Sophos Managed Detection and Response

24/7 全天候威胁侦测和响应

Sophos MDR 是全托管 24/7 全天候服务，专家专责侦测并响应以您的计算机、服务器、网络、云工作负荷、电子邮件帐户等为目标的网络攻击。

勒索软件和防止入侵服务

始终在线的安全运营的需求已经成为必要条件。但是，现代运营环境的复杂性以及网络威胁的发展速度，使得大多数组织越来越难以自行成功管理侦测和响应。

借助 Sophos MDR，我们的专家团队阻止人主导的高级攻击。我们采取措施，在威胁可以中断业务运行或威胁敏感数据前消除威胁。Sophos MDR 可以定制，具有不同服务层级，可以通过我们的专利技术或利用您的现有网络安全技术投资提供。

以服务形式提供网络安全

扩展式侦测与响应 (XDR) 功能在数据所在位置提供完全安全覆盖，在其支持下，Sophos MDR 可以：

- **比安全工具自行发现更多网络威胁**
  我们的工具自动拦截 99.98% 的威胁，允许我们的分析师关注于追捕只能由接受过深度培训的人员才能发现并阻止的最成熟攻击者。
- **代表您采取措施，阻止威胁破坏您的业务**
  我们的分析师在数分钟内侦测、调查和响应威胁 — 无论您需要全规模事件响应还是帮助您作出准确决策。
- **辨识威胁根本原因以阻止未来事件**
  我们主动采取措施，提供建议减少对您组织的风险。更少事件意味着对 IT 和安全团队、员工以及客户造成的中断更少。

与您已有的网络安全工具兼容

我们可以从获奖屡获殊荣的产品系列提供您需要的技术，或者我们的分析师可以利用现有网络安全技术侦测并响应威胁。

Sophos MDR 兼容 Microsoft、CrowdStrike、Palo Alto Networks、Fortinet、Check Point、Rapid7、Amazon Web Services (AWS)、Google、Okta、Darktrace 等供应商的安全遥测。通过 Sophos 自适应网络安全生态体系 (ACE) 和 Sophos X-Ops 威胁情报部门的信息，自动整合、关联和排序遥测信息优先级。

产品亮点

- 通过 24/7 全天候威胁响应专家团队，阻止勒索软件和其他人为主导的高级攻击
- 最大化您现有网络安全技术的 ROI
- 让 Sophos MDR 执行全规模事件响应，与您一起管理安全事件，或者提供详细威胁通知和指引
- 利用 24/7 全天候监测和端点侦测与响应 (EDR) 功能，提高网络保险的理赔范围
- 减轻内部 IT 和安全人员的负担，让其专注于业务实现

SOPHOS

满足您所处状况的 MDR

Sophos MDR 可自定义，提供不同服务层级和威胁响应选项。让 Sophos MDR 运营团队执行全规模事件响应，与您一起管理网络威胁，或者在发现威胁时通知内部安全运营团队。我们的团队快速学习攻击的对象、内容、时间和方式。我们可以很快响应威胁。

关键功能

24/7 全天候威胁监测和响应

我们在威胁影响您的数据或导致停机前加以发现并响应。在 6 个全球安全运营中心 (SOC) 的支持下，Sophos MDR 提供全天候覆盖。

兼容非 Sophos 安全工具

Sophos MDR 可以集成第三方端点、防火墙、身份识别、电子邮件和其他安全技术的遥测信息作为 Sophos ACE 的一部分。

全规模事件响应

确定活跃威胁后，Sophos MDR 运营团队可以代表您执行一套丰富的响应操作，远程破坏、隔离和完全消除对手攻击。

每周和每月报告

Sophos Central 是实时提醒、报告和管理的单一仪表板。每周和每月报告提供安全调查、网络威胁和安全状态的相关信息。

Sophos 自适应网络安全生态体系

Sophos ACE 自动阻止恶意活动，支持我们搜索需要人为干预以侦测、调查并消除的微弱威胁信号。

专家领导的威胁追捕

由训练有素的分析师执行的主动威胁追捕发现并快速消除比安全产品自身可以侦测的更多威胁。Sophos MDR 运营团队还可以利用第三方供应商遥测信息开展威胁追捕，分辨能避开所部署工具集侦测的攻击者行为。

直接电话支持

您的团队可以直接呼叫我们的安全运营中心 (SOC)，检查潜在威胁和活跃事件。Sophos MDR 运营团队 24/7/365 全天候在线，遍布全球 26 个地点的支持团队作为其坚强后盾。

专门的威胁响应负责人

我们为您提供一名专门威胁响应主管，在我们确定事件后立刻与您的内部团队和外部合作伙伴协作，并与您合作直到解决事件。

根本原因分析

除了提供主动建议以改善您的安全状态，我们还执行根本原因分析，辨识导致事件的根本问题。我们为您提供解决安全弱点的规范性指南，这样以后无法再被利用。

Sophos 帐户运行状况检查

我们为 Sophos XDR 管理的端点持续检查设置和配置，确保其以峰值水平运行。

威胁隔离

对于未选择 Sophos MDR 执行全规模事件响应的组织，Sophos MDR 运营团队可以执行威胁隔离操作，打断威胁并阻止传播。这减少内部安全运营团队的工作量，让他们可以快速执行修复操作。

情报简报：“Sophos MDR ThreatCast”

