Cloudflare Email Security

Fornecer proteção autônoma e multicanal para comunicação segura no ambiente de trabalho

Proteja-se contra ataques de phishing direcionados

Bloqueie e isole facilmente ameaças que outras soluções não detectam

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. À medida que as organizações continuam a adotar cada vez mais serviços de e-mail em nuvem através do Microsoft 365 e do Google Workspace para apoiar melhor os trabalhadores híbridos, os agentes de ameaças têm se voltado para ataques mais direcionados e de baixo volume, capazes de escapar dos gateways de e-mail seguros (SEGs) tradicionais, como o Proofpoint e o Mimecast.

É por isso que a solução de segurança de e-mail nativa de nuvem da Cloudflare foi projetada exclusivamente para aproveitar a inteligência de campanha preventiva, a análise de conteúdo baseada em ML e uma plataforma Zero Trust unificada para deter as ameaças de phishing antes que elas cheguem à sua força de trabalho.

91%

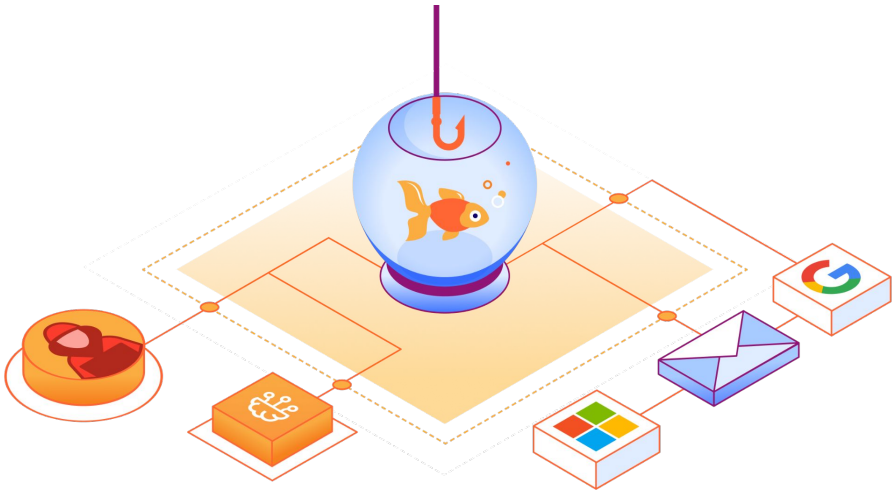
de todos os ataques cibernéticos começam com um e-mail de phishing[1]

50 bi

em perdas com ataques de BEC na última década[2]

81%

das organizações sofreram um ataque multicanal nos últimos 12 meses[3]



Pare o comprometimento de email empresarial (BEC)

Detecte contas falsificadas e comprometidas com análise contextual em camadas baseada em ML.

Isole ataques adiados e multicanal

Isole os usuários de conteúdo malicioso da web que é entregue por meio de links desconhecidos e ofuscados.

Bloqueie ransomware e anexos maliciosos

Evite que tentativas de extorsão e códigos maliciosos comprometam sua organização.

Maior proteção e simplicidade

Implemente segurança em camadas que oferece maior proteção por uma fração do custo

À medida que os ataques de phishing continuam a proliferar, a Microsoft e o Google continuam a desenvolver funcionalidades nativas que permitem recursos essenciais de proteção de e-mail e dados, como autenticação, arquivamento e criptografia do lado do cliente. No entanto, os agentes de ameaças evoluíram suas táticas para executar ataques mais direcionados e evasivos que muitas vezes contornam os controles de segurança nativos e geram uma taxa de sucesso mais alta.

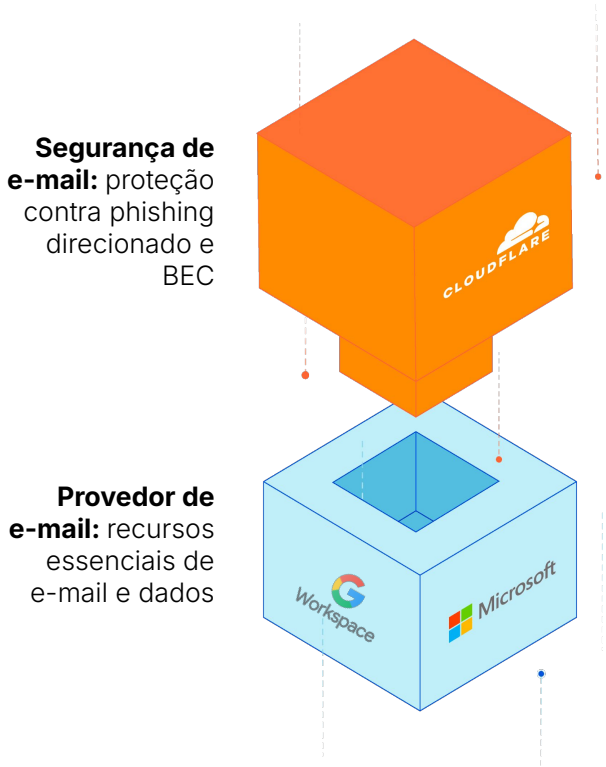
Ao utilizar a Cloudflare, as organizações podem bloquear ou isolar automaticamente ataques de phishing direcionados que utilizam links e anexos malicioso além de contas comprometidas para roubar informações confidenciais e cometer fraudes financeiras.

