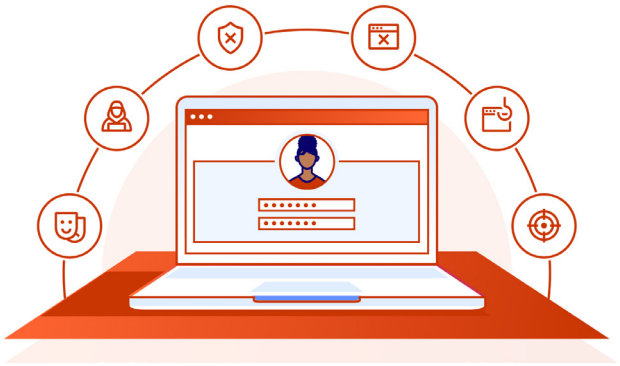
防范多渠道网络钓鱼，保障员工安全

分层保护，不局限于收件箱



概述

网络钓鱼攻击不再仅局限于电子邮件

虽然电子邮件仍然是网络钓鱼活动最普遍且最有效的传递机制，但攻击者越来越多地运用巧妙的策略，通过用于日常沟通和协作的多个渠道（即，各种应用）将用户作为攻击和利用的目标。这些攻击通常利用巧妙混淆的链接来欺骗用户，并引导目标用户访问恶意内容和不安全的环境。

更多渠道 = 更多利用员工的方式

通过电子邮件和其他协作应用中的欺骗性链接将用户作为攻击的目标，攻击者可以绕过传统的检测方法，同时以一种增加真实感的方式来吸引用户。这将会增加员工点击恶意 Web 内容、泄露凭据或泄露敏感信息的风险。电子邮件安全只能在阻止源于收件箱的攻击时才有所帮助，但如果这些攻击传播到其他应用，则需要更广泛的安全解决方案阻止这些攻击。

挑战

多渠道威胁可能会绕过传统的电子邮件过滤

多渠道攻击会利用复杂的链接混淆和各种协作应用，诱骗用户点击恶意内容或泄露敏感信息。这种类型的攻击可能难以有效应对，因为：

- **链接混淆**（URL 重定向/缩短程序）
- **基于图像的 URL**（二维码）
- **延迟攻击**（投递后激活）
- **分布式参与**，跨各种工作应用

89%

的安全决策者担心多渠道威胁[1]

#1

恶意链接是最大的网络钓鱼威胁（根据检测量）[2]

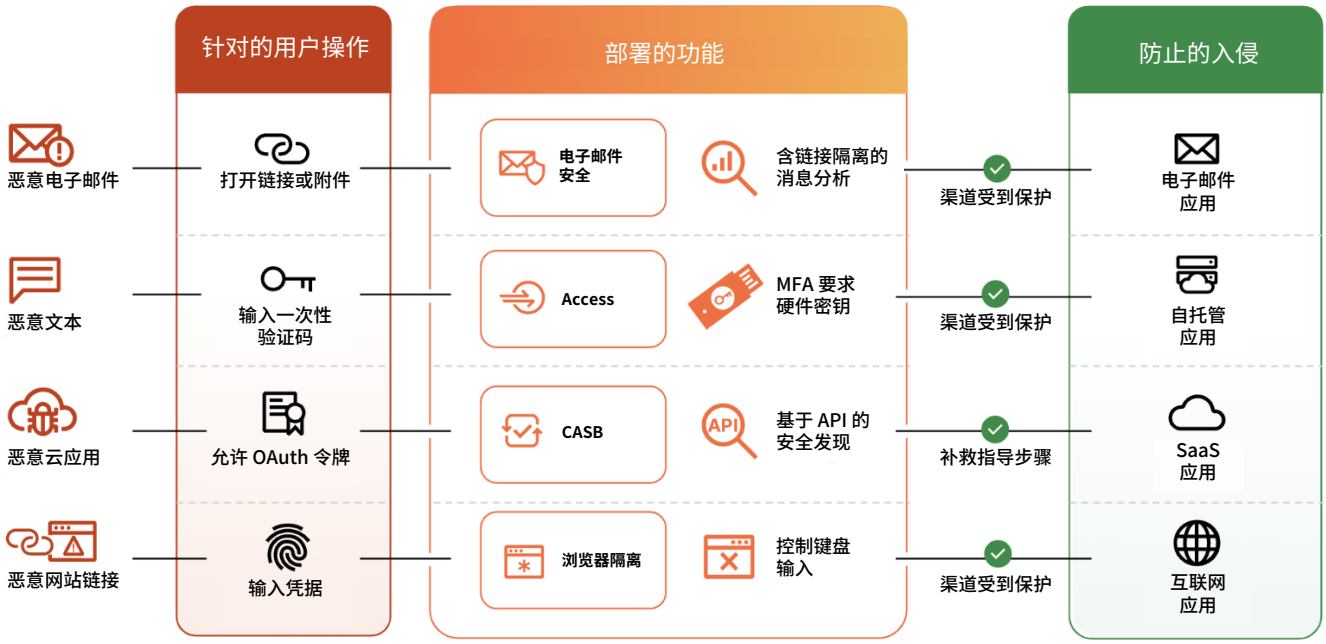
81%

的组织在过去 12 个月中遭受过多渠道攻击[1]

