Palo Alto Networks

确保今天的安全，共创美好的明天

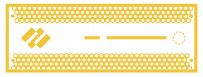
Palo Alto Networks 不仅能够为数字企业提供当下所需的网络安全服务，还能为日后的工作打好安全基础，让企业无需在二者间权衡和纠结，这样的网络安全合作伙伴仅此一家。我们承诺将双管齐下，在保障数字企业的安全方面绝不妥协退让。

下面将介绍我们如何为您提供保护。

STRATA
BY PALO ALTO NETWORKS

Strata

立刻保护您的企业免受未来威胁。通过 Palo Alto Networks 的智能网络安全保护任何地方的用户、应用和数据。


新一代防火墙

PA-Series

VM-Series

CN-Series


App-ID


Content-ID


User-ID


Device-ID

Panorama

DNS Security

企业 DLP

Threat Prevention

URL Filtering

WildFire

IoT Security

GlobalProtect

5G 安全

SD-WAN

新一代防火墙

物理、虚拟以及云交付的保护方式

将多个互不相关的安全产品整合到一个简单的网络安全解决方案中，放心拥抱数字化转型。基于机器学习的新一代防火墙 (NGFW) 是一个统一、集成且一流的网络安全解决方案，采用集中管理的物理、虚拟、容器化以及基于云的形式交付。行业首款基于机器学习的新一代防火墙能够阻止未知威胁，面向所有网络环境（包括物联网）进行安全监测并提供保护，同时利用自动化策略推荐减少错误。我们已连续九年当选 Gartner 网络防火墙魔力象限的领导者，为您的园区、混合云、分支机构以及移动用户提供强大的安全保护。

PA-Series

物理新一代防火墙

PA-Series 物理新一代防火墙专为使用多个高速接口进行高性能的安全处理，以便实现最大吞吐量的目标而设计。PA-Series 新一代防火墙为数据中心、园区边界、分支机构、工业装置和移动 5G 基础设施提供对企业网络流量（包括物联网和 5G 流量）的可视性、安全保护和控制力。

VM-Series

虚拟新一代防火墙

在难以或无法部署硬件防火墙的环境中，使用 VM-Series 虚拟新一代防火墙是最理想的选择。VM-Series 防火墙以虚拟形式提供 Palo Alto Networks 新一代防火墙的全部功能，它具有内联网络安全和高级威胁防御功能，能够为公有云、私有云、虚拟化数据中心和分支机构提供一致的保护。

CN-Series

容器新一代防火墙

CN-Series 容器新一代防火墙以容器形式提供 Palo Alto Networks 新一代防火墙的全部功能，旨在使安全控制措施尽可能贴合容器工作负载的需要，并获得制定安全策略所使用的关键容器情境。因此，CN-Series 防火墙可以对容器 pod 之间以及容器应用和传统工作负载（如虚拟机和裸机服务器）之间允许通过的流量（无论是出站、入站还是横向流量）执行威胁防御和其他高级网络安全服务，如 IPS 和 URL 过滤。

App-ID

应用分类功能

App-ID™ 是获得专利的流量分类计数，仅在 Palo Alto Networks 防火墙上提供。不论应用使用什么端口、协议、TLS/SSL/SSH 加密方式（包括 TLS 1.3 和 HTTP/2）或任何其他规避策略，它都可以识别应用的身份。它将应用签名、应用协议解码和启发式等多种分类机制应用到您的网络流量流，以准确识别应用。系统识别应用后，策略检查便会让您确定如何处理该应用。例如，您可以阻截应用；允许应用启动并进行威胁扫描；检测未授权的文件传输和数据模式；或者使用 QoS 进行加工。从基于端口的传统防火墙规则转变为基于 App-ID 技术的防火墙规则，极大地降低了遭受攻击的可能性。Policy Optimizer 是 PAN-OS® 中的一项功能，通过使用简单的工作流和 PAN-OS 收集的情报，可以将传统规则轻松转变为基于 App-ID 的控制，从而增强安全防护效果。

