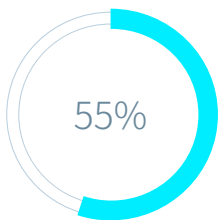


Sophos 扩展侦测与响应 (XDR)

防御复杂的多阶段、多途径攻击

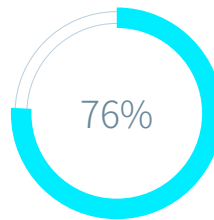
迅速阻止攻击至关重要。Sophos XDR 提供强大的工具和威胁情报，依托 Sophos 自适应 AI 原生开放平台，帮助您在整个 IT 环境中侦测、调查并响应可疑活动。



在 55% 的勒索软件攻击中，攻击者利用合法凭证和未知漏洞渗透组织。¹



在 Sophos 事件响应团队调查的案例中，攻击者的平均滞留时间为 7 天。²



各自为政的工具会造成数据孤岛和额外的手动操作。76% 的组织在过去一年中经历了网络安全倦怠。³

产品亮点

- 全面掌握所有关键攻击面的可疑活动与规避型威胁。
- 开放式 XDR 平台，内置丰富的集成能力。
- 提升现有技术投资回报。
- 借助优先级侦测与 AI 驱动工具，快速调查并响应威胁。
- 内置业界领先的端点防护与 EDR 能力。

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 将扩展侦测与响应与业界领先的端点防护深度融合，在威胁进入人工调查前即予以阻断，减轻工作负担。

掌握全面的攻击面可见性

发现的越多，行动就越快。我们的开放、可扩展架构通过将来自您现有安全投资中的威胁信息整合到统一的侦测与响应平台中，提供对整个 IT 环境的可见性。Sophos XDR 包括与广泛工具和技术的集成。

通过生成式人工智能 (GenAI) 加速安全运营

最大化分析师效率，加速调查与响应。Sophos XDR 包含的 AI 人工智能驱动工具通过提供实时洞察、情景化威胁数据，并提供明确的建议，来简化调查过程。

专为优化与统一而设计的开放平台

通过统一的视图全面掌握您的 IT 生态系统，便于集中精力调查高优先级问题，而非杂乱无用的警报。借助 AI 驱动的优先级排序和分析，识别最严重的威胁，并通过稳健的调查 workflow 和案件管理工具与团队成员进行协作。

高效侦测、调查与响应

Sophos XDR 提供旨在提高安全分析师和 IT 管理员效率的工具和工作流程。自动生成的案件帮助您快速调查潜在威胁，了解事件的范围和原因，并最大限度地缩短响应时间。



AI 优先级排序的侦测

轻松识别需要立即关注的可疑活动。Sophos XDR 基于风险自动对侦测结果进行优先级排序，并提供完整上下文信息。



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。



快速调查和捕猎威胁

自然语言 AI 搜索与预置查询模板，让您无需精通 SQL，也能快速获取调查所需信息。



自动响应

自动化操作比如如进程终止、勒索软件回滚、网络隔离和自适应攻击防护，能够快速遏制威胁，为您的团队节省宝贵时间。



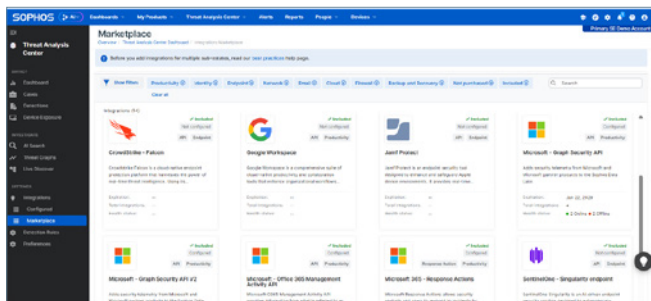
协作个案管理

自动创建个案，支持快速调查，并提供完善的案件管理工具，便于团队协作。

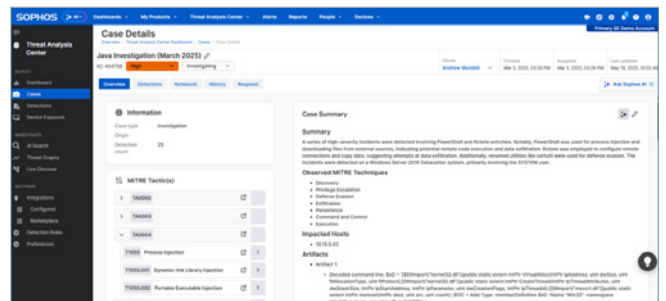


分析师响应操作

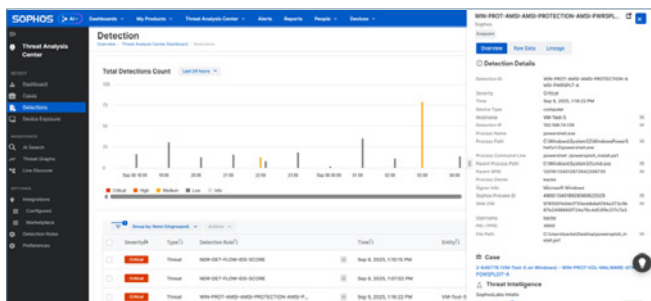
执行广泛的响应操作，快速遏制和消除威胁，包括在 Microsoft 365 环境中的操作。



