

Proofpoint Impersonation Protection

Proteja suas comunicações com parceiros, clientes e fornecedores confiáveis



Principais destaques

- **Proteja suas comunicações empresariais confiáveis contra ameaças de impostura**
- **Evite que você e sua marca sejam vítimas de abuso por impostura**
- **Monitore domínios parecidos maliciosos e providencie sua remoção**
- **Detecte e defenda-se contra fornecedores arriscados, inclusive contas comprometidas de fornecedores**
- **Proteja o e-mail enviado em seu nome por aplicativos, dispositivos, plataformas de SaaS e agentes de IA**
- **Respaldado por Nexus[®] AI, autoaprendizagem, LLMs e análise comportamental**

A maioria das organizações depende do e-mail para fazer negócios.

Porém, atacantes descobriram como sequestrar comunicações empresariais confiáveis e a IA generativa tornou esses ataques mais rápidos, mais convincentes e mais fáceis de escalar.

Eles podem se passar por sua organização, sua marca ou seus parceiros de negócios e criar mensagens e sites convincentes em questão de minutos em vez de horas.

Segundo o Internet Crime Complaint Center do FBI, o comprometimento de e-mail corporativo (BEC) gera consistentemente bilhões de dólares em perdas a cada ano e essas perdas continuam aumentando ano após ano. O FBI também começou a rastrear a IA como um fator de ameaça distinto, atribuindo dezenas de milhões de dólares em perdas por BEC especificamente a ataques com um componente de IA confirmado — e adverte que esse número provavelmente subestima a dimensão real.

Esses ataques geralmente combinam várias táticas de impostura, inclusive domínios falsificados, domínios parecidos e contas comprometidas de fornecedores. Juntas, essas táticas colocam em risco comunicações com parceiros, clientes e fornecedores confiáveis e tornam difícil para os destinatários distinguir as mensagens legítimas das fraudulentas.

A Proofpoint adota uma abordagem holística e multicamada para proteger sua organização e sua marca contra abusos por impostura. Fornecemos as ferramentas, a tecnologia e os recursos necessários para autenticar e-mails gerados por usuários e por aplicativos, proteger as mensagens enviadas em seu nome, identificar contas de fornecedores arriscadas ou potencialmente comprometidas e monitorar domínios parecidos maliciosos para que possam ser removidos.

Proteja sua marca contra impostura

Uma das táticas de impostura mais comuns é a falsificação de domínios, e a IA generativa tornou as mensagens falsificadas mais rápidas de produzir e mais difíceis de distinguir das reais. Na ausência de controles de segurança adequados, os atacantes podem facilmente roubar seus domínios confiáveis e usar IA para criar mensagens altamente convincentes em grande escala. Isso os permite visar seus clientes, parceiros e até mesmo seus funcionários com um nível de rapidez e refinamento que não existia um ano atrás. A autenticação de e-mail é a maneira mais eficaz de evitar isso.

O Proofpoint Impersonation Protection simplifica a implementação do DMARC ao orientar você em cada etapa de sua implantação, além de possibilitar que tanto e-mails de usuários quanto de aplicativos sejam autenticados. Nossos especialistas colaboram para identificar seus remetentes legítimos. Eles também garantem que todos os seus e-mails, inclusive os de remetentes terceiros autorizados, sejam autenticados adequadamente.

A integração com o Proofpoint Threat Protection permite impor, com confiança, a autenticação DMARC em mensagens recebidas. Ela acrescenta uma camada de defesa contra tentativas de impostura geradas por IA que falsificam seus domínios confiáveis. Ela também permite substituir políticas de DMARC sem bloquear e-mails legítimos ou comprometer a segurança com o uso de listas seguras. Essa integração proporciona visibilidade sobre o tráfego de e-mail de entrada e saída. Você pode ver todos os e-mails enviados que usam seus domínios confiáveis, inclusive aqueles enviados por terceiros e, cada vez mais, por agentes de IA agindo em seu nome.

Defenda-se contra contas comprometidas de fornecedores

Os atacantes estão explorando cada vez mais a cadeia de fornecimento para comprometer comunicações empresariais confiáveis. Eles costumam usar contas comprometidas de fornecedores para sequestrar threads de e-mail entre você e seus parceiros de negócios. A IA generativa pode ajudá-los a estudar conversas anteriores e imitar a maneira de escrever de um fornecedor, dificultando a detecção de mensagens fraudulentas. Como esses e-mails podem vir de contas de fornecedores legítimos e não conter cargas maliciosas, os atacantes podem evitar os controles tradicionais de autenticação e detecção. O resultado podem ser perdas financeiras significativas, roubo de dados, extorsão ou ransomware.

