CLOUDFLARE

RESUMO DA SOLUÇÃO

Proteja sua força de trabalho contra phishing multicanal

Proteção em camadas que se estende além da caixa de entrada

VISÃO GERAL

Os ataques de phishing não se limitam mais apenas ao e-mail

Embora o e-mail continue sendo o mecanismo de entrega mais prevalente e eficaz para campanhas de phishing, os invasores estão cada vez mais usando táticas inteligentes que visam e exploram usuários em vários canais (por exemplo, aplicativos) usados para comunicação e colaboração diárias. Esses ataques geralmente empregam links habilmente ofuscados para enganar os usuários e direcionar seu alvo para conteúdo malicioso e ambientes inseguros.

Mais canais = mais maneiras de explorar funcionários

Atacar funcionários com links enganosos em e-mails e outros aplicativos de colaboração permite que os invasores contornem os métodos tradicionais de detecção enquanto envolvem os usuários de uma forma que aumenta a percepção de autenticidade. Isso aumenta o risco de um funcionário clicar em conteúdo malicioso da web, divulgar credenciais ou vazar informações confidenciais. A segurança de e-mail só pode ajudar quando um ataque se origina por meio de caixas de entrada, mas uma solução de segurança mais ampla é necessária para bloquear esses ataques quando eles se espalham para outros aplicativos

DESAFIOS

Ameaças multicanal podem ignorar a filtragem de e-mail tradicional

Ataques multicanal aproveitam a ofuscação de links complexa e vários aplicativos de colaboração para induzir os usuários a clicar em conteúdo malicioso ou vazar informações confidenciais. Esse tipo de ataque pode ser difícil de abordar devido a:

- **Ofuscação de links** (redirecionamentos/encurtadores de URL)
- **URLs baseados em imagens** (códigos QR)
- **Ataques adiados** (ativados após a entrega)
- **Engajamento distribuído** entre aplicativos de trabalho

89%

dos tomadores de decisão de segurança estão preocupados com ameaças multicanal[1]

Número 1

Links maliciosos são a principal ameaça de phishing com base no volume de detecção [2]

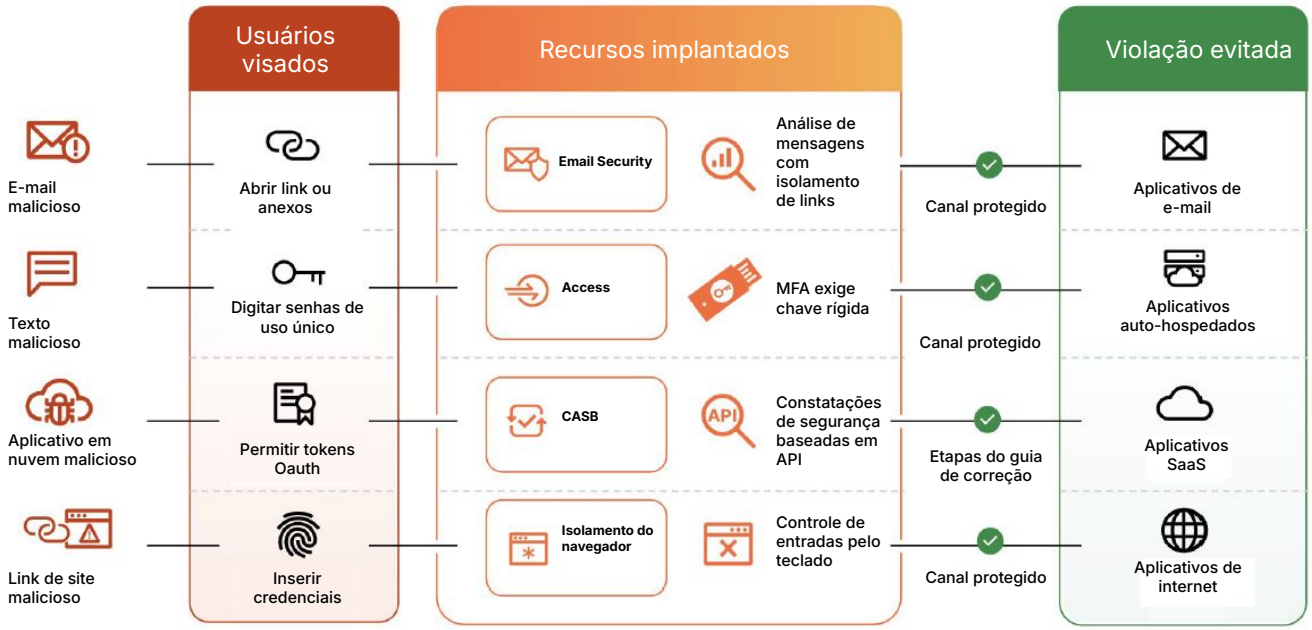
81%

das organizações sofreram um ataque multicanal nos últimos 12 meses[1]

