proofpoint.

GUIA DE COMPRAS

Como escolher a melhor segurança de e-mail para a sua organização

Capacidades fundamentais

Estas são as principais capacidades que você deve procurar ao avaliar uma solução moderna de segurança de e-mail:

1. Proteção contra a mais ampla variedade de ameaças
2. Detecção e resposta automatizadas
3. Opções de implantação flexíveis
4. Uma experiência de usuário excelente
5. Proteção contra ameaças além do e-mail

Visão geral

O e-mail continua sendo um vetor primário de ameaças cibernéticas. Porém, nos últimos anos, a superfície de ataque expandiu-se para além do e-mail, conforme as pessoas passaram a se comunicar e a colaborar em múltiplos canais digitais. Não surpreende que os criminosos cibernéticos estejam se adaptando para aproveitar essa tendência. De fato, eles estão tendo mais êxito do que nunca ao distribuir uma ampla variedade de ameaças centradas em pessoas em todos os canais digitais.

Em resposta a isso, as organizações estão reunindo, como em uma colcha de retalhos, os melhores produtos individuais disponíveis no mercado para lidar com essas ameaças. Infelizmente, isso cria lacunas em suas defesas e deixa muitos riscos por resolver.

Além disso, gerenciar e integrar diferentes ferramentas de segurança é complicado e caro. Para evitar essas armadilhas, as organizações precisam de uma solução de segurança de e-mail abrangente que possa defender contra ameaças centradas em pessoas, atuais e emergentes, em uma única plataforma.

Neste guia descrevemos as principais capacidades que você deve procurar em uma solução de segurança de e-mail completa. Também exploramos as razões pelas quais essas capacidades são importantes.

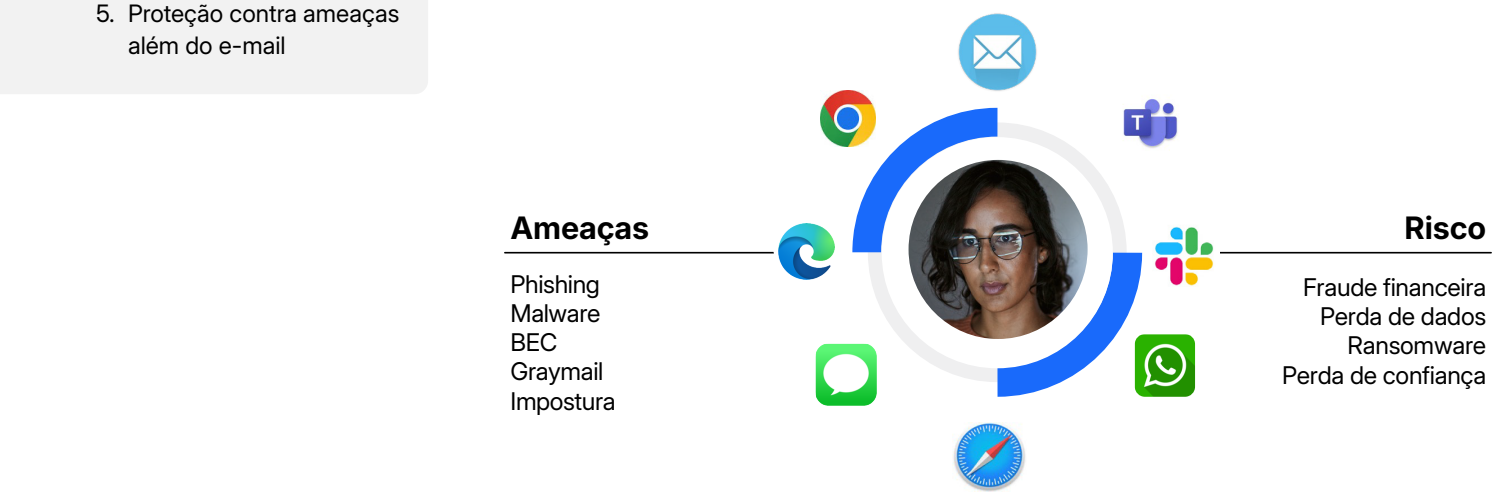
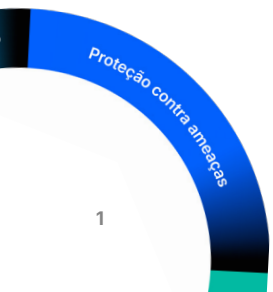


Figura 1. Classificação dos tipos de ameaça entregues por e-mail.