O Proofpoint Impersonation Protection ajuda você a detectar e se defender contra fornecedores arriscados, inclusive contas potencialmente comprometidas. Ele usa IA comportamental, autoaprendizagem e inteligência sobre ameaças de toda a grande base de clientes da Proofpoint para revelar sinais de comprometimento de fornecedores, inclusive ataques que usam IA generativa para produzir iscas mais convincentes. Controles adaptáveis, como o isolamento automático de URLs, ajudam a reduzir a exposição a ameaças de remetentes comprometidos. A integração com o Proofpoint Threat Protection, combinada com o contexto das relações entre remetente e destinatário, ajuda a otimizar a resposta a incidentes de terceiros e sua investigação.

Detecte e remova sites maliciosos, inclusive sites parecidos

Malfeitores criam sites projetados especificamente para ataques. Alguns se fazem passar por outras organizações, marcas ou instituições para induzir seus funcionários, clientes ou parceiros a confiarem neles. Outros imitam a sua própria organização, usando domínios e páginas muito parecidos com o seu logotipo, layout e experiência de marca. A IA generativa tornou os dois tipos de ataque mais fáceis de produzir, mais difíceis de detectar e mais rápidos de escalar. Os malfeitores usam esses sites para phishing de credenciais, BEC, ataques de telefonia (Telephone-Oriented Attack Delivery, TOAD) e outros esquemas que dependem de uma presença digital convincente.

Com o Proofpoint Impersonation Protection, monitoramos continuamente domínios recém-

registrados que possam se passar pela sua organização e fornecemos o contexto necessário para avaliar o risco potencial.

A detecção é apenas o primeiro passo. Quando você envia um site suspeito para nossa equipe de remoção, nós o investigamos, coletamos as evidências disponíveis e trabalhamos para mitigar atividades maliciosas e remover o site. Mantemos relacionamentos em uma ampla rede de provedores de infraestrutura de Internet e parceiros confiáveis, inclusive autoridades de registro, provedores de hospedagem, provedores de serviços de e-mail, parceiros de listas de bloqueio e muito mais.

Nossa equipe gerencia o processo de remoção em seu nome, para que você não precise determinar quem contatar ou qual documentação é necessária. Nossos serviços de remoção vão além de domínios parecidos e oferecem suporte para mitigação de subdomínios e URLs maliciosos, bem como de domínios não parecidos.

