

Sophos Endpoint 和 EDR

完整的端点防护、侦测与响应

业界最先进的 AI 驱动端点安全解决方案

Sophos Endpoint 采用预防优先的策略和顶尖的端点安全技术，为抵御高级网络攻击提供无与伦比的防护。Sophos Endpoint Detection and Response (EDR) 端点侦测与响应是一套涵盖防护、侦测与响应的全面解决方案，包含 Sophos Endpoint，专为安全分析师和 IT 管理员设计。无论端点和服务器位于办公场所、远程环境还是云端，都能实现全面保护与监控，防范可疑活动。

以预防为先的安全策略

Sophos Endpoint 采用全面的、预防优先的安全策略，能够在不依赖单一技术的情况下自动阻止威胁。深度学习 AI 模型可防御已知和新型攻击。而控制措施能减少攻击面，同时结合行为分析、反勒索软件、反漏洞利用以及其他先进技术，快速在威胁升级前加以阻止。

自适应防御

当 Sophos Endpoint 侦测到人工操作型攻击时，会以“架起防御”方式动态启用额外防护，及时阻止攻击敌手的攻击行动。这一由 Sophos 独有的业界首创功能，可最大限度减少攻击面，中断并遏制攻击，阻止网络犯罪分子进一步行动，同时为您的团队争取宝贵的响应时间。

取得隐匿威胁的深入信息

Sophos EDR 提供 AI 优先级排序的威胁侦测，突出显示需要立即关注的可疑活动。即使设备处于离线状态，您都可通过访问 Sophos data lake 数据湖中丰富的本地设备数据与遥测信息（包括历史活动记录），以实时分析活动。

加速并赋能您的团队

Sophos EDR 专为 IT 通才和安全分析师设计。强大的工具可帮助您的团队通过与设备的直接安全连接，快速、轻松地执行广泛的 IT 运维任务。以结果为导向的 AI 工具可简化调查与响应流程，使您的团队能够快速、精准地调查并消除针对端点和服务器的可疑活动与隐蔽威胁。

产品亮点

- 预防优先的策略，可减少攻击面并快速阻止威胁
- 凭借业内领先的防护技术，抵御本地和远程勒索软件攻击，保障数据安全。
- 利用业界首创的动态防御机制，自动适应主动攻击敌手和手动键盘攻击。
- AI 优先级排序的侦测可突出显示团队应重点关注的领域。
- 以结果为导向的 AI 工具可简化对可疑活动和隐蔽威胁的调查与响应流程。
- 为 IT 通才和安全分析师提供强大的工具。

以预防为先的安全策略可有效减少您的受攻击面

早期阻止攻击的所需资源相较于在攻击链的后期进行监控和修复要低得多。Sophos Endpoint 包含先进的防护技术，可拦截最广泛类型的攻击。Web、应用程序和外设控制功能可有效减少受攻击面，阻止常见攻击媒介，从而降低攻击者渗透环境的可能性。

Web 防护

拦截出站浏览器的连接，并阻止前往恶意或可疑网站的流量。它防止用户被重定向到恶意软件交付或网络钓鱼网站，以在交付阶段阻止威胁。

Web 控制

阻止访问不良或不适当内容。在整个组织内执行可接受的网络使用规范，并防止数据外泄。

下载信誉

使用 SophosLabs 全球威胁情报分析下载文件，根据普及度、创建时间和来源提供判定结果，并提示用户封锁信誉度低或未知的文件。

应用程序控制

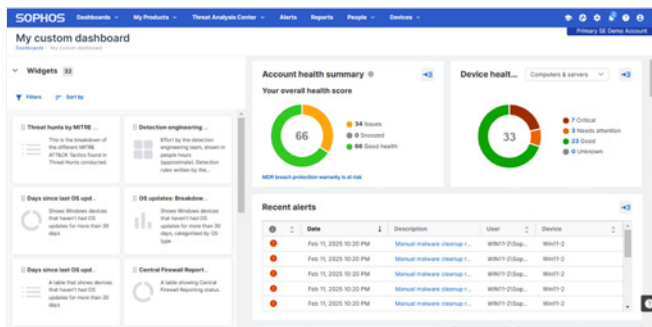
阻挡可能存在漏洞、不适合您环境，或可能被用于恶意目的的应用程序。Sophos 提供了预定义类别，以阻止或监控应用程序，从而免除通过哈希值阻止单个应用程序的繁琐任务。

