Cortex XDR 端点防护解决方案指南

借助用于端点防护、检测和响应的单一云交付代理，保护您的端点免遭从未见过的攻击。

优点

- 利用基于 AI 的本地分析和行为威胁防护，阻止恶意软件。
- 阻截引发安全问题的漏洞利用。
- 将网络、端点和云资产中的端点防护与检测和响应统一起来。
- 通过云原生部署和管理来简化运营。

根据 MITRE 测试，实现行业领先的攻击技术检测率。

高级恶意软件和基于脚本的攻击能够轻松绕过传统防病毒软件，并可能大肆破坏您的业务。为了保护端点，您所采用的解决方案需能够提供出色的防护并利用 AI 持续适应快速变化的威胁，领先于攻击者。

Cortex XDR 代理能够全面保护您的端点。其通过在执行文件前后对文件进行分析，发现攻击迹象，包括零日恶意软件、无文件攻击和基于脚本的攻击。您可以在端点中快速部署统一的云交付代理，从而立即开始阻截高级攻击并收集用于检测和响应的数据。

消除零日恶意软件、勒索软件和无文件攻击

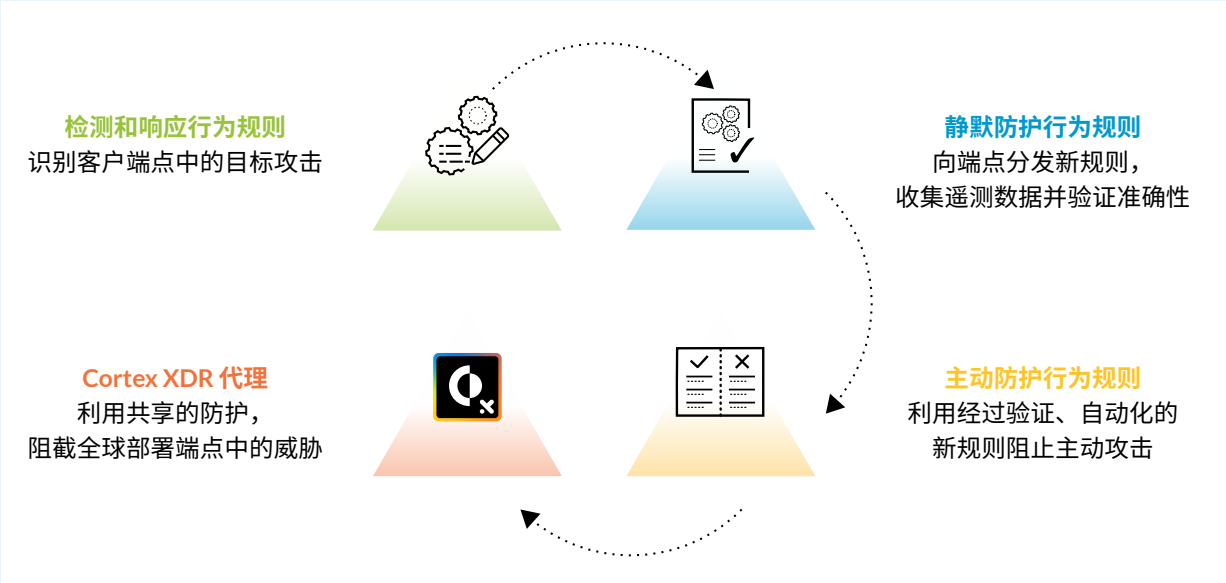
Cortex XDR 代理通过统一多个互补的引擎，提供全面的防御堆栈，利用一个代理阻止每个可能的攻击载体：

- **基于 AI 的本地分析**使用由全球来源提供的大量数据集支持的本地机器学习模式，在恶意软件执行前对其进行阻截。该模式基于独特的敏捷框架而构建，支持持续更新以确保始终可提供最新的本地防护。
- **与基于云的 WildFire® 恶意软件防御服务的集成**可深度检测未知文件，并在 Palo Alto Networks 端点代理、新一代防火墙和云基础架构中自动共享情报。
- **行为威胁防护**通过识别与恶意软件和无文件攻击相关的事件序列，阻截最隐蔽的威胁。此引擎可检查多个相关流程的行为以发现攻击，即使个别操作不一定预示着存在恶意活动。
- **基于行为的勒索软件防护**通过检测尝试修改或加密文件的进程保护您的端点免遭勒索软件的攻击，针对隐秘的勒索软件再增添一层防御。

- **凭证窃取防护**防止 Mimikatz 等工具访问系统密码，确保攻击者和恶意内部人员无法滥用凭证或升级权限。
- **计划和按需的恶意软件扫描**可发现休眠恶意软件，包括恶意可执行文件、DLL 和 Office 宏，以缓解风险，即使文件尚未打开也能发现。

利用静默规则最大限度地提高行为威胁防护的准确度

行为威胁防护通过紧密结合威胁研究、对客户网络中主动威胁的可视性以及静默规则遥测，提供准确及时的防护，以确保有效的安全性，所有代理在全球获得快速更新。每个新规则都以静默模式开始，让 Cortex XDR 研究人员可以快速推出新规则，并保持极低的误报率。



阻截漏洞利用技术以尽早拦截攻击

攻击者通常利用系统和应用漏洞来控制端点并安装恶意软件。为了始终领先于不断演变的漏洞利用，Cortex XDR 代理会识别漏洞利用技术和方法，而不是简单地利用签名来检测漏洞利用。通过阻止漏洞利用的每一步，该代理可以打破攻击生命周期并使威胁无效化。

