリシーを設定するには、 **[Manage (管理)] > [Configuration (設定)] > [NGFWとPrisma Access] > [Network Policies (ネットワーク ポリシー)] > [SD-WAN]**を選択します。

ルール

共有コンテクストのプレ ルールとポスト ルールは、共有コンテクストですべての管理対象ファイアウォールの共有ポリシーとして、またはデバイス グループ コンテクストで特定のデバイス グループ用として定義できます。

- **[Pre Rules (プレ ルール)]** – ルール順序の先頭に追加され、最初に評価されるルールです。プレ ルールを使用すれば、組織の利用規約に対する遵守を徹底させることができます。例えば、プレ ルールによって特定の URL カテゴリへのアクセスをブロックしたり、すべてのユーザーの DNS トラフィックを許可することができます。
- **Post Rules**（ポスト ルール） – ルール順序の末尾に追加され、プレ ルールとファイアウォールでローカルに定義されているルールの後に評価されるルールです。通常、ポスト ルールには、**App-ID™**、**User-ID™**、またはサービスに基づいてトラフィックへのアクセスを拒否するルールが含まれます。

プロファイル

SD-WAN ポリシー ルールで指定されたアプリケーションとサービスのセットに適用するプロファイルを作成します。

パスの品質

SD-WAN を使用すると、一意のネットワーク品質要件を持つアプリケーション、アプリケーション フィルタ、アプリケーション グループ、サービス、サービス オブジェクト、およびサービス グループ オブジェクトの各セットのパス品質プロファイルを作成し、SD-WAN ポリシー ルールでそのプロファイルを参照できます。プロファイルでは、レイテンシー、ジッター、パケットロスの 3 つのパラメータに最大しきい値を設定します。SD-WAN リンクがいずれかのしきい値を超えると、ファイアウォールは、このプロファイルを適用した SD-WAN ルールに一致するパケットに新しい最適パスを選択します。

SaaS の品質

SD-WAN を使用すると、Software-as-a-Service（SaaS）品質プロファイルを作成し、ハブまたはブランチ ファイアウォールとサーバー側 SaaS アプリケーション間のパスの健全性の質を測定し、パスの健全性の質が低下した場合の SaaS アプリケーションの信頼性とスワップ パスの正確なモニタリングが可能となります。これにより、ファイアウォールは、別のDirect Internet Access（DIA、ダイレクト インターネット アクセス）リンクにフェイルオーバーするタイミングを正確に決定することができます。

SaaS 品質プロファイルを使用すると、アプリケーション アクティビティを監視するアダプティブ ラーニング アルゴリズムを利用して、あるいはアプリケーションの IPアドレス、FQDN、または URL を使用し、SaaS アプリケーションを指定して、監視する SaaS アプリケーションを指定できます。

トラフィックの配布

このトラフィック分散プロファイルでは、セッションの分散と、パスの品質が低下したときにより適切なパスにフェイルオーバーするためにファイアウォールが使用する方法を選択します。ファイアウォールが SD-WAN トラフィックを転送するリンクを決定する際に考慮するリンク タグを追加します。作成した各 SD-WAN ポリシー ルールにトラフィック分散プロファイルを適用します。

エラーの修正

音声、VoIP、ビデオ会議等、パケットの損失や破損に影響を受けやすいアプリケーションが SD-WAN トラフィックに含まれている場合、エラー訂正の手段として、Forward Error Correction（FEC、転送エラー修正）またはパケット複製のいずれかを適用することができます。FEC を使用すると、受信ファイアウォール（デコーダ）は、エンコーダがアプリケーション フローに埋め込むパリティ ビットを使用することにより、損失したパケットや破損したパケットを回復することができます。エラー訂正の代替方法であるパケット複製では、アプリケーション セッションが 1 つのトンネルから 2 番目のトンネルに複製されます。これらの方法のいずれかを使用するには、Error Correction Profile（エラーの修正プロファイル）を作成し、特定のアプリケーションの SD-WAN ポリシー ルールで参照します。

（また、ファイアウォールがエラー修正で選択可能なインターフェースを、SD-WAN Interface Profile（SD-WAN インターフェース プロファイル）で、インターフェースが Eligible for Error Correction Profile interface selection（エラーの修正プロファイル インターフェース選択に適格）を明らかにして指定する必要があります。）

SD-WAN インターフェイス

SD-WAN インターフェース プロファイルを作成して ISP 接続の特性を定義し、リンクの速度およびファイアウォールのリンク監視頻度を指定し、リンクのリンクタグを指定します。複数の

リンクで同じリンクタグを指定すると、物理リンクがリンクバンドルあるいはファットパイプにグループ化 (バンドル化) されます。イーサネット インターフェースを保存する前に、SD-WAN インターフェース プロファイルを設定し、SD-WAN 対応イーサネット インターフェースで SD-WAN インターフェースを指定する必要があります。

Link Tags (リンク タグ)

リンクタグを作成して、SD-WAN トラフィック分散およびフェイルオーバー保護中にアプリケーションとサービスが特定の順序で使用する 1 つまたは複数の物理リンクを識別します。複数の物理リンクをグループ化すると、物理リンクの状態が悪化した場合に、アプリケーションとサービスの品質を最大化することができます。

リンクをグループ化する方法を計画する際は、リンクの使用または目的を考慮して、適切にグループ化を行います。例えば、低コストあるいはビジネスクリティカル以外のトラフィックを対象とするリンクを設定している場合、リンクタグを作成してインターフェースをグループ化し、トラフィックがビジネスに不可欠なアプリケーションあるいはサービスに影響を与える可能性がある高コストのリンクではなく、主にこの低コストリンクを通過させることができます。

管理:ID サービス

どこで使用できますか?	何が必要ですか?
• Prisma Access (Managed by Panorama or Strata Cloud Manager) • Software NGFW Creditsによって資金提供されたものを含むNGFW	これらの各ライセンスには、Strata Cloud Managerへのアクセスが含まれています。 ❑ Prisma Access ❑ AIOps for NGFW Premium ❑ Strata Cloud Manager Essentials ❑ Strata Cloud Manager Pro → Strata Cloud Managerで利用できる機能は、使用するライセンスによって異なります。

IDサービスを管理し、特定のユーザーのみがネットワーク上の適切なデータにアクセスできることを確認する方法を学びます。

開始するのは、 **[Manage (管理)] > [Configuration (設定)] > [NGFWとPrisma Access] > [Identity Services (IDサービス)]**に進んでください。

IDサービスを使用すると、次のことが可能になります。

- PrismaAccessをアイデンティティプロバイダ（IdP）に接続し、管理:認証で使用する認証方法を選択することで、正当なユーザーのみがネットワークにアクセスできるようになります。
- 管理:Cloud Identity EngineでActive Directory(アクティブディレクトリ)情報への読み取り専用アクセスをPrisma Accessに許可します。
- セキュリティ ポリシーを一貫して適用し、リモートネットワークサイトやサービス接続サイト（本社やデータセンター）のオンプレミスデバイスと管理:アイデンティティ情報再配信でIDデータを共有できます。

管理:認証

どこで使用できますか?	何が必要ですか?
• Prisma Access (Managed by Panorama or Strata Cloud Manager) • Software NGFW Creditsによって資金提供されたものを含むNGFW	これらの各ライセンスには、Strata Cloud Managerへのアクセスが含まれています。 ❑ Prisma Access ❑ AIOps for NGFW Premium ❑ Strata Cloud Manager Essentials ❑ Strata Cloud Manager Pro

どこで使用できますか?	何が必要ですか?
	→ Strata Cloud Managerで利用できる機能は、使用するライセンスによって異なります。

最も保護されたリソースに正当なユーザーのみがアクセスできるようにするために、Prisma Access は、SAML、TACACS+、RADIUS、LDAP、Kerberos、MFA、ローカル データベース認証、SSO のサポートなど、複数の認証タイプをサポートしています。

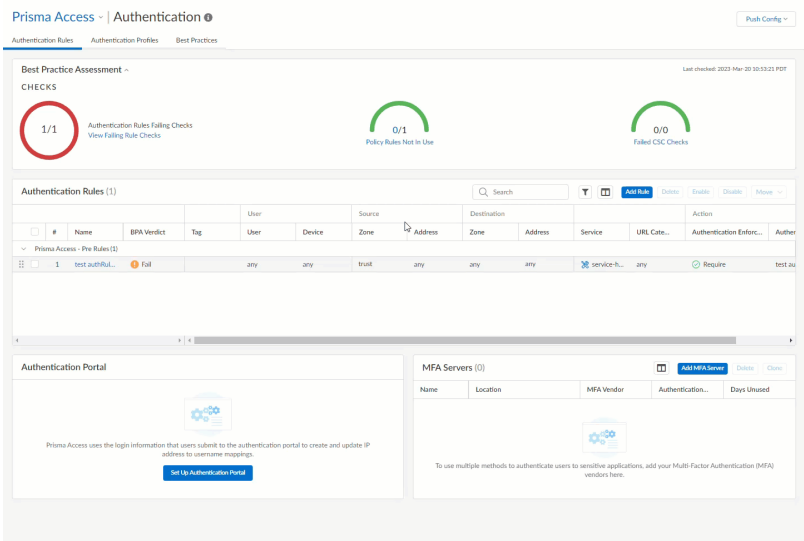
認証ポリシーをセットアップするには、**[Manage (管理)]** > **[Configuration (設定)]** > **[NGFWとPrisma Access]** > **[Identity Services (IDサービス)]** > **[Authentication(認証)]**に進みます。

Prisma Access が認証を提供するために統合するサービスと、認証のセットアップを計画する際に考慮すべき機能は次のとおりです。

認証サポート

SAML	ユーザーがネットワーク外のサービスおよびアプリケーションにアクセスする場合、SAML を使用してPrisma Accessを内外両方のサービスおよびアプリケーションに対するアクセスを制御するアイデンティティ プロバイダ（IdP）と統合できます。SAMLシングル サインオン(SSO)を使用すると、1回のログインで複数のアプリケーションにアクセスできるようになります。これは、各ユーザーが多数のアプリケーションにアクセスし、アプリケーションごとに認証を行うとユーザーの生産性が低下するような環境で役立ちます。この場合、SAML シングル サインオン(SSO)により、1回のログインで複数のアプリケーションにアクセスできるようになります。同様に、SAML シングル ログアウト（SLO）により、ユーザーが一つのセッションからログアウトするだけで複数のアプリケーションのセッションを終了できるようにすることが可能です。SSOは、GlobalProtectアプリを通じてアプリケーションにアクセスするモバイル ユーザー、または認証ポータルを通じてアプリケーションにアクセスするリモート ネットワークのユーザーに対して機能します。SLOはGlobalProtectアプリ ユーザーが利用できます。 認証シーケンスでは*SAML*認証プロファイルを使用できません。
TACACS+	Terminal Access Controller Access-Control System Plus（TACACS+）は、中央のサーバーを通して一元的に本人確認および認証を行えるようにするプロトコルの一種です。TACACS+ はユーザー名およびパスワードを暗号化するため、パスワードのみを暗号化する RADIUS よりも安全で

	す。また、UDP を使用する RADIUS と異なり、TACACS+ は TCP を使用するためより安定しています。
RADIUS	Remote Authentication Dial-In User Service（RADIUS）は、広くサポートされているネットワーク プロトコルであり、一元的な本人確認および認証を提供します。Prisma AccessにRADIUSサーバーを追加して、多要素認証を実装することもできます。
LDAP	Lightweight Directory Access Protocol（LDAP）は、情報ディレクトリにアクセスするための標準的なプロトコルです。LDAPを使用して、認証ポータルを通じてアプリケーションまたはサービスにアクセスするユーザーを認証できます。
Kerberos	Kerberosは、当事者を識別するための固有のキー (チケットと呼ばれる) を使用して当事者間での安全な情報交換を可能にする認証プロトコルです。Kerberosを使用すると、認証ポータルを通じてアプリケーションにアクセスするユーザーを認証できます。Kerberos SSO が有効な場合、ユーザーはネットワークに初めてアクセスした際だけログインを求められます（Microsoft Windows へのログインなど）。この最初のログイン後、ユーザーはSSOセッションの有効期限が切れるまで再度ログインすることなく、ネットワーク内の任意のブラウザベースのサービスにアクセスできます。 Kerberosを使用するには、まずユーザーを認証するPrisma AccessのKerberosアカウントが必要です。Kerberos キータブを作成するためにアカウントが必要です。キータブとは、ファイアウォールあるいはPanoramaのプリンシパル名およびハッシュされたパスワードを含むファイルです。SSO プロセスにはキータブが必要です。 Kerberos SSO は、Kerberos 環境の内部にあるサービスおよびアプリケーションに対してのみ利用できます。外部のサービスおよびアプリケーションに対して SSO を有効化する場合、SAMLを使用します。
Cloud Identity Engine	Cloud Identity Engine (CIE) は、Prisma Access - Explicit Proxyのデプロイメントにおいてモバイル ユーザーに対してユーザー識別とユーザー認証の両方を提供します。Cloud Identity Engineは、Explicit Proxy認証キャッシュ サービス(ACS)と統合され、SAML IDプロバイダ(IdP)を使用してExplicit Proxyモバイル ユーザーに認証を提供します。
MFA	多要素認証(MFA)を使用すると、異なるタイプ(要素と呼ばれる) の複数の認証チャレンジを実装して、最も機密性の高いサービスとアプリケーションを保護できます。例えば、重要

	な財務文書に対しては、検索エンジンよりも強力な認証が必要になるかもしれません。 Prisma Accessには、サポートされているMFAベンダーのリストが組み込まれており、新しいベンダーが追加されると自動的に更新されます。 
ローカルデータベース認証	Prisma Access上でローカルに実行され、ユーザー アカウント (ユーザー名とパスワード、またはハッシュ化されたパスワード) が含まれるデータベースを作成します。このタイプの認証は、プレーンテキストのパスワードを知らず、パスワードのハッシュだけを知っているケースで、既存の UNIX アカウントの認証情報を再利用するユーザーアカウントを作成する際に便利です。プレーンテキストのパスワードを使用するアカウントの場合、パスワードの複雑さおよび有効期限を設定することもできます。この認証方法は、認証ポータルまたはGlobalProtectアプリを通じてサービスやアプリケーションにアクセスするユーザーが利用できます。

認証機能のハイライト

SSO	SAMLまたはKerberos を使用している場合は、シングル サインオン(SSO)を実装できます。これにより、ユーザーは1回認証するだけで複数のサービスやアプリケーションにアクセスできるようになります。SAML および Kerberos が SSO をサポートしています。
認証ポータル	認証ルールに一致するWeb要求をPrisma Accessログイン ページにリダイレクトし、認証を求めます。Prisma Accessは、ユーザーがこの認証ポータルに送信する情報を

	使用して、IP アドレスとユーザー名のマッピングを作成または更新します。 これはリモート ネットワークの場合に特に役立ち、ユーザー(またはグループ)に基づいてトラフィックを継続的に監視および適用できます。ユーザーが認証ルールに一致するWebトラフィック(HTTPまたはHTTPS)を開始すると、Prisma Accessはユーザーに認証ポータルを通じて認証するように要求します。Prisma Accessは、ユーザーがポータルに送信する情報に基づいて、IPアドレス - ユーザー名間マッピングを作成または更新します。これにより、リモート ネットワーク サイトで誰が最も機密性の高いアプリケーションやデータにアクセスしているかを正確に把握できるようになります。
認証シーケンス	異なる目的で複数の種類の認証を使用する場合、認証シーケンスを設定してプロファイルを順位付けすることができます。Prisma Access は、ユーザーの認証に成功するまで、この順位に基づいて各プロファイルをチェックします。

認証の仕組み

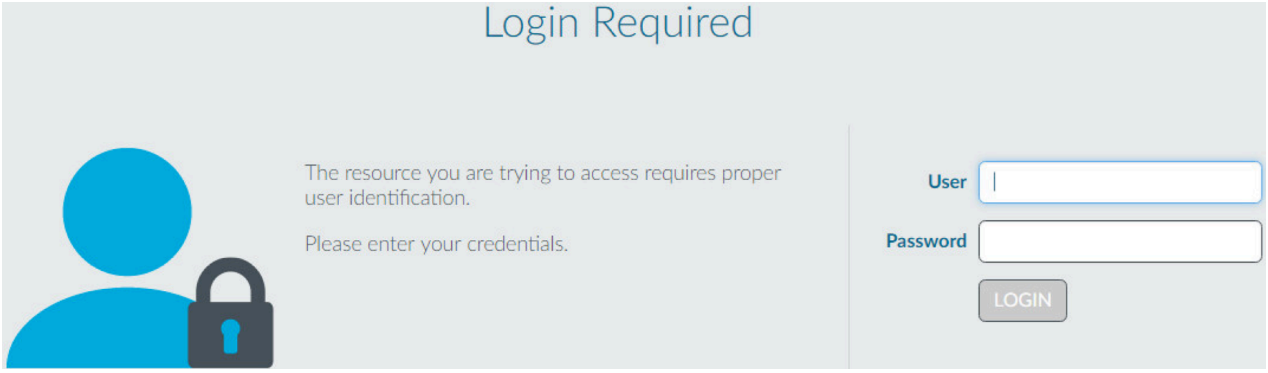
組織の認証サービスをPrisma Accessに追加すると (手順はこちら)、Prisma Accessは複数のポイントでユーザーを認証します。

- **Prisma Access**に接続すると

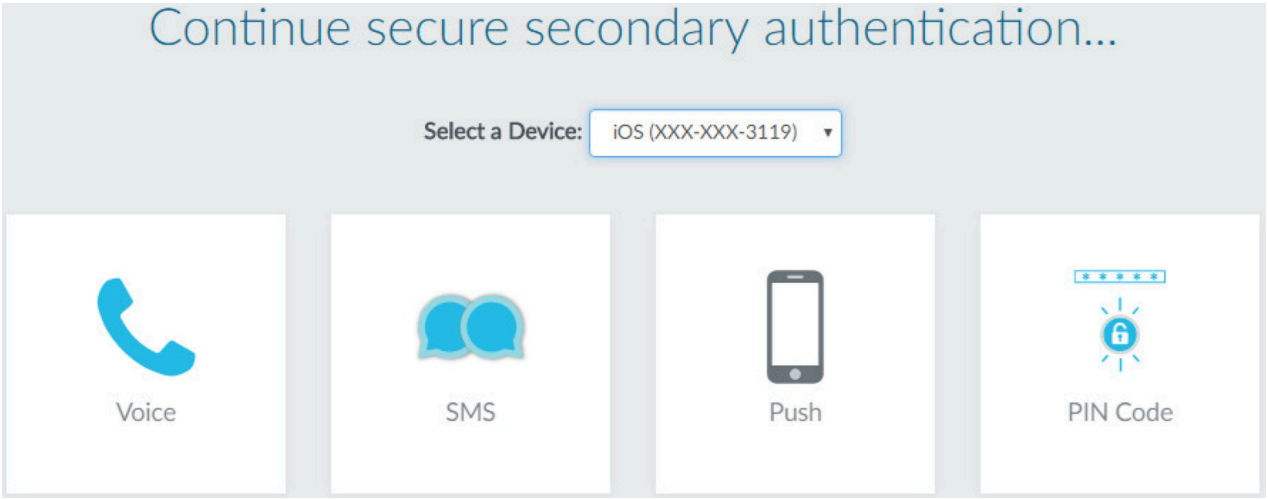
  モバイル ユーザーがPrisma Accessに対して認証する方法を定義する方法はこちらよりご確認いただけます。リモート ネットワーク トラフィックは安全なVPNトンネルを介してルーティングされるため、リモート ネットワークのユーザーがPrisma Accessに接続するための認証設定を定義する必要はありません。
- ユーザートラフィックが追加の認証の要件を満たしている場合

  エンタープライズ アプリケーションや保護されたネットワーク リソースにアクセスするために、ユーザーに (1つまたは複数の方法を使用して) 認証を要求する方法はこちらよりご確認いただけます 。

ユーザーが認証要件に一致するWebトラフィックを生成すると、Prisma Accessは、ログインとパスワード、音声、SMS、プッシュ、ワンタイム パスワード(OTP)認証などの1つ以上の方法 (要素) を使用して認証するようにユーザーに要求することで、ユーザーが正当であることを確認します。Prisma Accessが使用する要素はすべて、 認証プロファイルで指定した認証サービスと設定に基づいています。最初の要素 (ログインとパスワード) については、ユーザーは認証ポータルを通じて認証します。



その他の要素については、ユーザーは多要素認証ログイン ページを通じて認証します。



ユーザーを認証した後、Prisma Accessはセキュリティ ルールを評価して、アプリケーションへのアクセスを許可するかどうかを決定します。Prisma Accessは、安全なアクセスのために指定されたアプリケーション、サービス、またはリソースにユーザーがアクセスしようとするすべてのアクティビティを記録します。

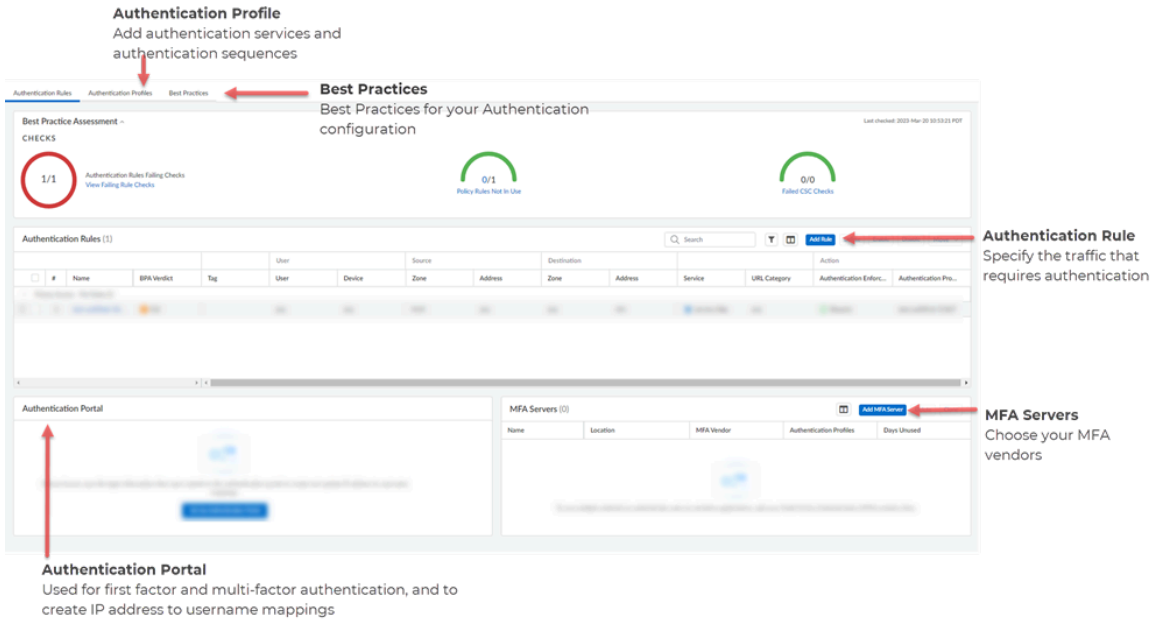
管理:認証のセットアップ

どこで使用できますか?	何が必要ですか?
• Prisma Access (Managed by Panorama or Strata Cloud Manager)	以下のいずれかです。 ❑ Prisma Accessライセンス ❑ Strata Cloud Manager Pro → Strata Cloud Managerで利用できる機能は、使用するライセンスによって異なります。

Prisma AccessをStrata Cloud Managerに認証を設定するには、まずPrisma Accessに認証サービスを追加します。次に、認証を要求するトラフィックを指定します。これらの設定に基づい

て、MFAや認証シーケンスなどの認証機能を追加したり、Prisma AccessでIPアドレスとユーザー名のマッピングを作成および更新したりできます。

Prisma Accessによる認証を有効にするために必要な設定がすべて一箇所にまとめられています。**[Manage (管理)]** > **[Identity Services (IDサービス)]** > **[Authentication (認証)]**。

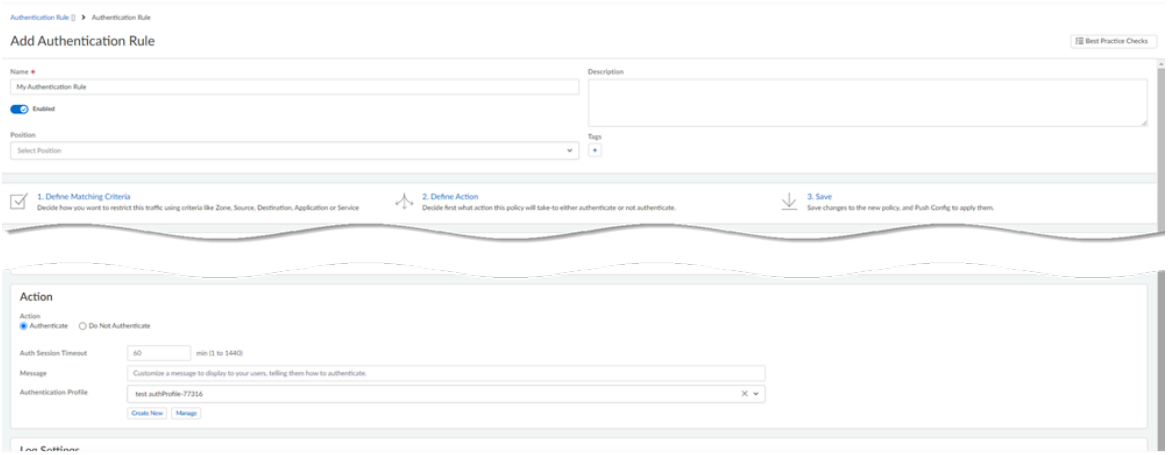


認証ルールここでは認証を要求するトラフィックを指定します

認証ルールの設定には、ルールへの認証プロファイルの追加も含まれます。Prisma Accessは、認証ルールに一致するトラフィックを検出すると、認証プロファイルで定義され

た認証方式と設定を一致するトラフィックに適用します。プロファイルは、ユーザーが認証を受けるために必要な方法を定義するものです。

1. **Manage (管理) > Identity and Access Services (IDとアクセスサービス) > Authentication (認証) > Authentication Rule (認証ルール)**、そして**[Add Authentication Rule (認証ルールの追加)]**に順に移動します。
2. 認証を必要とするユーザー、サービス、URLカテゴリを定義します。
3. ルールのアクションを ［**Authenticate (認証)**］ に設定し、このルールに一致するトラフィックに使用する認証方式を定義するプロファイルを選択します。



認証プロファイルここに認証サービスを追加し、認証設定を定義します

ユーザーの認証に使用するサービス（SAML、TACACS+、RADIUS、LDAP、Kerberos）にPrisma Accessを接続し、認証設定を定義します（たとえば、ログイン試行の失敗に対する制限を設定します）。

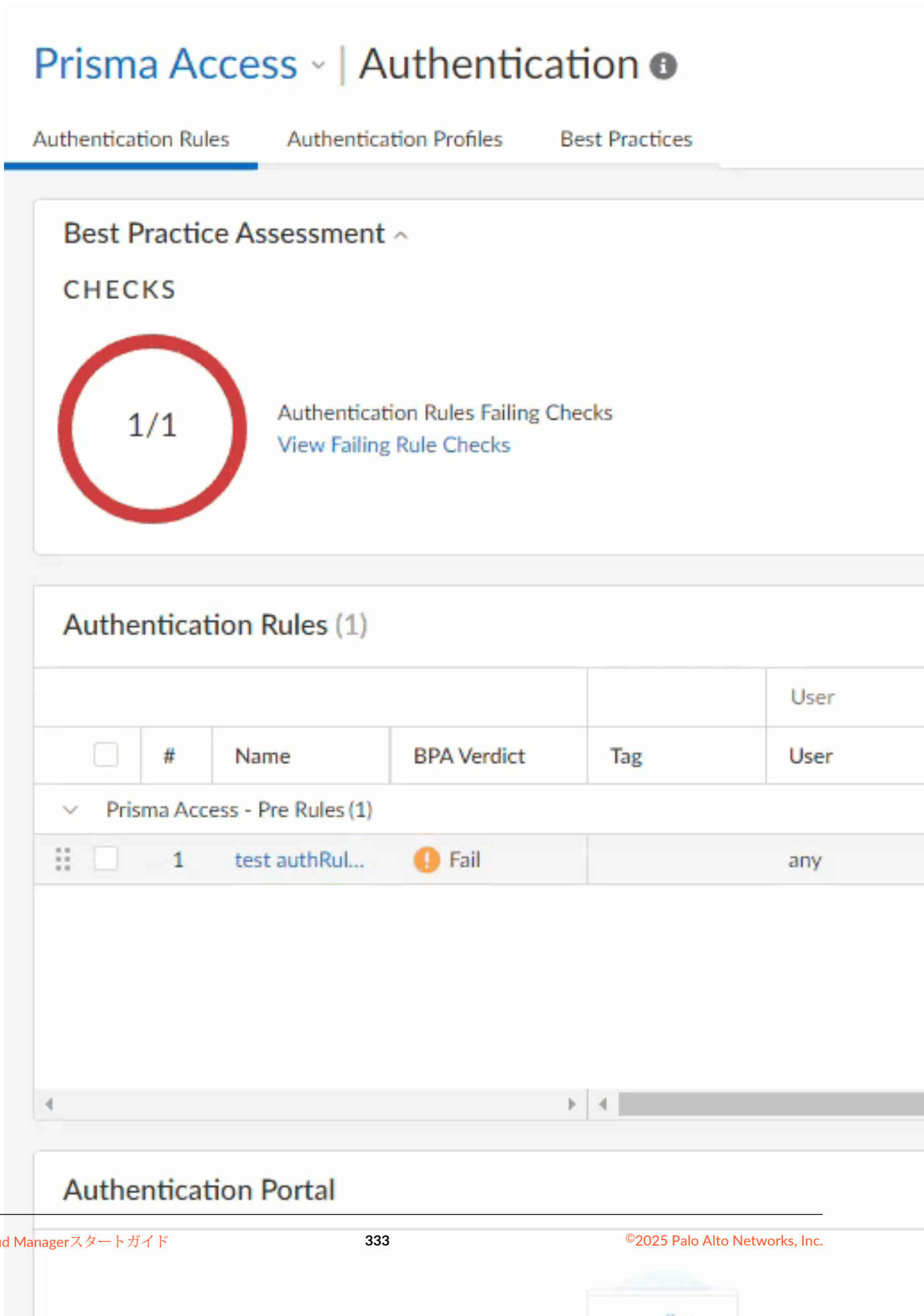
オンプレミス認証サービスを使用している場合は、まずオンプレミス認証サービスを*Prisma Access*に接続するサービス接続を作成する必要があります。次に、ここに戻って認証プロファイルを設定します。

[Manage (管理)] > [Identity and Access Services (IDとアクセスサービス)] > [Authentication (認証)] > [Authentication Profile (認証プロファイル)] > [Add Profile (プロファイルの追加)]に移動し、プロファイルの設定から始めます。**[Auth Type (認証タイプ)]**:

Prisma Accessがサービスに接続できるようにする、選択した認証サービスの詳細を追加し、ユーザー資格情報とロール権限を読み取るように求められます。認証をカスタマイズするための追加設定はプロファイルで提供され、設定している認証の種類によって異なる場合があります。

MFAサーバー使用しているMFAベンダーを指定

機密性の高いアプリケーションに対するユーザー認証に複数の方法を使用するには、使用するMFAベンダーを追加することから始めます(**MFA**サーバーの追加)。Prisma Accessでは、MFAベンダーのリストを提供しており、その中から選択できます。

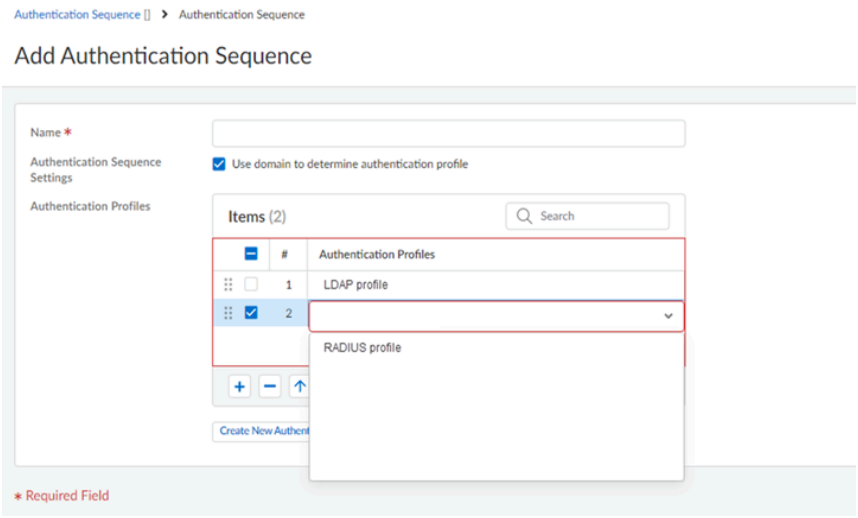


認証ポータルリモートネットワークサイトのユーザー用の認証ポータル(別名キャプティブポータル)を設定し、Prisma AccessでIPアドレスとユーザー名のマッピングを作成できるようにする

第1要素認証(ログインとパスワード)の場合、リモートネットワークサイトのユーザーは認証ポータルを通じて認証を受ける必要があります。認証が成功すると、Prisma Accessは必要な追加認証要素ごとにMFAログインページを表示します。Prisma Accessは、ユーザーが送信した資格情報を使用して、IPアドレス - ユーザー名間マッピングを作成および更新します。つまり、リモートネットワークサイトの誰がウェブコンテンツやエンタープライズアプリケーションにアクセスしているかを常に把握できます。

認証シーケンスPrisma Accessで試したい順に認証プロファイルをランク付けする

[Manage (管理)] > [Identity and Access Services (IDとアクセスサービス)] > [Authentication (認証)] > [Authentication Profile (認証プロファイル)]および**[Add Authentication Sequence (認証シーケンスを追加)]**を選択して、認証プロファイルをランク付けします。Prisma Accessは、1つがユーザー認証に成功するまで、それぞれを順番にチェックします。



管理:認証プロファイル

どこで使用できますか?	何が必要ですか?
• Prisma Access (Managed by Panorama or Strata Cloud Manager)	以下のいずれかです。 ❑ Prisma Accessライセンス ❑ Strata Cloud Manager Pro → Strata Cloud Managerで利用できる機能は、使用するライセンスによって異なります。

認証プロファイルは、ファイアウォールの Web インターフェイスにアクセスする管理者、およびキャプティブポータルあるいは GlobalProtect を通じてアプリケーションにアクセスするエンドユーザーのログイン情報を検証する認証サービスを定義します。また、認証プロファイルはシングルサインオン（SSO）などのオプションも定義します。

- Kerberos
- Cloud Identity Engine

Cloud Identity Engine

どこで使用できますか?	何が必要ですか?
• Prisma Access (Managed by Strata Cloud Manager)	❑ Prisma Accessライセンス

Cloud Identity Engine (CIE) は、Prisma Access - Explicit Proxyのデプロイメントにおいてモバイル ユーザーに対してユーザー識別とユーザー認証の両方を提供します。Cloud Identity Engineは、Explicit Proxy認証キャッシュ サービス(ACS)と統合され、SAML IDプロバイダ(IdP)を使用してExplicit Proxyモバイル ユーザーに認証を提供します。

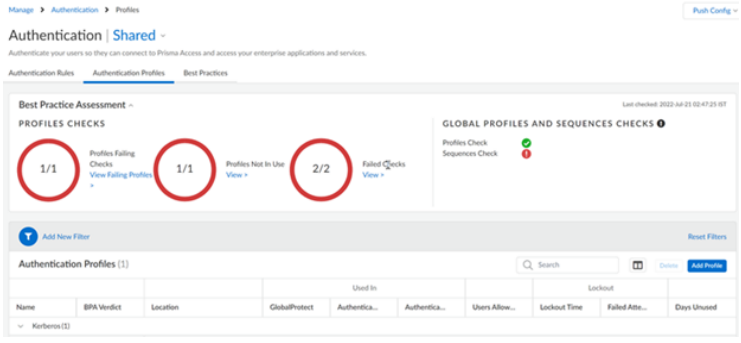
Cloud Identity Engineでユーザーを認証するための認証プロファイルを構成します。

SAML/CIE認証方式は、クラウド認証サービス（CAS）が有効になっている場合にのみ表示されます。CIE認証またはCASがPrisma Accessテナントでサポートされていない場合は、SAML認証方式のみが表示されます。

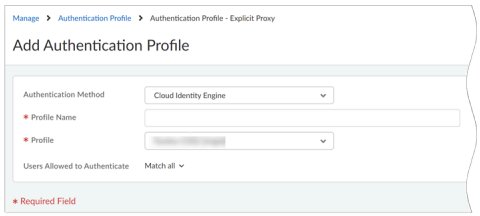
開始する前に：

- 明示プロキシガイドラインを確認します。
- Cloud Identity Engineで認証プロファイルをセットアップします。

STEP 1 | **[Manage (管理)] > [Configuration (設定)] > [Identity Services (IDサービス)] > [Authentication (認証)]**に進み、設定スコープを［明示的なプロキシ］ に設定し 、 ［認証プロファイル］の［プロファイルの追加]を選択します。



STEP 2 | **[Authentication Method (認証方法)]**の方法を選択します:**Cloud Identity Engine**。



STEP 3 | 一意のプロファイル名を入力します。

STEP 4 | Cloud Identity Engineで設定したCloud Identity Engine認証プロファイルを選択します。

STEP 5 | 変更を保存します。

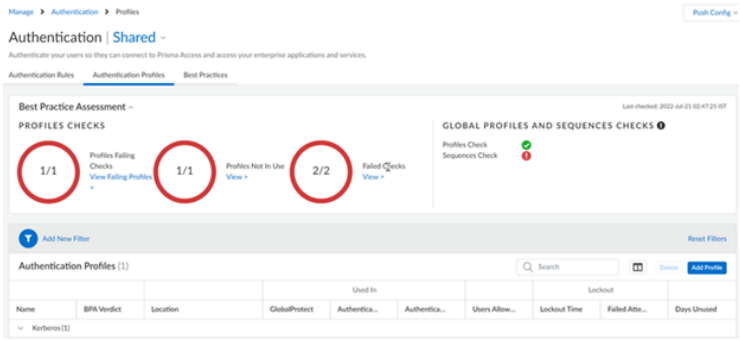
Kerberos

どこで使用できますか?	何が必要ですか?
• Prisma Access (Managed by Strata Cloud Manager)	❑ Prisma Accessライセンス

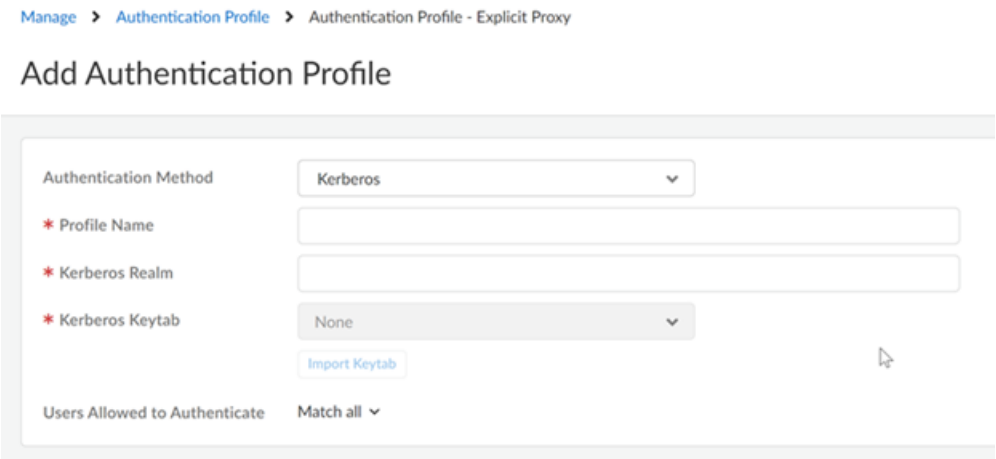
Kerberos は、チケットを使用して、保護されていないネットワークを介して通信するノードが、身元を互いに安全に証明できるようにするコンピュータネットワーク認証プロトコルです。

認証プロファイルは、ポータルまたはゲートウェイがユーザーを認証する際に使用するサーバープロファイルを指定します。Explicit Proxyモバイルユーザーが Prisma Accessに接続するためのKerberos認証プロファイルを設定する手順は、次のとおりです。

STEP 1 | **[Manage (管理)]** > **[Configuration (設定)]** > **[Identity Services (IDサービス)]** > **[Authentication (認証)]** > **[Authentication Profiles (認証プロファイル)]**および**[Add Profile (プロファイルを追加)]**に移動します。



STEP 2 | **[Authentication Method (認証方法)]**の方法を選択します:**Kerberos**。



STEP 3 | サーバープロファイルを識別する**[Profile Name**（プロファイル名）**]**を入力します。認証プロファイルは、ポータルまたはゲートウェイがユーザーを認証する際に使用するサーバープロファイルを指定します。

STEP 4 | **Kerberos Realm**（**Kerberos** レルム）を入力して（最大 127 文字）、ユーザーのログイン名のホスト名部分を指定します。例: ユーザー アカウント名が user@EXAMPLE.LOCAL の場合、レルムは EXAMPLE.LOCAL になります。

STEP 5 | Kerberosアカウント情報を含む**Kerberos Keytab**ファイルをインポートします。入力を促されたら、キータブ ファイルのBrowse（参照）を行い、**[Save (保存)]**をクリックします。認証中は、エンドポイントは最初にキータブを使用して SSO の確立を試みます。

STEP 6 | ［**Kerberos Key**］タブを選択します。

STEP 7 | **[Save(保存)]**をクリックします。

管理:Cloud Identity Engine

どこで使用できますか?	何が必要ですか?
• Prisma Access (Managed by Panorama or Strata Cloud Manager) • Software NGFW Creditsによって資金提供されたものを含むNGFW	これらの各ライセンスには、Strata Cloud Managerへのアクセスが含まれています。 ❑ Prisma Access ❑ AIOps for NGFW Premium ❑ Strata Cloud Manager Essentials ❑ Strata Cloud Manager Pro → Strata Cloud Managerで利用できる機能は、使用するライセンスによって異なります。

Cloud Identity Engine (ディレクトリ同期) は、Prisma Accessに アクティブディレクトリ情報への読み取り専用アクセスを許可します。これにより、ユーザーやグループのセキュリティポリシーや復号化ポリシーを簡単に設定および管理できるようになります。

