Proofpoint Advanced Email Security

Proteja-se contra ameaças de e-mail avançadas, simplifique operações e tenha uma visibilidade decisiva sobre o risco das pessoas e o seu cenário de ameaças

Produtos

- Proofpoint Email Protection
- Proofpoint TAP
- Proofpoint TRAP
- Proofpoint Email Isolation
- Proofpoint Browser Isolation
- Proofpoint Security Awareness Training
- Proofpoint Email Fraud Defense
- Proofpoint Internal Mail Defense
- Proofpoint Email Encryption
- Proofpoint Email DLP

Principais vantagens

- Bloqueie ameaças que contêm ransomware, anexos e URLs maliciosos ou que tentam praticar fraudes de e-mail
- Remedeie automaticamente mensagens enviadas por usuários ou ativadas após a entrega com fluxos de trabalho integrados
- Tenha uma visibilidade inigualável sobre o seu pessoal, sobre ameaças e outros insights, como riscos associados a fornecedores ou à nuvem
- Distribua facilmente políticas DMARC e imponha autenticação com rapidez e segurança para bloquear e-mails fraudulentos que falsificam domínios confiáveis
- Instrua e capacite os seus usuários para fazer deles uma forte linha de defesa contra ameaças à segurança cibernética

O e-mail é um recurso fundamental para empresas modernas. Ele também é o vetor de ameaças nº 1. Além disso, os ataques via e-mail — de ataques de phishing a comprometimento de e-mail corporativo (BEC), ataques a cadeias de fornecimento, ransomware e comprometimento de contas de nuvem — estão sempre evoluindo. Por isso, proteger efetivamente esse vetor contra ameaças provou ser um desafio, até mesmo para as maiores e mais complexas organizações. A Proofpoint pode ajudar.

Mais organizações da Fortune 100, da Fortune 1000 e da Global 2000 confiam na Proofpoint para lidar com essas ameaças do que em qualquer outro provedor de segurança de e-mail avançada. Nossa solução adota uma abordagem de API e em linha para enfrentar o desafio. Isso assegura proteção total para todas as mensagens recebidas e enviadas. Ela não se concentra apenas nos e-mails que as soluções de segurança tradicionais deixam passar. A abordagem integrada e em camadas reduz o risco de ataques bem-sucedidos detectando as ameaças com precisão e mais rapidamente. Com um conjunto avançado de detecção e uma plataforma expansível, você pode melhorar a eficiência operacional. Com insights decisivos, você pode compreender melhor os riscos enfrentados. Você também pode executar ações proativas e responder com mais rapidez e eficácia.

Detecte e bloqueie ameaças avançadas

Obtenha uma eficácia na qual você pode confiar

Com a inteligência contra ameaças e a detecção da Proofpoint, você terá uma defesa sólida contra ameaças sofisticadas enquanto minimiza falsos positivos.

Nós utilizamos reputação, recriação de URLs e análise em área restrita (sandbox) tanto preditiva quanto no momento do clique, para detectar ameaças com cargas virais, como as que chegam através de anexos e URLs. Detecção em caso de evasão e ocultação, como CAPTCHA, proteção por senha, sites com renderização lenta, redirecionadores e sites de compartilhamento de arquivos estão incluídos.

Também utilizamos modelos de inteligência artificial (AI) e autoaprendizagem (ML) do Nexus Threat Graph para detectar ataques sem carga viral, como BEC. Os modelos de AI/ML contam indícios, como risco de fornecedor, indícios de usuários em pacotes de colaboração, processamento de linguagem natural no conteúdo, relacionamentos com destinatários e intenções. Dados contextuais e de referência permitem-nos identificar rapidamente os e-mails que podem ser maliciosos.

Figura 1. Nexus Threat Graph.

No atual cenário de ameaças centradas em pessoas, os seus usuários são o seu maior ativo — e também o seu maior risco.

E eles funcionam perfeitamente com nossa inteligência contra ameaças e outros mecanismos de detecção direcionada. Isso minimiza falsos positivos.

