proofpoint.

GUIA DO COMPRADOR

Guia do CISO para combater ameaças centradas em pessoas e em IA

Capacidades fundamentais

Estas são as cinco capacidades necessárias para proteger sua organização contra ameaças centradas em pessoas e em IA:

1. Visibilidade abrangente sobre ameaças e insights sobre riscos
2. Proteção automatizada contra ameaças no e-mail e além
3. Segurança para comunicações empresariais confiáveis
4. Orientação para os funcionários
5. Proteção contra sequestro de contas

Visão geral

Os perpetradores de ameaças continuam ampliando seus esforços para extrair dados e explorar comunicações empresariais para fins de ganho financeiro. Embora essas ameaças continuem aumentando em número, as táticas de ameaça permanecem em grande parte as mesmas. Phishing, malware, ransomware, comprometimento de e-mail corporativo (BEC) e engenharia social ainda são maneiras comuns de visar pessoas.

A novidade é que a IA está potencializando essas táticas já conhecidas. Os perpetradores de ameaças estão utilizando grandes modelos de linguagem para criar iscas de phishing hiperpersonalizadas, automatizar 80% a 90% da cadeia de ataque e lançar campanhas de várias estágios e por diversos canais em uma escala sem precedentes. A Proofpoint observou um aumento de 94% nas ameaças de e-mail direcionadas a clientes somente em 2025. A IA também está introduzindo vetores de ataque totalmente novos, como os ataques de injeção de prompts, que transformam assistentes de IA corporativos em armas por meio de instruções ocultas incorporadas em e-mails.

Neste guia, vamos explorar as principais capacidades necessárias para construir uma defesa forte contra todas as ameaças centradas em pessoas e em IA — sejam baseadas em e-mail ou não. Também vamos sugerir o que levar em consideração ao escolher a plataforma de segurança ideal para você.

Figura 1. Ameaças e riscos em espaços de trabalho digitais.

1. Visibilidade abrangente sobre ameaças e insights sobre riscos

Para deter ameaças centradas em pessoas e em IA, você precisa saber quais dos seus usuários estão sendo visados — e como. Isso permite que você aplique controles de segurança adaptáveis para proteger as pessoas que estão sob maior risco.

A visibilidade abrangente sobre ameaças no e-mail e em canais digitais proporciona uma imagem completa das suas vulnerabilidades.

Isto é o que você quer que a solução mostre:

- **Quem está sendo visado**, bem como as ameaças enfrentadas e se houve interação com os atacantes
- **Detalhes forenses**, inclusive o perpetrador da ameaça, a família de ameaças, os usuários afetados, as técnicas e temas do ataque e os objetivos da campanha de ataque
- **Usuários sob risco**, identificando as pessoas que constituem risco para a sua organização e por que
- **Ameaças dentro de comunicações empresariais confiáveis**, inclusive domínios ou sites semelhantes e falsificados que podem prejudicar a reputação da sua marca
- **Mudanças comportamentais e inteligência sobre ameaças** que podem revelar indícios de que um dos seus fornecedores ou um terceiro confiável pode estar comprometido
- **Atividades suspeitas** indicadoras de possíveis sequestros de contas ativas

Uma plataforma baseada em IA pode correlacionar sinais entre essas dimensões, utilizando gráficos de relacionamentos para estabelecer padrões de comunicação normais como referência, modelos de linguagem para interpretar a intenção das mensagens e inteligência sobre ameaças para contextualizar o comportamento dos atacantes. Como resultado, você obtém insights sobre risco mais detalhados e mais decisivos do que os obtidos apenas por meio de análise manual.

US$ 4,88 M

é o custo médio de uma violação de dados em um ataque de phishing ou BEC .[1]

1. IBM. *Relatório sobre o custo de uma violação de dados*. 2024.

A visibilidade não só é importante em implantações iniciais, como precisa ser contínua. Isso garante que você possa ajustar continuamente o seu nível de proteção conforme os ataques mudam.