解决方案

识别每个网络钓鱼风险点，确保统一安全性

阻止多渠道攻击需要一个平台，能够解决员工工作流程和应用内交互中存在的各种漏洞。这正是 Cloudflare 提供最完整的网络钓鱼解决方案的原因，该解决方案专注于为员工和应用提供无缝保护。凭借 Cloudflare One 平台，组织可以充分利用本机集成的电子邮件安全 (ES) 以及 Zero Trust 服务来部署分层保护，保障电子邮件、自托管应用、SaaS 应用和互联网应用安全，从而提供纵深防御以阻止欺诈性支付和数据泄露。



先发制人，阻止通过电子邮件传播的威胁

利用 AI/ML 支持的内容分析，检测商业电子邮件入侵 (BEC)、恶意软件和其他源自电子邮件的威胁，以实现自动化防护。

防止用户凭据被盗所致的数据泄露

在凭证被盗或泄露的情况下，通过有条件访问与要求硬件密钥来阻止数据泄露，以此作为最后一道防线。

阻止并隔离基于链接的规避型攻击

保护用户免受针对性攻击，这些攻击利用巧妙混淆、难以捕获的链接，通过常用的消息应用诱骗员工。

阻止通过电子邮件传播的威胁 (ES)

电子邮件是最常用且最常遭到利用的商业应用，有鉴于此，保护用户免受试图通过电子邮件来利用其信任的网络钓鱼攻击比以往任何时候都更加重要。通过使用 Cloudflare 解决方案来增强或替换现有电子邮件防御措施，组织可以自动缓解利用嵌入式电子邮件链接、附件，以及利用假冒或被盗账户来窃取敏感信息和实施金融欺诈的复杂网络钓鱼攻击。

Cloudflare 的轻量级云原生解决方案可以在几分钟内部署，为 Microsoft 和 Google 的内置电子邮件功能提供补充。Cloudflare 自动化程度更高，仅需极少微调即可实现最佳结果，从而显著减少了持续管理所需的时间和精力。

商业电子邮件泄露 (BEC)
AI/ML 提供支持的内容分析会解构每一条消息，评估对话历史记录、写作模式、情绪和其他变量，以确定发件人的真实性。

勒索软件和恶意附件
使用针对有效负载的 ML 检测模型、无特征检测、计算机视觉、远程提取以及其他形式的分析，识别已加密和未加密的恶意有效负载。

恶意电子邮件链接
将用于解构和深入分析复杂 URL 的先进技术与自适应链接隔离相结合，确保员工获得安全、顺畅的 Web 体验。

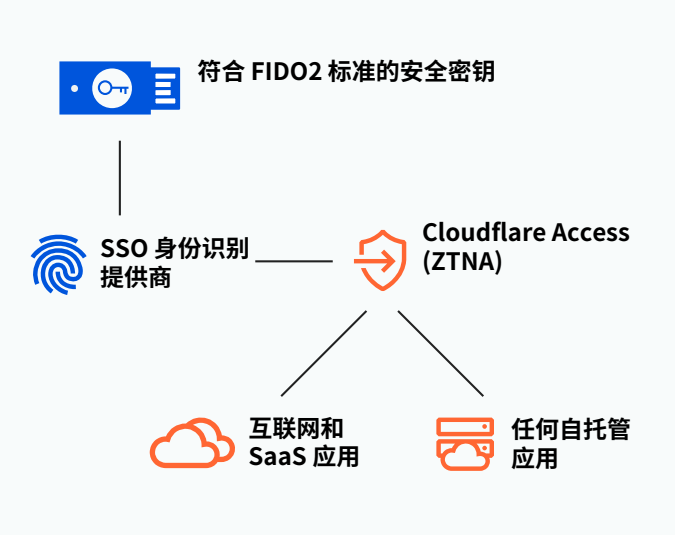
缓解 OAuth 网络钓鱼攻击 (CASB)

OAuth 网络钓鱼利用合法身份识别提供商和授权工作流程，诱骗用户授予恶意应用访问权限。Cloudflare One 平台能够检测此类应用，并提供补救措施指导来快速缓解这些威胁。