Cloud Identity Engineは、オンプレミスのアクティブディレクトリとAzureアクティブディレクトリの両方で動作します。

Prisma AccessでCloud Identity Engineをセットアップするには、まずハブに行ってCloud Identity Engineをアクティブにし、Prisma Accessに追加します。次に、Prisma Accessにアクセスして、Prisma Accessがディレクトリデータにアクセスできることを確認します。

STEP 1 | Cloud Identity Engineのアクティベート

Cloud Identity Engineは、ハブ上のサポートされている任意のアプリとアクティブディレクトリ情報を共有できます。無料で、利用開始に認証コードは必要ありません。Cloud Identity Engineセットアップには、ハブでのCloud Identity Engineアプリの有効化、Active Directoryマッピングを収集するためのCloud Identity Engineエージェントの構成、Cloud Identityとエージェント間の相互認証の構成が含まれます。

Cloud Identity Engineインスタンスは、Prisma AccessとStrata Logging Serviceをデプロイしたのと同じリージョンにデプロイしてください。

STEP 2 | Prisma AccessのCloud Identity Engineを有効にする。

Prisma AccessをCloud Identity Engineに関連付けるには、Prisma Accessの初回有効化時またはそれ以降にいつでも行うことができます。

- **Prisma Access**を起動している間:Cloud Managed Prisma Accessを最初にアクティブ化するときに、Prisma Accessで使用するCloud Identity Engineインスタンスを選択できます。Prisma Accessと同じリージョンにデプロイされているインスタンスを必ず選択してください。
- **Prisma Access**を有効化したら、以下のようになります。既存のPrisma Accessインスタンスに対してCloud Identity Engineを有効にするには、ハブにログインします。ハブ設定のドロップダウン（上部メニューバーの歯車を参照）から、［アプリを管理］を選択します。更新するPrisma Accessインスタンスを見つけ、Prisma Accessで使用するCloud Identity Engineインスタンスを選択します。

STEP 3 | Prisma AccessがCloud Identity Engineに接続されていること、Cloud Identity EngineがPrisma Accessとディレクトリ情報を共有していることを確認します。

- 自分のディレクトリがPrisma Accessで確認できることを確認します。

  [Manage (管理)] > [Configuration (設定)] > [Identity Services (IDサービス)] > [Cloud Identity Engine]に移動します。
- ポリシールールにユーザおよびグループを追加できることを確認します。

  [Manage (管理)] > [Security Services (セキュリティサービス)] > [Security (セキュリティ)]または**[Decryption (復号化)]**を選択します。セキュリティまたは復号ポリシー規則で、[ユーザー]ドロップダウンにアクティブディレクトリユーザーおよびグループエン

トリが表示されることを確認します。これで、これらのユーザーとグループをセキュリティおよび復号ポリシールールに追加できます。

想定どおりに実施されていないトラフィックをトラブルシューティングします。特定のファイアウォールのステータスをチェックして、想定されているポリシー（設定済み）と実施されているポリシーが一致しないかどうかを把握できます。

管理:アイデンティティ情報再配信

どこで使用できますか?	何が必要ですか?
• Prisma Access (Managed by Panorama or Strata Cloud Manager) • Software NGFW Creditsによって資金提供されたものを含むNGFW	これらの各ライセンスには、Strata Cloud Managerへのアクセスが含まれています。 ❑ Prisma Access ❑ AIOps for NGFW Premium ❑ Strata Cloud Manager Essentials ❑ Strata Cloud Manager Pro → Strata Cloud Managerで利用できる機能は、使用するライセンスによって異なります。

Strata Cloud Managerを使用して、NGFWとPrisma AccessのID再配信を設定および管理します。

- Prisma Access
- NGFW

アイデンティティ情報再配信 (Prisma Access)

セキュリティ ポリシーを一貫して適用できるように、Prisma AccessはGlobalProtectがローカルで検出したIDデータをPrisma Access環境全体で共有します。Prisma Accessは、リモートネットワークサイトやサービス接続サイト（本社やデータセンター）のオンプレミスデバイスとIDデータを共有することもできます。

Prisma Access Cloud Managementでは、IDデータの再配信をデフォルトで一部有効にし、残りの部分については、再配信を有効にする設定を非常にシンプルにしました（共有するデータを選択するチェックボックスをオンにするだけです）。

アイデンティティ配信ダッシュボードから、アイデンティティデータの共有方法を確認し、データの再配信を管理できます（**Manage (管理)** > **Configuration (設定)** > **Identity Services (IDサービス)** > **Identity Redistribution (ID再配信)**。

再配信できるアイデンティティデータには、次のものがあります。

- HIPデータ
- IPアドレスとタグのマッピング

- IPアドレスとユーザのマッピング
- ユーザーとタグのマッピング
- 隔離されたデバイス

IDの再配信を始める:

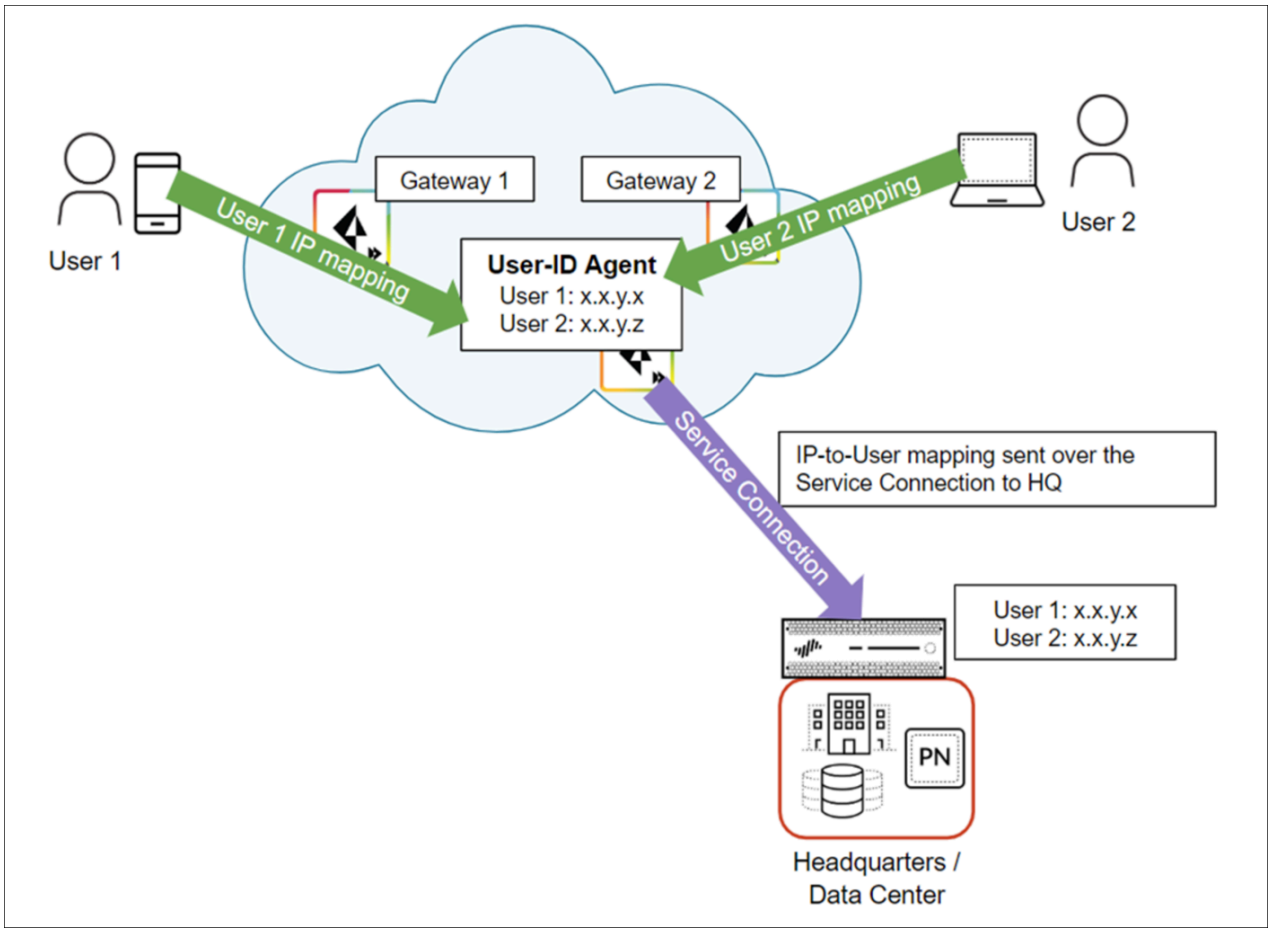
ID再配信の仕組み

モバイルユーザーが、ユーザーベースのポリシーを持つデバイスによって保護されたリモートネットワークロケーションまたは本社/データセンターのリソースにアクセスするには、プリズマアクセスのモバイルユーザーとリモートネットワークのユーザーのIDデータを、そのオンプレミスデバイスに再配信する必要があります。

ユーザーがPrisma Accessに接続すると、Prisma AccessはユーザーのIDデータを収集して保存します。

次の例は、Prisma Accessで既存のIPアドレス対ユーザー名マッピングを持っている、2人のモバイルユーザーを表したものです。次にPrisma Accessはサービス接続を使って、本社/データセンターを保護するオンプレミスデバイスにマッピングを再配信します。

Prisma Access Cloud Managementは、サービス接続をID再配信エージェント（User-IDエージェントとも呼ばれる）として自動的に機能させる。



IDの再配信を設定する

サービス接続の設定を確認する

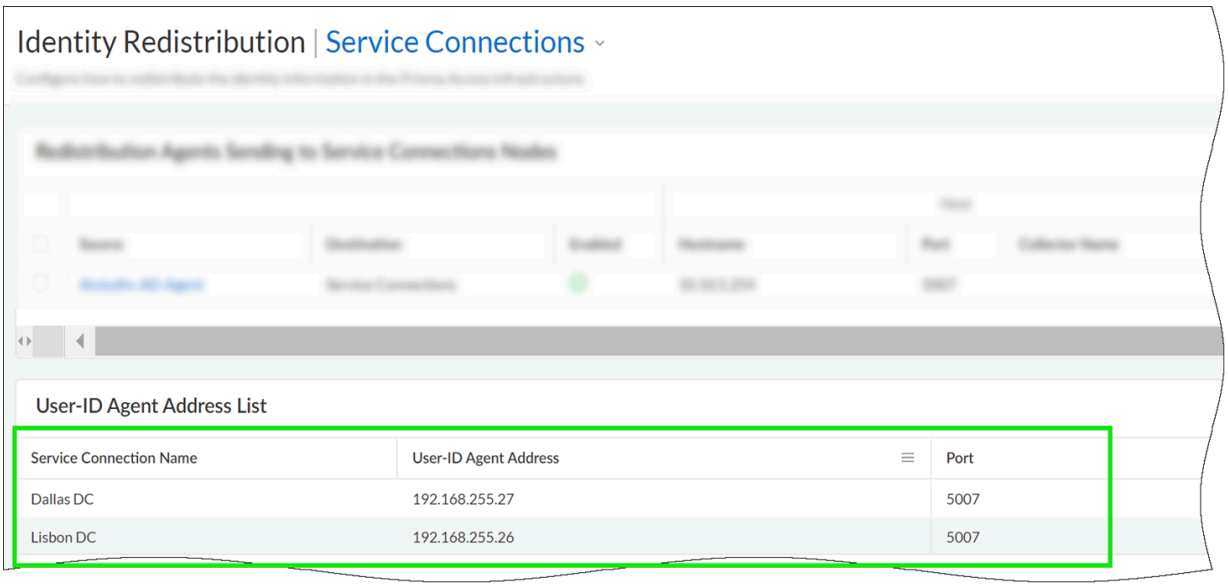
本社またはデータセンターにサービス接続をまだ設定していない場合は、まずサービス接続を設定します。Prisma AccessでIDデータを環境全体で共有するためには、サービス接続が必要です。Prisma Accessでは、サービス接続が自動的に再配信エージェントとして動作するようにします。新規作成したサービスコネクションサイトにユーザー ID エージェント アドレスが割り当てられていることが確認できたら、このサイトを再配信エージェントとして使用できます。Prisma Access ではこの処理が自動的に行われ、数分かかります。**Manage (管理) > Configuration (設定) > Identity Services (IDサービス) > Identity Redistribution (IF再配信)**に移動し、 設定範囲 をサービス接続に設定して、サービス接続のユーザーIDエージェントの詳細を確認します。

Prisma AccessからオンプレミスデバイスへのIDデータの送信

サービス接続のUser-IDエージェント情報は、オンプレミスデバイスにIDデータを配信するためのPrisma Accessの設定に必要なすべてです。

Manage (管理) > Configuration (設定) > Identity Services (IDサービス) > Identity Redistribution (IF再配信)に移動し、 設定範囲 をサービス接続に設定して、サービス接続のユーザーIDエージェントの詳細を取得します。

Prisma AccessをPanoramaや次世代ファイアウォール上のデータ再配信エージェントとして構成するには、これらの詳細を使用します。



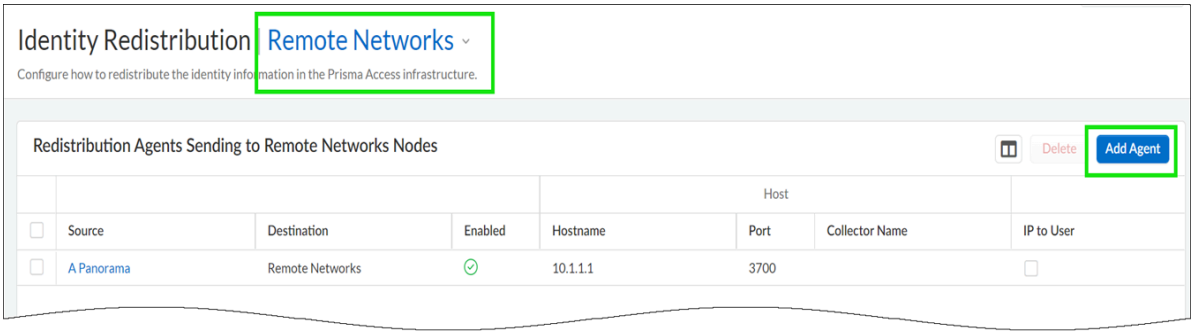
オンプレミスデバイスからプリズマアクセスへのアイデンティティデータの送信

オンプレミスのデバイスを再配信エージェントとしてPrisma Accessに追加します。追加したデバイスは、アイデンティティデータをPrisma Accessに配信できるようになります。

- リモートネットワークサイトのデバイスから

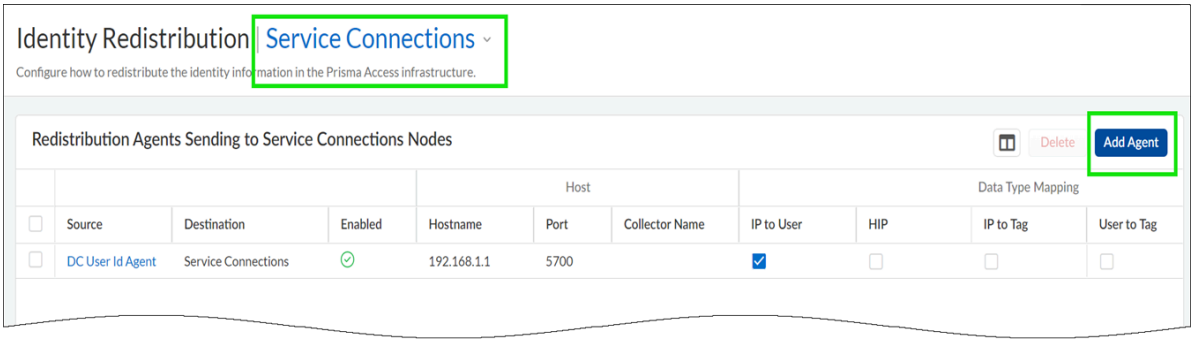
  Identity Redistribution (ID再配信)ダッシュボードを開き、設定範囲をリモートネットワークに設定し、エージェントを追加します。ホストの詳細を指定するだけでなく、デバイス

がPrisma Accessと共有するデータのタイプを選択します。オプション設定には、名前とデバイスの事前共有キーが含まれます。



- サービス接続サイトのデバイスからの場合：

  Identity Redistribution (ID再配信)ダッシュボードを開き、設定範囲をサービス接続に設定し、エージェントを追加します。ホストの詳細を指定するだけでなく、デバイスがPrisma Accessと共有するデータのタイプを選択します。オプション設定には、名前とデバイスの事前共有キーが含まれます。



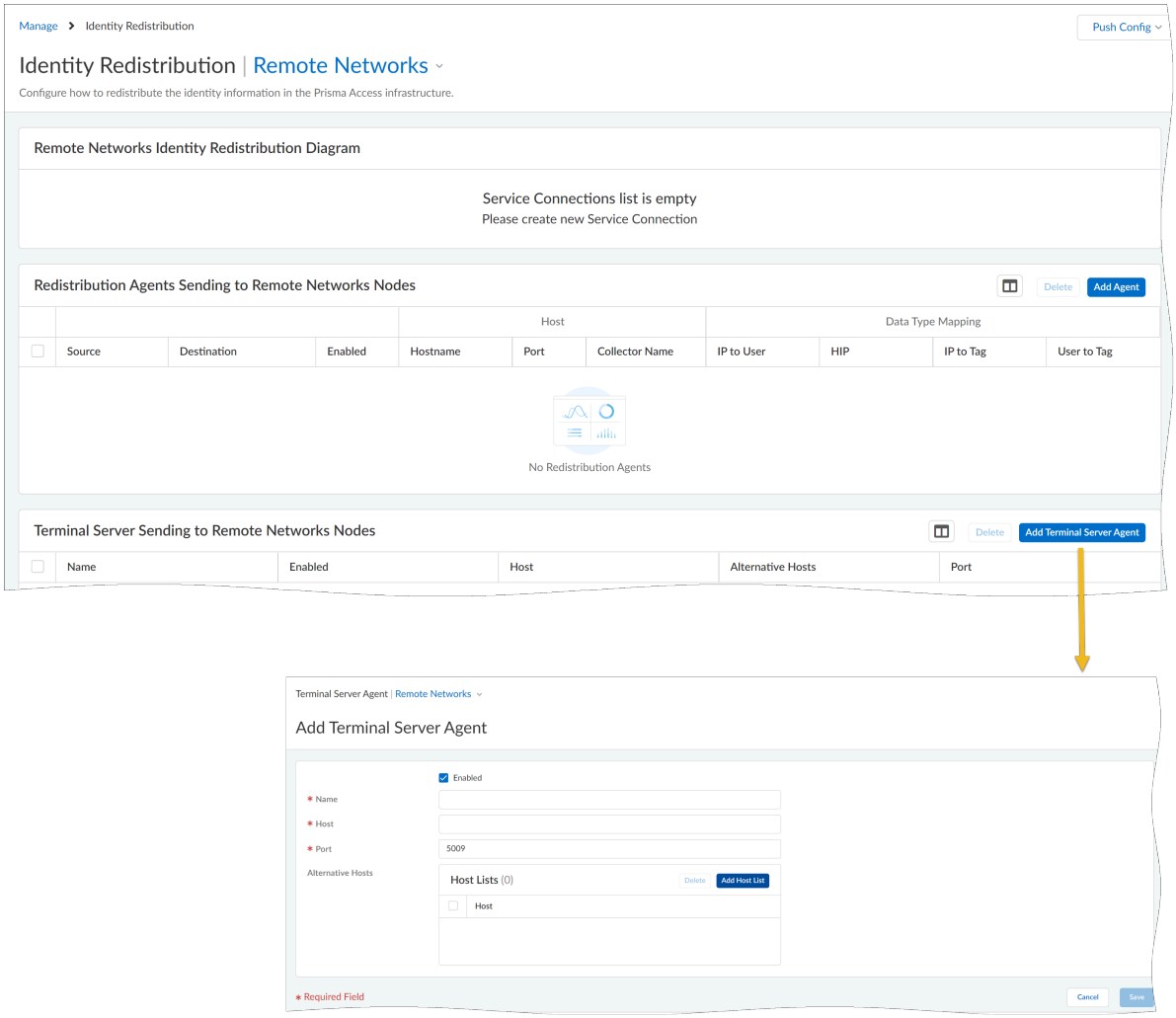
ターミナルサーバエージェントのユーザーマッピングの設定

Windowsベースのターミナル サーバー上の特定のユーザーを識別するため、ターミナル サーバー(TS)エージェントは各ユーザーにポート範囲を割り当てます。TSエージェントは、

割り当てられたポート範囲をPrisma Accessに通知するため、Prisma Accessはユーザーとユーザーグループに基づいてポリシーを適用できます。

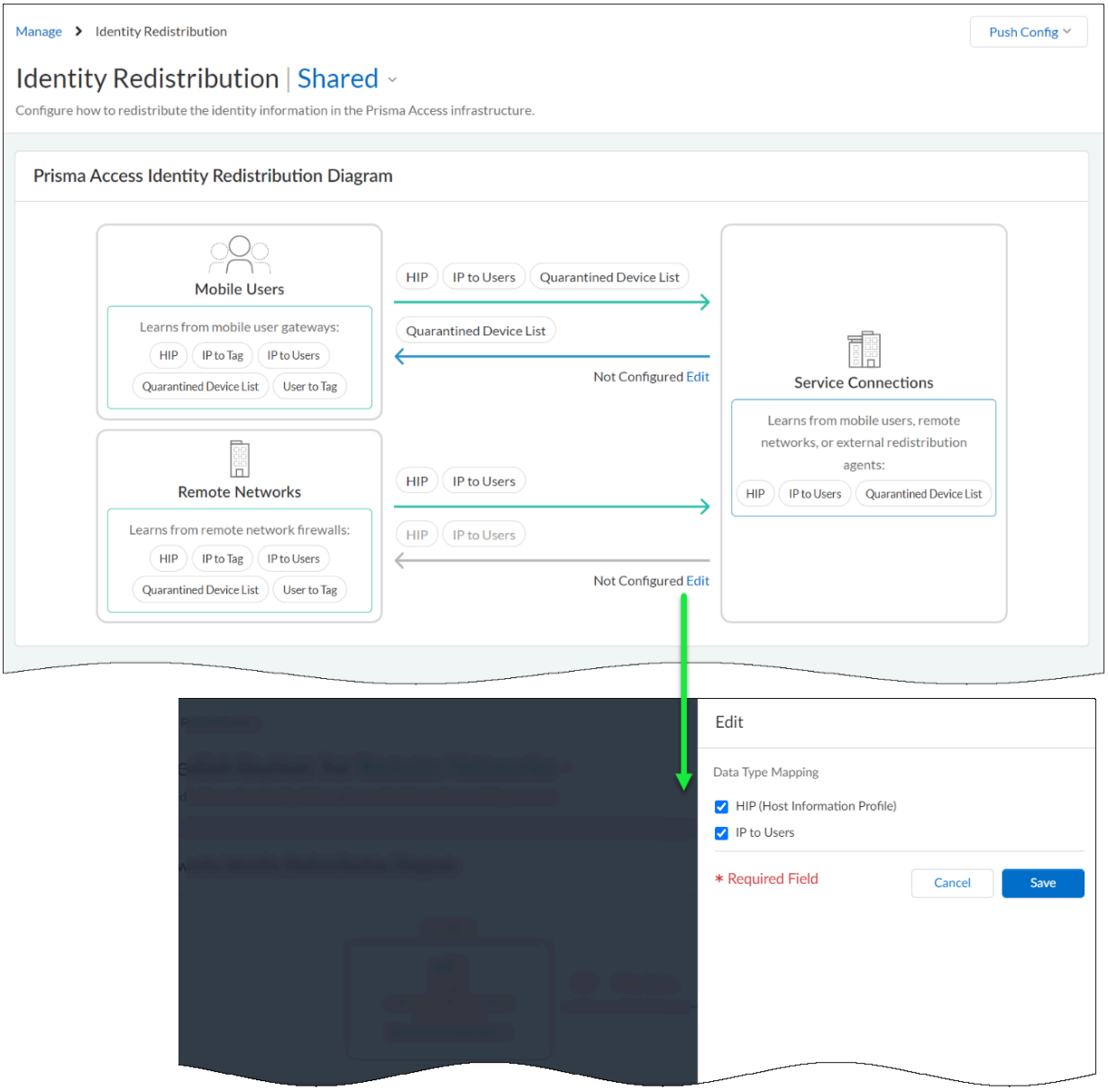
[ID再配信]ダッシュボードで、構成範囲をリモートネットワークに設定し、「ターミナルサーバーからリモートネットワークノードへの送信」の「ターミナルサーバーエージェント」を追加します。

- デフォルトでは、設定は有効になっています。
- TSエージェントの名前を入力します。
- TSエージェントがインストールされているWindowsホストのIPアドレスを入力します。
- エージェントがユーザーマッピング要求をリッスンするポート番号を入力します。ポートはデフォルトで5009に設定されています。
- 変更を保存します。



Prismaアクセス環境全体にIDデータを配信

[Identity Redistribution(ID再配信)]ダッシュボードで、図を編集して、各送信元から収集し、Prisma Access全体で共有するIDデータを指定します。



変更を有効にするには、Prisma Accessに設定をプッシュします。

アイデンティティ情報再配信 (NGFW)

大規模なネットワークでは、すべてのファイアウォールがマッピング情報ソースに直にクエリを送るよう設定する代わりに、再配信を通じて一部のファイアウォールだけがマッピング情報を収集するよう設定することで、リソースを合理的に使用できます。データの再配信では、指定した種類の情報のみを、選択したデバイスのみに、きめ細かく再配信できます。サブネットと範囲

を使用して、IP ユーザー マッピングまたは IP タグ マッピングをフィルタリングし、ファイアウォールがポリシールール適用に必要なマッピングのみを収集するようにもできます。

データを再配信するには、以下のアーキテクチャ タイプを使用できます。

- 単一リージョンのハブ アンド スポーク アーキテクチャ:

  ファイアウォール間でデータを再配信するには、ベストプラクティスとしてハブ アンド スポーク アーキテクチャを使用します。この設定では、ハブ ファイアウォールは、Windows User-IDエージェント、Syslogサーバ、ドメイン コントローラ、その他のファイアウォールなどの送信元からデータを収集します。ハブ ファイアウォールからデータを収集するように、再配信クライアント ファイアウォールを設定します。

- 複数のリージョン向けのマルチハブおよびスポークアーキテクチャ:

  複数のリージョンにファイアウォールを導入していて、すべてのリージョンのファイアウォールにデータを配信し、ユーザーのログイン場所に関係なくポリシールールを一貫して適用できるようにしたい場合は、複数のリージョンにマルチ ハブ アンド スポーク アーキテクチャを使用できます。

- 階層アーキテクチャ:

  データの再配信に、階層アーキテクチャを使用することもできます。たとえば、User-ID 情報などのデータを再配信するには、再配信シーケンスをレイヤーに編成します。各レイヤーには1つ以上のファイアウォールがあります。最下部レイヤーでは、ファイアウォールで実行されている PAN-OS 統合 User-ID エージェントと Windows サーバーで実行されている Windows ベース User-ID は IP アドレスをユーザー名にマッピングします。上位レイヤーは、下位レイヤーの最大 100 個の再配信ポイントからマッピング情報および認証タイムスタンプを受け取るファイアウォールを持っています。最上部レイヤー ファイアウォールはすべてのレイヤーからのマッピングおよびタイムスタンプを集約します。このデプロイメントにより、最上部レイヤー ファイアウォールのすべてのユーザーにポリシールールを設定し、下位レイヤー ファイアウォールが担当する、対応するドメインのユーザー サブセットに地域または機能別ポリシールールを設定するオプションが提供されます。

想定どおりに実施されていないトラフィックをトラブルシューティングします。特定のファイアウォールのデータプレーンのステータスをチェックして、想定されているポリシー（設定済み）と実施されているポリシーが一致しないかどうかを把握できます。

STEP 1 | Strata Cloud Managerにログインします。

STEP 2 | お使いのStrata Cloud Managerデプロイメントがアイデンティティ再配布の設定要件を満たしていることを確認します。

1. Strata Cloud ManagerテナントのCIE(Cloud Identity Engine)を設定して有効化します。

   IDの再配送を利用するために必要です。

   1. アクティブ化 クラウド ID エンジン アプリ。
   2. Cloud Identity Engineをセットアップする。

2. **[Manage (管理)] > [Configuration (設定)] > [NGFWとPrisma Access] > [Objects (オブジェクト)] > [Address Groups (アドレス グループ)]**を選択し、必要なIPアドレスとタグのマッピングを持つダイナミックアドレスグループを追加します。

   アドレスグループの「タイプ」で、**[Dynamic (ダイナミック)]**を選択します。必要に応じてダイナミックアドレスグループを設定し、保存します。

3. **[Manage (管理)] > [Configuration (設定)] > [NGFWとPrisma Access] > [Objects (オブジェクト)] > [Dynamic User Groups (ダイナミックユーザーグループ)]**を選択し、必要なユーザー名とタグのマッピングを持つダイナミックユーザーグループを 追加 します。

   必要に応じてダイナミックユーザーグループを設定し、保存します。

STEP 3 | **[Manage (管理)] > [Configuration (設定)] > [NGFWとPrisma Access] > [Identity Services (IDサービス)] > [Identity Redistribution (ID再配布)]** を選択し、アイデンティティ再配布を設定する ［Configuration Scope (設定範囲)］ を選択します。

［**Folders (フォルダ)**］からフォルダまたはファイアウォールを選択するか、［**Snippets (スニペット)**］を選択して、スニペットでアイデンティティの再配布を設定できます。

STEP 4 | エージェントの追加。

STEP 5 | エージェントにわかりやすい名前を入力します。

STEP 6 | ホストのIPアドレスを入力します。

STEP 7 | ポートを入力します（範囲は1～65535）。

STEP 8 | **Data Type Mapping (データ タイプ マッピング)**を選択します。

- **IP** からユーザ – ユーザ ID の IP アドレスとユーザ名のマッピング。
- ホスト情報プロファイル（**HIP**） – ダイナミックアドレス グループの IP アドレスとタグのマッピング。
- **IP to Tag (IPからタグ)** – ダイナミックユーザー グループのユーザー名とタグのマッピング。
- **User to Tag (ユーザーからタグ)** – HIPオブジェクトとプロファイルを含むGlobalProtectのHIPデータ。
- **Quarantined Device List**（隔離デバイスリスト） – GlobalProtect が隔離対象として識別するデバイス。

STEP 9 | **Save**（保存）を選択します。

STEP 10 | （NGFWのクラウド管理のみ）ファイアウォールのID再配布を有効にします。

1. **[Manage (管理)] > [Configuration (設定)] > [NGFWとPrisma Access] > [Device Settings (デバイス設定)] > [Device Setup (デバイスセットアップ)] > [Management (マネジメント)]** を選択し、**[Customize (カスタマイズ)]**を選択して **uid-agent** サービスのサービスルートを設定します。

   サービスルートを作成する設定スコープを選択します。［**Folders (フォルダ)**］からフォルダまたはファイアウォールを選択するか、［**Snippets (スニペット)**］を選択して、スニペットでサービス ルートを設定できます。
2. 他のファイアウォールから再配信するデータをクエリされた際にファイアウォールが応答できるようにします。

   1. **[Manage (管理)] > [Configuration (設定)] > [NGFWとPrisma Access] > [Device Settings (デバイス設定)] > [Device Setup (デバイスセットアップ)] > [Management (マネジメント)]**を選択し、ユーザー**ID**ネットワークサービスを有効にします。
   2. **[Manage (管理)] > [Configuration (設定)] > [NGFWとPrisma Access] > [Device Settings (デバイス設定)] > [Interfaces (インターフェース)]**を選択して、レイヤー3インターフェイスを作成または選択します。

      詳細設定を展開します。**Other (その他)**では、管理プロファイルを作成または編集してユーザー**ID**を有効にします。

   - 選択

STEP 11 | 構成をプッシュします。

管理:ローカルユーザーとグループ

どこで使用できますか?	何が必要ですか?
• Prisma Access (Managed by Panorama or Strata Cloud Manager) • Software NGFW Creditsによって資金提供されたものを含むNGFW	これらの各ライセンスには、Strata Cloud Managerへのアクセスが含まれています。 ❑ Prisma Access ❑ AIOps for NGFW Premium ❑ Strata Cloud Manager Essentials ❑ Strata Cloud Manager Pro → Strata Cloud Managerで利用できる機能は、使用するライセンスによって異なります。

管理者とエンドユーザーの認証情報をローカルに保存します。GlobalProtectまたは認証ポータルを使用して認証する管理者およびエンドユーザーからの認証情報を保存できます。

ローカル データベース認証を設定するには、ファイアウォールのローカルで実行され、ユーザーアカウント（ユーザー名およびパスワード、あるいはパスワードのハッシュ）およびユーザーグループを含むデータベースを作成します。ファイアウォールの Webインターフェースに

アクセスする管理者を認証するため、および認証ポータルあるいは GlobalProtect を通じてアプリケーションにアクセスするエンドユーザーを認証するために、ファイアウォールのローカルにあるユーザーデータベースを設定できます。

ローカル データベース認証は認証プロファイルに関連付けることができるため、異なるユーザーのグループがKerberosシングル サインオン（SSO）やマルチファクター認証（MFA） など、別々の認証設定を必要とするようなデプロイ環境を実現することができます。認証プロファイルを使用する管理者アカウントでは、パスワードの複雑さと有効期限の設定は適用されません。この認証方式は、ファイアウォールにアクセスする管理者、および認証ポータルあるいは GlobalProtect を通して、サービスおよびアプリケーションにアクセスするエンドユーザーに対する認証のために利用できます。

[Manage (管理)] > [Configuration (設定)] > [NGFWとPrisma Access] > [Identity Services (IDサービス)] > [Local Users & Groups (ローカルユーザーとグループ)]に進み、認証データの収集を開始します。

ローカルユーザーを作成する

STEP 1 | Strata Cloud Managerにログインします。

STEP 2 | **[Manage (管理)] > [Configuration (設定)] > [NGFWとPrisma Access] > [Identity Services (IDサービス)] > [Local Users & Groups (ローカルユーザーとグループ)] > Local Users (ローカルユーザー)**を選択し、ローカルユーザーを作成する「構成スコープ」を選択します。

［フォルダ］からフォルダまたはファイアウォールを選択するか、［スニペット］を選択してスニペットでローカルユーザーを設定できます。

STEP 3 | ローカルユーザーの追加。

STEP 4 | ユーザー名を入力します。

STEP 5 | ローカルユーザーが「有効」になっていることを確認します。

認証のためにローカル・ファイアウォール・データベースからローカル・ユーザーを削除するのではなく、チェックを外し（無効化）、そのユーザーが認証用に有効にならないようにすることができます。

STEP 6 | **Password** [パスワード]と **Confirm Password** [パスワードの確認]を入力します。

STEP 7 | **Save**（保存）を選択します。

STEP 8 | **Push Config (構成をプッシュ)**します。

ローカルユーザーグループの作成

複数のローカルユーザを単一のローカルグループにグループ化して、ローカルファイアウォールデータベースにグループ情報を追加します。ローカルユーザグループを作成して、同じ認証要件を持つ複数のローカルユーザを管理できます。

STEP 1 | Strata Cloud Managerにログインします。

STEP 2 | **[Manage (管理)] > [Configuration (設定)] > [NGFWとPrisma Access] > [Identity Services (IDサービス)] > [Local Users & Groups (ローカルユーザーとグループ)] > Local Users Groups (ローカルユーザーグループ)**を選択し、ローカルユーザーグループを作成する[Configuration Scope (設定範囲)]を選択します。

［**Folders (フォルダ)**］からフォルダまたはファイアウォールを選択するか、［**Snippets (スニペット)**］を選択してスニペット内のローカルユーザーグループを設定できます。

STEP 3 | ローカルユーザーグループを追加します。

STEP 4 | ローカルユーザーグループの名前を入力します。

STEP 5 | 前の手順で作成したローカルユーザーを追加します。

STEP 6 | **Save**（保存）を選択します。

STEP 7 | **Push Config (構成をプッシュ)**します。

管理:デバイス設定

どこで使用できますか?	何が必要ですか?
• Software NGFW Creditsによって資金提供されたものを含むNGFW	☐ Strata Cloud Manager Essentials ☐ AIOps for NGFW Premium または Strata Cloud Manager Pro → Strata Cloud Managerで利用できる機能は、使用するライセンスによって異なります。

デバイス設定から、クラウドマネージドファイアウォールの以下の設定を行うことができます。

設定	詳説
インターフェイス	ファイアウォールが一度に複数の展開で動作できるようにインターフェイスを設定します。 ［**Ethernet (**イーサネット**)**］タブの［ローカルデバイス構成の表示］を使用して、ローカルファイアウォールとStrata Cloud Managerに存在するさまざまな構成を表示します。
routing	ファイアウォールのルーティングプロファイル、論理ルータ、およびスタティック ルートを設定します。
IPSec トンネル	IPパケットがトンネルを通過するときに認証および暗号化されるようにIPSecトンネルを設定します。
DHCP	DHCPを設定して、TCP/IPおよびリンク層の設定パラメータを提供し、TCP/IPネットワーク上に動的に設定されるホストにネットワーク アドレスを提供します。
ゾーン	ネットワークを機能ゾーンと組織ゾーンにセグメント化するようにゾーンを設定して、攻撃対象領域を減らします。
DNS プロキシ	DNSプロキシを設定して、DNSクライアントとサーバー間の仲介役となるようにファイアウォールを設定します。
デバイスのセットアップ	ファイアウォールの管理インターフェースと補助インターフェースのサービスルート、接続設定、許可サービス、管理アクセス設定を行うようにデバイスをセットアップします。

設定	詳説
proxy	プロキシとファイアウォールの機能を1つのデバイスに統合するWebプロキシを設定します。Strata Cloud Manager用の *Web*プロキシには、レガシールータスタックが必要です。これを有効にしたい場合は、アカウントチームにお問い合わせください。
バーチャルワイヤー	ファイアウォール上の接続された2つのインターフェイスがスイッチングやルーティングを行う必要がないように、ファイアウォールインターフェイスをトポロジに統合するように仮想ワイヤを設定します。
グローバルプロテクト	クラウド管理されたNGFWをGlobalProtectゲートウェイおよびポータルとして有効にすることで、あらゆる場所のユーザーに柔軟で安全なリモートアクセスを提供することができます。

管理:グローバル設定

どこで使用できますか?	何が必要ですか?
• Prisma Access (Managed by Panorama or Strata Cloud Manager)	以下のいずれかです。 ❑ Prisma Accessライセンス ❑ Strata Cloud Manager Pro → Strata Cloud Managerで利用できる機能は、使用するライセンスによって異なります。

Strata Cloud Managerでグローバル設定を確認して設定する （**[Manage (管理)] > [Configuration (設定)] > [NGFWとPrisma Access] > [Global Settings (グローバル設定)]**）

オブジェクト	詳説
SaaS アプリの管理	SaaSアプリごとにSaaSアプリケーションを一元管理。SaaS App Managementでは、エンタープライズ用のアプリを安全に有効化するために使用できる機能を確認できます。
ユーザーコーチング通知テンプレート	機密データを含むトラフィックが検査およびブロックされたときに、ユーザーがEnterprise Data Loss Prevention (E-DLP)インシデントを生成した場合に、エンドユーザー通知テンプレートを一元管理してAI-Powered ADEMを通じてユーザーに警告します。
自動VPN	ネットワークデバイスの設定やVPNトンネルの確立を手動で行うのは面倒な作業であり、設定ミスが起こりやすい。自動VPNは、ネットワークデバイス間のVPNトンネルを自動的に作成します。自動VPNを使用すると、複数のローカルエリアネットワーク（LAN）を接続するVPNクラスタを作成できます。自動VPNを備えたSD-WANにより、SD-WANのデプロイメントと管理が容易になります。

ユーザーコーチング通知テンプレート

どこで使用できますか?	何が必要ですか?
• Prisma Access (Managed by Strata Cloud Manager)	❑ GlobalProtect appバージョン 6.3 以降 ❑ Enterprise Data Loss Prevention (E-DLP)ライセンス ❑ Prisma Accessモバイルユーザー ライセンス ❑ Prisma Accessライセンス またはEnterprise DLPライセンスを含む以下のいずれかのライセンス ❑ Prisma AccessCASBライセンス ❑ Next-Generation CASB for Prisma Access and NGFW (CASB-X)ライセンス

エンドユーザーコーチング通知テンプレートを使用すると、ユーザーがEnterprise Data Loss Prevention (E-DLP)インシデントを生成したときにAccess Experienceユーザー インターフェース（UI）に表示される通知を設定できます。Enterprise DLPインシデントは、機密データを含むファイルがダウンロードまたはアップロードされた場合、または機密データを含むファイルベース以外のトラフィックがWebフォームに投稿された場合に生成されます。

機密データと見なされるものを決定するには、1つ以上のインライン**DLP**ルールを追加します。機密データと見なされるものを定義するトラフィック一致条件を含むDLPルール。DLPルールは、同じ名前のEnterprise DLPデータプロファイルから派生しています。さらに、ファイルベースまたは非ファイルベースのEnterprise DLPインシデントが生成されるときのカスタムメッセージを設定できます。Enterprise DLPインシデントが生成された後、インシデントを生成したユーザーは、アップロード、ダウンロード、または投稿された機密データに関する詳細情報をデータセキュリティ通知で確認できます。

ユーザーが同じインシデントを生成した回数に関係なく、30秒間に1つのインシデントにつき1つの通知のみが表示されます。たとえば、ユーザーが機密データを含むファイルをBox Webアプリケーションにアップロードしようとして、Enterprise Data Loss Prevention (E-DLP)がそのアップロードをブロックした場合などです。その後、ユーザーはすぐに同じファイルをさらに5回アップロードしようとしますが、そのたびにブロックされます。この場合、ユーザーが機密性の高い日付を含むファイルをBox Webアプリケーションにアップロードすることを合計6回ブロックされたにもかかわらず、Access Experienceアラートは1回しか生成されません。