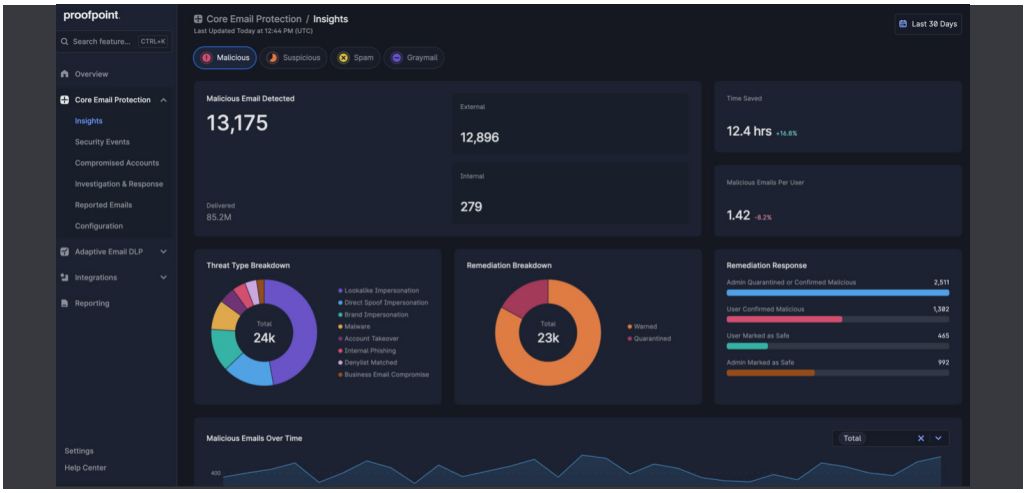


Figura 2. Uma visão abrangente das ameaças transmitidas por e-mail evitadas pelo Proofpoint Core Email Protection.

US$ 55B

Perdas em todo o mundo devido a fraudes de BEC entre 2013 e 2023[2]

60 segundos

Tempo médio que um usuário leva para se deixar enganar por um e-mail de phishing[3]

1. Proteção contra a mais ampla variedade de ameaças

O custo médio de uma violação de dados causada por um ataque de phishing ou comprometimento de e-mail corporativo (BEC, Business Email Compromise) é de R$ 4,88 milhões.[1] É o segundo custo de violação mais alto, atrás apenas do custo de elementos internos maliciosos. Porém, cada ameaça que passa pelas brechas pode ser cara em termos de perdas financeiras e prejuízos à reputação.

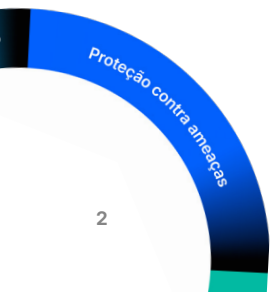
As equipes de segurança querem reduzir, tanto quanto possível, a exposição de suas organizações ao risco. A única maneira de fazer isso efetivamente é bloquear a mais ampla variedade de ameaças.

