# Proofpoint Email Fraud Defense

## Principais vantagens

- Facilita a implementação de DMARC com orientação em cada etapa da implantação
- Protege a sua marca contra uso em ataques de fraude de e-mail, sem bloquear os e-mails legítimos
- Identifica automaticamente os seus fornecedores e o risco que eles representam
- Mostra todo o e-mail enviado por meio dos seus domínios confiáveis e de similares
- Assegura uma hospedagem confiável de registros SPF, DKIM e DMARC com serviços de autenticação hospedados pela Proofpoint
- Integra-se com o gateway de e-mail da Proofpoint, líder do setor, para ajudar a impor DMARC com confiança e flexibilidade
- Mostra taxas de aprovação de DMARC para domínios pertencentes à empresa e gerenciados no Microsoft 365

Esse conjunto de soluções é parte da plataforma integrada de Human-Centric Security da Proofpoint que atende as quatro áreas principais de riscos baseados em pessoas.


O Proofpoint Email Fraud Defense simplifica a sua implementação de DMARC com fluxos de trabalho orientados e suporte de consultores qualificados. Nosso produto protege a reputação da sua empresa contra ataques de fraude de e-mail. Ele mostra as origens dos e-mails enviados por meio dos seus domínios e de similares. Ele também reduz o risco de fornecedor identificando os seus fornecedores e domínios semelhantes registrados por terceiros.

O Proofpoint Email Fraud Defense orienta você ao longo da implantação do DMARC. Ele ajuda a proteger os seus clientes, parceiros comerciais e funcionários contra fraudes de comprometimento de e-mail corporativo (BEC). Com o Proofpoint Email Fraud Defense, a Proofpoint protege a sua marca contra uso em ataques de fraude de e-mail e reduz o risco de recebimento de ameaças de impostura. Nós autenticamos todos os e-mails entregues à sua organização ou enviados por ela. Tudo isso é feito sem bloquear os e-mails legítimos.

## Facilidade de uso

### Consultores dedicados e orientação especializada

Para ajudar a configurar a autenticação de e-mail, a Proofpoint cria um plano de projeto para você. O plano possui fluxos de trabalho orientados que simplificam o processo de configuração. Nossos consultores ajudam você em cada etapa do plano. Nós trabalhamos com você para identificar todos os seus remetentes confiáveis — inclusive terceiros e TI oculta — e assegurar que eles sejam devidamente autenticados. Nós também analisamos o seu ambiente de e-mail para ajudá-lo a priorizar tarefas com base nas suas necessidades, como volume de e-mail e principais remetentes.

### Serviços hospedados de autenticação

O Proofpoint Email Fraud Defense inclui serviços de SPF hospedado, DKIM hospedado e DMARC hospedado. Esses serviços hospedados ajudam você a configurar e a gerenciar políticas de Sender Policy Framework (SPF), DomainKeys Identified Mail (DKIM) e DMARC. Eles também são serviços distribuídos geograficamente e com tolerância a falhas que asseguram confiabilidade.

#### SPF hospedado

- Ajuda você a superar o limite tradicional de 10 consultas de DNS imposto pelo SPF
- Reduz a sobrecarga da atualização de registros SPF
- Atualiza registros em tempo real com a devida validação de sintaxe
- Melhora a segurança de SPF ocultando a sua infraestrutura de envio
- Facilita o gerenciamento em massa de múltiplos domínios que utilizam a mesma infraestrutura de envio

### DKIM hospedado

- Simplifica a configuração e o gerenciamento de seletores e chaves DKIM
- Oferece opções flexíveis de hospedagem para seletores de DKIM (delegados ou não)
- Oferece suporte para extensões de segurança de DNS (DNSSEC)
- Permite importação simples de chaves públicas e seletores DKIM

### DMARC hospedado

- Simplifica a configuração e o gerenciamento de registros DMARC para os seus domínios
- Compatível com DNSSEC
- Permite importação simples de registros DMARC existentes

## Proteção abrangente de marcas

Para proteger a sua marca, o Proofpoint Email Fraud Defense evita que e-mails fraudulentos sejam enviados por meio dos seus domínios confiáveis.

### Identifique domínios semelhantes aos seus

O Proofpoint Email Fraud Defense utiliza informações de registro de domínio do Proofpoint Domain Discover. Ele detecta domínios recém-registrados que estejam imitando a sua marca em ataques de e-mail ou em sites de phishing. A Proofpoint analisa milhões de domínios e conecta dados de registro com dados próprios sobre atividade de e-mail e ataques. Nós mostramos a você os domínios suspeitos e como os atacantes estão falsificando sua marca. Nós também alertamos quando domínios suspeitos tornam-se ativos.

O add-on Proofpoint Takedown reduz a exposição dos seus clientes, parceiros e funcionários a domínios parecidos com o seu. Você pode solicitar a remoção de um domínio malicioso junto à instituição de registro ou ao provedor de hospedagem, rede de entrega de conteúdo (CDN) ou provedor de e-mail. Você também, pode exportar os domínios a serem bloqueados no gateway de e-mail da Proofpoint.

### Visibilidade de 360 graus sobre o seu ecossistema de e-mail

O Proofpoint Email Fraud Defense mostra todos os e-mails enviados utilizando os seus domínios confiáveis. Isso inclui e-mails enviados para caixas de correio de clientes, gateways comerciais e o seu próprio gateway.

Nosso dashboard mostra qual dos seus domínios os atacantes tentaram sequestrar e a taxa de abuso de cada um. Ele mostra os remetentes autorizados e seus registros DMARC, bem como as suas políticas e taxas de aprovação de SPF, DKIM e DMARC.

O Proofpoint Email Fraud Defense oferece a você recomendações e insights decisivos. Você não precisa se preocupar com descumprimento de DMARC ou bloqueio de e-mails válidos enquanto bloqueia os atacantes.

## Visibilidade sobre riscos de fornecedor

O Proofpoint Email Fraud Defense vai além da implementação de DMARC ao mostrar também os seus riscos de fornecedor. O Nexus Supplier Risk Explorer identifica os seus fornecedores, verifica seus registros DMARC e mostra seus riscos. Nosso produto mostra a você mensagens entregues através de domínios parecidos com os seus. Ao priorizar os alertas com base nos níveis de risco, nós ajudamos você a se concentrar nos incidentes mais críticos.

## Integração com o Proofpoint Email Gateway

O Proofpoint Email Fraud Defense trabalha com o gateway de e-mail da Proofpoint para impor DMARC no tráfego de entrada. Ele ajuda você a verificar a reputação DMARC de um domínio para que o seu gateway não bloqueie e-mails válidos que falhem no DMARC. Ele também ajuda você a criar políticas alternativas para e-mails válidos sem reduzir a sua postura de segurança.

## Visibilidade de DMARC para o Microsoft 365

Mesmo que você utilize o Microsoft 365 com os seus registros de intercâmbio de e-mail (MX) apontados para os servidores de recebimento da Microsoft, o Proofpoint Email Fraud Defense pode mostrar a conformidade dos seus domínios com DMARC. Essa visibilidade ajuda você a impor DMARC sobre o tráfego de entrada de seus domínios com confiança.

## SAIBA MAIS

Para obter mais informações, visite **proofpoint.com/br**.