Aumente seus controles de segurança de e-mail existentes

A solução de segurança de e-mail nativa de nuvem da Cloudflare pode ser implantada em minutos para aprimorar as implantações de SEG existentes ou complementar os recursos de e-mail integrados fornecidos pela Microsoft e pelo Google. Com pouco ou nenhum ajuste necessário, as organizações podem obter maior proteção contra phishing com menos tempo e esforço dedicados ao gerenciamento contínuo da segurança.

"Desde que implementamos a Cloudflare [sobre o M365], observamos uma redução de 50% no número de e-mails maliciosos ou suspeitos que nossos usuários recebem todos os dias. Isso libera várias horas que podemos reinvestir em outras metas."

Werner Enterprises
(Fortune 1000)



Reinvestir as horas economizadas com o aumento da automação

A solução automatizada e leve da Cloudflare oferece integração perfeita com os fluxos de trabalho da Microsoft e do Google, ao mesmo tempo que fornece uma interface de usuário única e intuitiva para atividades de analistas.

Atingir 99,997% de eficácia de detecção

A combinação dos recursos nativos do provedor de e-mail com a proteção contra phishing e BEC da Cloudflare garante que as empresas tenham cobertura abrangente para riscos mínimos.

Obter maior valor com menor custo

Substituir implantações desatualizadas, caras e complexas pela solução de baixo impacto da Cloudflare pode reduzir a sobrecarga operacional, recursos redundantes e ajustes excessivos.

Pare ataques sofisticados de BEC

US$ 50 bilhões em perdas relatadas e aumentando

Com os ataques de BEC responsáveis por uma quantidade impressionante de perdas na última década, é surpreendente que algumas organizações ainda não tenham priorizado o combate a uma forma tão eficaz de fraude financeira. Embora os ataques de BEC representem uma percentagem muito menor de ameaças de phishing, muitas vezes passam despercebidos pelos SEGs e pelos fornecedores de e-mail em nuvem, resultando em maiores perdas financeiras. Esses ataques direcionados são difíceis de detectar porque aproveitam contas falsificadas ou comprometidas e o contexto de conversas para se passarem por funcionários ou fornecedores confiáveis.

Ampliar os princípios Zero Trust para o e-mail

Ao aproveitar uma conta de e-mail de funcionário ou fornecedor comprometida, os invasores podem escapar dos controles de segurança tradicionais que apenas tentam confirmar a legitimidade da conta do remetente. A Cloudflare vai um passo além ao analisar uma ampla gama de atributos comportamentais, padrões de escrita, indicadores de sentimento e histórico de conversas para determinar a autenticidade do remetente. Os modelos de ameaças baseados em ML e a ampla inteligência da rede da Cloudflare fornecem a arma mais eficaz contra contas comprometidas usadas para extrair pagamentos fraudulentos.

Figura 1: Análise de mensagens

Detectar BEC com análise contextual baseada em ML

A identificação precisa de ataques de BEC requer mais do que apenas uma análise estrutural de uma mensagem. A detecção bem-sucedida também envolve uma compreensão granular das variações no estilo e na intenção da conversa. A telemetria de rede expansiva da Cloudflare (mais de 3 trilhões de solicitações de DNS diariamente) e os modelos de ML em evolução alimentam o Analytics Engine de pequenos padrões que desconstrói todos os aspectos de uma mensagem de e-mail para avaliar padrões de escrita, sentimento, contexto histórico e muitas outras variáveis que ajudam a descobrir a autenticidade do remetente.

