解决方案手册

Sophos Managed Detection and Response

24/7 全天候威胁侦测和响应

Sophos MDR 是由专家提供的全托管 24/7 服务，他们侦测并响应针对您的计算机、服务器、网络、云工作负载、电子邮件账户、备份等的网络攻击。

勒索软件和入侵防护服务

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

通过托管检测与响应 (MDR) 功能在数据所在位置提供全面的安全覆盖，Sophos MDR 可以：

- **到比安全工具自身能识别的更多的网络威胁侦测**
  我们的工具自动阻挡 99.98% 的威胁，这使得我们的分析师能够专注于捕猎那些最先进的攻击者，只有经过高度训练的真人专家才能发现并阻止这些攻击者。

- **代表您采取措施，阻止威胁干扰您的业务**
  我们的分析师在数分钟内侦测、调查和 - 无论您需要全规模事件响应还是帮助您作出准确决策。

- **识别威胁的根本原因，避免未来事件发生**
  我们主动采取措施并提供建议，以降低贵组织的风险。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。

与您现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 的开放式 AI 原生平台兼容多种身份识别、网络、防火墙、电子邮件、云、生产力、备份和端点安全解决方案 - 并且无需额外费用，即可集成 Microsoft 和 Google Workspace。

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

MDR 满足您的需求

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 全天候威胁监控与响应

我们在威胁影响您的数据或导致停机前加以发现并响应。以 7 个全球安全运营中心 (SOC) 作为后盾，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、网络、身份辨识、电子邮件、备份和恢复等技术的遥测数据。

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。拥有 Sophos MDR Complete 授权许可证，您将获得无限制的全面事件响应，无上限和额外费用。

报告与服务见解

Sophos Central 是实时提醒、报告和管理的单一仪表板。详细报告与执行仪表板提供安全调查、网络威胁和安全状态的见解。

包括端点和工作负载保护

Sophos MDR 分析师可以利用您现有端点防护方案的遥测数据来侦测和响应针对您的计算机和服务器的威胁。或者，专用 Sophos Endpoint，享受更卓越的保护，无需额外费用。

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 运营团队提供全天候 24/7/365 服务，并得到全球 26 个据点支持团队作后盾。

专职事件响应负责人

我们为您指派专职事件响应负责人，一旦发现事件，负责人将立即与您的内部团队和外部合作伙伴协作，并与您合作，直至事件得到解决。

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 帐户健康检查

我们为 Sophos MDR 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

每周的 Sophos MDR “ThreatBrief” 简报和每月的现场 “ThreatCast” 网络研讨会，专为 Sophos MDR 客户而设，提供最新的威胁情报和安全最佳实践的深度见解。

入侵防护保固

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。

由 Sophos X-Ops 提供强大支持

Sophos X-Ops 汇聚在攻击环境中深厚的专业知识。我们的精英团队提供无与伦比的威胁情报，并持续为您构建和部署新的侦测规则，以应对活跃对手及其不断演变的战术。

所包括的集成

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 Endpoint

拦截高级威胁并侦测跨端点的恶意行为

Sophos MDR 定价中包含的产品

Workload Protection

为 Windows 和 Linux 服务器以及容器提供高级保护和威胁侦测

Sophos MDR 定价中包含的产品

Sophos Mobile

保护您的 iOS 和 Android 设备以及数据免受最新移动威胁的影响

产品单独出售；无需额外成本集成

Sophos Firewall

监测并筛选传入和传出网络流量，在高级威胁造成破坏前加以阻止

产品单独出售；需订购 Xstream Protection；集成无需额外费用

Sophos Email

通过先进的人工智能保护收件箱免受恶意软件的影响，阻止定向身份冒充和网络钓鱼攻击

产品单独出售；无需额外成本集成

Sophos Cloud Optix

阻止云服务关键数据泄露，并在 AWS、Azure 和 Google Cloud Platform 等关键云服务中获得可见性

产品单独出售；无需额外成本集成

Sophos ZTNA

用最小权限访问替代远程访问 VPN，安全连接您的用户到您的网络应用程序

产品单独出售；无需额外成本集成

第三方端点保护

集成包括：

- Broadcom Symantec
- CrowdStrike
- Cylance
- Jamf
- Microsoft
- SentinelOne
- Trend Micro

使用 Sophos ‘XDR Sensor’ 代理程序，与其他端点保护解决方案兼容

Microsoft 安全工具

- Defender for Endpoint
- Defender for Office 365
- Defender for Cloud Apps
- Defender for Identity
- Entra ID Protection
- Microsoft 365 Defender
- Microsoft Purview DLP

