Sophos MDR for Microsoft Defender

针对微软环境的专家领导的威胁响应

Sophos 托管式侦测和响应 (MDR) 服务为您的团队提供了高技能的专家负责的全天候监控、调查和响应Microsoft Security警报，伸延您团队的能力。

最大化您的Microsoft Security投资

许多组织已经投资了Microsoft Security套件，但可能没有足够的内部专业知识来有效地使用微软的多产品技术堆栈来侦测、调查和响应每天数百个安全警报：

- 全球网络安全从业人员的缺口已经达到 340 万[1]。
- 71% 的安全团队发现很难在其工具产生的杂讯中确定要调查哪些安全警报[2]。
- 拥有专门安全操作团队的组织的威胁响应时间中位数为 16 小时，这给攻击者留下了大量的时间在网络中进行操作[3]。

Sophos MDR for Microsoft Defender能对 Microsoft 环境提供了最强大的威胁侦测、搜索和响应功能。我们的分析师全天候监控、调查并响应Microsoft Security警报，执行即时的人工主导的响应行动，以阻止已确认的威胁，平均威胁响应时间为 38 分钟，比行业基准快 96%。

侦测并阻挡 Microsoft Defender 无法防范的威胁

使用 Sophos MDR for Microsoft Defender，我们的Microsoft Security专家使用以下微软产品的安全数据侦测、调查和响应威胁：

- Microsoft Defender for Endpoint
- Microsoft Defender for Identity
- Microsoft Defender for Cloud
- Microsoft Defender for Cloud Apps
- Identity Protection (Azure AD)
- O365 Security & Compliance Center
- Microsoft Sentinel
- Office 365 Management Activity

此外，我们的专有侦测、世界一流的威胁情报和人工主导的威胁捕猎增加了额外的防御层，识别和阻止比Microsoft Security工具本身所能更多的威胁。

组织还可以集成非微软安全工具，和来自 Sophos 解决方案的或者其他许多供应商，如 Palo Alto Networks、Fortinet、Check Point、AWS、Google、Okta、Darktrace 等的遥测资源，以实现完整的可见性和保护。

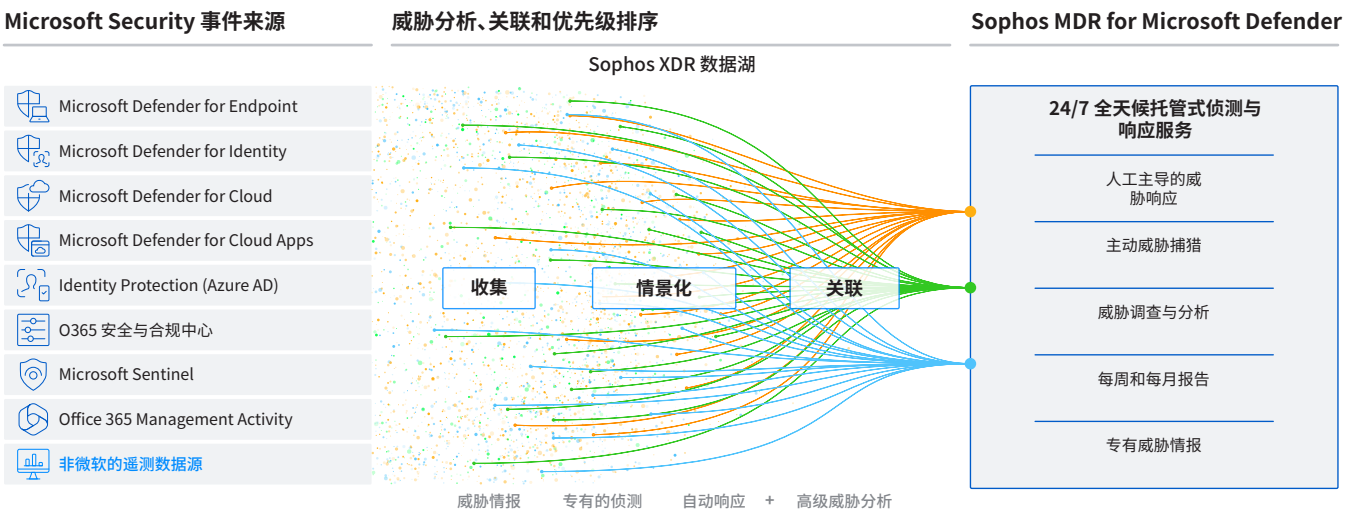
产品亮点

- Sophos MDR 分析师全天候监控、调查和响应Microsoft Security警报，立即采取行动阻止已确认的威胁。
- 服务功能扩展到 Microsoft Defender for Endpoint 和 Microsoft Sentinel 之外，以提供跨 Microsoft Security 平台的覆盖。
- 当识别出主动威胁时，Sophos MDR 操作团队可以代表您执行一系列广泛的威胁响应操作
- 利用 Sophos 的专有侦测技术、威胁情报和人工主导的威胁捕猎提供额外的防御层
- 集成非 Microsoft 工具和遥测源，以阻止针对您的网络、用户和客户的攻击

1 2022 Cybersecurity Workforce Study, (ISC)2
2 The State of Cybersecurity 2023: The Business Impact of Adversaries, Sophos
3 Gartner Cybersecurity Business Value Benchmark database, 2022

SOPHOS

Sophos MDR for Microsoft Defender：关键业务能力



全天候威胁监控

我们的Microsoft Security专家在威胁危及您的数据或造成操作中断之前侦测并阻止威胁。在六个全球安全运营中心 (SOC) 的支持下，Sophos 提供全天候覆盖。

人为威胁响应

Sophos MDR 团队可以代表您执行一系列广泛的威胁响应操作，以破坏、遏制和消除攻击者。威胁响应行动包括：

- 隔离使用 Sophos Central 的主机
- 应用基于主机的防火墙 IP 阻挡
- 终止流程
- 强制注销用户会话
- 停用用户账户
- 移除恶意工件
- 将恶意哈希值添加到 Sophos Central 中的阻挡列表

主动、人为的威胁捕猎

由训练有素的分析师执行的主动威胁捕猎，可以发现并迅速消除威胁，并识别逃避已部署工具集侦测的攻击者行为。

与非Microsoft Security工具兼容

Sophos MDR 以与非微软安全工具和遥测源集成，以侦测和阻止整个环境中的攻击。

每周和每月报告

Sophos Central 提供实时警报、报告和管理选项，同时每周和每月的报告提供关于安全调查、网络威胁和您组织安全状况的深入信息。

每月威胁情报简报

Sophos MDR 团队提供的“Sophos MDR ThreatCast”是每月的简报，提供最新威胁情报和安全最佳实践的见解。

专有的侦测

Sophos 平台内置了专有的侦测、高级威胁分析和世界级威胁情报，增加了额外的防御层，比Microsoft Security工具本身可以识别更多的威胁。

要了解更多信息，请访问：

www.sophos.com/microsoft-defender

中国（大陆地区）销售咨询
电子邮件：salescn@sophos.com

23-07-10 DS-ZHCN (DD)

SOPHOS