解决方案手册

Sophos Endpoint

由 Intercept X 驱动

业界最先进的 AI 驱动端点安全解决方案

由 Intercept X 技术驱动的 Sophos Endpoint 提供卓越的防护能力，在高级攻击对您的系统造成影响之前将其拦截。强大的端点和扩展式侦测与响应 (EDR/XDR) 工具使您的组织能够捕猎、调查和响应可疑活动和攻击指标。

以预防为先的安全策略

Sophos Endpoint 采用全面，以预防为主的安全方法，而非依赖于单一的技术来阻止网络威胁。多个深度学习 AI 模型能够防御已知和前所未见的攻击。Web、应用程序和外围设备控制减少受攻击面，并阻止常见攻击媒介。行为分析、反勒索软件、反利用技术以及其他先进技术可以快速阻止威胁在扩展之前，从而让资源紧张的 IT 团队减少需要调查和解决的事件。

严密的勒索软件防护

Sophos Endpoint 是业界最强大的零接触端点防御方案，可有效抵御高级勒索软件攻击。CryptoGuard 技术可实时阻止恶意加密，并将所有受影响的文件自动回滚到其原始状态，从而最大限度地减少对业务的影响。

适应性防御

业界首创的动态防御，可适应以响应主动攻击敌手和手动键盘攻击。这剥夺攻击者执行操作的能力，有效干扰并遏制攻击，同时争取宝贵的响应时间。

易于设置和管理

Sophos Central 是强大的云端网络安全管理平台，统一管理所有 Sophos 下一代安全解决方案。推荐的安全技术和功能默认启用，确保您无需调整，即可立即获得最强大的防护。

值得信赖的端点安全行业领导者

Sophos Endpoint 持续获得客户、分析师和独立测试机构的高度认可。Sophos 已连续 16 次获评为 Gartner® 魔力象限™ 中的端点防护平台领域的领导者，并在 2025 年春季 G2 Grid® 报告中获评为首屈一指的端点侦测与响应解决方案。

产品亮点

- 多种深度学习 AI 模型可防御已知和前所未见的攻击。
- 通过 web、应用程序和外设控制减少受攻击面，阻止常见攻击媒介。
- 利用行为分析、反勒索软件、反漏洞利用和其他先进技术，在威胁升级前迅速拦截。
- 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。
- 通过强大的 EDR 和 XDR 工具，捕猎、调查并响应可疑活动。