2. Proteção automatizada contra ameaças no e-mail e além

O cenário de ameaças evolui constantemente. Infelizmente, as organizações frequentemente carecem de profissionais especializados em segurança e dos recursos necessários para acompanhar as mudanças. Consequentemente, é comum que as equipes simplesmente não tenham tempo para investigar cada evento de segurança. Além disso, o custo desses eventos está aumentando.

É por isso que você precisa de uma solução que possa detectar e bloquear ameaças com precisão e eficiência, sem afetar a produtividade. À medida que as ameaças são cada vez mais geradas e transmitidas por IA, suas capacidades de detecção também precisam ser baseadas em IA.

Isto é o que você quer que a solução faça automaticamente:

- **Bloquear ameaças antes da entrega,** com uma eficácia de pelo menos 99,999% para que elas nunca cheguem às caixas de entrada dos usuários
- **Detectar e bloquear ameaças geradas por IA**, inclusive mensagens de BEC criadas por IA, phishing personalizado por IA e ataques ocultos de injeção de prompts que têm como alvo assistentes de IA como o Microsoft Copilot.
- **Analisar padrões comportamentais de e-mails enviados internamente, utilizando tecnologia de inteligência sobre ameaças baseada em IA e modelos de autoaprendizagem para detectar atividades de phishing lateral**
- **Inspecionar e bloquear URLs maliciosos em tempo real para assegurar que eles não cheguem aos usuários por e-mail ou plataformas de colaboração e mensagens**
- **Detectar e responder a contas de provedores de identidade (IdP) comprometidas** hospedadas na nuvem
- **Analisar códigos QR suspeitos antes da entrega** por meio de visão computacional e análise semântica com base em IA, além de oferecer análise em área restrita
- **Inserir tags de advertência** nas mensagens suspeitas

Quando um atacante consegue acesso inicial, é essencial detectar e responder a essa ameaça rapidamente. Isso pode significar a diferença entre um incidente menor e uma violação em grande escala.

3. Segurança para comunicações empresariais confiáveis

As comunicações digitais são essenciais para as organizações. Por isso os malfeitores se empenham tanto em infiltrar comunicações confiáveis. Quando os destinatários podem ser levados a pensar que estão interagindo com fontes confiáveis, ataques como BEC, phishing e ransomware têm mais chances de êxito.

Para maximizar suas chances de enganar pessoas, os malfeitores utilizam uma ampla variedade de táticas de impostura. A IA tornou a falsificação de identidade muito mais eficaz. Os atacantes agora podem gerar, em questão de segundos, mensagens bem elaboradas e contextualmente adequadas que imitam o tom e o estilo de redação de um executivo. Portanto, é essencial contar com várias camadas de proteção para impedi-los.

- **Viabilize a autenticação de e-mail** , tanto para e-mails gerados por usuários quanto por aplicativos
- **Ofereça um ambiente seguro e dedicado** para retransmissão de e-mails transacionais gerados por aplicativos
- **Auxilie na implementação de DMARC** para maximizar a eficácia da autenticação de e-mail e assegurar total conformidade com DMARC
- **Proteja contra domínios semelhantes** e inclua detecção e assistência para bloqueio e remoção física desses domínios
- **Monitore o surgimento de contas de fornecedor comprometidas** utilizando IA comportamental e inteligência sobre ameaças e execute medidas automatizadas para se defender contra elas

Ao proteger suas comunicações empresariais confiáveis, você não só protege os seus funcionários, mas também protege os seus clientes e parceiros comerciais.

71%

dos funcionários admitiram ter comportamentos arriscados, como reutilizar senhas ou clicar em links desconhecidos.[2]

2. Proofpoint. *Relatório State of the Phish.* 2024.

4. Orientação para os funcionários

Mesmo que a tecnologia bloqueie 99% das ameaças, o 1% restante ainda pode resultar em um incidente grave. É aí que o comportamento humano se torna o fator decisivo. Os perpetradores de ameaças geralmente precisam que o seu pessoal os auxilie em suas campanhas maliciosas.

