思科高级网络钓鱼保护

增强对复杂身份欺骗威胁的防御，始终比邮件攻击领先一步

为本地邮件部署以及 Office 365 和 GSuite 等云邮件平台提供保护

网络攻击者不断寻找新方法来潜入您的网络；欺骗、勒索软件、网络钓鱼、零日攻击和企业邮件入侵 (BEC) 全都是攻击者利用身份欺骗来成功入侵组织的一些新方式。根据 FBI 的数据，BEC 通过冒充您的 CEO 或其他高管欺骗毫无戒心的员工，让全球的企业损失了 53 亿美元[1]。组织越来越需要增加保护层来保护用户免遭欺诈性发件人的攻击。

思科®高级网络钓鱼保护提供发件人身份验证和 BEC 检测功能。它使用先进的机器学习技术、实时行为分析、关系建模和遥感勘测来抵御基于身份欺骗的威胁。这些情报会不断调整，以便实时获得发件人的相关信息，防范漏洞并增强保护。

机器学习的强大功能

思科高级网络钓鱼保护利用了机器学习建模以下三方面的功能。

- 确定收件人所判定的邮件发件人身份
- 分析与该身份相关的预期发送行为以确定有无异常
- 衡量关系以确定预期发送行为；关系越密切（例如同事之间），行为异常阈值就越严格，因为如果被骗，他们面临的整体风险更高

预防

- 不含恶意负载或 URL 的 BEC
- 使用受感染账户和社交工程的攻击
- 网络钓鱼
- 勒索软件
- 零日攻击
- 欺骗

优势

- 可以快速部署基于传感器的解决方案，以确保您的用户完全免受破坏性漏洞攻击
- 提供另一层防御，以更有效地保护您的邮件环境
- 实时获得发件人的相关信息，了解并验证邮件身份和行为关系，以防止 BEC 攻击
- 自动删除用户收件箱中的恶意邮件，并调用身份欺骗技术，以防止电汇欺诈或其他高级攻击
- 详细了解邮件攻击活动，包括保护的邮件总数和阻止的攻击

工作原理

思科高级网络钓鱼保护通过云或在本地以轻量级传感器的形式部署。

- 传感器接收安全邮件网关判定 “安全” 的所有邮件
- 确定邮件是否是恶意邮件
- 预先配置的策略会立即阻止或重定向邮件以进行进一步的事件调查

技术亮点

- 基于每天 3 亿多次模型更新，使用预测性人工智能对可信通信进行建模
- 一流的 BEC 保护结合快速 DMARC、高级显示名称保护和类似域检测功能来阻止攻击
- 合作伙伴欺诈防御为供应链合作伙伴建模，自动生成并持续更新策略，从而防止可信合作伙伴受到欺诈
- 支持增强型机器学习功能的账户接管 ID 能够为 ATO 威胁行为建模，以阻止来自受感染邮件账户的攻击
- 智能内容检测将基于 AI 的仿冒分析、URL 和文件分析结合在一起，以检测避开了 SEG 的恶意内容
- 邮件调查分析和执行提供可定制的策略，通过自动警报或 API 集成来强制采取措施或向安全运营团队报告恶意活动

1 企业邮件入侵、邮件账户入侵，诈骗造成 50 亿美元的损失，2017 年