Cloudflare Email Security

提供自主、多渠道保护，确保工作空间通信安全

防止有针对性的网络钓鱼攻击

轻松阻止或隔离其他解决方案遗漏的威胁

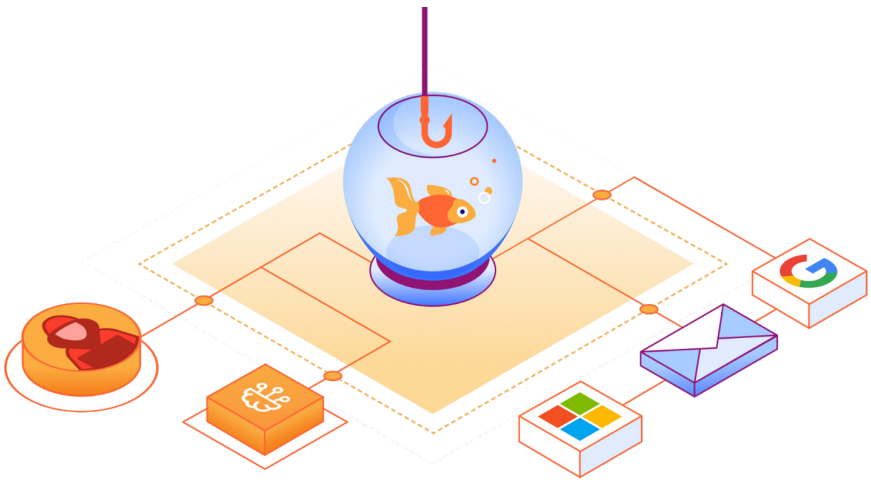
电子邮件是最常用、被利用最多的商业应用，因此保护用户以防试图利用他们信任的网络钓鱼攻击比以往任何时候都更加关键。随着组织越来越多采用 Microsoft 365 和 Google Workspace 等云电子邮件服务来更好地支持混合办公人员，威胁行为者已经转向更有针对性、低容量的攻击，能够规避传统的安全电子邮件网关 (SEG)，例如 Proofpoint 和 Mimecast。

因此，Cloudflare 的云原生电子邮件安全解决方案独特地利用预防性的攻击活动情报、基于机器学习的内容分析以及一个统一的 Zero Trust 平台，以便在钓鱼威胁到达您的员工之前予以阻止。

91%
的网络攻击从一封钓鱼邮件开始[1]

500 亿美元
过去十年来 BEC 攻击造成的损失[2]

81%
的组织在过去 12 个月内经历过一次多渠道攻击[3]



阻止企业电子邮件破坏 (BEC)

通过分层、基于机器学习的上下文分析来检测冒充和被入侵的账户。

隔离延迟和多渠道攻击

保护用户，隔离通过未知或欺骗性链接传递的恶意 Web 内容。

拦截勒索软件和恶意附件

防止勒索企图和恶意代码危害您的组织。

更强保护，更加简单

实施分层安全，以低得多的成本提供更好的保护

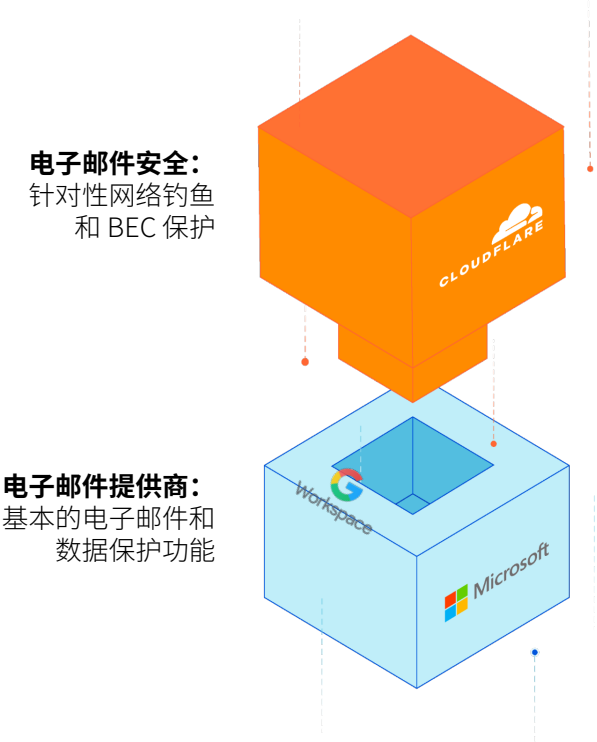
随着网络钓鱼攻击不断扩散，Microsoft 和 Google 继续构建原生功能，以提供基本的电子邮件和数据保护能力，例如身份验证、归档和客户端加密。然而，威胁行为者也改进了策略，以执行更具针对性和规避性的攻击，此类攻击往往绕过原生安全控制，实现更高的成功率。

