BPA 和安全保证最佳实践入门

Version 9.1

docs.paloaltonetworks.com

techDOCS paloalto NETWORKS

Contact Information

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

About the Documentation

- To ensure you are viewing the most current version of this document, or to access 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

March 5, 2020

Table of Contents

最佳实践入门

安全最佳实践可防止已知和未知威胁，缩小攻击范围并提供流量可见性，从而了解和控制网络上的应用程序、用户以及内容。实施安全最佳实践时，您可以：

- 最大限度减少成功入侵的可能性。
- 确定攻击者的存在。
- 保护宝贵的数据。
- 保护客户、合作伙伴和员工，从而保护您的业务声誉。
- 帮助实现零信任安全环境。

要转移到安全最佳实践，首先需要了解当前的网络安全状况并确定需要改进的地方。Palo Alto Networks 提供指导性转移路径：最佳实践评估 (BPA) 与安全过渡步骤和最佳实践技术文档相结合。

如果您预订 Premium 版本（2019 年 11 月 1 日或之后）或 Platinum 支持合同，则有机会为安全保证做好准备。安全保证可让您获得 Palo Alto Networks 安全专家支持以及相应的工具，从而帮助您进行初步事件调查。

- 确定最佳实践并确定优先级
- 访问和运行 BPA
- 安全保证

确定最佳实践并确定优先级

Palo Alto Networks 的最佳实践评估 (BPA) 使用技术支持文件来分析 Panorama 和下一代防火墙配置设置，并将配置与 Palo Alto Networks 最佳实践进行比较。BPA 显示了最佳实践安全采用情况的当前状态，并建议进行特定更改，从而使配置符合安全最佳实践。运行 BPA 不仅可以让您了解如何改善安全状况，还设定了随后进行对比的基准，并提供了技术文档的链接，向您介绍如何将 BPA 的建议过渡为最佳实践配置。

利用迭代的优先级方法，逐步将安全状态转化为最佳实践状态，您可以按照自己的节奏和满意水平衡量进度：

STEP 1 | 将技术支持文件上传到客户支持门户并自行访问和运行 BPA，或者联系 Palo Alto Networks SE 销售代表或合作伙伴，以便在 Panorama 和/或新一代防火墙上运行 BPA。

如果您自行运行 BPA，我们建议您联系 Palo Alto Networks SE 或合作伙伴，以帮助解释结果和讨论后续步骤。

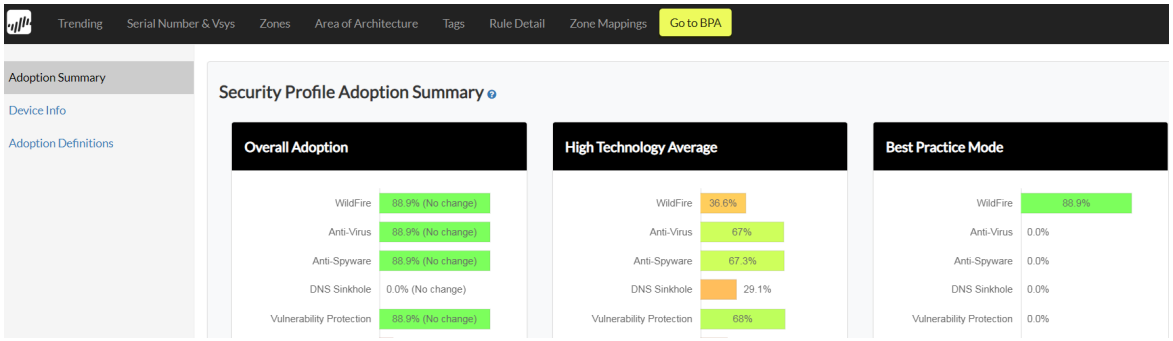
STEP 2 | 确定第一个改进区域并确定优先级，以便开始过渡至最佳实践。

不管是您的 Palo Alto Networks SE 或合作伙伴运行 BPA，还是您自行运行 BPA，您的 SE 或合作伙伴都可以帮助制定优先级计划，以便安全地分阶段实施最佳实践。计划先从最安全，最简单，影响最大的更改开始，例如将防病毒、反间谍软件、漏洞保护和 WildFire 分析配置文件应用到安全策略允许规则。

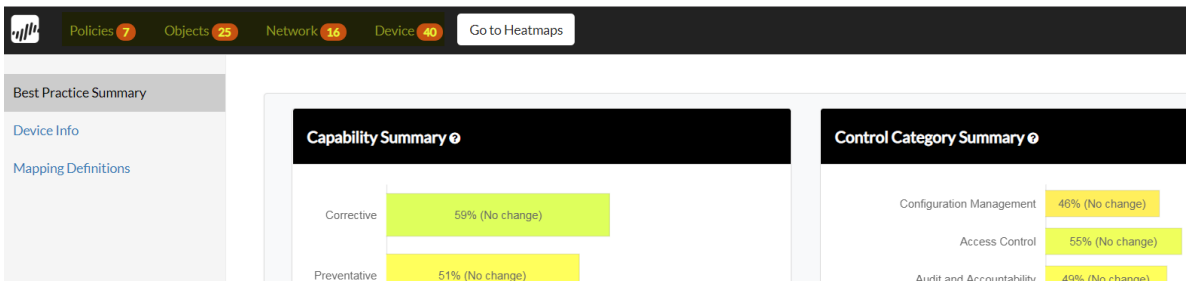
STEP 3 | 使用 BPA 的技术文档链接可配置优先考虑的最佳实践。

下载 BPA 报告可获得一个 .zip 文件，其中包含详细的 HMTL 报告、执行摘要和列出失败的最佳实践检查的 Excel 电子表格。通过两种方式可以链接到技术文档：

