proofpoint.

Proofpoint Secure Email Relay

Uma solução melhor para controlar e proteger e-mails transacionais de aplicativos e parceiros de SaaS

Principais vantagens

- Protege e-mails transacionais de aplicativos internos, bem como de provedores de serviços SaaS, como Salesforce, ServiceNow e Workday
- Acelera a implementação de DMARC viabilizando a assinatura DKIM de e-mails de todas as origens, antes do envio
- Protege o seu domínio confiável contra abusos que envolvam remetentes comprometidos e provedores de serviços de e-mail vulneráveis cujos IPs estejam nos seus registros SPF
- Protege dados confidenciais em e-mails de aplicativos, como informações de identificação pessoal (PII) e informações pessoais de saúde (PHI), com DLP e encriptação de cargas
- Substitui retransmissores locais por uma alternativa segura baseada em nuvem
- Evita perturbações no e-mail do usuário isolando-o do e-mail do aplicativo

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

O Proofpoint Secure Email Relay (SER) consolida e protege e-mails transacionais. Ele evita que remetentes de terceiros comprometidos enviem e-mails maliciosos utilizando os seus domínios e viabiliza a assinatura DKIM para ajudar você a cumprir com a conformidade DMARC. Como solução hospedada, o Proofpoint SER ajuda você a atingir os seus objetivos de migração para a nuvem.

Os aplicativos estão mudando de sistemas locais para a nuvem. Essa migração pode expandir a superfície de ataque da sua organização. E-mails enviados "por você" podem vir de aplicativos remetentes de terceiros fora do seu controle. Essa configuração deixa as identidades de e-mail vulneráveis a falsificações. Sem controles adequados em vigor, atacantes podem roubar facilmente a identidade da sua empresa. Em seguida, eles podem se aproveitar dos ambientes de nuvem dos remetentes autorizados. Depois disso, eles podem enviar e-mails maliciosos autorizados como se fossem você. Tais mensagens passam por SPF/DKIM/DMARC. Elas podem ser enviadas diretamente para os seus clientes, parceiros e funcionários.

O Proofpoint SER aplica nossos controles de segurança e conformidade aos e-mails transacionais de aplicativos que utilizam a sua identidade. Esses tipos de e-mail originam-se de aplicativos internos ou de parceiros de SaaS de terceiros como Salesforce, ServiceNow e Workday. Isso inclui faturas, códigos de autenticação, confirmações etc. Eles podem estar isolados dos e-mails gerados pelo usuário, mas o Proofpoint SER dá a eles o mesmo nível de proteção.

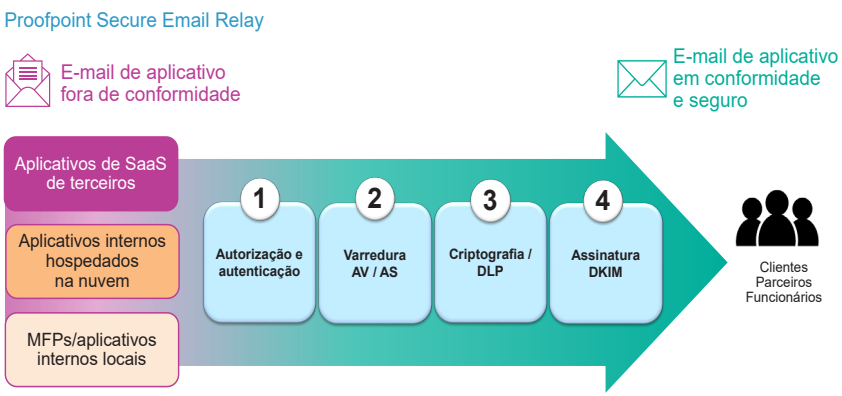

Figura 1. Garanta um e-mail transacional seguro, limpo e em conformidade.

