电子邮件链接隔离

隔离电子邮件链接，减少攻击面并简化操作

应用浏览器隔离保护和控制措施，降低网络钓鱼风险

挑战：复杂的多渠道网络钓鱼

多渠道网络钓鱼涵盖电子邮件和 Web 交付，能够狡猾地躲避过滤规则。常见的这些类型包括：

- **延迟网络钓鱼：**电子邮件中起初无害的链接，后续在交付之后通过恶意目的地武器化。
- **云服务网络钓鱼：**危险的 HTTPS 链接与常见的云服务（例如 Google Drive、Box）非常相似

要阻止这种威胁，必须配备现代电子邮件保护，在所有链接中严格执行 Zero Trust 的“从不信任、始终验证”原则。

解决方案：电子邮件链接隔离

集成远程浏览器隔离 (RBI)
云电子邮件安全 (CES) 的功能
一丝不苟，加强网络钓鱼
防范。Cloudflare Area 1
客户可以开启
Cloudflare 浏览器隔离
以让这些
多渠道攻击失去意义。

从而预防凭据收集或保密数据失窃等网络钓鱼影响管理员可以在隔离的网页上控制用户交互（例如限制键盘输入和文件上传）。

此外，在隔离的浏览器中打开电子邮件链接，就会在远离本地设备的云端运行所有代码，让恶意软件失去意义。

分析师感言：

“在外部解析的基于电子邮件的 URL 常常用于对员工进行网络钓鱼。隔离这些 URL，就可减少网络钓鱼攻击得逞的机会。”

“大部分攻击是通过公共互联网实施的，用户进行 Web 浏览或点击电子邮件链接时，容易受欺骗而访问恶意站点。直接从最终用户的桌面去除（或者，更强烈的方式是隔离）浏览器，就可显著改善企业安全态势，包括防范勒索软件攻击。”

“针对特定高风险用户（例如财务团队）或用例（例如呈现基于电子邮件的 URL）评估和试点浏览器隔离解决方案，尤其是在您的组织厌恶风险的情况下。” [1]

Gartner®

阅读更多

集成 CES 和 RBI 的商业效益

加强网络钓鱼防范

电子邮件隔离不仅防止在本地执行网络钓鱼链接中的有害代码，还会应用数据保护控制措施，防止敏感信息落入歹人之手。

释放 IT 和安全性生产力

只需点击几次，即可为任何网站开启电子邮件隔离。

IT 和安全团队不用麻烦地配置过滤策略，这些策略可能存在“过度拦截”（从而阻碍用户生产力）和“拦截不足”（从而让威胁漏网）的风险。

示范用例：阻止延迟网络钓鱼

问题：延迟网络钓鱼逃避检测

利用合适的手段和动机，延迟网络钓鱼活动能够绕过传统的保护措施。

活动设置：攻击者可能首先使用合适的电子邮件身份验证（SPF、DKIM、DMAR）和无害的网页，从新创建的域发送看起来真实的电子邮件。

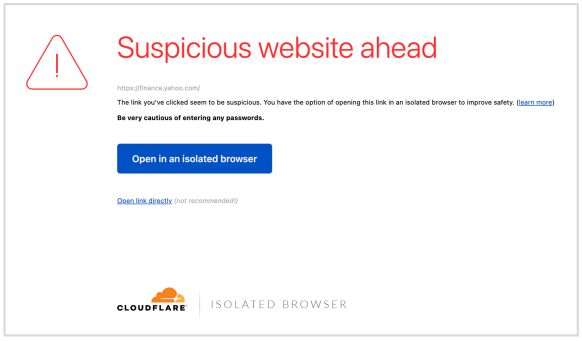
成功交付到收件箱：这些电子邮件可能通过安全电子邮件网关、基于身份验证的过滤器或依赖基于信誉的信号和其他确定性技术的其他服务来逃避检测。