Veja pelo que procurar em uma solução de segurança de e-mail:

- **Uso de inteligência sobre ameaças em tempo real.** Uma inteligência sobre ameaças atualizada até o último minuto ajuda a identificar ameaças emergentes. Contudo, a inteligência sobre ameaças é mais do que apenas dados. Equipes de pesquisa de ameaças altamente treinadas também precisam estar envolvidas. Quando uma solução dispõe de ambas, é possível analisar tendências em escala global mais rapidamente e com mais eficiência. Isso inclui detecção e rastreamento de criminosos cibernéticos avançados e agentes de governos estrangeiros, bem como identificação de mudanças no cenário de ameaças.
- **Uso de inteligência artificial para detecção de ameaças.** Para deter ataques de e-mail baseados em manipulação com cargas virais maliciosas, é essencial dispor de uma estrutura de detecção multicamada e orientada por inteligência artificial. Procure por grandes modelos de linguagem, gráficos comportamentais e de relacionamentos, autoaprendizagem e pela capacidade de interpretar imagens. Esses recursos ajudarão a assegurar que as ameaças sejam bloqueadas em grande escala.
- **Monitoramento contínuo de ameaças.** A capacidade de analisar URLs e anexos em uma área restrita (sandbox) é importante. Igualmente importante é *quando* analisá-los na área restrita. Para capturar ataques perdidos ou de efeito retardado, procure uma solução que detecte e bloqueie ameaças ao longo de todo o ciclo de vida da ameaça. Isso significa pré-entrega, pós-entrega e no momento em que o usuário clica.
- **Visibilidade sobre os usuários visados.** Você precisa saber quem está sendo atacado, como está sendo atacado e como a pessoa age. É importante saber como a pessoa está sendo visada, a quais dados ela tem acesso e se ela tende a cair nos golpes dos ataques. Com essas informações, você pode viabilizar as medidas de proteção certas, no momento exato.

Quando as ameaças são capturadas precocemente, a sua organização fica mais segura. Além disso, as suas equipes de segurança e de TI não perdem tempo valioso respondendo a incidentes ou remediando-os.

1. IBM. *Cost of a Data Breach Report* (Relatório sobre o custo de uma violação de dados). 2024.
2. FBI. "Business Email Compromise: The $55 Billion Scam" (Comprometimento de e-mail corporativo: a fraude de US$ 55 bilhões). Setembro de 2024.
3. Verizon. *Data Breach Investigations Report* (Relatório de investigações de violações de dados). 2024.



2. Detecção e resposta automatizadas

Mensagens maliciosas entregues em caixas de entrada ou denunciadas por usuários podem sobrecarregar as equipes de segurança e reduzir sua produtividade. Analisar e remover essas ameaças manualmente demanda muito tempo. É essencial detectar e responder às ameaças rapidamente. Isso pode significar a diferença entre um incidente menor e uma violação em grande escala.

Veja pelo que procurar em uma solução de segurança de e-mail:

- **Uma caixa de correio para denúncia de abuso à base de IA.** Mensagens suspeitas denunciadas pelos usuários devem ser processadas o mais rapidamente possível. Quando essas mensagens são direcionadas automaticamente para uma caixa de entrada monitorada por máquina, elas podem ser analisadas por inteligência artificial e condenadas sem serem revisadas pelas suas equipes de segurança ou de TI. Um sistema de resposta automatizada também deve informar aos usuários que suas denúncias foram recebidas. Isso fecha o circuito de feedback e reforça comportamentos positivos.
- **Automatização de coordenação e remediação.** Não se deve permitir que e-mails maliciosos fiquem nas caixas de entrada dos usuários. Eles devem ser removidos automaticamente de todas as caixas de entrada de sua organização. Além disso, certifique-se de que a solução se integre facilmente com as suas ferramentas de SIEM/SOAR existentes. Isso proporcionará a você uma visão mais unificada do seu ecossistema de segurança.
- **Fluxos de trabalho simplificados.** As ferramentas de segurança devem facilitar o trabalho dos analistas. Por exemplo, os analistas podem trabalhar melhor com fluxos de trabalho intuitivos e resumos de ameaças claros gerados por inteligência artificial. Recursos como pesquisa integrada e alertas priorizados podem ajudá-los a caçar ameaças rapidamente. Eles também são beneficiados por ferramentas que aceleram qualquer remediação restante após a automação.

Quando a eficiência da sua equipe de segurança aumenta, as defesas da sua organização ficam mais fortes. Você também aproveita ao máximo os seus recursos e investimentos em segurança atuais.