Outros exemplos de e-mails transacionais são:

- Notificações de extratos
- Notificações de entrega de encomendas
- Confirmações de pedidos
- Recibos de vendas eletrônicas
- Cotações de seguros geradas
- Solicitações de opinião ou relatos de experiência
- Notificações de tarefas
- Notificações de alarme de dispositivos ou de IoT
- Gerenciamento de alertas/emergências

O Proofpoint SER facilita o DMARC assinando com DKIM todos os e-mails. Ele avalia os e-mails utilizando tecnologia antispam/antivírus. Ele também reduz o risco para dados confidenciais viabilizando a encriptação de cargas e DLP de e-mail. O Proofpoint SER coloca você no controle da sua identidade de e-mail. Ele assegura que os seus clientes, parceiros e funcionários recebam apenas e-mails autênticos de você.

Proteja o e-mail contra ambientes vulneráveis

E-mails de aplicativo e provedores de serviços de e-mail podem ser autorizados a enviar e-mail utilizando os seus domínios. Frequentemente, porém, eles não seguem as melhores práticas de segurança. Isso pode resultar em comprometimento de contas ou abuso da plataforma. Em ambos os casos, malfeitores podem utilizar os seus domínios confiáveis para enviar e-mails maliciosos que passem pela autenticação de e-mail.

O Proofpoint SER adota um sistema fechado que só permite que entidades corporativas verificadas utilizem o seu serviço de retransmissão de e-mail. Usuários espúrios não podem registrar contas gratuitas em nossa plataforma. Isso reduz em muito o risco representado por provedores de serviços de e-mail vulneráveis ou comprometidos.

O Proofpoint SER também aceita com segurança e-mails dos seus aplicativos autorizados por autenticação SMTP e TLS (STARTTLS). Ele aplica medidas antispam/antivírus da Proofpoint a cada mensagem. O Proofpoint SER bloqueia qualquer e-mail que pretenda enviar e-mails maliciosos autorizados como se fosse você. Você também pode consolidar e-mails de aplicativo por trás de IPs confiáveis e de boa reputação. Estes podem ocultar remetentes de aplicativo que enviam e-mails de malfeitores como se fossem você.

Acelere a implementação de DMARC

Alguns provedores de aplicativos ou SaaS não têm suporte para assinaturas DKIM. Você pode ter DMARC de passagem única baseado apenas no SPF, mas sem DKIM o seu e-mail legítimo não tem a redundância de autenticação necessária. Isso dificulta que ele sobreviva a um encaminhamento, por exemplo. O Proofpoint SER permite que tais e-mails transacionais cumpram plenamente a conformidade DMARC assinando as mensagens com DKIM antes do envio. Isso permite uma implementação mais rápida de políticas de rejeição de DMARC nos seus domínios, para que malfeitores não possam mais falsificá-los.

Cumpra a conformidade regulatória de e-mails de aplicativo

Os aplicativos estão migrando para a nuvem. Com isso, as organizações frequentemente ficam com opções de e-mail aquém do ideal, do ponto de vista da conformidade regulatória. Algumas direcionam o e-mail de aplicativo por sistemas locais. No entanto, isso as expõe a ambientes externos vulneráveis. Algumas agregam soluções isoladas baseadas na nuvem. Porém, estas costumam não oferecer uma visão consolidada das atividades.

O Proofpoint SER permite que você cumpra padrões de conformidade regulatória com o seu e-mail de aplicativo. E-mails de aplicativos com acesso a informações de identificação pessoal (PII) e informações pessoais de saúde (PHI) podem ser encriptados no transporte e na carga. O SER também permite que você aplique soluções de prevenção de perda de dados (DLP) e arquivamento ao seu e-mail de aplicativo, para que ele cumpra regulamentos SEC/FINRA.

A Proofpoint oferece serviços opcionais de suporte ao proprietário do aplicativo, planejamento e execução de migração e entregabilidade pós-implementação para o Proofpoint Secure Email Relay.

SAIBA MAIS

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

0102-012-07-05 5/24

proofpoint.