解决方案概要

Sophos Endpoint for Legacy Platforms

捍卫重要系统：关键系统的全方位安全解决方案

制造业和医疗保健等行业的组织经常需要为专门系统 (包括机械和医疗设备) 运行采用传统操作系统的端点。网络犯罪分子往往针对这些传统系统，因为它们为入侵网络提供了更容易的缺口，这使得强大的端点安全至关重要。Sophos Endpoint for Legacy Platforms 为 Windows 和 Linux 系统提供全面保护，由自适应的 AI 原生网络安全平台驱动。

使用案例

1 | 简化网络安全管理

期望结果：简化跨所有设备的端点安全部署和管理。

解决方案：只支持现代操作系统的安全解决方案驱使组织为传统系统部署不同的单独解决方案，给 IT 和安全团队带来管理负担。而 Sophos 在 Sophos Central 为传统和现代平台都提供行业领先的端点安全防护，这是是一个强大的基于云的管理平台，统一了所有 Sophos 下一代安全解决方案。

2 | 推迟困难且昂贵的升级

期望结果：保护超出平台厂商支持期限的关键设备。

解决方案：在运营技术（OT）环境中的端点可能难以升级或替换，而且成本高昂，因此设备可能会保留现状依然未受保护，或需要额外的安全缓解措施。而 Sophos 在平台厂商提供的标准支持结束日期之后，依然保护一系列 Windows 和 Linux 操作系统。

3 | 用下一代安全技术保护传统设备采 </45

期望结果：传统系统受先进的网络安全技术保护。

解决方案：Sophos 的端点安全技术根植于我们独特的以预防为先的方法，可减少数据泄露并提高侦测和响应成效。Web、应用程序和外围控制可减少威胁面，并阻止针对您的传统设备的常见攻击媒介，而 AI 模型可防范已知和前所未见的攻击。我们独特的 CryptoGuard 反勒索软件和反漏洞利用技术能够快速阻止威胁，因此资源有限的 IT 团队需要调查和解决的事件就会相继减少。

4 | 侦测、调查和应对高级威胁

期望结果：消除无法单靠技术阻止的复杂攻击。

解决方案：传统操作系统可能缺乏现代系统中存在的安全功能和更新，使其成为攻击敌手更容易利用的目标。Sophos 的 AI 驱动的 EDR 和 XDR 工具让您侦测、调查和响应跨您的所有设备的的可疑活动，包括传统系统。拥有有限内部资源的组织可以采用 Sophos MDR 服务来监控和响应高级威胁。

行业认可

Gartner

连续 16 次荣登 2025 年 Gartner® 端点保护平台魔力象限™ 领导者之一

Gartner Peer Insights Customers' Choice 2025

2025 年 Gartner® Peer Insights ™ 端点保护平台的“客户之选”。

操作系统覆盖[1]:

- Windows 7
- Windows 8.1
- Windows Server 2008 R2
- Windows Server 2012/2012 R2
- Red Hat Enterprise Linux 7
- CentOS 7
- Oracle Linux 7
- Debian 10
- Ubuntu 18.04 LTS

查阅详情：
www.sophos.com/endpoint

[1] 发布时的操作系统覆盖范围正确。请参考产品文以档获取最新信息。

Gartner, Magic Quadrant for Endpoint Protection Platforms, Evgeny Mirolyubov, Deepak Mishra, Franz Hinner, 14 July 2025.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。

2025-08-19 SB-ZHCN (MP)