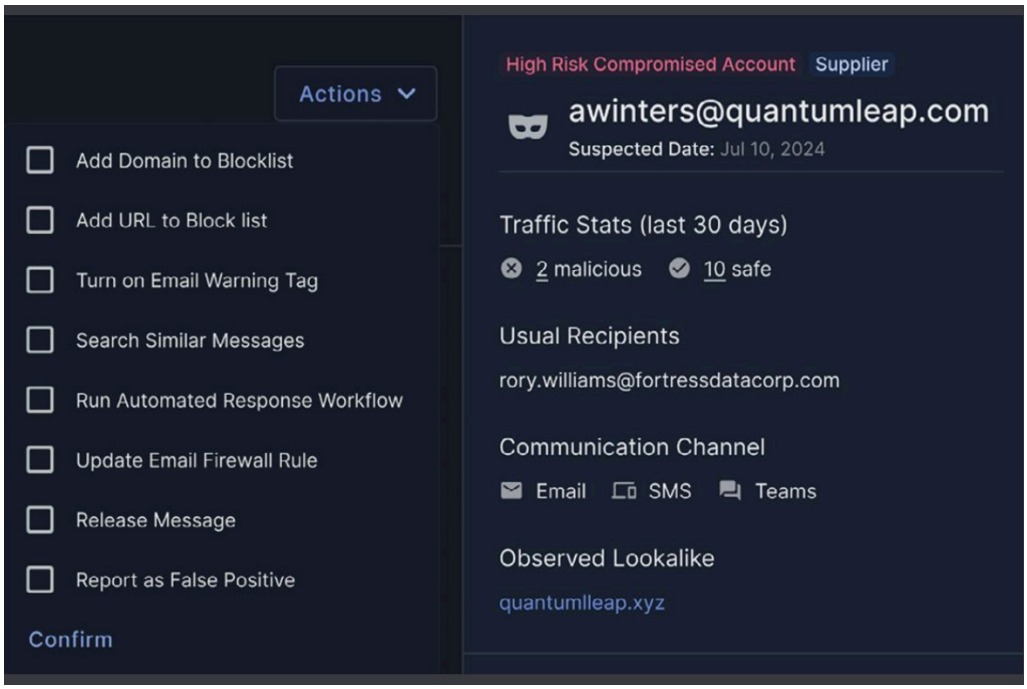


Figura 3. Exemplo de fluxos de trabalho de detecção e resposta automatizados no Proofpoint Core Email Protection.

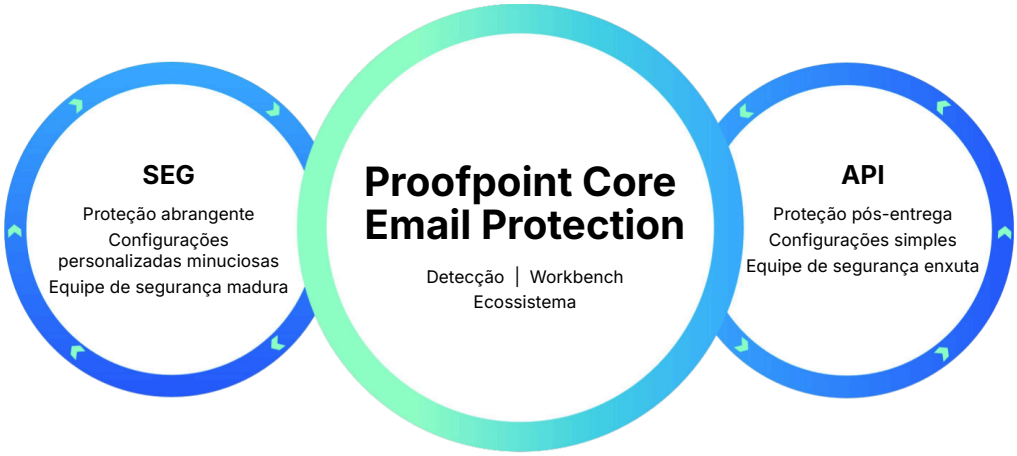


Figura 4. Vantagens da implantação via SEG e API com o Proofpoint Core Email Protection.