STEP 1 | テナントでエンドユーザーコーチングを有効にするには、Palo Alto Networks担当者にお問い合わせください。

STEP 2 | WindowsまたはmacOSにGlobalProtect appバージョン6 6.3以降をインストールします。

STEP 3 | Strata Cloud Managerにログインします。

STEP 4 | Autonomous DEMを有効化します。

Strata Cloud Managerで、**[Workflows (ワークフロー)]** > **[Prisma Accessのセットアップ]** > **[GlobalProtect]** > **[GlobalProtectアプリケーション]**を選択し、**[Add App Settings (アプリケーション設定を追加)]**を選択します。DLPインシデントを生成したときに、Access Experience UIでユーザーに通知を表示するには、これらの必須設定を構成する必要があります。

- **[Autonomous DEM and GlobalProtect Log Collection for Troubleshooting (トラブルシューティングのための自律型DEMとGlobalProtectのログ収集)]**を有効にする
- **DEM for Prisma Access (Windows および Mac のみ)**–**[Install and User Cannot enable or DisableDEM (インストール。ユーザーはDEMを有効または無効にできない)]** を選択します。
- **DEM for Prisma Access**バージョン**6.3**以降（**Windows**および**Mac**のみ） – **[Install the Agent (エージェントのインストール)]**を選択します。

STEP 5 | （macOSのみ） ［Access Experience (アクセスエクスペリエンス)］UIで、［**Settings (設定)]** > **[Notifications (通知)**］を選択し、**[Allow notifications (通知を許可)]**を有効にします。

この設定は、各ユーザーのAccess Experience UIで有効にする必要があり、ユーザーのデスクトップに通知を表示するために必要です。必要に応じて、残りのAccess Experience通知設定を構成します。

STEP 6 | Enterprise DLPを設定します。

1. 復号プロファイルとポリシー ルールを作成します。

   これは、Enterprise DLPがトラフィックを復号化して機密データを検査する場合に必要です。

2. カスタムデータパターンを作成して一致条件を定義します。

   または、カスタムデータパターンを作成する代わりに、事前定義済みデータパターンを使用することもできます。

3. データプロファイルを作成し、データパターンを追加します。

   カスタムデータプロファイルのみがサポートされます。デフォルトでは、事前定義済みのすべてのDLPルールのアクションが「**Alert (アラート)**」に設定されています。DLPルールアクションを編集するために、事前定義済みデータ プロファイルのクローンを作成する必要がある場合。

4. DLPルールを変更します。

   - DLPルールを変更する場合は、**[Action (アクション)]**を**[Block (ブロック)]**に設定する必要があります。Access Experience UIでアラートを生成するために必要です。**[Action (アクション)]**が**[Alert (アラート)]**に設定されている場合、アラートは表示されません。
   - DLPルールをプロファイル グループに追加し、プロファイル グループをセキュリティ ポリシー ルールにアタッチします。これは、Enterprise DLPがDLPインシデントを生成し、その後 Access Experience UIに通知を生成するために必要です。

STEP 7 | **[Manage (管理)] > [Configuration (設定)] > [NGFWとPrisma Access] > [Global Settings (Global設定)] > [User Coaching Notification Template (ユーザーコーチング通知テンプレート)]** および **[Add Notification Template (通知テンプレートの追加)]**を選択します。

STEP 8 | 一般情報を設定します。

1. 製品名がインライン**DLP**であることを確認します。

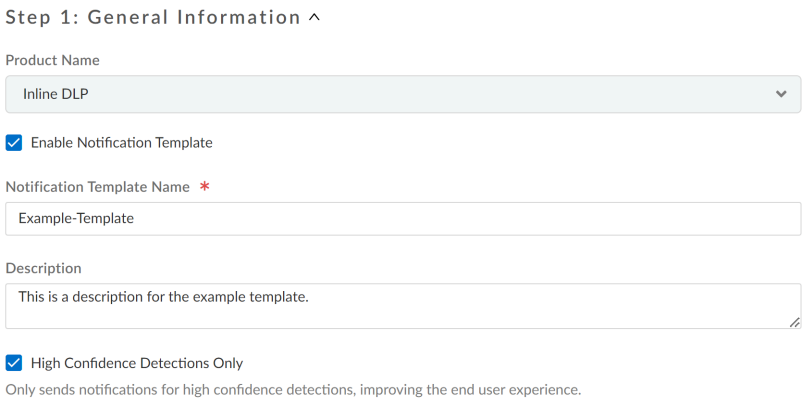
   これはデフォルト設定で変更できません

2. 保存後にテンプレートを有効にするには、**[Enable Notification Template (通知テンプレートを有効にする)]**を選択します。

   この設定はデフォルトで有効になっています。

3. 分かりやすい通知テンプレート名を入力します。
4. （任意）通知テンプレートの説明を入力します。
5. （任意）信頼度の高いトラフィックが一致した場合にだけAccess Experienceアラートを生成するには、［**High Confidence Detections Only (高い信頼度の検出のみ)**］を選択します。

   高い信頼度の一致は、一致したトラフィックを検出するときのEnterprise DLPの信頼度を反映します。正規表現（正規表現）パターンの場合、これは設定された近接キーワードへの文字距離に基づきます。機械学習（ML）パターンの場合、この信頼度はMLモデルによって計算されます。

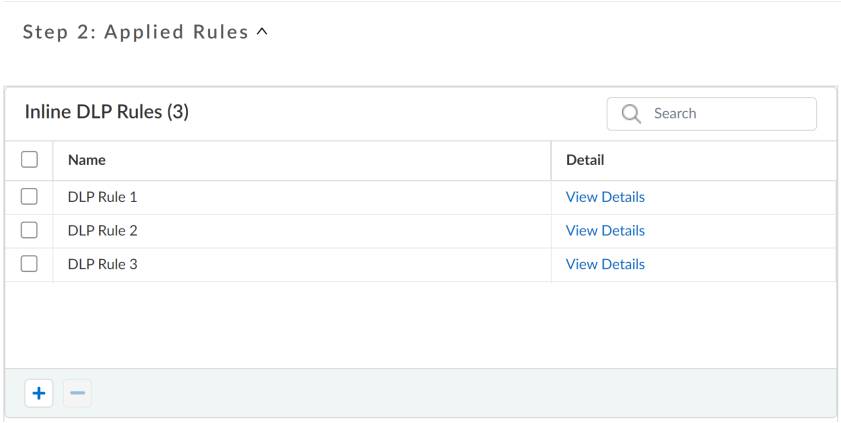


STEP 9 | 通知テンプレートに1つ以上の適用ルールを追加します。

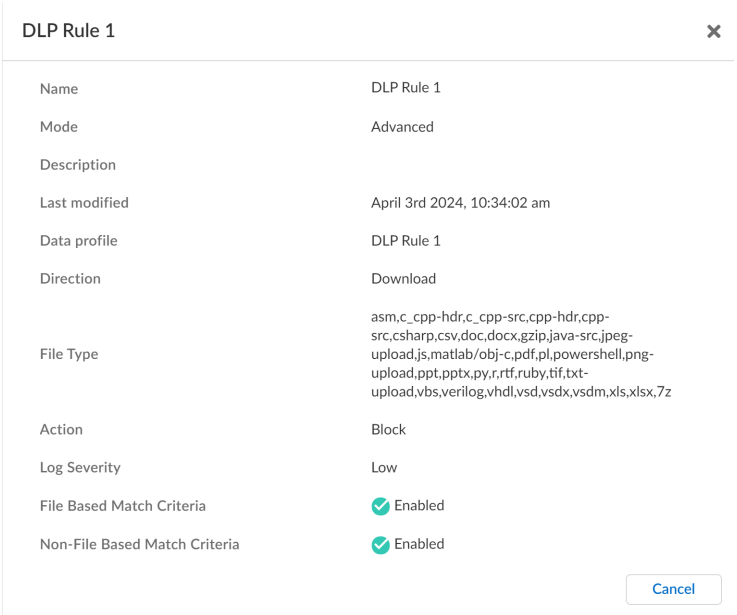
DLPルールは、ルールのアクションをブロックに設定し、セキュリティ ポリシー ルールにアタッチされたプロファイルグループに追加して、Access Experience通知を生成する必要があります。セキュリティ ポリシー ルールに関連付けられたプロファイル グループに追加されたDLPルールのみを追加します。これは、Enterprise DLPがDLPインシデントを生成し、そ

の後 Access Experience UIに通知を生成するために必要です。1つのDLPルールを複数のユーザーコーチング通知テンプレートに追加できます。

通知テンプレートに追加されたすべてのDLPルールは、Enterprise DLPがDLPルールに関連付けられたデータプロファイルに一致する機密データをブロックしたときに、同じ通知メッセージを生成します。



追加した各DLPルールの詳細を表示して、特定の検査の詳細を確認できます。これには、トラフィック検査の**[Direction (指示)]**、適用可能なファイルタイプ、処理、およびDLPルールがファイルベース一致基準、非ファイルベース一致条件、またはその両方について検査を行っているかどうかが含まれます。



STEP 10 | DLPルールに関連付けられたデータプロファイルに一致する機密データをEnterprise DLPがブロックしたときにユーザーが受信する通知メッセージを定義します。

メッセージテンプレートは、Enterprise DLPが機密データをブロックしたときにユーザーが受け取るAccess Experienceトースト通知です。メッセージテンプレートでは、次の変数を使用できます。各変数の括弧を含める必要があります。

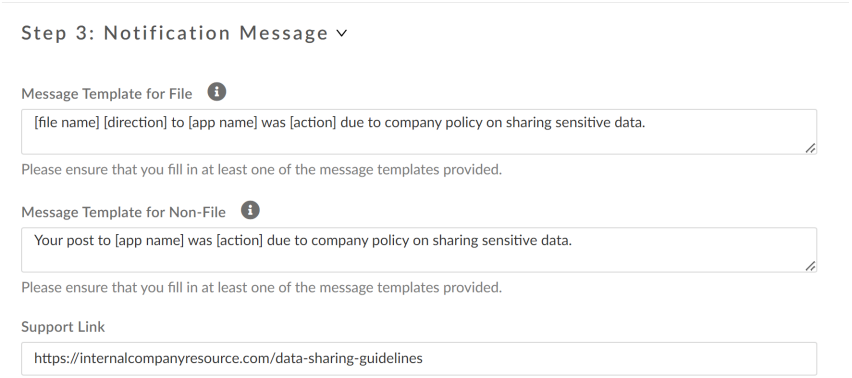
- **[**ファイル名**]** – Enterprise DLPによってブロックされた機密データを含むファイル名と拡張子。
- （ファイルベースのみ）［**direction (**指示**)**］ – Enterprise DLPがファイルのアップロードまたはダウンロードをブロックしたかどうかを指定します。
- **[**アプリ名**]** – アプリケーションユーザーがファイルベース以外のコンテンツへのアップロード、コンテンツからのダウンロード、またはコンテンツの投稿を試みました。
- **[**アクション**]** – 機密データが検出されたときに実行されるアクションEnterprise DLP。この値は常にブロックされます。

1. ファイルベース検出のメッセージテンプレートを定義します。

   DLPルールがファイルベースの検出用に構成されていない場合は、この手順を省略します。
2. 非ファイルベース検出のメッセージテンプレートを定義します。

   DLPルールがファイルベース以外の検出用に構成されていない場合は、この手順を省略します。
3. サポートリンクを追加します。

   Access Experienceのトースト通知には、機密データの共有やダウンロードに関する会社のポリシーを説明するリンクを直接追加できます。



STEP 11 | **Save**（保存）を選択します。

STEP 12 | Enterprise DLPインシデントを生成したユーザーは、データセキュリティ通知を表示して、アップロード、ダウンロード、または投稿された機密データのスニペットを確認できます。

管理:業務

どこで使用できますか?	何が必要ですか?
• NGFW (Managed by Panorama or Strata Cloud Manager) • VM-Seriesを含む	❑ AIOps for NGFW Premium license (use the Strata Cloud Manager app) → Strata Cloud Managerで利用できる機能は、使用するライセンスによって異なります。

トラブルシューティング

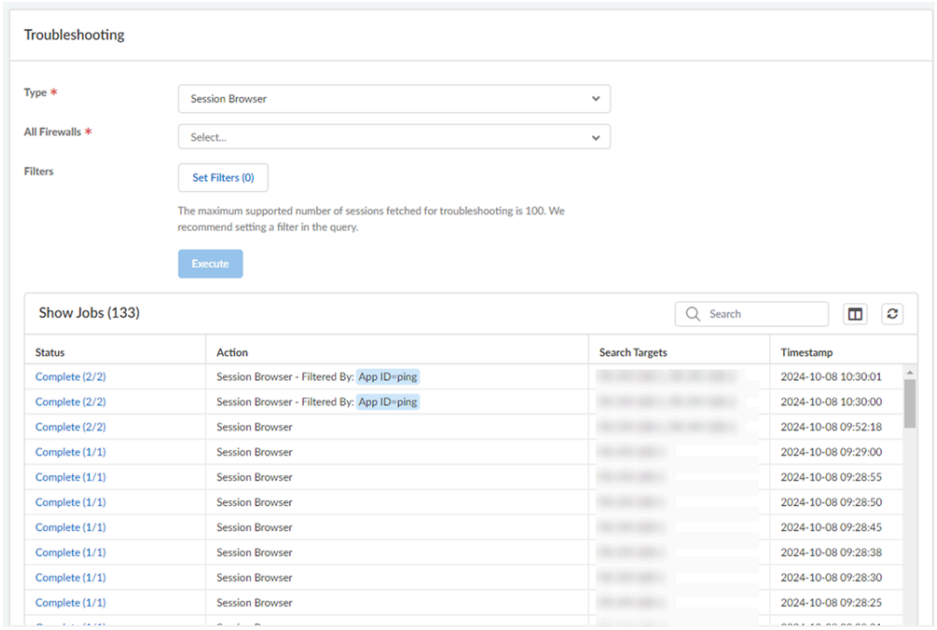
Strata Cloud ManagerからNGFWのトラブルシューティングを実行でき、さまざまなファイアウォールインターフェース間を移動する必要はありません。

トラブルシューティングの詳細については、こちらをクリックしてください。

トラブルシューティングダッシュボードでは、Strata Cloud Managed NGFWのネットワーク、ID、ポリシーに関する問題をトラブルシューティングできます。トラブルシューティングダッシュボードを使用すると、次の領域について異常や問題のある設定を特定できます。

- ❑ DNSプロキシ
- ❑ NAT
- ❑ ユーザグループ
- ❑ ダイナミック アドレス グループ
- ❑ ダイナミック ユーザグループ
- ❑ ユーザID
- ❑ セッションブラウザ

開始するには、**[Manage (管理)]** > **[Configuration (設定)]** > **[NGFWとPrisma Access]** > **[Operations (オペレーション)]** > > **[Troubleshooting (トラブルシューティング)]** > **[Session Browser (セッションブラウザ)]**に進みます。



管理:IoT ポリシーの推奨事項

どこで使用できますか?	何が必要ですか?
• Prisma Access （*Strata Cloud Manager*または*Panorama*の設定管理付き） • NGFW （*Strata Cloud Manager*または*Panorama*の設定管理付き）	❑ Strata Cloud Managerで設定を管理するには、少なくともこれらのライセンスのうち 1 つが必要です。NGFWとPrisma Accessを統合管理するには、両方が必要です： ❑ Prisma Accessライセンス ❑ AIOps for NGFW Premium license (use the Strata Cloud Manager app) ❑ Strata Cloud Manager Essentials ❑ Strata Cloud Manager Pro ❑ 高度なIoTセキュリティ製品（Enterprise IoT Security Plus、Industrial IoT Security、Medical IoT Security）のIoT Securityサブスクリプション

IoT Securityは、デバイスプロファイルごとに整理されたセキュリティ ポリシールールの推奨事項を自動生成してStrata Cloud Managerに提供します。プロファイルごとに、アプリケーションごとに1つの推奨事項があります。プロファイルを選択し、使用するルール推奨事項を選択します。次に、適用する次世代ファイアウォールまたはPrisma Accessデプロイメントタイプを選択します。

始めましょう

[セキュリティ ポリシールールの推奨事項]を選択し、次世代ファイアウォールまたはPrisma Accessに適用します。

STEP 1 | 次世代ファイアウォール用のフォルダまたはスニペットを作成します。

定義済みのフォルダまたは以前に作成したフォルダやスニペットを使用する場合は、この手順をスキップします。*Prisma Access*フォルダは事前定義済みです。

フォルダは、本質的にはさまざまな種類のルール、セキュリティ設定、およびオブジェクトを保持するコンテナです。IoT SecurityIoT Securityが生成したポリシールールの推奨事項をインポートする場合、フォルダには次世代ファイアウォールまたはPrisma Accessのデプロイメントが保持されます。

スニペットもコンテナの一種で、複数のフォルダに関連付けることができます。フォルダとスニペットを使用すると、ファイアウォールまたは導入の任意のグループにポリシールールをインポートできます。

例えば、Californiaという名前のフォルダを作成し、その中に60個のファイアウォールを配置した後、Hawaiiという名前の別のフォルダを作成し、その中に15個のファイアウォールを配置することができます。次に、CA-HIというスニペットを作成し、カリフォルニアとハワイのフォルダに適用します。カリフォルニアのファイアウォールにのみルールの推奨事項をインポートする場合は、スコープをフォルダに設定し、カリフォルニアフォルダを選択します。ルールの推奨事項をカリフォルニアとハワイの両方にインポートする場合は、スコープを**[Snippet (スニペット)]**に設定し、CA-HIスニペットを選択します。

フォルダ構造の階層によっては、カリフォルニアやハワイの上にUS-Westのような親フォルダがあるかもしれません。次に、範囲が［**US-West (米国西部)**］を選択したフォルダに設定されているときにルールの推奨事項をインポートすると、カリフォルニアとハワイの両方の子フォルダがインポートされたルールを継承します。ただし、カリフォルニアやハワイにルールをインポートする場合、［US-West (米国西部)］フォルダの下にオレゴン、アラスカ、ワシントン、アリゾナなどの兄弟フォルダがある場合、この方法は機能しません。この場合、CA -HIスニペットを使う必要があります。

STEP 2 | セキュリティ ポリシー ルールを作成します。

1. **[Manage (管理)] > [Configuration (設定)] > [IoT Policy Recommendation (IoTポリシーの推奨事項)]**を選択します。
2. プロファイル名を選択します。

   IoT Securityは、機械学習を使用して、同じデバイスプロファイル内のIoTデバイスの通常の許容可能なネットワーク動作に基づいて、セキュリティ ポリシー ルールの推奨事項を

自動的に生成します。Strata Cloud Managerは、これらの推奨事項をアプリケーションごとに整理したリストを表示します。それぞれの動作について、次のことがわかります。

振る舞いコンポーネント	説明
アプリケーションリスク	アプリケーションに内在するリスクのレベルを、1から5までのリスク増加の尺度でさまざまな要因によって判定したものです。
セキュリティポリシーが作成されました	ここにフォルダまたはスニペットの名前が1つ以上表示される場合は、この動作に対してセキュリティ ポリシー ルールが以前に作成されたことを示します。そのうちの1つをクリックすると、プロファイル、アプリケーション、フォルダまたはスニペットの名前、およびポリシールールアクションが表示されたサイドパネルが開きます。ここに「**No** (いいえ)」が表示された場合は、ルールがまだ作成されていないことを示します。
発見された場所	**Internal** (内部)は、宛先がローカルネットワーク上にあることを示します。**External** (外部)は、宛先がローカル ネットワークの外部にあることを示します。
局所観察	**Yes** (はい)は、IoTセキュリティテナント環境で動作が確認されたことを示します。**No** (いいえ)は、複数のIoTセキュリティテナント環境で観測されたが、お客様の環境では確認されなかったことを示します。
アプリの使用状況	**Common** (共通)は、1つのアプリケーションが複数のIoTセキュリティテナント環境で検出されたことを示します。**Unique** (ユニーク)は、同じプロファイルにデバイスがある他のテナントの環境では確認されていないことを示します。
宛先アドレスとFQDN	これは、推奨されるポリシールールの宛先です。Any、IPアドレス、FQDNのいずれかになります。
宛先プロファイル	プロファイルは、宛先が内部であり、宛先のデバイスプロファイルが識別される場合に表示されます。

振る舞いコンポーネント	説明
最後に出現した日時	ローカルで観測された動作の場合、最後に観測されたときのタイムスタンプです。ローカルで観察されない一般的な動作については、ダッシュが表示されます。

3. 1つ以上の動作を選択してから、セキュリティ ポリシーを作成します。
4. 作成されるセキュリティ ポリシールールを確認し、Strata Cloud Managerがルールを適用する設定範囲を選択します。

   フォルダ内の1つ以上の次世代ファイアウォールまたはPrisma Accessデプロイメントにルールを適用するには、**[フォルダ]**を選択し、[範囲の選択]からフォルダを選択します。

   スニペット内の1つ以上の次世代ファイアウォールまたはPrisma Accessデプロイメントにルールを適用するには、**[Snippets (スニペット)]**を選択してから、[スコープの選択]からスニペットを選択します。
5. セキュリティ ポリシーを作成します。

STEP 3 | 次世代ファイアウォールとPrisma Accessの導入に設定をプッシュします。

1. **[Manage (管理)]** > **[Operations (オペレーション)]** > **[Push Config (設定をプッシュ)]**を選択します。
2. 設定を変更したフォルダを選択し、**[Push Config (設定をプッシュ)]**、**[Push (プッシュ)]**、そして再度**[Push (プッシュ)]**します。

   Strata Cloud Managerでは、選択したフォルダの［Job ID (ジョブID)］列にID番号が表示され、［Push Status (プッシュステータス)］列に設定プッシュのステータスが表示されます。

   Push Status (プッシュステータス)が**[Pending (保留中)]**から**[Success (成功)]**に変わったら、プッシュされた設定の実行が開始されたことがわかります。
3. プッシュジョブのステータスを表示するには**[Manage (管理)]** > **[Operations (オペレーション)]** > **[Push Status (プッシュステータス)]**を選択します。ここでは、親ジョブのステータスと、ファイアウォールまたはデプロイメントごとに1つずつある子ジョブのステータスも確認できます。

管理:Enterprise DLP

どこで使用できますか?	何が必要ですか?
• Prisma Access （*Strata Cloud Manager*または*Panorama*の設定管理付き） • NGFW （*Strata Cloud Manager*または*Panorama*の設定管理付き）	• Enterprise Data Loss Prevention (E-DLP)ライセンス • **NGFW (Managed by Panorama)** – デバイス管理ライセンスのサポートおよびPanorama • **Prisma Access (Managed by Strata Cloud Manager)**—Prisma Accessライセンス • **SaaS Security**—SaaS Securityライセンス • **NGFW (Managed by Strata Cloud Manager)**—サポートおよびAIOps for NGFW Premiumライセンス またはEnterprise DLPライセンスを含む以下のいずれかのライセンス • Prisma AccessCASBライセンス • Next-Generation CASB for Prisma Access and NGFW (CASB-X)ライセンス • Data Securityライセンス

Enterprise Data Loss Prevention (E-DLP)は、不正アクセス、誤用、抽出、共有から機密情報を保護します。 Strata Cloud ManagerのEnterprise DLPにより、NGFW、Prisma Accessモバイルユーザー、リモートネットワーク全体で組織のデータセキュリティ基準を適用し、機密データの損失を防ぐことができます。

主な機能

- エンタープライズデータ損失防止（**E-DLP**）ダッシュボード

  Enterprise DLPの設定と管理を行うには、**[Manage (管理)]** > **[Configuration (設定)]** > **[Data Loss Prevention (** データ損失防止 **- DLP)]**に移動します 。

  Enterprise DLP設定は、Enterprise DLPを使用している製品間で共有されます。他の場所で設定された設定がここに表示されることがあります。ここで設定できる一部の設定は、他の製品でも活用できます。

- 定義済み+カスタム**Enterprise DLP**設定

  Enterprise DLPには、最も機密性の高いコンテンツの保護を迅速に開始するために使用できるビルトイン設定が含まれています。

  - 定義済みregexとMLベースのデータパターンは、スキャンして保護する可能性のある一般的な種類の機密情報(クレジットカードや社会保障番号など)を指定する
  - 定義済みデータプロファイルは、一般的に同じタイプの強制を必要とするデータパターンをグループ化します

  Strata Cloud Manager上で直接カスタムデータパターンやプロファイルを作成することもできます。

- **DLP**インシデントの調査

  DLPインシデントは、トラフィックがStrata Cloud Managerのセキュリティポリシールールにアタッチされたデータプロファイルと一致すると生成されます。DLPインシデントダッシュボードでは、一致したデータパターン、トラフィックの送信元と宛先、ファイルおよびファイルタイプなど、インシデントをトリガーしたトラフィックの詳細を表示できます。

- サポートされているファイル形式の画像をスキャンする

  OCR（光学文字認識）により、データの誤用、紛失、盗難を未然に防ぐセキュリティ体制をさらに強化します。OCRを使用すると、DLPクラウドサービスは、Enterprise DLPフィルタリングプロファイルに一致する機密情報を含む画像で、サポートされているファイルタイプをスキャンできます。

- 完全データマッチング **(EDM)**

  EDMは、機密データの流出を監視し、保護する高度な検出ツールです。EDMを使用して、データベース、ディレクトリサーバー、構造化データファイル（CSVおよびTSV）などの構造化データソースで、社会保障番号、医療記録番号、銀行口座番号、クレジットカード番号などの機密性の高いPII（個人識別情報）を高い精度で検出します。

- カスタム ドキュメント タイプ

  知的財産や機密情報を含むカスタムドキュメントをEnterprise Data Loss Prevention (E-DLP)にアップロードして、カスタムドキュメントタイプを作成できます。カスタムドキュメントタイプは、高度なデータプロファイルで一致条件として使用され、流出を検出して防止します。

- 電子メール**DLP**

  電子メールDLPは、AI/MLを活用したデータ検出により、機密情報を含むEメールの流出を防止します。たとえば、エンタープライズDLPは、組織内の営業マンから個人のEメールに送信されるアウトバウンド電子メールを介して機密データが流出するのを防ぐことができます。

- **Enterprise DLP**のロールベースのアクセス

  Strata Cloud Manager内のEnterprise DLPコントロールへのロールベースのアクセスを有効にできます。これにより、Enterprise DLPのさまざまな部分に対する読み取りおよび書き込みアクセス権を持つユーザーを制御できます。

始めましょう

STEP 1 | Strata Cloud ManagerでEnterprise DLPを有効にします。

Enterprise DLPを設定するには、DLPクラウドサービスがトラフィックを検査できるように復号化プロファイルを作成する必要があります。**[Manage (管理)]** > **[Configuration (構成)]** > **[Security Services (セキュリティサービス)]** > **[Decryption (復号化)]**を選択します。

1. **[Manage (管理)]** > **[Configuration (設定)]** > **[NGFW**と**Prisma Access]** > **[Security Services (セキュリティサービス)]** > **[Decryption (復号化)]**を選択し、**[Add Rule (ルールを追加)]**します。

   事前定義済みの復号プロファイル設定により、Enterprise DLPはトラフィックを検査できます。**Strip ALPN**（**Advanced Settings (詳細設定)** > **SSL Forward Proxy (SSL**フォワードプロキシ**)**）を有効にする必要がない限り、定義済みの復号化プロファイル設定の変更は必要ありません。
2. 復号化プロファイルを**SSL**フォワードプロキシ復号化ルールに追加します。

- エンタープライズDLPを有効にする方法

STEP 2 | （任意）**[Manage (管理)]** > **[Configuration (設定)]** > **[Data Loss Prevention (** データ損失防止 **- DLP)]** > **[Detection Methods (検出方法)]**を選択し、データパターンを作成します。

カスタムEnterprise DLPデータパターンを作成して、機密性が高く、保護が必要なコンテンツを指定できます。これはフィルタリング対象のコンテンツです。正規表現に基づくカスタムデータパターンまたはファイルプロパティに基づくデータパターンを作成できます。

- データパターンの作成方法はこちら

STEP 3 | データプロファイルを作成する

同様に適用すべきデータパターンをデータプロファイルにグループ化します。また、データプロファイルを使用して、追加の一致基準と照合の信頼度レベルを指定することもできます。

- データプロファイルの作成方法はこちら

STEP 4 | DLPルールを作成する

Enterprise DLPで保護するトラフィックとファイルの種類を指定します。DLPインシデントを検出したときにEnterprise DLPが実行するアクションを設定します。

- DLPルールの作成方法はこちら

管理:SaaS セキュリティ

どこで使用できますか?	何が必要ですか?
• Prisma Access （*Strata Cloud Manager*または*Panorama*の設定管理付き）	❑ Prisma Accessライセンス

SaaS Security Inlineにより、承認対象アプリと非承認対象アプリケーションのクラウドベースの脅威とリスクの高いユーザーアクティビティを特定。

SaaS Security Inlineは、Cloud Managed Prisma Accessに組み込まれており、ネットワークとCASBのセキュリティを一元的に確認できます。SaaSの可視性（高度な分析とレポート機能を含む）を提供するため、組織はネットワーク上でのSaaSアプリケーションの使用を承認または承認されていないデータセキュリティ リスクを把握できます。

Cloud Access Security Broker（CASB）バンドルには、SaaS Security Inline、エンタープライズデータ損失防止（DLP）Inline、SaaSセキュリティAPI、データ損失防止（DLP）API、SaaSセキュリティ体制管理（SSPM）が含まれています。

次世代Cloud Access Security Broker（CASB-X）ライセンスには、SaaS Security Inline、SaaSセキュリティAPI、SaaSセキュリティ体制管理（SSPM ）、エンタープライズDLPなどのCASBコンポーネントがすべて含まれています。CloudマネージドPrisma Access、PanoramaマネージドPrisma Access、PanoramaマネージドNext Generation Firewall (NGFW) の各デバイスでシングルテナント環境に適用できます。

SaaS セキュリティを***Strata Cloud Manager***で利用する上で必要なこと。

始めましょう

以下は、SaaS Security Inline on Prisma Access Cloud Management (Prisma Access Cloud管理におけるSaaS Security Inline)の立ち上げ手順です。

SaaS SecurityアドオンライセンスがPrisma Accessサブスクリプションに含まれていることを確認します。

[Manage (管理)] > **[Configuration (構成)]** > **[Overview (概要)]**に進み、ライセンスで利用可能な内容を確認してください。

まだの場合は、ハブでSaaS Security Inlineアプリケーションをアクティベートします。

アクティベーション後、SaaS Security InlineはすべてのSaaSアプリケーションとユーザーを自動的に検出し、Strata Logging Serviceに蓄積されたPrisma Accessログからユーザーのアクティビティと利用状況のデータを分析します。

管理者の役割とアクセスを確認および管理します。

［**Settings (設定)**］ > ［**Identity and Access (IDとアクセス)**］に進み 、[Prisma Access Cloud Management］でSaaSのセキュリティコントロールにロールベースでアクセスできるようにします。

*SaaS Security*を包括的に管理するには、*SaaS Security Inline*アプリケーションの管理者でもある必要があります。*Prisma Access Cloud Management*ダッシュボードから***SaaS Security Console***に直接ジャンプして、*SaaS Security Inline*の管理者を追加できます。

Prisma Access Cloud Managementの**SaaS Security**ダッシュボードをご覧ください。

[Manage (管理)] > **[Configuration (設定)]** > **[Security Services (セキュリティサービス)]** > **[SaaS Security (SaaSセキュリティ)]**を順に選択します。

すべてのダッシュボードビューは、Prisma Access Cloud Managementで直接サポートされます。これらのビューを調べて、リスクの高いSaaSアプリケーションとユーザー、およびSaaSセキュリティ体制管理を特定します。SaaSセキュリティ体制管理（SSPM）は、継続的な監視を通じて、承認されたSaaSアプリケーションの設定ミスを検出し、修正するのに役立ちます。

SaaSセキュリティレポートを確認し、共有します。

SaaS Security Inlineには、高度な集計データとビューでアプリケーション使用状況のスナップショットを提供するSaaS Securityレポートが含まれています。このレポートは、SaaSセキュリティチームと経営幹部とのコミュニケーションツールとして役立ちます。このオンデマンドPDFレポートは、SaaSセキュリティチームと共有して定期的にチェックインしたり、組織で使用しているSaaSアプリケーションとそれらが引き起こすセキュリティ リスクを強調するために、レポートを経営陣に電子メールで送信したりできます。

- SaaSセキュリティレポートはこちら

- SaaS Security Inlineアプリケーションで SaaS Securityレポートを生成する方法はこちら

SaaS SecurityとPrisma Access Cloud Managementでできることは、他にもあります。

SaaS ポリシーの推奨事項

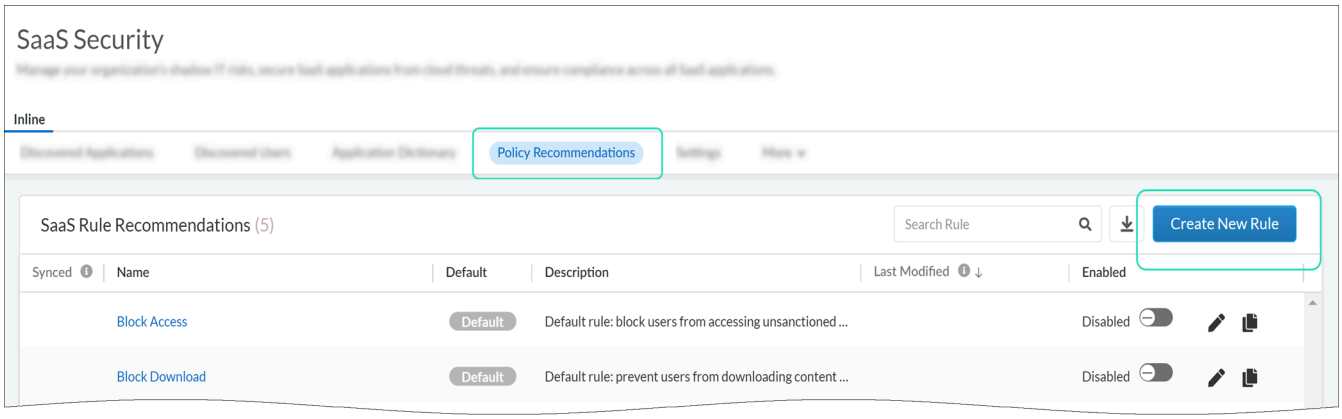
SaaSアプリケーションの可視化と制御を実現するために、SaaSセキュリティ管理者は、App-ID Cloud Engine（ACE）が提供する特定のSaaS App-IDを使用してSaaSルールの推奨事項を作成します。

Prisma Access Cloud Managementでは、SaaS Security管理者が推奨するルールを確認し、受け入れることを選択できるようになりました。SaaSルールの推奨事項がWebアクセスポリシーに追加されます。SaaSルールの推奨事項を利用するには、Webセキュリティを有効にする必要があります。

開始手順 — **SaaS**ポリシーの推奨事項を確認し、受け入れるためのワークフローをここで確認します。

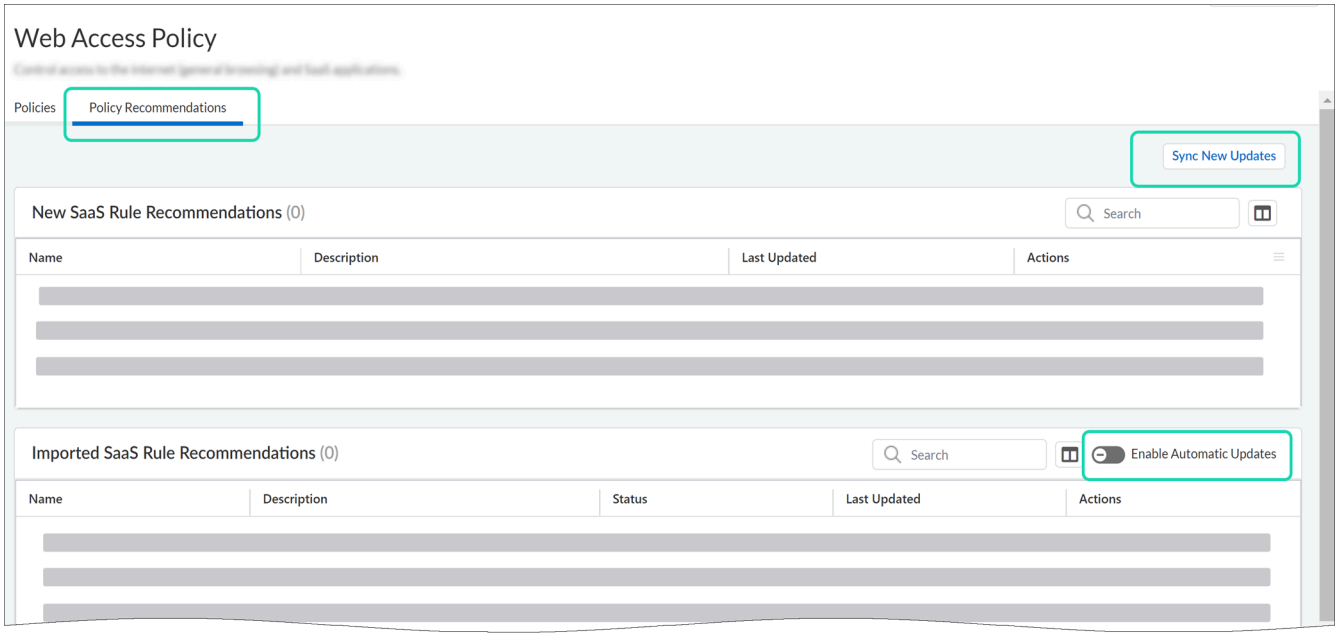
1. SaaSセキュリティ管理者は、SaaS Security InlineアプリケーションまたはPrisma Access Cloud ManagementでSaaSルールの推奨事項を直接作成します。

   Prisma Access Cloud Managemenで、**[Manage (管理)]** > **[Configuration (設定)]** > **[Security Services (セキュリティサービス)]** > **[SaaS Security (SaaSセキュリティ)]**を順に選択します。

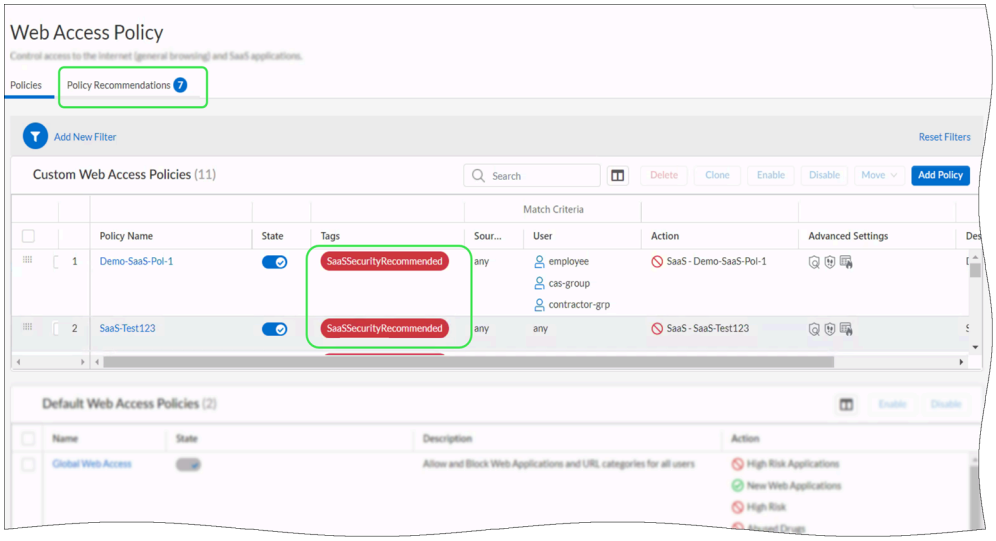


2. SaaSルールの推奨事項を確認してインポートできます。

   # **[Manage (管理)]** > **[Web Security (Webセキュリティ)]** > **[Web Access Policy (Webアクセスポリシー)]**



3. インポートしたSaaSルールの推奨事項にはラベルが貼られているので、簡単に識別できます。



管理:Prisma SD-WAN

どこで使用できますか?	何が必要ですか?
• Prisma SD-WAN	❑ Prisma SD-WANライセンス

Prisma SD-WANは、レガシーWAN（ワイドエリアネットワーク）を徹底的に簡素化された安全なアプリケーションファブリック（AppFabric）に変換し、異種混在の基盤となるトランスポートを統一されたハイブリッドWANに仮想化する、ソフトウェア定義型のワイドエリアネットワーク（SD-WAN）ソリューションを提供します。システムの中核となるのは、アプリケーション パフォーマンス エンジンです。

詳細なアプリケーション駆動型分析の表示、堅牢なポリシーの構築、WANのパフォーマンスベースのトラフィック管理が可能です。Prisma SD-WANは、インスタントオンネットワーク（ION）デバイスを通じて、WANの設計、構築、および管理方法を簡素化し、データセンタークラスのセキュリティをネットワークエッジまで安全に拡張します。

Prisma SD-WANは、フロー転送操作のスタックポリシーをサポートします。中央で定義されたポリシーを使用して、各IONデバイスはリンク間の自動パス選択、トラフィックシェーピング、アクティブ/アクティブ負荷分散などのアクションを実行し、Prisma SD-WANコントローラーはすべてのWANリンクにわたってアプリケーションのパフォーマンスと応答時間を完全に可視化します。

Prisma SD-WANは、アプリケーションパフォーマンスのSLA（Service Level Agreement）とビジネスの優先順位に基づいて、ネットワークアプリケーションのパフォーマンスを制御します。Strata Cloud Managerを使用して、Prisma SD-WANのポリシー、リソース、CloudBlades、およびシステム設定を構成できます。

[Manage (管理)] > **[Prisma SD-WAN]** を選択して、以下の構成を管理します。

- [Policies (ポリシー)]
- [Resources (リソース)]
- [CloudBlades]
- [System (システム)]

管理:Prisma SD-WANに関するポリシー

どこで使用できますか?	何が必要ですか?
• Prisma SD-WAN	❑ Prisma SD-WANライセンス

Prisma SD-WANはスタックポリシーとオリジナルポリシーをサポートします。中央で定義されたポリシーを使用して、各IONデバイスはリンク間の自動パス選択、トラフィックシェーピング、アクティブ/アクティブ負荷分散などのアクションを実行します。またPrisma SD-WANコントローラは、すべてのWANリンクでアプリケーションのパフォーマンスと応答時間を完全に可視化します。

Strata Cloud Managerを使用してPrisma SD-WANにポリシーを設定します。

STEP 1 | **[Manage (管理)] > [Prisma SD-WAN] > [Policies (ポリシー)]**。

Prisma SD-WAN

:では、以下の種類のポリシーを設定することができる。

- Path (パス)