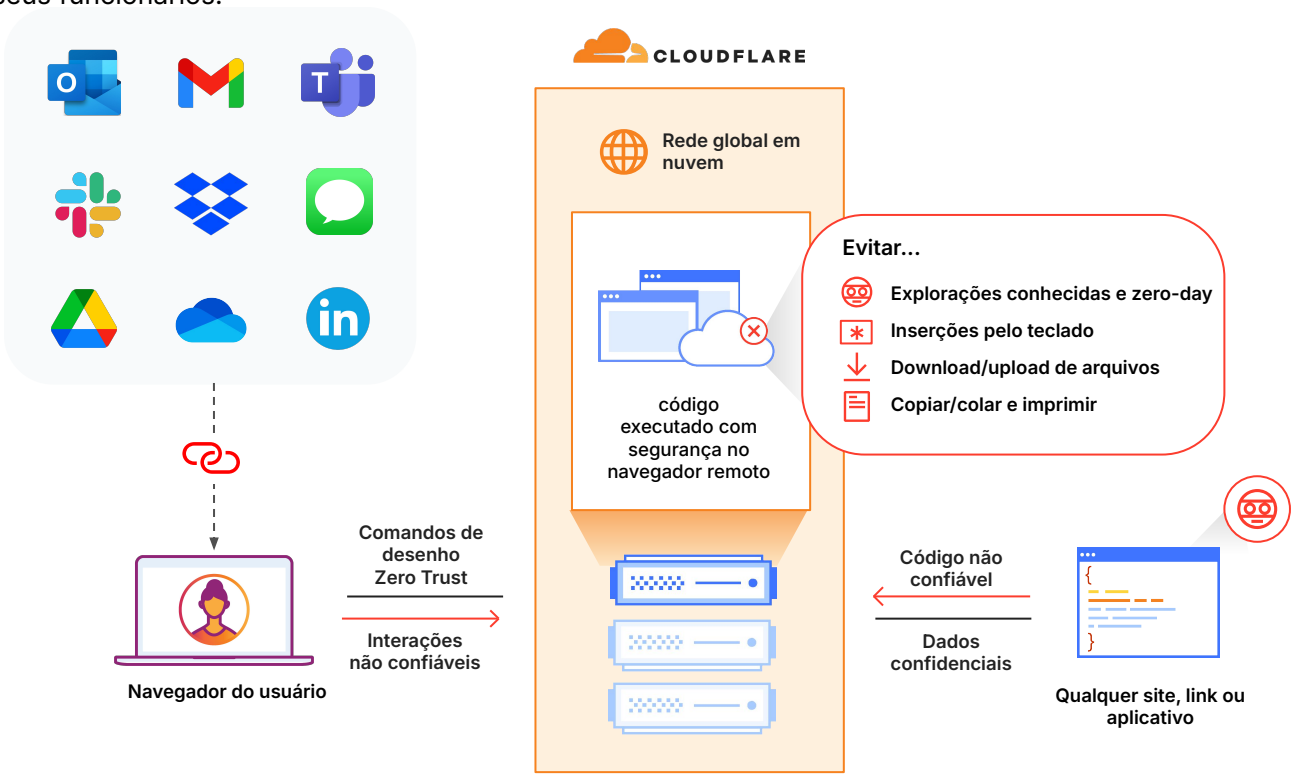
Isolar ataques baseados em links

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 outros aplicativos para entregar esses links complica ainda mais o processo de garantir que funcionários e dados estejam protegidos contra ataques de phishing direcionados.

A 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 a 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.



Investigação e resolução rápidas

Gerenciamento de segurança intuitivo e de baixo impacto

Com maior automação e configuração mínima necessária para obter resultados ideais, a Cloudflare reduz significativamente o tempo e o esforço necessários para o gerenciamento contínuo da segurança de e-mail. As equipes de segurança podem obter imediatamente uma visão completa de todas as principais métricas e tendências no painel, com a capacidade de clicar em detalhes mais granulares em torno das mensagens sinalizadas. O detalhamento das tendências permite a descoberta rápida dos tipos de ataques frequentes, dos quais os executivos estão sendo alvo, dos ataques adiados mitigados e de outros pontos de dados críticos.

Todas as análises de dados, telemetria, observações de ameaças e indicadores de comprometimento (IOCs) estão disponíveis por meio de uma API extensa para fácil integração aos fluxos de trabalho de analistas e ferramentas de orquestração existentes.

> "Costumo dizer aos colegas de trabalho como a Cloudflare é simples e fácil de usar como uma solução SaaS baseada em nuvem e exponho como estou satisfeito com seu alto nível de precisão."
>
> **Japan Airlines**

Detecção e resposta gerenciadas (PhishGuard)

O serviço de segurança de e-mail gerenciado da Cloudflare, PhishGuard, complementa sua equipe SOC existente para liberar ciclos de investigação de segurança e fornecer inteligência contra ameaças valiosa. O PhishGuard pode ajudar a neutralizar campanhas de phishing auxiliando em investigações, avaliações de ameaças internas, remoções de fraudes ativas e necessidades complexas de remediação. O PhishGuard amplia recursos de segurança e a experiência para notificar ativamente sobre possíveis fraudes e ameaças internas, ao mesmo tempo em que realiza a busca por ameaças por e-mail.