3. Opções de implantação flexíveis

A sua arquitetura, as suas prioridades de segurança e os seus requisitos de conformidade estão em constante mudança. Uma solução de segurança de e-mail deve ser capaz de crescer e mudar com você. Mesmo que uma implantação baseada em API seja a melhor abordagem agora, pode deixar de ser conforme a sua empresa evolui e vice-versa. Não ficar preso a uma única abordagem de implantação assegura a possibilidade de otimizar a sua cobertura com base no seu risco.

Em última instância, quando você tem opções, as suas equipes de segurança e de TI podem construir e expandir as suas defesas para um sucesso de longo prazo. E a sua organização pode manter uma proteção robusta enquanto cresce.

Eis o que você deve considerar:

- **Implantação de gateway de e-mail seguro (SEG).** Os SEGs oferecem proteção completa para uma ampla variedade de ambientes. Essa opção é a melhor quando se deseja uma segurança de e-mail altamente personalizável. SEGs permitem maximizar a sua proteção de ponta a ponta com proteção pré e pós-entrega, além de ao clicar. Eles oferecem opções flexíveis de configuração, bem como visibilidade sobre riscos pessoais.
- **Implantação com base em API.** Essa opção proporciona integração fácil e controles predefinidos dentro de plataformas de nuvem, como Microsoft 365. A implantação pode ser concluída em minutos. É a escolha certa se você precisa de uma segurança de e-mail poderosa, mas com pouca interação humana, e se está procurando uma experiência administrativa de configurar uma vez e nunca mais, com insights sobre ameaças de fácil entendimento e capacidades de remediação automatizada.

Ao escolher um fornecedor com opções de implantação versáteis, você obtém a detecção de que precisa. Você também ajuda a garantir que a sua segurança esteja preparada para o futuro.

74%

Percentual de CISOs que acreditam que as pessoas são a maior vulnerabilidade da empresa[4]

40%

A conscientização quanto à segurança pode reduzir os cliques dos funcionários em ameaças do mundo real em mais de 40% em menos de seis meses[5]

4. Uma experiência de usuário excelente

Há um ditado que diz que o seu maior risco e a sua melhor detecção ocupam o mesmo espaço: entre a cadeira e o teclado. Se você quer que as mensagens maliciosas sejam bloqueadas, as pessoas precisam ter as ferramentas certas.

Quando estão sobrecarregadas, as chances de que elas ignorem ameaças reais ou cometam erros são maiores. Spam, graymail ou alarmes falsos constantes aumentam o risco. Os funcionários precisam de avisos claros e decisivos, ferramentas intuitivas para denúncia e simulações de phishing bem elaboradas para reforçar comportamentos positivos de segurança.

Veja pelo que procurar em uma solução de segurança de e-mail:

- **Detecção de spam/graymail.** Spam e mensagens enviadas em massa abarrotam as caixas de entrada e distraem os usuários. Até mesmo graymail, como e-mails de vendas não solicitados, podem prejudicar a produtividade. A segurança de e-mail que mantém as caixas de entrada limpas e organizadas melhora a experiência do usuário e ajuda os funcionários a manter o foco em suas tarefas.
- **Orientação aos usuários sobre mensagens maliciosas.** E-mails suspeitos podem ser maliciosos ou legítimos — apenas o usuário pode dizer. Notificações com visualização contextual informam os usuários sobre os indícios de ameça encontrados nas mensagens. Ao mesmo tempo, anexos ou links de URL maliciosos associados à mensagem suspeita são automaticamente neutralizados, exigindo que o usuário interaja com a notificação antes de interagir com o e-mail em questão.
- **Proteção no momento do clique.** Até mesmo funcionários bem intencionados podem cometer um deslize e clicar em uma ameaça quando estão assoberbados. Proteções no momento do clique, como banners de advertência, ajudam os usuários a parar para pensar antes de interagir. Enquanto isso, janelas de navegação isoladas acrescentam uma camada extra de defesa ao bloquear roubo de credenciais e downloads de malware.
- **Personalização do treinamento para conscientização quanto à segurança.** Frequentemente, simulações de phishing e treinamento para conscientização são as principais maneiras pelas quais os funcionários lidam com ferramentas de segurança de e-mail. As ferramentas mais eficazes oferecem treinamento em tempo real aos usuários quando estes clicam em algum phishing. Elas também oferecem pequenos módulos interativos adequados ao nível de conhecimento de cada usuário. Essa abordagem personalizada aumenta o grau de conscientização e melhora o comportamento a longo prazo.