防止凭据暴露所致的数据泄露 (ZTNA)

虽然许多组织实施了大量的预防措施，以避免员工凭据落入坏人之手，但令人痛苦的事实却是，预防措施永远无法确保 100% 万无一失。如果凭据不幸被盗或意外泄露，则必须要有最后一道防线来防止全面泄露。

借助 Cloudflare Access 作为每个资源（包括自托管或非 Web 资源）的聚合层，组织可以始终执行符合 FIDO2 标准的身份验证，以实现防网络钓鱼的 MFA。因此，即使员工凭据被泄露，组织仍然能够确保其数据得到保护。



隔离基于链接的攻击 (ES + RBI + SWG)

基于链接的攻击已成为窃取凭据、加载恶意软件/勒索软件以及提取敏感信息的首选方法。通过电子邮件、聊天、短信、社交以及云盘的组合来传递此类链接，使得确保员工和数据免受针对性网络钓鱼攻击的过程更加复杂。

Cloudflare 浏览器隔离会在我们的全球云网络（而非用户的本地设备）上远程渲染所有 Web 代码，通过这种方式解决基于链接的网络钓鱼攻击问题。这减轻了恶意软件和浏览器 zero-day 漏洞的影响，同时还提供针对用户行为的精细化控制（例如，禁用键盘输入），以防止凭据收集和数据泄漏。

消除网络钓鱼风险，而不减慢员工效率

通过集成基于我们独特的网络矢量渲染 (NVR) 技术构建的下一代浏览器隔离功能，Cloudflare 能够提供无缝、安全且可扩展的解决方案，用于隔离潜在恶意的链接。与高带宽消耗的技术不同，NVR 会向设备流式传输安全绘制命令。这有助于消除恶意 Web 内容的风险，同时不影响最终用户体验。得益于 NVR 技术和 Cloudflare 的低延迟网络，组织可以隔离多渠道威胁，同时确保员工生产力不受影响。

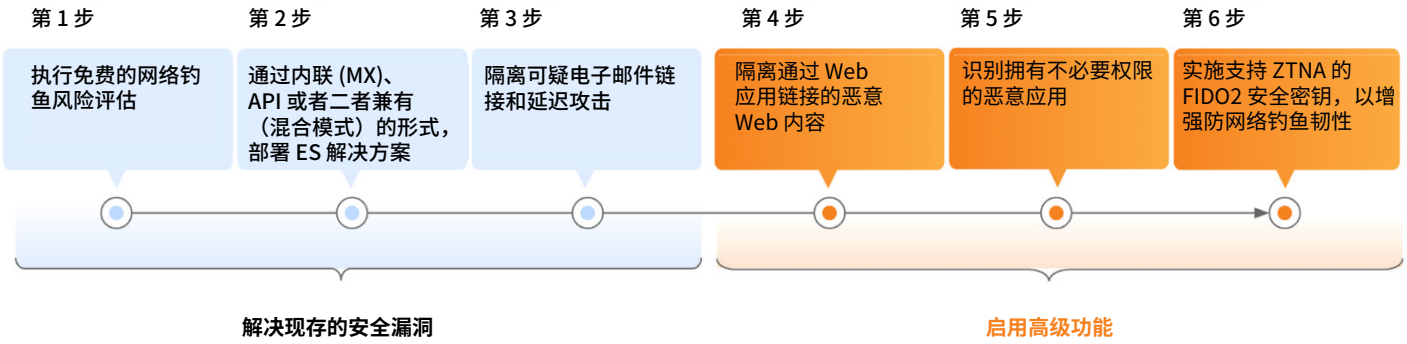
优势

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。

使用 Cloudflare One 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，快速解决最关键的网络钓鱼渠道问题；然后轻松启用其他 Zero Trust 服务，将保护扩展到所有渠道，从而有效地阻止已知和新兴网络钓鱼威胁。

- **少干预、高效率的防护：**
  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

在几分钟内运行免费的 Retro Scan（O365 收件箱），查看过去 14 天内哪些网络钓鱼威胁成功送达，或请求进行网络钓鱼风险评估 (PRA)，监测收件箱中接收的邮件是否存在网络钓鱼。与其他开箱即用的零调整提供商进行比较，了解哪一种电子邮件安全解决方案能够提供最快捷、最简单的保护。

了解哪些网络钓鱼威胁正在突破防御措施

运行一次追溯扫描　申请网络钓鱼风险评估

CLOUDFLARE

1. 2023 年 Forrester Opportunity Snapshot：来源
2. 2023 年网络钓鱼威胁报告来源