Cortex XDR 代理通过多种方法阻止漏洞利用：

- **漏洞利用前的防护**能在攻击者启动漏洞利用前阻止侦查活动和漏洞分析技术，有效阻止攻击。
- **基于技术的漏洞利用防御**通过阻截缓冲区溢出或 DLL 劫持等漏洞利用技术，进而在无需事先了解威胁的情况下防御已知漏洞利用和零日漏洞利用。
- **内核漏洞利用防御**可阻止在操作系统内核进行的漏洞利用，防止其创建有升级权限（即系统级别权限）的进程。Cortex XDR 代理同样可阻止在内核中加载并运行恶意代码的注入技术，例如 WannaCry 和 NotPetya 攻击中所使用的技术。

利用 Cortex XDR 快速发现和调查威胁

Cortex XDR 代理主动阻截攻击并收集丰富的端点数据，用于 Cortex XDR、类别定义的企业级防护、检测和响应平台（运行于端点、网络和云数据中），以阻止复杂攻击。统一的用户界面便于管理用于检测和响应的警报和事件，以及用于 Cortex XDR 代理的策略。

Cortex XDR 通过提供每个威胁的全面信息并自动揭露根本原因，加速警报分类和事件响应。通过将不同类型的数据拼接在一起并简化调查，Cortex XDR 缩短了从分类到威胁搜寻等每个安全运营阶段所需的时间和经验。与执行点紧密集成让您可以在未来快速响应威胁，并运用从调查中获得的知识检测类似攻击。

实时响应攻击

Cortex XDR 代理提供一系列响应选项以快速控制威胁，同时让分析师能够推进其调查并收集其他端点信息。

为了解决威胁，分析师和管理员需能够：

- **隔离端点**，通过禁用受入侵端点中的所有网络访问，只允许 Cortex XDR 管理控制台的流量通过，避免这些端点与其他端点通信或将其感染。
- **终止进程**，阻止所有正在运行的恶意软件继续在端点中执行恶意活动。
- **阻截给定文件的额外执行**，在策略中将其列入黑名单。
- **隔离恶意文件**，如果 Cortex XDR 代理没有隔离文件，则隔离这些文件并从工作目录中移除。
- **检索特定文件**，针对正在调查的端点中的文件，以便进一步分析。
- **通过实时终端直接访问端点**，获取业内最灵活的响应操作以运行 Python、PowerShell 或系统命令或脚本；审查和管理主动进程；查看、删除、移动或下载文件。
- **利用开放式 API 协调响应**，允许第三方工具应用执行策略并从任何位置收集代理信息。

在端点、网络和云安全中应用一致的协调策略

Cortex XDR 代理与 WildFire、新一代防火墙以及 Prisma™ Access 紧密集成，为您的整个企业环境提供一致的防护。该集成能够不断改进安全状态，包括协调防御零日攻击。Palo Alto Networks 产品无论何时观察到未知的恶意软件，都会将有问题的文件发送至 WildFire 进行分析。如果可疑的恶意软件被判定为恶意，系统几分钟内便会自动向所有新一代防火墙、端点代理和受 Prisma Access 保护的用户分发新的保护措施。

安全管理 USB 设备

USB 设备提供各种功能，但它们也会带来风险。当用户无意中将恶意闪存驱动器连接到计算机，或将机密数据复制到备份磁盘驱动器时，所在的组织会面临攻击和数据丢失的风险。高级攻击者甚至能够利用恶意软件感染看似无害的 USB 设备，例如键盘和 Web 相机。Cortex XDR 包含功能强大的设备控制模块，让您可以监控和保护 USB 访问，无需在您的所有主机上安装其他端点代理。您可以根据 Active Directory® 组和组织单位分配策略，按设备类型限制使用，并按供应商、产品和序列号分配只读或读/写策略例外。利用该设备控制模块，您可以轻松管理 USB 访问，并缓解基于 USB 的威胁，让自己高枕无忧。

从云端轻松部署

运营团队可从云原生管理服务在其所有端点上快速安装代理。Cortex XDR 代理通过消除对本地日志和管理服务器的需求，加快防护并简化运营。与复杂繁琐的旧有防病毒解决方案相比，最终用户可体验到更佳的性能和更少的中断。

利用全面的操作系统支持保护您的所有端点

Cortex XDR 代理可以在未知和已知的攻击破坏系统前阻止这些攻击，为运行所有主要操作系统（Windows®、macOS®、Linux 和 Android®）的端点提供保护。相比之下，原生操作系统安全功能仅保护各自的端点，因而会形成碎片化的保护方式，使端点容易遭受攻击并降低事件响应速度。有关支持操作系统的完整列表，请访问 Palo Alto Networks 兼容性矩阵。

面向受限网络的本地代理服务

本地代理服务将 Cortex XDR 代理扩展到无法直接连接互联网的设备。现在，这些代理可将该代理服务用作面向 Cortex XDR 管理服务的通信代理，接收最新的安全控制台，将内容发送至 Cortex™ Data Lake 和 WildFire，而无需直接访问互联网。

CORTEX XDR™
BY PALO ALTO NETWORKS

免费咨询热线：400 9911 194
网址：www.paloaltonetworks.cn
邮箱：contact_salesAPAC@paloaltonetworks.com

cortex-xdr-endpoint-protection-solution-guide-b-120319