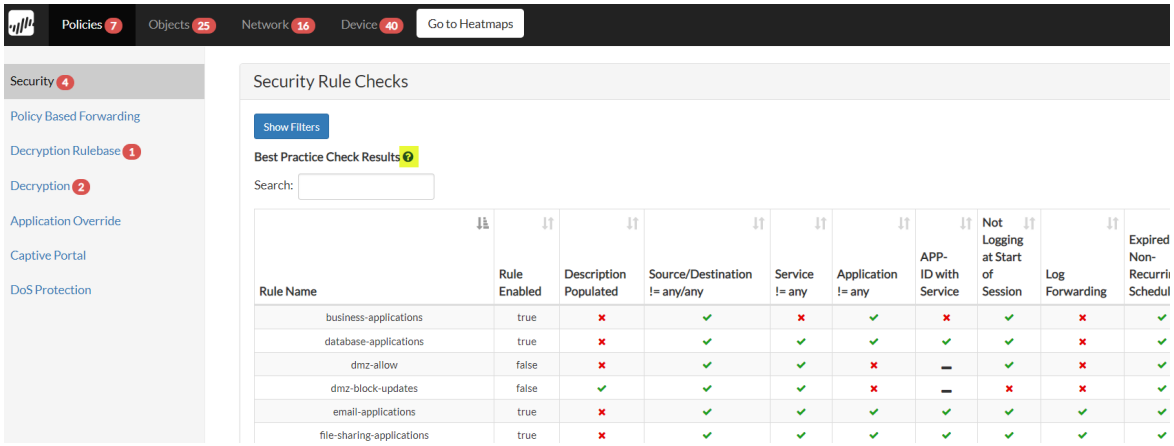
- 从电子表格 —“Documentation（文档）”选项卡提供了每个失败检查的链接。此外，“Policies（策略）”、“Objects（对象）”、“Network（网络）”和“Device（设备）”选项卡的“Check ID（检查 ID）”列中的标识号也直接链接到“Documentation（文档）”选项卡中的相关行。
- 从 HTML 报告 — 打开 HTML 报告时，您会看到一个总结最佳实践采用情况的热图。**Go to BPA**（转到 **BPA**）以访问报告。



在 BPA 摘要页面上，请查看所选配置评估的 **Policies**（策略）、**Objects**（对象）、**Network**（网络）或 **Device**（设备）详细报告。



在详细报告中单击带圆圈的蓝色？，了解关于配置检查的说明和基本原理，并获得最佳实践配置的技术文档链接。



对于安全配置文件（漏洞保护、防病毒、反间谍软件、URL 筛选，文件阻止），在迁移至最佳实践安全配置文件时，请按照安全转换建议确保业务关键型应用程序的可用性。

STEP 4 | 实施第一组最佳实践更改后，再次运行 BPA 以测量进度并帮助验证更改是否按预期工作。

将第一次的 BPA 输出与下一次的 BPA 输出对比可查看安全状况的改进程度。确定下一个改进区域并确定优先级。

STEP 5 | 使用 BPA 的技术文档链接来配置优先考虑的下一组最佳实践。

STEP 6 | 按照自己的节奏，重复执行运行 BPA 的过程可测量进度并确定后续步骤的优先级，然后使用技术文档配置最佳实践。

STEP 7 | 现在就开始 — 访问和运行 BPA 或联系 Palo Alto Networks SE 或合作伙伴，立即开始转化至更安全的网络！

访问和运行 BPA

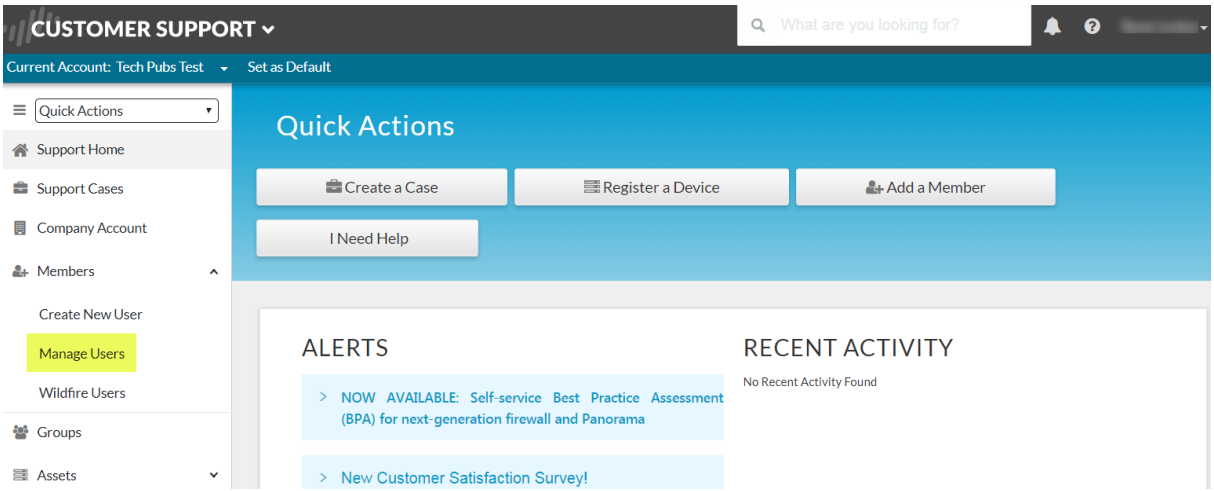
从客户支持门户获取最佳实践评估 (BPA)。超级用户帐户自动具有 BPA 访问权限，并且可以将 *BPA* 用户角色分配到标准用户的配置文件，从而使标准用户可以运行 BPA。本过程向超级用户展示如何授予标准用户访问权限以及如何运行 BPA。您还可以查看短视频如何运行 BPA以及如何理解结果。

此外，如果您预订 Premium 版本（2019 年 11 月 1 日或之后）或 Platinum 支持合同，则有机会准备和激活安全保证。安全保证可让您获得 Palo Alto Networks 安全专家支持以及相应的工具，从而帮助您进行初步事件调查。我们强烈建议您运行 BPA 来衡量采用的七个关键安全功能，并确保采用率至少已达到行业平均水平，让您的网络得到更完善的保护。Premium 或 Platinum 支持合同，以及显示七个关键安全功能采用率符合行业平均水平的最新 BPA 衡量指标可自动激活安全保证。

