proofpoint.

GUIA DE PLANEJAMENTO

Migração de um gateway de e-mail legado para Proofpoint

Os gateways de e-mail seguros (SEGs) legados foram criados para impedir spam e malware conhecido. No entanto, os atacantes de hoje usam ameaças sofisticadas e técnicas multivetoriais, como comprometimento de e-mail corporativo (BEC), sequestro de contas (ATO), phishing com códigos QR e evasão de MFA — ameaças com as quais os gateways de e-mail legados não foram projetados para lidar. Portanto, se você está usando um, há um risco maior de sua organização sofrer uma violação de segurança, além de custos operacionais exorbitantes.

Se você deseja mudar para a Proofpoint para obter mais segurança, este guia de planejamento o ajudará a planejar o caminho da migração. Ele foi criado para clientes da Barracuda, Cisco (IronPort), Forcepoint (Websense), Symantec Email Security.cloud (MessageLabs), Trellix (FireEye/McAfee) e Trend Micro.

Estas instruções passo a passo ajudarão você a avaliar a eficácia do seu gateway legado, mensurar seus custos e criar um cronograma para a migração. A Proofpoint oferece opções de implantação flexíveis — SEG, API ou uma abordagem em fases — para que você possa escolher a que melhor se adapta ao seu ambiente. Para simplificar esse processo, a equipe da Proofpoint pode fornecer ferramentas gratuitas — como nossa avaliação rápida de riscos, nosso relatório de lacunas e nossa avaliação de valor empresarial — para quantificar a redução de riscos e o retorno do investimento (ROI).

Passo 1: quantificar a eficácia da sua proteção

Comece pela visibilidade. Avalie o desempenho das suas defesas atuais — e o que está passando despercebido — para estabelecer uma base de comparação clara.

- Analise relatórios de falsos negativos, que podem ser encontrados em registros administrativos e em tíquetes de SIEM/IR. Isso pode ajudar você a entender a escala e o alcance das detecções falhas.
- Documente a porcentagem de e-mails denunciados pelos usuários que foram confirmados como verdadeiros positivos, o que ajudará a quantificar o tempo despendido pelos analistas na resolução de falsos positivos.
- Identifique os incidentes de sequestro de contas que foram detectados por outros sistemas. Como exemplos podemos citar abuso de regras de caixa de correio, viagens ou geolocalizações impossíveis e evasão de MFA.
- Analise tentativas de phishing interno/lateral detectadas por outros sistemas ou denunciadas por usuários.
- Execute uma avaliação rápida de risco da Proofpoint. Isso lhe dará uma visão baseada em dados sobre as ameaças que seu gateway atual ou sua configuração do Microsoft 365 pode estar ignorando.

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

Passo 2: calcular o custo das operações normais

Segurança não se resume apenas ao que você bloqueia — mas ao grau de eficiência com que você opera. Avalie o tempo, o esforço e a fadiga dos analistas associados a triagem manual, falsos positivos e fluxos de trabalho fragmentados para revelar o verdadeiro custo de manter seu gateway legado.

- Documente quantos cliques e minutos/horas são necessários para que seus analistas investiguem um único caso de phishing. (Não é incomum que os analistas precisem de mais de 12 cliques e percam várias horas para resolver cada caso.) Identifique também onde costumam ocorrer atrasos.
- Monitore as horas que os analistas dedicam à triagem da caixa de correio de abuso. Calcule quanto tempo os analistas despendem revisando e-mails denunciados por usuários a cada semana. Descubra também qual é a porcentagem dessas mensagens que se revelam ameaças reais em vez de alarmes falsos.
- Calcule o tempo despendido por sua equipe na preparação de relatórios. Observe quanto tempo sua equipe leva para compilar e formatar as métricas de segurança em relatórios acabados para executivos ou para o conselho diretor. Muitas vezes, isso exige exportação manual de dados e trabalho com planilhas.
- Converse com os analistas de segurança e documente seus pontos de frustração. Quais problemas surgem com mais frequência? Por exemplo, ruído, falsos positivos e excesso de consoles.