Content-ID

内容分类功能

您可以通过 Content-ID™ 技术来利用多项先进的威胁防御技术，在单次扫描中对所有允许的流量进行全面分析。借助 Content-ID 技术，我们的新一代防火墙能够阻截漏洞利用、缓冲区溢出并进行端口扫描；还能防止攻击者使用规避和混淆方法。我们云交付的安全服务（例如 Threat Prevention 和 URL Filtering）利用 Content-ID 阻截出站恶意软件通信，阻截对已知恶意软件和网络钓鱼下载站点的访问，并降低与传输未经授权的文件和数据相关的风险。使用 Content-ID 技术可以在一次网络流量扫描中实现全面的威胁防御，从而优化新一代防火墙的性能。

User-ID

用户分类功能

User-ID™ 技术可帮助定义策略，这些策略在出站或入站方向上基于用户或用户组安全启用应用。例如，您可以只允许 IT 部门在标准端口上使用 SSH、telnet 和 FTP 工具。应用 User-ID 技术后，无论用户身在何处（总部、分支机构或家中）或使用何种设备，策略将始终适用于用户。您不仅可以按 IP 地址了解用户级别的应用活动，还能够生成关于用户活动的信息性报告。此外，您无需对应用进行任何更改，便可针对用户执行多重身份验证 (MFA)。

您可以使用 User-ID 技术防止公司凭证外泄，并阻止攻击者使用遭窃取的凭证在您的网络中横向移动。通过使用动态用户组 (DUG)，无论是出现新的威胁指标还是有新的业务需求（例如为一组用户授予临时访问权限），管理员都可以动态更改用户访问权限或执行 MFA。

Device-ID

设备分类功能

Device-ID™ 是一种新的策略结构，让管理员可以根据设备特征编写策略。它让安全团队可以了解事件与设备的关系，并根据设备编写策略，而不是根据随时间变化的 IP 地址或位置来编写。借助 Device-ID，我们的新一代防火墙可以采取限制措施，仅针对物联网设备执行已知的良好行为、在网络中阻截使用过时操作系统的设备、快速跟踪单个设备中的威胁，并将“设备”用作其他策略类型的维度。您可以在安全、解密、服务质量 (QoS) 以及身份验证策略中使用 Device-ID。Device-ID 在 Panorama 和运行 PAN-OS 10.0 或更高版本的所有基于机器学习的新一代防火墙（VM-50 和 CN-Series 除外）中可用。

Panorama

管理解决方案

Panorama™ 可为任何形式和地点的所有 Palo Alto Networks 防火墙提供集中式网络安全管理解决方案。它通过简化安全策略的配置、部署和管理，降低了安全工作的复杂性。Panorama 可提供对网络流量、日志和威胁的集中可视性和全面洞察。它通过辅助管理更新，借助基于策略的操作实现自动化的威胁响应，并使用与第三方系统进行的基于 API 的集成，降低了管理工作负担。

网络安全团队可重新了解并控制其安全状况，整合工具并使网络安全防护实现自动化。Panorama 可以管理规则和动态安全更新，因此，您可以有效应对不断升级的网络威胁。您可通过有效管理软件更新来简化操作，自动计划内容更新，从而尽可能维持最佳的整体安全状况。借助单一管理解决方案，您可以充分利用一个平台中的所有安全投资功能和附加的订阅服务。

DNS Security

防御使用 DNS 的攻击

80% 的恶意软件使用 DNS 建立命令和控制 (C2) 通道。由于流量过高，许多企业都缺少可恰当监控流量的工具，导致攻击者通常隐藏在 DNS 中。为了防御 DNS 中的威胁，需要具备出色的检测和分析功能，这些功能可为安全人员快速有效地制定策略和响应威胁提供所需的情境。我们的 DNS Security 服务应用预测分析、机器学习和自动化来阻截利用 DNS 发动的攻击。通过与新一代防火墙紧密集成，您可以获得自动化防护，防止攻击者绕过安全措施，而且无需独立工具或对 DNS 路由进行更改。您可以快速预测并拦截恶意域，使隐藏在 DNS 隧道中的威胁失效，并应用自动化以快速查找并控制受感染设备。

DNS Security 报告让您能够比以往更深入地了解威胁，在宏观、行业及企业级别获得 DNS 流量的完整可视性。基于云的防护可得到无限扩展并始终保持最新状态，您的企业可以利用这一关键的全新控制点阻止使用 DNS 的攻击。为实时保护 DNS，Palo Alto Networks 将一流的检测功能与分析和内联执行结合在一起。