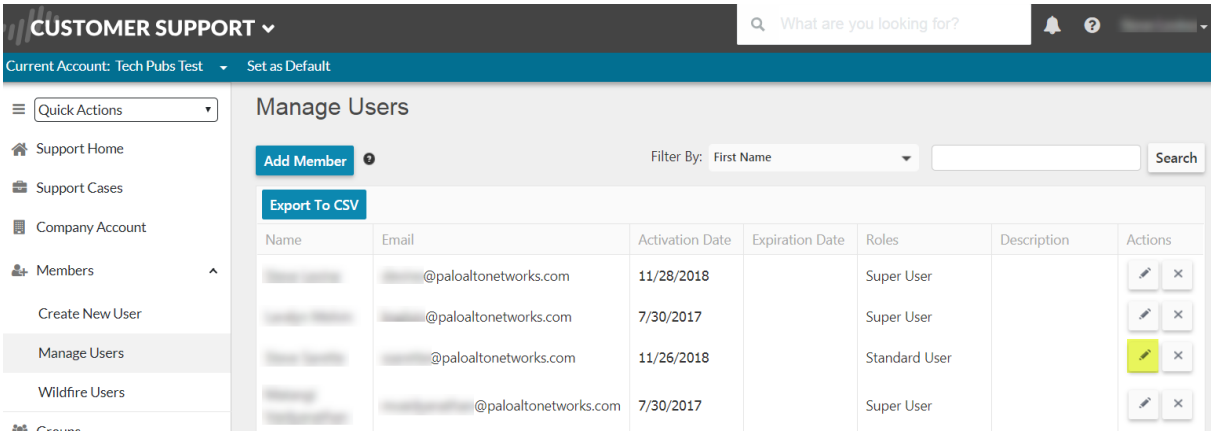
- 从客户支持门户访问 BPA
- 生成和下载 BPA 报告

从客户支持门户访问 BPA

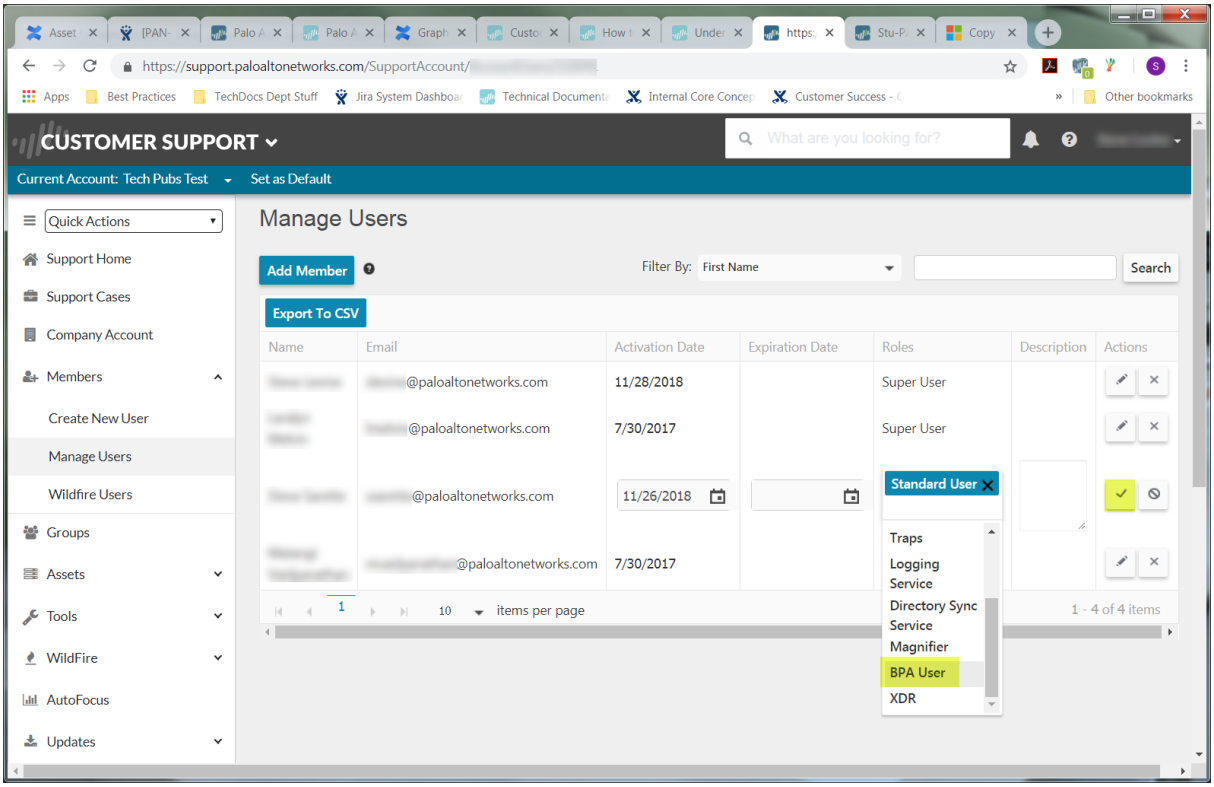
STEP 1 | 在客户支持门户的身份验证主屏幕上，选择 **Members**（成员）> **Manage Users**（管理用户）。



