CLOUDFLARE

解决方案简述

强身份验证如何帮助阻止钓鱼攻击

安全密钥和 Zero Trust 方法可挫败钓鱼攻击

网络钓鱼造成的威胁

数据丢失，网络入侵，帐户被盗

有针对性的网络钓鱼攻击是当今组织面临最危险的威胁手段之一。网络钓鱼和社会工程攻击的目的是操纵人们提供敏感信息或访问权限。登录凭据是常见的目标。

这种性质的攻击成功会导致：

- 帐户盗用
- 更大范围供应链攻击的一环
- 数据泄露，例如个人可识别信息 (PII) 和知识产权
- 恶意软件攻击（例如勒索软件）

幸运的是，一些非常有效的解决方案可以降低网络钓鱼的风险。其中最重要的一种是多因素身份验证 (MFA) 。

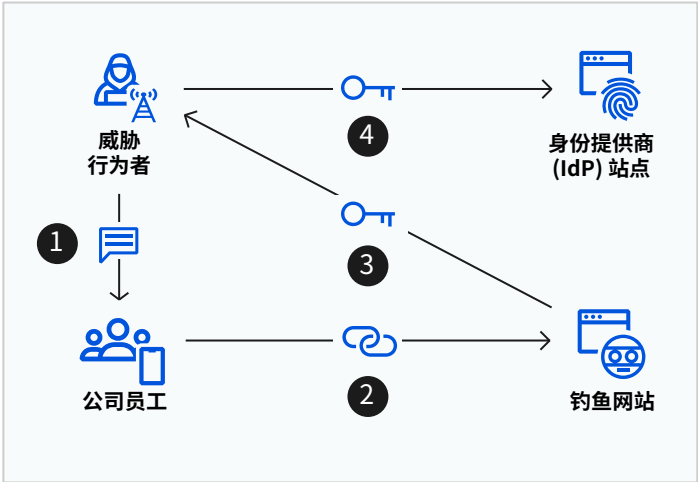


图 1： 短信钓鱼攻击剖析。1. 发送看似合法的短信。2. 链接到看似合法的网站。3. 受害者的登录凭据和基于时间的一次性代码被实时转发。4. 登录到真正的公司 IdP 网站。

多因素身份验证如何帮助阻止钓鱼攻击

MFA 让密码偷窃毫无意义

如果使用了多因素身份验证 (MFA)，登录时不但要提供用户名和密码，还需要一个密钥。如果没有这个密钥，用户无法登录帐户，攻击者也无计可施。

使用软密钥的 MFA

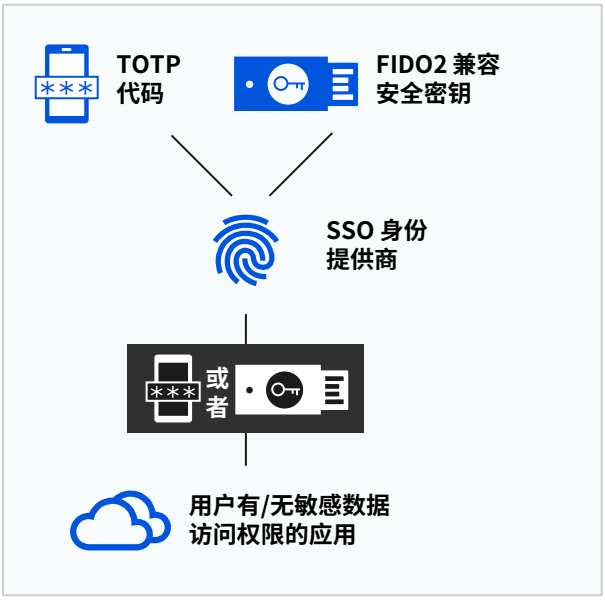
MFA 的一种常见实施是使用软密钥，例如基于时间的一次性口令 (TOTP)。TOTP 一般通过手机短信、电子邮件或应用发送。虽然比单因素身份验证更安全，但软密钥有可能被攻击者截获。