Passo 3: escolher seu caminho de migração

Assim como seu ambiente e suas prioridades evoluem, a sua segurança de e-mail também deve evoluir. A Proofpoint oferece uma flexibilidade que fornecedores de modelo único não conseguem proporcionar. Nosso diferencial está em oferecermos três caminhos de migração:

- **Opção 1: complementar com proteção baseada em API.** Essa opção exige pouco esforço e tem alto impacto. Integre o Proofpoint Core Email Protection API com o Microsoft 365 para obter proteção imediata contra ameaças, como BEC, ATO e phishing. Isso também proporciona suporte para organizações que estão migrando de seu gateway de e-mail legado para um modelo Microsoft + Proofpoint, oferecendo proteção contínua durante e após a migração.
- **Opção 2: começar com API e depois passar para SEG.** Isso requer um esforço moderado, mas tem um impacto maior. Comece com o Proofpoint API para obter ganhos operacionais rápidos e redução de riscos. Em seguida, faça a transição para o Proofpoint SEG ao longo do tempo para obter controle de roteamento, atender mudanças em exigências de conformidade ou assegurar defesas avançadas em camadas.
- **Opção 3: substituir completamente o SEG.** Elimine completamente seu gateway de e-mail (SEG) legado e migre seus registros MX para o Proofpoint SEG para obter controle total e proteção completa pré-entrega.

Passo 4: planejar e comandar sua migração

Valide os resultados antes da implementação completa. Um projeto piloto controlado permite testar a solução da Proofpoint em conjunto com seu gateway existente, confirmar detecções mais robustas e respostas mais rápidas, além de gerar confiança respaldada por dados junto à liderança.

- Defina seus critérios de sucesso antecipadamente. O que você espera alcançar? Como exemplos podemos citar detecção de ameaças aprimorada, redução de falsos positivos, remediação mais rápida e prevenção de ATO.
- Observe possíveis melhorias na detecção executando a proteção de e-mail da Proofpoint no modo silencioso.
- Procure pelo seguinte no seu projeto piloto:
  - Resultados claros, lado a lado, mostrando as ameaças que a Proofpoint detectou e que o seu gateway de e-mail legado deixou passar
  - Um resumo fácil de ler das lacunas de cobertura
  - Um relatório de valor comercial que quantifique o tempo economizado pela sua equipe e a redução de riscos para a sua organização em valores monetários.

Passo 5: criar sua cronologia

Planeje uma transição em fases que esteja alinhada com ciclos de renovação, disponibilidade de pessoal e tolerância ao risco. Com o suporte de migração da Proofpoint, você pode modernizar a proteção sem interrupções.

- Crie um plano de 3 fases:
  1. Piloto
  2. Execução paralela
  3. Transição efetiva
- Revise seu cronograma de renovação de licenças e seus ciclos orçamentários. Se necessário, procure oportunidades de rescisão contratual.
- Opere seu sistema antigo paralelamente, como uma rede de segurança, até que a liderança esteja confiante na sua nova implantação.
- Utilize os serviços Premium da Proofpoint para uma experiência de migração de alto nível. Nossas equipes de serviços Advisory e Applied oferecem conhecimento prático para otimizar configurações, acelerar a implementação e assegurar proteção contínua durante sua transição.

Conclusão

Ao escolher a Proofpoint, você não precisa percorrer essa jornada sozinho. Oferecemos roteiros de migração, modelos piloto e histórias reais de sucesso de clientes para orientar seu caminho. Seja para começar com API, migrar gradualmente para SEG ou substituir completamente o seu gateway de e-mail legado, nós ajudamos você a migrar com confiança e a alcançar resultados mensuráveis.

Por que a Proofpoint?

Sobre a Proofpoint

Proteção de pessoas

3,4 T de e-mails examinados por ano

>1,4 T de SMS/MMS examinados por ano

124 M de ataques de comprometimento de e-mail corporativo (BEC) bloqueados por mês

>183 M de simulações de phishing por ano

0,8 T de anexos examinados por ano

21 T de URLs examinados por ano

177 M de ataques telefônicos bloqueados por ano

Adoção pelo mercado

Mais de 2,7 M de clientes

Mais de 150 provedores globais de Internet e operadoras móveis

>80% da F100 protegida pela Proofpoint

57% da F100 usando Proofpoint DLP

>63% da F1000 protegida pela Proofpoint

proofpoint.

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

DESCUBRA A PLATAFORMA DA PROOFPOINT →