CLOUDFLARE

RESUMO DA SOLUÇÃO

Cloudflare + Microsoft 365 Proteção contra phishing

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

Abandone o gateway legado e atualize sua proteção contra phishing

No início dos anos 2000, os gateways de e-mail seguros (SEGs) foram introduzidos para lidar com uma necessidade crescente em torno do roteamento e filtragem de e-mail. Embora os SEGs tenham sido bem-sucedidos em sua missão por muitos anos, seu design fundamental tornou impossível para eles acompanhar o ritmo conforme as ameaças de phishing crescem rapidamente em escopo e sofisticação.

Atualizar continuamente conjuntos de regras e políticas manuais que foram originalmente criados para servidores locais apenas inflaciona a quantidade de tempo e esforço envolvidos na manutenção de um SEG. Isso resulta em um aumento no custo e na complexidade, mas ainda não consegue capturar as ameaças mais perigosas, como ataques de comprometimento de e-mail empresarial (BEC). O aumento na sobrecarga e a diminuição na eficácia podem ser atribuídos a:

- **Táticas emergentes de phishing e ameaças zero-day** - os ataques de phishing modernos empregam táticas cada vez mais enganosas projetadas para escapar de filtros estáticos e controles tradicionais. Isso dificulta para os SEGs bloquear novas ameaças que não possuem indicadores conhecidos de comprometimento.
- **Implementações complexas** - os SEGs exigem configuração extensa e ajuste constante para se adaptarem a ameaças emergentes, além de exigirem vários módulos complementares para utilizar totalmente seus recursos.
- **Resposta a incidentes demorada** - quando atividades suspeitas ou maliciosas ignoram os controles de SEG implantados, o processo de investigação e resposta pode ser longo e trabalhoso, envolvendo uma colcha de retalhos de interfaces e fluxos de trabalho.

Implemente proteção de alta eficácia e baixo impacto

À medida que as organizações continuam a adotar o Microsoft 365 para aprimorar a comunicação e a colaboração para sua força de trabalho híbrida, é essencial aproveitar os recursos de segurança nativos da Microsoft ao integrar soluções complementares baseadas em aprendizado de máquina para bloquear e isolar automaticamente as ameaças mais perigosas. Essa estratégia não apenas reduz significativamente o risco de phishing, mas também simplifica os fluxos de trabalho, minimizando o tempo e o esforço necessários para o gerenciamento contínuo da segurança.

91%

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

Número 1

vetor de ataque para cometer fraude e obter acesso[2]

US$ 50 bi

em perdas com ataques de BEC na última década[3]

US$ 4,88 mi

representa o custo médio de uma violação de dados em 2024[4]

1. 2020 Deloitte research
2. Microsoft SIR Report
3. 2023 FBI IC3 PSA
4. 2024 IBM Cost of a Data Breach

Recursos de segurança de e-mail da Microsoft

Remover a sobreposição de SEG para reduzir riscos e custos

Os analistas concordam que consolidar recursos para minimizar a sobreposição de funcionalidades está ajudando as organizações a reduzir custos e complexidade. No entanto, eles também aconselham as organizações a avaliar cuidadosamente os recursos nativos para garantir que eles satisfaçam todos os casos de uso.

À medida que a Microsoft continua a desenvolver seus recursos essenciais de segurança de e-mail, a crescente sobreposição com SEGs deu às organizações uma oportunidade de otimizar as operações de segurança aproveitando os recursos já incluídos em sua licença E3 ou E5. Essa mudança permite que as organizações eliminem implantações de SEG complexas e caras, redirecionando uma fração desse orçamento para integrar soluções leves que abordam efetivamente as ameaças de phishing mais perigosas.

O Cloudflare Email Security fornece uma solução integrada e de baixo impacto que aumenta o Microsoft 365 usando análise de ameaças de aprendizado de máquina para automatizar a detecção de BEC e ataques multicanal.

As áreas de funcionalidade SEG sobrepostas incluem:

- **Higiene de e-mail**
  Políticas baseadas em regras para spam e mensagens em massa, com detecção baseada em assinatura para malware conhecido.
- **Proteção contra URLs e anexos**
  Reescrita básica para todos os links de e-mail e recursos de sandbox para anexos.
- **Investigação e caça a ameaças**
  Pesquisa de e-mail, investigação e correlação de incidentes, caça e remediação.
- **Proteção de informações**
  Políticas de criptografia, arquivamento e DLP para e-mail, arquivos e endpoints.
- **Conscientização e treinamento**
  Simulações de ataques de phishing e treinamento para usuários finais.

Proteção Exchange Online contra DDoS

Inclusa em todos os planos e fornece higiene de e-mail essencial para filtrar em massa, spam e malware.

- Antispam
- Proteção contra malware baseada em assinatura

Microsoft Purview (DLP)

Regras de prevenção contra perda de dados e aplicação configuráveis. Integrado com o Microsoft Information Protection.

- DLP para e-mail e arquivos
- DLP para Teams
- DLP para endpoints

Defender for O365 Plano 1

Controles de segurança adicionais para proteção básica contra links e anexos maliciosos.