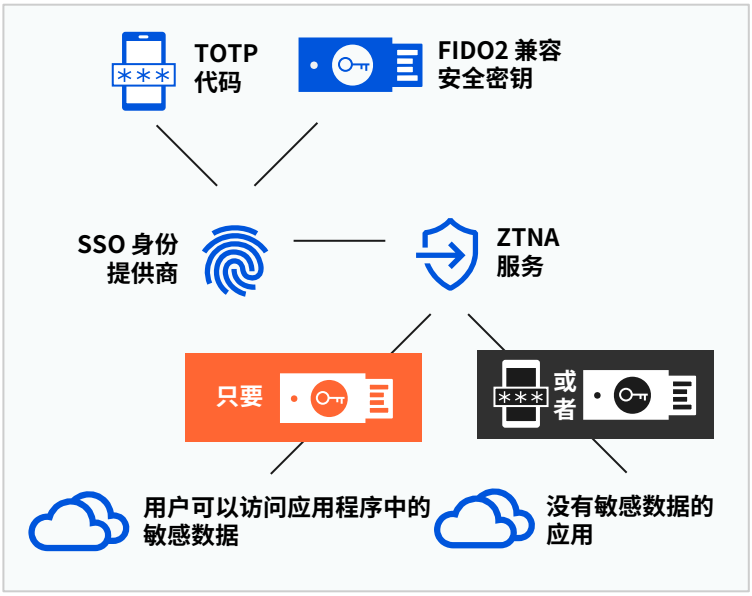
使用安全密钥的 MFA

兼容 FIDO2 的安全密钥发放后，无法被攻击者截获，在没有物理接触的情况下几乎不可能被盗。Google 的研究表明，使用 FIDO2/U2F 兼容安全密钥阻止了 100% 的帐户接管尝试。[1]

选择性地实施强身份验证

一些 IAM 解决方案可能支持强身份验证，但不允许管理员真正要求这样做。通过使用 ZTNA，您可以确保对包含敏感数据的应用特别要求兼容 FIDO2 的身份验证。Cloudflare 对每次身份验证都要求安全密钥 MFA，显著加强了我们的安全态势。

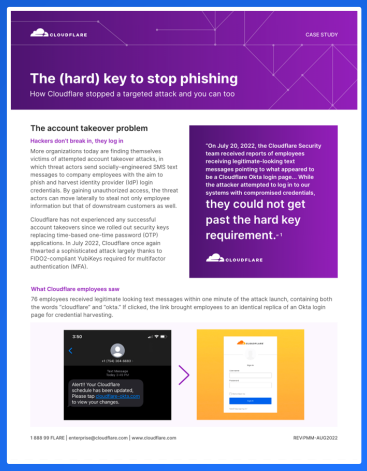




“2022 年 7 月 20 日，Cloudflare 安全团队收到员工报告称收到了看似合法的短信，指向一个看似 Cloudflare Okta 登录页面的网页……虽然攻击者企图使用泄露的凭据登录我们的系统，

但他们无法通过硬件密钥要求。” [2]

CLOUDFLARE



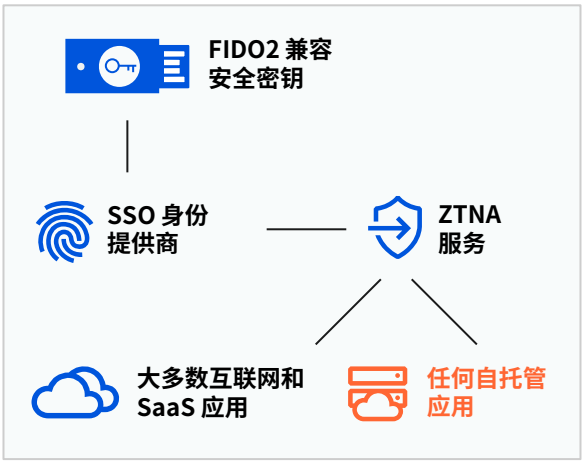
在所有地方推行强身份验证

适用于所有应用的 FIDO2 兼容 MFA

为云服务实施 MFA 有多种传统方式，尤其是在使用单点登录 (SSO) 服务时。但对于传统应用或非 Web 应用而言，这可能比较困难，因为其中许多应用原生不支持这种身份验证。

利用 ZTNA 简化实施

Zero Trust 网络访问 (ZTNA) 充当所有资源的聚合层，为每个资源启用严格的身份验证策略。SaaS、自托管和非 Web 应用程序都可以置于 ZTNA 之后，从而更容易对所有应用实施强身份验证。



实施强身份验证的要点

1

集中您的 IAM

集中身份和访问管理 (IAM)，以便更简单地对所有应用实施 MFA。

2

选择性地要求 MFA

根据身份和上下文，选择性要求 MFA—— TOTP + FIDO2 或仅 FIDO2。

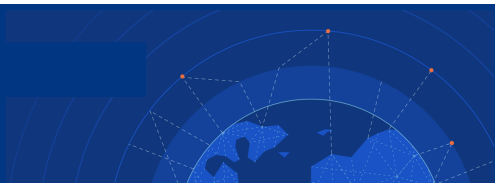
3

支持移动设备

发放适用于笔记本电脑、台式电脑、服务器以及移动设备的 FIDO2 解决方案。

加速您的 Zero Trust 路线图

预约架构研讨会



尚未准备好进行评估？

申请免费试用

1. krebsonsecurity.com/2018/07/google-security-keys-neutralized-employee-phishing/
2. Cloudflare 博客文章，2022 年 8 月 9 日，”一个复杂钓鱼骗局的机制以及我们如何阻止它” ，blog.cloudflare.com/2022-07-sms-phishing-attacks/