解决方案概要

Sophos XDR

利用 EDR 和 XDR 抵御主动攻击敌手

攻击敌手不断发展他们的技术，以利用漏洞并加速攻击时间表。缩短侦测和响应的时间从未如此重要。Sophos 的统一扩展式侦测和响应 (XDR) 平台使您能够快速侦测、调查和响应安全生态系统中的多阶段威胁和主动攻击敌手。

实用案例

1 | 从强有力的防御开始

期望结果：预先阻止更多威胁，以减轻您的工作负担。

解决方案：将调查的重点放在入侵发生之前就加以阻止。Sophos XDR 包含卓越的防护功能，可以在高级威胁升级之前就加以快速阻止。利用先进技术，包括人工智能、行为分析、反勒索软件和反漏洞利用，来保护端点和服务器。

2 | 加速威胁响应

期望结果：快速侦测、调查和响应威胁。

解决方案：通过 Sophos X-Ops 提供的威胁情报，利用人工智能优先排序侦测，让您迅速轻松地识别需要立即关注的可疑事件。进行威胁捕猎，并通过优化的调查工作流程、强大的搜索功能、协作案例管理工具和自动响应来迅速作出反应。

3 | 攻击面的可见性

期望结果：获得所有关键攻击面的规避性威胁的全面可见性和洞察力。

解决方案：利用 Sophos 完全集成和 XDR就绪的解决方案，提供超越端点的可见性，或者发挥您现有的技术投资。整合广泛的第三方端点、防火墙、网络、电子邮件、身份辨识和云安全解决方案生态系统，通过统一的 XDR 平台侦测和响应威胁。

4 | 适用于所有使用者的强大性能

期望结果：一般 IT 人员和安全分析师都能够轻松进行调查和响应。

解决方案：专为专门的内部 SOC 团队和负责安全以及其他 IT 职责的管理员而设计，Sophos XDR 有助于最大化使用者效率，并提供全面的可见性和指导，帮助您迅速响应威胁。

Gartner

在 2023 年 Gartner XDR 市场指南中得到认可

MITRE ATT&CK

在 2023 年 MITRE Engenuity ATT&CK 评估中取得优异成绩

G2 Leader

被 G2 用户评为排名第一的 XDR 解决方案 (2023 年春季)

了解更多并试用 Sophos XDR：
sophos.com/xdr

SOPHOS

2023-11-08 DS-ZHCN (MP)