通过叠加 Cloudflare 保护，组织能够自动阻止或隔离利用恶意链接、附件和被破坏账户来窃取敏感信息和进行金融欺诈的针对性钓鱼攻击。

增强您现有的电子邮件安全控制

Cloudflare 的云原生电子邮件安全解决方案部署仅需短短几分钟，即可增强现有的 SEG 部署，或补充由 Microsoft 和 Google 提供的内置电子邮件功能。由于几乎无需任何调优，组织在日常解决方案管理投入更少时间和精力，即可实现更强大的网络钓鱼保护。

> “自从 [在 M365 上] 部署 Cloudflare 以来，我们发现用户每天收到的恶意或可疑电子邮件数量减少了 50%。这为我们腾出好几个小时，可重新投入到其他目标上。”
>
> **Werner Enterprises**
> （财富 1000 强公司）



重新利用通过提高自动化程度而节省的工时

Cloudflare 的自动化、轻量级解决方案可与 Microsoft 和 Google 的工作流程无缝集成，同时为分析活动提供一个统一、直观的用户界面。

实现 99.997% 的检测效果

将电子邮件提供商的原生功能与 Cloudflare 的钓鱼和 BEC 保护相结合，确保企业以最小风险实现全面覆盖。

以更低成本实现更大价值

使用 Cloudflare 的低干预解决方案替代过时、昂贵和复杂的部署，可以减少运营开销、冗余功能和过度调优。

阻止复杂 BEC 攻击

报告损失达到 500 亿美元，并继续增长

鉴于过去十年来 BEC 攻击造成了令人震惊的巨额损失，一些组织仍然没有优先考虑应对这种有效的金融欺诈形式，实在让人惊讶。尽管 BEC 攻击只占钓鱼威胁的很小比重，但它们经常被 SEG 和云电子邮件提供商漏检，导致更大的财务损失。这些有针对性的攻击很难被捕获，因为它们利用冒充或被破坏的账户和会话上下文来伪装成员工或受信任的供应商。

将 Zero Trust 原则扩展到电子邮件

当利用被破坏的员工或供应商电子邮件账户时，攻击者可以规避传统的安全控制，因为这些控制只尝试确认发件人账户的合法性。Cloudflare 则更进一步，通过分析一系列行为属性、行文模式、情绪指标和对话历史来确定发件人的真实性。Cloudflare 基于机器学习的威胁模型和广泛的网络情报提供了最有效的武器，以抵御用于获得欺诈性付款的被破坏账户。

图 1： 消息分析

使用基于机器学习的上下文分析检测 BEC

准确识别 BEC 攻击不仅需要对消息进行结构分析。成功的检测还涉及有关对话风格和意图的细致理解。Cloudflare 庞大的网络遥测能力（每天 3 T+ DNS 请求）和不断演进的机器学习模型驱动我们的小模式分析引擎，该引擎对电子邮件信息的每一个方面进行解构，以评估行文模式、情绪、历史背景和其他各种变量，从而帮助确定发件人的真实性。

隔离基于链接的攻击

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、社交和其他应用的组合来传递这些链接，进一步增加了确保员工和数据免受针对性钓鱼攻击的难度。

Cloudflare 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，从而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。

杜绝网络钓鱼风险而不拖慢员工效率

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。

快速调查和解决

直观、低干预的安全管理

Cloudflare 自动化程度更高，仅需极少配置即可实现最佳结果，从而显著减少了日常电子邮件安全管理所需的时间和精力。安全团队可以立即在仪表板中查看到所有顶级指标和趋势的完整视图，并能够点击查看已标记消息的更多详情。深入研究趋势可以快速发现频繁攻击的类型，哪些管理人员成为目标，得到缓解的延迟攻击，以及其他关键数据点。

所有分析、遥测、威胁观察和破坏指标 (IOC) 都可以通过一个广泛的 API 进行访问，以便轻松集成到现有的分析师工作流程和编排工具中。

> “我经常跟同事说，Cloudflare 是一种简单、易用的云端 SaaS 解决方案，我对其高度准确性非常满意。”
>
> **日本航空**

托管检测和响应 (PhishGuard)

