Sophos Endpoint

防止网络入侵、勒索软件和数据丢失

Sophos Intercept X 提供针对高级攻击的无与伦比的保护。它采用了一系列先进的技术，以在威胁影响您的系统之前阻止最广泛的威胁。强大的 EDR 和 XDR 工具使您的组织能够追踪、调查和应对可疑活动和攻击指标。

以预防为主的方法

Intercept X 采用了全面的端点保护方法，而不依赖于单一的安全技术。Web、应用程序和外围设备控制可以减小攻击面并阻止常见的攻击途径。AI、行为分析、反勒索软件、反漏洞利用技术以及其他顶尖技术可以在威胁升级之前加以停止。这意味着资源紧缺的 IT 团队需要调查和处理的事件会变得更少。

环境敏感型防御

这些额外的动态防御措施是行业首创的。它们提供根据攻击环境信息而自动适应的自动保护。这样可以剥夺攻击者的操作能力，扰乱和遏制攻击，同时争取宝贵的响应时间。

易于设置和管理

Sophos Central 是一个云管理平台，用于管理所有 Sophos 产品。我们推荐的保护技术已默认启用，确保您立即获得最强大的保护设置，无需调整。还可以进行精细控制。帐户系统健康检查能够识别安全状态的漂移和高风险的错误配置，使管理员可以一键轻松解决问题。

Synchronized Security 同步安全

Intercept X 与 Sophos Firewall、Sophos ZTNA 和其他产品共享状态和健康信息，以提供对威胁和应用程序使用情况的额外可见性。同步安全将在执行清理时自动隔离受骇设备，然后在威胁被中和后恢复网络访问，无需管理员干预。

产品亮点

- 利用深度学习人工智能阻止前所未见的威胁
- 阻止勒索软件，并将受影响的文件回滚至安全状态
- 阻止攻击链中使用的漏洞利用技术和恶意行为
- 自动调整防御措施以应对攻击者行为的变化
- 通过应用程序、设备和 web 控制减小攻击面
- 通过一键修复，识别安全状态漂移和高风险的错误配置
- 通过 XDR 进行威胁捕猎，支持 IT 运营安全保健
- 以全托管服务形式提供 24/7/365 全天候安全
- 即使是远程办公环境也可以轻松部署、配置和维护

SOPHOS

阻止勒索软件

Intercept X 包括 CryptoGuard，这先进的反勒索软件技术可以阻止新的变种或前所未见的勒索软件。CryptoGuard 检查文件的内容，以侦测在您网络上运行的加密和勒索软件。被勒索软件加密的文件将自动回滚到安全状态，不论大小或文件类型，最大限度地减少对业务生产力的影响。

扩展式侦测与响应 (XDR)

强大的 EDR/XDR 功能使您能够在 Sophos 和第三方安全控制中追踪、调查和响应可疑活动。在 Sophos 数据湖中进行威胁捕猎或转向到设备以获取实时数据和长达 90 天的历史数据。获取一个对于您组织环境的综合视图，当中网罗用于专为SOC 团队和 IT 管理员而设计的威胁侦测、调查和响应的Sophos X-Ops 威胁情报。

阻止漏洞利用攻击

防漏洞利用攻击技术阻止攻击者赖以入侵设备，盗窃凭据和分发恶意软件的技术。Sophos 为所有应用大规模部署了基于设备的崭新反漏洞利用方法。Intercept X 可开箱即用，其构建在 Microsoft Windows 提供的基本保护之上，并添加了不少于 60 种专有、预配置和调整过的漏洞利用缓解措施。Intercept X 通过阻止攻击链中使用的技术，来保护系统免受无文件攻击和零日漏洞利用的威胁。

托管式侦测与响应 (MDR)

Sophos MDR 是一项全面的威胁追踪、侦测和事件响应服务，与 Sophos 和第三方安全控制集成，提供专门的 24/7 全天候的安全团队，来侦测和中和最精密和复杂的威胁。

授权许可概述

产品特点	Intercept X Advanced	Intercept X Advanced with XDR	Intercept X Advanced with MDR Complete
下一代威胁保护 Web 保护，深度学习反恶意软件	✓	✓	✓
阻止恶意活动和环境敏感型防御 反勒索软件防护，反漏洞利用技术，自适应攻击防护	✓	✓	✓
降低威胁暴露 Web 控制，外围设备控制，应用程序控制，数据丢失防护(DLP)，帐户系统健康检查	✓	✓	✓
侦测和响应 (EDR/XDR) 可疑活动侦测，威胁捕猎，调查工具，响应措施		✓	✓
托管式侦测与响应 (MDR) 全面托管的 24/7 全天候威胁捕猎、侦测和事件响应服务			✓

立即免费试用

注册即可享受 30 天免费试用
www.sophos.cn/intercept-x

中国（大陆地区）销售咨询
电子邮件：salescn@sophos.com

23-09-07 DS-ZHCN (DD)

SOPHOS