CLOUDFLARE

解决方案简述

Cloudflare + Microsoft 365 网络钓鱼防护

提供自主、多渠道保护，确保工作空间通信安全

抛弃传统网关，升级网络钓鱼防护

在 21 世纪初，引入了安全电子邮件网关 (SEG)，以应对日益增长的电子邮件路由和过滤需求。虽然多年来 SEG 成功完成了使命，但是随着网络钓鱼威胁的范围和复杂程度快速增长，SEG 的基本设计使它们无法跟上这种增长速度。

持续更新最初为本地服务器构建的手动规则集和策略只会增加维护 SEG 所需的时间和精力。这导致了成本和复杂程度增加，同时仍然无法捕捉到最危险的威胁，如商业电子邮件泄露 (BEC) 攻击。开销的增加和效率的降低可归因于：

- **新出现的网络钓鱼策略和 zero-day 威胁：**现代攻击采用欺骗性越来越强的策略，旨在躲过静态过滤器和传统控制。这使得 SEG 难以阻止缺少已知入侵指标的新威胁。
- **复杂的部署：**SEG 需要大量的配置和不断的调整来应对新出现的威胁，同时还需要多个附加模块来充分利用其功能。
- **耗费时间的事件响应：**当可疑或恶意活动绕过部署的 SEG 控制时，调查和响应过程可能会漫长而繁琐，涉及到各种各样的界面和工作流程。

部署高效率、低干预的保护

随着组织继续采用 Microsoft 365 来增强其混合型员工的沟通和协作，务必在利用 Microsoft 的原生安全功能的同时，集成基于机器学习的补充解决方案，以自动阻止和隔离最危险的威胁。该策略不仅可显著降低网络钓鱼风险，还可简化工作流程，最大限度地减少持续安全管理所需的时间和精力。

91%

的网络攻击从网络钓鱼电子邮件开始[1]

排名第 1 的

攻击手段，用于实施欺诈并获得访问权限[2]

500 亿美元

过去十年来 BEC 攻击造成的损失[3]

488 万美元

这是 2024 年数据泄露平均成本[4]

1. 2020 年 Deloitte 研究
2. Microsoft SIR 报告
3. 2023 年 FBI IC3 PSA
4. 2024 年 IBM 数据泄露成本

Microsoft 的电子邮件安全性功能

移除 SEG 重叠以降低风险和成本

分析师一致认为，整合功能以最大限度地减少重叠功能有助于组织降低成本和复杂性。然而，他们也建议组织仔细评估原生功能，以确保它们满足所有用例。

随着 Microsoft 继续构建其基本电子邮件安全功能，与 SEG 的重叠日益增加为组织提供了一个机会，通过利用其 E3 或 E5 许可证中已包含的功能来简化安全操作。这一转变使组织能够消除复杂且昂贵的 SEG 部署，将一部分预算重新分配用于集成轻量级解决方案，以有效解决最危险的网络钓鱼威胁。

Cloudflare 电子邮件安全提供了一种集成的低干预解决方案，它使用机器学习威胁分析来增强 Microsoft 365，以自动检测 BEC 和多渠道攻击。

与 SEG 功能重叠的领域包括：

- **电子邮件卫生**
  基于规则的垃圾邮件和群发邮件策略，以及基于签名的已知恶意软件检测。
- **URL 和附件保护**
  针对所有电子邮件链接的基本重写和针对附件的沙盒功能。
- **调查和威胁搜寻**
  电子邮件搜索、事件调查和关联、搜寻和补救。
- **信息保护**
  电子邮件、文件和端点的加密、存档和 DLP 策略。
- **意识和培训**
  为最终用户提供网络钓鱼攻击模拟和培训。

Exchange Online Protection

包含在每个计划中，并提供基本的电子邮件卫生功能，以过滤群发邮件、垃圾邮件和恶意软件。

- 反垃圾邮件
- 基于签名的恶意软件防护

Microsoft Purview (DLP)