  フロー転送とトラフィックシェーピング操作のためのスタックパスポリシーを設定する。

- Performance (パフォーマンス)

  パフォーマンスポリシーを構成して、アプリケーションのパフォーマンスとアプリケーションのSLAを測定します。

- QoS

  ビジネスの優先順位を指定するためのスタックQoSポリシーを設定します

- Security (セキュリティ)

  スタックセキュリティポリシーを設定し、ブランチ内のアプリケーションアクセスを決定するルールを定義します。

- NAT

  スタックNATポリシーを設定して、パブリックネットワークまたはプライベートネットワークに接続された内部ネットワークのプライバシーを確保します。

- セキュリティ(オリジナル)

  レガシーセキュリティポリシーです。IONデバイスソフトウェアバージョン6.0.1以降の新規ユーザーの場合、スタックセキュリティポリシーのみを設定できます。元のポリシーまたはレガシーポリシーを構成している場合は、デバイスをリリース6.0.1にアップグレードする前に、これらのレガシーポリシーをスタックポリシーに変換する必要があります。

- ネットワーク(オリジナル)

  レガシーネットワークポリシーです。IONデバイスソフトウェアバージョン6.0.1以降の新規ユーザーの場合、スタックネットワークポリシーのみを設定できます。元のポリシーま

たはレガシーポリシーを設定している場合は、デバイスをリリース6.0.1にアップグレードする前に、これらのレガシーポリシーをスタックポリシーに変換する必要があります。

STEP 2 | ポリシースタックをサイトにバインドするには**[Bindings (バインド)]**を選択します。

Path、QoS、Security、および NATスタックのポリシー ルールを有効にするには、ポリシースタックをサイトにバインドする必要があります。サイトにバインドできるパス、QoS、セキュリティ、および NATスタックは一度に1つだけです。

管理:Prisma SD-WANのリソースタイプ

どこで使用できますか?	何が必要ですか?
• Prisma SD-WAN	❑ Prisma SD-WANライセンス

さまざまなタイプのリソースをPrisma SD-WANで管理できます。

Strata Cloud Managerを使用してPrisma SD-WAN内のリソースを管理します。

[Manage (管理)] > **[Prisma SD-WAN]** > **[Resources (リソース)]**。

Prisma SD-WAN:

では、次のタイプのリソースを管理できます。

- アプリケーション

  PrismaのSD-WANソリューションの中核となるアプリケーションです。ネットワークに配置されたIONデバイスは、パフォーマンス、コンプライアンス、セキュリティに関するポリシーが維持されるように各アプリケーションフローを積極的に分析し、各フローに最適なネットワーク接続を使用します。IONデバイスは、パス選択、QoS、ファイアウォールポリシーにアプリケーション定義とフィンガープリント技術を使用します。

  システム アプリケーションはデフォルトで使用できますが、企業要件に合わせてカスタム アプリケーションを構成できます。

- 回路カテゴリ

  回路カテゴリは、ネットワークに存在する可能性のあるさまざまな種類の回線および接続を論理的にグループ化したものです。このグループ化により、ネットワーク全体のネットワークポリシールールが簡素化され、再利用可能になります。たとえば、インターネットケーブルブロードバンド、従量制インターネットLTEリンク、衛星インターネットリンク、インターネットDSL、プライベートMPLSなどです。

- ネットワークコンテキスト

  ネットワークコンテキストは、同じアプリケーションに異なるネットワークポリシールールを適用する目的で、ネットワークトラフィックをセグメント化します。ネットワークコンテキストのあるルールは、常にネットワークコンテキストのないルールよりも優先されます。1つ以上のネットワークコンテキストを作成できますが、個々のLANネットワークは1つのネットワークコンテキストにしか属しません。有効にするには、ネットワークコンテキストを適切なLANセグメントに接続する必要があります。

- サービスおよびDCグループ

  サービスおよびDCグループを使用して、サードパーティのエンドポイントをグループにマッピングし、サイト間の一意性を考慮してネットワークポリシールールを作成する際に柔軟性を持たせることができます。サイトの場所に関係なく、ポリシー ルールは変わらないという意図があります。

- セキュリティ ゾーン

  セキュリティゾーンは、トラフィックが検査およびフィルタリングの対象となる施行境界を指定します。各セキュリティ ゾーンは、デバイスの物理インターフェイス、論理インターフェイス、またはサブインターフェイスに接続されたネットワークにマップされます。これらのゾーンレベルのインターフェイスは、VLAN、レイヤー3 VPN、レイヤー2 VPN回線などの物理回線および仮想回線のプロキシとして機能します。

- サイトテンプレート

  サイト設定テンプレートを使用すると、デプロイメント要件に応じたサイトテンプレートをカスタマイズして作成できるため、ブランチオフィスやデータセンターを大規模に簡単に効率的にデプロイできます。このテンプレートを使用すると、複数のサイトをデプロイできます。既存のテンプレートを使用したり、既存のテンプレートを編集したり、新しいテンプレートを作成して複数のサイトをデプロイしたりできます。

- プレフィクスフィルタ

  プレフィクスとは、1つ以上の個別のIPアドレスまたはIPアドレスサブネットのグループです。プレフィックスは、パスセットポリシーとプライオリティポリシーとともに使用されます。スコープはグローバルまたはローカルのいずれかです。

- 設定プロファイル

  設定プロファイルを使用して、さまざまなタイプのリソースの設定を構成します。

  - IPsec

    ブランチデバイスとクラウドセキュリティサービスのエンドポイント間のIPsec VPN接続を構成するIPsecプロファイルを作成します。

  - IPFIX

    IPFIX プロファイルは、コレクタ設定、フィルタ設定、フロー情報要素をエクスポートするためのテンプレート、およびフローサンプラー設定を識別するグローバル IPFIX 設定オブジェクトです。

  - APN

    APN（アクセスポイント名）プロファイルを作成して、セルラーデータ接続のネットワークパスを定義します。携帯電話ネットワークに接続するにはAPN情報が必要です。

  - DNS

    ドメイン ネーム システム(DNS)プロファイルを構成して、DNSサービスの設定パラメータを指定します。一般的に設定されるパラメータには、DNSサーバ、ドメインとア

ドレスのマッピング、キャッシュの設定、DNSSECの設定などがあります。DNSサービス プロファイルの作成後、デバイスにバインドされます。

- NTPテンプレート

  NTPサーバーを追加または編集するには、NTP(ネットワーク タイム プロトコル)設定テンプレートを使用します

- マルチキャスト

  WANマルチキャスト設定プロファイルを作成し、ブランチサイトに関連付けて、ブランチサイトのマルチキャストWANマルチキャストルーティングを有効にします。

- VRF

  グローバル（デフォルト）仮想ルーティングおよび転送テーブル（VRF）プロファイルを作成して関連付け、すべてのブランチサイトおよびデータセンターサイトに割り当てます。

- IoTディスカバリー

  IoTデバイスの可視性を使用して、ネットワーク内のデバイスを識別します。Prisma SD-WANブランチIONデバイスは、パケットを検査して情報を抽出し、特定のフォーマットでStrata Logging Serviceに送信するメッセージを生成します。

管理:CloudBlades for Prisma SD-WAN

どこで使用できますか?	何が必要ですか?
• Prisma SD-WAN	❑ Prisma SD-WANライセンス ❑ それぞれのCloudBladeのライセンス

Prisma SD-WANCloudBladesプラットフォームを使用してIONデバイスに安全にアクセスし、カスタマイズされたテンプレートを使用してWebインターフェースのワークフローを自動化することで、運用の複雑さを軽減します。

Strata Cloud Managerを使用してPrisma SD-WANでCloudBladesを設定します。

[Manage (管理)] > **[Prisma SD-WAN]** > **[CloudBlades]**を選択します。

Prisma SD-WANでサブスクリプションしているCloudBladesを閲覧できるようになります。関連するCloudBlade統合ガイドの手順を使用して、CloudBladeを設定します。

管理:Prisma SD-WANのシステムリソース

どこで使用できますか?	何が必要ですか?
• Prisma SD-WAN	❑ Prisma SD-WANライセンス

[System (システム)]タブで利用可能なリソースを使用して、ユーザーと権限をPrisma SD-WANで管理および監視します。

[Manage (管理)] > **[Prisma SD-WAN]** > **[System (システム)]**を選択します。

Prisma SD-WAN:

では、次のタイプのシステムリソースを設定できます。

- ライセンス管理

  ライセンス管理を使用して、仮想IONの認証トークンを生成します。これにより、環境への仮想デバイスの不正な追加を防止するための制御セットが提供されます。

- 監査ログ

  監査ログを使用して、システムの構成変更レコードを表示します。これらのログは、コンプライアンスおよびトラブルシューティングの目的で使用できます。監査ログは、サイト、システム、またはサイトのサブセットで行われた変更、変更の所有者、変更時刻、変更の範囲などの情報を提供します。

- エンタープライズプレフィックス

  エンタープライズプレフィックスを使用すると、Prisma SD-WANデータセンターサイトでブランチサイトへのルーティングと到達可能性を簡単にアドバタイズできます。

- アクセス管理
  - ユーザーアクセス
    - ユーザー管理

      企業の要件に応じて、システムロールを持つ新しいユーザーを追加します。システムロールは、各ロールに対して事前に定義された権限セットです。これらのロールには、1つ以上のシステム権限の集合が含まれます。使用できるシステムロールには、ルート、スーパー管理者、IAM管理者、ネットワーク管理者、セキュリティ管理者、表示専用ユーザーがあります。

    - カスタムロール

      既存のシステムロールと権限をさまざまな方法で組み合わせてカスタムロールを構築できます。システム権限のセットを組み立てるか、システムロールに対して権限を追加または削除することによって作成できます。

- パスワード要件

  パスワードの文字要件とセキュリティ要件を設定します。古いパスワードの再利用やパスワードの更新の頻度も設定できます。

- デバイスアクセス
  - デバイスツールキットユーザーアクセス
  - デバイスオフラインアクセスポリシー
- テナントアクセス
  - 認証トークン

    Prisma SD-WAN APIにアクセスするための認証トークンの設定トークンをユーザーに生成したら、それを使ってAPI呼び出しを繰り返すことで、APIへのアクセスに不要なログインが不要になります。

    認証トークンにアクセスできるユーザーは、トークンに割り当てられたすべての権限にアクセスできます。

    [Manage (管理)] > [System (システム)] > [Tenant Access (テナントアクセス)] > [Auth Tokens (認証トークン)] > [Create Auth Token (認証トークンの作成)]を選択して認証トークンを作成します。
- ID管理
  - クラウドIDエンジン

管理:Prisma Access Browser

どこで使用できますか?	何が必要ですか?
• Prisma Access (Managed by Strata Cloud Manager)	❑ Prisma Accessライセンス

Strata Cloud Managerから、**[Manage (管理)]** > **[Configuration (説明)]** > **[Prisma Access Browser]**を選択します。

Prisma Access Secure Enterprise Browser (Prisma Access Browser)は、管理されていないデバイスにまで保護を拡張するネイティブに統合されたEnterprise Browserを通じて、管理されているデバイスと管理されていないデバイスの両方を保護する唯一のソリューションである。「Prisma Access Browserとは」を参照します

ホーム

ホームとは、Strata Cloud ManagerからPrisma Access Browserにアクセスするときのランディングページです。ホームページから、Prisma Access Browser Dashboardsを使って、ユーザーの振る舞いや閲覧データの分析から意味のあるインサイトを取得することができます。ユーザー振る舞い、データ漏洩防止、Webセキュリティ、ポリシーなど、監視したいユースケースに応じたさまざまなダッシュボードが用意されています。各ダッシュボードにはウィジェットのコレクションが含まれており、ウィジェットの一部は複数のダッシュボードに表示されます。

分析

「Prisma Access Browserイベント」画面は、Enterprise Browserのデプロイメント環境内のすべてのアクティビティを調査し、ポリシーやルールが適切に機能しているかどうかを確認するための重要な可視性ツールです。Prisma Access Browserイベント調査を行う場所です。

ディレクトリ

- ユーザー ディレクトリは、ユーザとそのPrisma Access Browser接続デバイスに関する情報、ユーザグループへのメンバシップ、および関連するポリシー ルールの中央の場所として機能します。Prisma Access Browserのユーザーの管理
- デバイスディレクトリは、Prisma Access Browserのデバイスとデバイスグループの名簿を提供します。Prisma Access Browserデバイスの管理
- Prisma Access Browserには、検証済みアプリケーションの既存リストが付属しています。検証済みアプリケーションリストは、Palo Alto Networks App-ID™のアプリケーションカタログを参照し、定期的にクラウドデータベースと同期されます。カスタムアプリケーションやプライベートアプリケーションを作成することもできます。Prisma Access Browserアプリケーションの管理
- Prisma Access Browserは、エンドユーザーがブラウザにインストールした拡張機能を含むExtensionディレクトリを保持しています。この情報により、適切な企業ポリシー管理、可視性の管理、リスク分析が可能になります。Prisma Access Browser Extensionsの管理

ポリシー

- Rules(ルール)を使用して、さまざまなポリシーの影響を受けるユーザー、ユーザー グループ、デバイス グループを指定できます。これらのルールは、Webアプリケーションへのアクセス、セキュリティポリシー、およびカスタマイズオプションを管理します。ルールを利用することで、組織のツールやコンポーネントへのユーザーアクセスを正確に制御できます。Prisma Access Browserポリシー ルールの管理
- Prisma Access Browserルールのコントロールは、個々の規則の本文内で設定できます。プロファイル（外部コントロール）は、再利用可能な（レガシー）プロファイルを保存して、後でルールに追加したいときに使用できます。Prisma Access Browserのポリシープロファイルの管理
- サインイン ルールを使用して、Prisma Access Browserにアクセスできるユーザーとデバイスを決定します。Prisma Access Browserのサインインルールの管理
- ポリシー ルール内でバイパス条件を定義した後、ユーザが を実行してアクションを実行しようとしたり、対応するルールによってブロックされているサイトにアクセスしたりしたときに、バイパス要求を送信できます。バイパス条件を設定するには、権限要求を有効にするプロンプト アクションを設定します。ポリシー ルールをバイパスするPrisma Access Browserの要求の管理。

管理

次の機能を使用して、追加機能のための統合管理を実施します。

- Microsoft 365
- Microsoft Information Protection
- Google Workspace
- Votiro
- CrowdStrike Falcon Intelligence
- OPSWAT MetaDefender
- YazamTech SelectorIT
- Symantec DLP

管理:業務

どこで使用できますか?	何が必要ですか?
• Prisma Access （*Strata Cloud Manager*または*Panorama*の設定管理付き） • Software NGFW Creditsによって資金提供されたものを含むNGFW	❑ Strata Cloud Managerで設定を管理し、NGFWとPrisma Accessを統合管理するには、次のライセンスの両方が必要です。 ❑ Prisma Access[ライセンス] ❑ AIOps for NGFW Premium license (use the Strata Cloud Manager app) ❑ Strata Cloud Manager Essentials ❑ Strata Cloud Manager Pro → どのライセンスを使用しているかによって、Strata Cloud Managerで利用できる機能や性能は異なります。

Strata Cloud Manager操作を使用して、設定の変更をプッシュしたり、過去の設定プッシュを確認したり、設定バージョンのスナップショットを管理して、設定をロードしたり、以前の設定バージョンに戻したりできます。

- 設定変更をプッシュする
- 設定のプッシュのステータスを確認する
- 設定のクリーンアップ方法を見る

管理:設定のプッシュ

どこで使用できますか?	何が必要ですか?
• Prisma Access （*Strata Cloud Manager*または*Panorama*の設定管理付き） • Software NGFW Creditsによって資金提供されたものを含むNGFW	❑ Strata Cloud Managerで設定を管理し、NGFWとPrisma Accessを統合管理するには、次のライセンスの両方が必要です。 ❑ Prisma Access[ライセンス] ❑ AIOps for NGFW Premium license (use the Strata Cloud Manager app) ❑ Strata Cloud Manager Essentials ❑ Strata Cloud Manager Pro → どのライセンスを使用しているかによって、Strata Cloud Managerで利用できる機能や性能は異なります。

設定を変更し、それを有効にする準備ができたら、変更をファイアウォールにプッシュする必要があります。すべての構成変更をプッシュするか、プッシュに含める特定の管理者を選択するかを選択できます。最初の構成プッシュでは、すべての管理者からの変更をプッシュする必要があります。Prisma Accessにプッシュする構成変更を選択できます。

- **Web** セキュリティ

  Web セキュリティの更新をPrisma Accessにプッシュします。
- モバイルユーザー **— (GlobalProtect)**

  Global Protectの更新をPrisma Accessにプッシュします。
- モバイルユーザ - 明示型プロキシ

  明示的なプロキシの更新をPrisma Accessにプッシュします。
- リモートネットワーク

  リモート ネットワークの更新をPrisma Accessにプッシュします。
- サービスコネクション

  サービスコネクションの更新をPrisma Accessにプッシュします。

別の設定のプッシュが行われている間に、別の設定をプッシュできます。Prisma Accessは、送信された順序で設定の変更を適用します。

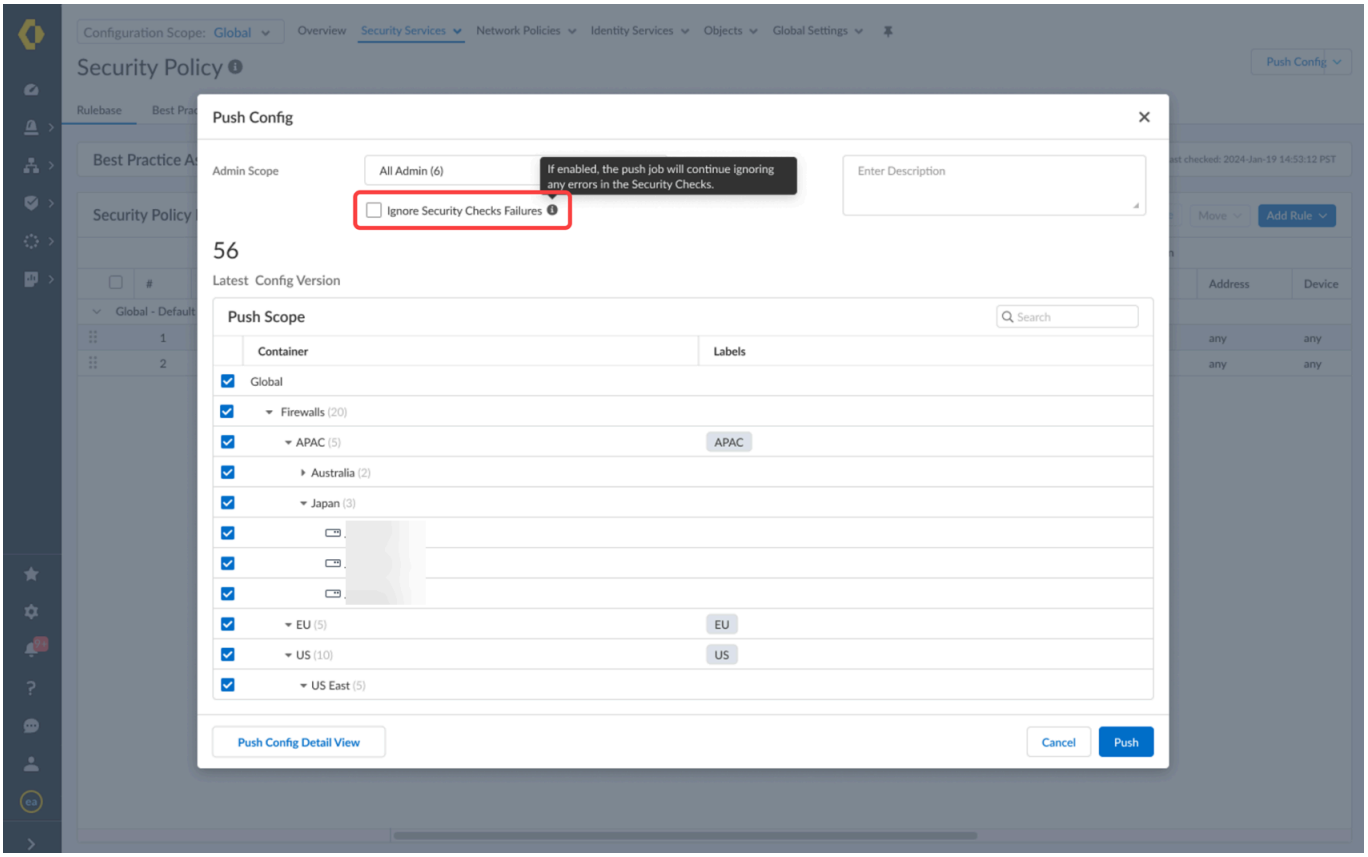
構成が誤ってプッシュされた場合、または変更によってネットワークまたはセキュリティが中断された場合は、Prisma Accessの設定を最新の実行中のPrisma Accessの設定に戻すことができます。これにより、Prisma Accessの設定を、機能することがわかっていてネットワーク セキュリティが損なわれない実行中の設定に戻すことができます。特定の実行設定を選択するオプションはありません。Prisma Access は、最後に実行された既知の設定を自動的に選択し、それに戻します。

STEP 1 | Strata Cloud Managerにログインします。

STEP 2 | 必要に応じて構成を変更します。

STEP 3 | **[Push Config (設定をプッシュ)]**をクリックし 、設定の変更 をプッシュします 。

または、***[Manage (管理)] > [Operations (オペレーション)] > [Push Config To Devices (デバイスへの設定のプッシュ)]***を選択することもできます。



[Push Config (プッシュ構成)] ダイアログ ボックスでは、 セキュリティ チェックの失敗を無視できます。この機能を使用すると、特定のチェックによってプロセスがブロックされる場合でも、プッシュ操作を続行できます。チェック ボックスをオフのままにした場合 (デフォルト設定)、「ブロック」アクションによるベスト プラクティス チェックが失敗すると、Strata Cloud Manager はプッシュを停止します。

STEP 4 | (任意) 新しいフィルターを追加します。

フィルターを適用することで、プッシュ スコープに表示されるデバイスをフィルターできます。フィルターを適用すると、プッシュ スコープに表示されるファイアウォールまたはPrisma Accessデプロイメントにのみ影響し、プッシュ先のデバイスには影響しません。

STEP 5 | プッシュ スコープを編集します。

プッシュ スコープを編集すると、ファイアウォールまたはPrisma Accessデプロイメントの一部またはすべてに対象を絞った構成変更をプッシュできます。

次に該当する場合は、部分的な設定プッシュはサポートされていないため、全体の*Strata Cloud Manager*構成をプッシュする必要があります。

- 新しいテナントを構成します 。これが最初の構成プッシュになります。
- *Strata Cloud Manager*にファイアウォールを導入します。
- *Prisma Access*モバイル ユーザーとリモート ユーザーをオンボードします。
- フォルダーの名前を変更するか、 フォルダー を移動して、別のフォルダーの下にネストします。
- ファイアウォールを別のフォルダーに移動します。
- スニペットの名前を変更したり、関連付けたり、関連付けを解除したりします。
- 設定をロードします。
- 設定を最後にプッシュされた構成または以前の設定バージョンのスナップショットに戻します。

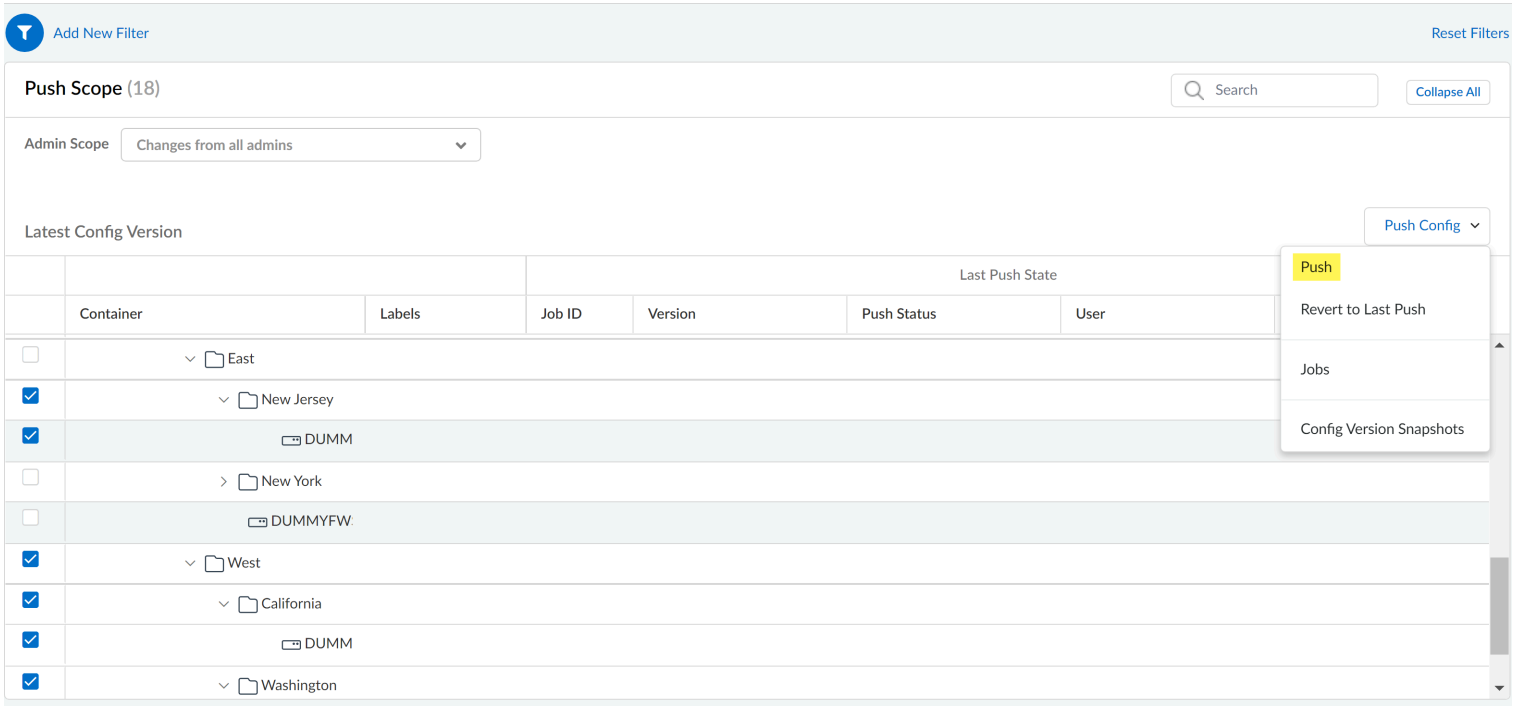
- 管理スコープ - プッシュに含める管理者設定の変更を選択します。デフォルトでは、管理者スコープは現在のユーザーを選択し、そのユーザーによって行われた変更は、選択したファイアウォールまたはPrisma Accessデプロイメントにプッシュされます。すべての管理者からの変更を 選択すると、すべての管理者によって行われたすべての構成変更が含まれます。

  管理スコープを編集して特定の管理者を選択すると、選択した管理者によって行われたすべての構成変更が含まれます。このオプションは、最初の構成プッシュを実行するときには使用できません。プッシュに含める特定の構成変更を選択することはサポートされていません。
- プッシュ スコープ - プッシュ先のデプロイメント タイプまたはフォルダーを選択します。デプロイメントまたはフォルダーを選択すると、構成の変更がすべてのファイアウォールまたはデプロイメントにプッシュされます。

  子フォルダーを含むフォルダーを選択すると、すべての子フォルダーと、関連付けられているファイアウォールまたはPrisma Accessデプロイメントがプッシュに含まれます。特定のファイアウォールまたはPrisma Accessのデプロイメントを選択すると、それに関連付けられているフォルダーが自動的に選択されます。

STEP 6 | プッシュ構成 と プッシュ。

プッシュ ターゲットを確認して、 プッシュします。



STEP 7 | 設定プッシュのステータスを確認します。

設定が誤ってプッシュされた場合、または変更によってネットワークまたはセキュリティが中断された場合は、Prisma Accessの設定を元に戻すことができます。

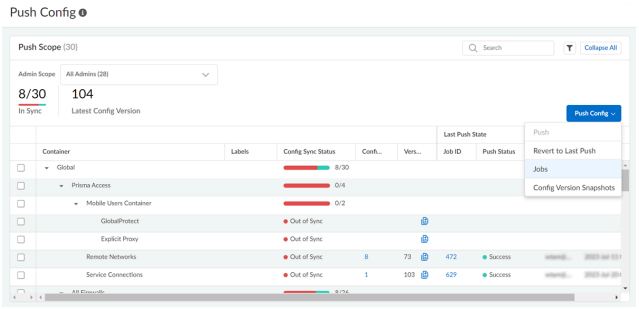
設定バージョンの復元、読み込み、比較

Prisma Access の求人を見る

Prisma Access で ジョブ 履歴を表示して、管理者が開始した操作の詳細や、自動コンテンツおよびライセンスの更新を表示できます。これには、設定のコミット、プッシュ、および元に戻すことが含まれます。[Jobs (ジョブ)]ビューを使用すれば、失敗した操作についてトラブルシューティングを行ったり、完了したコミットに関する警告について調査を行ったり、保留中のコミットをキャンセルしたりすることができます。

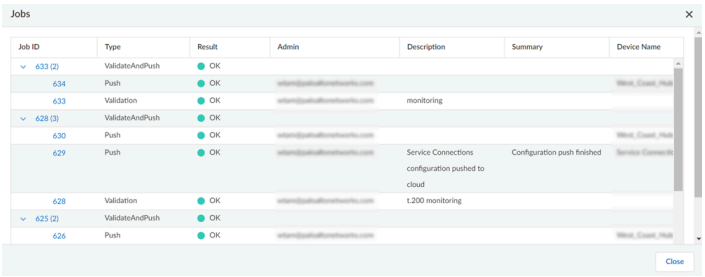
STEP 1 | Prisma Access を起動します。

STEP 2 | 上部のメニュー バーで **[Push Config (設定をプッシュ)]** を選択し、Prisma Access ジョブを表示します。



STEP 3 | 次のいずれかのタスクを実行します。

- 警告または障害を調査する- 警告または障害の詳細については、[概要] 列のエントリを読み取ります。
- コミットの説明を表示する- 管理者がコミットの説明を入力した場合は、[Description (説明)] 列を参照してコミットの目的を理解できます。
- キュー内の操作の位置を確認する- 操作の位置とステータスを表示して、操作の位置を決定します。



管理:プッシュステータス

どこで使用できますか?	何が必要ですか?
• Prisma Access （*Strata Cloud Manager*または*Panorama*の設定管理付き） • Software NGFW Creditsによって資金提供されたものを含むNGFW	❑ Strata Cloud Managerで設定を管理し、NGFWとPrisma Accessを統合管理するには、次のライセンスの両方が必要です。 ❑ Prisma Access[ライセンス] ❑ AIOps for NGFW Premium license (use the Strata Cloud Manager app) ❑ Strata Cloud Manager Essentials ❑ Strata Cloud Manager Pro → どのライセンスを使用しているかによって、Strata Cloud Managerで利用できる機能や性能は異なります。

ファイアウォールへの過去の設定プッシュのプッシュステータスを確認し、プッシュ操作の結果、プッシュを開始した管理者、対象のファイアウォールなどの詳細を確認します。

STEP 1 | Strata Cloud Managerにログインします。

STEP 2 | 設定変更をプッシュします。

STEP 3 | **[Manage (設定)] > [Operation (オペレーション)] > [Push Status (プッシュステータス)]**を選択し、確認する設定プッシュ操作を探します。

STEP 4 | 確認する設定プッシュのジョブIDを展開します。

設定検証ジョブは、設定プッシュが発生する前に必ず実行されます。複数のファイアウォールにプッシュする場合、各設定プッシュにはプッシュの詳細を持つ一意のジョブIDが設定されます。

STEP 5 | 設定プッシュステータスの詳細を確認します。

たとえば、プッシュの結果、設定プッシュを開始した管理者、設定プッシュの概要、設定プッシュの終了時刻と開始時刻を確認します。

設定プッシュの結果は、プッシュが成功した場合は「OK」、設定プッシュに失敗した場合は「FAIL」のいずれかになります。

STEP 6 | ファイアウォールへの設定プッシュの一意のジョブIDをクリックして、[ジョブの詳細]を確認します。

[ジョブの詳細]には、設定プッシュの実行時に発生する警告とエラーに関する詳細情報が表示されます。たとえば、ファイアウォールへのプッシュが失敗した場合、[Job Details (ジョブの詳細)]を確認して、設定プッシュが失敗した原因を把握できます。

管理:設定バージョン スナップショット

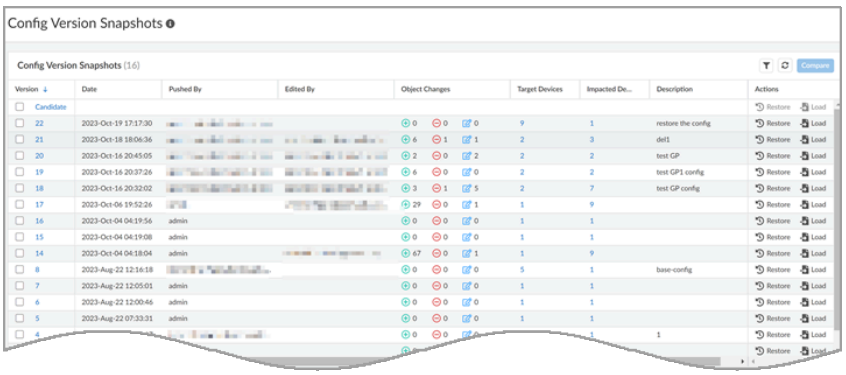
どこで使用できますか?	何が必要ですか?
• Prisma Access （*Strata Cloud Manager*または*Panorama*の設定管理付き） • Software NGFW Creditsによって資金提供されたものを含むNGFW	❑ Strata Cloud Managerで設定を管理し、NGFWとPrisma Accessを統合管理するには、次のライセンスの両方が必要です。 ❑ Prisma Access[ライセンス] ❑ AIOps for NGFW Premium license (use the Strata Cloud Manager app) ❑ Strata Cloud Manager Essentials ❑ Strata Cloud Manager Pro → どのライセンスを使用しているかによって、Strata Cloud Managerで利用できる機能や性能は異なります。

設定スナップショットでは、Strata Cloud Manager設定履歴を確認できます。設定プッシュが意図しないセキュリティ上の影響や、トラフィックに予期しない影響を与える場合は、以前のバージョンに戻すことで回復できます。設定を比較して、バージョン間で何が変わったかを確認することもできます。

構成スナップショットの概要

「スナップショットバージョンの構成」画面は、プッシュされた構成の確認、構成スナップショットと構成候補との比較、および古い構成の読み込みや復元を行う場所です。

[Manage (管理)] > [Operations (運用)] > [Config Version Snapshots (設定スナップショット)]を選択して、設定スナップショットを検索し、バージョンを復元、ロード、または比較します。



1. ［**Add New Filter (新しいフィルタの追加)**］ – フィルタを選択して、設定バージョンをカラム別にソートおよびフィルタリングします。

2. **[Version (バージョン)]** – プッシュされた設定のバージョン番号。

   Candidate (候補)では、現在保留中の設定変更とStrata Cloud Managerを以前の設定バージョンと比較できます。

   設定バージョン番号は増分です。例えば、バージョンが*10*で、設定バージョン*2*を復元すると、設定バージョンが*10*から*11*に変わります（*2*と表示されません）。
3. **Date (日付)** – 設定がプッシュされた日付と時刻。
4. **Pushed By (プッシュ者)** – 変更をプッシュした管理者。
5. **Edited By (変更者)** – プッシュされる前に設定変更を行った管理者。
6. **Object Changes (オブジェクトの変更)** – 設定がプッシュされたときに追加、削除、または変更されたオブジェクトの数を確認できます。
7. **Target Devices (ターゲット デバイス)** – 設定のスコープでターゲットとされたデバイスがスナップショットをプッシュします。

   Restore (復元)アクションを実行する場合、操作を実行するデバイスを選択できます。
8. ［**Impacted Devices (影響を受けるデバイス)**］ – 前回の設定プッシュ以降に変更されたデバイス。デバイスは、以前の設定プッシュスナップショットにのみ影響があると見なされます。

   影響を受けるデバイスと対象デバイス

   *A*と*B*の*2*つのデバイスがあり、デバイス*A*にのみプッシュする場合、*A*が*Target and Impacted (*標的と影響を受けた*)*デバイスになります。

   その後、デバイス*A*とデバイス*B*に再度プッシュすると、*A*と*B*は両方とも対象デバイスになりますが、*B*だけが「影響を受けたデバイス」になります。

   ロードアクションを実行すると、表示されているデバイスが影響を受けます。
9. 説明 – 設定がプッシュされた時点で提供された情報を確認します。
10. リフレッシュ – スナップショット表の情報を更新します。
11. フィルターのリセット – すべてのフィルタをクリアすると、すべての設定バージョンが表示されます。
12. 比較 – バージョンによって何が変わったかを確認します。

    一度に比較できるのは*2*つのバージョンのみです。

13.アクション – コンフィギュレーション バージョンを復元またはロードできます。

- 復元 – 以前の設定バージョンを復元します。

  コンフィギュレーション バージョンを復元すると、元のプッシュの範囲内で展開上の実行コンフィギュレーションが直接更新されます。［**Push Config (**設定をプッシュ**)**］を実行する必要はありません。

  設定プッシュの元の範囲にあるすべてのデバイスまたはデプロイメントを復元するか、復元する特定のデバイスまたは展開を選択します。設定を拡張して、元のスコープ外のデバイスやデプロイメントを含めることはできません。

  設定バージョンを復元しても、候補設定は削除または変更されません。実行中の設定が保存されます。設定を復元すると、実行コンフィギュレーションのバージョンが更新されるだけです。復元アクションを使用すると、デプロイメントが同期していないように見えることがあります。

- ロード – Strata Cloud Managerで以前のバージョンを候補構成として読み込みます。古い設定が読み込まれると、現在の候補設定は失われます。

  新しい候補設定の更新や、元の設定スナップショット以外の新しいデバイスや展開への設定の適用を行い、準備ができたら［**Push Config (**設定をプッシュ**)**］します。

- 保存 – 候補構成を既知の構成として使用する名前付きスナップショットとして保存します。設定がわかっていると、展開を既知の実行可能な状態に簡単に戻すことができます。[名前付きスナップショット]と、自動的にログに記録される構成のプッシュ[バージョンスナップショット]を切り替えることができます。

*Strata Cloud Manager*では、最大*6*ヶ月分のスナップショットまたは*200*個のスナップショットが保存されます。

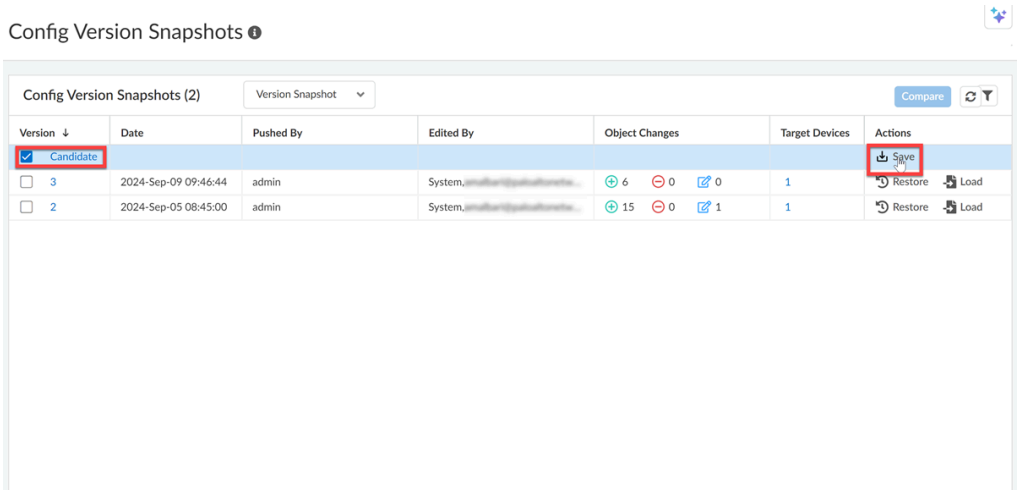
名前付きスナップショットを保存する

現在の設定候補を名前付きスナップショットとして保存します。部分的な設定を名前付きスナップショットとして保存することはできません。名前付きスナップショットを保存すると、既知の設定状態をロードできます。最終的に ［Config Versions Snapshot (設定バージョンのスナップショット)］ テーブルから循環される個々のスナップショットを追跡する必要はありません。

STEP 1 | Strata Cloud Managerにログインします。

STEP 2 | **[Manage (**管理**)]** > **[Operations (**運用**)]** > **[Config Version Snapshots (**設定バージョン スナップショット**)]**を選択します。

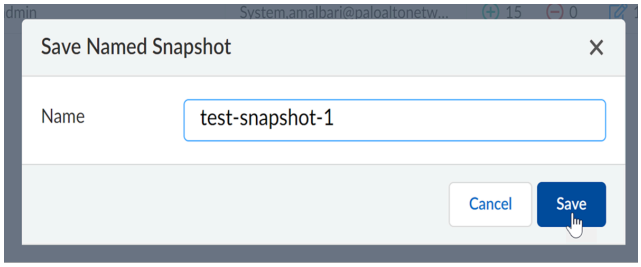
STEP 3 | **Candidate (候補)**を選択します。



STEP 4 | **Save**（保存）をクリックします。

STEP 5 | 「名前」に64文字以内で入力します。

スナップショットの「名前」は、デフォルトで**config_year-month-day-timestamp**になります。

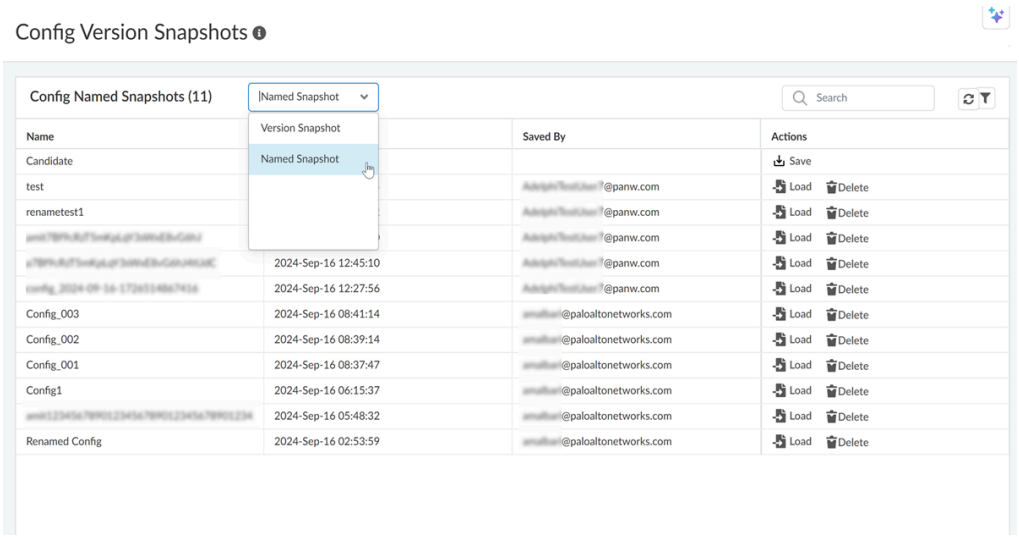


STEP 6 | スナップショットを保存します。

STEP 7 | （任意）［Config Version Snapshot (設定バージョンスナップショット)］ 表の ［**Named Snapshots (名前付きスナップショット)**］ に移動して、スナップショットが保存されたことを確認します。

