解决方案手册

Sophos Extended Detection and Response
Sophos 扩展式侦测与响应

借助全面的 EDR 和 XDR 来抵御活跃的攻击敌手

迅速阻止攻击至关重要。Sophos XDR 提供了强大的工具和威胁情报，让您能够在整个 IT 环境中侦测、调查和响应可疑活动。

建基于最强大的保护之上

当更多的威胁被提前阻止时，资源紧张的 IT 团队需要调查和解决的事件就会减少。Sophos 将 XDR 与业界最强大的端点防护相结合，在需要手动调查威胁之前就将其阻止，减轻您的工作负担。

内置端点侦测与响应 (EDR)

Sophos XDR 包括全面的 EDR 工具，包括强大的、可定制的搜索功能，可以访问 90 天的端点和服务器数据，以及对设备的安全远程访问。可以调查问题、安装/卸载软件、终止进程等等。

将可见性扩展至端点之外

发现的越多，行动就越快。来自 Sophos 和非 Sophos 产品的事件被摄取、过滤、关联和优先级排序——扩展至所有关键攻击面的可见性，使您能够快速侦测和阻止活跃的攻击敌手。

广泛的 Sophos XDR 就绪的解决方案

Sophos 技术在 XDR 平台上无缝协同工作，以提供最佳的安全成效。原生解决方案集成包括 Sophos Endpoint、Sophos Workload Protection、Sophos Mobile、Sophos Firewall、Sophos NDR、Sophos ZTNA、Sophos Email 和 Sophos Cloud。

与您现有的工具和技术兼容

利用广泛的非 Sophos 安全工具的遥测技术，从现有的技术投资中获得更多的投资回报率，同时加快安全操作。集成包括身份识别、网络、防火墙、电子邮件、云、生产力和端点安全技术。

产品亮点

- 获得所有关键攻击面可疑活动的可见性
- 统一的 XDR 平台，集成广泛的 Sophos 解决方案
- 利用现有工具和广泛非 Sophos 技术集成的投资来提升效益
- 通过人工智能排优先序的侦测和优化的工作流程，快速调查和响应威胁
- 包括 Sophos 行业领先的端点保护和 EDR 功能

加快侦测、调查和响应

Sophos XDR 包含旨在最大限度地提高安全分析师和 IT 管理员的效率的工具和功能。人工智能引导的调查帮助您快速了解事件范围和原因，并最大限度地缩短响应时间。

跨所有关键攻击面的 AI 排优先序的侦测

轻松识别需要立即关注的可疑活动。Sophos XDR 自动根据风险对侦测进行优先级排序，提供完整的背景信息。

快速调查和捕猎威胁

强大的搜索工具，包括预设查询模板，使您能够无需成为 SQL 专家都可更快地找到所需数据。

协作个案管理

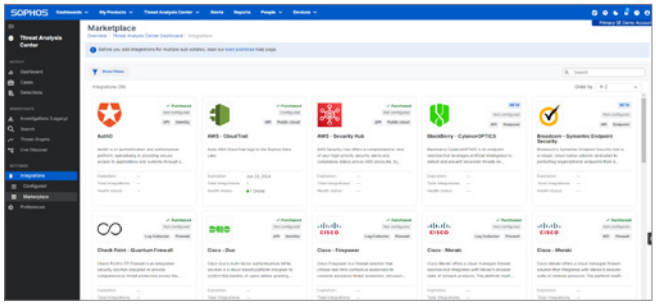
自动创建个案，支持快速调查，并提供全面的个案管理工具，便于与团队其他成员合作。

MITRE ATT&CK Framework 映射

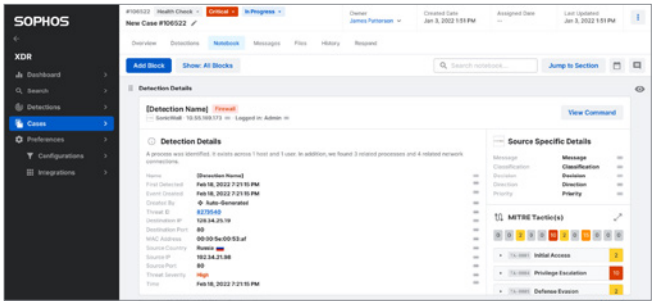
侦测和个案自动映射到 MITRE ATT&CK Tactics，使您能够轻松识别防御中的漏洞并优先改进。

自动化和加速响应

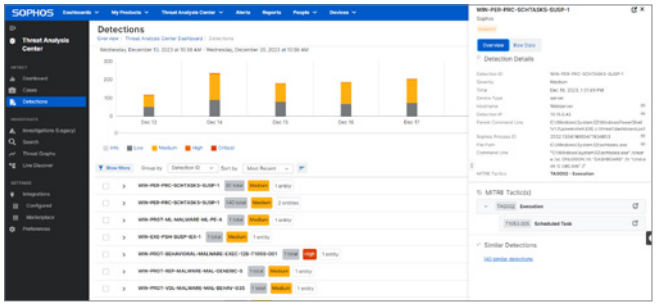
自动执行的操作，如进程终止、勒索软件回滚和网络隔离，可以迅速遏制威胁，为您节省宝贵的时间。