可配置的数据丢失预防规则和执行。与 Microsoft 信息保护集成。

- 针对电子邮件和文件的 DLP
- 针对 Teams 的 DLP
- 针对端点的 DLP

Defender for O365 计划 1

针对恶意链接和附件的基本保护的附加安全控制。

- 安全链接（URL 重写）
- 安全附件（沙盒处理）
- 内部电子邮件保护

Defender for O365 计划 2

包括计划 1 中的所有功能，外加威胁搜寻、调查、训练和响应的附加功能。

- 威胁搜寻
- 跨域事件关联
- 网络攻击模拟训练

E3 许可证

E3 许可证 + 合规性

E3 许可证 + 合规性 + 安全性

E5 许可证

● 完整　● 受限制　● 无

	SEG	M365	Cloudflare
威胁防护			
允许/阻止列表	●	●	●
已知的恶意发件人	●	●	●
已知的恶意 URL/附件	●	●	●
垃圾邮件/群发邮件过滤	●	●	●
机器学习（内容分析）	●	●	●
Zero-Day 恶意软件/勒索软件	●	●	●
恶意链接	●	●	●
URL 重写（点击时间分析）	●	●	●
自适应链接隔离	●	●	●
商业电子邮件泄露 (BEC)	●	●	●
员工假冒	●	●	●
供应商假冒	●	●	●
员工入侵 (ATO)	●	●	●
供应商入侵	●	●	●
DMARC 管理	●	●	●
恶意应用检测（OAuth 钓鱼）	●	●	●
Web 内容安全性	●	●	●
安全意识和培训	●	●	●
威胁响应			
单一、直观的界面	●	●	●
自动威胁分类	●	●	●
快速搜索和调查	●	●	●
自动撤回	●	●	●
按需报告	●	●	●
托管检测和响应服务	●	●	●
数据保护			
加密	●	●	●
存档	●	●	●
电子邮件 DLP	●	●	●
云 DLP（协作应用）	●	●	●
网络 DLP	●	●	●

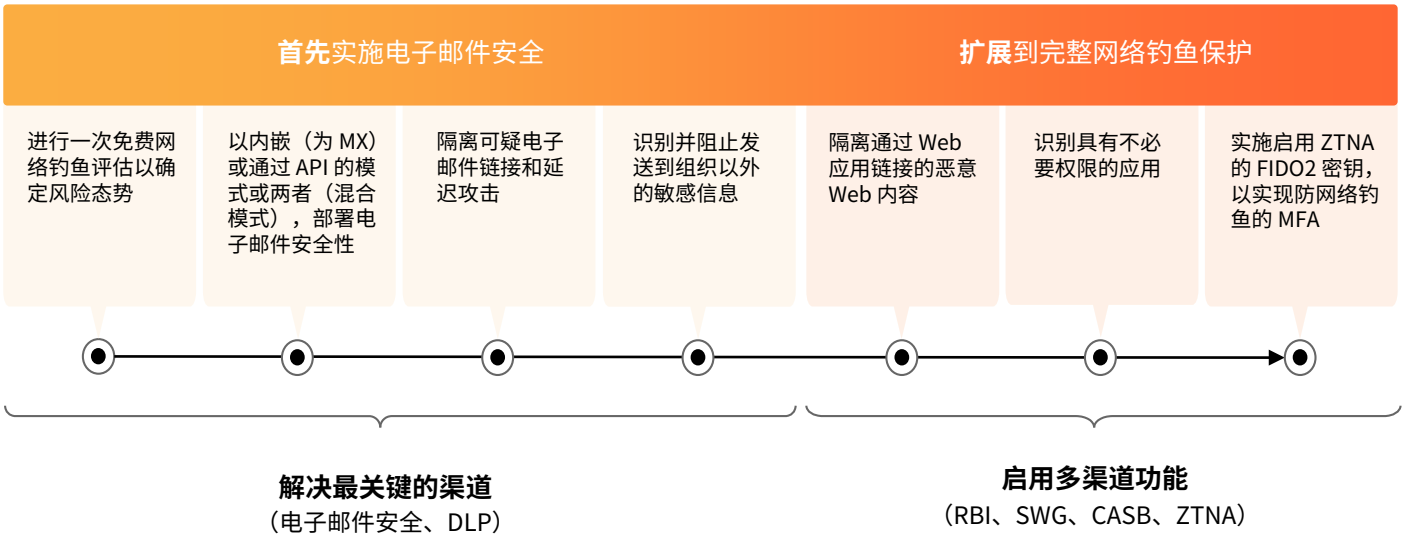
优势

完成多渠道保护

随着网络钓鱼活动迅速扩展到电子邮件之外，组织现在比以往任何时候都更迫切地需要实施一种能够快速、简单地实现全面多渠道保护的网络钓鱼解决方案。

借助 Cloudflare 的统一安全平台，组织可以首先部署行业领先的电子邮件安全解决方案，以快速解决最关键的网络钓鱼渠道；然后轻松启用 Zero Trust 服务，将保护扩展到所有渠道，从而有效阻止已知和新出现的网络钓鱼威胁。

- **低干预、高效率的威胁检测**
  利用只需极少调整的行业领先的检测功效来最大程度地降低网络钓鱼风险。
- **更大整合，更低成本**
  通过完全整合的单一平台解决所有网络钓鱼使用案例，从而减少支出。
- **快速部署，易于管理：**
  确保立即保护，同时减少持续管理所需的时间和精力。



评估与比较

评估您当前的电子邮件防御能力，看看哪些威胁被遗漏了

在几分钟内运行一次免费的回溯扫描，查看过去 14 天内哪些网络钓鱼威胁侥幸逃脱，或者请求进行网络钓鱼风险评估 (PRA) 来监控收件箱中是否存在送达时含有网络钓鱼威胁的电子邮件。与其他开箱即用未经调优的提供商进行比较，看看哪一个电子邮件安全解决方案提供最快、最简单的保护。

运行一次追溯扫描　申请网络钓鱼风险评估