改到恶意链接：成功交付电子邮件后，攻击者可能更改受攻击者控制的网页，将链接改到恶意目的地。例如，常见情况是改到用于收集凭据的假登录页面。

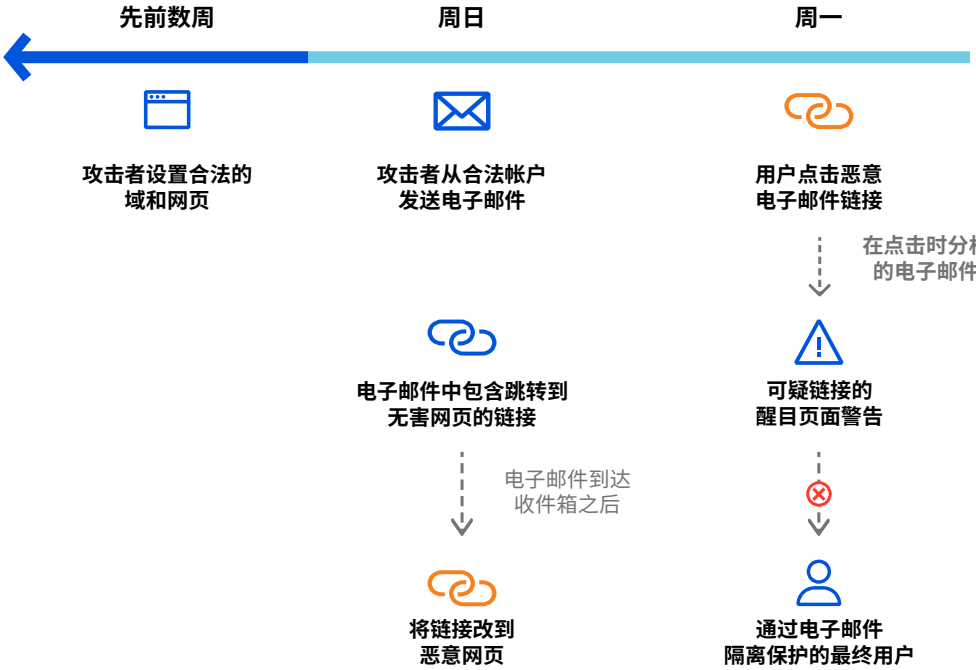
解决方案：交付后隔离可疑链接

电子邮件链接隔离提供了交付后的关键保护层。Cloudflare 会分析用户在电子邮件中点击的任何链接。如果链接被视为可疑或有风险，Cloudflare 会显示醒目的警告页面 *（如下所示）*，如果用户浏览进去，则隔离该网页。