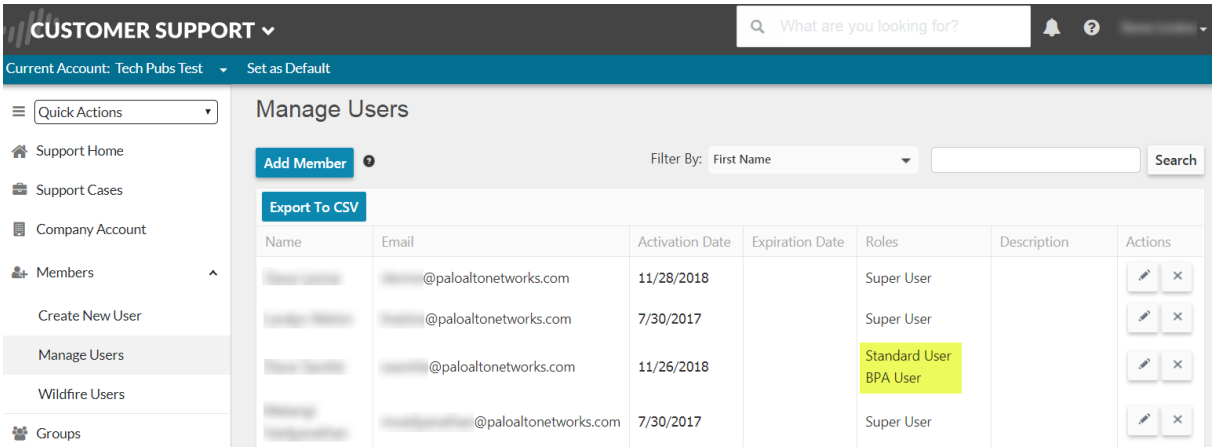
STEP 2 | 单击铅笔图标可编辑要为其分配 BPA 权限的标准用户。



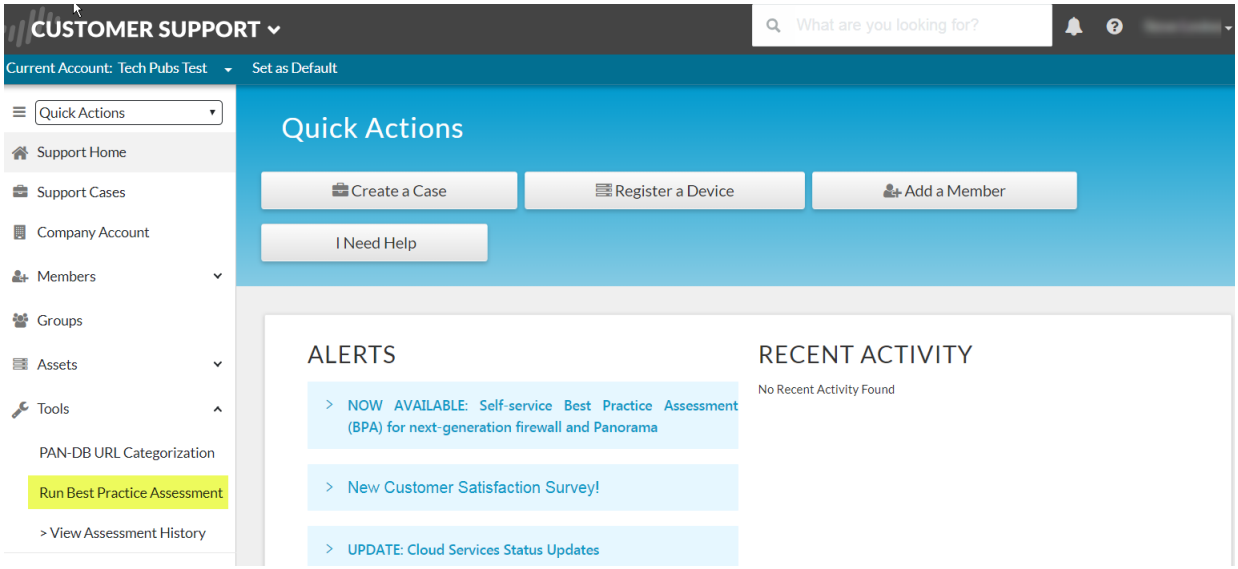
STEP 3 | 选择 **BPA User**（**BPA** 用户）角色，然后单击更新复选标记以添加新角色。



STEP 4 | 现在，标准用户已获得 BPA 用户角色的权限。



STEP 5 | 具有 BPA 用户角色的超级用户和标准用户可以登录到客户支持门户，以访问和运行 BPA（**Tools**（工具）> **Run Best Practice Assessment**（运行最佳实践评估））。



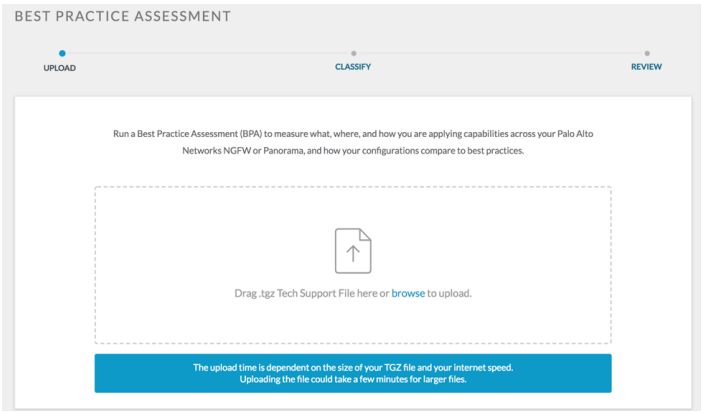
生成和下载 BPA 报告

获得 BPA 访问权限后，您可以为 Panorama 设备或新一代防火墙生成 BPA 报告。

如果可能，请为 *Panorama* 设备（而不是单个新一代防火墙）生成 *BPA* 报告，以便在一份报告中获得对环境中所有防火墙的全面可见性。定期生成报告以衡量采用安全功能和安全最佳实践的进度。

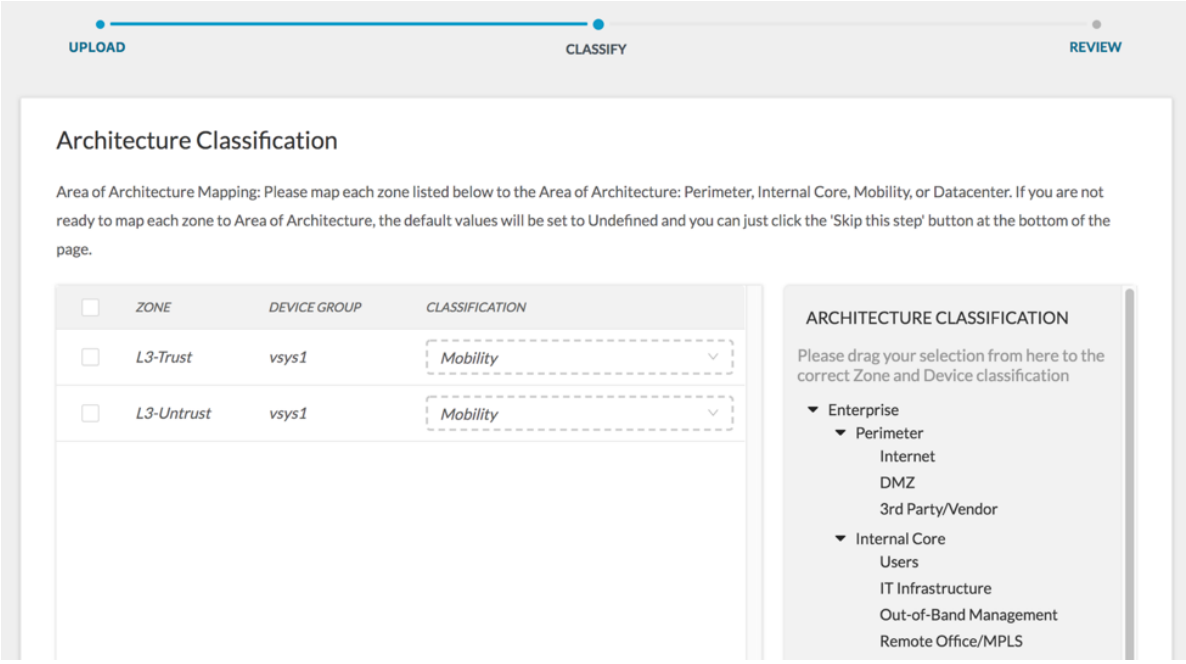
STEP 1 | 在客户支持门户窗口中拖放一个技术支持文件 (.tgz file)，或浏览到技术支持文件。