Recursos e vantagens do PhishGuard:

- Envios de phishing gerenciados e resposta a incidentes para resolução mais rápida.
- Notificações proativas de BEC e fraude para que as organizações possam responder rapidamente no início do ciclo de vida do ataque.
- Recursos dedicados para monitoramento em tempo real, análises periódicas de contas e avaliações contínuas de ameaças.
- Assinaturas de bloqueio personalizadas com base em uma análise de ameaças do ambiente gerenciado.

+ de 1100

Horas economizadas anualmente com a automação de esforços de triagem manual

A solução automatizada da Cloudflare elimina tarefas manuais e demoradas para melhorar os tempos de resposta e desbloquear ciclos adicionais.

50%

Redução na entrega de e-mails maliciosos ou suspeitos (no M365)

Colocar a Cloudflare em camadas sobre o Microsoft 365 permite que as organizações detectem ataques direcionados e reduzam o número geral de e-mails maliciosos.

40

Total de horas gastas em sete anos na configuração de segurança de e-mail

A segurança de e-mail de baixo impacto da Cloudflare requer pouca configuração inicial e ajuste contínuo reduzido, proporcionando alta eficácia de detecção pronta para uso.

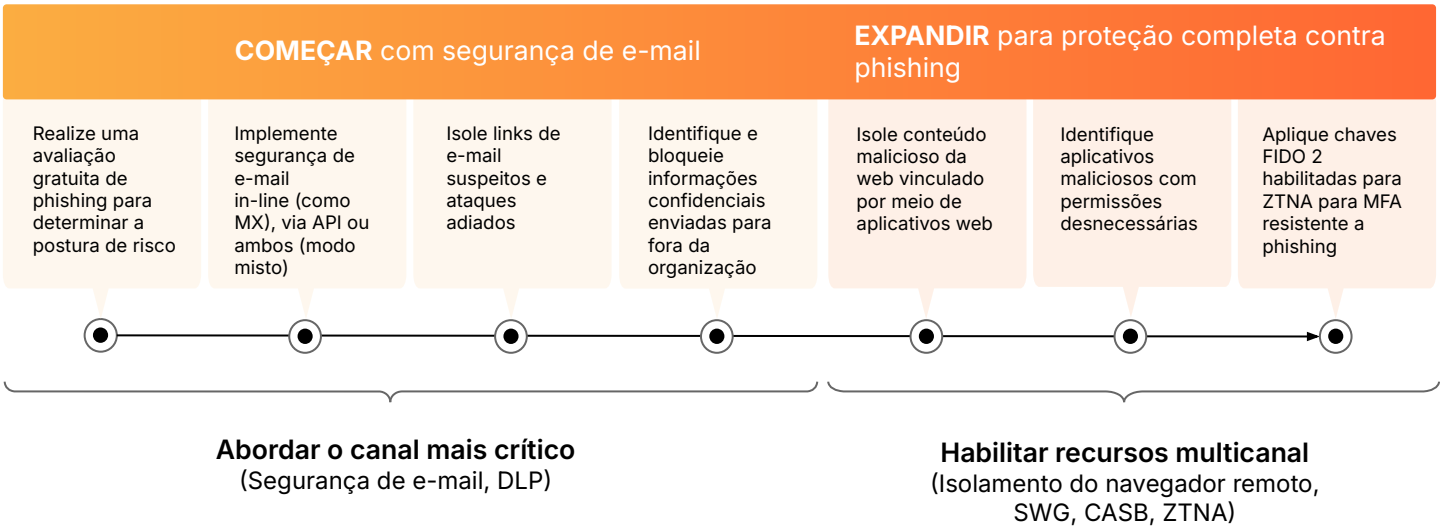
VANTAGENS

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 de phishing que forneça um caminho rápido e simples para a proteção multicanal completa.

Com a plataforma de segurança unificada da Cloudflare, 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 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 em minutos para ver quais ameaças de phishing passaram despercebidas nos últimos quatorze dias ou solicite uma avaliação de risco de phishing (PRA) para monitorar caixas de entrada em relação a phishing à medida que 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.

Executar um Retro Scan | Solicite uma PRA

1. 2020 Deloitte research: Fonte
2. 2023 FBI IC3 PSA: Fonte
3. 2023 Forrester Opportunity Snapshot: Fonte