外围（设备）控制

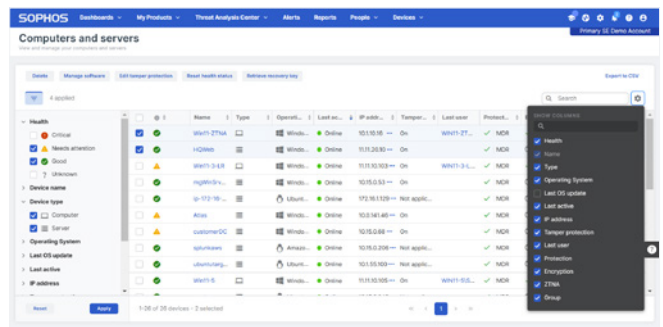
监控并阻止对可移动存储设备、蓝牙和移动设备的访问，防止特定硬件连接到您的网络。

数据丢失防护

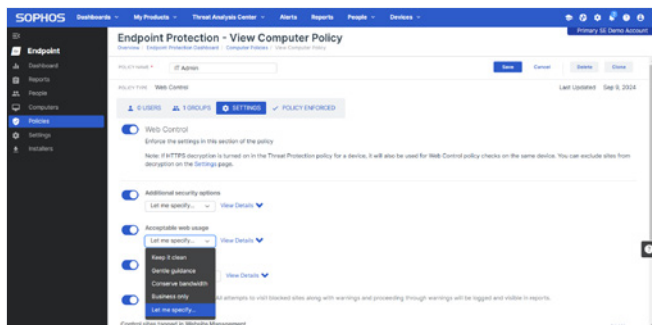
监控或限制包含敏感数据的文件传输。例如，防止用户通过网页版电子邮件发送机密文件。



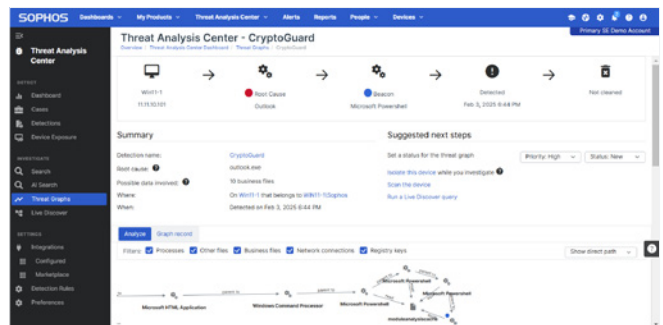
创建自定义仪表板以满足您的需求。



易于设置和管理的端点安全。



可自定义的政策，预设启用建议的设定。



分析威胁并确定其根本原因。

预防为主策略可快速拦截威胁

尽早侦测和修复威胁可降低风险。Sophos Endpoint 在威胁升级前迅速加以阻止，让资源有限的 IT 团队减少需要调查和解决的事件。Sophos 提供强大的威胁防御能力，其在独立安全测试中持续获得顶尖评分得以验证。

严密的勒索软件防护



根据 Microsoft 2024 年《数字防御报告》，在 70% 的成功攻击中都发现有远程加密，其中 92% 源自网络中的非受管设备。Sophos Endpoint 提供最强大的零接触端点防御，有效抵御本地和远程勒索软件攻击。其先进的 CryptoGuard 技术可侦测加密尝试，无论其来源如何。

- 阻止新的和新型勒索软件变种。
- 实时检查文件变化，以侦测恶意加密行为。
- 防止远程勒索软件通过网络远端加密文件。
- 自动将已加密文件恢复至原始未加密状态，采用专有技术，无需依赖 Windows Shadow Copy Service。
- 保护所有文件类型和大小，同时将对性能的影响减到最低。
- 保障主引导记录（MBR）安全，防御针对硬盘的高级攻击。

深度学习（AI 驱动）恶意软件防御

通过分析文件属性和预测性推理以识别威胁，来侦测并阻止已知和未知的恶意软件。

反漏洞利用

通过强化应用程序内存并应用运行时代码执行防护机制来保护进程完整性。Sophos Endpoint 内置超过 60 种反利用技术，全部默认启用，无需额外培训或调优。这些技术带来的防护远远超过 Windows 以及大多数其他端点安全解决方案所能提供的。

行为防护

持续监控进程、文件和注册表事件，以侦测并阻止恶意行为和进程。它还执行内存扫描，检查正在运行的进程以便侦测只有在进程执行过程中才能发现的恶意代码，并侦测攻击者为规避侦测在运行进程的内存中植入恶意代码。

同步安全 (Synchronized security)

Sophos Endpoint 与 Sophos Firewall、Sophos Wireless、Sophos 零信任网络访问 (ZTNA) 及其他 Sophos 产品共享状态和健康信息，提供关于威胁和应用程序使用情况的额外可见性，并自动隔离受感染设备。

