服务器工作负载防护

Linux 防护

Intercept X Advanced for Server、Intercept X Advanced for Server with XDR 和 Intercept X Advanced for Server with MDR

云或数据中心、主机和容器。保护您现在的基础设施，随着 Sophos 高影响工作负载防护升级，对成本影响低。

减少侦测和响应时间

获得主机和容器工作负载的全面可见性，在恶意软件、漏洞和异常行为立足前发现他们。扩展侦测与响应 (XDR) 提供主机、容器、端点、网络流量和云提供商原生安全服务的详细信息。

云原生行为和漏洞攻击运行时侦测发现威胁，包括容器逃逸、内核漏洞攻击和权限提升尝试。简化威胁调查工作流程优先安排高风险事件侦测，整合相关事件以提高效率和节约时间。

提高安全操作

通过中央管理控制台提供的可操作主机和容器运行时可见性和威胁侦测对抗威胁，或者与现有威胁响应工具和大量部署选项集成。

Sophos Central 管理 - 轻量 Linux 代理为安全团队提供所需的关键信息，在一个位置调查并响应行为、漏洞攻击和恶意软件威胁。此部署选项监测 Linux 主机，允许团队从一个面板管理所有 Sophos 解决方案，在威胁追踪、修复和管理之间无缝移动。

API 集成 - Sophos Linux Sensor 是为性能微调的高度灵活的部署选项。Linux sensor 利用 API 在主机或容器环境中集成丰富运行时威胁侦测与现有威胁响应工具。提供更丰富的侦测，创建自定义规则集的控制，以及调节主机资源优化的配置选项。

轻松实现性能

Intercept X for Server 防护为 DevSecOps 工作流程优化，发现发生的复杂攻击，无需内核模块、协同、基准或系统扫描。优化资源限制，包括 CPU、内存和数据收集限制，进一步避免主机过载和稳定性问题导致的高成本停机。确保优化应用程序性能和运行时间。

亮点

- 保护云、现场和虚拟 Linux 工作负载及容器安全
- 减少侦测和响应威胁时间
- 针对性能很关键的使命关键型工作负载优化
- 通过扩展侦测与响应 (XDR) 利用端点、网络、电子邮件、云、M365 和移动数据
- 通过提供的云安全状态管理，了解并保护您的更广泛云环境
- 以全托管服务形式提供 24/7/365 全天候安全

SOPHOS

自动化云安全核查清单

设计您的云环境，利用可见性和维护工具满足最佳做法标准，集成云安全状态管理覆盖更广泛的公共云环境：

- 主动发现 Amazon AWS、Microsoft Azure 和 Google Cloud Platform (GCP) 上未经审核的活动、主机和容器镜像漏洞、错误配置
- 通过 Sophos 主机防护和 Sophos Firewall 部署的详细库存与可见性，持续发现云资源
- 自动叠加安全最佳做法标准，发现状态漏洞，找出快速成功和关键问题
- 发现用户 IAM 角色行为中的高风险异常，快速指出异常访问模式、位置和恶意行为以避免外泄

合作关系扩充您的团队

Sophos 托管式检测与响应专家 SOC 分析师与您的团队合作，24/7/365 全天候监测您的环境，代表您主动追踪并修复威胁，提供提高效率所需的 Linux 专业知识。Sophos 分析师响应潜在威胁，寻找隐患迹象，对发生的事件、地点、时间、方式和原因提供详细分析。

技术规格

有关最新信息，请阅读 Linux 系统要求。有关 Windows 功能的详细信息，请参见 Windows 数据表。

产品特点	Intercept X Advanced for Server	Intercept X Advanced for Server with XDR	Intercept X Advanced for Server with MDR Complete
Linux Protection Agent （包括恶意软件扫描、防漏洞攻击、文件扫描等）	✔	✔	✔
Linux Sensor （通过 API 集成 Linux 和容器运行时威胁侦测与现有威胁响应工具）		✔	✔
Cloud Infrastructure Security （监测云安全状态，防止安全和合规性风险）	✔	✔	✔
XDR （扩展式侦测与响应）		✔	✔
MDR （托管式检测与响应 – 24/7/365 全天候威胁追踪与响应服务）			✔

立即免费试用

注册即可享受 30 天免费试用
www.sophos.cn/server

中国（大陆地区）销售咨询
电子邮件：salescn@sophos.com

22-10-21 DS-ZHCN (PC)

SOPHOS