超级用户可以创建技术支持文件（**Device**（设备）> **Support**（支持）> **Tech Support File**（技术支持文件）或 **Panorama** > **Support**（支持）> **Tech Support File**（技术支持文件））。



STEP 2 | （可选）将每个区映射到架构区域，或单击 **Skip this step**（跳过此步骤），从而在没有映射区域的情况下运行 BPA。

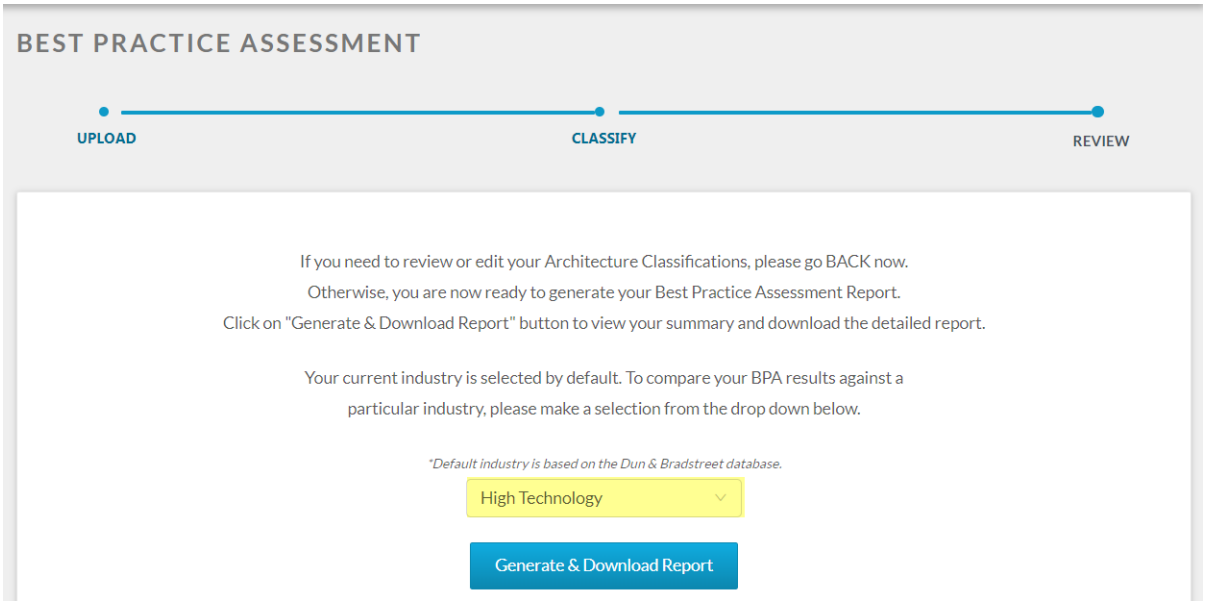
从架构分类拖放架构值，使用 **Classification**（分类）下拉列表中选择一个值，或者选中多个复选框以选择多个区域，然后一次性将值应用到全部选定区域。



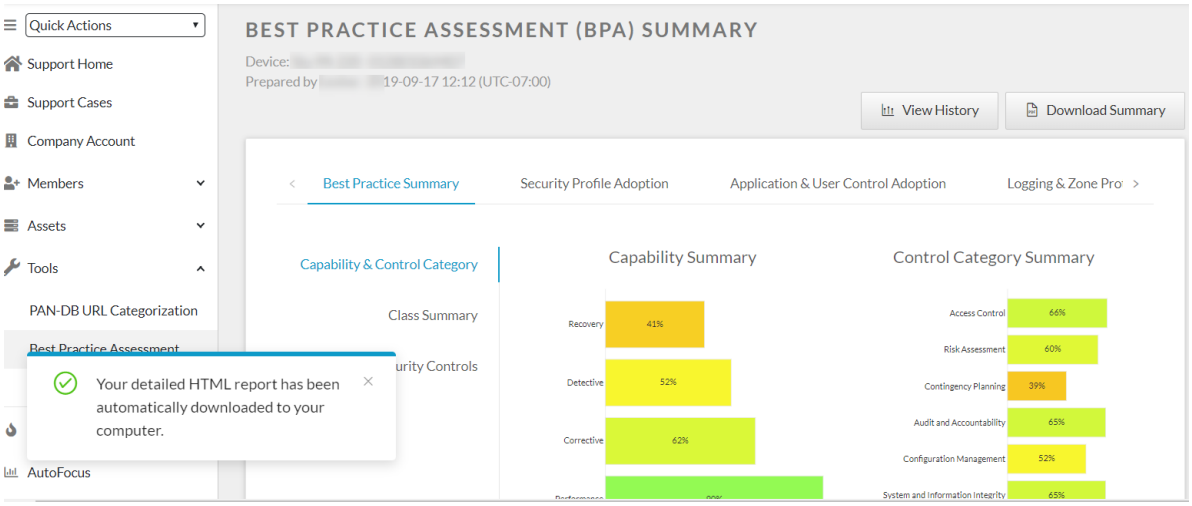
STEP 3 | 确定与您的帐户对应的行业，然后生成并下载 BPA 报告（**Generate & Download Report**（生成和下载报告））。