名前付きスナップショットの管理

管理者は自分の名前付きスナップショットを削除できます。スーパーユーザーはすべての名前付きスナップショットを削除できます。



スナップショットを復元する

以前にプッシュした設定を復元します。古い設定を復元すると、配置およびデバイスで実行されている設定が更新されます。これらの変更はStrata Cloud Managerに反映されないため、展開とデバイスが同期していないように見えることがあります。

元の設定プッシュの範囲にあった設定済みデバイスのみ、選択したバージョンに復元できます。

STEP 1 | Strata Cloud Managerにログインします。

STEP 2 | **[Manage (管理)] > [Operations (運用)] > [Config Version Snapshots (設定バージョン スナップショット)]**を選択します。

STEP 3 | 復元する設定バージョンを選択します。

1. （任意）バージョン番号を選択して、構成スナップショットによって行われた変更を確認します。

STEP 4 | のバージョンを復元します。

1. （オプション）復元アクションの対象にするデバイスを選択します。
2. 復元する。

STEP 5 | （任意）**[Manage (管理)] > [Configuration (設定)] > [Operations (運用)] > [Push Config (設定のプッシュ)]**を選択し、設定が復元されたことを確認します。

スナップショットを読み込む

以前の設定スナップショットをロードして、候補設定として使用します。

設定が読み込まれたら、プッシュする前に変更を続けることができます。

STEP 1 | Strata Cloud Managerにログインします。

STEP 2 | **[Manage (管理)] > [Operations (運用)] > [Config Version Snapshots (設定バージョン スナップショット)]**を選択します。

STEP 3 | ロードする設定バージョンを選択します。

1. （任意）バージョン番号を選択して、構成スナップショットによって行われた変更を確認します。

STEP 4 | バージョンをロードします。

STEP 5 | （任意）必要に応じて、読み込まれた設定候補を変更します。

STEP 6 | 構成をプッシュします。

管理:セキュリティ態勢

どこで使用できますか?	何が必要ですか?
• Prisma Access （*Strata Cloud Manager*または*Panorama*の設定管理付き） • Software NGFW Creditsによって資金提供されたものを含むNGFW	❑ Strata Cloud Managerで設定を管理し、NGFWとPrisma Accessを統合管理するには、次のライセンスの両方が必要です。 ❑ Prisma Access[ライセンス] ❑ AIOps for NGFW Premium license (use the Strata Cloud Manager app) ❑ Strata Cloud Manager Essentials ❑ Strata Cloud Manager Pro → どのライセンスを使用しているかによって、Strata Cloud Managerで利用できる機能や性能は異なります。

これらのツールを使用してセキュリティ態勢を改善し、セキュリティ ポリシーのベストプラクティスに従って脅威から保護されていることを確認します。

- デプロイメントのセキュリティ体制チェックをカスタマイズして、管理:セキュリティ体制の設定に関連する推奨事項を最大限に高めます。
- 設定クリーンアップを使用して、未使用の設定オブジェクトとポリシー ルールを識別し、削除します。
- コンプライアンスチェックを設定して、許容しすぎるセキュリティルールを磨き、ネットワークで実際に使用されているアプリケーションのみを許可するように最適化します。
- 独自の管理:セキュリティ体制の設定の作成 – 既存のベストプラクティス チェックをカスタマイズし、組織のビジネス要件により適合するように特別な免除を作成および管理します。
- Policy Analyzer (ポリシーアナライザ)を使用すると、セキュリティ ポリシー ルールの更新が要件を満たし、エラーや設定ミス（ルールの重複や競合を招く変更など）が発生しないことを迅速に確認できます。

管理:ポリシーアナライザー

どこで使用できますか?	何が必要ですか?
• NGFW (Panorama管理) • VM-Series, funded with Software NGFW Credits(Panorama管理) • Prisma Access (Managed by Panorama)	❑ 以下のライセンスのうち少なくとも1つが必要です。 ❑ AIOps for NGFW Premium license (use the Strata Cloud Manager app) ❑ Strata Cloud Manager Pro ❑ Panorama管理デプロイメント用Panorama CloudConnectorプラグイン

セキュリティ ポリシー ルールの更新は、時間的制約を伴うことが多く、迅速な対応が求められます。ただし、セキュリティ ポリシーのルールベースに対して行う更新は、要件に適合し、エラーや設定ミス（ルールの重複や矛盾を招くような変更）が発生しないようにする必要があります。

これに向けて、Strata Cloud ManagerのPolicy Analyzer (ポリシーアナライザー)を使用すると、変更要求を実装するときに時間とリソースを最適化できます。Policy Analyzer (ポリシーアナライザー)は、特定のルールを分析して、意図に沿った統合や削除の可能性を提案するだけでなく、ルールベースのシャドウ、冗長性、汎化、相関、統合などの異常もチェックします。

Policy Analyzer (ポリシーアナライザー)を使用して、セキュリティ ポリシーのルールベースを追加または最適化します。

- 新しいルールを追加する前に – 新しいルールを追加する必要があるかどうかを確認します。Policy Analyzer (ポリシーアナライザー)は、可能であれば別のルールを追加せずに、要件を満たすために既存のセキュリティポリシールールを変更する最善の方法を推奨します。
- 既存のルールベースの合理化と最適化：肥大化を最小限に抑え、競合を排除するために、また、トラフィックの実施がセキュリティ ポリシーのルールベースの意図と一致するように、ルールをアップデートできる場所を確認できます。

変更をコミットする前と後の両方でセキュリティ ポリシー ルールを分析します。

- 変更前ポリシー分析 – 新しいルールの影響を評価し、既存のルールに対して新しいルールの意図を分析して、その意図に最も適合する方法を推奨できます。
- 変更後ポリシー分析 – 時間の経過とともに蓄積されたシャドウ、冗長性、およびその他の異常を特定することで、既存のルールベースをクリーンアップできます。

詳細については、 Policy Analyzer (ポリシー アナライザー) を参照してください。

管理:ポリシー オプティマイザー

どこで使用できますか?	何が必要ですか?
• Prisma Access （*Strata Cloud Manager*または*Panorama*の設定管理付き） • Software NGFW Creditsによって資金提供されたものを含むNGFW	❑ Strata Cloud Managerで設定を管理し、NGFWとPrisma Accessを統合管理するには、次のライセンスの両方が必要です。 ❑ Prisma Access[license (ライセンス)] ❑ AIOps for NGFW Premium license (use the Strata Cloud Manager app) ❑ Strata Cloud Manager Pro → どのライセンスを使用しているかによって、Strata Cloud Managerで利用できる機能や性能は異なります。

早期アクセスが可能な期間にポリシーオプティマイザーをお試しください。早期アクセス期間を超えてこの機能を使用し続けることにご関心がありましたら、アカウントチームにご連絡ください。

ルールが広すぎると、ネットワークで使用されていないアプリケーションが許可されるため、セキュリティギャップが発生します。Policy Optimizer を使用すると、これらの過度に寛容なルールを、実際に使用しているアプリケーションのみを許可する、より具体的で焦点を絞ったルールに変換できます。

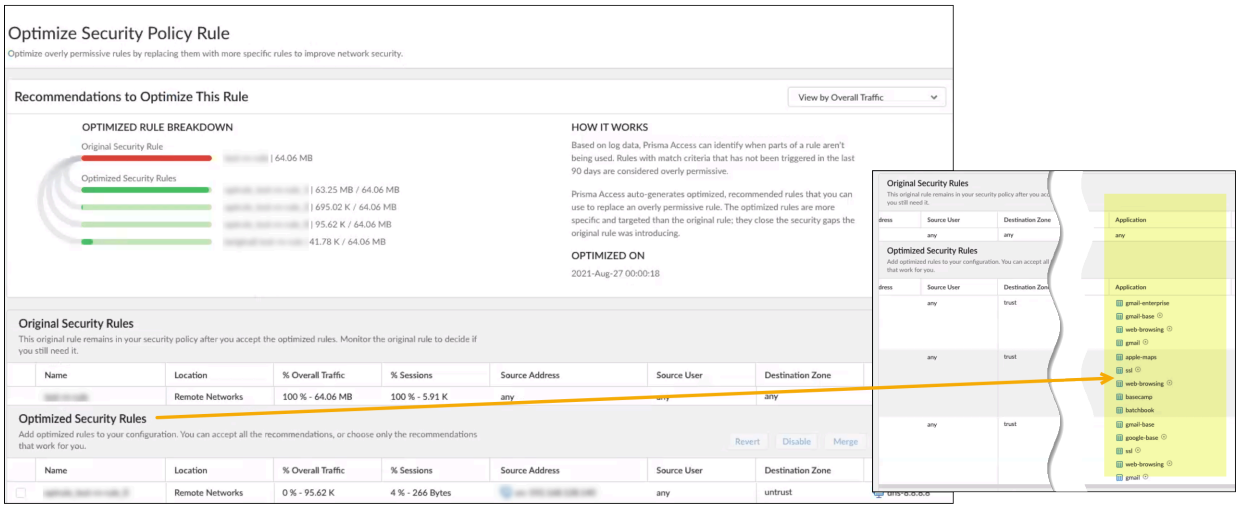
ポリシーの最適化には、過去90日以上作成されたルールのみが考慮されます。

動作の仕組み

Strata Cloud Managerは、ログデータを分析し、任意のアプリケーショントラフィックを許可しているときにルールを過剰許容として分類します。ルールは90日以上経過している必要があります。このようなルールが、企業で使用する必要のないトラフィックを許可している場合、セキュリティの抜け穴をもたらす可能性があります。

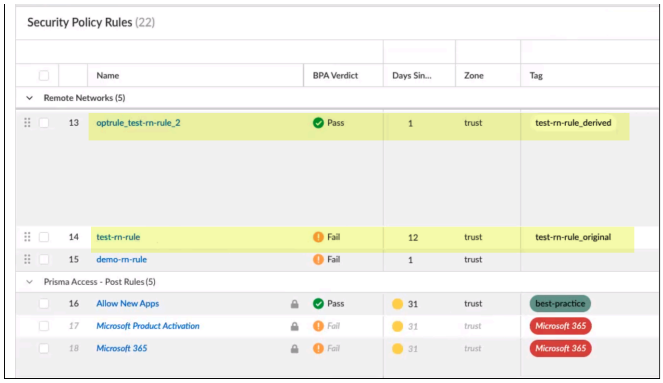
Strata Cloud Managerは、許容度が過剰と判断されたルールに対して、ルールを最適化するための推奨事項を自動生成します。新しい推奨ルールは、元のルールよりも具体的で対象を絞ったものです。過去90日間にネットワークで検出されたアプリケーションだけを明示的に許可します。

寛容すぎるルールを選択し、最適化の推奨事項を確認し、調整して受け入れてください。これらのルールをより具体的で推奨されるルールに置き換えると、セキュリティ体制が強化されます。



ルールを最適化するための推奨事項を受け入れても、元のルールは削除されません。元のルールは、セキュリティ ポリシーの新しいルールの下にリストされたままです。これは、ルールを監視し、必要がないと確信できる場合は削除できるようにするためです。

元のルールと最適化されたルールの両方にタグが付いているので、セキュリティ ポリシーで簡単に識別できます。



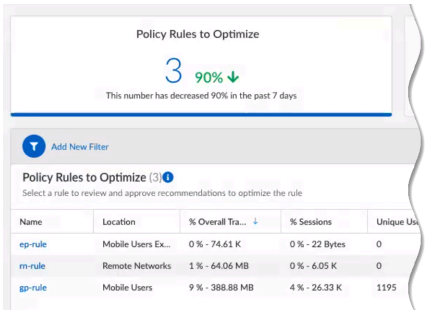
ルールの最適化

STEP 1 | **[Config Cleanup (クリーンアップの設定)]**にアクセスして、最適化できるルールがあるかどうかを確認してください。

[Manage (管理)] > **[Security Posture (セキュリティ体制)]** > **[Policy Optimizer (ポリシーオプティマイザー)]**

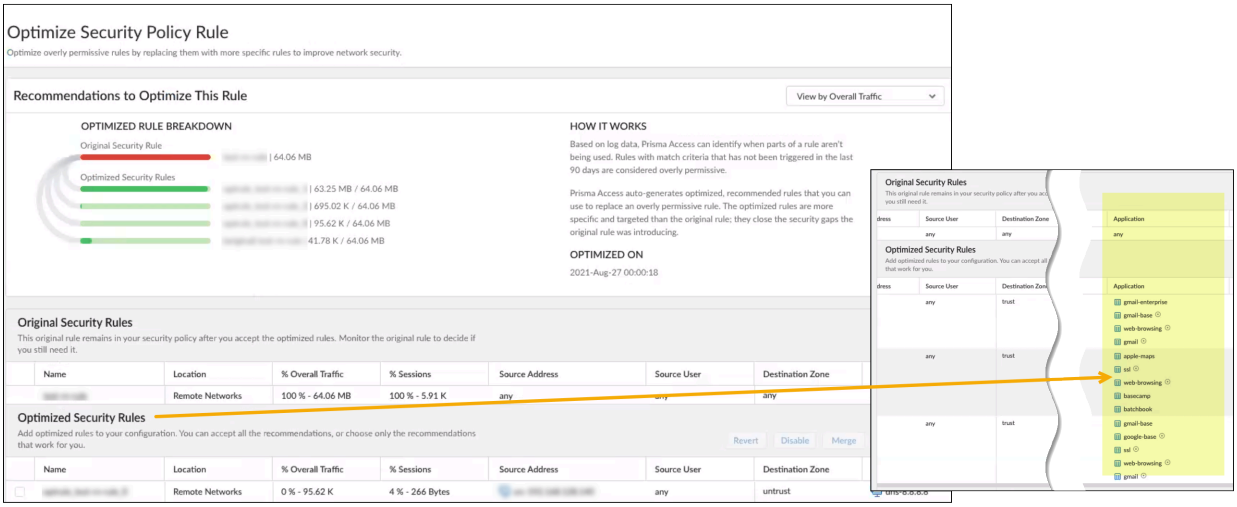
STEP 2 | 過度に許容されるルールを確認し、ルールを選択して最適化の推奨事項を確認します。

許容しすぎるルールが複数ある場合は、最もトラフィックに影響しているルールの最適化に焦点を当てます。セキュリティ体制の強化に向けて、最も大きなメリットが得られます。



STEP 3 | 推奨される最適化されたルールを確認します。

それぞれの新しいルールがカバーする元のルールのトラフィックがどのくらいになるかを確認できます。各新しいルールが適用する特定のアプリケーションに注目してください。



STEP 4 | ルールの推奨事項の一部またはすべてを受け入れます。

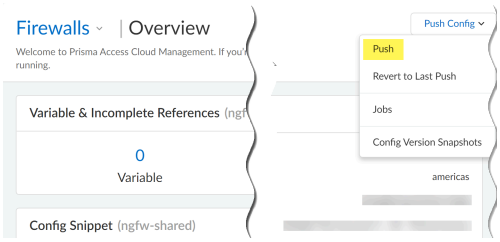
最適化された新しいルールを受け入れると、ルールがルールベースに追加されます。それらはまだアクティブになりません。これは、次のステップでPrisma Accessを**[Push Config (**プッシュ コンフィグ**)]**したときに発生します。

[Accept All (すべて受け入れる**)]**は、推奨ルールをそのまま受け入れます。また、最適化されたルールを受け入れる前に変更を加えることもできます:

- 最適化からルールを削除します。最適化から除外するルールのリストに、このルールを追加します（今回と今後）。
- 最適化されたルールを無効にします。これは、このルールを受け入れていないことを意味し、ルールベースに追加されません。
- 行った変更を元に戻します。これにより、編集した内容が取り消され、ルールが推奨事項に戻ります。
- ルールをマージします。推奨ルールのいずれかが似ているとわかった場合は、これを実行することを決定する場合があります。

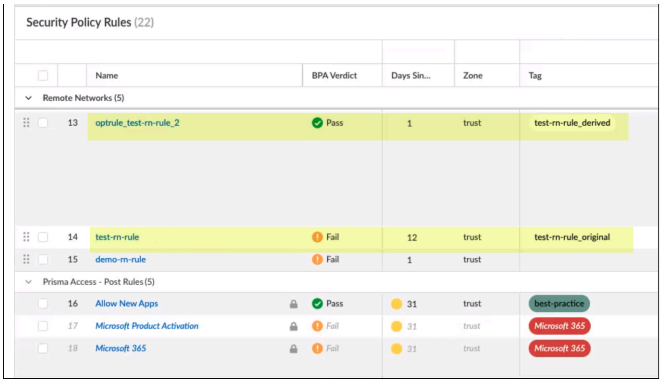
最適化されたルールを受け入れると、**Update Rulebase (**ルールベースの更新**)**のメッセージが表示されます。同意すると、最適化されたルールがセキュリティ ポリシーに追加されます。しかし、まだトラフィックを強制していません。

STEP 5 | **Push Config (**設定をプッシュ**)**を実施してPrisma Accessに送信し、最適化ルールの適用を開始します。



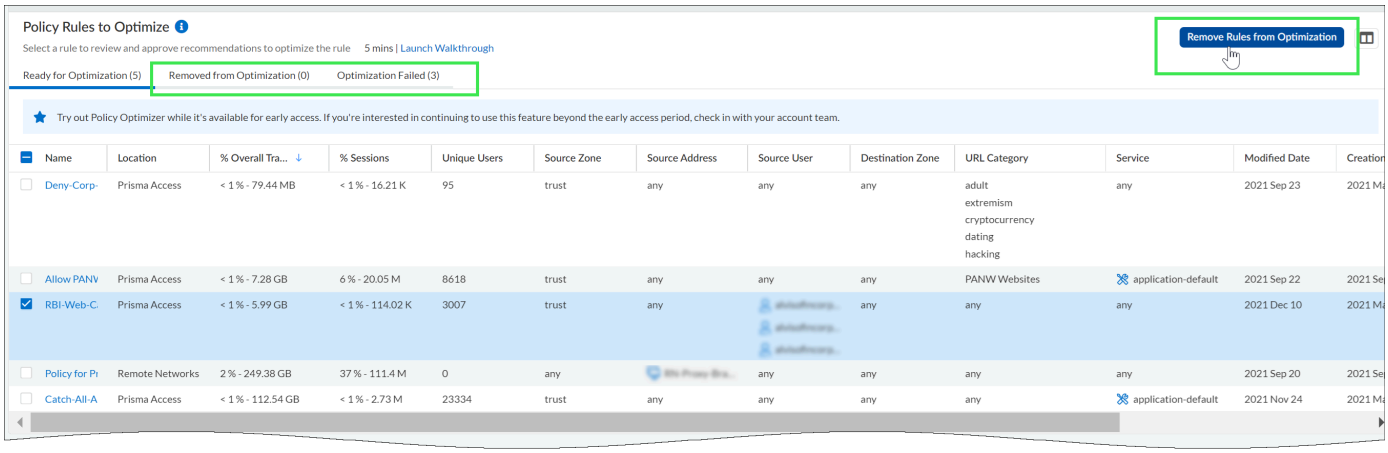
STEP 6 | 元のルールは、必要ないと確信するまで監視しましょう。

元の、過度に許容されたルールはセキュリティ ポリシーに残ります。ルールベースに最適化されたルールの下にリストされ、タグが付いているので、簡単に識別できます。タグ名はルール名に _original を付加します（たとえば、security-rule-name_original）。



最適化からルールを除外する

ルールを**Excluded from Optimization (**最適化から除外リスト**)**に移動すると、Prisma Accessによって最適化されません。ルール設定はそのまま残ります。

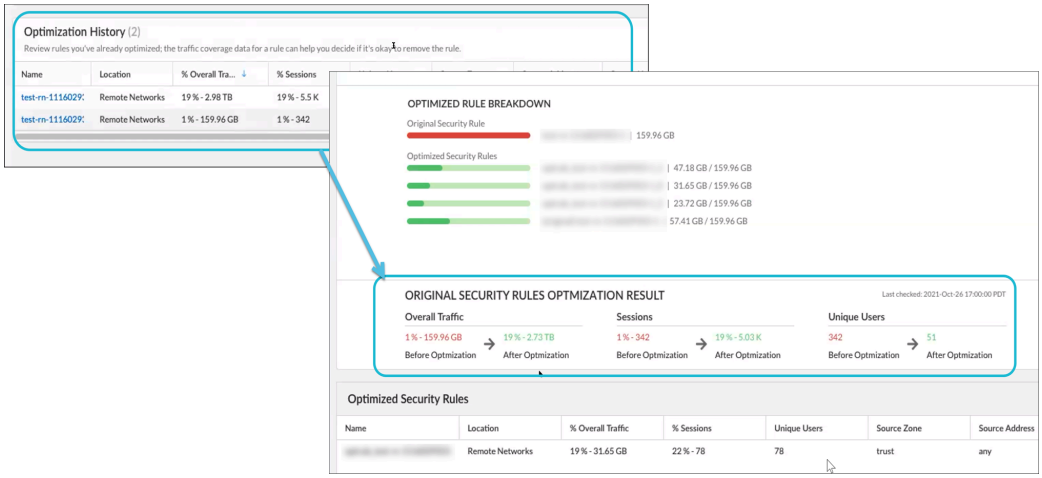


除外リストにルールを移動した後は、必ず［**Push Config (**設定をプッシュ**)**］してください。設定をプッシュした後、ルールがリストに表示されるまでに最大24時間かかることがあります。ルールを後で最適化リストに追加し直すことはいつでも選択できます。

トラックの最適化結果

Policy Optimizer (ポリシーオプティマイザー)は、最適化したセキュリティルールの履歴を表示します。過去のデータには最適化結果が含まれます。オリジナルルールのトラフィックカバレッジと最適化されたルールを比較します。

[Policy Optimizer History (ポリシーオプティマイザーの履歴**)]**に表示されるデータは、過去30日間のものです。元のルール（最適化したルール）が6か月間ヒットしなかった場合、ポリシーオプティマイザの履歴から削除され、代わりにゼロヒット ポリシー ルールとして分類されます。



管理:構成のクリーンアップ

どこで使用できますか?	何が必要ですか?
• Prisma Access （*Strata Cloud Manager*または*Panorama*の設定管理付き） • Software NGFW Creditsによって資金提供されたものを含むNGFW	❑ Strata Cloud Managerで設定を管理し、NGFWとPrisma Accessを統合管理するには、次のライセンスの両方が必要です。 ❑ Prisma Access[ライセンス] ❑ AIOps for NGFW Premium license (use the Strata Cloud Manager app) ❑ Strata Cloud Manager Pro → どのライセンスを使用しているかによって、Strata Cloud Managerで利用できる機能や性能は異なります。

Config Cleanup (設定クリーンアップ)を使用して、未使用の設定オブジェクトとポリシー ルールをStrata Cloud Manager設定より識別し、削除します。未使用の設定オブジェクトを削除すると、雑然とした設定オブジェクトがなくなり、セキュリティの実施に必要な設定オブジェクトだけが保持されるため、ファイアウォールの管理が容易になります。

STEP 1 | Strata Cloud Managerにログインします。

STEP 2 | **[Manage (管理)]** > **[Security Posture (セキュリティ体制)]** > **[Config Cleanup (設定のクリーンアップ)]**を選択します

STEP 3 | 過去6ヶ月間のStrata Cloud Manager設定全体にわたって未使用のオブジェクトとポリシールールを選択します。

- ［**Policy Rules to Optimize (最適化のためのポリシールール)**］ – 過剰に許容されるポリシールールを見直して、実際に使用しているアプリケーションのみを許可する、より具体的で集中的な規則に変換します。
- ［**Unused Objects (未使用オブジェクト（過去6ヶ月分）)**］ – 過去6ヶ月間に任意の設定またはポリシー ルールで未使用になったすべての設定オブジェクト。
- ゼロヒットオブジェクト（過去**6**ヶ月） – ポリシー ルール内の設定オブジェクトがゼロヒットを受ける設定オブジェクトを含むポリシー ルール。

  ここにリストされている設定オブジェクトは、関連付けられているポリシールールでのみゼロヒットを受信しています。彼らの使い方は、彼らが使われている他のポリシー ルールでヒットを受け取るかもしれません。
- ［**Zero Hit Rules** （ゼロヒットルール）（過去**6**ヶ月］ – 過去 6ヶ月間にトラフィックが一致しなかったすべてのポリシー ルール。

STEP 4 | 特定の未使用オブジェクトとポリシー ルールを対象とする追加のフィルタを適用します。

Add New Filter (新しいフィルタの追加**)**は、未使用オブジェクト（過去6ヶ月）とゼロヒット ポリシー ルール（過去6ヶ月）でサポートされています。

- **Unused Objects (**未使用オブジェクト**)**（過去**6**ヶ月） – 次の項目に基づいて、未使用オブジェクトをフィルタリングおよび削除できます。
  - ［**Name (**名前**)**］ – 特定の設定オブジェクト名を検索して選択します。
  - **[Location (**場所**)]** – 設定オブジェクト名が作成された設定範囲。
  - ［**Object Type (**オブジェクトタイプ］ – 設定オブジェクトのタイプ。
  - ［**Days Unused (**未使用日数**)**：設定オブジェクトが使用された日数。
    - **<50** – 未使用期間が50日未満。
    - **>= 50**、**<=100** – 50~100日間未使用。
    - **<50** – 100日以上未使用。
- ゼロヒットポリシールール（過去**6**ヶ月） – 名前、ゼロヒット日数、または送信元と宛先の任意のデータに基づいて、ゼロヒットポリシー ルールをフィルタリングして有効、無効、または削除できます。

管理:セキュリティ体制の設定

どこで使用できますか?	何が必要ですか?
• Software NGFW Creditsによって資金提供されたものを含むNGFW • Prisma Access (Managed by Panorama or Strata Cloud Manager) • Prisma SD-WAN	これらの各ライセンスには、Strata Cloud Managerへのアクセスが含まれています。 ❑ Prisma Access ❑ AIOps for NGFW Premium license (use the Strata Cloud Manager app) ❑ Prisma SD-WAN ❑ Strata Cloud Manager Essentials ❑ Strata Cloud Manager Pro → Strata Cloud Managerで利用できる機能は、使用するライセンスによって異なります。

Strata Cloud Manager は、CIS (Center for Internet Security) や NIST (National Institute of Standards and Technology) などの業界固有の標準サイバーセキュリティ制御に準拠した事前定義済みの ベストプラクティス チェック のセットと、組織の特定のニーズに基づいて作成したカスタム チェックを活用します。これらのチェックでは、クラウド インフラストラクチャ内の構成と設定を評価し、ベストプラクティスやコンプライアンス要件からの逸脱を特定します。

Strata Cloud Managerのセキュリティ ポスチャ チェックには、ネットワーク セキュリティ、データ保護、IDおよびアクセス管理など、さまざまなセキュリティ ドメインが含まれます。これらのチェックでは、ファイアウォール ルール、暗号化、認証メカニズム、および設定の全体的な整合性を評価します。

構成で逸脱が検出されると、Strata Cloud Managerは実用的な洞察と修復の推奨事項を提供し、誤った構成や非準拠の設定を修正するプロセスの一部を自動化して、手動による介入を最小限に抑えながら安全で準拠したクラウド環境を管理できるようにします。

セキュリティ体制の設定では、AIOpsとStrata Cloud Managerのセキュリティ チェック設定ページの両方の機能が統合されます。

[Manage (管理)] > [Security Posture (セキュリティ体制)] > [Settings (設定)] を選択して、デプロイメントのセキュリティ体制チェックを表示、管理、カスタマイズし、関連する推奨事項を最大限に活用します。

- セキュリティ チェック – 構成を評価するために使用されるベストプラクティス チェックのリスト。

  構成はこれらのチェックと比較され、デバイスのセキュリティ状態が評価され、セキュリティ アラートが生成されます。環境に応じてこれらのチェックを管理するには、次のアクションを実行できます。

  1. カスタム チェックの重大度レベルを設定して、デプロイメントにとって最も重要なチェックを識別します。

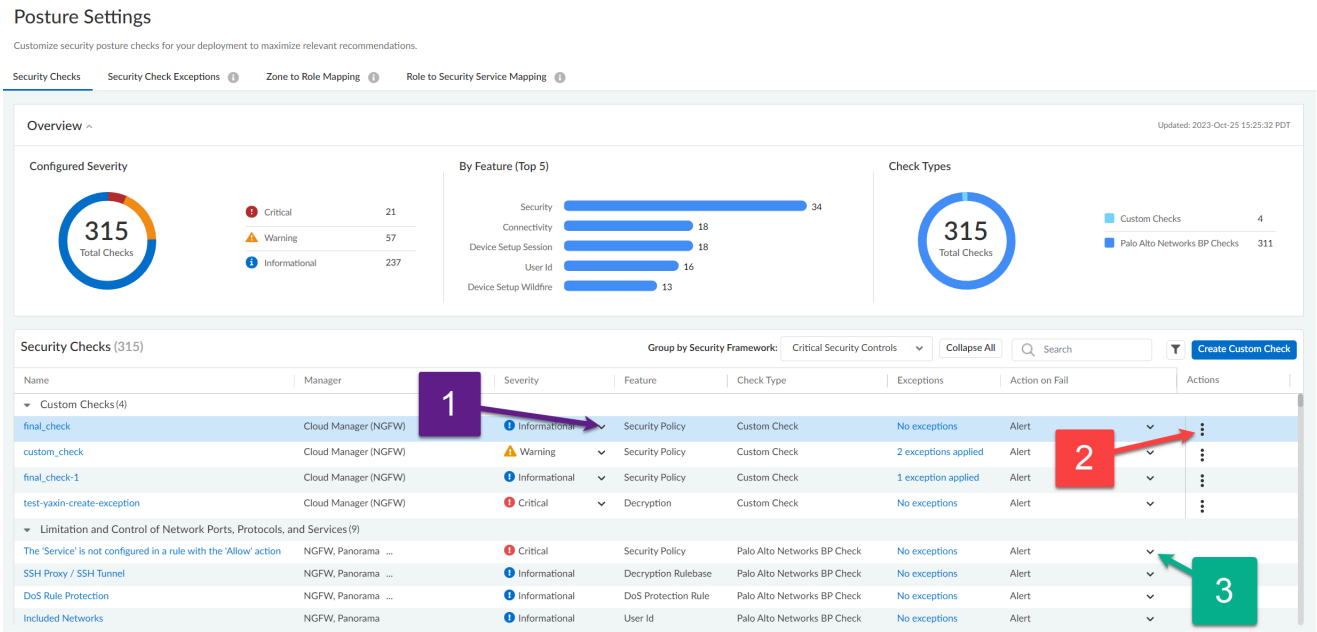
     カスタム チェックの重大度レベルは変更できますが、*Palo Alto Networks* ベストプラクティス チェックの重大度レベルは固定されており、変更できません。

  2. 独自のカスタム チェックを作成 および 削除し 、既存のチェックを 複製 および編集して新しいチェックを作成し、デプロイメントの一部に適用したくないチェックに対して 特別な例外を作成します 。

     これらのチェックの初期ロールアウトの一環として、カスタム チェック フレームワークにあるチェックを複製できます。

  3. チェックが失敗した場合の応答を設定します。
     - アラート (デフォルト) - 失敗したチェックに対してアラートを発します。
     - ブロック - 潜在的な誤った構成がデプロイメント環境に入る前にそれを阻止します。ブロックは、管理方法に応じて次のいずれかを意味します。
       - **Strata Cloud Manager** のインライン チェック - 準拠していない設定のコミットやプッシュを防止しますが、設定をローカルに保存することは防止しません。
       - **Strata Cloud Manager**でのリアルタイム* インライン チェック- 準拠していない設定を保存することを阻止します。
       - **Panorama** 管理**- 非準拠の設定をPanoramaにコミットすることはできませんが、Panorama候補設定に保存することはできます。
       - PAN-OS Webインターフェース、API、または CLI管理 - ブロックは、クラウド管理またはPanorama管理されていない設定には適用されません。

       - *論理的な複雑さのため、一部のインライン チェックは、リアルタイムではなく、固定スケジュールで非同期的に実行されます。設定のリアルタイム チェックに失敗すると、ローカルであってもその設定の保存は阻止されます。
       - ***Panorama*でブロック コミット アクションを強制するには、Panorama CloudConnector プラグインが 必要です。



- セキュリティチェックの例外

  指定したデバイスまたはデバイスのグループに対する個別のチェックをオフにします。
- ゾーンとロールのマッピング

  カスタマイズされた推奨事項を取得するには、NGFW のゾーンをロールにマップします。
- ロールとセキュリティサービスのマッピング

  すべての NGFW のゾーンとロール間のトラフィックに必要なセキュリティサービスを管理します。

カスタムチェックを作成する

既存のチェックから独自のカスタム チェックを作成します。または、手順4に進み、最初からカスタム チェックを作成します。

STEP 1 | **[Manage (管理)] > [Security Posture (セキュリティ体制)] > [Settings (設定)]**を選択します

STEP 2 | 複製するチェックを識別し、 複製します。

STEP 3 | 複製したチェックを編集し 、手順5に進んで変更を加えます。

STEP 4 | **[Manage (管理)] > [Security Posture (セキュリティ体制)] > [Settings (設定)]**を選択し、次に**[Create Custom Check (カスタムチェックの作成)]**を選択します。

STEP 5 | チェックの **[General Information (一般情報)]** を指定します。カスタム チェックには 名前 と 説明が必要ですが、カスタム チェックの意図とベストプラクティスを他のユーザーが理解できるように、チェックの 推奨事項 と 根拠 も追加する必要があります。

STEP 6 | 任意 オブジェクト タイプ – チェックを作成する設定のセクションで、チェックの作成時に選択できる 一致するルール プロパティ を決定します。

STEP 7 | カスタム チェックには **Logic Builder (**ロジック ビルダー**)** を使用します。

1. 式の追加 – 設定の一致条件を記述する1行のロジック。

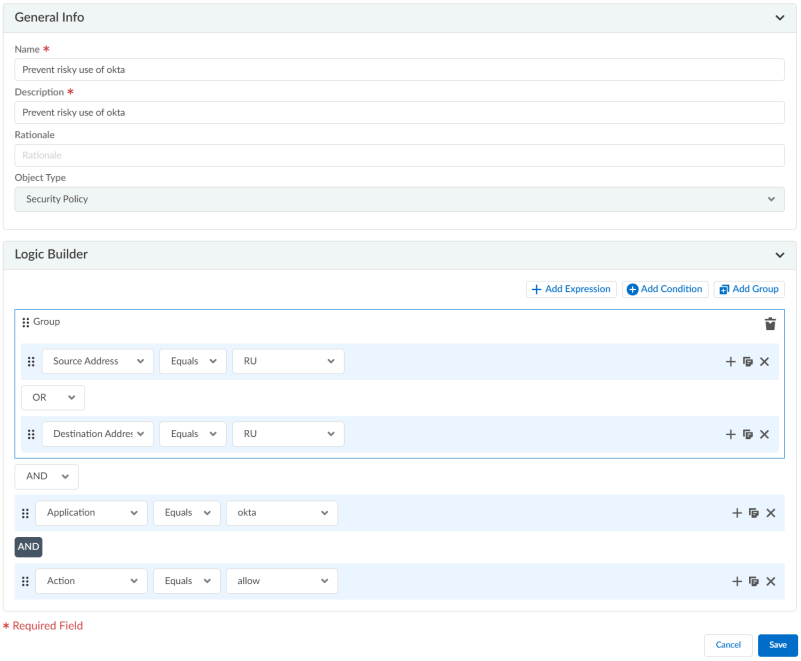
一致するルールプロパティ	一致演算子	具体的な基準
• 一般 - 名前、説明、役職、スケジュール • ソース - ゾーン、アドレス、ユーザー • 宛先 - ゾーンとアドレス • アプリケーション、サービス、およびURL • アクションおよび高度な検査	• です • ではない • 空白 • 空白ではない • Starts with (次で始まる) • Ends with (次で終わる) • 含む • Greater than • In • 等しいかそれ以上 • 等しいかそれ以下 • 未満 • 等しい • 次の値と等しくない • 次を含まない • すべて • いくつかの • どれも	[テキストフィールド]

2. 条件の追加 – 論理演算子 (AND、OR、IF、THEN、ELSE、ELSE IF など) を使用して、式、追加条件、およびグループを接続または結合します。

3. グループの追加 – 式、条件、またはその両方のセットを作成します。このグループをまとめると、True (真)または False (偽)の条件が生成されます。

   - ＋ 新しい式または条件を追加します
   - 式または条件を複製します
   - ✕ 式または条件を削除します

   この例の式は、ロシアのIPアドレスとの間のOktaトラフィックを許可するポリシールールを検出すると警告を発します。この例は、ロジック ビルダーがどのように機能するかを単に説明しているだけであり、推奨を目的としたものではありません。



STEP 8 | チェックを保存します。

チェックの管理

セキュリティ チェックでは、次のいずれかの アクション を実行できます。

- クローン* – チェックのコピーを作成します。
- 編集** – 既存のカスタム チェックに変更を加えます。
- 削除** – 作成したカスタム チェックを削除します。

アクションを実行するチェックを選択し、適切なアクションを選択します。

- *一度に複製できるチェックは*1*つだけです。
- **カスタム チェックのみ編集または削除できます。
- カスタム チェックを編集するには、管理者から許可を得る必要がある場合があります。

チェックの例外を作成する

必要に応じて、デプロイメント内でチェックが適用される場所を制限できます。

STEP 1 | **[Manage (管理)] > [Security Posture (セキュリティ体制)] > [Settings (設定)] > [Security Check Exceptions (セキュリティチェックの例外)]** を選択し、 **[Create Security Check Exception (セキュリティ チェック例外の作成)]** を選択します。

または、**[Manage (管理)] > [Security Posture (セキュリティ体制)] > [Settings (設定)]**を選択し、除外するチェックを特定して選択します **([例外]** 列)。

STEP 2 | チェックの 例外ルールを作成する ために必要な情報を指定します。例外の名前、理由、条件を指定します。

セキュリティ チェック例外 機能は現在、アラート、 ベストプラクティス 、 セキュリティ体制インサイトのダッシュボードにのみ適用されます。

STEP 3 | 任意 例外の意図と履歴を他の人が理解できるように、例外の チケット番号 または 説明 を追加します。

STEP 4 | 例外を保存します 。

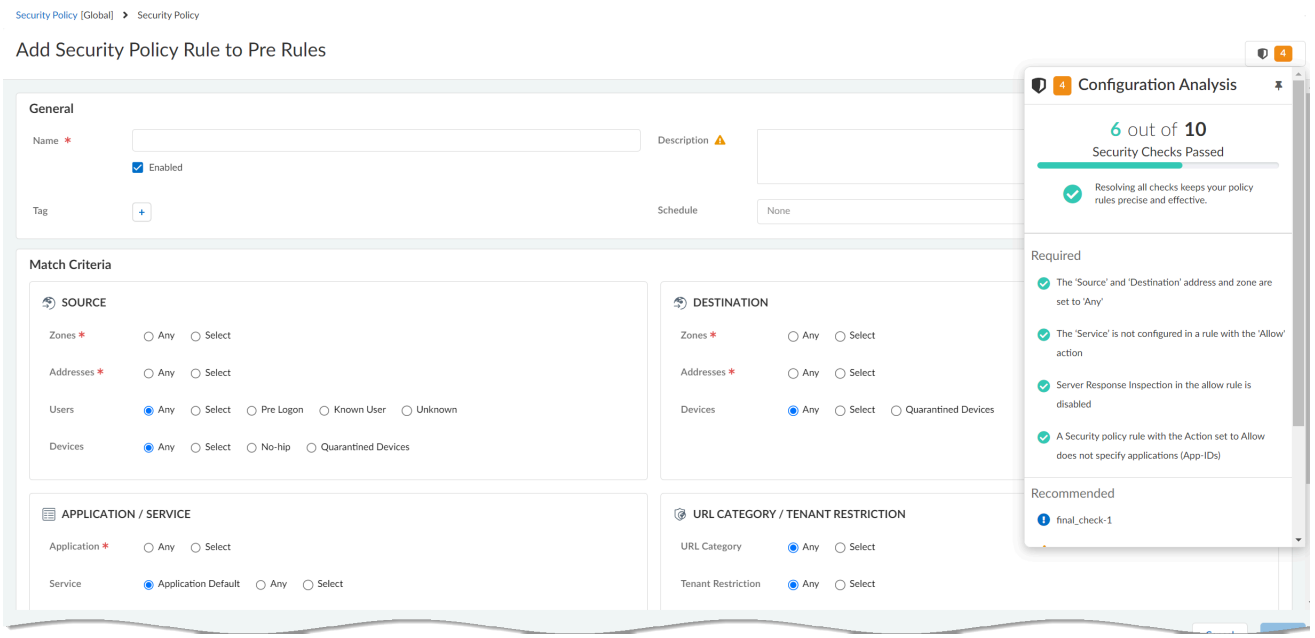
職場でのチェック

フィールド レベルのチェックでは、構成がベストプラクティスまたはカスタム チェックと一致していない場所が表示されます。チェックではベストプラクティス ガイダンスがインラインで提供されるため、すぐに対処できます。