企业数据丢失防护

数据保护和合规性

Palo Alto Networks 企业数据丢失防护 (DLP) 可以发现每个网络、云中以及用户的敏感数据（例如个人身份信息 (PII) 和知识产权 (IP)）并进行监控和保护，是行业首款云交付的安全服务。使用单一云服务和预定义的策略，无论是在本地、针对远程工作人员还是在云中，都可以轻松、一致地实现数据隐私和合规性。与复杂的传统 DLP 产品相比，我们的企业 DLP 原生集成到了现有的 Palo Alto Networks 控制点，使 TCO 大幅降低了三成，简化了部署和维护工作，同时无需使用额外的基础架构。

Threat Prevention

漏洞利用、恶意软件和 C2 防御

我们的 Threat Prevention 服务可利用 IPS 功能，自动阻止已知的客户端和服务器端漏洞利用，提供内联恶意软件防护以及阻截出站 C2 流量。无论使用什么端口、协议或加密方式，Threat Prevention 可检查所有威胁流量，因此没有什么威胁能被掩盖。该服务包含的 IPS 防护基于签名匹配和异常检测，能够导入并以热门格式（如 Snort 和 Suricata®）自动应用签名和规则。Threat Prevention 通过搜索网络攻击生命周期内各个时期的威胁（不仅是在威胁首次进入网络时），提供零信任模型中的分层防御。

通过对所有威胁使用统一的签名格式，可在单个集成的扫描中执行所有分析，并消除使用多次扫描的服务常见的多余过程，以确保实现快速的处理。Threat Prevention 会在每个数据包通过新一代防火墙时对其执行彻底检查，仔细查看数据包标头和有效负载内的字节序列。根据这一分析，我们能够确定数据包的重要详细信息，包括使用的应用、来源和目标、协议是否符合 RFC，以及有效负载是否包含漏洞利用程序或恶意代码。除了单个数据包，我们还会分析多个数据包的到达顺序和序列的上下文，以捕获和防御规避技术。这一切都在单次扫描内完成，因此，网络流量可以保持所需的速度。

URL Filtering

恶意站点和网络钓鱼防御

URL Filtering 使您能够安全地使用 Web 解决业务需求。这一云交付的服务可以在基本 Web 过滤的基础上提供额外保护，通过以独特方式结合的静态分析和机器学习来识别威胁。只需几毫秒即可识别出网络钓鱼页面和 JavaScript 攻击。新的恶意 URL 每天都会以成千上万的数量涌现，我们必须即时识别出这些恶意网页，才能有效阻止网络攻击。自动防护可阻止访问传输恶意软件和窃取凭证的恶意站点，从而防止任何数据丢失。通过扩展防火墙策略，企业面临的攻击风险可降至最低，并从始终保持最新状态的防护功能中受益。基于应用和用户的策略可简化复杂的 Web 安全规则，减少运营开销。

为准确确定类别和风险等级，URL Filtering 会扫描网站，并使用机器学习和静态及动态分析来分析网站内容。它会将 URL 分为良性和恶意两类，您可以将这两类 URL 轻松纳入新一代防火墙策略中，以对 Web 流量实现整体控制。发现新分类的恶意 URL 后，URL Filtering 会立即阻截它们，而无需分析师进行干预。

WildFire

恶意软件防御

WildFire® 恶意软件防御服务是业界最先进的基于云的分析和防御引擎，可成功抵御高度规避的零日漏洞利用和恶意软件。WildFire 超越了用于检测未知威胁的传统方法，集合多种互补技术的强大优势，可实现高精度的防规避检测，包括动态分析、静态分析、机器学习和裸机分析。WildFire 可持续提供创新的全新检测引擎，不会产生传统“先控制再放行”网络沙箱解决方案共有的对运营产生的影响。它通过对已识别威胁的行为、威胁指标以及阻截威胁的方式提供详细洞察，为安全团队节省时间和资源。

WildFire 还利用在云中不断打磨的威胁模型，为在物理和虚拟新一代防火墙中交付的基于内联机器学习的革命性引擎提供支持。这种创新型无签名功能可以防御恶意内容（如未知的可移植可执行文件以及来自 PowerShell 的危险无文件攻击），可完全内联运行，无需云提交步骤。