您可以使用下拉列表更改行业，从而通过 BPA 与其对比您的结果。如果要在生成报告之前更改任何设置，您可以返回并执行更改。

通过 **Generate & Download Report**（生成和下载报告）可以下载详细的 BPA 报告、执行摘要报告，以及一个显示系统的失败最佳实践检查的电子表格。从该表格可以访问和运行 BPA。



STEP 4 | 生成的 BPA 显示执行摘要，并告知已将详细的 HTML 报告下载到您的计算机。



STEP 5 | 现在，您已经了解了如何运行 BPA，请转到客户支持门户并立即尝试（或联系 Palo Alto Networks SE 或合作伙伴以运行 BPA），从而开始转换到更安全的网络。

如果订阅 *Premium* 版本（*2019* 年 *11* 月 *1* 日或之后）或 *Platinum* 支持合同，请使用 *BPA* 准备您的安全状况，以便利用安全保证，从而帮助您进行初步事件调查。

安全保证

如果在网络中检测到可以活动，在您最需要时，安全保证会通过 Palo Alto Networks 提供额外的帮助。安全保证提供：

- 获得 Palo Alto Networks安全专家的帮助及其专业的威胁情报工具和威胁追踪实践。
- 高级日志和入侵指标 (IOC) 分析。
- 包括自定义产品安全建议的配置评估。
- 加速过渡至事件响应 (IR) 供应商来帮助您管理和解决事件的下一步建议。

为了利用安全保证，必须订阅 Premium 支持合同（2019 年 11 月 1 日或之后）或 Platinum 支持合同。

安全保证的第一步是执行最佳实践评估 (BPA) 来测量对七个关键安全功能的采用：WildFire、防病毒、防间谍软件、DNS Sinkhole、URL 筛选、漏洞保护和日志记录。建议您确保这些安全功能的采用率至少达到行业平均水平。

执行 BPA 并采用更高级别的关键安全功能可以为您的网络提供更完善的保护，而且有助于避免事件。BPA 还会衡量许多其他安全功能的采用水平，如 App-ID 和 User-ID、区域配置，以及其他安全配置文件，如文件阻止和 DoS 保护配置文件，同时，BPA 会提供关于如何改进安全状态的建议。

定期运行 *BPA*（例如，每月或每季度）来衡量关键安全功能的采用率，了解网络安全状态，并确定安全改进的优先级。

订阅 Premium 支持合同（2019 年 11 月 1 日或之后）或 Platinum 支持合同并运行 BPA，如果它显示您的七个关键安全功能的采用率已达到行业平均水平，则会自动启用安全保证。为了达到行业平均水平，如果您在采用这些主要功能时需要协助，请联系 Palo Alto Networks 销售代表，从而帮助您定义要求，提供评价标准等。如果由于业务原因，导致您的关键安全功能的采用率无法达到此水平，请与 Palo Alto Network 销售代表合作，确定如何获得安全保证的优势。

要采用的七个关键安全功能

我们强烈建议采用以下七个关键安全功能，原因如下：

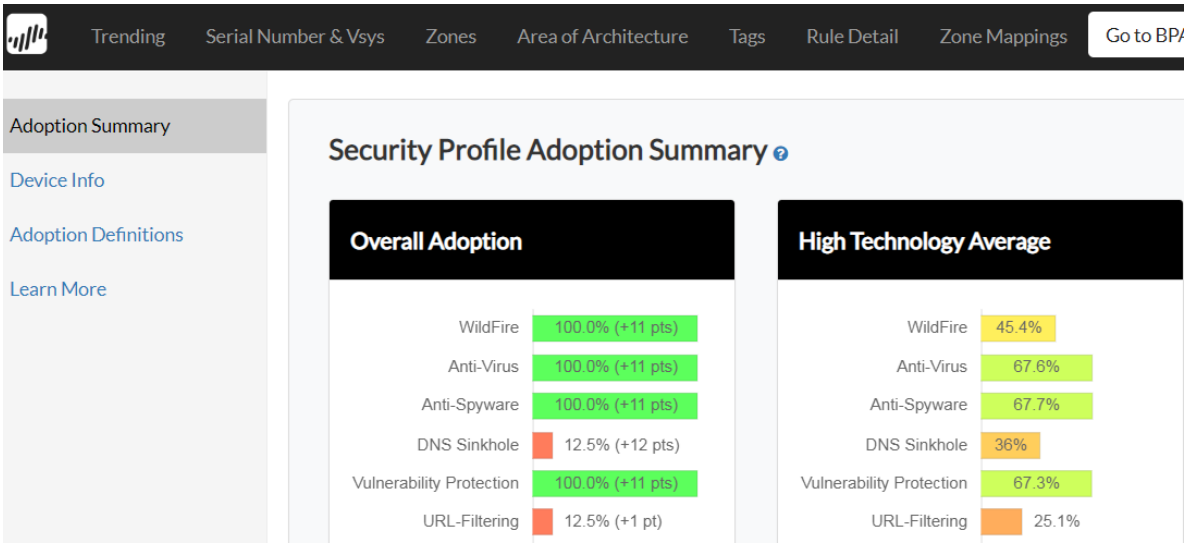
- **WildFire** — 将 WildFire 安全配置文件附加到允许流量的安全策略规则，从而保护您的网络，防御新的未知威胁。WildFire 是一款可以防御高级持久性威胁 (ATPs) 的强大防御工具。
- 防病毒软件 — 将防病毒软件安全配置文件附加到允许流量的安全策略规则，从而阻止未知恶意文件，如恶意软件、勒索软件、蠕虫和病毒。
- 防间谍软件 — 将防间谍软件配置文件附加到允许流量的安全策略规则，从而检测在服务器或端点上运行的恶意代码发起的命令和控制 (C2) 流量，并阻止遭到入侵的系统在您的网络中建立出站连接。
- **DNS Sinkhole** — 配置附加到允许流量的安全策略规则的防间谍软件安全配置文件的 DNS Sinkhole 部分。DNS Sinkhole 通过跟踪主机来识别尝试访问可疑域名的潜在受影响主机，从而防止这些主机访问可疑域名。
- **URL** 过滤 — 将 URL 过滤配置文件附加到允许流量的安全策略规则，从而阻止访问高风险 Web 内容（以及可能包含恶意内容的站点）。通过 URL 过滤配置文件和 URL 类别，您可以精确控制允许访问的网站类别。
- 漏洞防护 — 将漏洞防护安全配置文件附加到允许流量的安全策略规则，从而阻止攻击者利用客户端和服务器端安全漏洞来将恶意负载传送到您的网络和用户，同时阻止攻击者利用安全漏洞在您的网络中横向移动。