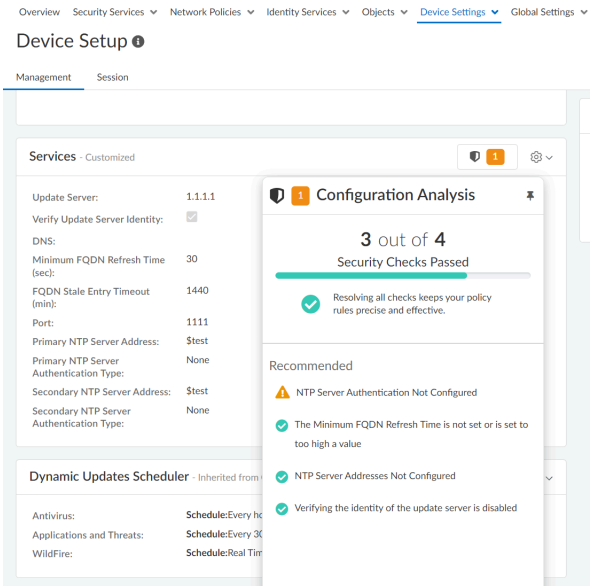
また、セキュリティ チェックをどこにいても表示および管理することもできます。

- ポリシー ルールの作成と管理 – セキュリティ ポリシー ルールを使用すると、ルールを適用してアクションを実行できます。ルールは、必要に応じて一般化または特定化できま

す。([**Manage** (管理)] > [**Configuration** (設定)] > [**NGFW**と**Prisma Access**] > [**Security Services** (セキュリティサービス)] > [**Security Policy** (セキュリティ ポリシー)])



- [Setup Devices (デバイスのセットアップ)]- ファイアウォールの管理インターフェイスと補助インターフェイスのサービス ルート、接続設定、許可されたサービス、および管理アクセス設定を構成します。(**Manage** (管理) > **Configuration** (設定) > **NGFW**と**Prisma Access** > **Device Settings** (デバイス設定) > **Device Setup** (デバイスのセットアップ))



保存しようとしている設定が合格基準を満たしていない場合は、問題を修正するか、警告をオーバーライド*して変更を保存するかを選択できます。

- * オーバーライド権限はロールベースのアクセス制御 *(RBAC)* によって管理されており、このオプションを表示するにはロールに対して有効にする必要があります。オーバーライド、カスタム チェック、例外に関するアクションは、監査ログに記録されます。***Incidents and Alerts (***インシデントおよびアラート***)Log Viewer (***ログ ビューア***)Audit (log type))***監査 *(*ログ タイプ*)_*。
- カスタム チェック、オーバーライド、例外で行ったすべての操作は、監査に記録されます。***[Incidents and Alerts (***インシデントおよびアラート***)] > [Log Viewer (***ログ ビューア***)] > [Audit (log type) (***監査 *(*ログ タイプ*))]*。

管理:アクセス制御

どこで使用できますか?	何が必要ですか?
• Prisma Access （*Strata Cloud Manager*または*Panorama*の設定管理付き） • Software NGFW Creditsによって資金提供されたものを含むNGFW	❑ Strata Cloud Managerで設定を管理し、NGFWとPrisma Accessを統合管理するには、次のライセンスの両方が必要です。 ❑ Prisma Access[ライセンス] ❑ AIOps for NGFW Premium license (use the Strata Cloud Manager app) ❑ Strata Cloud Manager Pro ❑ Software NGFW Credits (ソフトウェアNGFWクレジット) *(VM-Series software NGFW用)* → どのライセンスを使用しているかによって、Strata Cloud Managerで利用できる機能や性能は異なります。

ロールベースのアクセス制御（RBAC）では、管理ユーザー（管理者）の権限およびロールを定義できます。すべての管理者は、ロールと認証方式を指定するユーザーアカウントを持っている必要があります。Prisma Access Cloud Managementは、カスタムRBACを実装しており、ロールまたは特定の権限を管理し、管理ユーザーにアクセス権を割り当てることができます。RBACを使用すると、Cloud Management内でユーザーとさまざまなリソースへのアクセスを管理できます。

*SaaS Security Inline and Behavior Threats*では、*RBAC*はサポートされていません。***[Discovered Apps (検出されたアプリ)]***と***[Behavior Threats (振る舞いの脅威)]***のすべてのタブは、割り当てられたロールに関係なく、すべてのユーザーに表示されます。

その他の***RBAC***リソース

- Common Servicesを使用できるユーザー:ID&アクセス:クラウド管理対象Prisma Access
- Common Services の一般的なフローとは何ですか。ID&アクセス
- Common Servicesによるロールと権限について

管理者ロール

Prisma Accessのユーザーとは、管理権限を割り当てられた人々のことであり、ロールはサービスで管理者が保有しているアクセス権のタイプを定義しています。ロールを割り当てる場合、アクセス許可グループと管理者が管理できるアカウントグループを指定します。ハブには、Prisma Accessを利用する管理者向けに以下の権限グループが用意されています。

- アプリ管理者：指定されたアプリにフルアクセスでき、今後アプリに追加されるすべてのインスタンスも含みます。アプリケーション管理者は、アプリケーションインスタンスに対してロールを割り当てたり、そのアプリケーションに固有のアプリケーションインスタンスをアクティブ化したりすることができます。
- インスタンス管理者：このロールが割り当てられたアプリケーションインスタンスにフルアクセスします。インスタンス管理者は、他のユーザーを、アプリケーションインスタンスのインスタンス管理者にすることもできます。アプリケーションに事前定義済みまたはカスタムロールがある場合、インスタンス管理者はそれらのロールを他のユーザーに割り当てることができます。
- スーパーリーダー：すべての構成要素、ログ、および設定を表示できます。スーパーリーダーは他の設定を変更できません。
- 監査管理者：ログとログ設定のみを表示および管理することができます。監査管理者は他の設定を変更することはできません。
- 暗号管理者：ログの表示、IKE、IPSec、マスターキー管理、証明書設定などの暗号設定の管理が可能です。暗号管理者は、他の設定を表示したり変更したりすることはできません。
- セキュリティ管理者：ログを表示し、暗号管理者ロールで使用できる暗号設定以外のすべての設定を管理できます。
- **Web**セキュリティ管理者：Webセキュリティに関連する構成要素のみを表示できます。
- 情報漏えい対策管理者：エンタープライズDLP設定にはアクセスできますが、設定変更をPrisma Accessにプッシュすることはできません。
- データセキュリティ管理者：エンタープライズDLPおよびSaaSセキュリティコントロールにアクセスできますが、構成の変更をPrisma Accessにプッシュすることはできません。
- **SaaS**管理者:SaaSのセキュリティ設定にはアクセスできますが、設定変更をPrisma Accessにプッシュすることはできません。

カスタムロールベースのアクセス制御：セットアップ

ここでは、事前定義されたロールを使用する方法やカスタムロールを作成する方法、ロールをユーザーに割り当てる方法、Prisma Accessアプリケーションにアクセスする際のユーザースコープを管理する方法について説明します。

STEP 1 | Common Servicesによるカスタムロールの追加

事前定義済みロールよりも細かいアクセス制御が必要な場合は、カスタムロールを追加して、ユーザーに適用する権限を定義できます。カスタムロールは、事前定義されたロールと同様に、アクセス権とアクセス権セットのセットです。事前定義されたロールとは異なり、各カスタム ロールは、定義されているTSG(テナント サービス グループ)の下の階層のユーザーのみに割り当てることができます。これにより、異なる顧客によって定義された、類似した名前のカスタムロール間での名前の競合を回避できます。

階層の最上位レベル(親レベル)にカスタムロールを追加すると、そのロールが下位にネストされたテナントに割り当てられるため、親テナントが子テナントを管理できます。

STEP 2 | Common Servicesによるユーザーアクセスの追加

Common Services：Access and Identityを使用すると、作成したテナントだけでなく、プラットフォームへのユーザーアクセスを追加できます。

STEP 3 | Common Services によるテナント ユーザまたはサービス アカウントへの定義済みのロールの割り当て

すでにユーザを追加していて、さらにロールを追加する場合は、事前定義されたロールをバッチで割り当てることもできます。ロールと権限の追加情報を確認します。

STEP 4 | 新しいスコープを作成する： Prisma Access クラウド管理ID

Prisma Access Cloud Managementを使用すると、（管理者として）管理スコープをクラウド管理ユーザー（管理者以外）に割り当て、フォルダーやスニペットなどのスコープに基づいて権限を関連付けることができます。

パーミッションは、システムで許可されているアクションです。アクセス権は、システム内のオブジェクトの読み取り、書き込み、および削除に使用するアプリケーションプログラミングインターフェイス（API）呼び出しの特定のセットを表します。すべての権限はロールにグループ化されます。

管理:スコープ管理

どこで使用できますか?	何が必要ですか?
• Prisma Access （*Strata Cloud Manager*または*Panorama*の設定管理付き） • Software NGFW Creditsによって資金提供されたものを含むNGFW	❑ Strata Cloud Managerで設定を管理し、NGFWとPrisma Accessを統合管理するには、次のライセンスの両方が必要です。 ❑ Prisma Access[license (ライセンス)] ❑ AIOps for NGFW Premium license (use the Strata Cloud Manager app) ❑ Strata Cloud Manager Pro → どのライセンスを使用しているかによって、Strata Cloud Managerで利用できる機能や性能は異なります。

スコープ管理を設定して、カスタムロールベースのアクセス制御を適用します。これにより、特定のフォルダ、ファイアウォール、Prisma Accessのデプロイメント、スニペット構成にアクセスおよび変更できるStrata Cloud Manager管理者を指定できます。クラウド管理者にスコープ管理を定義することで、過剰なプロビジョニングが行われないようにし、選択したフォルダー、ファイアウォール、Prisma Accessデプロイメント、スニペット構成の読み取りおよび書き込みアクセス権限を定義します。Common Services Multiple Platform Roles and Enterprise Roles (共通サービス複数のプラットフォーム ロールとエンタープライズ ロール)は、Strata Cloud Manager管理者の読み取りおよび書き込みアクセス権限を定義するために使用されます。

スコープ管理構成は、Strata Cloud Managerテナント全体に定義されます。スコープ管理は、特定のフォルダ、Prisma Access、ファイアウォールの[Configuration Scope (設定スコープ)]に対して定義することはできません。

スコープオブジェクトを作成できるのは、クラウド管理管理者またはスーパーユーザーのみです。スコープ管理ウィジェットは、他のロールを持つユーザーは利用できません。

STEP 1 | Strata Cloud Managerにログインします。

STEP 2 | **[Manage (管理)]** > **[Access Control (アクセス制御)]** > **[Scope Management (スコープ管理)]**を選択します。

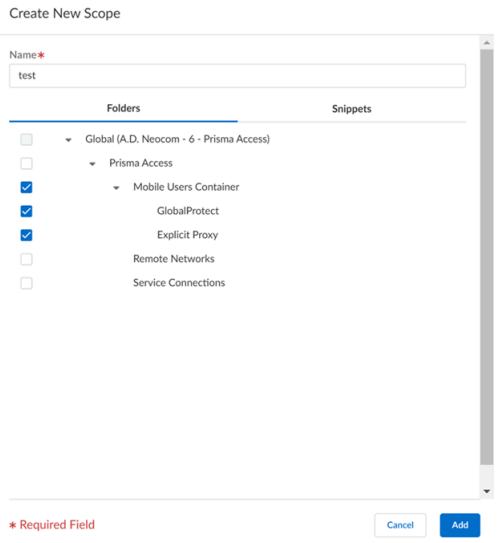
STEP 3 | 新しいスコープを作成します。

STEP 4 | スコープ管理の構成を定義します。

スコープ管理の設定は、スコープオブジェクトとしてラベル付けされます。

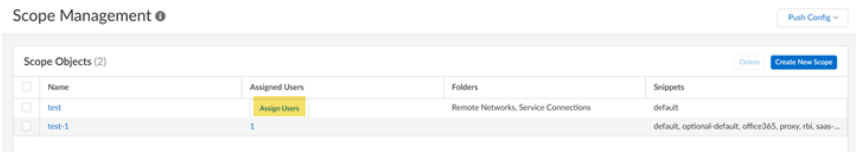
1. 分かりやすい **Name**（名前）を入力します。
2. **[Folders (フォルダ)]**を選択し、スコープに含めるフォルダ、ファイアウォール、およびPrisma Accessデプロイメントにチェック(有効化)します。

   ファイアウォールを選択すると、選択したファイアウォールが関連付けられているフォルダもスコープ管理設定に含まれます。親フォルダではなく、すぐに関連付けられたフォルダのみが対象となります。
3. ［**Snippets (スニペット)**］を選択し、含めるスニペットにチェック（有効）を入れます。
4. scopeオブジェクトを追加します。



STEP 5 | スコープ管理設定をStrata Cloud Manager管理者に適用します。

1. 前の手順で作成したスコープオブジェクトにユーザーを割り当てます。



2. Strata Cloud Manager管理者のロールを選択します。たとえば、すべてのテナントのすべての機能にアクセスする必要があるユーザーに対して、MSPスーパーユーザーを選択できます。

   デフォルト設定は `None`（なし）です。使用可能な各ロールの読み取りおよび書き込みアクセス権限の詳細については、「Common Services Multiple Platform and Enterprise

Roles (共通サービス 複数のプラットフォームとエンタープライズのロール)」を参照してください。

> 現在割り当てられている *Common Services* ロールを削除するには、特定の *Strata Cloud Manager*管理者および***Clear Role(***ロールをクリア***)***を選択します。これにより、デフォルトの*[None (なし)]*ロールが管理者に適用されます。

3. 既存のスコープを変更して名前を編集し、フォルダを追加または削除するには、スコープオブジェクトを選択し、必要に応じてスコープを変更して、スコープを更新します。
4. 割り当てられたユーザを変更するには、ユーザを追加またはユーザを変更するには、**[Assigned Users (**割り当てユーザー**)]**をクリックして必要に応じて変更し、ウィンドウを閉じます。

管理:IP の制限

どこで使用できますか?	何が必要ですか?
• Prisma Access （*Strata Cloud Manager*または*Panorama*の設定管理付き） • Software NGFW Creditsによって資金提供されたものを含むNGFW	❑ Strata Cloud Managerで設定を管理し、NGFWとPrisma Accessを統合管理するには、次のライセンスの両方が必要です。 ❑ Prisma Access[ライセンス] ❑ AIOps for NGFW Premium license (use the Strata Cloud Manager app) ❑ Strata Cloud Manager Pro → どのライセンスを使用しているかによって、Strata Cloud Managerで利用できる機能や性能は異なります。

Prisma Accessクラウド管理管理者の信頼できるIPアドレスを指定します。Prisma Accessクラウド管理にアクセスできるのは、これらの送信元IPアドレスからログインした管理者（および認証に成功した管理者）のみです。

IPアドレスはパブリックアドレスである必要があります。デフォルトでは、信頼されたアドレスは強制されません（リストは任意に設定されています）。

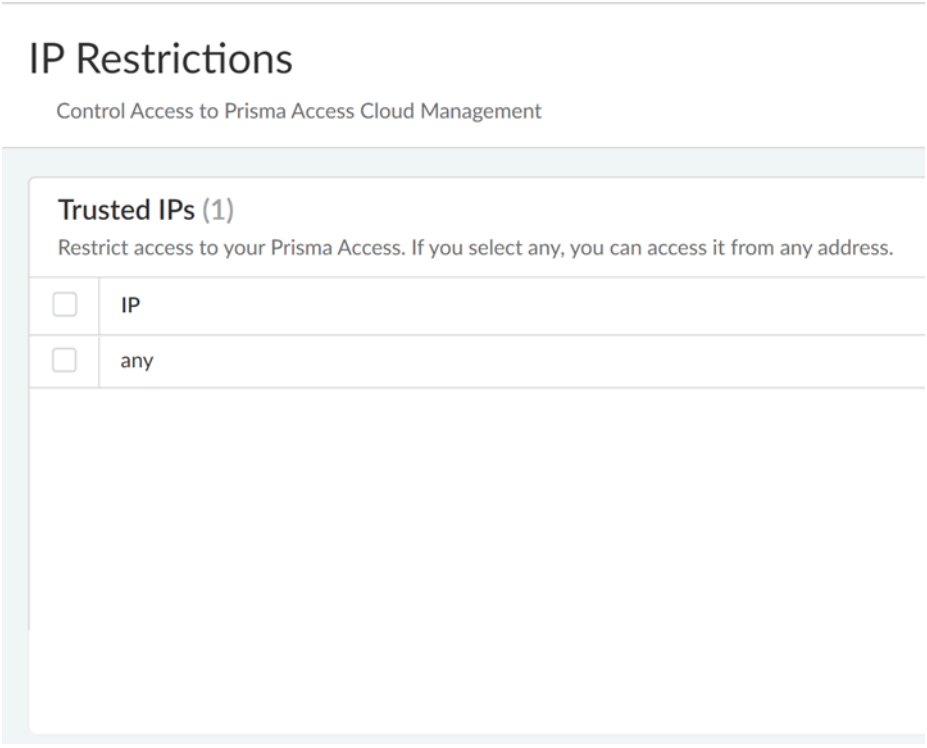
まず、 **[Manage (管理)]** > **[Access Control (アクセス制御)]** > **[IP Restrictions (IP制限)]**をご覧ください。

IP制限の場合、サブネットアドレスはサポートされません。IPアドレスとIPアドレスの範囲のみがサポートされています。次の IP アドレスおよびサブネットと重複するサブネットは指定しないでください。Prisma Accessはこれらの IP アドレスおよびサブネットを内部使用のために予約します。

- 169.254.169.253および169.254.169.254
- 100.64.0.0/10
- 169.254.201.0/24
- 169.254.202.0/24

RFC 1918 準拠および RFC 6598 準拠の IP アドレス プールを使用することを

推奨します。RFC 1918非準拠およびRFC 6598準拠の（パブリック）IPアドレスの使用はサポートされていますが、インターネットのパブリックIPアドレス空間と競合する可能性があるため、お勧めできません。



ワークフロー:ログ - Strata Cloud Manager

どこで使用できますか?	何が必要ですか?
• Prisma Access (Managed by Strata Cloud Manager) • NGFW (Managed by Strata Cloud Manager) • Prisma SD-WAN	ワークフローに応じて、これらのライセンスの1つ以上: ❑ AIOps for NGFW Premiumライセンス ❑ Strata Logging Service ライセンスが必要です ❑ Prisma Accessライセンス ❑ Prisma SD-WAN ❑ リモートブラウザ分離ライセンス

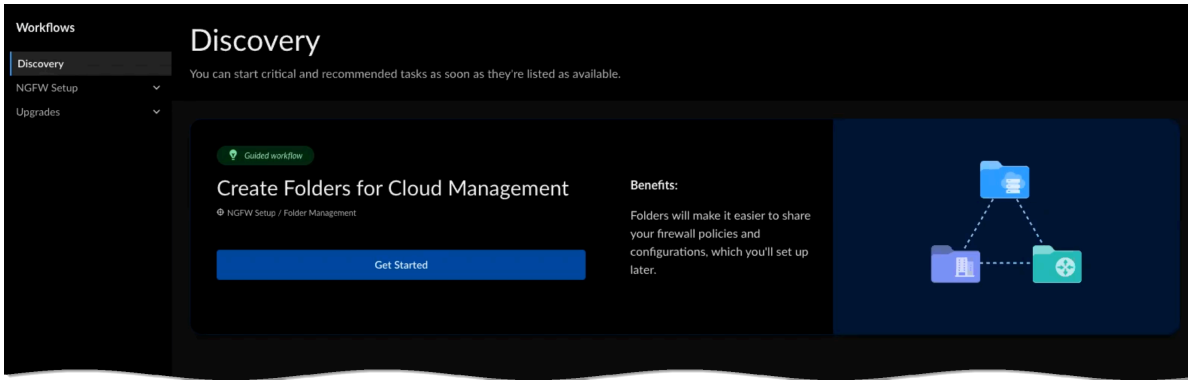
最初にワークフローに移動すると、セキュリティ体制の改善や設定管理の最適化のために実行できる重要な推奨アクションが、**[Discovery (検出)]**ダッシュボードに表示されます。これらのアクションが利用可能になると、すぐに表示されます。引き続き、NGFWとPrisma Accessのモバイルユーザーとリモートネットワークのセットアップとオンボードを行い、NGFWのソフトウェアアップグレードを計画します。

- オンボーディング タスクの検出
- セットアップ Prisma Access
- NGFWのセットアップ
- セットアップ Prisma SD-WAN
- ソフトウェアのアップグレード(NGFW)
- ソフトウェアのアップグレード(Prisma Access)

ワークフロー:Discovery（検出）

どこで使用できますか?	何が必要ですか?
• Prisma Access (Managed by Strata Cloud Manager) • NGFW (Managed by Strata Cloud Manager) • Prisma SD-WAN	❑ AIOps for NGFW Premiumライセンスまたはは Prisma Accessライセンス

検出では、重要なタスクや推奨タスクが利用可能になり次第、開始します。ガイド付きのワークフローや、自分で完了できるタスクがあるかもしれません。このトピックでは、ガイド付きワークフローを使用してフォルダ構造を作成し、デバイスに簡単に直感的に割り当てる方法を説明します。



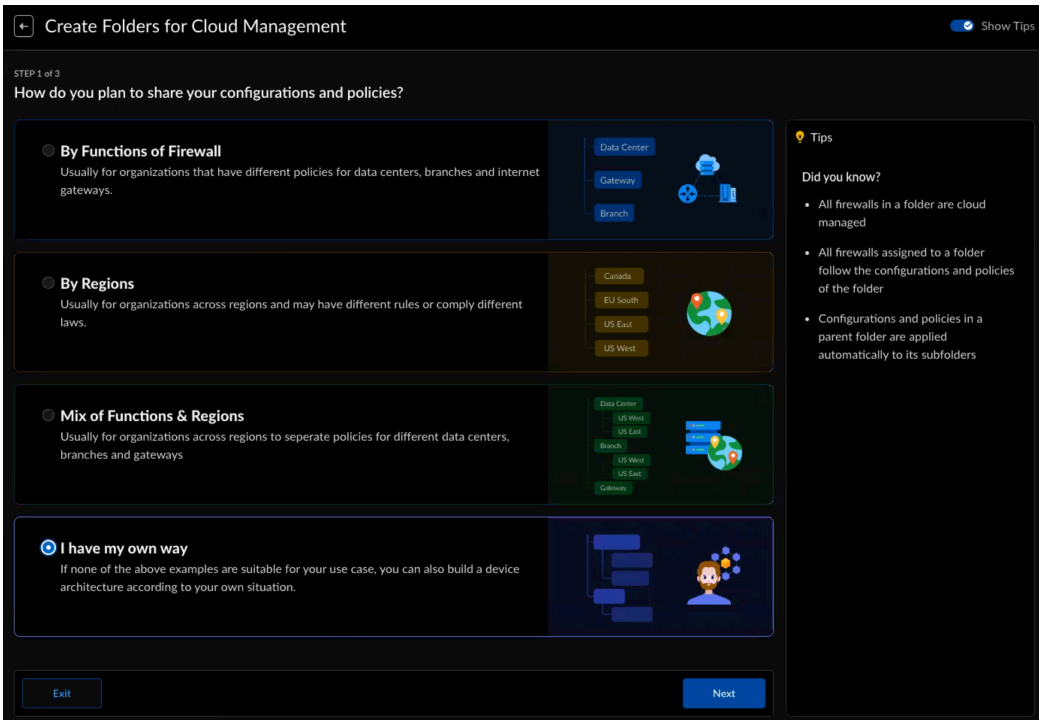
ファイアウォール用のフォルダを作成する手順は、次のとおりです。

STEP 1 | **[Workflows (ワークフロー)]** > **[Discovery (検出)]**に移動し、**[Get Started (開始)]**を選択します。

STEP 2 | ポリシー ルールと設定を共有する方法を選択します。

- ファイアウォールの機能別 – データセンター、ブランチオフィス、インターネットゲートウェイについて、組織ごとに異なるポリシーがありますか?このような選択肢もあるかもしれません。
- 地域別 – 組織が異なる規則を持つ地域または異なる法律を遵守する地域にまたがっていますか?このオプションを検討してください。
- 機能と地域の混在 – 地域をまたがる組織では、データセンター、支店、インターネットゲートウェイごとにポリシーを分ける必要がありますか?このオプションを試してみてください。
- 独自の方法 – 上記の例のいずれもユースケースに適さない場合は、状況に応じてデバイスアーキテクチャを構築することもできます。

この例では、「**I have my own way (独自の方法)**」オプションを選択します。

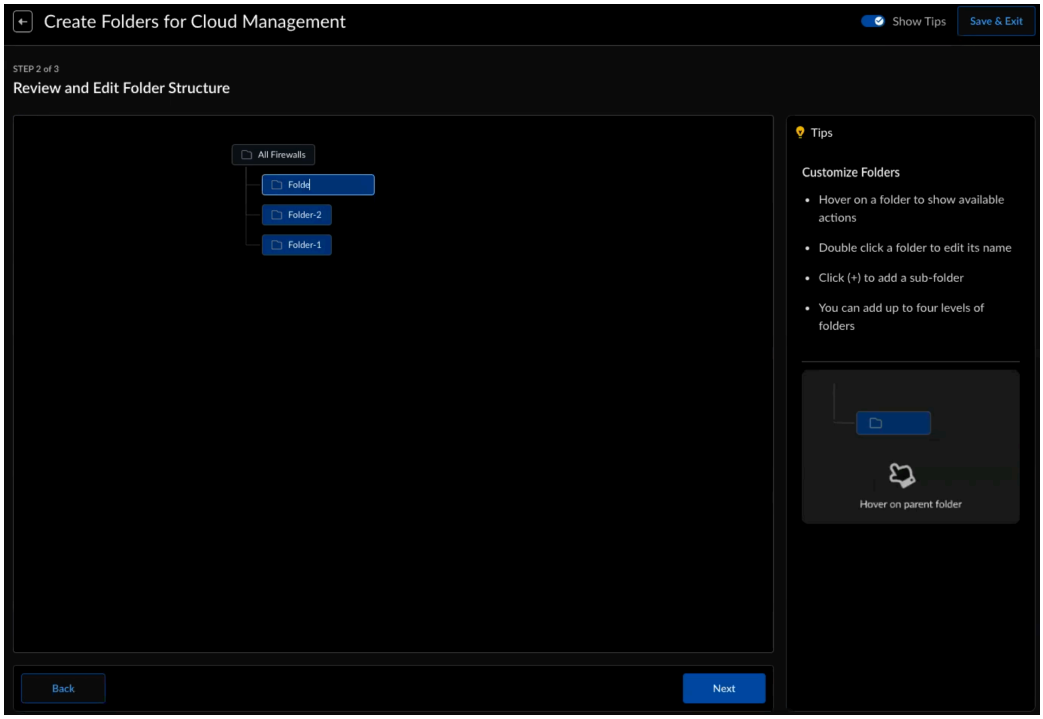


ヒントを表示をオンにすると、情報に基づいた意思決定に役立つヘルプヒントが表示されます。

STEP 3 | [次へ]を選択してフォルダ構造を構築します。

STEP 4 | 以下のアクションを使用して、手順1で選択したテンプレートに基づいてフォルダ構造を構築します。次の作業を行えます。

- 新しいフォルダの追加 – フォルダにカーソルを合わせると、新しいフォルダを追加するオプションが表示されます。をクリックし、新しいフォルダに名前を付けます。
- フォルダの削除 – フォルダにカーソルを合わせると、フォルダを削除するオプションが表示されます。を選択してフォルダを削除します。
- フォルダ名の変更 – フォルダをダブルクリックすると、フォルダの新しい名前を入力します。Enterキーを押すか、テキストフィールドの外側をクリックして新しい名前を有効にします。
- 子を持つフォルダノードを展開または折りたたむ **(Expand or Collapse)**ことを実施します。

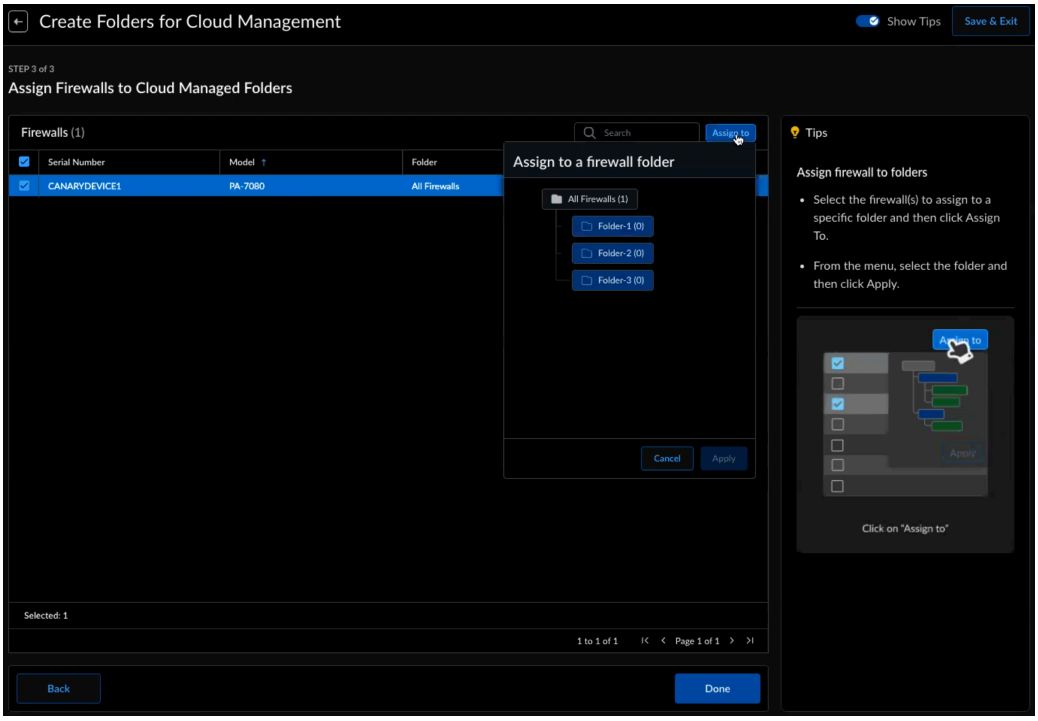


- フォルダツリーは、最大4つのレベルを持つことができます。
- トップレベルのフォルダは削除も名前の変更もできません。
- 特定のフォルダアクションに関するヒントについては、「ヒント」を確認してください。
- 作業内容を保存します。いつでも終了して、後で戻ってきてください。

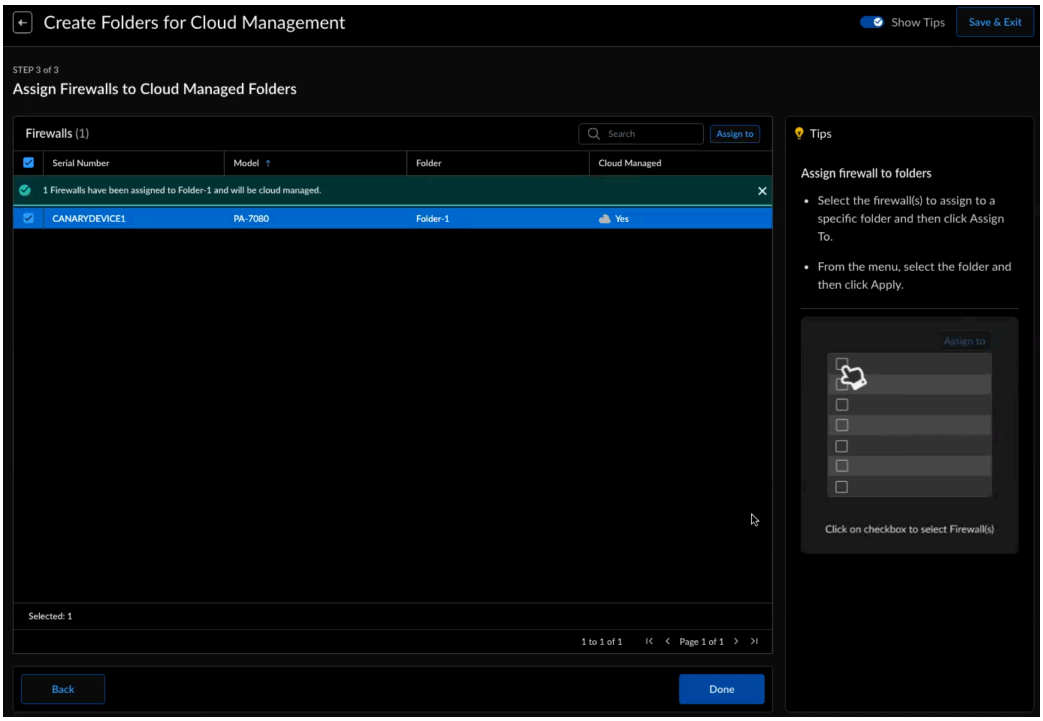
STEP 5 | [次へ]を選択し、ファイアウォールをフォルダに割り当てます。

STEP 6 | このリストから1つ以上のファイアウォールを選択します。

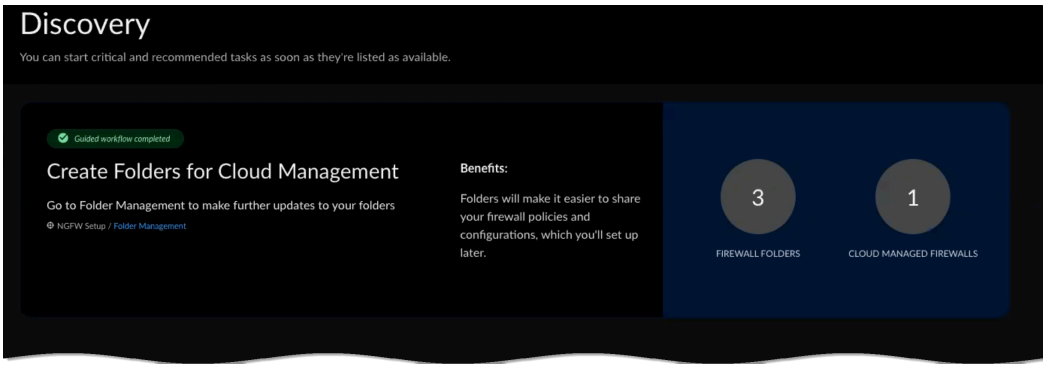
STEP 7 | **[Assign To (割り当て先)]**を選択し、ファイアウォールを割り当てるフォルダを選択して、**[Apply (適用)]**を選択します。クラウド管理は、クラウド管理フォルダーに割り当てたファイアウォールに対して有効になります。

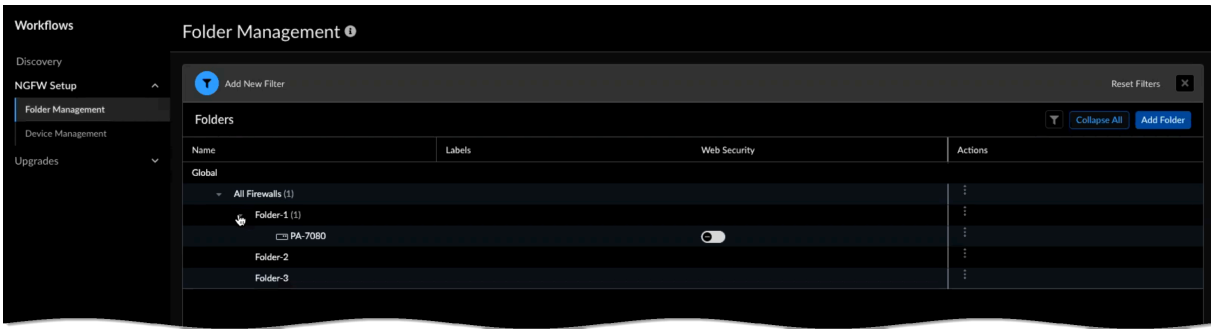


STEP 8 | 割り当てを確認し、完了を選択します。



作成したフォルダと割り当てたファイアウォールは、**[Discovery (検出)]**のメインページと**[NGFW Setup (NGFWセットアップ)]** > **[Folder Management (フォルダ管理)]**タブに表示されます。





ワークフロー:NGFW のセットアップ

どこで使用できますか?	何が必要ですか?
• NGFW (Managed by Strata Cloud Manager)	❑ NGFWのクラウド管理にはAIOps for NGFW Premiumライセンスが必要 ❑ ロギングにはStrata Logging Serviceライセンスが必要です ❑ Prisma Accessライセンスをお持ちの場合は、**[Folder Management (フォルダ管理)]**を使用して事前定義済みフォルダを表示し、フォルダのWeb Security (ウェブセキュリティ)を有効にすることができます

クラウド管理用のNGFWのセットアップの一環として、次世代ファイアウォールをStrata Cloud Managerにオンボードする必要があります。オンボーディングには、同様の設定が必要なファイアウォールをグループ化するためのフォルダのセットアップが含まれます。ワークフロー:フォルダ管理についてさらに詳しく知りたい場合は、[デバイス管理]ページを使用して、フォルダ階層内のすべてのデバイスの詳細を表示します。

STEP 1 | Strata Logging ServiceとAIOps for NGFW Premiumのライセンスをアクティベートする。

ロギングにはStrata Logging Serviceライセンス、NGFWのクラウド管理にはAIOps for NGFW Premiumライセンスが必要です。

STEP 2 | フォルダを1つ以上作成します。

フォルダは、ファイアウォールまたはデプロイメントタイプを論理的にグループ化し、設定管理を簡素化するために使用されます。

STEP 3 | Strata Cloud Managerにファイアウォールを導入します。

ファイアウォールをStrata Cloud Managerにオンボードするには、ファイアウォールのローカルPanorama設定を構成し、ファイアウォールをお使いのStrata Cloud Managerテナントに関連付ける必要があります。オンボード後は、ファイアウォールの一般設定とセッション設定を続けることができます。

STEP 4 | （HA のみ）必要に応じて、管理対象ファイアウォールを高可用性（HA）構成に設定します。

STEP 5 | スニペットを作成します。

スニペットは、フォルダ、デプロイメント、または個々のファイアウォールに適用される設定オブジェクトをグループ化するために使用します。これにより、迅速に適用およびプッシュできる共通の基本設定を標準化できるため、オンボーディング プロセスが簡素化および迅速化されます。

STEP 6 | 設定オブジェクトを作成します。

設定オブジェクトは、ネットワークおよびポリシー ルール設定の設定ブロックです。

STEP 7 | ネットワークおよびポリシー ルールの設定を作成および設定します。

STEP 8 | Strata Cloud Managerからマネージドファイアウォールへの[Push configuration changes (プッシュ設定変更)]

ワークフロー:デバイス管理

どこで使用できますか?	何が必要ですか?
• NGFW (Managed by Strata Cloud Manager)	☐ AIOps for NGFW Premium

Strata Cloud Managerが管理するPalo Alto NetworksのNGFWを*Cloud Managed Device* (クラウド管理対象デバイス)と呼びます。Strata Cloud Managerは、PAN-OS 10.2.3以降が稼働するファイアウォールを管理できます。

Strata Cloud Managerの前提条件の詳細については、こちらをクリックしてください。

[Device Management (デバイス管理)]ダッシュボード **([Workflows (ワークフロー)] > [NGFW Setup (NGFWセットアップ)] > [Device Management (デバイス管理)])** を使用すると、すべての管理対象デバイスに関する重要なデバイスとバージョンの詳細を確認し、クラウド管理に移行するデバイスを選択できます。

すべてのクラウドマネージドNGFWの詳細を見る

［**Cloud Managed Devices (クラウド管理対象デバイス)**］タブ （**Workflows (ワークフロー) > NGFW Setup (NGFWセットアップ) > Device Management (デバイス管理) > Cloud Managed Devices (クラウド管理対象デバイス)**） には、すべてのSCMオンボード ファイアウォール、それらに割り当てられているフォルダー、およびそれらに関する重要な詳細が表示されます。

デバイス情報	詳説
氏名	NGFWの名前と、その下に編成されているフォルダ。
ラベル	NGFWに添付されているラベル。
設定同期ステータス	NGFWの同期ステータスは、次の状態です： • 同期されている • 同期されていない
HA 状態	オンボードNGFWのHAステータス： • **Active** [アクティブ] - 正常なトラフィック処理状態 • **Passive** [パッシブ] - 正常なバックアップ状態

デバイス情報	詳説
	• **Initiating** [始動中] - ファイアウォールの起動後最大60秒はこの状態におかれます • **Non-functional** [機能停止中] - エラー状態 • **Suspended** [保留中] - 管理者がファイアウォールをサスペンドしていることを示します • **Tentative** [一時的な状態] - アクティブ/アクティブ環境におけるリンクまたはパスのモニタリングイベント用
シリアルナンバー	オンボードNGFWのシリアルナンバー。
model	オンボードNGFWのモデル番号。
タイプ	彼らは、オンボードNGFWをタイプします。 • VM • PA
アドレス	オンボードNGFWのIPアドレス。
ライセンス	オンボードNGFWのライセンス情報 • 一致 • 不一致
ソフトウェアのバージョン | アプリケーションと脅威 | アンチウイルス | URLフィルタリング	ファイアウォールに現在インストールされているソフトウェアとコンテンツのバージョンが表示されます。詳細は、「ファイアウォールのソフトウェアとコンテンツの更新」を参照してください。
デバイス ディクショナリー	ファイアウォールがインポートするためのファイル。ディクショナリ ファイルは、推奨されるセキュリティ ポリシー ルールをインポートする際に選択するためのデバイス属性のリストをStrata Cloud Managerおよびファイアウォール管理者に提供します。
アクション	オンボード ファイアウォールのアクション: • ライセンス情報の取得 • 再起動 • ルーティングモードの変更 • ローカル設定管理 • 強制ブートストラップ

NGFWをクラウド管理対象デバイスから削除する

［**Available Devices** (利用可能デバイス)］タブには、すでにStrata Cloud Managerで管理されているSCMおよびNGFWにオンボード可能なNGFWがすべて表示されます。

*Strata Cloud Manager*のオンボーディングプロセスの詳細については、こちらをクリックしてください。

[使用可能なデバイス]タブを使用して、デバイスをStrata Cloud Managerに出し入れできます。

STEP 1 | Strata Cloud Managerにログインします。

STEP 2 | **[Workflows(ワークフロー)]** > **[NGFW Setup(NGFWセットアップ)]** > **[Device Management (デバイス管理)** > **Available Devices (利用可能なデバイス)]**を選択します。

1. ファイアウォールをStrata Cloud Manager外に移動するには、**[Back to Available Devices (利用可能なデバイスに戻る)]**を選択します。

