电子邮件安全

通过云电子邮件安全保护您的人员和关键信息免于恶意软件，以及不含恶意软件的网络钓鱼和模仿举动，再次信任您的收件箱。

阻止网络钓鱼和骗子威胁

许多网络攻击从网络钓鱼开始。危险不在于电子邮件本身，而是让人们所做的事情，例如包含恶意链接或攻击者试图欺骗您启动恶意软件的电子邮件。

Sophos 将网络钓鱼骗子拦截在外，自动识别不含恶意软件的模拟和商业电子邮件破坏攻击的高价值目标，然后通过对邮件内容机器学习分析、发件人身份验证、URL 保护和云沙箱来拦截攻击。

阻止恶意软件进入收件箱

多层防护利用超过 35 年的威胁情报、信誉和行为分析以及先进的机器学习，让恶意软件和恶意 URL 再也无法进入收件箱。

Sophos 的云沙箱分析所有文件进程、文件活动、注册表活动和网络连接，阻止勒索软件、其他形式恶意软件、漏洞攻击和 PUA。利用深度学习人工智能拦截零日威胁。

对数据安全安心

Sophos Email 通过无缝集成加密自动扫描邮件和附件中的敏感数据。

通过针对组和各个用户的多规则 DLP 策略阻止数据丢失，确保保护敏感信息，发现所有电子邮件和附件中的财务、保密内容、健康信息和 PII。

加密邮件，添加数字签名以通过 S/MIME 验证发件人身份，或者选择可自定义的加密选项，包括 TLS 加密、附件加密（PDF 和 Office），或者附加全 Web 门户加密。

产品亮点

- 与商业电子邮件提供商集成：Microsoft 365、Google Workspaces Gmail 等
- 基于 API 的电子邮件安全，用于 Microsoft 365，带有投递后保护
- 拦截垃圾邮件、恶意软件、勒索软件和恶意 URL
- 拦截不含恶意软件的网络钓鱼和模仿攻击
- 利用电子邮件加密和数据防丢失功能保护敏感数据
- 还在 AWS Marketplace 提供

SOPHOS

Microsoft 365 安全

Sophos Email 可在数分钟内与 Microsoft 365 (M365) 电子邮件集成。基于 API 的电子邮件安全确保更快设置和电子邮件处理。

- Sophos 邮件流规则连接可在 Sophos Central 控制台中数分钟完成，无需 MX 记录重定向。
- 只要威胁状态发生改变，持续投递后保护自动移除含有新感染 URL 的网络钓鱼电子邮件。
- 直接集成邮件流意味着更快处理所有电子邮件，同时仍提供同样的先进防护。

中央化威胁情报实现更快响应

最大化安全投资，通过 Sophos XDR 数据湖的端点和电子邮件防护的共享威胁情报，找出环境中从未见过的攻破迹象。扩大 Microsoft 365 套件、服务器工作负荷、移动设备和网络等中的可见性。

全面报告

Sophos 通过清晰的仪表板、邮件总结和详细威胁报告扩大可见性。

- 邮件历史记录（显示系统处理的所有邮件日志）
- 邮件总结（显示所有电子邮件总结）
- 沙箱高级威胁总结（结论报告，包括 VirusTotal 结果 & MITRE ATT&CK Matrix 战术）
- 点击时间总结（拦截、警告和允许的 URL 量）
- DLP 违规（DLP 策略记录的邮件）
- 投递后总结（投资后移除的 M365 邮件总结）
- 许可证使用总结

提高团队效率

通过 Sophos 的单个云管理控制台，在一天中做更多工作。数百万人信任 Sophos 提高他们的网络安全消息，以及简化设置、部署和管理电子邮件防护、端点、服务器负载、移动设备安全、防火墙、零信任、公共云安全等，全部来自单个位置。

Sophos Email 功能亮点

访问 www.Sophos.cn/email 查看所有功能

防护功能	Email Advanced	防护功能	Email Advanced
Microsoft 365 邮件流规则	✓	显示名称分析	✓
Microsoft 365 投递后防护	✓	类似域名检查	✓
防垃圾邮件和恶意软件扫描	✓	多规则 DLP 策略	✓
云沙箱	✓	内容控制列表	✓
恶意 URL 检测	✓	实施 TLS 加密	✓
点击时 URL 重写	✓	S/MIME	✓
SPF、DKIM、DMARC	✓	基于推送的加密	✓
模仿网络钓鱼防御	✓	基于拉取的加密	附加组件

了解更多信息，或联系专家

www.sophos.cn/email

中国（大陆地区）销售咨询
电子邮件：salescn@sophos.com

22-02-23 DS-ZHCN (PS)

SOPHOS