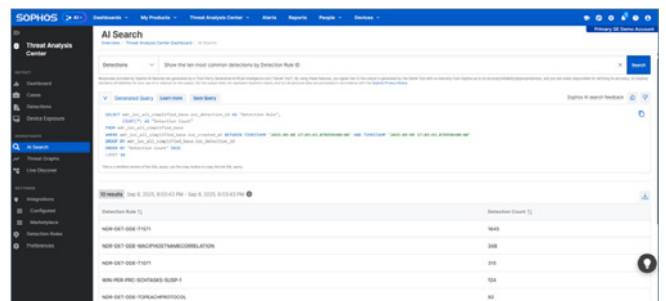
支持与 Sophos 及非 Sophos 解决方案的集成。



个案管理与协作工具。



AI 优先级侦测，覆盖所有关键攻击面。



自然语言 AI 搜索——不需要 SQL 专业知识

通过生成式人工智能（GenAI）加速安全运营

Sophos XDR 广泛的生成式 AI 能力赋能团队做出更明智的决策，更快遏制威胁，全面提升分析师与业务信心。

Sophos XDR 自动包含 GenAI 功能。



AI Assistant

引导不同技能水平的用户完成案件调查的每个阶段，最大限度提高效率，快速阻止威胁。



AI 搜索

采用自然语言来加速日常任务，降低安全运营的技术障碍。



AI 个案摘要

提供清晰易懂的侦测概览和处置建议，帮助分析师快速决策。



AI 命令分析

分析复杂的命令行参数，揭示其意图和影响，并以通俗易懂的语言进行解释。

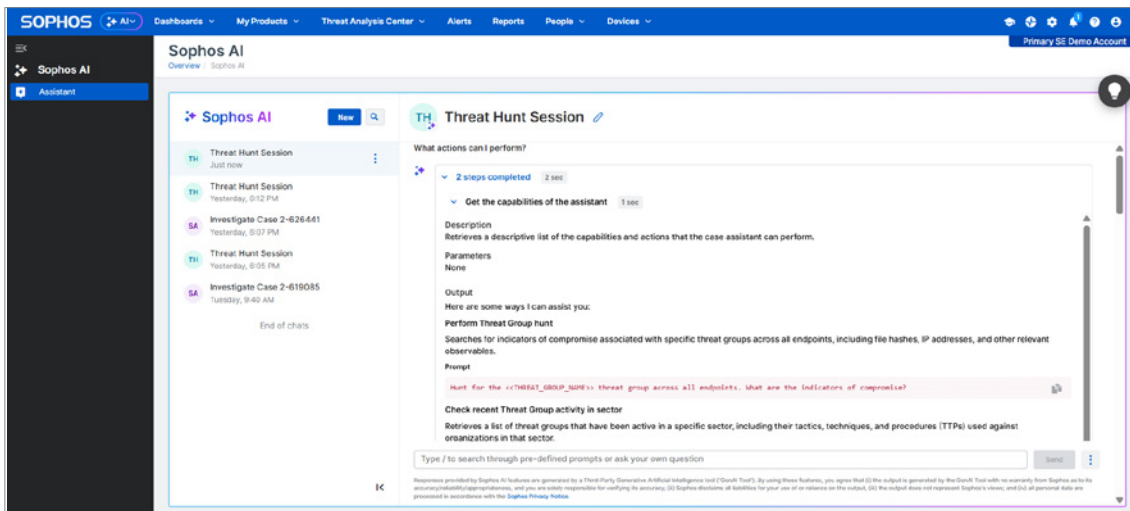


Sophos AI Assistant

Sophos AI Assistant 让从 IT 通才到 Tier 3 SOC 分析师的各类用户都能轻松获取所需信息，加快威胁调查进程并快速遏制威胁。

- 执行广泛的 SecOps 任务：分析可疑命令、列出 IOC（入侵指标）、结合威胁情报丰富数据，并生成详细报告等。
- 使用日常语言提问，或使用 Sophos 威胁专家提供的预定义提示。受益于清晰的摘要和推荐的后续步骤。
- 与 Sophos 一线安全分析师协作设计：受益于真实世界的工作流和 Sophos MDR 专家的丰富经验。
- 根据威胁态势持续更新：持续提供来自 Sophos X-Ops 的最新调查技术和威胁情报，确保能力始终保持前沿。

