Cloudflare Area 1 电子邮件安全

先发制人地保护用户，防范网络钓鱼、商业电子邮件攻击 (BEC) 和电子邮件供应链攻击。

网络钓鱼是组织面临的最频繁和最昂贵的网络威胁之一。

Cloudflare Area 1 是一个云原生电子邮件安全平台，可以在攻击用户收件箱之前识别并阻止，从而更有效地抵御鱼叉式网络钓鱼、BEC 和其他规避现有防御的高级威胁。

Area 1 与 Microsoft 和 Google 环境及工作流程深度集成，从而增强云电子邮件提供商的内建安全。

Area 1 是我们 Zero Trust 服务的一部分。

阻止针对性的网络钓鱼威胁

Area 1 可防范各种各样的网络钓鱼攻击，从大规模活动到酝酿数月的针对性电子邮件供应链攻击。

网络钓鱼

Verizon 2021 DBIR 将网络钓鱼列为最常见的入侵策略。通过大规模 Web 爬取、细微模式分析和增强检测，Area 1 可在网络钓鱼攻击到达用户收件箱前数日就将其阻止。

BEC 和社会工程威胁

在 BEC 中，攻击者冒充或入侵可信任的实体来窃取金钱和数据。Area 1 分析电子邮件通信的内容和上下文，以阻止这些犹如“大海一针的”威胁。

电子邮件供应链攻击

攻击者破坏供应商的电子邮件，观察邮件模式，并拦截现有邮件线程以发动发票诈骗。Area 1 分析电子邮件线程，消息情绪和社交图谱，以阻止这些复杂的攻击。

敲诈勒索邮件

据 Gartner 估计，40% 的勒索软件攻击是从电子邮件开始的。Area 1 帮助主动防御包含勒索软件的电子邮件，阻止它们到达最终用户，并在恶意信息传播开来前将其清除。

比传统电子邮件网关技高一筹

先发制人

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。

基于上下文

利用先进的检测技术（语言分析、计算机视觉、社交图谱绘制等）来捕获 BEC、供应商电子邮件欺诈和其他无负载的威胁。

全面

涵盖所有电子邮件攻击类型（URL、有效负载、BEC）、手段（电子邮件、web、网络）和攻击渠道（外部、内部、可信合作伙伴）。

持续不断

在电子邮件到达收件箱之前、期间和之后，采用带有威胁防护层的纵深防御。

优势

增强原生电子邮件安全

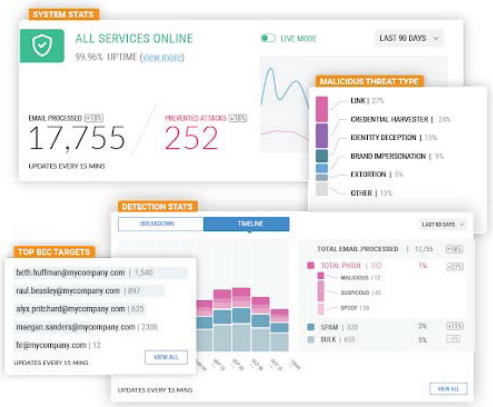
阻止高级网络钓鱼和规避内置安全保护措施的 BEC 攻击。利用对云电子邮件环境的深度集成，对电子邮件的生产效率几乎没有影响。

采用云优先的架构

避免笨拙和不灵活的传统电子邮件网关，采用现代化的可伸缩架构。减少在重复原生电子邮件安全能力的安全层上的花费。

为您的安全运营中心（SOC）团队节省时间

部署仅需数分钟，无需任何硬件、代理或设备。释放时间以用于创建和调优策略。利用 SIEM 和 SOAR 集成来加速 SOC 调查。



申请网络钓鱼风险评估

申请在您的实时电子邮件生产流量上运行 Area 1，并实时查看哪些电子邮件攻击突破您的现有安全控制。

评估不需安装任何硬件或软件，也不会影响电子邮件流。

在这里申请评估。