实时防护

借助实时查找 SophosLabs 最新的全球威胁情报，扩展全面的本地设备防护，提供额外的文件环境信息、决策验证、误报抑制以及文件信誉。我们的一级威胁研究提供了来自 Sophos 广泛的产品组合和全球客户群的额外实时情报。

应用程序锁定

阻止与浏览器和应用程序处理程序不常相关的异常行为，防止其被滥用。例如，web 浏览器或 Office 应用程序试图启动 PowerShell。

反恶意软件扫描界面 (AMSI)

Windows 反恶意软件扫描接口 (AMSI) 可判断脚本（如 PowerShell 或 Office 宏）是否安全，包括在运行时被混淆或生成的情况，从而阻止恶意软件直接从内存加载的无文件攻击。Sophos 还拥有针对试图逃避 AMSI 侦测的恶意软件的专有缓解措施。

恶意流量侦测

通过拦截来自非浏览器进程的流量，并分析其是否指向恶意地址，从而侦测设备是否试图与命令与控制 (C2) 服务器通信。

自适应防御

Sophos Endpoint 提供业界首创的动态防御，可实时适应来对抗主动攻击敌手及手动键盘攻击，来实现自动化保护。自适应防御会阻止那些在常规情况下看似无害，但在攻击过程中可能造成危害的操作。它们能够动态响应并中断正在进行的攻击，即使攻击者已经取得立足点，业无需触发告警或依赖恶意代码来侦测。

自适应攻击防护

动态防御可在侦测到手动键盘攻击时，动态加强端点防护，遏制攻击敌手行动，同时争取更多响应时间。

严重攻击警告

根据对全组织的威胁侦测，通知系统管理员多个端点上正在发生的严重攻击活动。

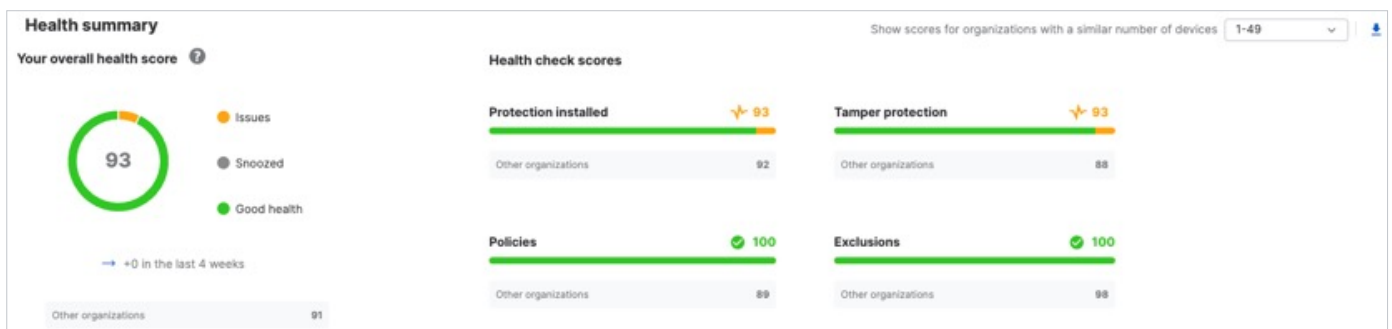
	行为防护	自适应攻击防护	严重攻击警告
范围	单个设备	单个设备	整个网络环境
优势	行为引擎可阻止主动攻击敌手的攻击的早期阶段	提高防护敏感度以预防攻击	向您发出需要立即响应的攻击警报
触发	行为规则	侦测到黑客工具集	侦测到高影响的主动攻击敌手迹象，包括组织级的相关性和界限值
类比	 “开启防御！”	 “升起防御！”	 “红色警戒！”

Sophos Endpoint 的自适应防御功能

强大的默认政策与安全状态偏移识别

默认情况下，Sophos Endpoint 会启用我们推荐的防护技术，立即为您提供最强的保护设置。无需进行复杂的配置或调优。但如有需要，您也可以选择更精细的控制。

不恰当的政策设置、排除项以及其他配置问题，都可能导致您的安全状况受到威胁。帐户健康检查功能可识别安全状态偏移和高风险的配置错误，并让您一键即可修复问题。



帐户健康检查

加速侦测、调查与响应

Sophos EDR 是一套涵盖防护、侦测与响应的全面解决方案，专为 IT 通才和安全分析师设计。Sophos EDR 让您响应隐蔽威胁并降低其对业务的潜在影响，从而降低安全风险。Sophos Endpoint 已包含在其中，并与 Sophos EDR 原生集成。