Nós examinamos o e-mail com nossa análise multicamada de conteúdo, de reputação e de área restrita (sandbox). Isso detém efetivamente as ameaças avançadas de e-mail, inclusive ransomware e malware polimórfico, antes que os usuários sejam atingidos. Nós oferecemos análises em área restrita (sandbox) preditivas e no momento do clique para detectar e bloquear URLs maliciosos. A recriação de URLs protege os seus usuários em qualquer rede e dispositivo. Isso também ajuda a determinar se uma mensagem foi utilizada como arma após a entrega.

Clique seguramente com o isolamento de e-mail e de navegador

O Proofpoint Email Isolation e o Proofpoint Browser Isolation proporcionam um ambiente seguro para os seus usuários acessarem sites, webmail pessoal e e-mail corporativo com segurança. Os atacantes tentam várias táticas e vetores de ameaça para obter acesso aos seus sistemas, como ao comprometer contas de fornecedores. Eles podem, por exemplo, visar os seus usuários através de e-mail pessoal ou canais desprotegidos. Com o isolamento, você pode desativar uploads e downloads. Você também pode restringir a entrada de dados enquanto um site é analisado em tempo real. Isso não leva mais que alguns segundos. A tecnologia acrescenta uma camada extra para evitar roubo de credenciais, malware e ransomware. Isso é particularmente útil contra e-mails de phishing que contêm URLs envenenados após a entrega.

Evite fraudes com autenticação de e-mail

A autenticação de e-mail acrescenta uma camada adicional de proteção. Ela é, comprovadamente, uma maneira eficaz de deter ameaças de impostura sem malware, como o BEC. Porém, as organizações hesitam em adotar e impor padrões DMARC devido ao risco de bloquear e-mails legítimos.

A Proofpoint ajuda você a distribuir e impor DMARC com confiança, sem bloquear o fluxo de mensagens legítimas. Ela protege contra domínios falsos e e-mails fraudulentos que utilizam os seus domínios confiáveis. Ela detém os e-mails fraudulentos no gateway da Proofpoint enquanto protege a identidade de e-mail da sua empresa. Além disso, você pode ver todas as ameaças de impostura, inclusive domínios maliciosos parecidos com o seu, em um painel unificado. Você tem essa visibilidade independentemente da tática utilizada ou da pessoa visada. Com nosso serviço Virtual Takedown, você pode evitar proativamente ataques de e-mail com domínios fraudulentos parecidos com o seu antes que eles o atinjam.

Nós simplificamos a sua jornada pelo DMARC com um consultor experiente que o orienta em cada etapa da sua distribuição. Nós trabalhamos com você para identificar todos os seus remetentes confiáveis, inclusive de terceiros, para assegurar que eles sejam devidamente autenticados. A Proofpoint já ajudou mais de um terço das empresas da Fortune 1000 nesse processo. Podemos trabalhar com as configurações mais sofisticadas.

Proteja e-mails internos e contenha ameaças rapidamente

A proteção dos e-mails internos é tão importante quanto a proteção dos e-mails recebidos. Os atacantes utilizam contas comprometidas para enviar phishing, BEC ou malware. Nós examinamos os e-mails internos quanto à presença de conteúdo malicioso na forma de URLs e anexos. Quando detectamos um e-mail interno malicioso, é possível removê-lo e colocá-lo em quarentena automaticamente. Você pode fazer isso mesmo que outros usuários já tenham recebido o e-mail e encaminhado para outras pessoas. Também fornecemos relatórios que mostram quaisquer contas que possam ter sido comprometidas. Isso permite que você tome providências rapidamente em relação a essas contas.

Obtenha visibilidade sobre os ataques e a sua superfície de ataque humana

Para mitigar e comunicar melhor o risco para a gerência e a diretoria, você precisa saber:

- Quais usuários estão sob maior risco e como eles estão sendo visados
- Insights, objetivos, perpetradores e tendências do cenário de ameaças
- Outros indícios, como insights de risco de nuvem e de fornecedor

A Proofpoint oferece tudo isso e mais. Com nossa abordagem de plataforma, você tem uma compreensão completa do risco centrado em pessoas, sem compartimentação de dados. Nós capacitamos você a ser mais proativo contra ameaças sofisticadas.

