proofpoint.

RESUMO DA SOLUÇÃO:

Proteção para prestadores de serviços de saúde com a Proofpoint

Proteja pessoas, agentes de IA e dados de pacientes para garantir uma prestação de cuidados segura e resiliente

Visão geral

À medida que a prestação de cuidados se torna mais digital, distribuída e automatizada, os profissionais de saúde enfrentam uma superfície de ataque que está se expandindo em todos os lugares ao mesmo tempo. Por motivo de escassez de mão de obra, a equipe geralmente está ocupada demais para seguir protocolos de segurança. Serviços de nuvem e dispositivos médicos conectados adicionam novos pontos de entrada para ataques. Fluxos de trabalho viabilizados por IA introduzem novas vulnerabilidades.

Os perpetradores de ameaças perceberam toda essa mudança e a estão usando a seu favor. Eles entendem que as violações na área de saúde geralmente começam com pessoas ou com os agentes de IA que atuam em seu nome. Eles estão se concentrando em ataques baseados em identidade, engenharia social e abuso de acesso confiável.

A Proofpoint ajuda hospitais, sistemas desaúde, clínicas e redes integradas de atendimento a proteger seus médicos, funcionários, sistemas e pacientes. Ela protege todo o ecossistema de pessoas, agentes de IA e dados. Nossas soluções integradas de cibersegurança e conformidade reduzem o risco de violações, protegem informações confidenciais e viabilizam uma prestação de cuidados resiliente e ininterrupta.

Alvos de alto valor no setor de saúde

Os prestadores de serviços de saúde estão entre as organizações mais visadas atualmente. Eles não só atuam sob intensa pressão, como gerenciam grandes volumes de dados altamente confidenciais, inclusive:

- Informações de saúde protegidas (PHI), como registros médicos, resultados de diagnósticos e dados de tratamentos
- Informações de identificação pessoal (PII)
- Dados financeiros, de cobrança e de folha de pagamento

Essas informações são altamente valiosas para os atacantes e sua perda pode custar caro. Uma violação pode resultar em penalidades regulatórias, processos judiciais, danos à reputação e prejuízos ao atendimento e à segurança do paciente.

Os profissionais de saúde também enfrentam desafios que são exclusivos da prestação de cuidados:

- Os médicos precisam de acesso rápido e ininterrupto aos sistemas.
- As comunicações geralmente contêm informações confidenciais e urgentes.
- As equipes de atendimento colaboram entre hospitais, clínicas, laboratórios e terceiros.
- Escrutínio jurídico, auditorias e investigações são comuns.

Esse conjunto de soluções faz parte da plataforma integrada Human-Centric Security da Proofpoint, protegendo pessoas e dados no espaço de trabalho agêntico.

Ferramentas de colaboração por e-mail e na nuvem são essenciais para cuidados coordenados. Porém, elas também são os principais pontos de entrada para atacantes cibernéticos.

O *relatório de investigações de violações de dados de 2025* da Verizon constatou que 60% das violações envolveram o elemento humano.

Desafios de cibersegurança dos prestadores de serviços de saúde

À medida que os prestadores de serviços de saúde modernizam suas operações, eles enfrentam vários riscos crescentes.

Proteção de dados de pacientes e dados clínicos

Os prestadores de serviços de saúde devem proteger PHI, PII e dados financeiros. E eles precisam fazer isso em e-mails, plataformas de nuvem e endpoints. Qualquer violação pode desencadear violações de HIPAA e HITECH, penalidades relacionadas a privacidade, problemas de conformidade com PCI DSS e litígios onerosos.

Gerenciamento do risco interno em ambientes clínicos

O risco interno elevado está em toda parte. Não só a rotatividade da força de trabalho é alta, como há mudanças constantes de funcionários, prestadores de serviços e residentes. Há amplo acesso a prontuários eletrônicos de saúde (EHRs). A exposição acidental de dados, o compartilhamento de credenciais e o uso indevido do acesso podem resultar em violações reportáveis.

Prevenção de ameaças de falsificação de identidade e sequestro de contas

Os prestadores de serviços de saúde dependem de um ecossistema complexo de terceiros. Isso pode incluir laboratórios, fornecedores de dispositivos e de suprimentos, seguradoras e agências governamentais. Os atacantes exploram essas relações confiáveis usando comprometimento de e-mail corporativo (BEC), falsificação de identidade de fornecedores e phishing de credenciais. Contas de serviço e caixas de correio compartilhadas são alvos particularmente atraentes.