Uma experiência de usuário harmoniosa pode capacitar os seus funcionários a se manterem conscientes enquanto realizam suas tarefas.

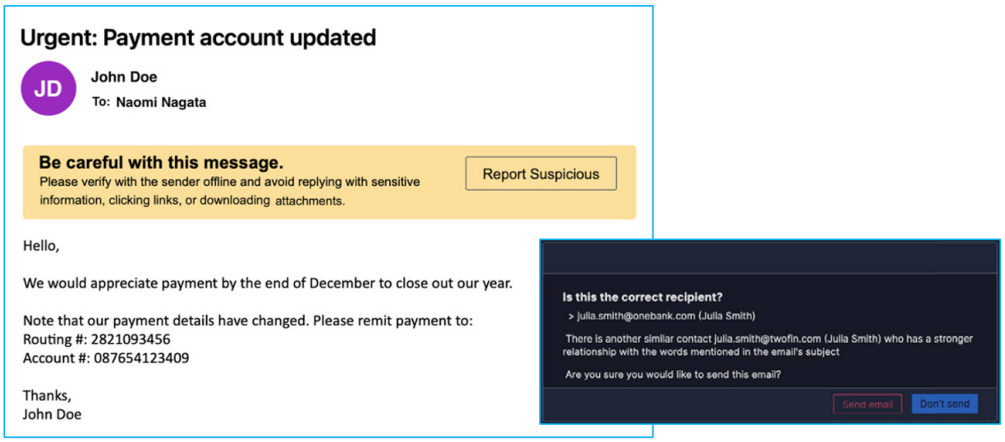


Figura 5. Exemplo de alerta de mensagem entregue indevidamente e um banner de advertência de e-mail.

4. Proofpoint. *Voice of the CISO.* 2024.
5. Pesquisa do Proofpoint ZenGuide.

2.524%

Aumento em ameaças com URL entregues por phishing com base em SMS nos três últimos anos[6]

5. Proteção contra ameaças além do e-mail

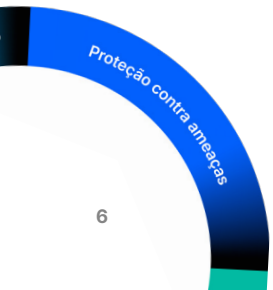
Com a expansão do espaço de trabalho digital, é importante dispor de uma plataforma adaptável. Ela deve ser capaz de proteger não apenas o e-mail, mas também canais de comunicação digital mais recentes. Os criminosos cibernéticos não estão mais limitando seus ataques ao e-mail. Eles seguiram os usuários até plataformas como Microsoft Teams, Slack, Zoom, LinkedIn e WhatsApp, que são novos vetores de ataque.

Para que uma solução esteja preparada para o futuro, ela deve incluir proteções avançadas adicionais, como autenticação de e-mail baseada em DMARC, detecção de contas de nuvem comprometidas com alta fidelidade e visibilidade sobre ameaças de e-mail com base em fornecedores.