这不仅是一款 AI 工具，更融合了全球领先托管侦测与响应（MDR）团队的专业经验，打造为智能助手。



Sophos “XDR-ready” (XDR 就绪) 产品集成

Sophos 解决方案无缝协作，提供最佳的安全成效。我们屡获殊荣的产品 - 涵盖 Endpoint、Firewall、NDR、ZTNA、Email 和 Mobile - 均已全面集成至 XDR 平台，并自动包含业界领先的 **Sophos Endpoint** 防护能力。

SOPHOS ENDPOINT

阻止针对端点和服务器的高级威胁，包括复杂的勒索软件攻击。

Sophos XDR 默认包含

SOPHOS EDR

侦测、调查和响应针对端点的可疑活动和规避性威胁。

Sophos XDR 默认包含

SOPHOS ITDR

监控环境中的身份识别风险，并获取暗网上泄露凭证的情报。

产品单独出售；无需额外成本集成

SOPHOS FIREWALL

监测并过滤进出网络的流量，在高级威胁造成破坏前将其阻断。

产品单独出售；需要有 Xstream Protection 订阅；集成无需额外费用

SOPHOS NDR

持续监测网络内部活动，侦测设备之间原本难以察觉的可疑行为。

产品单独出售；集成无需额外费用。通过 SPAN 端口镜像兼容任意网络。

SOPHOS ZTNA

以最小权限访问替代远程访问 VPN，安全连接用户与网络应用。

作为 Sophos Workspace Protection 套件的一部分单独销售；集成无需额外费用。

SOPHOS MOBILE

保护 iOS 和 Android 设备及数据免受最新移动威胁侵害。

产品单独出售；无需额外成本集成

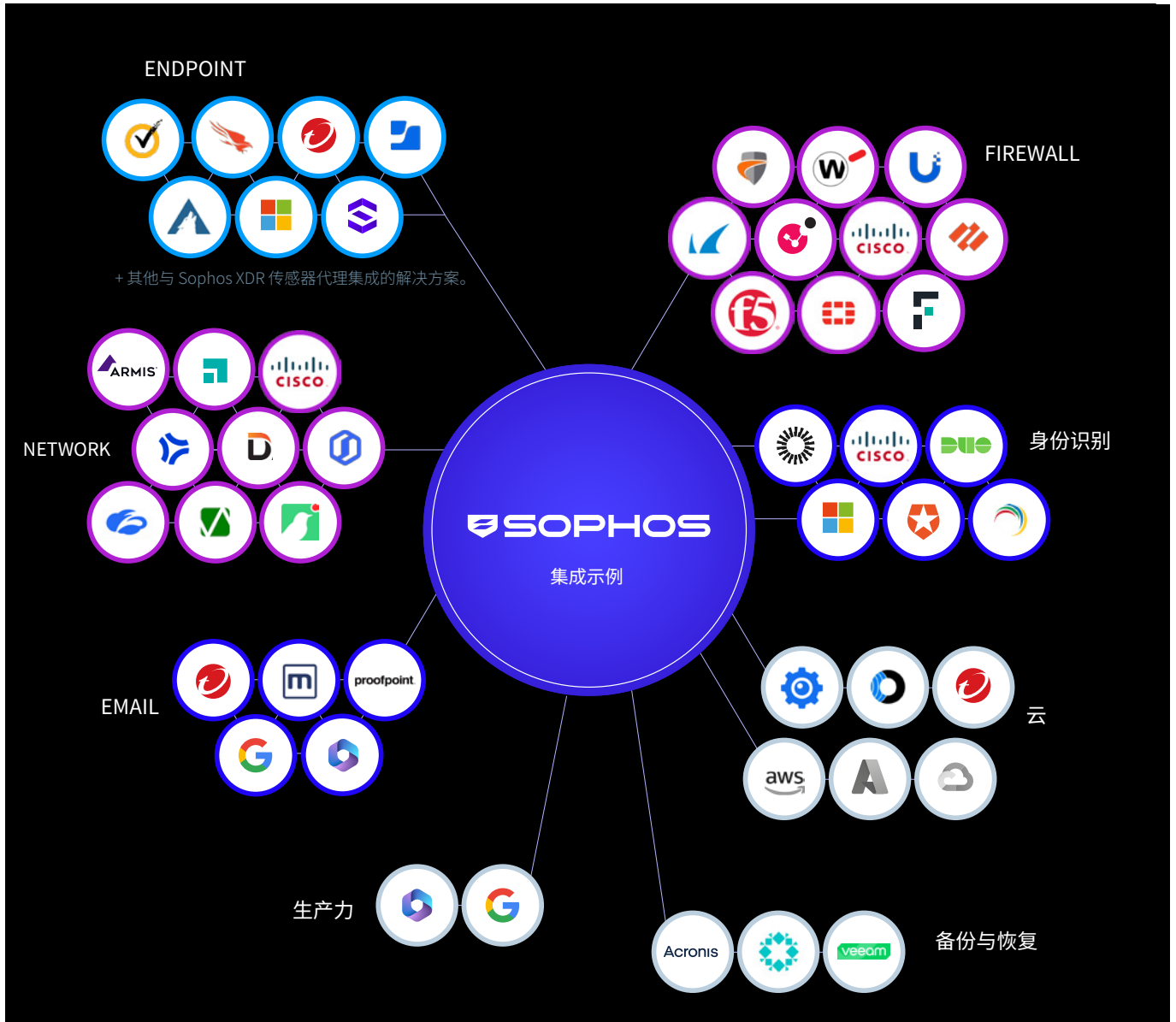
SOPHOS EMAIL

借助先进 AI 保护收件箱免受恶意软件侵害，并阻止定向冒充和钓鱼攻击。

产品单独出售；无需额外成本集成

充分利用您的非 Sophos 技术投资

将现有的安全工具集成到我们的开放平台，获得更高的 ROI。Sophos XDR 包含可即用的集成，涵盖广泛的第三方生态系统，包含端点、防火墙、网络、电子邮件、身份识别、备份、云安全和生产力工具，包括 Microsoft 365。



以上为非 Sophos 技术集成的代表示例。

建基于全球最佳的端点保护之上

将调查的重点放在入侵发生之前就加以阻止。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 与业界领先的端点防护深度融合，在威胁进入人工调查前即予以阻断，从而减轻工作负担。

Sophos XDR 订阅包括 Sophos Endpoint，提供高级反勒索软件和反漏洞利用、AI 驱动的恶意软件防护，以及可在应对主动攻击时动态提高防护级别的自适应防御。

