解决方案概要

# Sophos Endpoint

## 利用 AI 驱动的安全防护，预防入侵、勒索软件攻击及数据丢失

Sophos Endpoint 提供无与伦比的高级网络攻击防御。通过全面的纵深防御作法，包括严密的勒索软件保护，可在最广泛的威胁对系统造成影响之前加以阻挡。GenAI 驱动的 EDR 和 XDR 工具帮助您的团队快速、精准地侦测、调查并响应复杂的多阶段威胁。

## 使用案例

### 1 | 以预防为主的方法

**期望结果：**在前期阻止更多的威胁，以最大限度地降低风险，并减少调查和响应的工作负担。

**解决方案：**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了攻击面，并阻止常见攻击向量。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。

### 2 | 自适应防御

**期望结果：**借助动态防护功能，可以随攻击演化自动调整，从而阻止主动攻击敌手。

**解决方案：**当 Sophos Endpoint 侦测到实际手动操作的攻击时，它会自动激活额外的防御，采取“提高防御屏障”的方法以阻止攻击敌手。在这种增强的防护模式下，远程管理工具下载等可疑活动将被立即阻止，从而为您的团队争取宝贵的额外时间来响应。

### 3 | 侦测与响应

**期望结果：**防御无法单靠技术阻止的复杂的多阶段攻击。

**解决方案：**强大的 EDR 和 XDR 工具让您可以侦测、调查和响应 Sophos 和第三方安全产品的可疑活动。内部资源有限的组织可以使用 Sophos 托管式侦测与响应 (MDR) 服务，或利用 Sophos 事件响应服务长约服务，在出现网络入侵时快速取得我们精英专家团队的支持。

### 4 | 简化管理

**期望结果：**专注于安全威胁，而不是管理。

**解决方案：**Sophos Central 是基于云的 AI 原生网络安全管理平台，统一管理所有 Sophos 下一代安全解决方案。强大的默认政策设置可确保贵组织能够立即拥有建议的防护，而无需额外的培训或调整。Sophos Central 的帐户运行状况检查可辨识配置问题，并提供简单的即点即修修复功能，以加强您的安全状态。

Gartner

*连续 15 次荣登 2024 年 Gartner® 端点保护平台魔力象限™ 领导者之一*

Gartner Peer Insights Customers' Choice 2024

*2024 年 Gartner® 端点保护平台客户之声报告中的“客户之选”*

SE Labs

*在独立的第三方防护测试中获得行业领先的佳绩*

**#1**

*最强大的零接触端点防御，抵御远程勒索软件*

**了解更多并开始免费试用：**
www.sophos.com/endpoint

© 版权所有 2025。Sophos Ltd. 保留所有权利。英格兰和威尔士注册编号 2096520，The Pentagon、Abingdon Science Park、Abingdon、OX14 3YP、UK。Sophos 是 Sophos Ltd. 的注册商标。所有提及的其他产品和公司名称均属各自拥有者的商标或注册商标。

Gartner Magic Quadrant for Endpoint Protection Platforms, 23 September 2024, Evgeny Mirolyubov, Franz Hinner, Deepak Mishra, Satarupa Patnaik, Chris Silva. Gartner 是 Gartner, Inc. 和 / 或其附属公司在美国和国际上注册的商标和服务标志，而 Magic Quadrant 是 Gartner, Inc. 和 / 或其附属公司的注册商标，在此已获得授权使用。保留所有权利。Gartner 不认可于研究出版物中描述的任何供应商、产品或服务内容，以及没有建议技术用户仅选择具有最高评分或其他头衔的厂商。Gartner 的研究发表作品由 Gartner 研究企业的意见组成，不应被解释为对事实的陈述。Gartner 对于此项研究不做任何担保，明示或者暗示，包括任何用于商业用途或者某个特定目的的承诺。

SOPHOS

2025-02-03 SB-ZHCN (MP)