Enfrente o risco com insights centrados em pessoas

No atual cenário de ameaças centradas em pessoas, os seus usuários são o seu maior ativo. Eles também são o seu maior risco. Nós oferecemos a você uma visibilidade incomparável sobre ataques direcionados e sua superfície de ataque humana.

Nós mostramos quem constitui o maior risco para a sua organização e por que. Nosso relatório Very Attacked People™ (VAP ou “pessoas muito atacadas”) indica quais dos seus usuários estão sendo mais visados. Nosso relatório Top Clickers mostra quais dos seus usuários clicaram em mensagens maliciosas reais. Você pode inserir e rastrear VIPs no dashboard. Munido desses insights, você pode implementar controles adaptáveis para os seus usuários arriscados para priorizar e mitigar o risco. Esses controles podem incluir treinamento direcionado de conscientização quanto à segurança, isolamento de navegador e autenticação por múltiplos fatores.

Receba insights centrados em ameaças como contexto

Nós oferecemos informações forenses detalhadas em tempo real sobre ameaças e campanhas. Nossa análise profunda de ameaças mostra tudo: quem foi atacado, a origem do ataque e como foi o ataque. Nós também determinamos o objetivo do ataque. (Podemos saber, por exemplo, se ele procurava vazar dados, instalar ransomware, praticar fraude etc.) Nós fazemos correlações entre ataques de e-mail e logins suspeitos. Isso ajuda você a revelar e a evitar o comprometimento de contas mais efetivamente. A plataforma oferece análises comparativas abrangentes dos tipos de ameaças e objetivos recebidos em relação a outras empresas da mesma área de atuação.

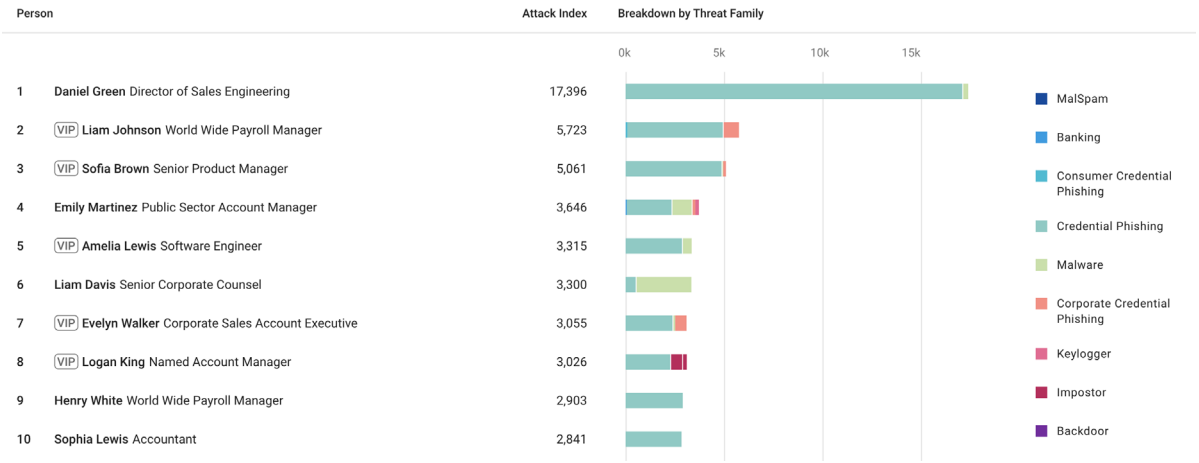

Figura 2. O relatório de pessoas muito atacadas (VAP) da Proofpoint mostra os usuários e os tipos de ameaça de maior risco.