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

阻止流向对恶意网站的出站浏览器流量，在威胁投递阶段就加以拦截，有效防止网络钓鱼和恶意软件攻击。

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

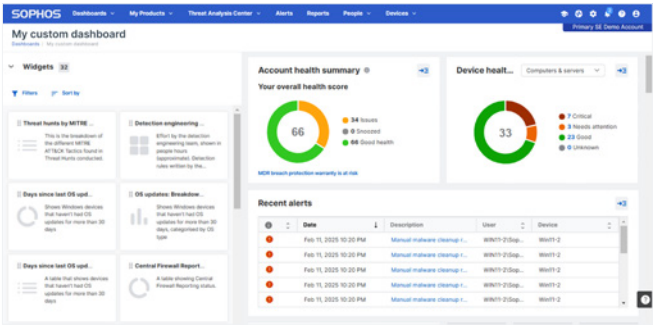
通过预定义类别来阻止易受攻击或不适当的应用程序，无需逐个根据哈希值进行拦截。

外围（设备）控制

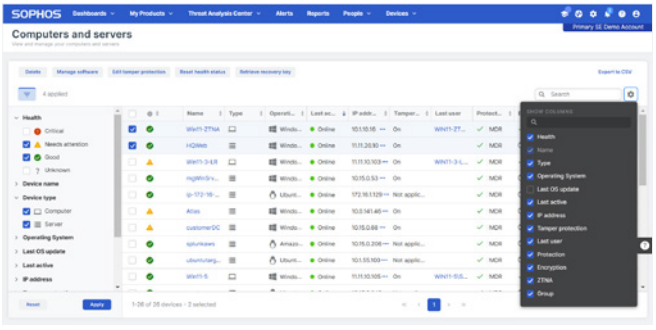
监控并阻止对可移动存储设备、蓝牙和移动设备的访问，防止特定硬件连接到您的网络。

数据丢失防护

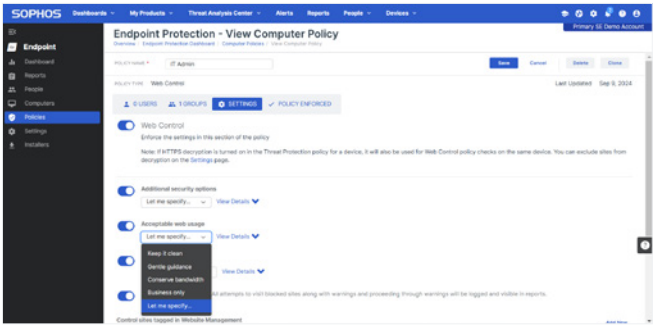
监控或限制包含敏感数据的文件传输。例如，防止用户通过网页版电子邮件发送机密文件。



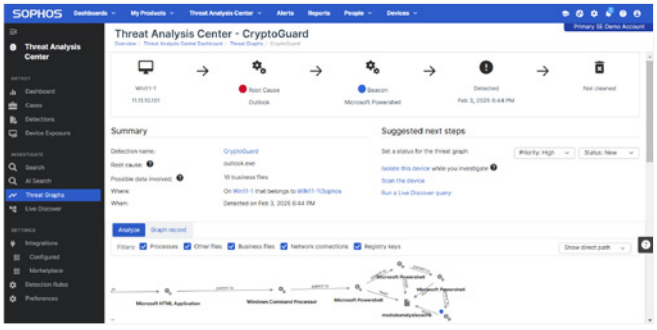
创建自定义仪表板以满足您的需求。



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。

预防为先的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。

AI 驱动的深度学习恶意软件防护

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

通过内存加固和 60 多种反漏洞利用技术来保护进程完整性，无需调整，并超越原生 Windows 及其他安全解决方案的能力。

行为防护

监控进程、文件和注册表事件，以侦测并阻止恶意活动。扫描内存，检查运行中的进程以发现隐藏威胁，并侦测攻击者为了规避侦测而注入恶意代码的行为。

同步安全（Synchronized security）

Sophos Endpoint 与 Sophos Firewall、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

通过实时查询 SophosLabs 的全球威胁情报，以查找额外的档案环境内容、决策验证、误报减量及档案信誉，来扩展强大的装置端防护。

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。

反恶意软件扫描界面 (AMSI)

Windows 反恶意软件扫描界面（AMSI）阻止恶意软件直接从内存加载的无文件攻击。Sophos Endpoint 还包括专有的针对规避 AMSI 侦测的缓解措施。

恶意流量侦测

通过拦截并分析非浏览器流量中的恶意目的地，来侦测出和命令与控制 (C2) 服务器通讯的装置。

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。Sophos Endpoint 会阻止那些在日常环境中不一定带有恶意，但在攻击情境下存在危险性的操作。这一功能可以动态响应和中断作动中的攻击，即使攻击者可能在没有引起警觉，也没有使用恶意代码的情况下取得立足点。