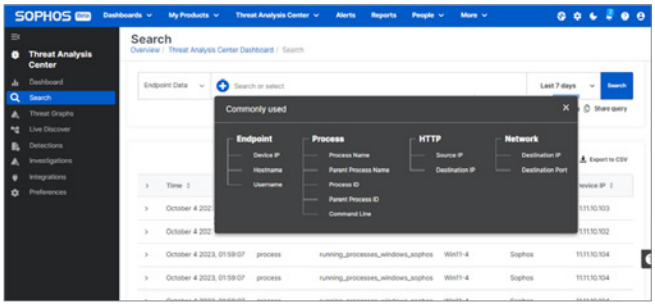
兼容 Sophos 和第三方解决方案



强大的个案管理和协作工具



AI 排优先序侦测所有关键攻击面



简单而强大的搜索——不需要 SQL 专业知识

Sophos XDR 包括的集成功能

无需额外成本把以下来源的安全数据和Sophos XDR 平台集成。利用遥测来源扩大您跨环境的可见性，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。

Ep Sophos 端点

拦截高级威胁并侦测跨端点的恶意行为

Sophos XDR定价中包含的产品

WP 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 XDR定价中包含的产品

Mob 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

Fw 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；无需额外成本集成

Em 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

Cld Sophos Cloud

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

ZT 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

兼容：

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

+与具有 Sophos ‘XDR Sensor’ 代理的其他解决方案兼容

Microsoft Security Tools

- Defender for Endpoint
- Defender for Cloud
- Defender for Cloud Apps
- Defender for Identity
- Microsoft Entra ID
- Azure Sentinel
- Office 365 Security and Compliance Center

90 天数据保留

在 Sophos Data Lake 数据湖中保存来自 Sophos 产品和第三方（非 Sophos）产品的数据

延长至 1 年的可选附加组件

Microsoft Audit Logs

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

通过购买Integration Packs 集成包，可以将以下来源的安全数据集成到 Sophos XDR 平台。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 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

兼容：

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

网络

兼容：

- Darktrace
- Secutec
- Thinkst Canary
- Skyhigh Security

身份识别

兼容：

- Auth0
- Duo
- ManageEngine
- Okta

包括微软集成
无需额外收费

电子邮件

兼容：

- Proofpoint
- Mimecast

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

公共云

兼容：

- AWS Security Hub
- AWS CloudTrail
- Orca Security

通过单独销售的 Sophos Cloud 产品，您可以集成额外的 AWS、Azure 和 GCP 数据

备份与恢复

兼容：

- Veeam

1 年数据保留

在 Sophos 数据湖中保存来自 Sophos 产品和第三方（非 Sophos）产品的数据

建基于全球最佳的端点保护之上

将在入侵发生之前就加以阻止，让您专注于调查。大多数 XDR 产品迫使分析师浪费宝贵的时间来调查本应由其保护方案阻止的事件。Sophos 将 XDR 与业界最强大的端点防护相结合，在需要手动调查威胁之前就将其阻止，并减轻您的工作负担。

Sophos XDR 订购包括 Sophos Intercept X Endpoint，提供先进的反勒索软件和反漏洞利用功能、人工智能驱动的恶意软件保护以及动态调整保护级别的环境敏感型防御。

访问 www.sophos.com/zh-cn/products/endpoint-antivirus.aspx了解更多

以完全托管的服务形式取得侦测与响应能力

选择使用 Sophos XDR 来自行侦测与调查威胁，或者选择使用 24/7 全天候托管服务，解放您的员工让其专注其他工作。通过 Sophos 托管式侦测与响应 (MDR)，我们的专业威胁猎手和分析师团队可以为您提供即时的安全运营中心，包括全面的事件响应能力。

访问www.sophos.com/zh-cn/products/managed-detection-and-response了解更多

包含在 Sophos XDR 订购中

	Sophos XDR
AI排优先序的侦测和指导式调查	✓
个案管理、协作和响应行动	✓
简单而强大的搜索工具来捕猎和调查	✓
Sophos Endpoint 端点和 Workload Protection 解决方案 (Intercept X Advanced)	✓
端点侦测与响应 (EDR) 工具	✓
云数据保留	90 天 (可延长至一年)
用于 EDR 的丰富端点和服务器的设备上数据	✓
与 Sophos 解决方案集成: Sophos Endpoint, Sophos Workload Protection, Sophos Mobile, Sophos Firewall, Sophos ZTNA, Sophos Email, Sophos Cloud	✓
Sophos 网络侦测与响应 (NDR)	可选的附加组件
与非 Sophos Endpoint Protection 解决方案集成	✓
与 Microsoft 解决方案集成	✓
与 Google Workspace 生产力解决方案集成	✓
与非 Sophos 防火墙、网络、电子邮件、云、身份、备份和恢复解决方案集成	可选的附加组件

看看客户为什么选择 Sophos XDR

Sophos 是扩展式侦测与响应领域公认的领导者，备受业界认可。

Gartner

Sophos 在连续 14 次报告中被评为 2023 年 Gartner® 魔力象限™ 端点保护平台领域的领导者

Gartner Peer Insights Customers' Choice 2023

Sophos 是 EPP、MDR、防火墙和移动威胁防御领域唯一被选为客户之选的厂商

G2 Leader

在 2024 年冬季报告中，G2 将 Sophos 评为端点保护、EDR、XDR、防火墙和 MDR 的领导者

OMDIA

Sophos 成为 2023 年度 Omdia Universe for Comprehensive XDR排名最高而且是唯一的领导者

MITRE ATT&CK

Sophos 在 2023 年 MITRE Engenuity ATT&CK 评估中 取得了优异的成绩

SE Labs

Sophos 在独立测试中始终取得业界领先的保护成绩

立即免费试用

注册即可享受 30 天免费评估试用，
请访问：www.sophos.com/xdr

中国（大陆地区）销售咨询
电子邮件：salescn@sophos.com

2024-02-01 DS-ZHCN (NP)

SOPHOS