Veja o que mais procurar:

- **Autenticação de e-mail simplificada.** Uma das maneiras mais eficazes de bloquear mensagens falsificadas é com autenticação de e-mail, tanto para mensagens recebidas quanto enviadas. Para ajudar a assegurar a proteção da marca, procure um fornecedor que ofereça serviços gerenciados ou de hospedagem para simplificar a implantação da autenticação. A orientação de especialistas pode ser inestimável no que se refere ao DMARC.
- **Detecção de contas comprometidas.** A combinação de visibilidade sobre ameaças de e-mail (como cliques da vida real em mensagens de phishing) com alertas de um intermediador de acesso à nuvem proporciona uma detecção mais precisa de contas comprometidas. Isso reduz os falsos positivos e viabiliza respostas automatizadas, como redefinição obrigatória de senhas ou cancelamento do compartilhamento de arquivos confidenciais.
- **Proteção contra phishing além do e-mail.** URLs maliciosos são atualmente o método de entrega mais comuns dos ataques, em parte porque podem ser enviados para usuários em qualquer lugar, inclusive por meio de aplicativos de mensagens, colaboração e redes sociais. Escolha uma solução que possa inspecionar URLs em tempo real, para que links maliciosos sejam bloqueados em qualquer lugar e sempre que os usuários tentarem acessá-los.
- **Redução do risco de fornecedor.** Sem a visibilidade certa, identificar ameaças na sua cadeia de fornecimento pode ser desafiador. Soluções de segurança de e-mail com capacidades próprias de risco de fornecedor podem atribuir pontuações de risco e detectar contas de fornecedor comprometidas, ajudando a evitar a fraude de e-mail. Quando combinada com autenticação, essa abordagem proativa pode reforçar a proteção contra um dos vetores de ataque mais difíceis de identificar.

Com essas capacidades, as suas equipes podem se manter à frente de ameaças novas e emergentes, não importando de onde estas se originem.



6. Pesquisa da Proofpoint.

Conclusão

Mais de 94% das ameaças que visam os seus funcionários são iniciadas por e-mail.[7] Por isso é essencial ter uma defesa forte para esse vetor primário.

Para maximizar a sua proteção contra ameaças, procure uma solução de segurança de e-mail abrangente que inclua proteções básicas e avançadas. Ela deve detectar e responder às ameaças automaticamente. E deve oferecer uma experiência de usuário excelente. O ideal é uma solução que tenha opções de implantação flexíveis para se adaptar a mudanças futuras. Ela também deve proteger canais digitais além do e-mail, inclusive ferramentas de colaboração, plataformas de mensagens e aplicativos de nuvem.

Você conta com as melhores soluções pontuais fragmentadas? Nesse caso, você tem espaço para melhorar as suas defesas de e-mail. Agora é a hora de avaliar o quanto a sua segurança protege você contra todas as ameaças centradas em pessoas no e-mail e além.

A Proofpoint oferece segurança centrada em pessoas

O Proofpoint Core Email Protection capacita a sua organização a reduzir o risco em todos os lugares onde o seu pessoal interage — hoje e no futuro.

O Proofpoint Core Email Protection bloqueia 99,99% das ameaças de e-mail antes que elas se tornem comprometimentos. Respaldado por nossa estrutura de detecção à base de inteligência artificial e líder do setor, Proofpoint Nexus, ele identifica e corrige ameaças de e-mail avançadas, inclusive phishing, BEC, malware, ransomware, sequestro de contas, impostura, engenharia social e mais. Com um console moderno e intuitivo, os analistas de segurança trabalham eficientemente com visibilidade de ameaças abrangente e fluxos de trabalho de remediação automatizados. A arquitetura de nossa solução está preparada para o cenário de ameaças de amanhã, oferecendo opções flexíveis de implantação com base em SEG e API.

É por isso que mais de 2 milhões de clientes, inclusive 85 empresas da Fortune 100, contam com a Proofpoint para proteger seus funcionários e seus negócios com uma segurança centrada em pessoas.

Para saber mais, entre em contato com nossa equipe de vendas em sales@proofpoint.com.

7. Pesquisa da Proofpoint.

proofpoint.

A Proofpoint, Inc. é uma empresa líder em cibersegurança e conformidade 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 85% 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/br.

Conecte-se com a Proofpoint: LinkedIn

DESCUBRA A PLATAFORMA DA PROOFPOINT →

0203-010-07-02