Porém, ataques não são a única preocupação. Os usuários frequentemente sacrificam a segurança de suas organizações em prol da conveniência. Segundo o relatório *State of the Phish de 2024* da Proofpoint:

- 71% dos funcionários admitiram ter comportamentos arriscados, como reutilizar senhas ou clicar em links desconhecidos.
- 96% desses funcionários sabiam que seu comportamento era arriscado, mas mesmo assim correram o risco.

À medida que as ferramentas de IA se tornam parte integrante dos fluxos de trabalho diários, os funcionários também enfrentam novos riscos, como compartilhar dados confidenciais com aplicativos de IA não autorizados ou desencadear inadvertidamente injeções de prompts ocultos ao interagir com assistentes de IA.

Quando ataques e ações descuidadas por parte do usuário se combinam, as chances de uma violação ser bem-sucedida são muito maiores. Por isso você precisa educar os seus usuários.

Procure uma solução que:

- **Utilize os seus dados sobre ameaças** para identificar os seus usuários mais visados e de maior risco
- **Forneça aos usuários uma educação baseada em risco** que utilize exemplos de ameaças da vida real, como aquelas que realmente visam a sua organização
- **Tenha foco em mudança comportamental**, e não apenas em cumprir um requisito para o seu treinamento anual de segurança
- **Incentive os funcionários** proporcionando visibilidade sobre suas pontuações de risco individuais, bem como seu impacto na postura de segurança da sua organização
- **Avalie a eficácia** e forneça relatórios valiosos que ajudem você a aprimorar a sua estratégia
- **Aborde os riscos da IA em conteúdos de treinamento**, inclusive o uso seguro de ferramentas de IA generativa e como reconhecer ataques de engenharia social gerados por IA

Uma tecnologia robusta, combinada com vigilância humana, é fundamental para bloquear ameaças centradas em pessoas. Todos têm um papel vital a desempenhar na proteção das operações da sua empresa.

5. Proteção contra sequestro de contas

Dados da Proofpoint mostram que 99% das organizações enfrentam tentativas regulares de sequestro de contas (ATOs). Esses ataques são uma forma de roubo de identidade, na qual um criminoso cibernético obtém acesso ou "sequestra" uma conta on-line. Não surpreende que provedores de identidade baseados na nuvem — como Microsoft Entra ID, Google e Okta — sejam os mais visados. Essas contas servem como gateways de login único (SSO) para o conjunto de aplicativos corporativos de um usuário.

E não são apenas as suas contas que são motivo de preocupação. Cibercriminosos também comprometem contas de parceiros comerciais confiáveis para realizar reconhecimento e lançar novos ataques. Essas contas comprometidas servem como ponto de entrada para ataques em várias etapas que se espalham por todo o ecossistema de uma organização, roubando dados confidenciais, realizando transações fraudulentas e causando estragos.

IA e autoaprendizagem são essenciais para monitorar comunicações empresariais em grande escala e automatizar respostas. Modelos de IA comportamental são capazes de detectar sinais sutis de comprometimento de conta — como padrões incomuns de login, comportamentos anômalos no envio de e-mails ou mudanças nas relações de comunicação — que sistemas baseados em regras não conseguiriam identificar.

Procure uma solução que:

- **Monitore continuamente todas as contas** em serviços de provedores de identidade baseados na nuvem, como Microsoft Entra ID, Google e Okta
- **Utilize inteligência sobre ameaças** em conjunto com dados comportamentais e autoaprendizagem para detectar contas comprometidas
- **Defenda contra ataques de sequestro de contas** que contornam autenticação por múltiplos fatores (MFA); 65% das contas sequestradas tinham MFA ativada[4]
- **Acelere suas investigações,** proporcionando uma visão centralizada das atividades subsequentes ao sequestro de conta
- **Automatize as capacidades de resposta**, como suspensão de contas, redefinições forçadas de senhas e reversão de alterações maliciosas em regras de caixa de correio e configurações de MFA
- **Remova aplicativos** de terceiros suspeitos como parte da limpeza pós-sequestro

99%

das organizações enfrentam tentativas regulares de sequestro de contas (ATOs).[3]

3. Pesquisa da Proofpoint.
4. Ibid.

Os sequestros de contas podem ser onerosos e prejudicar a sua marca. Uma proteção forte é essencial para reduzir o seu risco.