Sophos MDR 运营团队提供的“Sophos MDR ThreatCast”是专为 Sophos MDR 客户提供的每月简报。它提供最新威胁情报和安全最佳做法的信息。

Breach Protection Warranty

包含在所有Sophos MDR Complete年度(一至五年)和月度许可证中，保修涵盖高达100万美元的响应费用。无任何担保层级、最短合同期限或额外购买要求。

Sophos 服务层级

	Sophos MDR Essentials	Sophos MDR Complete
专家领导的 24/7 全天候威胁监测和响应	✓	✓
兼容非 Sophos 安全产品	✓	✓
每周和每月报告	✓	✓
每月情报简报：“Sophos MDR ThreatCast”	✓	✓
Sophos 帐户运行状况金叉	✓	✓
专家领导的威胁追捕	✓	✓
威胁隔离：中断攻击，阻止传播 使用完整 Sophos XDR 代理（防护、侦测和响应）或 Sophos XDR Sensor（侦测与响应）	✓	✓
在活跃事件中直接电话支持	✓	✓
全规模事件响应：完全消除威胁 需要完整 Sophos XDR 代理（防护、侦测和响应）		✓
根本原因分析		✓
专门威胁响应负责人		✓
Breach Protection Warranty 赔付总共最多 100 万美元的响应费用		✓

Sophos MDR 包括许多集成功能

可以免费集成以下来源的安全数据供 Sophos MDR 运营团队使用。利用遥测来源扩大您环境内的可见性，生成新的威胁侦测，提高现有威胁侦测的保真度，开展威胁追捕，实现其他响应功能。

Sophos XDR

唯一结合本机端点、服务器、防火墙、云、电子邮件、移动和 Microsoft 集成的 XDR 平台

Sophos MDR定价中包含的产品

Sophos Firewall

监测并筛选传入传出网络流量，阻止高级威胁造成破坏

产品单独出售；免费集成

Sophos Endpoint

阻止高级威胁并侦测可疑行为—包括模拟合法用户的攻击者

Sophos MDR定价中包含的产品

Sophos Email

保护收件箱不受恶意软件影响，受益于先进人工智能阻止针对性身分假冒和网络钓鱼攻击带来的好处

产品单独出售；免费集成

Sophos 云端

阻止关键云服务内的云数据外泄并获得可见性，包括 AWS、Azure 和 Google Cloud Platform

产品单独出售；免费集成

90 天数据保留

在 Sophos 数据湖中保存来自所有 Sophos 产品和任何第三方（非 Sophos）产品的数据

Microsoft安全工具

- Microsoft Defender for Endpoint
- Microsoft Defender for Cloud
- Microsoft Defender for Cloud Apps
- Microsoft Defender for Identity
- Identity Protection (Azure AD)
- Microsoft Azure Sentinel
- Office 365 Security and Compliance Center

Microsoft审核日志

提供有关通过Office 365 Management Activity API摄入的用户、管理员、系统以及政策动作与事件的信息

Google Workspace

从Google WorkspaceAlert CenterAPI摄入安全遥测

第三方端点防护

兼容…

- Microsoft
- CrowdStrike
- SentinelOne
- Trend Micro
- BlackBerry (Cylance)
- Broadcom (Symantec)

附加功能集成

可以通过购买集成包，集成以下第三方来源的安全数据供 Sophos MDR 运营团队使用。利用遥测来源扩大您环境内的可见性，生成新的威胁侦测，提高现有威胁侦测的可信度，开展威胁追捕，实现其他响应功能。

Sophos Network Detection and Response

持续监测网络内的活动，发现设备之间发生的被忽视的可疑活动

通过 SPAN 端口镜像兼容任何网络

防火墙

兼容…

- Palo Alto Networks
- Fortinet
- Check Point
- Cisco Firepower
- Cisco Meraki
- SonicWall
- WatchGuard

身份识别

兼容…

- Okta
- Duo
- ManageEngine

公共云

兼容…

- AWS Security Hub
- AWS CloudTrail
- Orca Security

Email

兼容…

- Proofpoint
- Mimecast

网络

兼容…

- Darktrace
- Tinkst Canary
- Vectra

1 年数据保留

Sophos MDR Guided Onboarding

作为额外购买，Sophos MDR Guided Onboarding 可提供远程加入协助。该服务为顺利高效部署提供实践支持，确保最佳做法配置，提供培训以便最大程度发挥您的 MDR 服务投资的价值。Sophos Professional Services 部门会指派专属联系人，在服务启用后 90 天和您一起工作，确保实作成功。。Sophos MDR Guided Onboarding 包括：

第 1 天 – 实施

- 项目启动
- 配置 Sophos Central 并检查功能
- 建立和测试部署过程
- 配置 MDR 集成
- 配置 Sophos NDR 传感器
- 企业内部署

第 30 天 – XDR 培训

- 学习像 SOC 一样思考和行动
- 了解如何追踪入侵指标
- 了解将 XDR 平台用于管理任务
- 学习为未来调查开展查询

第 90 天 安全状态评估

- 检查当前政策，获得最佳做法建议
- 讨论还未使用的，可能提供额外防护的功能
- 符合 NIST 框架的安全评估
- 接收总结报告和我们审核的建议

要了解更多信息，请访问：

sophos.com/mdr

中国（大陆地区）销售咨询
电子邮件：salescn@sophos.com

23-06-04 DS-ZHCN (DD)

SOPHOS