- 日志记录 — 对所有流量启用日志记录（允许和拒绝），从而为系统事件和网络流量事件提供带时间戳的审核线索。日志可以为事件调查提供关键信息。日志转发可让您将所有防火墙的日志发送到 Panorama 或外部，并在汇总后进行分析。

采用这些关键安全功能可以大大改善您的安全状态，缩小攻击范围，提高对网络流量的可见性，阻止已知的和新的攻击，同时保护对您的网络上最宝贵的数据、资产、应用程序和服务。

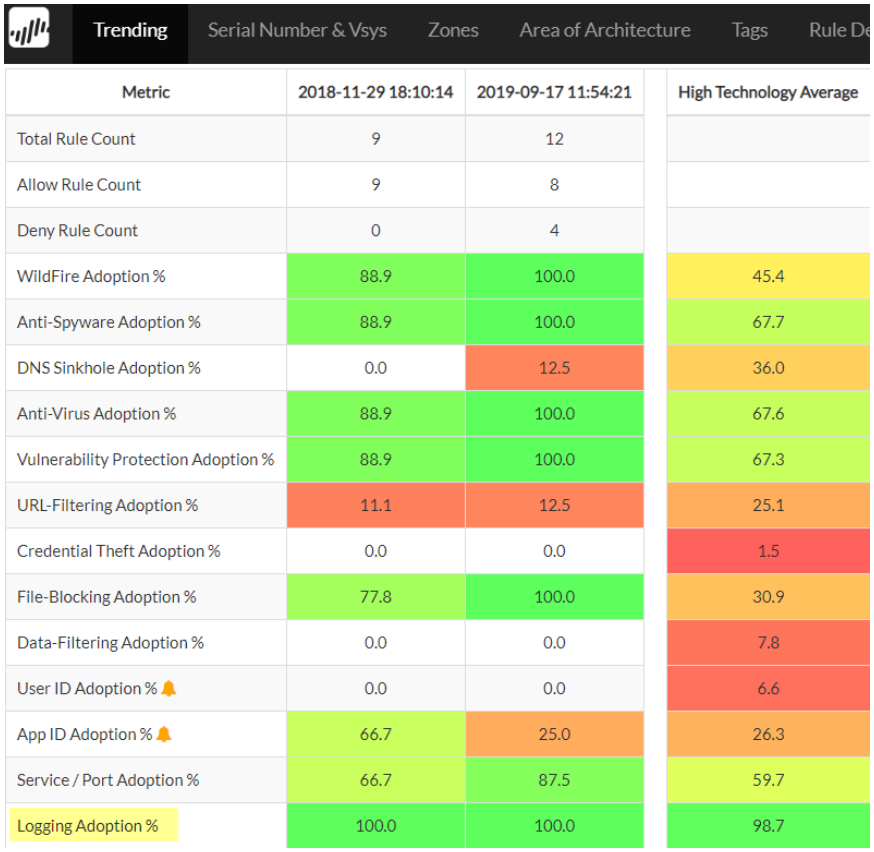
检查七个关键安全功能的采用率

在生成和下载 BPA 结果时收到的详细 BPA 报告（HTML 格式）中，请转到采用率摘要页面，检查六个安全配置文件（WildFire、防病毒软件、防间谍软件、DNS Sinkhole、漏洞防护和 URL Filtering）功能的综合采用率，以及您的行业对这些功能的平均采用率（日志记录需要单独检查）。采用率摘要页面会显示您的安全功能采用率与行业平均采用率的对比信息，帮助您确定采用率差距。例如，如果您属于高科技行业：



结果表明四个功能的配置符合行业平均采用率水平：WildFire、防病毒软件、防间谍软件和漏洞防护配置文件。结果还表明两个功能的配置未达到行业平均采用率水平：DNS Sinkhole 和 URL 过滤。这说明要采取下一步行动：在防间谍软件配置文件中配置 DNS Sinkhole 并将 URL 过滤应用到 Internet 流量。

在详细的 HTML BPA 报告中，请转到 **Trending**（趋势）页面，以便检查您的日志记录功能综合采用率和您的行业的日志记录平均采用率。



Metric	2018-11-29 18:10:14	2019-09-17 11:54:21	High Technology Average
Total Rule Count	9	12	
Allow Rule Count	9	8	
Deny Rule Count	0	4	
WildFire Adoption %	88.9	100.0	45.4
Anti-Spyware Adoption %	88.9	100.0	67.7
DNS Sinkhole Adoption %	0.0	12.5	36.0
Anti-Virus Adoption %	88.9	100.0	67.6
Vulnerability Protection Adoption %	88.9	100.0	67.3
URL-Filtering Adoption %	11.1	12.5	25.1
Credential Theft Adoption %	0.0	0.0	1.5
File-Blocking Adoption %	77.8	100.0	30.9
Data-Filtering Adoption %	0.0	0.0	7.8
User ID Adoption %	0.0	0.0	6.6
App ID Adoption %	66.7	25.0	26.3
Service / Port Adoption %	66.7	87.5	59.7
Logging Adoption %	100.0	100.0	98.7

该页面不仅会显示您的采用率水平与行业平均水平的对比，还会显示您的采用率水平与上次运行 BPA 时的水平的对比。这是一种随着时间的推移而改进的安全措施，如果结果表明您的安全状态并没有您想要的那样完善，那么也是一种行动号召。

