Intercept X

Intercept X Advanced、Intercept X Advanced with XDR、Intercept X Advanced with MTR

Sophos Intercept X 是行业领先的端点安全解决方案，可减少攻击面，阻止攻击运行。结合防漏洞利用攻击、防勒索软件、深度学习人工智能和控制技术，阻止攻击进一步影响您的系统。Intercept X 采用全面深度防御方法保护端点，而不是依赖某一项主要安全技术。

阻止未知威胁

Intercept X 深度学习 AI 擅长侦测和阻止恶意软件，即使从未见过。实现方法是审查来自数亿样本的文件属性来识别威胁，无需特征码。

阻止勒索软件

Intercept X 包含先进的防勒索软件功能，可以侦测和阻止勒索软件攻击中用到的恶意加密进程。已经加密的文件将回滚至安全状态，减少对业务生产的任何影响。

阻止漏洞利用攻击

防漏洞利用攻击技术阻止攻击者用来威胁设备，盗窃凭据和分发恶意软件的漏洞利用攻击技术。通过阻止攻击链中用到的技术，Intercept X 保护您的企业不受免文件攻击和零日漏洞威胁。

减少攻击面

控制可以在环境中运行的应用程序和设备，阻止恶意网站和潜在有害应用程序 (PUA) 接触用户或设备。

Synchronized Security 同步安全

Sophos 解决方案组合后的效果更佳。例如，Intercept X 和 Sophos Firewall 将共享数据，自动隔离受威胁的设备，同时执行清理，消除威胁后恢复网络访问。所有这些无需管理员干预。

产品亮点

- 利用深度学习人工智能阻止从未见过的未知威胁
- 阻止勒索软件，并将受影响的文件回滚回安全状态
- 阻止攻击链中用到的漏洞利用攻击技术
- 通过应用程序、设备和 Web 控制减小攻击面
- 通过 XDR 执行威胁追踪和 IT 运营安全卫生
- 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

扩展侦测与响应 (XDR)

Sophos XDR 提供更好的准确度，减少企业执行威胁追踪和 IT 运营安全卫生的工作量。行业领先的防护减少有害杂讯，按照优先级排列的侦测与人工智能指导的调查方便轻松了解开始的地方并快速采取行动。本机端点、服务器、防火墙、电子邮件、云、移动和 O365 集成在数据湖中可用，或者引导至设备获取实时状态和最多 90 天历史数据。

Managed Threat Response (MTR)

Sophos 专家团队提供的 24/7/365 全天候威胁捕猎侦测与响应服务。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。

简单管理

Intercept X 通过所有 Sophos 解决方案的云管理平台 Sophos Central 管理。
这是面向所有设备和产品的单一面板，方便部署、配置和管理您的环境，即使是远程办公设置。

人工智能和专家支持的数据

Intercept X 结合深度学习人工智能和 SophosLabs 专家的网络安全知识，融合两者优点，为企业提供行业领先的威胁情报。

技术规格

Intercept X 支持 Windows 和 macOS 部署。有关最新信息，请阅读 Windows 系统要求和 Mac 数据表。

授权详情概述

产品特点	Intercept X Advanced	Intercept X Advanced with XDR	Intercept X Advanced with MTR Advanced
基础防护 （包括应用程序控制、行为侦测等）	✓	✓	✓
下一代防护 （包括深度学习、防勒索软件、免文件攻击防护等）	✓	✓	✓
XDR （扩展侦测与响应）		✓	✓
Managed Threat Response （MTR – 24/7/365 全天候威胁捕猎与响应服务）			✓

立即免费试用

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

中国（大陆地区）销售咨询
电子邮件：salescn@sophos.com

22-01-10 DS-ZHCN (PS)