SOLUÇÃO

Segurança unificada em todos os pontos de exposição ao phishing

Parar ataques multicanal requer uma plataforma que possa abordar todo o escopo de vulnerabilidades que existem nos fluxos de trabalho dos funcionários e nas interações no aplicativo. É por isso que a Cloudflare oferece a solução contra phishing mais completa, focada em fornecer proteção contínua entre funcionários e aplicativos. Aproveitando a plataforma Cloudflare One, as organizações podem tirar proveito dos serviços de segurança de e-mail (ES) e Zero Trust integrados nativamente para implantar proteção em camadas para e-mail, aplicativos auto-hospedados, aplicativos SaaS e aplicativos da internet, fornecendo defesa em profundidade para impedir pagamentos fraudulentos e violações de dados



Impedir preventivamente ameaças transmitidas por e-mail

Detecte comprometimento de e-mail empresarial (BEC), malware e outras ameaças originadas de e-mail com análise de conteúdo alimentada por IA/ML para proteção automatizada.

Evitar violações resultantes de roubo de credenciais

Impeça violações com acesso condicional e requisitos de chave física que atuam como uma última linha de defesa caso credenciais sejam roubadas ou comprometidas.

Bloquear e isolar ataques evasivos baseados em links

Isole os usuários de ataques direcionados que atraem funcionários através de aplicativos de mensagens comumente usados por meio de links habilmente ofuscados que são difíceis de capturar.

Acabe com as ameaças transmitidas por e-mail (ES)

Com o e-mail representando o aplicativo corporativo mais usado e explorado, é mais importante do que nunca proteger os usuários contra ataques de phishing que buscam manipular sua confiança por meio do e-mail. Ao aumentar ou substituir as defesas de e-mail atuais pela Cloudflare, as organizações podem mitigar automaticamente ataques de phishing sofisticados que aproveitam links de e-mail incorporados, anexos e contas personificadas ou comprometidas para roubar informações confidenciais e cometer fraudes financeiras.

A solução leve e nativa de nuvem da Cloudflare pode ser implantada em minutos para complementar os recursos de e-mail integrados fornecidos pela Microsoft e pelo Google. Com maior automação e ajuste mínimo necessário para resultados ideais, a Cloudflare reduz significativamente o tempo e o esforço necessários para o gerenciamento contínuo.

Comprometimento de e-mail empresarial (BEC)
A análise de conteúdo com tecnologia de IA/ML desconstrói cada mensagem para avaliar o histórico de conversas, padrões de escrita, sentimentos e outras variáveis para determinar a autenticidade do remetente.

Ransomware e anexos maliciosos
Modelos de detecção de ML em conteúdos maliciosos, detecção sem assinatura, visão computacional, extração remota e outras formas de análise são usados para identificar conteúdos maliciosos criptografados e não criptografados.

Links de e-mail maliciosos
Técnicas avançadas para desconstruir e detalhar URLs complexos são combinadas com isolamento de link adaptável para garantir uma experiência na web segura e sem atrito para os funcionários.

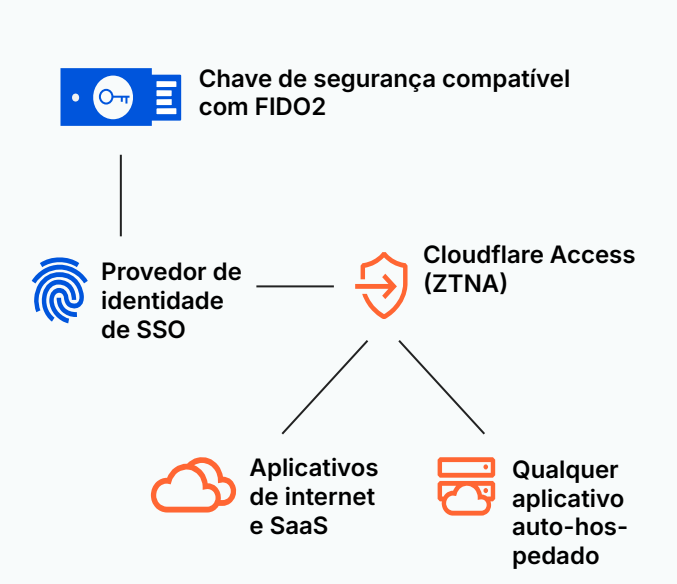
Mitigar ataques de phishing OAuth (CASB)

O phishing OAuth aproveita provedores de identidade legítimos e fluxos de trabalho de autorização para induzir usuários a conceder permissões a aplicativos maliciosos. A plataforma Cloudflare One oferece a capacidade de detectar esses aplicativos enquanto fornece orientação de correção para mitigar rapidamente essas ameaças.