如果配置文件和日志记录结果表明您所有七个功能的采用率符合行业平均水平，则会自动启用安全保证。为了达到行业平均水平，如果您在采用这些主要功能时需要协助，请联系 Palo Alto Networks 销售代表，从而帮助您定义要求，提供评价标准等。如果由于业务原因，导致您的关键安全功能的采用率无法达到此水平，请与 Palo Alto Network 销售代表合作，确定如何获得安全保证的优势。

改善七个关键安全功能的采用率

将 BPA 与 Palo Alto Networks 技术文档结合使用，从而确定需要改善的安全功能并进行需要的改善，尤其是这七个关键安全功能。改善安全状态可以帮助您保护用户和您的宝贵设备、资产、应用程序和服务。

- **WildFire** — 安全地将 WildFire 配置文件过渡至最佳实践，然后实施 WildFire 最佳实践。最佳实践 WildFire 配置文件是默认配置文件。
- 防病毒软件 — 安全地将防病毒配置文件过渡至最佳实践，然后实施防病毒最佳实践（或相对而言略加严格的数据中心防病毒最佳实践）。
- 防间谍软件和 **DNS Sinkhole** — DNS Sinkhole 配置位于防间谍软件安全配置文件的 **DNS Signatures**（**DNS** 签名）选项卡上。将防间谍软件配置文件安全过渡到最佳实践，然后实施防间谍软件最佳实践（或相对而言略加严格的数据中心防间谍软件最佳实践）。
- **URL** 过滤 — 安全地将 URL 过滤配置文件过渡到最佳实践，然后实施 URL 过滤最佳实践。
- 漏洞防护 — 安全地将漏洞防护配置文件过渡到最佳实践，然后实施漏洞防护最佳实践（或相对而言略加严格的安全中心漏洞防护最佳实践）。
- 日志记录 — 默认情况下，安全策略规则在会话结束时记录日志。

此外，BPA 和技术文档显示如何改善许多其他安全功能，如 App-ID、User-ID、文件阻止配置文件、DoS 和区域保护以及凭据窃取保护。一些主要资源包括：

- BPA 入门 — 介绍如何利用 BPA 来审查安全功能的采用率和识别采用率差距，评估您的配置（包括策略、对象、网络和设备以及 Panorama 配置），以及确定更改优先级，包括加强设备管理状态，改善流量可见性和实时初步最佳实践控制。
- 解密最佳实践 — 介绍如何通过解密您的业务模型、隐私考虑和法规允许的所有流量来提高可见性，从而让您可以检查最大流量和为您的网络访问加密威胁。
- DoS 和区域保护最佳实践 — 介绍如何利用分层方法防范试图破坏您的网络的拒绝服务 (DoS) 攻击，并保护您的网络周边、区域和个人设备。
- 应用程序和威胁内容更新最佳实践 — 根据您的业务要求，以最佳方式部署内容和应用程序更新，确保为您的网络防范最新威胁并识别最新应用程序。

通过最佳实践门户和向最佳实践过渡页面可以找到所有这些文档和其他许多资源。

如何寻求安全保证

如果遇到可疑活动，当您寻求安全保证时，必须提供一组有关关于可疑事件的具体数据，以便 Palo Alto Networks 的专家调查该活动。

- 寻求安全保证前要收集的数据
- 寻求安全保证

寻求安全保证前要收集的数据

Palo Alto Networks 的专家至少需要关于可疑活动的以下信息才能开始诊断潜在问题。请在寻求安全保证之前先收集这些数据。

关于可疑活动的基本详细信息：

- 可疑攻击向量和类型：哪些可疑活动的证据提醒了您的管理或响应团队？
- 时间线：
  - 如果知道，提供初始可疑攻击的日期和时间。
  - 确定潜在问题的时间。
- 事件详细信息：
  - 受影响系统的已知 IP 地址。
    - 通过 NAT 公开可用的受影响主机的 IP 地址。
    - 可能使一个或多个系统成为目标的关键服务，例如，数据库、Web 服务、远程访问（RDP、Citrix 等）服务器。
  - 可能与攻击相关的已知或可疑 IP 地址。
  - 遭到泄露的用户帐户的用户 ID（如果有）。
- 拓扑图或概括信息：防火墙相对于受影响主机的位置。（不需要完整网络拓扑图。）
- 恶意软件和入侵指标：
  - 样本。
  - 哈希。

防火墙数据：

- 技术支持文件：
  - 从防火墙上生成并上传技术支持文件，即可疑活动发生时在潜在受影响的设备路径下产生的文件。
  - 如果使用 Panorama 管理防火墙，则生成并上传 Panorama 技术支持文件。
- 防火墙日志：从防火墙和 Panorama 设备导出发生可疑活动之前两小时的日志。导出日志之前，请验证 CSV 行设置的值至少为 65535 行（**Device**（设备）> **Setup**（设置）> **Management**（管理）> **Logging and Reporting Settings**（日志记录和报告设置））。如果该值较小，请将其增大到最大 65535 行。如果已启用日志，根据 IP 地址信息和时间戳详细信息为以下每个基本日志类别导出日志（您可以过滤日志以根据 IP 地址和事件来显示条目）：

- 数据过滤日志
- 流量日志
- 威胁日志
- URL 过滤日志
- User-ID 日志（如果您怀疑涉及横向移动）
- WildFire 提交日志

务必了解部署的日志保留策略和日志保留能力，以确保不检查不相关的数据。管理员可能需要执行其他操作，例如从防火墙或其他日志服务器导出数据，从而确保调查期间数据的连续性和完整性。

更多识别可疑活动有意义的数据的方法：

- 使用应用程序命令中心 (ACC)。ACC 可以显示发生可疑活动之前、期间和之后的流量峰值、异常以及变化。
- 利用威胁监控报告查看发生可疑活动之前、期间和之后的一段时间内的主要威胁。

寻求安全保证

收集关于可疑活动的数据以确保及时分析相关信息后，您就为寻求安全协助做好了准备。您可以通过两种方式寻求安全协助：

- 登录到客户支持门户。点击 **Create a Case**（创建案例）以开立支持案例。填写该表单时，请选择 **Threat**（威胁）。
- 您的销售工程师 (SE) 可以代表您开立支持案例。