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

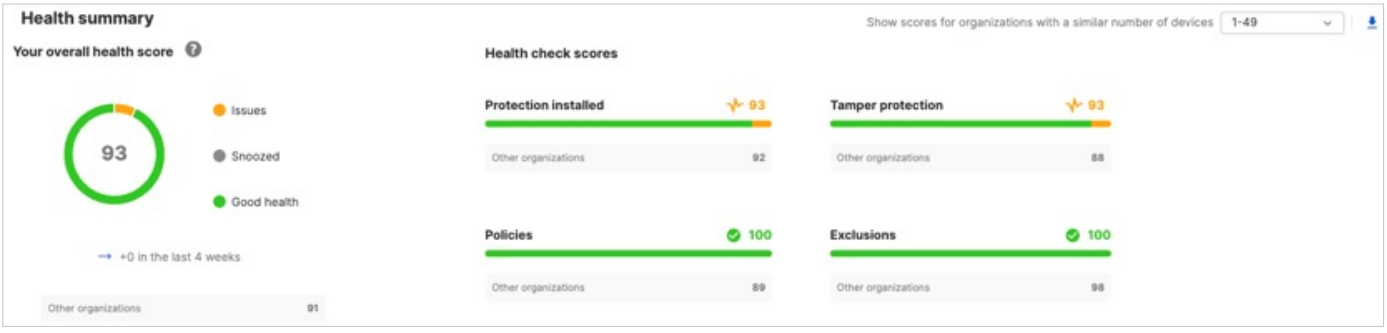
根据对全组织的威胁侦测，通知系统管理员多个端点上正在发生的严重攻击活动。

	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

识别安全状态的偏差

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差和高风险的配置错误，并让您一键修复问题。



帐户健康检查

其他防护层（附加功能）

Sophos ZTNA

通过终极 VPN 替代品，安全地将您的用户连接到应用程序。Sophos ZTNA 是唯一与下一代端点防护紧密集成的零信任网络访问解决方案。

设备加密

鉴于设备每日都可能丢失或被盗，全磁盘加密至关重要。与 Sophos Endpoint 整合的设备加密功能可有效管理 BitLocker（Windows）和 FileVault（macOS）。

加速侦测、调查与响应

Sophos Endpoint 可自动预先拦截绝大多数威胁，减少需要调查的安全事件数量。针对需要人工分析的可疑活动和威胁，Sophos 提供强大的分析能力，能够快速侦测、调查并响应所有主要攻击媒介。

Sophos XDR

Sophos Extended Detection and Response (XDR) 扩展式侦测与回应使您能够在您的整个安全环境中捕猎、调查并响应可疑活动及多阶段攻击。我们的强大 GenAI 工具由安全分析师设计，适用于各种技术水平的用户 - 从普通 IT 人员到资深 SOC 分析师，均可快速调查威胁并消除攻击敌手的威胁。

Sophos XDR 提供与端点、防火墙、网络、电子邮件、身份辨识、生产力、云和备份解决方案的广泛生态系统的现成集成，使您能够从现有安全工具中获得更多投资回报。

欲了解更多信息，请访问：www.sophos.com/XDR

Sophos MDR

对于缺乏内部资源管理威胁侦测和响应的组织而言，Sophos Managed Detection and Response (MDR) 托管式侦测与响应是由一组安全分析师、威胁猎人和事件响应专员组成的菁英团队所提供的全天候服务。Sophos MDR 使用来自 Sophos 和第三方安全解决方案的遥测数据，来侦测并消除即使是最复杂的威胁。

Sophos MDR 根据您的需求提供多种服务层级和响应模式，可适应您的组织需求，并与您现有的工具和技术兼容。

欲了解更多信息，请访问：www.sophos.com/MDR

	Sophos Endpoint	Sophos XDR	Sophos MDR
下一代威胁防护 AI 驱动的深度学习反恶意软件和 web 防护	✓	✓	✓
恶意活动拦截 反勒索软件、反漏洞利用、适应性防御	✓	✓	✓
威胁暴露减少 数据丢失防护 (DLP)、web、外设和应用控制功能	✓	✓	✓
侦测与响应 强大的威胁调查和响应工具		✓	✓
关键攻击面可视化 Sophos 与第三方技术集成		✓	✓
托管式侦测与响应 24/7 全天候专家主导的威胁监控和事件响应			✓

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。

IDC

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

Gartner Peer Insights Customers' Choice 2025

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

2025-07-16 BR-ZHCN (NP)

SOPHOS