Evitar violações de credenciais comprometidas (ZTNA)

Embora muitas organizações implementem medidas preventivas extensivas para evitar que as credenciais dos funcionários caiam nas mãos erradas, a dura verdade é que as medidas preventivas nunca são 100% infalíveis. No caso infeliz de as credenciais serem roubadas ou vazadas inadvertidamente, deve haver uma última linha de defesa para evitar uma violação total.

Com o Cloudflare Access atuando como uma camada de agregação em torno de cada recurso, incluindo recursos auto-hospedados ou não web, as organizações podem impor consistentemente a autenticação compatível com FIDO2 para MFA resistente a phishing. Portanto, mesmo no caso de as credenciais dos funcionários serem comprometidas, as organizações ainda conseguem garantir que seus dados estejam protegidos.



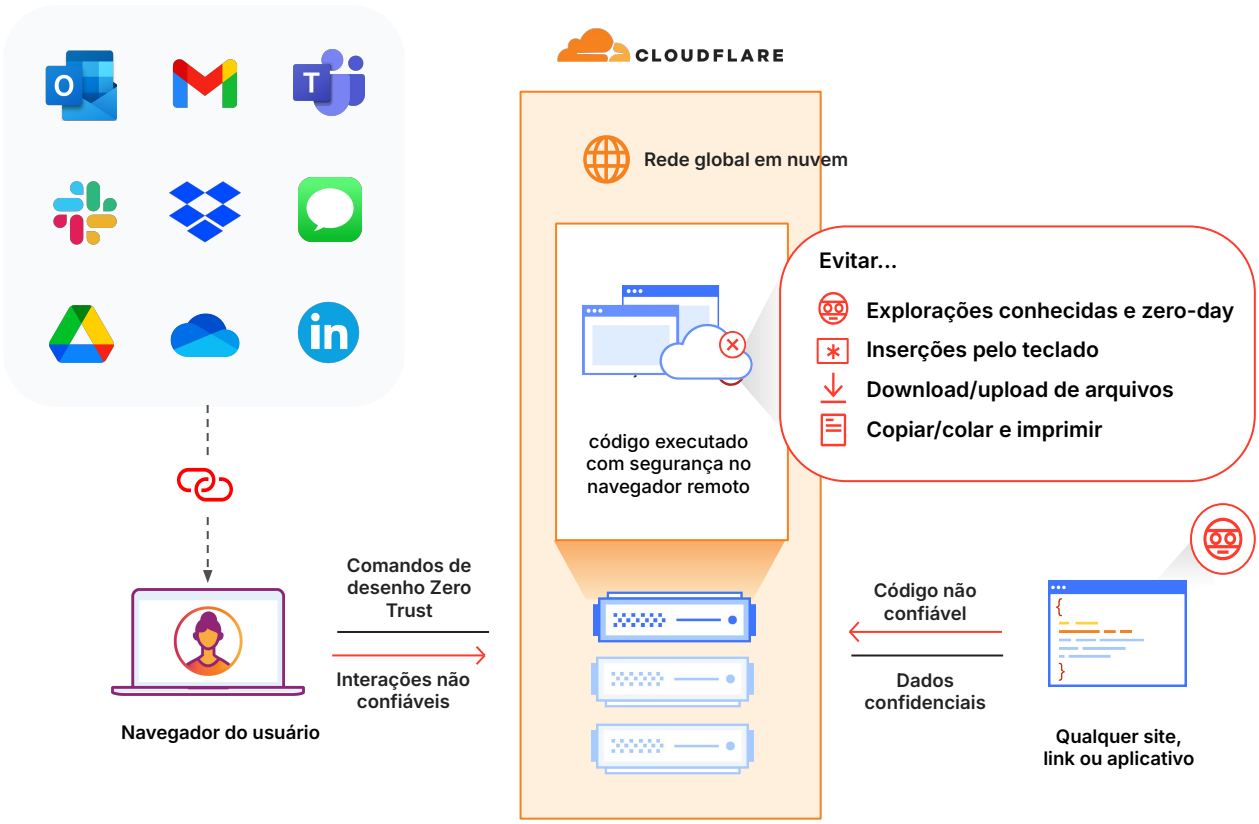
Isolar ataques baseados em links (ES + Isolamento do navegador remoto + SWG)

Ataques baseados em links se tornaram o método preferido para roubar credenciais, carregar malware/ransomware e extrair informações confidenciais. Usar uma combinação de e-mail, chat, SMS, redes sociais e drives em nuvem para entregar esses links complica ainda mais o processo de garantir que funcionários e dados estejam protegidos contra ataques de phishing direcionados.

