服务器工作负载防护

Windows 防护

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

Sophos Intercept X for Server 是行业领先的服务器安全解决方案，减少攻击面并阻止攻击运行。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 for Server 采用全面深度防御方法保护服务器，而不是依赖某一项主要安全技术。

阻止未知威胁

Intercept X for Server 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 for Server 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，盗窃凭证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 for Server 保护您的企业不受免文件攻击和零日漏洞威胁。

控制您的服务器

确保只有您想要的内容才可以运行。服务器锁定（白名单）确保服务器上只能运行您批准的应用程序。文件完整性监测将通知您是否存在未经授权更改重要文件的尝试。

了解更广泛的云环境

了解并保护整个多云库存。您可以侦测云工作负荷以及关键云服务，包括 S3 bucket、数据库和免服务器功能，识别可疑行为，发现不安全部署，弥补安全漏洞。

亮点

- 保护云、现场和虚拟服务器部署安全
- 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，并将文件回滚回安全状态
- 阻止攻击链中用到的漏洞攻击技术
- 通过 XDR 执行威胁追踪和 IT 运营安全卫生
- 了解并保护更广泛的云环境，如 S3 bucket 和数据库
- 以全托管服务形式提供 24/7/365 全天候安全

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噪声，按照优先级排列的侦测与人工智能指导的调查方便了解入手和快速应对点。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。

人工智能和专家支持的数据

Intercept X for Server 结合深度学习人工智能和 SophosLabs 专家的网络安全知识，兼具两者优点，为企业提供行业领先的威胁情报。

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 for Server 通过所有 Sophos 解决方案的云管理平台 Sophos Central 管理。这是面向所有服务器、设备和产品的单一面板，方便部署、配置和管理您的云、现场、虚拟和混合部署。

技术规格

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

功能	Intercept X Advanced for Server	Intercept X Advanced for Server with XDR	Intercept X Advanced for Server 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）	✔	✔	✔
服务器控制 （包括服务器锁定、文件完整性监测等）	✔	✔	✔
CSPM （云安全状态管理 – 查看并保护更广泛的云环境）	✔	✔	✔
XDR （扩展式侦测与响应）		✔	✔
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/server

中国（大陆地区）销售咨询
电子邮件：salescn@sophos.com

22-04-07 DS-ZHCN (PC)

SOPHOS