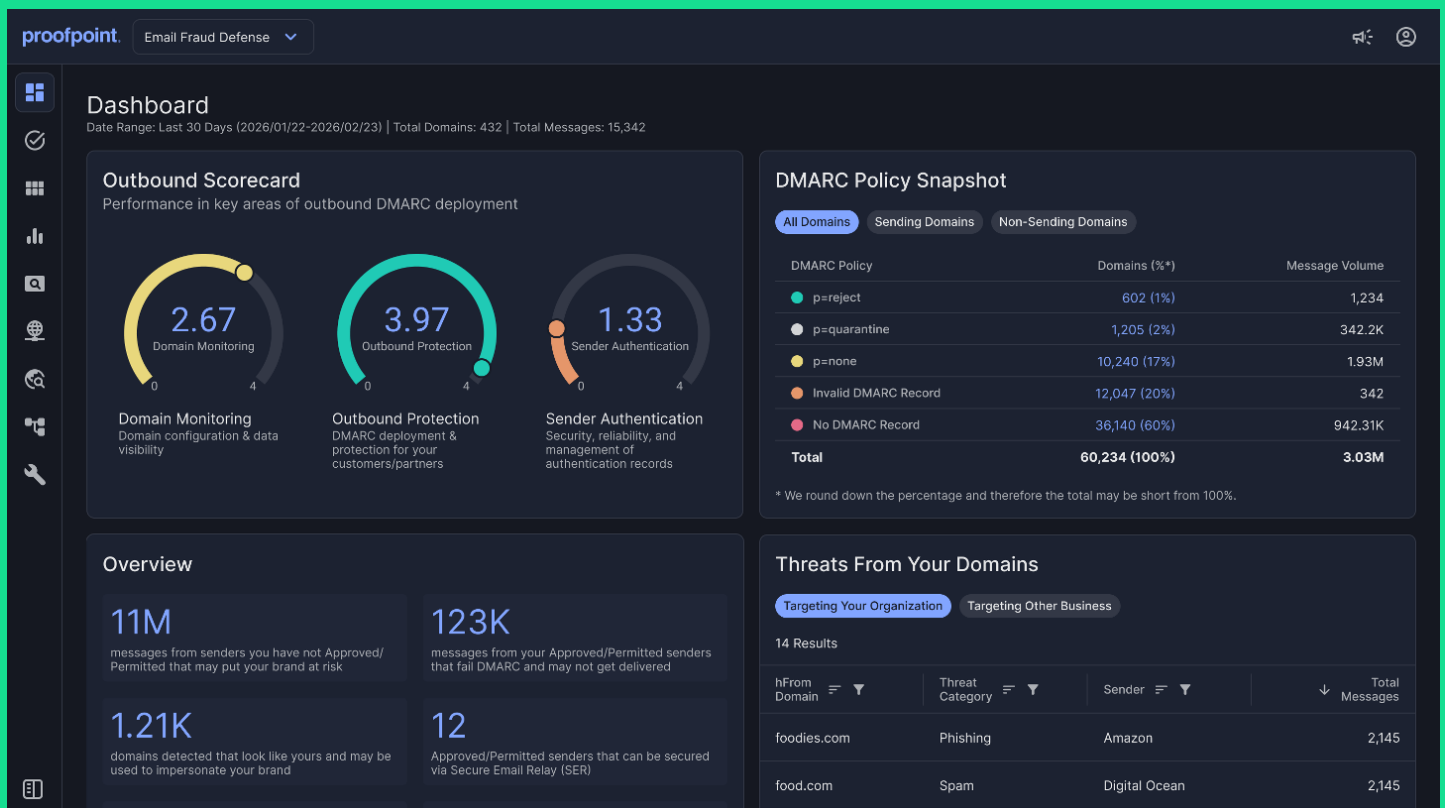


Figura 1. A Proofpoint oferece visibilidade sobre ameaças de falsificação de domínio, domínios parecidos maliciosos com os seus e e-mails enviados usando seus domínios confiáveis.

Proteja o e-mail enviado em seu nome

Nem todos os e-mails que saem do seu domínio vêm de uma pessoa digitando uma mensagem. Plataformas de RH enviam avisos de pagamento, ferramentas de CRM enviam recibos de clientes, dispositivos de escritório enviam notificações de digitalização para e-mail e fax e agentes de IA estão começando a gerar mensagens em seu nome. Cada fonte pode se tornar uma abertura para abusos. Se um aplicativo, dispositivo ou serviço de envio é comprometido, atacantes podem usar esse canal confiável para enviar e-mails maliciosos que parecem vir de você, passam em verificações de autenticação e, quando aprimorados com IA generativa, são mais convincentes do que nunca.

O Proofpoint Impersonation Protection preenche essa lacuna com um retransmissor seguro e dedicado para remetentes automatizados que usam seus domínios, desde aplicativos internos e dispositivos de escritório até plataformas de SaaS e agentes de IA. Ele aceita e-mails somente de fontes verificadas e autenticadas, aplica varreduras avançadas anti-spam e antivírus a cada mensagem e assina com DKIM os e-mails aprovados. Isso ajuda suas fontes externas a manter o alinhamento com DMARC e a conformidade com SPF sem interromper o fluxo legítimo de e-mails. O SER também isola esse tráfego por trás de IPs dedicados e confiáveis, ajudando a proteger sua infraestrutura de envio e a reputação da sua marca contra malfeitores que, de outra forma, poderiam se aproveitar da confiança no seu domínio.

Obtenha visibilidade, controle e suporte de conformidade

O Proofpoint Impersonation Protection oferece visibilidade e controle centralizados sobre serviços de envio de alto volume, como o Amazon SES. Você pode ver o que está saindo em massa do seu domínio e rastrear as mensagens até o aplicativo, dispositivo ou agente de IA que as enviou. Criptografia e prevenção de perda de dados opcionais ajudam a proteger dados confidenciais, inclusive informações de identificação pessoal (PII) e informações protegidas de saúde (PHI), em mensagens transacionais. Esses controles podem apoiar a conformidade com estruturas e regulamentações, como os requisitos da HIPAA, SEC e FINRA.

O Proofpoint Impersonation Protection também ajuda você a se alinhar aos principais requisitos dos provedores de caixa de entrada quanto à identidade do remetente e integridade da mensagem para remetentes em massa. Com suporte para cabeçalhos de cancelamento de assinatura e gerenciamento centralizado de listas, ele ajuda os e-mails legítimos a continuarem chegando à caixa de entrada.

Saiba mais

Para obter mais informações, visite [proofpoint.com/br](https://www.proofpoint.com/br).

Sobre a Proofpoint, Inc. A Proofpoint, Inc. é líder global em cibersegurança centrada em pessoas e agentes, protegendo a forma como pessoas, dados e agentes de IA se conectam por e-mail, nuvem e ferramentas de colaboração. A Proofpoint é uma parceira confiável de mais de 80 empresas da Fortune 100, mais de 10.000 grandes corporações e milhões de organizações menores, ajudando a combater ameaças, prevenir perda de dados e desenvolver resiliência, tanto de pessoas quanto de fluxos de trabalho de IA. A plataforma de segurança de colaboração e de dados da Proofpoint ajuda organizações de todos os tamanhos a proteger e capacitar suas equipes para que possam adotar a IA de forma segura e confiante. Saiba mais em www.proofpoint.com/br

Conecte-se com a Proofpoint: [LinkedIn](#)

Proofpoint é uma marca registrada ou marca comercial da Proofpoint, Inc. nos Estados Unidos e/ou em outros países. Todas as demais marcas comerciais contidas neste documento são propriedade de seus respectivos donos.