访问 sophos.com/endpoint 了解更多

获得以完全托管服务形式提供的侦测与响应

您可以选择使用 Sophos XDR 自行侦测与调查威胁，或选择全面的 7 × 24 托管服务，释放员工精力。通过 Sophos Managed Detection and Response (MDR)，我们经验丰富的分析师团队可为您提供即时的安全运营中心，并具备全面的事件响应能力。

访问 sophos.com/mdr 了解更多

包含在 Sophos XDR 订阅中

	Sophos XDR
AI 生成的威胁评分和排优先级的侦测	✓
个案管理、协作和响应行动	✓
自然语言搜索工具，助力威胁追踪与调查	✓
GenAI 驱动的 XDR 功能： AI Assitant、AI 案件摘要、AI 命令分析、AI 搜索	✓
包含 Sophos Endpoint（或使用您现有的非 Sophos 端点解决方案）	✓
侦测数据保留在 Sophos 数据湖中（标准为 90 天）	✓
支持 1 年数据保留	可选的附加组件
与 Sophos 解决方案原生集成： Sophos Endpoint、Sophos Mobile、Sophos Firewall、Sophos ZTNA、Sophos Email	✓
与非 Sophos 端点、防火墙、网络、电子邮件、云、安全、备份、Microsoft 365 和 Google Workspace 解决方案的集成	✓
Sophos 网络侦测与响应 (NDR)	可选的附加组件
Sophos Identity Threat Detection and Response (ITDR)	可选的附加组件

看看客户为什么选择 Sophos XDR

Sophos 是扩展侦测与响应领域的公认领导者，并获得广泛的业界认可。

Gartner

连续第 16 次入选 2025 年 Gartner® endpoint 防护平台魔力象限™ 领导者。



在 2025 年 Gartner® 扩展侦测与响应客户之声报告中，Sophos 获评为“客户之选”。



领导者

在 G2 2025 年春季 Overall Grid® 报告中，Sophos 获评为扩展侦测与响应领域的领导者。



Sophos XDR 在 MITRE ATT&CK Evaluations for Enterprise products 中表现强劲。



Sophos 在 SE Labs 独立安全测试中持续取得业界领先的防护成绩。

- 1 Sophos 2025 勒索软件现状报告
- 2 2025 年 Sophos 主动攻击敌手报告
- 3 Sophos 2025 年网络安全倦怠问题应对报告

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.cn/xdr

中国（大陆地区）销售咨询
电子邮件：salescn@sophos.com