- Links seguros (reescrita de URL)
- Anexos seguros (sandboxing)
- Proteção interna de e-mail

Defender for O365 Plano 2

Inclui tudo no plano 1, além de recursos adicionais para caça a ameaças, investigação, treinamento e resposta.

- Caça a ameaças
- Correlação de incidentes entre domínios
- Treinamento de simulação de ataque cibernético

Licença E3

Licença E3 + Conformidade

Licença E3 + Conformidade + Segurança

Licença E5

● Completo ● Limitado ● Nenhum

		SEG	M365	Cloudflare
Prevenção contra ameaças	Listas de permissões/bloqueios	●	●	●
	Remetente nocivo conhecido	●	●	●
	URL/anexo nocivo conhecido	●	●	●
	Filtragem em massa/spam	●	●	●
	Aprendizado de máquina (análise de conteúdo)	●	○	●
	Malware/ransomware zero-day	●	●	●
	Links maliciosos	●	●	●
	Reescrita de URL (análise de tempo de clique)	●	●	●
	Isolamento de link adaptável	○	○	●
	Comprometimento de e-mail empresarial (BEC)	●	●	●
	Falsificação de funcionário	●	●	●
	Falsificação de fornecedor	●	●	●
	Comprometimento de funcionário (ATO)	●	●	●
	Comprometimento de fornecedor	●	●	●
	Gerenciamento DMARC	●	●	●
	Detecção de aplicativo malicioso (OAuth Phish)	●	●	●
	Segurança de conteúdo da web	●	●	●
	Conscientização e treinamento sobre segurança	●	●	●
Resposta a ameaças	Interface única e intuitiva	○	●	●
	Triagem automática de ameaças	○	●	●
	Pesquisa e investigação rápidas	●	●	●
	Retração automática	●	●	●
	Relatórios sob demanda	●	●	●
	Serviço de detecção e resposta gerenciado	●	○	●
Proteção de dados	Criptografia	●	●	○
	Arquivamento	●	●	○
	DLP para e-mail	●	●	●
	DLP para nuvem (aplicativos de colaboração)	●	●	●
	DLP para rede	●	●	●

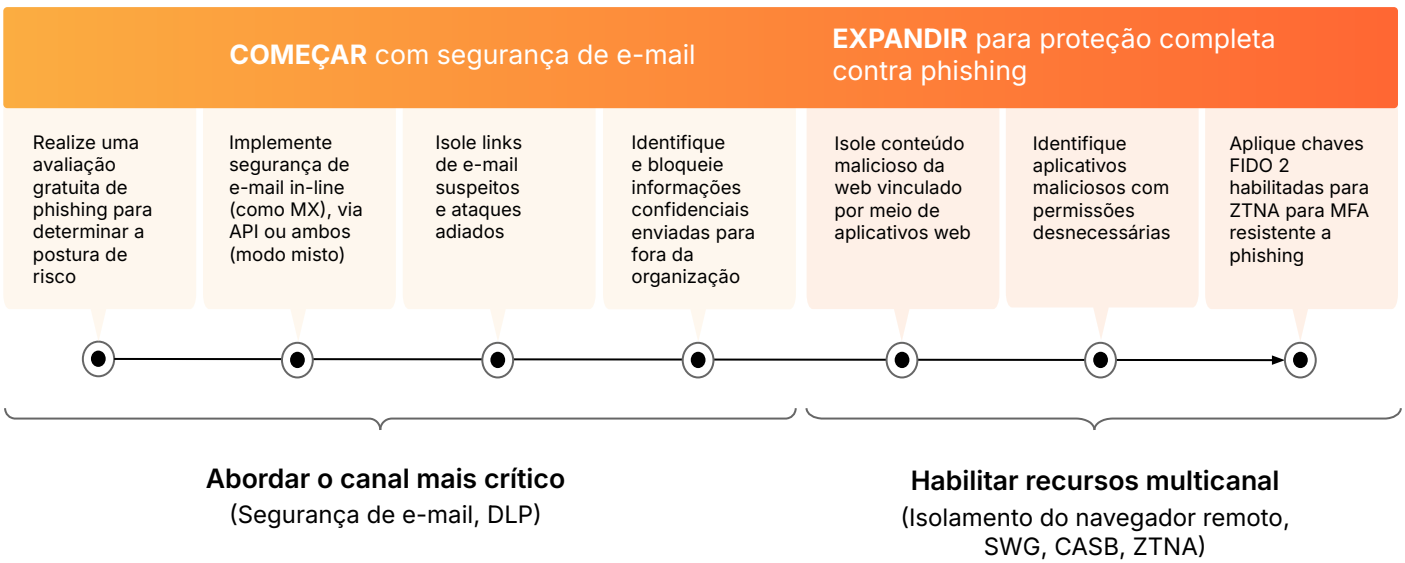
VANTAGENS

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 outros provedores sem nenhum ajuste pronto para uso para ver qual solução de segurança de e-mail oferece a proteção mais rápida e fácil.

Execute um Retro Scan

Solicite uma PRA

© 2024 Cloudflare, Inc. Todos os direitos reservados.