ファイアウォールでのローカル設定バージョンのスナップショットの復元

任意のバージョンを復元し、XML形式で設定の詳細をダウンロードすることができます。

STEP 1 | Strata Cloud Managerにログインします。

STEP 2 | **[Workflows (ワークフロー)]** > **[NGFW Setup (NGFWセットアップ)]** > **[Device Management (デバイス管理)]**を選択し、**[Actions (アクション)]**から**[Local Configuration Management (ローカル設定管理)]**を選択します。

STEP 3 | バージョンをロードして、ローカル設定を復元します。

STEP 4 | ファイアウォールのローカル設定を設定バージョンに置き換えるには、[はい] をクリックします。新しいコミットジョブが作成されます。

[Jobs (ジョブ)]ビューを使用すれば、失敗した操作についてトラブルシューティングを行ったり、完了したコミットに関する警告について調査を行ったり、保留中のコミットをキャンセルしたりすることができます。

STEP 5 | 選択したバージョンの設定詳細の表示をダウンロードします。

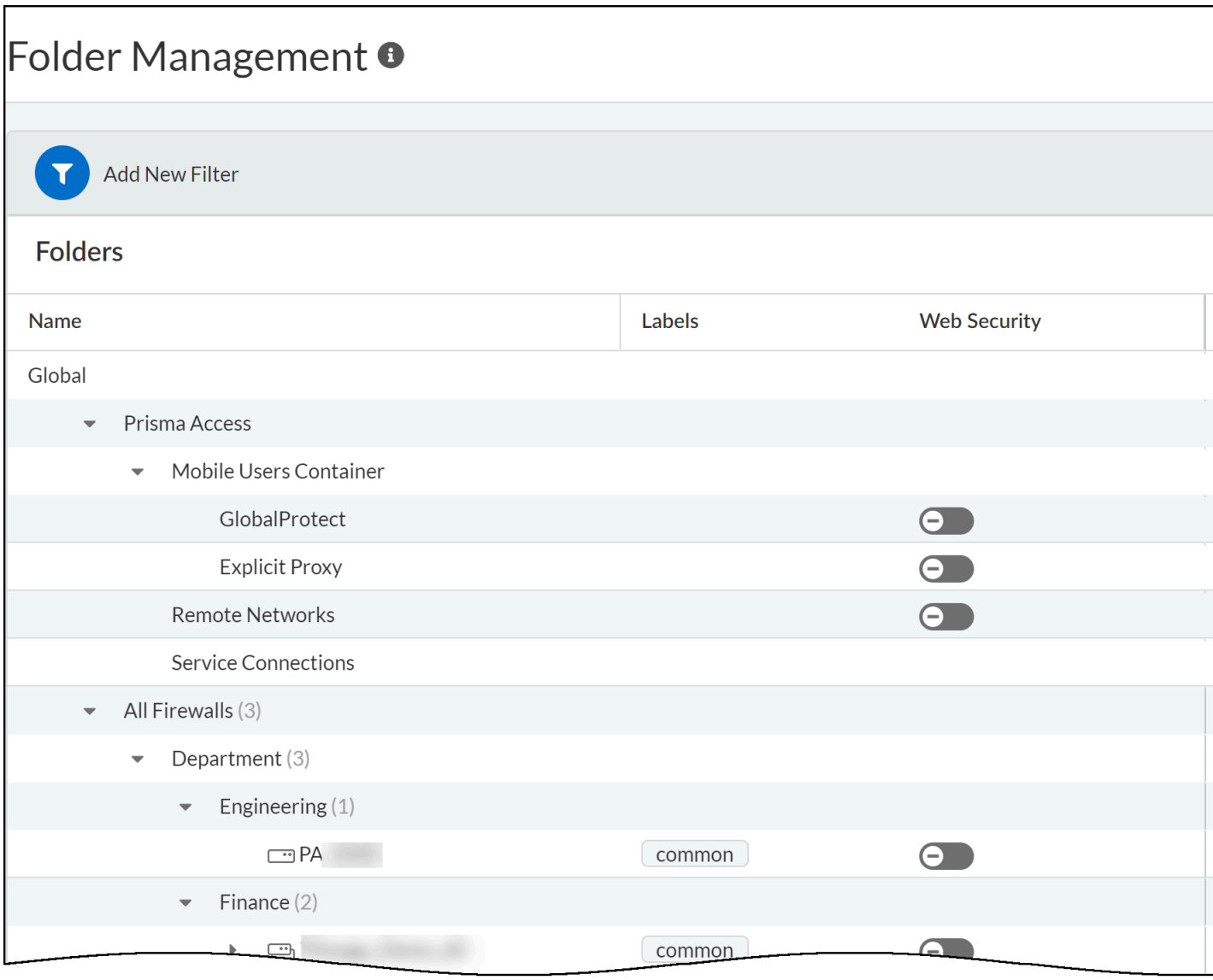
ワークフロー:フォルダ管理

どこで使用できますか?	何が必要ですか?
• Prisma Access (Managed by Strata Cloud Manager) • NGFW (Managed by Strata Cloud Manager)	☐ AIOps for NGFW Premiumライセンス ☐ Prisma Accessライセンス

フォルダは、ファイアウォールまたはデプロイメントタイプ(Prisma Accessモバイルユーザー、リモートネットワーク、またはサービス接続)を論理的にグループ化して、設定管理を簡素化するために使用されます。複数のネストされたフォルダを含むフォルダを作成して、同様の設定を

必要とするファイアウォールとデプロイメントをグループ化できます。すでにネストされているフォルダには、複数のネストされたフォルダを含めることもできます。

Prisma AccessとNGFWのフォルダは別々です。Prisma Accessデプロイメントのあるフォルダには NGFWをグループ化することはできません。しかし、共有設定をすべてのフォルダに対してグローバルに簡単に適用したり、管理:スニペットを使用して標準設定やポリシー要件を複数のフォルダに対して簡単に適用したりできます。



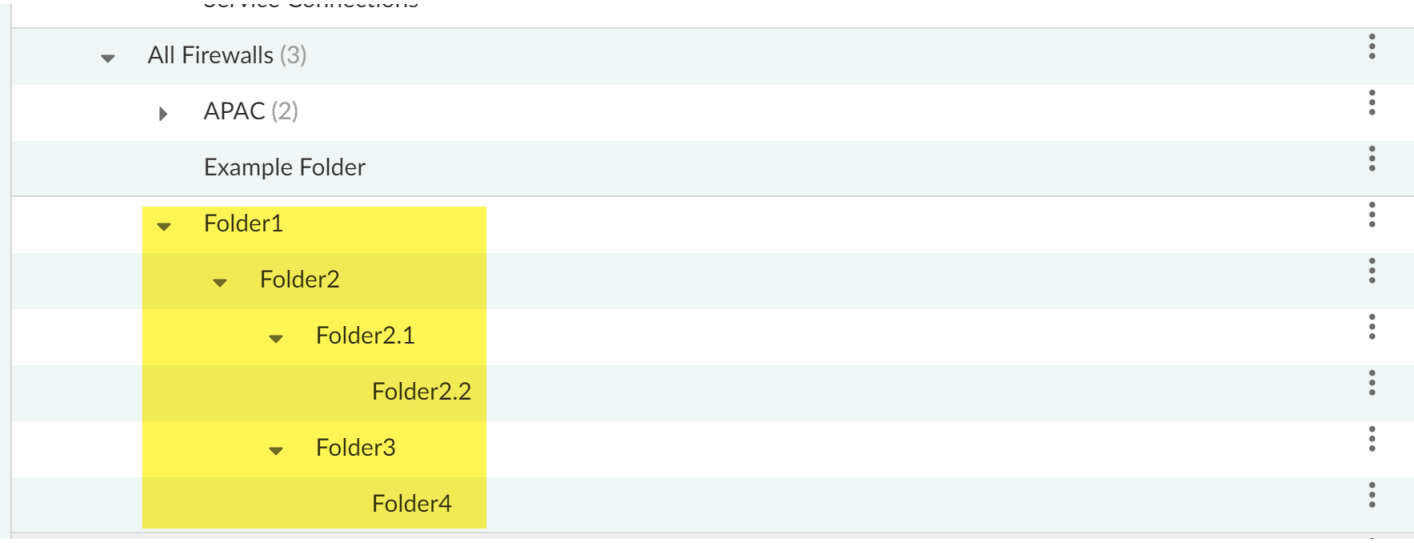
- NGFW
- Prisma Access

フォルダ管理(NGFW)

フォルダとファイアウォールの管理に役立つように、ラベルを適用して特定のファイアウォールのグループをフィルタリングし、設定変更の対象にすることができます。さらに、各フォルダには、現在インストールされているソフトウェアバージョン、動的コンテンツのリリースバージョ

ン、およびフォルダに関連付けられているファイアウォールのGlobalProtectアプリバージョンが表示されます。

ファイアウォールフォルダの場合、任意のフォルダ階層内で最大4Strata Cloud Managerつのネストされたフォルダをサポートします。デフォルトの `[All Firewall (全てのファイアウォール)]` フォルダは常にフォルダ階層の最上位レベルです。たとえば、フォルダ階層を設計するときは、次の点を考慮してください。以下の例では、`Folder1`、`Folder2`、`Folder3`、および`Folder4`が `[All Firewalls (すべてのファイアウォール)]`フォルダーの下にネストされており、この特定のフォルダー階層に他のフォルダーを追加することはできません。さらに、`Folder2.1`と`Folder2.2`は`Folder2`の下にネストされており、他のフォルダーをネストすることもできません。



フォルダーの作成

設定管理を簡素化するために、ファイアウォールを論理的にグループ化するフォルダを作成します。デフォルトの `Firewall (ファイアウォール)` フォルダまたは別の既存のフォルダの下にフォルダを作成できます。

STEP 1 | Strata Cloud Managerにログインします。

STEP 2 | **[Workflows (ワークフロー)]** > **[NGFW Setup (NGFW セットアップ)]** > **[Folder Management (フォルダ管理)]** と**[Add Folder (フォルダの追加)]** を選択します。

STEP 3 | フォルダにわかりやすい名前を付けます。

STEP 4 | （任意）フォルダの**Description**（説明）を入力します。

STEP 5 | （任意）必要に応じて、1つ以上の**Labels (ラベル)**を割り当てます。

既存のラベルを選択するか、作成したいラベルを入力して新しいラベルを作成できます。

STEP 6 | フォルダを作成する場所を指定します。

[All Firewalls(すべてのファイアウォール)]を選択するか、既存のフォルダを選択して、その下にフォルダをネストします。

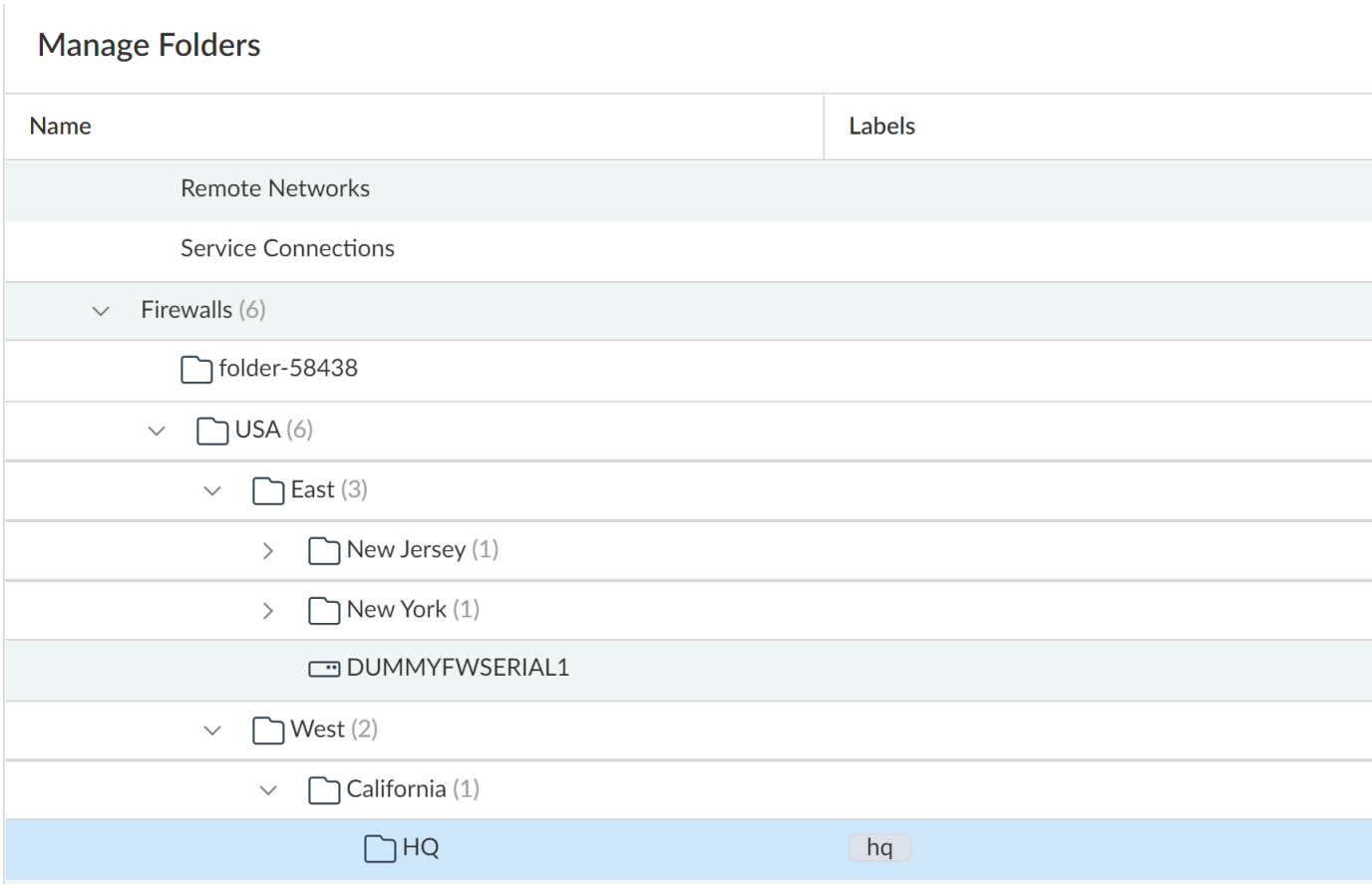
STEP 7 | フォルダを作成します。

フォルダの変更:

既存のフォルダを変更して、名前と説明を編集し、ラベルを追加または変更します。さらに、必要に応じてフォルダを移動または削除できます。

STEP 1 | Strata Cloud Managerにログインします。

STEP 2 | **[Workflows (ワークフロー)] > [NGFW Setup (NGFWセットアップ)] > [Folder Management (フォルダ管理)]** を選択し、[Actions (アクション)] メニューを展開します。



STEP 3 | 必要に応じてフォルダを変更します。

- フォルダを編集する
  1. フォルダ名を編集します。
  2. (任意) フォルダーの説明を編集します。
  3. ラベルを選択または作成します。

     フォルダにまったく異なるラベルを割り当てたり、ラベルを追加したりできます。
  4. **Save**（保存）を選択します。
- フォルダを移動し、宛先を選択します。

フォルダは次の方法で移動できます。

- フォルダを移動して別のフォルダの下にネストできます。
- ファイアウォールフォルダーの下にネストされたフォルダーを移動できます。
- ネストされたフォルダは、あるフォルダから別のフォルダに移動できます。

フォルダの宛先を選択したら、フォルダを移動します。

- フォルダを削除し、**OK** をクリックして確定します。

削除できるのは、ファイアウォールが関連付けられておらず、その下にフォルダーがネストされていないフォルダーのみです。

フォルダー管理 (Prisma Access)

Prisma Accessフォルダーは事前定義されており、それらを使用して設定範囲を指定し、Prisma Access のデプロイメントタイプ (モバイル ユーザー、リモート ネットワーク、サービス接続) がすべてのグローバル設定を受信し、次に各タイプに必要な設定または固有の設定を受信するようにすることができます。

フォルダーの下に定義された設定は、そのフォルダー階層の下にネストされたすべてのフォルダーに継承されます。例えば、AAフォルダの下にあるGlobalProtect、Explicit Proxy (明示型プロキシ)、Remote Networks (リモートネットワーク)、Service Connections (サービスコネクション)で共通する設定を構成することができます。同様に、 モバイル ユーザー コンテナ などの下のGlobalProtectとExplicit Proxyに共通する設定を構成できます。

Prisma Accessのフォルダー階層を編集することはできません。

フォルダレベルでは、Prisma Accessモバイルユーザー、リモートネットワーク、またはサービス接続のデプロイメントに対してWeb セキュリティを有効にすることもできます。

ワークフロー:Prisma SD-WANセットアップ

どこで使用できますか?	何が必要ですか?
• Prisma SD-WAN	☐ Prisma SD-WANライセンス

Strata Cloud Managerを使用して、Prisma SD-WANでブランチ サイト、データセンター サイト、およびIONデバイスをセットアップできます。

[Workflows (ワークフロー)] > **[Prisma SD-WANのセットアップ]**を選択します。

ワークフローをセットアップできる対象:

- 支店サイト

  [支店サイト]タブを使用して、ネットワーク内にブランチサイトを設定します。企業では、ネットワーク内に1つ以上のブランチを置くことができます。ブランチを作成すると、デフォルトドメインとポリシー ルールのセットを選択し、WANネットワーク、回線カテゴリ、回線ラベル、および回線仕様を設定できます。

- データセンター

  [データセンター]タブを使用して、ネットワーク内のデータセンターサイトをセットアップします。データセンター サイトは支店サイトに接続され、エンタープライズ アプリケーションやサービスをデータセンターでホストできます。

- デバイス

  [デバイス]タブを使用して、ネットワーク内のIONデバイスをセットアップします。IONデバイスは、ブランチサイトまたはデータセンターサイトに導入できます。これらは、あらゆる場所やデプロイメントシナリオのニーズを満たすハードウェアとソフトウェアの両方のフォームファクタで利用できます。支店やデータセンターのIONデバイスを接続し、請求し、割り当て、設定する必要があります。

ワークフロー:Prisma Accessセットアップ

どこで使用できますか?	何が必要ですか?
• Prisma Access (Managed by Strata Cloud Manager)	Prisma Accessライセンス

[Workflows (ワークフロー)] > Prisma Access[Setup (セットアップ)]を選択し、Prisma Accessの設定を開始します。

- リモート ネットワーク ロケーション、モバイル ユーザー、およびPrisma Accessサービス接続を計画している本社やデータセンター間の通信を可能にするために、サービス インフラをセットアップします。サービス接続は、データセンターへの接続を提供します。
- モバイルユーザーをオンボードし、Prisma Accessにどのように接続しているかを判断します。
- リモートネットワークに搭載し、支店などのリモートネットワーク拠点とその支店のユーザーを保護します。リモートサイトには、次世代ファイアウォール、またはサービスへのIPSecトンネルを確立できるSD-WANを含むサードパーティのIPSec準拠デバイスが必要です。
- サービスコネクションを追加して、モバイルユーザーとブランチネットワークのユーザーの両方が本社（HQ）またはデータセンター（DC）のリソースにアクセスできるようにします。サービスコネクションは、企業リソースへのアクセスを提供するだけでなく、モバイルユーザーが支店ロケーションに到達できるようにします。

ワークフロー: Prisma Access

どこで使用できますか?	何が必要ですか?
• Prisma Access (Managed by Strata Cloud Manager)	Prisma Accessライセンス

Prisma Accessを使用してリモート ネットワークとモバイル ユーザーを保護する前に、インフラストラ クチャ サブネットを設定する必要があります。

Prisma Accessは、ブランチ ネットワーク、モバイル ユーザー、Prisma Accessセキュリティ インフラ、およびサービス接続を介してPrisma Accessに接続する予定の本社やデータセンター ネットワークとの間の通信のために、サブネットを使用してネットワーク バックボーンを作成します。リモート ネットワークまたはサービス接続にダイナミック ルーティングを使用する場合は、RFC 6696準拠のBGPプライベートAS番号も構成する必要があります。

Prisma Access用のインフラストラクチャ サブネットを追加する場合は、次の推奨事項と要件に従ってください。

- RFC 1918 準拠のサブネットを使用します。Prisma Accessでは、RFC1918に準拠しない（パブリック）IPアドレスの使用をサポートしているが、インターネットのパブリックIPアドレス空間と競合する可能性があるため、推奨されない。

- 169.254.169.253、169.254.169.254、および100.64.0.0/10サブネット範囲と重複するサブネットは指定しないでください。Prisma AccessがこれらのIPアドレスとサブネットを内部使用のために予約しているからです。このサブネット ワークは既存のネットワークの拡張であるため、企業ネットワーク内で使用する IP サブネットや、Prisma Access [for Users (ユーザー用)] または [Prisma Access for Networks (ネットワークス用)] に割り当てるIPアドレスプールと重複することはできない。サービス インフラストラクチャには多数の IPアドレスが必要なので、/24 サブネットワーク (例: 172.16.55.0/24) を指定する必要があります。
- Prisma Accessが、リモート ネットワーク ロケーション、モバイル ユーザー、およびPrisma Accessオーバー サービス接続を計画している本社またはデータセンター間の通信を可能にするために使用できるインフラストラクチャ サブネットを入力します。インフラストラクチャ サブネットにはRFC 1918準拠のサブネットを使用します。

詳細は、Prisma Accessセットアップを参照してください。

インフラストラクチャのDNSをセットアップする

Prisma Accessでは、組織内部のドメインと外部のドメインの両方を解決するDomain Name System (ドメイン ネーム システム - DNS)サーバーを指定できる。 Prisma Accessは、DNSサーバーの設定に基づいてDNSリクエストをプロキシします。

インフラストラクチャDNSを設定すると、LDAPサーバーやDNSサーバーなどの企業ネットワーク上のサービスにアクセスできるようになります。特に、HQまたはデータセンターでこれらの種類のリソースにアクセスできるようにサービス接続を設定する予定の場合は、これが有効です。内部ドメイン リスト内のドメインに対するDNSクエリは、Prisma Accessリモート ネットワーク ユーザーとモバイル ユーザーがリソースを 利用できるように、ローカルDNSサーバーに送信されます。

これにより、すべてのトラフィックに適用される内部ドメイン リストがセットアップされます。必要に応じて、管理者ガイドを参照して、特定のモバイル ユーザー デプロイメントまたはリモート ネットワーク サイトにのみ適用される内部ドメイン リストを作成する方法を確認できます。

インフラストラクチャにDNSをセットアップする利点は次のとおりです。

- Prisma Accessが内部ドメインを解決できるようにします
- 内部ドメインと外部ドメインの両方を解決するためにDNSをセットアップする
- ドメインリスト内のドメインの前にワイルドカード (*) を使用します (例: *.acme.local または *.acme.com)。

詳しくは、DNS用Prisma Accessを参照してください。

ワークフロー:モバイルユーザー

どこで使用できますか?	何が必要ですか?
• Prisma Access (Managed by Strata Cloud Manager)	❑ Prisma Accessライセンス ❑ Strata Logging Serviceライセンス

モバイルユーザーを設定する前に、必要なライセンス(Prisma Accessモバイルユーザー向けのStrata Logging Serviceライセンスと適切なファイアウォール ストレージ スペースを備えたライセンス)。モバイルユーザーが他の接続ネットワークに接続する場合は、接続に必要な企業アクセスノード（CAN）を提供するZero Trust Network Access（ZTNA）またはEnterprise Editionのいずれかのライセンスが必要です。

最初に接続タイプを選択するか、GlobalProtect、明示的プロキシ、またはその両方を使用できます。どちらの接続タイプでも、Prisma Accessがモバイル ユーザーの環境をプロビジョニングできるようにするために、最初に入力する必要がある必須設定はわずかです。

1. Prisma Accessに接続します。

   セットアップする場所のモバイル ユーザーがどのようにPrisma Accessに接続すべきかを決定します。モバイル ユーザー ライセンスは、GlobalProtect接続と明示的なプロキシ接続の間で分割できます。一部のユーザーはGlobalProtectを介して接続でき、他のユーザーは明示的なプロキシを介して接続できます。

   モバイルユーザー デバイスにインストールされている GlobalProtectアプリケーションはPrisma Accessにトラフィックを送信します。
2. インフラストラクチャをセットアップします。

   基本的なインフラストラクチャ設定をセットアップしてから、接続タイプ (GlobalProtect または Explicit Proxy) に固有のインフラストラクチャ設定を構成します。

   モバイルユーザー デバイス上のプロキシ自動設定（PAC）ファイルにより、ブラウザ トラフィックがPrisma Accessにリダイレクトされます。
3. Prisma Accessロケーションを選択します。

   マップには、次のユーザー向けのPrisma Accessをデプロイできるグローバル地域が表示されます：北米、南米、ヨーロッパ、アフリカ、中東、アジア、日本、オーストラリア・ニュージーランド(オーストラリア、ニュージーランド)さらにPrisma Accessは、各地域内に複数の場所を提供し、ユーザーがユーザーのロケールに合わせたユーザー エクスペリエンスを提供する場所に接続できるようにします。最高のパフォーマンスを得るには、[すべて選択] を選択します。または、選択した各地域内でユーザーがアクセスする必要がある特定の場所を選択します。デプロイを1つのリージョンに制限することで、デプロイメントされたリージョンをよりきめ細かく制御し、ポリシーや業界の規制で必要なリージョンを除外できます。
4. Prisma Accessロケーションを追加します。

   ユーザーをサポートするPrisma Accessロケーションを追加するための設定を行います。
5. モバイルユーザーを認証します。

   正当なユーザーのみがサービスやアプリケーションにアクセスできるように、ユーザー認証をセットアップします。セットアップをテストするために、Prisma Accessはローカルで認証するユーザーを追加することもできるし、そのままエンタープライズ レベルの認証をセットアップすることもできます。

初期設定をPrisma Accessにプッシュすると、Prisma Accessはモバイル ユーザー環境のプロビジョニングを開始する。これには最大15分かかる場合があります。モバイルユーザーのロケーションを設定すると、モバイルユーザーのセットアップ ページ、サマリーの概要ページ、Prisma Accessインサイト内で確認できるようになります。

Prisma Access[Mobile Users (モバイルユーザー)] 詳細については、こちらをご覧ください。

ワークフロー:リモートネットワーク

どこで使用できますか?	何が必要ですか?
• Prisma Access (Managed by Strata Cloud Manager)	Prisma Accessライセンス

リモート ネットワークをPrisma Accessに接続する準備として、いくつのサイトを搭載するかを知る必要があります。この情報は、Prisma Accessでトラフィックをルーティングする方法などの接続要件を判断するのに役立ちます。リモートネットワークのデプロイメントを計画する際には、最適なセキュリティ ポリシー ルールを適切に設定するために、Prisma Accessをパススルーするアプリケーションを知る必要があります。同様に重要なのは、脅威プロファイルの設定を確立することです。さらに、一貫した脅威軽減戦略のために、一貫した脅威、URL、WildFireスキャンをすべてのルールに適用することを検討する必要があります。

詳細は、Prisma Access「 Remote Networks (リモートネットワーク)」を参照してください。

ワークフロー:サービスコネクション

どこで使用できますか?	何が必要ですか?
• Prisma Access (Managed by Strata Cloud Manager)	Prisma Accessライセンス

サービスコネクションは、モバイルユーザーと支店ネットワークのユーザーの両方が、本社（HQ）やデータセンター（DC）のリソースにアクセスすることを可能にします。サービスコネクションは、企業リソースへのアクセスを提供するだけでなく、モバイルユーザーが支店ロケーションに到達できるようにします。

[Workflows (ワークフロー)] > **Prisma Access [Setup (セットアップ)]** > **[Service Connections (サービスコネクション)]**を選択し、サービス接続を追加します。

最初に作成するトンネルは、サービス接続のプライマリトンネルです。このワークフローを繰り返して、オプションでセカンダリ トンネルをセットアップします。両方のトンネルがアップすると、プライマリ トンネルがセカンダリ トンネルよりも優先されます。プライマリサービス接続トンネルがダウンした場合、接続はプライマリトンネルが戻るまでセカンダリトンネルにフォールバックします。Prisma Accessは、トンネルの確立に使用するIPSecデバイスに基づいて、組み込みの推奨IKEおよびIPSecセキュリティ設定を提供する。推奨設定を使用して使用を開始することも、環境に合わせて必要に応じてカスタマイズすることもできます。

詳細は、「Prisma Accessサービスコネクション」を参照してください。

ワークフロー:リモートブラウザ分離

どこで使用できますか?	何が必要ですか?
• Prisma Access (Managed by Strata Cloud Manager)	Prisma Access 5.0 イノベーション

どこで使用できますか?	何が必要ですか?
	❑ Prisma Accessライセンス(モバイルユーザーまたはリモートネットワークライセンスサブスクリプション付き) ❑ リモート ブラウザ分離ライセンス

Palo Alto NetworksのRBI（Remote Browser Isolation）は、ユーザーの管理対象デバイスや企業ネットワークから離れたすべてのブラウジング アクティビティをPrisma Accessなどの外部エンティティに隔離して転送するソリューションです。これにより、悪意のあるコードやコンテンツをプラットフォーム内で保護し、隔離することができます。

RBIはPrisma Accessとネイティブに統合されているため、分離プロファイルを既存のセキュリティ ポリシーに簡単に適用できます。分離されたすべてのトラフィックは、Advanced Threat Prevention、Advanced WildFire、Advanced URL Filtering、DNS Security、SaaS Securityなどのすべて Cloud-Delivered Security Services (CDSS) が提供する解析と脅威防御を受けます。

ユーザーをRBIにオンボードする準備として、ユーザーによる隔離されたブラウジングのためにどのURLカテゴリを有効にするかを検討します。コピー＆ペースト機能、キーボード入力、ファイルのアップロード、ダウンロード、印刷などの共有オプションなど、ユーザーが実行することを禁止するブラウザアクションについて考えます。

詳細は、「リモートブラウザの分離」を参照してください。

ワークフロー:ソフトウェアのアップグレード

どこで使用できますか?	何が必要ですか?
• Prisma Access (Managed by Strata Cloud Manager) • NGFW (Managed by Strata Cloud Manager)	• Strata Cloud Managerで設定を管理するには、少なくともこれらのライセンスのうち 1 つが必要です。NGFWとPrisma Accessを統合管理するには、NGFWおよびPrisma Accessライセンスが必要です： ❑ Prisma Accessライセンス ❑ AIOps for NGFW Premium license (use the Strata Cloud Manager app) ❑ Strata Cloud Manager Pro

Strata Cloud Managerを使用して、NGFWおよびPrisma Accessのソフトウェア アップグレードを計画および管理する。実行できるワークフローは次のとおりです。

- アップグレードの推奨事項:アップグレードの推奨事項を作成し、アップグレード可能なデバイスに最適なソフトウェア バージョンを決定します。「ソフトウェアアップグレードの推奨事項」では、ファイアウォールで有効になっている機能を分析し、カスタマイズされた推奨事項を提供します。
- Prisma Accessアップグレードダッシュボード:特定のPrisma Accessのアップグレードに優先する時間帯を選択します。
- NGFW - スケジューラ:PAN-OSソフトウェア アップデートをスケジュールして、選択した日時にファイアウォールを対象のPAN-OSバージョンにアップグレードまたはダウングレードします。
- NGFW
- Prisma Access

ソフトウェアのアップグレード(NGFW)

[Workflows (ワークフロー)] > [Software Upgrades (ソフトウェアのアップグレード)] > [Upgrade Recommendations (アップグレードの推奨事項)] を選択します。次に、デバイスを分析し、アップグレードの推奨事項を作成することで、デバイスのアップグレードを計画します。

アップグレードの推奨事項

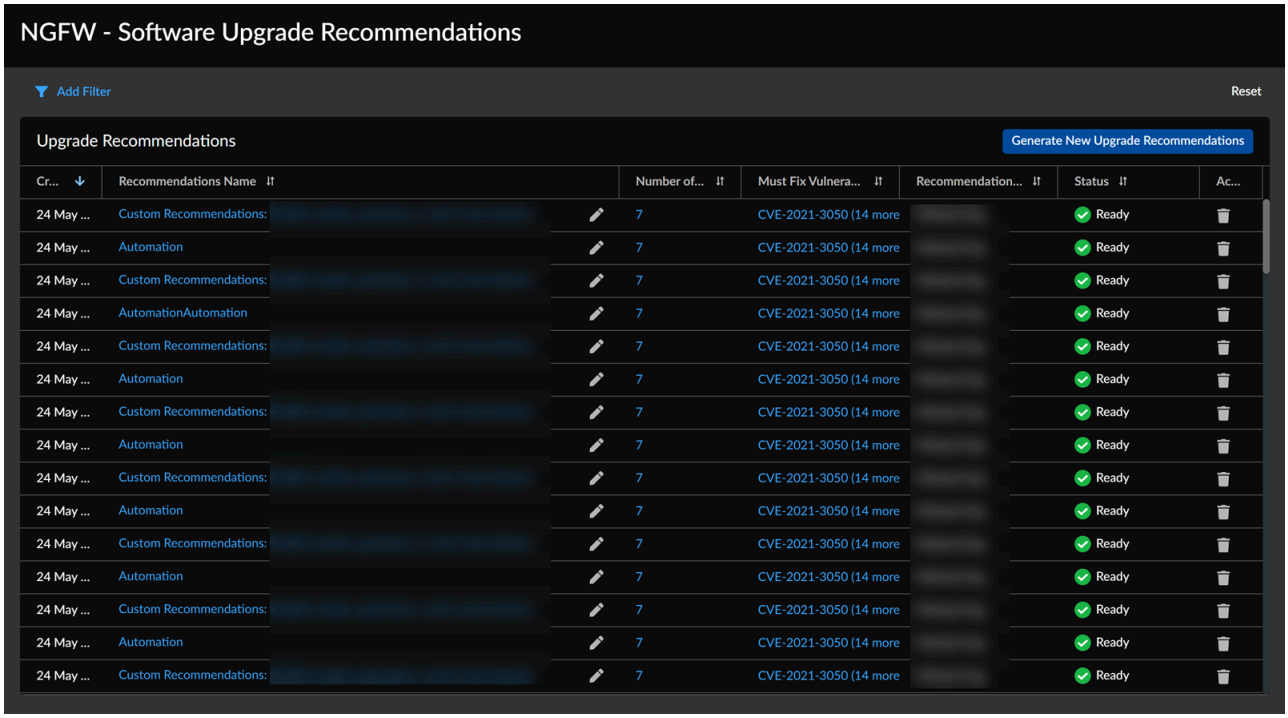
[Workflows (ワークフロー)] > [Software Upgrades (ソフトウェアのアップグレード)] > [Upgrade Recommendations (アップグレードの推奨事項)]では、推奨事項を作成して、アップグレード可能なデバイスに最適なソフトウェアバージョンを決定できます。「ソフトウェアアップグレードの推奨事項」では、ファイアウォールで有効になっている機能を分析し、以下を含むカスタマイズされた推奨事項を提供します。

- アップグレードできるデバイスに最適なソフトウェアバージョン。

- 各推奨ソフトウェアバージョンの新機能、動作の変更、脆弱性、ソフトウェアの問題に関する情報。

アップグレードの推奨事項の種類は次のとおりです。

- 毎週生成され、推奨されるアップグレード オプションを含むシステム生成の推奨事項。
- セキュリティアドバイザリの概要の特定のCVEに対して選択したデバイスに基づいて生成されるユーザー生成のカスタム推奨事項。
- ファイアウォールのテクニカルサポートファイル(TSF)のアップロードに基づいて生成 s あれるユーザー生成の推奨事項。



アップグレードの推奨事項のすべてのプランでは、以下のことができます。

- アップグレードが必要なデバイスの数と、脆弱性を修正する必要があるデバイスの数を表示する。
- 最適化レポートの名前を編集して、カスタム レポートを区別する。
- 推奨レポートを「作成日」、「プラン名」、および「推奨の生成者」でフィルタリングする。
- 失敗した、または不要になったアップグレードの推奨事項を削除する。

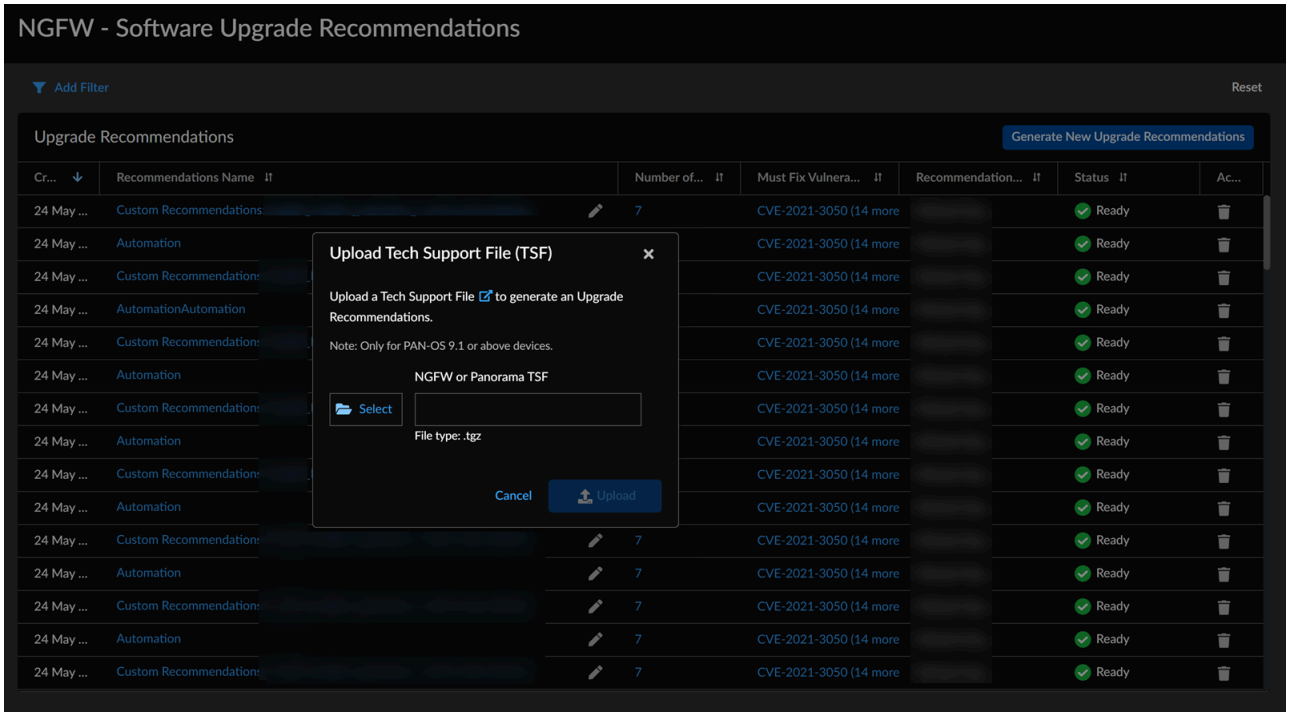
推奨レポートをクリックすると、デバイスのアップグレード オプションを含む詳細レポートが表示されます。アップグレード オプションを選択して、詳細を表示します。 表示できる詳細は、**[New Features (新機能)]**、**PAN-OS Known Vulnerabilities (PAN-OS** の既知の脆弱性)、**Changes of Behavior (**振る舞いの変化)そして **PAN-OS Known Issues (PAN-OS** の既知の問題)が含まれます。**PAN-OS Known Issues (PAN-OS**の既知の問題)の既知の問題の場合、**Associated Case Count (**関連するケースの数)の値は、この問題を報告した顧客の数で求められます。

Export (エクスポート) をクリックして、このレポートをCSV形式でダウンロードします。

オンデマンド ソフトウェア アップグレードの推奨事項の生成

1. **Workflows (ワークフロー)] > [ソフトウェアのアップグレード (Software Upgrades)] > [Upgrade Recommendations (アップグレードの推奨事項)]**に移動します。
2. 新しいアップグレード推奨事項を生成します。
3. テクニカルサポートファイル(TSF)を選択し、アップロードします。

- 一度にアップロードできるデバイスの*TSF*は*1*つだけで、*.tgz* ファイル形式の*TSF*である必要があります。
- ソフトウェア アップグレードの推奨事項は、レポート生成のために*PAN-OS*バージョン*9.1*以降を搭載したデバイスからの*TSF*をサポートします。



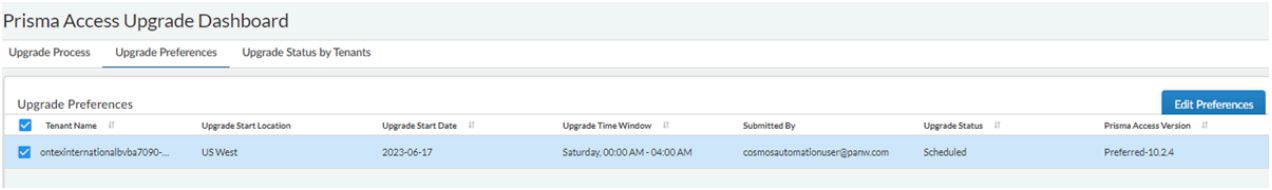
4. ステータスが**[Ready (用意)]**と表示された後に、ソフトウェアのアップグレードに関する推奨事項を表示します。TSFファイルのアップロード、ファイル形式、または処理に関連するエラーがあるかどうかを確認するために、**[Status (ステータス)]**列をチェックすることもできます。

ソフトウェアのアップグレード(Prisma Access)

[Workflows (ワークフロー)] > [Software Upgrades (ソフトウェアアップグレード)] > [Prisma Access]を選択すると、Prisma Accessデータプレーンのアップグレードプロセスに関する情報が表示されます。

次の作業を行えます。

- Prisma Accessデータプレーンのアップグレードプロセスを理解する。
- アップグレードの環境設定を選択します。



テナント名を選択して、アップグレード設定を選択します。詳細については、「Choose a Preferred Window for Certain Prisma Access Upgrades (特定のPrismaアクセスアップグレードにむけた優先ウィンドウの選択)」を参照してください。

ワークフロー:Prisma Access Browser

どこで使用できますか?	何が必要ですか?
• Prisma Access (Managed by Strata Cloud Manager)	☐ Prisma Access with Prisma Access Browserバンドルライセンス ☐ スーパーユーザーまたはPrisma Access Browserロール

Prisma Access Browserのオンボーディングを開始するには、**[Workflows (ワークフロー)]** > **Prisma Access [Setup (セットアップ)]** > **Prisma Access Browser**