WildFire 社区作为行业最大的企业恶意软件分析网络之一，可以有效利用从网络、端点、云以及第三方合作伙伴提交的威胁情报。当任何 WildFire 订户发现零日漏洞利用或恶意软件时，该服务可在全球任何地方首次发现威胁的数秒内，针对所有订户自动编排执行高精度的防规避保护。

IoT Security

面向企业和医疗保健的 IoT Security

IoT Security 是行业最全面的物联网安全解决方案，可在单一平台上提供基于机器学习的可视性、防御和实施功能。在市场上，唯一的解决方案是将机器学习与我们领先的 App-ID 技术以及众包遥测技术结合使用，分析所有设备（甚至是之前从未发现的设备），以便进行发现、风险评估、漏洞分析、异常检测和基于信任的策略建议。它还提供了内置的防御功能，而不是采用只发出警报的方法，因此能够保护所有设备免受各类威胁和漏洞的侵害。此外，对于医疗保健客户而言，IoT Security 解决方案还具有深入的可视性、集中的操作设备利用率洞察，以及增强的医疗设备安全性，可以最大程度提升投资回报率，让患者获得最佳体验。

IoT Security 可实现轻松部署，并提供与现有工作流的无缝集成，从而减轻基础架构、安全和网络团队的负担。例如，订阅服务使用资产管理 (CMMS/ITSM)、网络访问控制 (NAC)、安全信息和事件管理 (SIEM) 以及行业特定的设备情报数据库中丰富的原生集成产品组合，借助物联网情报强化现有安全团队的实力。

IoT Security 支持企业、医疗、ICS/SCADA 系统、建筑管理系统、智慧城市基础设施、石油和天然气、公用事业以及运输垂直行业中的用例。

GlobalProtect

移动用户安全

GlobalProtect™ 适用于端点的网络安全解决方案可以将我们市场领先的威胁防御功能扩展到移动员工，无论他们身在何处。Prisma Access 使用 GlobalProtect 为远程用户提供无客户端和基于客户端的加密访问。这样，企业便可将公司访问控制策略扩展到非托管设备，同时访问云端和数据中心内的应用。通过与企业移动性管理解决方案（包括 AirWatch®、Microsoft Intune® 和 MobileIron®）集成，它支持每应用 VPN。

Prisma Access 为远程工作人员提供零信任网络访问。它可将基于角色的访问控制 (RBAC)、数字体验监视 (DEM) 和威胁检测功能纳入到单个云交付平台中，该平台为每个远程用户提供了大规模的可扩展性和一致的安全远程访问权限。Prisma Access 在全球拥有 100 多个服务地点，通过提供行业领先的 SLA，确保服务可用性以及与世界各地的应用和服务的高性能连接。借助 Prisma Access，企业可以设置并实施精细的策略，以便通过单一平台基于用户身份、角色、位置以及设备连接状况来限制对服务和应用的访问。它通过随时检查所有端口上的所有应用流量，将 10 多种网络和安全产品整合到具有高级安全功能（包括反恶意软件、漏洞利用检测和凭证滥用预防）的单一服务中，以便创建并实施更高效的安全策略。

5G 原生安全

5G 网络安全

如今，随着企业的数字化转型进程，企业员工开始寻求使用 5G 网络，以利用云、自动化、AI 和物联网手段切实推进工业 4.0 转型。5G 网络更加依赖于云和边缘计算，继而催生出跨越多个供应商以及多云基础架构的高度分布式环境。Palo Alto Networks 5G 原生安全为您的云原生 5G 内核、分布式边缘云和企业 5G 网络提供最精细的安全保护。5G 原生安全提供一个简单且紧密集成的 5G 安全平台，该平台利用自动化、Kubernetes® 原生编排以及与开放 API 的集成来简化操作。利用由机器学习提供支持的自动化、云交付的威胁情报来防御以 5G 速度执行攻击的对手，并在全球范围内实时阻止 5G 网络中的已知和未知威胁。通过为 5G 层面安全、企业 5G 安全和多接入边缘计算 (MEC) 安全提供“安全即服务”产品来解锁新的收入来源方式。

5G 原生安全在我们的 PA-7000 Series 和 PA-5200 Series 新一代防火墙、VM-Series 虚拟新一代防火墙，以及 CN-Series 中分别以物理防火墙设备、虚拟化 5G 部署以及容器化云原生 5G 部署的形式受到支持。这意味着，如果您已经在使用我们的新一代防火墙，则可继续使用相同的平台来保护服务提供商 5G 基础架构或企业 5G 网络的安全。

