Sophos XDR

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

Intercept X 是业内唯一同步本机端点、服务器、防火墙、电子邮件、云和 O365 安全的 XDR 解决方案。凭借最丰富的数据集获取您企业环境的全盘视图和，方便专业 SOC 团队和 IT 管理员开展深度分析进行威胁侦测、调查和响应。

解答 IT 运行和威胁捕猎追踪问题

快速获得业务关键问题的答案。IT 管理员和网络安全专家在执行日常 IT 运行和威胁捕猎任务时，将发现真正的附加值。

从最佳防护开始

Intercept X 在攻击开始前就能加以阻止。这意味着得到更好的防护，用更少的时间调查自动阻止的事件。您还可以获取详细的威胁情报，获得必要的信息以便快速采取信息充分的决定。

了解关注重点

锁定重要问题，并获得按照优先级排列的可疑侦测与漏洞配置列表，该表格包含进一步调查需要的关键信息。选择预先编写的模板库以提出多种 IT 运营和威胁追踪问题，或者创建您自己的库。

缩短调查和响应时间

人工智能指导的调查帮助您快速了解事件范围和原因，缩短响应时间。访问设备获取实时状态和最多 90 天历史数据，或者数据湖中最多 30 天历史数据。

跨产品可见性

通过本机集成 Intercept X、Intercept X for Server、Sophos Firewall、Sophos Email、Sophos Mobile、Cloud Optix 和 Microsoft Office 365 数据，获得企业的最大可见性。

多平台多操作系统支持

检查您的环境，无论是云端、本地部署或者 Windows、macOS、Linux、Amazon Web Services、Microsoft Azure、Google Cloud Platform 和 Oracle Cloud Infrastructure 虚拟环境。

产品亮点

- 解答业务关键 IT 运行和威胁捕猎问题
- 利用按照优先级排列的侦测列表和人工智能指导的调查
- 对目标设备远程采取补救措施
- 全盘了解企业 IT 环境，需要时深入挖掘精细细节
- 本机端点、服务器、防火墙、电子邮件、云、移动和 O365 集成
- 访问预先编写的可定制模板使用案例库

SOPHOS

使用案例

IT 运行

- 为什么计算机运行速度慢?
- 哪些设备具有已知漏洞、未知服务或未授权的浏览器扩展程序?
- 是否正在运行应移除的程序?
- 识别未托管、来宾和物联网设备
- 为什么办公网络速度缓慢?是什么应用程序导致的?
- 查看丢失或毁坏设备上过去 30 天的异常活动
- 定位未打补丁或者软件过期的移动设备

威胁捕猎

- 哪些进程尝试在非标准端口进行网络连接?
- 显示最近修改过文件或注册表项的进程
- 列出侦测到的与 MITRE ATT&CK 框架映射的 IoC
- 将调查扩大到 30 天,无需恢复设备上线
- 从防火墙使用 ATP 和 IPS 侦测,调查可疑主机
- 比较电子邮件头信息、SHA 和其他 IoC,识别到可疑域的流量
- 找出多次登录失败的用户

包括内容

	扩展侦测与响应 (XDR)
跨产品数据源	✓
跨产品侦测、调查与响应	✓
按照优先级排列的侦测列表 & 人工智能指导的调查	✓
Sophos Data Lake	✓
Data lake 保留期限	30 天
实时状态信息	✓
磁盘数据保留期限	最多 90 天
威胁追踪 & IT 运营模板库	✓
Intercept X 防护功能	✓

有关授权许可证的更多详细信息,请参见 Intercept X 和 Intercept X for Server 授权许可指南。

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

22-01-06 DS-ZHCN (MP)

SOPHOS