90 天数据保留

在标准情况下，侦测数据将在 Sophos 数据湖中保留 90 天

Microsoft Office 365 Management Activity

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

附加集成

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。利用遥测数据源扩展您环境的可见性，生成新的威胁侦测，提升现有威胁侦测的可信度，进行威胁追捕，并启用额外的响应能力。

Sophos NDR

持续监测网络内的活动，发现原本无法发现的设备之间发生的可疑活动

通过 SPAN 端口镜像兼容任何网络

防火墙

集成包括：

- Barracuda
- Check Point
- Cisco Firepower
- Cisco Meraki
- Fortinet
- F5
- Forcepoint
- Palo Alto Networks
- SonicWall
- Ubiquiti
- WatchGuard

网络

集成包括：

- Cisco Umbrella
- Darktrace
- Secutec
- Skyhigh Security
- Thinkst Canary
- Vectra
- Zscaler

身份识别

集成包括：

- Auth0
- Cisco ISE
- Duo
- ManageEngine
- Okta

包含 Microsoft 集成无需额外费用

电子邮件

集成包括：

- Mimecast
- Proofpoint
- Trend Micro

Microsoft 365 和 Google Workspace 的集成已经包含在内，无需额外收费

云

集成包括：

- Orca Security

Sophos Cloud Optix 产品包含 AWS、Azure 和 GCP 集成，需单独购买。

备份与恢复

集成包括：

- Acronis
- Rubrik
- Veeam

1 年数据保留

在 Sophos 数据湖中保留长达 1 年的侦测数据

附加服务

由 Tenable 技术支持的 Sophos Managed Risk

通过主动攻击面漏洞管理服务，降低网络安全风险。 Sophos Managed Risk 可识别高优先级漏洞，以便在攻击中断您的业务之前采取措施防止攻击。可作为 Sophos MDR 的附加服务提供。

Sophos MDR 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	✓	✓
包含 Sophos Endpoint 和 Sophos Workload Protection	✓	✓
兼容非 Sophos 安全产品	✓	✓
服务洞察与报告	✓	✓
Sophos 威胁情报简报	✓	✓
Sophos 帐户健康检查	✓	✓
专家领导的威胁追捕	✓	✓
威胁隔离：中断攻击，阻止传播 使用完整的 Sophos XDR 代理程序或 Sophos ‘XDR Sensor’ 代理程序	✓	✓
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 需要完整的 Sophos XDR 代理程序	IR 服务附加组件 *	✓
专责事件响应负责人	IR 服务附加组件 *	✓
根本原因分析	IR 服务附加组件 *	✓
入侵防护保固		✓
包含 Microsoft 和 Google Workspace 集成	✓	✓
与非 Sophos 防火墙、网络、电子邮件、云、身份辨识、备份和恢复解决方案集成	附加组件	附加组件
Sophos 网络侦测与响应 (NDR)	附加组件	附加组件
Sophos Managed Risk，由 Tenable 提供技术支持	附加组件	附加组件

*Sophos IR Services Retainer 长约服务的年度订阅可享有事件响应服务的折扣。确保您获得一支由事件响应专家组成的精英团队随时待命，帮助您在发生入侵事件时迅速恢复业务。

引导式上线（可选）

Sophos MDR Guided Onboarding 可提供远程登录协助服务，可作为额外的可选购买项。该服务提供实际支持，以确保顺利高效的部署，确保最佳实践的配置，并提供培训，以最大化您的 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 - MDR 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 MDR 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

看看客户为什么选择 Sophos MDR

Sophos 是托管式侦测与响应领域的领先者，备受业界认可。

IDC

在 2024 年全球托管式侦测与响应 IDC MarketScape 报告中，我们被评为领导者。

Gartner peerinsights™

在 2024 年 Gartner® 托管式侦测与响应客户之声报告中，Sophos 获评为“客户之选”

G2 Leader

在 2025 年冬季 G2 Grid® 托管式侦测与响应报告中获客户评为总体领导者

FROST & SULLIVAN

在 2024 年 Frost Radar 全球托管式侦测与响应报告中，Sophos 获评为领导者之一。

MITRE | ATT&CK® Evaluations

在 MITRE ATT&CK Evaluations for Managed Services 表现优异

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

© Copyright 2025.Sophos Ltd. 保留所有权利。
英格兰和威尔士注册号：2096520，地址：The Pentagon, Abingdon Science Park, Abingdon, OX14 3YP, UK
Sophos 是 Sophos Ltd. 的注册商标。提及的所有其他产品和公司名称均为其各自所有者的商标或注册商标。

2025-02-03 BRZHCN (PS)

SOPHOS