SD-WAN

保护分支机构连接安全

通过在新一代防火墙中订阅 SD-WAN 功能，可以轻松采用具有原生集成的一流安全和连接技术的端到端 SD-WAN 架构。您可以将 Prisma Access 用作 SD-WAN 中心来优化性能，

以便增强用户体验。此外，还可以将 Prisma Access 用作服务，避免构建 SD-WAN 中心基础架构的麻烦。或者，您可以构建该中心，然后使用 Palo Alto Networks 新一代防火墙将基础架构互联起来。

PRISMA®
BY PALO ALTO NETWORKS

Prisma

Prisma® 是行业最全面的云安全产品组合。它使用产品套件加速您的数字化转型，旨在保护当今的云免受未来的威胁。


Prisma SaaS


Prisma SD-WAN


Prisma Access


Prisma Cloud

Prisma SaaS

SaaS 应用安全及合规性

Prisma SaaS 通过为云中的软件即服务 (SaaS) 应用和敏感数据提供可视性、合规性控制及一致的安全防护，支持安全地采用云技术。它有助于最大程度减少影子 IT 的使用，安全访问 Microsoft 365™、Salesforce®、Google Workspace™、Slack® 和 Box 等公司 SaaS 应用，并降低云中的数据泄露风险。

Prisma SaaS 可以让您的企业和数据无需面临云网络风险，这样您就可以安全地使用 SaaS 应用，并将敏感数据安全地存储在云中。作为 Palo Alto Networks 新一代防火墙的集成功能，该服务与整个公司范围的安全牢牢绑定在了一起，提供超越云访问安全代理 (CASB) 等零散单点控制方法的简化部署。

Prisma SD-WAN

保护云交付的分支机构

Prisma SD-WAN 是行业首款新一代 SD-WAN 解决方案，能够实现安全、云交付的分支机构，可提供高达 243% 的投资回报率。与引入成本和复杂性的传统 SD-WAN 解决方案不同，Prisma SD-WAN 可通过应用定义的策略确保出色的用户体验，并使用机器学习和自动化功能简化网络和安全操作。

Prisma Access

云交付式移动用户安全

Prisma Access 借助行业最完整的云交付平台改变了网络安全性，让企业能够安全地为远程工作人员提供支持。传统的网络安全产品并未提供对所有应用的访问权限和保护，相反，它们在安全性覆盖方面存在很大差距，无法实现企业随时随地办公的需求。只有 Prisma Access 能够对所有端口的所有应用流量（包括基于 Web、非基于 Web 以及 SSL/TLS 加密应用中的流量）实施全面的双向检测，无论流量产生自与互联网、云、数据中心的通信，还是分支机构间的通信，数据漏洞的可能性因此降低了 45%。

此外，Prisma Access 提供的安全覆盖范围比其他任何解决方案都更广泛，它将多个单点产品（包括防火墙即服务 (FWaaS)、零信任网络访问 (ZTNA)、CASB、安全 Web 网关 (SWG) 等）整合到一个平台中，并通过一个控制台对这些单点产品进行管理。Prisma Access 建立在可大规模扩展的网络之上，利用 Amazon Web Services (AWS®) 和 Google Cloud 的组合基础架构，在 76 个国家/地区拥有 100 多个服务访问点。这样，Prisma Access 便可提供由行业领先的 SLA 支持的超低延迟，确保最终用户获得绝佳的数字体验。

Prisma Cloud

云原生安全平台

Prisma Cloud 是全面的云原生安全平台 (CNSP)，在混合及多云环境中，为整个云原生技术堆栈、应用和数据提供行业最广泛的安全性和合规性覆盖。Prisma Cloud 可保护不同主机、容器、无服务器中的云原生应用，以及不同云平台中的其他平台即服务 (PaaS) 产品。它会在部署资源时动态发现这些资源，并将云服务提供的数据（资源配置、流日志、审核日志、主机和容器日志等）关联起来，以便为云环境和应用提供安全和合规性方面的洞察。它使用机器学习来分析用户、工作负载和应用行为，从而防御高级威胁。