Evite adotar uma abordagem fragmentada

Ao construir as suas defesas para e-mail e além, soluções separadas de vários fornecedores especializados podem parecer uma opção óbvia. Afinal, fornecedores especializados parecem bem equipados para lidar com tipos de ataque específicos. No entanto, essa abordagem compartimentada tem várias desvantagens.

Primeiramente, ela causa pontos cegos na segurança. Quando as ferramentas não se integram perfeitamente, as equipes de segurança podem achar difícil obter visibilidade sobre todo o ambiente de segurança. Isso não só aumenta as possibilidades de que as ameaças não sejam detectadas, como atrasa a resposta aos incidentes.

Ferramentas fragmentadas também não conseguem oferecer a abordagem de IA colaborativa necessária para conter as ameaças atuais. É necessário que modelos de linguagem, visão computacional, análise comportamental e inteligência sobre ameaças trabalhem em conjunto e compartilhem o contexto para detectar ataques sofisticados gerados por IA.

Além disso, é demorado e ineficaz que as equipes gerenciem várias ferramentas de segurança. Elas também precisam correlacionar dados entre pontos de controle isolados. A enorme quantidade de alertas que essas plataformas geram resulta em fadiga de alertas e ameaças não detectadas. Tudo isso aumenta os custos operacionais.

Por que não adotar uma abordagem mais eficaz? Adote uma plataforma de segurança pré-integrada e holística que lide com todas as ameaças centradas em pessoas. Ao trabalhar com um único parceiro confiável, você não só tem um gerenciamento simplificado, como também tem vantagens financeiras.

Conclusão

Uma estratégia abrangente de segurança centrada em pessoas pode proteger a sua organização contra uma ampla variedade de ameaças. Ao dar o seu primeiro passo rumo a essa meta, você deve começar com a solução certa. Procure uma solução que agregue inteligência sobre ameaças em e-mail, ferramentas de colaboração, plataformas de mensagens e aplicativos de nuvem. Ela também deve oferecer insights fundamentais sobre comportamentos arriscados dos usuários e ajudar a incrementar a sua cultura de segurança.

A sua solução atual limita-se apenas ao e-mail? Você depende de soluções pontuais fragmentadas? Se a resposta é sim, há espaço para melhorar. Agora é hora de avaliar o quanto a sua segurança protege você contra todas as ameaças centradas em pessoas no e-mail e além.

Consolide com a Proofpoint

O Proofpoint Prime Threat Protection oferece uma plataforma pré-integrada de proteção contra ameaças para proporcionar uma segurança completa. O Proofpoint Prime bloqueia ameaças em espaços de trabalho modernos, inclusive e-mail e canais digitais. Ele não só protege contra a mais ampla variedade de ameaças, como também faz isso com uma precisão inigualável. Respaldado pela plataforma Proofpoint Nexus AI (um conjunto de mecanismos de IA que inclui modelos de linguagem, autoaprendizagem, visão computacional, gráficos de relacionamentos e inteligência sobre ameaças), o Proofpoint Prime oferece uma eficácia de detecção de 99,999% contra ameaças tradicionais e geradas por IA.

Ele também oferece insights profundos sobre risco humano e reforça a resiliência dos usuários. Ele defende contra contas comprometidas de usuários e fornecedores para manter seguras as suas comunicações empresariais confiáveis.

A Proofpoint oferece a única arquitetura de segurança moderna com uma abordagem adaptável para proteção dos seus principais ativos e maiores riscos: seu pessoal. É por isso que mais de 2,7 milhões de clientes de todos os portes, inclusive mais de 80 empresas da Fortune 100, confiam na Proofpoint.

proofpoint.

DESCUBRA A PLATAFORMA DA PROOFPOINT →