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 EDR 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。



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。



安全分析师响应

您的团队可以隔离某个端点，在调查可疑活动时手动启用自适应攻击防护等操作。



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 案件摘要

提供易于理解的侦测概览和推荐的后续步骤，帮助您快速做出明智决策。



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。

Live Response 实时响应

Sophos EDR 让 IT 通才和安全分析师能够快速、精准地执行 IT 运维任务并修复威胁。与端点和服务器建立直接、安全且可审计的连接，使您能够在 Sophos 控制台中直接调查并修复潜在问题。



远程访问设备以执行以下操作：

- 安装和卸载软件
- 运行脚本和程序
- 编辑配置文件
- 关机 / 重启
- 运行第三方鉴证工具
- 以及更多

设备暴露

快速识别您环境中存在的风险、过时或存在漏洞的设备。设备暴露功能为您提供最易受威胁的设备的消息，并使您能够针对一段时间未进行操作系统更新的设备采取措施。

Sophos Endpoint 和 Sophos EDR 所包含的功能

	Sophos Endpoint	Sophos EDR
新一代端点防护 深度学习 (AI 驱动) 的恶意软件防护、反勒索软件、行为分析、反漏洞利用等。	✓	✓
Adaptive Defenses 适应防御 自适应攻击防护, 严重攻击警告	✓	✓
端点威胁暴露减少 包括 web 防护、web 控制、外围设备控制、应用控制和数据丢失防护	✓	✓
端点侦测与响应 (EDR) 侦测、调查并响应针对端点和服务器的攻击		✓
实时响应与设备暴露 Live R 为 IT 通才和安全分析师提供的强大工具		✓
侦测数据保留在 Sophos 数据湖中 (标准为 30 天)		✓ (可升级至 1 年)
Sophos Endpoint for Legacy Platforms 为传统和已停止支持的 Windows 和 Linux 操作系统提供全面安全防护	可选的附加组件	可选的附加组件
Sophos Device Encryption 设备加密 对 Windows 和 macOS 设备上的原生磁盘加密进行集中管理	可选的附加组件	可选的附加组件
Sophos 事件响应 (IR) 长约服务 一支顶尖专家团队在发生安全事件时随时待命	可选的附加组件	可选的附加组件

Sophos XDR

Sophos 扩展式侦测与响应 (XDR) 提供超越端点和服务器范围的可见性。它通过 Sophos 自适应 AI 原生开放平台, 提供强大的工具和威胁情报, 使您能够在整个 IT 生态系统中侦测、调查并消除威胁。

我们开放且可扩展的架构可整合您现有及未来的安全投入所产生的威胁信息, 从而在整个攻击面上实现可见性。Sophos XDR 内置与广泛生态系统的即开即用集成, 涵盖端点、防火墙、网络、电子邮件、身份识别、备份、云安全及生产力解决方案。

欲了解更多信息, 请访问: www.sophos.com/XDR

Sophos MDR

无论您身处安全防护的哪个阶段, 我们的 Sophos Managed Detection and Response (MDR) 服务始终助您领先攻击敌手一步。我们将易于使用的 AI 技术与全球一流安全专家相结合, 提供 24 小时不间断的威胁监控、预防、侦测与响应服务。

可根据需求灵活选择不同的服务等级与威胁响应模式。Sophos MDR 可整合您现有及未来的安全投入所生成的威胁信息。

欲了解更多信息, 请访问: www.sophos.com/MDR

了解客户为何选择 Sophos Endpoint

Sophos 是端点安全领域的知名领导者，并拥有业界认可作为背书。

Gartner

Sophos 在 2025 年 Gartner® 魔力象限™端点保护平台报告中，已连续 16 次获评为领导者。

SE Labs

Sophos 持续在独立端点安全测试中获得业界领先的防护成绩。



领导者

Sophos 是唯一一家在 G2 2025 春季整体 Grid® 报告中获评为端点防护套件、EDR、XDR、防火墙软件和 MDR 类别的领导者的厂商。



Sophos 获评为 2024 年 IDC MarketScape 中小型企业的全局现代端点安全的领导者之一。



Sophos 在 Gartner® Peer Insights™ 的 2025 年客户之声报告的端点防护平台领域中获得“客户之选”荣誉的厂商。

立即免费试用

注册免费试用 30 天，请访问：
sophos.com/endpoint

中国（大陆地区）销售咨询
电子邮件：salescn@sophos.com