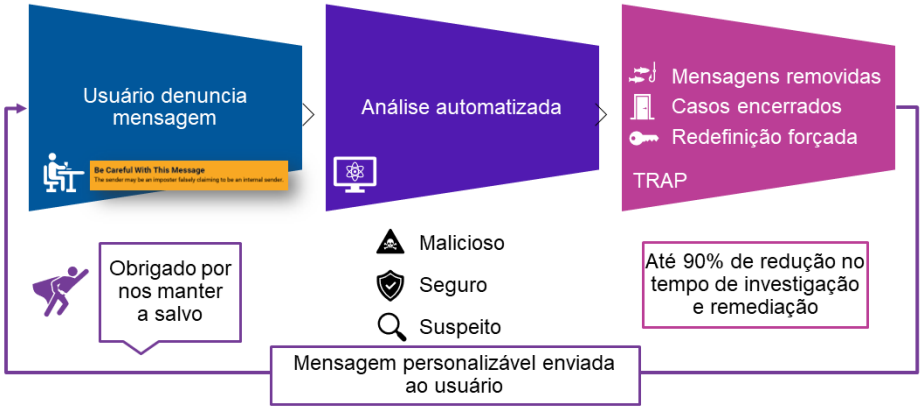

Figura 3. Closed-Loop Email Analysis and Response (CLEAR), solução de caixa de correio para denúncia automatizada de abuso da Proofpoint.

Integre insights sobre risco de comprometimento de nuvem e de fornecedor

Nós oferecemos visibilidade sobre risco de fornecedor e de comprometimento. A visibilidade sobre esses vetores de ataque permite que você resolva completamente ataques complexos. Com o Nexus Supplier Risk Explorer, nós identificamos automaticamente fornecedores potencialmente comprometidos, bem como os domínios que eles utilizam para enviar e-mail para os seus usuários. Além disso, com nosso recurso de defesa de SaaS incluso, você pode obter insights sobre usuários potencialmente comprometidos, arquivos maliciosos ou expostos e aplicativos arriscados de terceiros.

Aumente a eficácia operacional

As equipes de segurança de muitas organizações estão sobrecarregadas ou com falta de pessoal. Essas equipes frequentemente precisam gerenciar múltiplos produtos e fornecedores de segurança que nem sempre se comunicam entre si. Nós oferecemos uma solução integrada que se concentra nas ameaças mais importantes e que automatiza a detecção e a remediação de ameaças. Isso poupa tempo e dinheiro, possibilitando às equipes de segurança despender menos recursos internos na remediação do que se estivessem utilizando soluções de concorrentes.

Remova os e-mails maliciosos automaticamente

Nós eliminamos o trabalho manual e a adivinhação da resposta a incidentes. Isso ajuda você a resolver ameaças com mais rapidez e eficiência. Nós removemos e-mails de phishing que contêm URLs envenenados após a entrega. E podemos remover — com um clique ou automaticamente — quaisquer e-mails indesejados de contas internas que estejam comprometidas, mesmo que esses e-mails tenham sido encaminhados ou recebidos por outros usuários. Além disso, nosso Nexus Threat Graph oferece alertas e coleta e compara automaticamente dados forenses. Isso proporciona uma visão decisiva das ameaças. Com essa abordagem, você pode reduzir o tempo despendido na remediação de e-mail em até 90%.

Simplifique o processo de caixa de correio para denúncia de abuso

Nós ajudamos você a simplificar o processo de caixa de correio para denúncia de abuso e reduzimos a sua sobrecarga de TI. Os usuários podem denunciar mensagens suspeitas facilmente com apenas um clique. Eles podem fazer isso diretamente de uma tag de advertência de e-mail ou utilizando o complemento de denúncia de e-mail PhishAlarm®. Se for constatado que a mensagem denunciada é maliciosa, ela e todas as demais cópias poderão ser colocadas em quarentena automaticamente. Os seus usuários também receberão um e-mail personalizado informando que a mensagem era maliciosa. Isso ajuda a incentivar denúncias futuras de mensagens semelhantes. Os administradores podem obter relatórios detalhados sobre os comportamentos dos usuários e a precisão das denúncias de mensagens maliciosas em comparação com empresas da mesma área de atuação.