O Isolamento do navegador da Cloudflare resolve ataques de phishing baseados em links renderizando todo o código da web remotamente em nossa rede global em nuvem ao invés de no dispositivo local do usuário. Isso atenua malware e zero day do navegador, ao mesmo tempo em que fornece controle granular sobre as ações do usuário (por exemplo, desabilitar entradas pelo teclado) para evitar coleta de credenciais e vazamentos de dados.

Eliminar o risco de phishing sem desacelerar sua força de trabalho

Ao integrar recursos de isolamento do navegador de última geração criados com nossa tecnologia exclusiva Network Vector Rendering (NVR), a Cloudflare é capaz de fornecer uma solução perfeita, segura e escalável para isolar links potencialmente maliciosos. Ao contrário de técnicas pesadas em largura de banda, o NVR transmite comandos de desenho seguro para o dispositivo. Isso ajuda a eliminar o risco de conteúdo malicioso da web sem impactar a experiência do usuário final. Graças ao NVR e à rede de baixa latência da Cloudflare, as organizações podem isolar ameaças multicanal, garantindo produtividade sem interrupções para seus funcionários.



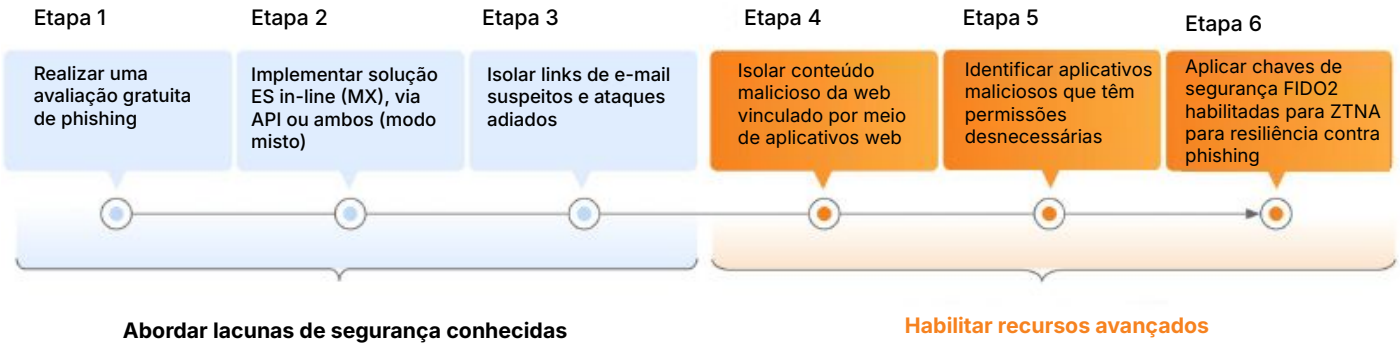
VANTAGENS

Proteção multicanal completa

À medida que as campanhas de phishing se expandem rapidamente para além do e-mail, agora é mais urgente do que nunca que as organizações implementem uma solução contra phishing que forneça um caminho rápido e simples para a proteção multicanal completa.

Usando a plataforma Cloudflare One, as organizações podem primeiro implantar a segurança de e-mail líder do setor para abordar rapidamente o canal de phishing mais crítico, depois, habilitar facilmente os serviços Zero Trust adicionais para estender a proteção a todos os canais, interrompendo efetivamente as ameaças de phishing conhecidas e emergentes.

- **Proteção de baixo impacto e alta eficácia:** minimize o risco de phishing com eficácia de detecção líder do setor que requer ajuste mínimo.
- **Maior consolidação, menor custo:** reduza os gastos com uma plataforma única e totalmente integrada que resolve todos os casos de uso de phishing.
- **Rápido de implantar, fácil de gerenciar:** garanta proteção imediata enquanto reduz o tempo e o esforço necessários para o gerenciamento contínuo.



Avalie e compare

Avalie suas defesas de e-mail atuais e veja quais ameaças não estão sendo detectadas

Execute um Retro scan gratuito (caixas de entrada do O365) em minutos para ver quais ameaças de phishing foram entregues nos últimos quatorze dias ou solicite uma avaliação de risco de phishing (PRA) para monitorar quaisquer caixas de entrada em relação a phishing conforme as ameaças são entregues. Avalie em relação a outros provedores que não têm ajuste pronto para uso para ver qual solução de segurança de e-mail oferece a proteção mais rápida e fácil.

Veja quais ameaças de phishing estão passando por suas defesas

Execute um Retro Scan | Solicite uma PRA

CLOUDFLARE

1. 2023 Forrester Opportunity Snapshot: Fonte
2. 2023 Phishing Threats Report Fonte