它利用业界最完善的合规性框架库，大幅简化了维持合规性的任务。Prisma Cloud 通过跨基础架构、PaaS、用户、开发平台、数据和应用工作负载的深度情境共享来实现这一目的。它可以与安全协调工具无缝集成，确保快速修复漏洞。

为了提供全生命周期的安全性，Prisma Cloud 跨 DevOps 工具链进行了集成，以便进行漏洞管理并实现合规性。通过使用海量 DevOps 插件，以及 IDE、SCM、CI 和 CD 技术，您的安全团队和 DevOps 可以为基础架构和应用提供安全保护，其中包括基础架构即代码 (IaC) 模板、主机、映像和函数。

CORTEX®
BY PALO ALTO NETWORKS

Cortex

Cortex® 是行业最全面的安全运营产品组合，可为企业提供领先的攻击面管理功能以及一流的防御、检测、自动化和响应功能。

AutoFocus

Cortex XDR

Cortex XSOAR

CRYPSIS™
A PALO ALTO NETWORKS COMPANY

Crypsis

EXPANSE
A PALO ALTO NETWORKS COMPANY

Expanse

AutoFocus

情境威胁情报

AutoFocus™ 情境威胁情报服务能够让您即时访问庞大且极其精确的威胁情报资源库，从而将其作为情报来源使用。借助行业最大的网络、端点和云情报源，获取对真实攻击独一无二的可视性。通过来自享誉全球的 Unit 42 威胁研究人员的最深入的情境，对每一次的威胁进行背景强化。通过利用自定义威胁来源和敏捷 API 将情报嵌入到工具中，为分析人员节省大量时间。

Cortex XDR

扩展的检测和响应

Cortex XDR™ 是行业首款扩展的检测和响应平台，可跨关键安全数据源阻止现代攻击。借助 Cortex XDR，您可以使用智能警报分组和事件评分来消除干扰，并专注于应对实际威胁。团队可以降低其工作的复杂性，用统一的防御、检测、调查和响应平台取代互不相关的单点产品。

Cortex XDR 可利用强大的端点保护功能自动阻截攻击，并使用行为分析功能来分析丰富的数据，从而准确检测整个环境中的威胁。它提供了每个事件的来龙去脉并揭示了根本原因，您的威胁调查速度将因此最多提升 8 倍。这款独特的产品简化了每个阶段的安全运营（从警报分类到威胁搜寻），减少了对经验丰富的安全分析人员的需求，并极大降低了检测和响应威胁的时间。与执行点的紧密集成可以加速控制，让您能够在最隐蔽的攻击造成损害前加以阻止。

Cortex XSOAR

扩展的安全编排、自动化和响应

Cortex XSOAR 借助行业最全面的安全编排、自动化和响应 (SOAR) 平台，大幅提高了 SOC 的效率。安全负责人可以使用统一的案例管理、自动化、实时协作及威胁情报管理方法，彻底转变其运营方式。团队可管理所有来源的警报，通过剧本进行流程标准化，对威胁情报采取行动，并自动响应所有安全用例，使响应时间缩短 90%，需要人工干预的警报量减少 95%。

Crypsis

事件响应服务

Crypsis Group 是 Palo Alto Networks 旗下的一家安全咨询公司，致力于通过提供最高质量的事件响应、风险管理和数字取证服务来打造更加安全的数字世界。公司通过防御和应对严重的网络威胁来为客户提供帮助和保护。我们具备全球响应能力、持续不断的技术创新以及精湛的网络安全专业知识，这让我们在迅速发展的威胁形势下能够保持领先地位。

Expanse

攻击面管理

Expanse 是一个自动化的攻击面管理 (ASM) 平台，可为企业面向互联网的全球资产和错误配置提供完整而准确的清单，以便不断发现、评估和缓解外部攻击面；标记危险通信；评估供应商风险；或评估并购目标的安全性。

敬请关注Palo Alto Networks官方微信或联系我们
热线： 400-9911-194
网址： www.paloaltonetworks.cn
邮件： Contact_SalesChina@paloaltonetworks.com

北京市朝阳区建国门外大街2号银泰写字楼C座31层 | 上海市长宁区红宝石路500号东银中心A座2802室 | 广州市天河区越秀金融大厦65层

咨询订购：400-010-8885、 8008106669@b.qq.com