Mude comportamentos com educação orientada por ameaças

As ameaças de e-mail modernas frequentemente exigem que seres humanos as ativem. Porém, os seus funcionários não precisam ser o elo mais fraco da sua defesa de segurança cibernética. Na verdade, funcionários conscientes quanto à segurança podem ser uma forte linha de defesa contra ataques cibernéticos.

A Proofpoint permite que você tome providências em relação às suas VAPs ou às pessoas que mais clicam. Os dados coletados sobre elas são integrados automaticamente em nossa plataforma de conscientização quanto à segurança. A plataforma utiliza esses dados para executar um programa de edução mais direcionado e impactante. Ela permite utilizar simulações de phishing do mundo real com base na inteligência contra ameaças da Proofpoint para criar experiências educativas oportunas e relevantes. Os usuários que se deixarem enganar na simulação recebem orientação imediata. Em seguida, eles podem ser inscritos automaticamente em treinamentos específicos. Nós também oferecemos aos usuários tags de advertência de e-mail com capacidades de denúncia de e-mails suspeitos. Essas tags oferecem indicações visuais e breves descrições personalizáveis do risco associado a um determinado e-mail e permitem que os usuários denunciem mensagens diretamente da tag. Isso ajuda os usuários a tomar decisões mais informadas. Esses recursos funcionam perfeitamente em todos os dispositivos e aplicativos.

Proteja-se contra perda de dados por e-mail

O e-mail é o vetor de ameaças n° 1, tanto de ameaças recebidas quanto de perda de dados por vazamento. Portanto, você precisa proteger seus dados confidenciais e evitar a perda de dados por e-mail. Visibilidade e imposição já estão inclusas para evitar perda de dados intencional ou acidental durante a comunicação por e-mail. A prevenção de perda de dados (DLP) por e-mail e a criptografia estão intimamente integradas. Elas podem ser gerenciadas de maneira centralizada na plataforma Information and Cloud Security. Com o novo gerenciador de alertas unificado, você pode personalizar explorações de dados predefinidas para procurar e gerar relatórios sobre as violações de DLP mais importantes. Simplifique operações com capacidades de remediação e fluxos de trabalho otimizados. Nós analisamos informações confidenciais contidas em dados tanto estruturados quanto não estruturados. Nós oferecemos políticas minuciosamente ajustadas e dicionários predefinidos. Estes identificam automaticamente dados protegidos por leis de conformidade regulatória e de privacidade de dados. Eles ajudam você a cumprir leis de proteção de dados de uma variedade de setores — inclusive PCI DSS, SOX, HIPAA, GDPR e mais — além de reduzir o seu trabalho manual. Quando combinados com criptografia, eles permitem definir e personalizar políticas exclusivas para criptografar automaticamente dados sigilosos no e-mail. Isso facilita o gerenciamento e a proteção dos dados confidenciais transmitidos.

Resumo

O Proofpoint Advanced Email Security protege efetivamente contra ameaças que visam o e-mail. Ele oferece visibilidade decisiva sobre os ataques e as pessoas mais atacadas. Nossa solução:

- Bloqueia ameaças avançadas antes que elas sejam entregues
- Proporciona visibilidade inigualável sobre o seu risco de pessoal, ameaças e outros insights
- Aumenta a eficácia operacional com resposta a ameaças automatizada e eficiente
- Instrui e capacita os usuários a se tornarem uma linha de defesa forte
- Protege contra perda de dados por e-mail

SAIBA MAIS

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

SOBRE A PROOFPOINT

A Proofpoint, Inc. é uma empresa líder em cibersegurança que protege as organizações em seus maiores riscos e seus ativos mais valiosos: sua equipe. Com um pacote integrado de soluções baseadas em nuvem, a Proofpoint ajuda empresas do mundo todo a deter ameaças direcionadas, proteger seus dados e tornar seus usuários mais resilientes contra ataques cibernéticos. Organizações líderes de todos os portes, incluindo 75% das empresas da Fortune 100, contam com a Proofpoint para obter soluções de segurança e conformidade centradas nas pessoas e que minimizem seus riscos mais críticos em e-mail, nuvem, redes sociais e Web. Mais informações estão disponíveis em **www.proofpoint.com**.

proofpoint.