Prisma Access Secure Enterprise Browser (Prisma Access Browser)は、管理されていないデバイスにまで保護を拡張するネイティブに統合されたEnterprise Browserを通じて、管理されているデバイスと管理されていないデバイスの両方を保護する唯一のソリューションである。「Prisma Access Browserとは」を参照します

オンボーディングは、次の項目を設定する一連のステップです。

- ユーザー認証とグループ
- Prisma Access統合
- routing
- SSOアプリケーションの実施
- ダウンロードと配布
- ブラウザポリシー

StrataクラウドマネージャーにPrisma Access Browserをオンボーディングする。

レポート:ログ - Strata Cloud Manager

どこで使用できますか?	何が必要ですか?
• Prisma Access （*Strata Cloud Manager*または*Panorama*の設定管理付き） • NGFW （*Strata Cloud Manager*または*Panorama*の設定管理付き） • Prisma SD-WAN	❑ これらの各ライセンスには、Strata Cloud Managerへのアクセスが含まれています。 ❑ Prisma Access ❑ AIOps for NGFW Premium license (use the Strata Cloud Manager app) ❑ Strata Cloud Manager Essentials ❑ Strata Cloud Manager Pro ❑ Prisma SD-WAN ❑ Software NGFW Credits （*VM-Series*ソフトウェア*NGFW*の場合） ❑ WANクラリティレポートライセンス ❑ レポートのダウンロード、共有、スケジュール設定の権限を持つロール。

Strata Cloud Managerにおけるネットワーク トラフィック パターン、帯域幅使用率、セキュリティ サブスクリプション データに関するレポートを取得します。レポートは、計画と監視の目的で使用できるネットワークに関する実用的な洞察を提供します。レポートは、特定のPrisma AccessおよびNGFWダッシュボード、Activity Insightsの概要、Prisma SD-WANでサポートされています。Prisma AccessユーザーとNGFWユーザーは、ダッシュボードをフル活用できるほか、ダッシュボードのデータをPDFとしてダウンロードしたり、レポートを組織内で共有したり、レポートが定期的に電子メールの受信トレイに配信されるようにスケジュール設定したりできます。レポートはPrisma SD-WANのライセンス付きサブスクリプションサービスです。Prisma SD-WAN内のコントローラ、拠点間、回線からレポートをダウンロードして表示できます。

Strata Cloud Managerでこれらのレポートを表示します。

- Prisma AccessとNGFW - レポートの生成は、Prisma AccessとNGFWのダッシュボードとアクティビティインサイトから行えます。ダッシュボード右上のこれらのアイコンは、このダッシュボードでレポートがサポートされていることを示します。**Reports (レポート)**メニューからレポートの生成、ダウンロード、共有、スケジュール設定を直接行うこともできます。

- Prisma SD-WAN - 次のWAN Clarityレポートを表示します。
  - WAN Clarity Branch レポート
  - WAN Clarity Data Center レポート
  - 総帯域幅使用状況レポート
- Prisma AccessおよびNGFW
- Prisma SD-WAN

レポート(Prisma AccessおよびNGFW)

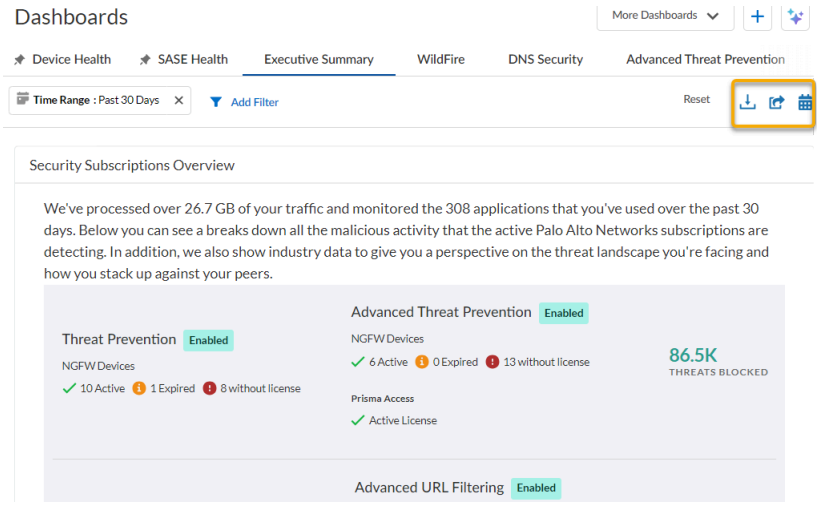
ダッシュボードとActivity Insightsの概要はPDFレポートとして組織内で共有でき、レポートをスケジュール設定することで、電子メールの受信トレイ（および同僚の受信トレイ）に一定間隔（日次、週次、月次）で配信することもできます。

組織内の人と簡単にレポートを共有できるように、このアプリ用にCloud Identity Engine（Directory Sync(ディレクトリ同期)）をセットアップします。Cloud Identity Engineは、ActiveDirectory (アクティブディレクトリ)情報への読み取り専用アクセス権を提供しますCloud Identity Engineをセットアップすれば、スケジュールレポートに受信者を簡単に追加できます。レポートの受信者はCloud Identity Engineと照合され、一致するものが見つからなかった場合は、サポートアカウントに関連付けられている電子メールアドレスドメインと照合して、追加の妥当性確認手順を実行します。これらのチェックにより、レポートが組織の外部に送信されないようにします。

レポートは、**[Reports (レポート)]**メニューから直接ダウンロード、共有、またはスケジュールできます。また、個々の**[ダッシュボード]**ページと**[nsights (インサイト)]> > [Activity Insights (アクティビティに関するインサイト)] > [Overview (概要)]**ページからもダウンロード、共有、スケジュールできます。レポートはPDFとして共有・ダウンロードされます。

レポートをダウンロード、共有、またはスケジュールするには:

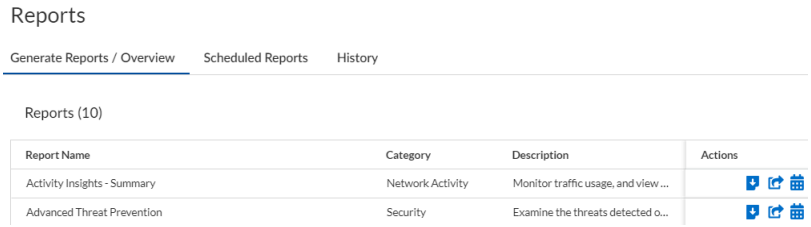
STEP 1 | これらのアイコンのいずれかをクリックします。**[Dashboard (ダッシュボード)]**ページまたは**[Insights (インサイト)]> > [Activity Insights (アクティビティに関するインサイト)] > [Overview (概要)]**ページから します。



または

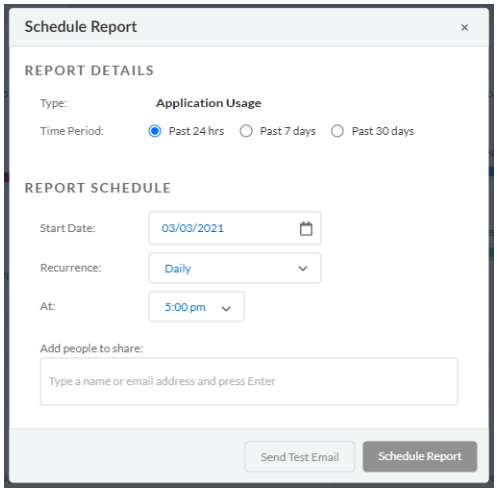
Strata Cloud Manager > [Reports (レポート)] > [Generate Reports/Overview (レポートの作成/概要)]をクリックし、レポート形式のリストからこれらのアイコン のいずれかを選択します。デフォルトでは、レポートの生成対象となるダッシュボードの種類に基づいて、過

去24時間のデータまたは30日間のデータでレポートが生成されます。レポートのスケジュール時にレポート内のデータを収集する期間をカスタマイズできます。

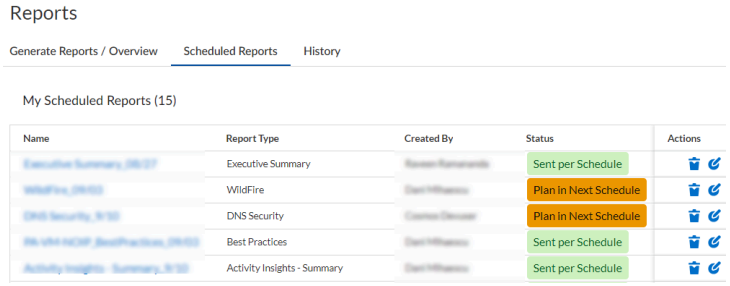


STEP 2 | レポートをスケジュールする場合は、以下を含むレポートパラメータの定義を続ける必要があります。

- データを収集する**Time Period (期間)**
- **[Recurrence (定期)]**は、レポートの配信頻度（日次、週次、月次）です。



スケジュールされているすべてのレポートは、**Strata Cloud Manager** > **[Reports (レポート)]** > **[Scheduled Reports (スケジュールレポート)]**タブから表示、編集、または削除できます。



[History (履歴)]には、過去30日間にダウンロードされたすべてのレポートが表示されます。

レポート(Prisma SD-WAN)

Prisma SD-WAN WAN Clarityレポートは、ネットワーク内のトラフィックの配信と帯域幅使用率の集計ビューを提供します。レポートパッケージ全体をダウンロードすることも、Prisma SD-WANコントローラからレポートを表示することもできます。これにより、1週間ごとの傾向比較や、サイトや回線間の比較が可能になります。

レポートは、ライセンスされたサブスクリプションサービスとしてすぐに使用できます。サブスクリプションを有効にするには、Prisma SD-WANセールスチームにお問い合わせください。

Prisma SD-WANWAN Clarityレポートには、次の項目が含まれます。

- WAN Clarity Branch レポート
- WAN Clarity Data Center レポート
- 総帯域幅使用状況レポート

レポートを表示するには

STEP 1 | **[Reports (レポート)]** > **[Prisma SD-WAN]**を選択します。

STEP 2 | **[WAN Clarity Reports]**の**[View Reports (レポートの表示)]**をクリックします。

STEP 3 | **[Time Range (時間範囲)]**を選択し、**[Report for (レポート対象)]**フィールドで次のいずれかを選択します。

- ブランチ
- データセンター
- 帯域幅の使用状況の集計

お気に入り:ログ - Strata Cloud Manager

どこで使用できますか?	何が必要ですか?
• Prisma Access （*Strata Cloud Manager*または*Panorama*の設定管理付き） • NGFW （*Strata Cloud Manager*または*Panorama*の設定管理付き）	❑ これらの各ライセンスには、Strata Cloud Managerへのアクセスが含まれています。 ❑ Prisma Access ❑ AIOps for NGFW Premium license (use the Strata Cloud Manager app) ❑ Strata Cloud Manager Essentials ❑ Strata Cloud Manager Pro ❑ 任意のテナントまたはテナント サービス グループ(TSG)対応アプリケーション ❑ ニーズに応じたロール

お気に入り機能を使用することで、関心のあるアイテムを保存し、Strata Cloud Manager内の任意の場所から必要なときにすばやくアクセスできます。リストの内容を整理、編集、削除することで、自分のプライベートリストでお気に入りのメニュー項目名をパーソナライズできます。

お気に入りは次のように管理いただけます。

- お気に入りに追加
- お気に入りを表示
- お気に入りの編集
- お気に入りの削除

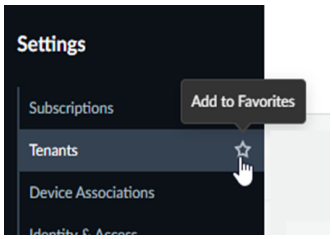
お気に入りに追加

どこで使用できますか?	何が必要ですか?
• Prisma Access （*Strata Cloud Manager*または*Panorama*の設定管理付き） • NGFW （*Strata Cloud Manager*または*Panorama*の設定管理付き）	❑ これらの各ライセンスには、Strata Cloud Managerへのアクセスが含まれています。 ❑ Prisma Access ❑ AIOps for NGFW Premium license (use the Strata Cloud Manager app) ❑ Strata Cloud Manager Essentials ❑ Strata Cloud Manager Pro ❑ 任意のテナントまたはテナントサービスグループ(TSG)対応アプリ ❑ ニーズに応じたロール

繰り返し移動する必要があるStrata Cloud Managerにメニュー項目やページがあり、それらの項目を都度検索したり移動したくない場合、これらの項目をお気に入りリストに保存できます。

STEP 1 | 保存するメニュー項目またはページに移動します。

STEP 2 | アイテムにカーソルを合わせると星のアイコンが表示されます。



STEP 3 | スターを選択すると、このアイテムをお気に入りに追加できます。

一番上のメニュー項目はお気に入りに追加できません。お気に入りに追加できるのはサブメニューのみです。

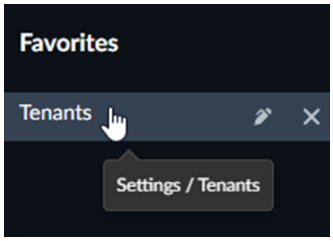
お気に入りを表示

どこで使用できますか?	何が必要ですか?
• Prisma Access （*Strata Cloud Manager*または*Panorama*の設定管理付き） • NGFW （*Strata Cloud Manager*または*Panorama*の設定管理付き）	❑ これらの各ライセンスには、Strata Cloud Managerへのアクセスが含まれています。 ❑ Prisma Access ❑ AIOps for NGFW Premium license (use the Strata Cloud Manager app) ❑ Strata Cloud Manager Essentials ❑ Strata Cloud Manager Pro ❑ 任意のテナントまたはテナント サービス グループ(TSG)対応アプリケーション ❑ ニーズに応じたロール

お気に入りを追加すると、お気に入りとその元の場所を表示できます。

STEP 1 | お気に入りを選択します。

STEP 2 | アイテムの上にマウスを置くと、場所のアイコンが表示されます。



STEP 3 | 実際の場所へのパスとメニュー名が表示されます。

お気に入りリスト内の項目をクリックすると、元の場所へ移動します。

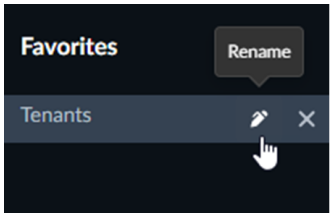
お気に入りの編集

どこで使用できますか?	何が必要ですか?
• Prisma Access （*Strata Cloud Manager*または*Panorama*の設定管理付き） • NGFW （*Strata Cloud Manager*または*Panorama*の設定管理付き）	❑ これらの各ライセンスには、Strata Cloud Managerへのアクセスが含まれています。 ❑ Prisma Access ❑ AIOps for NGFW Premium license (use the Strata Cloud Manager app) ❑ Strata Cloud Manager Essentials ❑ Strata Cloud Manager Pro ❑ 任意のテナントまたはテナント サービス グループ(TSG)対応アプリ ❑ ニーズに応じたロール

お気に入り追加後、お気に入りを編集してパーソナライズできます。

STEP 1 | お気に入りを選択します。

STEP 2 | アイテムにカーソルを合わせると編集アイコンが表示されます。



STEP 3 | 項目の名前を変更します。

お気に入りリストのアイテム名を変更しても、元のロケーションのアイテム名は変更されません。

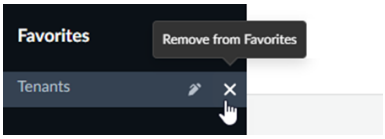
お気に入りの削除

どこで使用できますか?	何が必要ですか?
• Prisma Access （*Strata Cloud Manager*または*Panorama*の設定管理付き） • NGFW （*Strata Cloud Manager*または*Panorama*の設定管理付き）	❑ これらの各ライセンスには、Strata Cloud Managerへのアクセスが含まれています。 ❑ Prisma Access ❑ AIOps for NGFW Premium license (use the Strata Cloud Manager app) ❑ Strata Cloud Manager Essentials ❑ Strata Cloud Manager Pro ❑ 任意のテナントまたはテナントサービスグループ(TSG)対応アプリ ❑ ニーズに応じたロール

お気に入り追加後、お気に入りをリストから削除できます。

STEP 1 | お気に入りを選択します。

STEP 2 | アイテムにカーソルを合わせると、削除アイコンが表示されます。



STEP 3 | アイコンをクリックするとお気に入りがリストから削除されます。

お気に入りリストからアイテムを削除しても、元のアイテムは元の場所から削除されません。

設定:ログ - Strata Cloud Manager

どこで使用できますか?	何が必要ですか?
• Prisma Access (Managed by Strata Cloud Manager)	❑ 任意のテナントまたはテナント サービス グループ(TSG)対応アプリケーション ❑ ニーズに応じたロール ❑ ログを管理するためのStrata Logging Service

設定から、Strata Cloud Managerで提供されるすべてのサービスに関連するプロセスを管理できます。これらのプロセスには、

サブスクリプション

お使いの製品の承認されたサブスクリプションを表示します。

サブスクリプションを管理します。

Device Associations

デバイスとアプリのオンボーディングで最もよく使用される**Device Associations**を使用すると、次のことが可能になります。

- 新しいデバイスをテナントに関連付ける
- アプリとデバイスを関連付ける
- デバイスとアプリの関連付けを管理する

デバイスの関連付けを始めます。

製品

単一テナント環境の場合、製品の表示、起動、および管理は以下のように行います。

- 製品情報を取得する
- インスタンスの名前を変更する
- 共有の管理
- テナントを追加する

製品管理を開始します。

テナント

MSSP（マネージド セキュリティ サービス プロバイダー）または分散型エンタープライズの場合は、テナントによって表されるビジネス組織とユニットの階層を作成して管理できます。テナントからは、次のことができます。

- テナントの追加
- テナントの編集
- テナントライセンスの管理
- テナントの削除
- シングルテナントからマルチテナントデプロイメントへの移行

テナント管理を開始します。

ID&アクセス

すべてのアプリケーションとAPIベースのアクセスについて、ユーザーの役割と権限の認証と承認を制御します。ID&アクセスを通じて、以下の管理を行うことができます。

- ユーザーアクセス
- サービスアカウント
- ロール
- サードパーティIDプロバイダ統合

ID&アクセスを開始します。

監査ログ

Strata Cloud Managerのユーザーが開始したすべてのアクションの記録を表示する

監査ログを表示します。

IONライセンスの管理

仮想IONデバイスの認証トークンを生成します。これにより、環境への仮想デバイスの不正な追加を防止するための制御セットが提供されます。

IONライセンスを管理します。

ユーザー設定

ニーズに合わせて環境設定をカスタマイズします。たとえば、ディスプレイモードを選択します。

ユーザープリファレンスを設定します。

信頼できる**IP**リスト

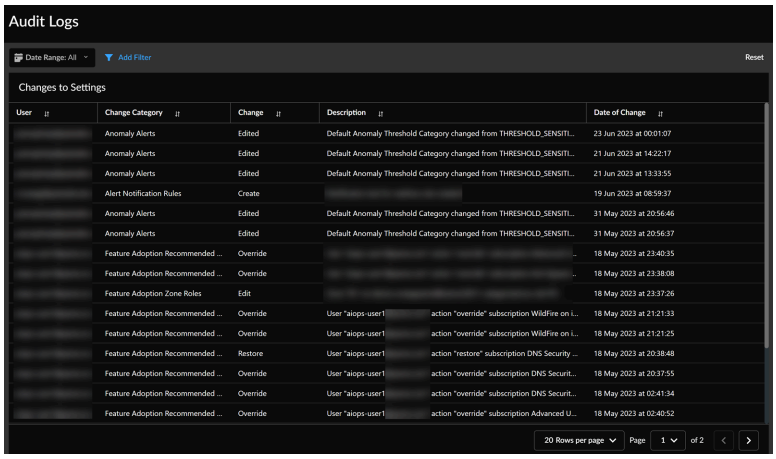
信頼できるIPリストを使用して、テナントごとに許可されるIPアドレスを指定することで、アプリケーションへのアクセスを制限できます。

信頼できるIPリストを設定します。

設定:監査ログ

どこで使用できますか?	何が必要ですか?
• Strata Cloud Manager	❑ 以下のいずれかが必要です: • AIOps for NGFW Freeアプリ • AIOps for NGFW Premium(Strata Cloud Managerアプリケーションを使用) • Strata Cloud Manager Essentials • Strata Cloud Manager Pro ❑ 以下の定義済みロールのいずれか:監査人、ビジネス管理者、データセキュリティ管理者、デプロイメント管理者、IAM管理者、マルチテナントIAM管理者、マルチテナント管理ユーザー、マルチテナント監視ユーザー、マルチテナントスーパーユーザー、ネットワーク管理者、セキュリティ管理者、SOCアナリスト、スーパーユーザー、階層1サポート、階層2サポート、表示専用管理者

[設定] > [監査ログ] には、Strata Cloud Managerのユーザーが開始したアクションのリストが表示されます。ここには、加えられた変更に関するログ、変更の所有者、変更の日時、および変更の説明が表示されます。これらのログは、コンプライアンスやトラブルシューティングの目的で使用できます。監査ログは、機能のある日付範囲、ユーザー、カテゴリ、および変更の種類でフィルタリングできます。



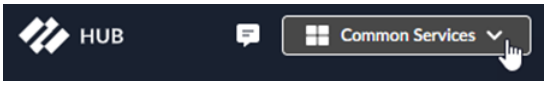
設定:信頼できるIPリスト

どこで使用できますか?	何が必要ですか?
• Strata Cloud Manager	☐ スーパーユーザー、マルチテナントスーパーユーザー、マルチテナントIAM管理者のIAMロール、または「信頼できるIPリスト」パーミッションセットを持つカスタムロール

クラウドで配信されるアプリケーションは、世界中のどこからでもアクセスできる利便性を提供します。しかし、これにより、盗まれた認証情報を使用したアクセス、辞書攻撃、その他の形式のブルートフォース攻撃など、アプリケーションへのアクセスを取得するリスクにさらされる可能性があります。

IDおよびアクセス管理によってこのリスクはいくらか軽減されますが、信頼できるIPリストを使用して、テナントごとに許可されるIPアドレスを指定することで、アプリケーションへのアクセスをさらに制限できます。

デフォルトでは、新しいテナントの作成中に、任意のIPアドレスからWebインターフェースとAPIの両方へのアクセスが許可されます。信頼できるIPリストは、テナントへのアクセスが許可されている信頼できるIPアドレスのリストです。信頼できるIPリストを使用して、1つのテナントへのアクセスを制限したり、マルチテナント階層で親テナントとその子へのアクセスを制限したりできます。マルチテナント階層では、親テナントに信頼できるIPリストを追加します。リストは親テナントから子テナントに継承され、トップダウンで適用されます。

Strata Cloud Managerから信頼できるIPリストを管理する方法	信頼できるIPリストを**hub**から管理する方法
Strata Cloud Managerから信頼IPリストを管理するには、**[Settings (設定)] > [Trusted IP List (信頼IPリスト)]**を選択します。  Strata Cloud Managerから信頼できるIPリストを管理でき、Strata Cloud ManagerのWebインターフェースとAPIは信頼できるIPのみへのアクセスを許可します。	hubから信頼できる IP リストを管理するには、 ハブのテナントビュー > **Common Services (共有サービス) > Trusted IP List (信頼できるIPリスト)**を選択します。  hubから信頼できるIPリストを管理できますが、hubは信頼できるIPの適用から除外されるため、hubへのアクセスは信頼できるIPに制限されません。アクセス権を持つべきStrata Cloud ManagerでIPアドレスがテナントからブロックされた場合は、hubにアクセスして、リストされたアクセス権があればアクセスをロック解除できます。

信頼できるIPを追加する

どこで使用できますか?	何が必要ですか?
• Strata Cloud Manager	❑ スーパーユーザー、マルチテナントスーパーユーザー、マルチテナントIAM管理者のIAMロール、または「信頼できるIPリスト」パーミッションセットを持つカスタムロール

ライセンスを有効化し、テナントを作成し、Strata Cloud Managerへのユーザーアクセスを管理したら、信頼できるIPアドレスを信頼できる IP リストに追加することで、テナントへのアクセスをさらに制限できます。デフォルトでは、どのIPアドレスでもアクセスが許可されます。

Strata Cloud Managerを使用して信頼できるIPを追加する。

STEP 1 | **[Settings (設定)]** > **[Trusted IP List (信頼できるIPリスト)]**を選択します。

STEP 2 | 検索またはスクロールしてテナントを見つけて選択します。

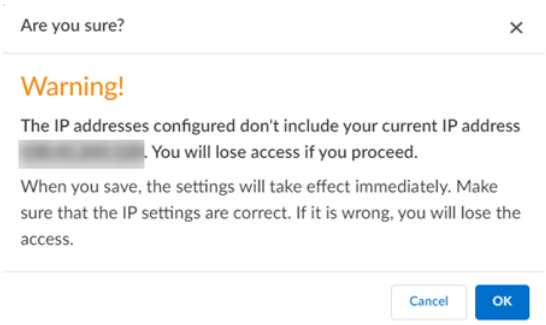
STEP 3 | **Add New**（新規追加）を選択します。

STEP 4 | このテナントにアクセスできるIPアドレスを入力します。

- このフィールドはCIDR表記をサポートしています。IPv4アドレスのみが許可されます。
- 単一のIPアドレスを使用することも、12.12.12.1/30などのサブネット マスクを含む範囲を使用することもできます。
- IPと範囲は検証されるため、サポートされていない項目についてはエラーが表示されます。
- **[Added By (追加者)]**フィールドは自動的に入力されます。

STEP 5 | **Save**（保存）を選択します。

変更はすぐに有効になるため、*IP*アドレスが正しいことを確認してください。*IP*アドレスが正しいと、テナントにアクセスできなくなる可能性があります。



STEP 6 | 親テナントに信頼できるIPリストを追加すると、そのリストは親テナントから子テナントに継承され、上から下へ適用されます。子テナントは独自の信頼できるIPリストを追加することもできます。

信頼できるIPの削除

どこで使用できますか?	何が必要ですか?
• Strata Cloud Manager	☐ スーパーユーザー、マルチテナントスーパーユーザー、マルチテナントIAM管理者のIAMロール、または「信頼できるIPリスト」パーミッションセットを持つカスタムロール

テナントの[Trusted IP List (信頼できるIPリスト)]に信頼IPを追加した後、信頼できるIPアドレスを削除すると、アクセス制限なしに戻すことができます。

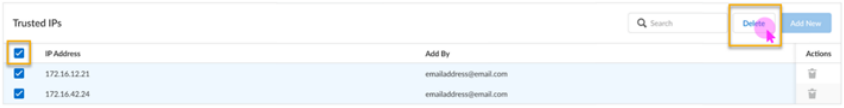
Strata Cloud Managerを使用して信頼できるIPを削除する。

STEP 1 | **[Settings (設定)] > [Trusted IP List (信頼できるIPリスト)]**を選択します。

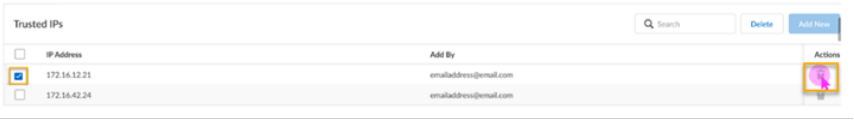
STEP 2 | 検索またはスクロールしてテナントを見つけて選択します。

STEP 3 | 以下のいずれかのオプションを使用します。

- 複数のIPを削除する – ［**IP Address (IP**アドレス**)**］チェックボックスをオンにして、すべてのIPアドレスを同時にハイライトしてから、［削除］ボタンを選択します。



- 単一のIPを削除する – IPの個別のチェックボックスをオンにしてから、［**Actions (**アクション**] > [Delete (**消去**)]**から削除します。



信頼できる*IP*リストを親テナントから継承した場合、子テナントからは継承されるため、子テナントから削除することはできません。信頼済み*IP*リストを子テナントから削除できるのは、子レベルで直接追加した場合だけです。

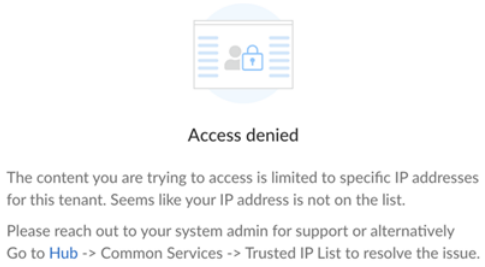
STEP 4 | プロンプトで**[OK]**を選択します。

変更はすぐに有効になります。信頼できるIPをすべて削除すると、IPアクセスは **Any (**何でも**)** に戻ります。

アクセスのロック解除

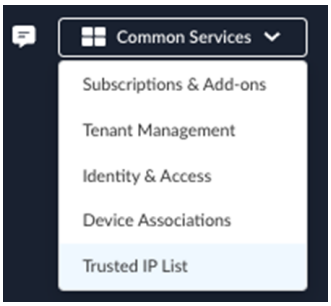
どこで使用できますか?	何が必要ですか?
• Strata Cloud Manager	❑ スーパーユーザー、マルチテナントスーパーユーザー、マルチテナントIAM管理者のIAMロール、または「信頼できるIPリスト」パーミッションセットを持つカスタムロール

テナントの信頼できるIPリストに信頼できるIPを追加すると、そのアクセスはStrata Cloud Managerによって強制されます。IPアドレスがテナントの信頼できるIPリストにない場合、アクセスしようとするとアクセス拒否メッセージが表示されます。

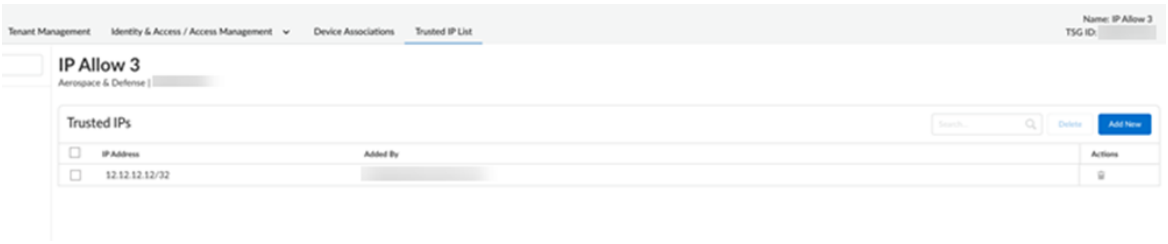


アクセス権を持つべきでIPアドレスがテナントからブロックされた場合は、hubにアクセスして、リストされたアクセス権があればアクセスをロック解除できます。

STEP 1 | [ハブのテナントビュー] > **[Common Services (共有サービス)]** > **[Trusted IP List (信頼できるIPリスト)]**を選択します。



STEP 2 | 信頼IPアドレスリストにIPアドレスを追加します。



設定:ユーザープリファレンス

どこで使用できますか?	何が必要ですか?
• Prisma Access (Managed by Strata Cloud Manager) • Strata Cloud Manager	次のいずれか ❑ AIOps for NGFW Freeまたはは AIOps for NGFW Premiumライセンス ❑ Strata Cloud Manager Essentials ❑ Strata Cloud Manager Pro

[Settings (設定)] > [User Preferences (ユーザープリファレンス)] で、ユーザープリファレンスを変更することで、特定のニーズに合わせてStrata Cloud Managerをカスタマイズできます。これらの設定には以下が含まれます。

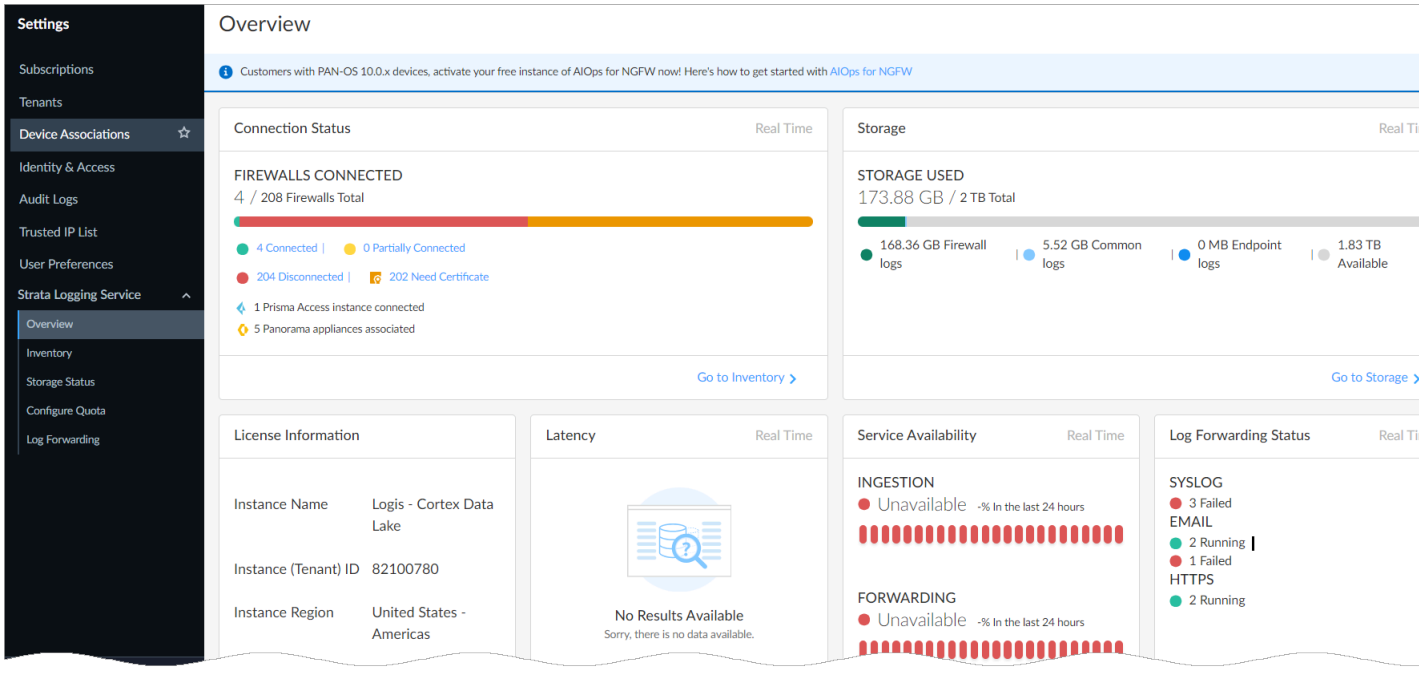
- ライト/ダーク/システムモード - ダークディスプレイモードとライトディスプレイモードのいずれかを選択するか、または独自のシステム設定に従うかを選択します。

設定:Strata Logging Service

どこで使用できますか?	何が必要ですか?
• Prisma Access (Managed by Strata Cloud Manager) • Prisma Access (Managed by Panorama) • NGFW (Managed by PAN-OS or Panorama) • NGFW (Managed by Strata Cloud Manager)	☐ Strata Logging Service

Strata Logging Service（旧称：Cortex Data Lake）は、当社のNGFW、Prisma Access、Cloud NGFW for AWSなどのセキュリティ製品によって生成されるコンテキストリッチな拡張ネットワークログを保存するクラウドベースのロギングシステムです。Strata Logging Serviceなら、ローカルコンピューティングとストレージの計画を立てることなく、増え続けるデータを収集でき、最初から拡張に対応できます。製品でアクティベートおよびStrata Logging Serviceをデプロイする方法を学びます。

さらに、ハブで利用できる*Strata Logging Service*アプリケーションでログにアクセスして管理することもできます。ログデータは、*Strata Logging Service*アプリケーションと*Strata Cloud Manager*の両方で同じですが、Webインターフェースの違いが異なります。



Strata Logging Serviceを使用して次のことを行います。

- Strata Logging Service インスタンスのステータスの確認 - ク-リック **Strata Logging Service** > 概要
- ビューとオンボーディング ファイアウォール、 Cloud NGFW、Prima Accessまたはは Panorama appliances - クリック **Strata Logging Service** > インベントリ
- 割り当てられたログストレージのクォータを表示する、利用可能なストレージ容量、およびログ受信率に基づくログの保持日数 - クリック**Strata Logging Service** > 容量ステータス
- 設定ログ保存クォータ- クリック **Strata Logging Service** > クォータの設定
- ログデータの検索、フィルタリング、エクスポート - クリック インシデントとアラート > ログビューア。ログビューアは、Strata Logging Serviceアプリケーションの Explore(探索)と同じ機能を備えています。
- 長期保存、SOC、内部監査のために外部サーバに ログデータを転送する - **Strata Logging Service** > **[Log Forwarding (ログ転送)]** をクリックします

アプリケーションエクスペリエンス

どこで使用できますか?	何が必要ですか?
• Prisma Access (Managed by Strata Cloud Manager)	❑ Prisma Accessライセンス ❑ ADEM ObservabilityライセンスまたはAI-Powered ADEMライセンス のいずれか

[Application Experience (アプリケーション エクスペリエンス)]ページは、自律型 DEMユーザーとリモートサイトの管理に使用します。監査ログを表示して、選択した**[Time Range (期間)]**にPrisma Accessの認証を受けた管理者を確認できます。

アップグレードオプションについては、「自律型DEM Agent アップグレードの管理」を参照してください。

エンドポイントエージェント管理

どこで使用できますか?	何が必要ですか?
• Prisma Access (Managed by Strata Cloud Manager)	❑ Prisma Accessライセンス ❑ ADEM ObservabilityライセンスまたはAI-Powered ADEMライセンス のいずれか

このタブを使用すると、登録済みのすべてのADEMユーザーに関する詳細を取得できます。取得出来る情報には以下が含まれます。ユーザーがオンライン（ユーザーデバイスがADEMサービスにキープアライブメッセージを送信している）かオフライン（ADEMサービスがユーザーデバイスからキープアライブメッセージを最後の10分間受信していない）か、ユーザーデバイスが最後に確認された日時、ADEMユーザーのユーザー名、デバイスタイプ、ホスト名、実行中のADEMエージェントのバージョンなど。

このタブの表の各行は、個別の行で一意のユーザーを表します。すべてのユーザー/デバイスの組み合わせは、一意のユーザーと見なされます。例えば、2人のユーザーがそれぞれ3台のデバイスにログインしている場合、ユニークユーザー数は6人になります。したがって、ログインしているデバイスの数によっては、ユーザー名が複数行にわたって重複する可能性があります。

このウィジェットの表のタイトルでは、［**Total Endpoint Agents (エンドポイントエージェント総数)**］ の数が監視対象のデバイスの総数を示します。ユーザー数は、ログインしているデバイスの数に関係なく、合計ユーザ数です。これは、各ユーザーがログインしているデバイスの数に関係なく、ライセンス消費量がユーザーの合計数に基づいているためです。

［**Last logged in User (最終ログインユーザー)**］ の左側にあるチェック ボックスを使用して、エンドポイントの行を選択して一括設定を行います。［Endpoint Agent Management (エンドポイ

ントエージェント管理)] テーブルからエントリを選択して削除すると、ライセンス エントリが解放されます。

列名	詳説
最後にログにしたユーザー	デバイスには、複数のユーザーがログインできます。この列には、このデバイスを使用してGlobalProtectにログインした最新のユーザーのユーザーIDが一覧表示されます。
デバイス	このデバイスで実行されているOS。
ホスト名	デバイスのホスト名。
最後に出現した日時	デバイスからDEMサーバに送信された最後のメッセージ。
初めて検出した日時	DEMサーバーがこのデバイスから受信した最初のメッセージ。
ユーザーの状態	現在のユーザーの接続ステータス。
モニタリング状態	デバイスでアプリテストが実行されているかどうか。
エンドポイントエージェントのバージョン	デバイスにインストールされているADEMエージェントのバージョン。

リモートサイトエージェント管理

どこで使用できますか?	何が必要ですか?
• Prisma Access (Managed by Strata Cloud Manager)	❑ Prisma Accessライセンス ❑ ADEM ObservabilityライセンスまたはAI-Powered ADEMライセンス のいずれか

このタブでは、デジタルエクスペリエンス管理に有効なブランチPrisma SD-WAN IONデバイスの詳細が表示されます。このタブでは、デバイスモデル、ホスト名、サイトステータス、監視状態 (サイトで監視が有効かどうか)、高可用性サーバのホスト名 (存在する場合)、リモートサイトエージェントのバージョンなど、登録されているすべてのADEMリモートサイトに関する詳細を取得できます。

列名	詳説
リモートサイト名	Pisma SD-WAN支店サイト。
デバイスモデル	Prisma SD-WAN IONデバイスのモデル番号。
ホスト名	IONデバイスのホスト名。
HAピアのホスト名	そのサイトで高可用性スタンバイIONデバイスが設定されているかどうか。
最後に出現した日時	IONデバイスからDEMサーバに送信された最後のメッセージ。
初めて検出した日時	DEMサーバがIONデバイスから受信した最初のメッセージ。
サイトの状態	サイトIONデバイスとDEMエージェントとの接続ステータス。
モニタリング状態	サイトがアプリケーションテストを実行するように設定されているかどうか。
リモートサイトエージェントのバージョン	IONデバイスにインストールされているADEMエージェントのバージョン。

ヘルススコアプロファイル

どこで使用できますか?	何が必要ですか?
• Prisma Access (Managed by Strata Cloud Manager)	❑ Prisma Accessライセンス ❑ ADEM ObservabilityライセンスまたはAI-Powered ADEMライセンス のいずれか

このタブにドメインの正常性スコアの詳細を表示します。

列名	詳説
ドメインヘルススコアメトリック名	ヘルススコアメトリックが計算されるドメインを一覧表示します。この列のドメイン名をクリックすると、下限と上限のしきい値、および数値がしきい値を超えたときに合計スコアにどの程度の影響（合計エクスペリエンス

列名	詳説
	スコアに対する割合）があるかなどの指標が表示されます。現在、これらのメトリックは管理者が設定した読み取り専用です。変更することはできません。
タイプ	ドメインの種類
関連ユースケース	計算されたエクスペリエンススコアが表示されるダッシュボードまたはウィジェット。

ADEM監査ログ

どこで使用できますか?	何が必要ですか?
• Prisma Access (Managed by Strata Cloud Manager)	❑ Prisma Accessライセンス ❑ ADEM ObservabilityライセンスまたはAI-Powered ADEMライセンス のいずれか

API呼び出しによってトリガーされるすべてのイベントの監査ログを表示します。

列名	詳説
イベント時間	ログを作成する原因となったイベントがトリガーされた時刻。
電子メール	ログ作成時に通知された人の電子メールアドレス。
詳説	イベントを発生させたAPI呼び出しによってログが作成されます。