管理员阻止恶意代码在本地设备上执行，并可应用数据保护控制措施，例如限制文件上传和下载、防止用户键盘输入或以只读模式打开页面。



延迟网络钓鱼活动的时间表



Cloudflare 在点击时分析每个链接

安全链接：用户将被透明地重定向到此站点。

恶意链接：用户被阻止进行浏览。

可疑链接：系统强烈建议用户放弃浏览，并弹出一个醒目的警告页面，鼓励他们在一个隔离的浏览器中查看链接。

将云电子邮件安全与 Cloudflare Zero Trust 集成

使用 Zero Trust 实现现代安全性

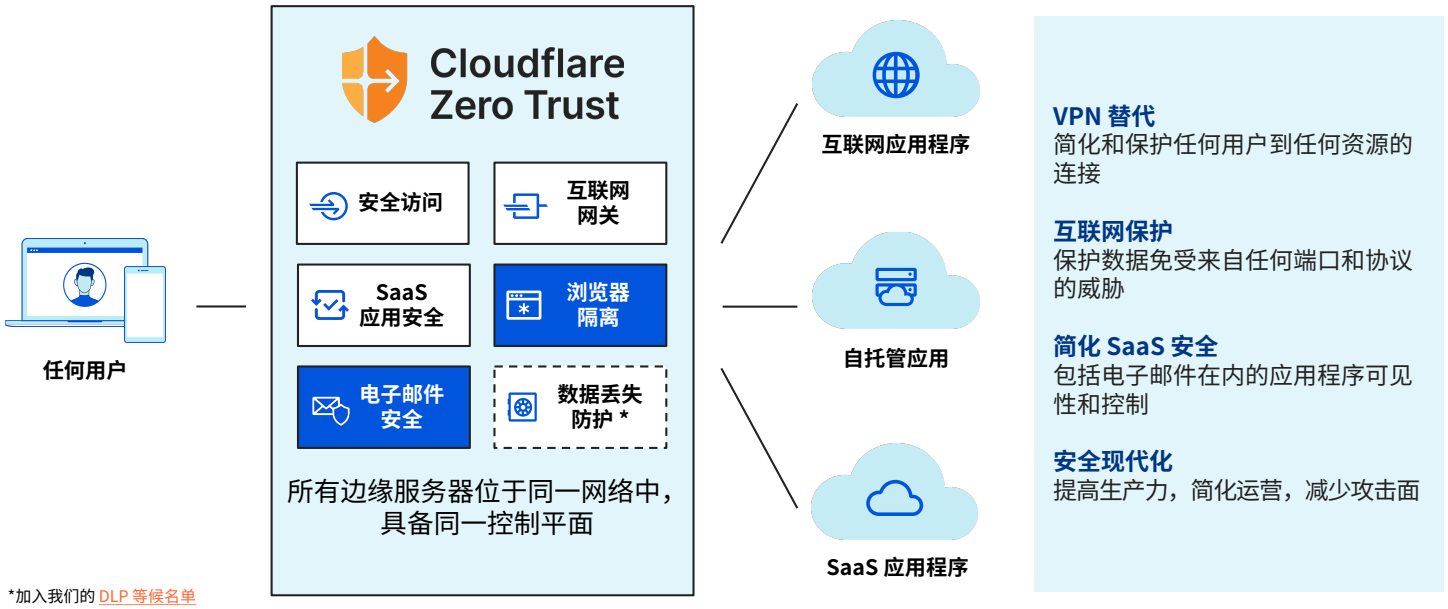
Cloudflare Zero Trust 平台在远程和办公室用户连接到企业应用程序和公共互联网时提高可见性、消除复杂性并降低风险。

2022 年 4 月 1 日，Cloudflare 完成了对 Area 1 Security 的收购，我们的愿景是增强我们的 Zero Trust 平台保护用户在电子邮件、Web 和网络缓解中免受网络钓鱼攻击的能力。在此处阅读更多信息。

电子邮件安全：Zero Trust 的核心组成部分

Cloudflare Area 1 Email Security 消除了对电子邮件的隐式信任，以先发制人的方式阻止网络钓鱼和商业电子邮件攻击 (BEC)，从而增强了 Zero Trust。

从不信任任何发件人，哪怕是内部人员。而是确保包括电子邮件在内的所有用户流量均得到验证、过滤、检查，免受来自互联网的威胁。电子邮件安全将被整合到 Cloudflare 的 Zero Trust 服务中，与 RBI、CASB 等成为一个强大的组合。



*加入我们的 DLP 等候名单

云电子邮件安全（CES）

- 将网络钓鱼事件响应时间缩短 90%。
- 提前确定攻击者的基础设施和交付机制，从而在攻击周期的最早阶段阻止网络钓鱼。
- 通过分析通信的内容、上下文和社交图谱，消除对电子邮件的隐式信任。
- 利用与 Microsoft、Google 和其他环境的集成，增强内置安全性

远程浏览器隔离（RBI）

- 在“只读模式”下打开有风险的站点以阻止凭据泄露，方法是控制用户交互（例如，键盘输入、复制和粘贴、上传/下载）。
- 在 Cloudflare 的网络上运行所有浏览器代码，将本地设备与恶意代码隔离。
- 交付无摩擦的快速最终用户体验。我们不采用典型的像素流传输，而是从远程浏览器绘制页面的确切副本，对于全球 95% 的互联网用户来说，延迟不到 50 毫秒。

立即预约网络钓鱼风险评估

联系我们

010 8524 1783 | enterprise@cloudflare.com | www.cloudflare.com

修订编号：PMM-2022JUN