Cloudflare 的托管电子邮件安全服务 PhishGuard 辅助组织现有的 SOC 团队，以释放安全调查周期并提供有价值的威胁情报。PhishGuard 可协助调查、内部威胁评估、主动打击欺诈和复杂的补救需求，从而帮助防御网络钓鱼活动。PhishGuard 扩展安全资源和专业知识，以主动通知潜在的欺诈和内部威胁，同时搜寻基于电子邮件的威胁。

PhishGuard 的功能和好处：

- 托管网络钓鱼提交和事件响应，以更快地解决问题。
- 主动 BEC 和欺诈通知，以便组织可以在攻击生命周期的早期快速响应。
- 用于实时监控、定期账户审查和持续威胁评估的专用资源。
- 基于对托管环境的威胁分析自定义阻止特征。

1100+

小时——通过自动化手动分类工作每年节省时间

Cloudflare 的自动化解决方案消除了手动、耗时的任务，缩短了响应时间，并释放了额外的周期。

50%

（在 M365 上叠加使用后）恶意或可疑邮件投递数量减少

在 Microsoft 365 之上叠加使用 Cloudflare 使组织能够捕获有针对性的攻击并减少恶意电子邮件的总数。

40

小时——七年内在电子邮件安全配置上花费的总时间

Cloudflare 的低干预电子邮件安全需要极少前期配置和持续调优，提供开箱即用的高检测效率。

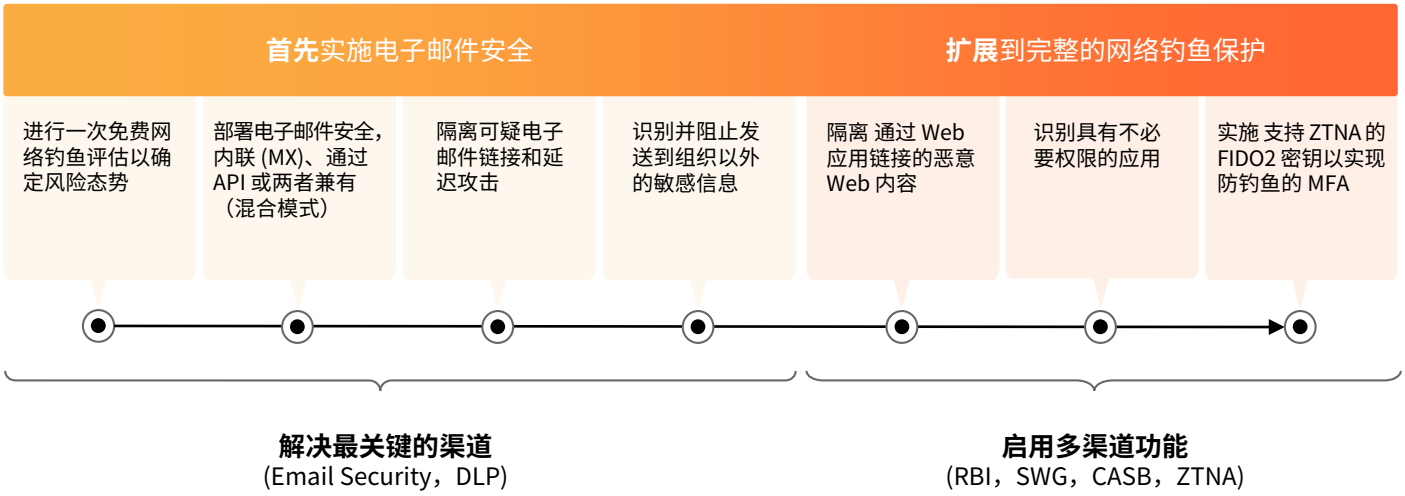
优势

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。

通过 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性，快速应对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——有效阻止各种已知和新兴的网络钓鱼威胁。

- **低配置、高效能的保护：**
  通过行业领先的检测效能，几乎无需调优，即可最大限度地降低网络钓鱼风险。
- **更高整合度，更低成本：**
  通过单一、全面集成的平台解决所有网络钓鱼用例，降低支出。
- **部署快捷，管理简单：**
  确保即时提供保护，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

1. 2020 年德勤 (Deloitte) 研究：来源
2. 2023 年联邦调查局网络犯罪投诉中心公共服务公告：来源
3. 2023 年 Forrester Opportunity Snapshot：来源