Resposta rápida a ameaças avançadas

As equipes de segurança enfrentam volumes de alertas avassaladores. Não é fácil acomodar o aumento correspondente em revisões manuais. Isso é especialmente verdadeiro quando os ataques atingem centenas de usuários ou vêm de identidades confiáveis que parecem legítimas.

Preparação para um ambiente de atendimento que prioriza a nuvem

Cada vez mais, os médicos acessam os sistemas remotamente e geralmente usam seus dispositivos pessoais. Não é mais prático rotear todo o tráfego por controles de segurança nas instalações locais. Para ter uma segurança eficaz, as equipes precisam ser capazes de ver quem está acessando dados confidenciais, bem como de que forma e por quê.

Uma abordagem centrada em pessoas e agentes para a segurança na área de saúde

Juntos, seres humanos e agentes agora formam a superfície operacional da prestação de serviços de saúde. Embora os médicos e a equipe iniciem processos de atendimento e administrativos, eles também são auxiliados. Muitas ações agora são executadas por agentes não humanos, inclusive:

- Contas de serviço e caixas de correio compartilhadas
- Identidades de nuvem e APIs
- Fluxos de trabalho de automação e sistemas orientados por IA
- Dispositivos médicos conectados
- Aplicativos clínicos e administrativos, como o Epic

É por isso que os ataques cibernéticos atuais não visam apenas a tecnologia. Eles exploram pessoas confiáveis e agentes confiáveis.

Infelizmente, as ferramentas tradicionais de segurança baseadas em perímetro não conseguem identificar a diferença entre ações legítimas e comportamentos maliciosos. Isso é especialmente verdadeiro quando os atacantes usam identidades comprometidas em vez de malware para suas atividades fraudulentas.

A Proofpoint protege esse ambiente correlacionando identidade, comportamento e acesso aos dados, tanto de pessoas quanto de agentes. Isso elimina os pontos cegos que são alvo de exploração ativa por parte dos atacantes.

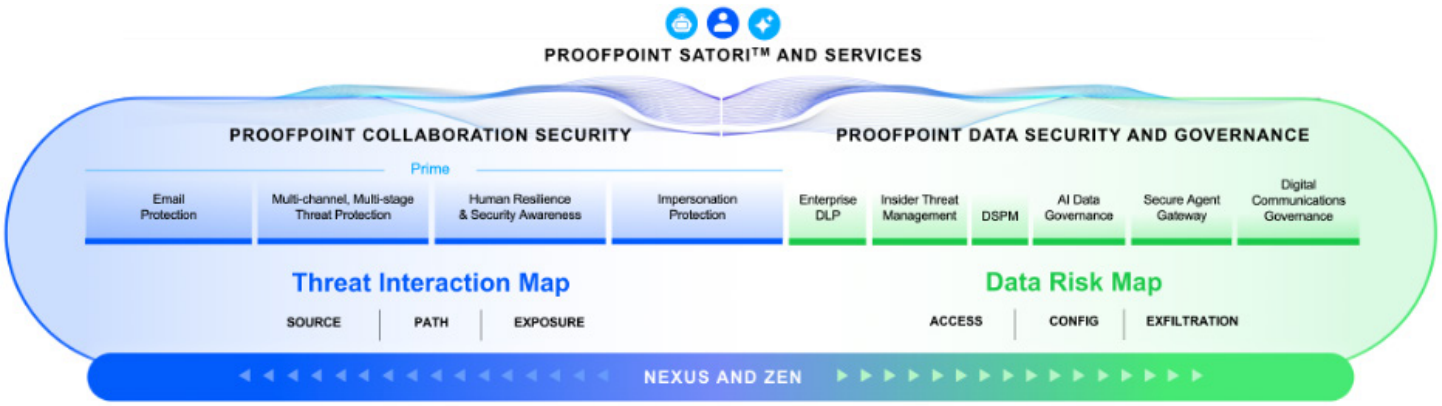


Figura 1. As soluções da Proofpoint protegem todo o ecossistema de pessoas, agentes de IA e dados.

Produtos

- Proofpoint Collaboration Security Prime
- Proofpoint Secure Email Relay
- Proofpoint Data Loss Prevention (DLP)
- Proofpoint Adaptive Email DLP
- Proofpoint Data Security Posture Management (DSPM)
- Proofpoint Satori
- Proofpoint Account Takeover Protection
- Proofpoint Insider Threat Management
- Proofpoint Digital Communications Governance
- Proofpoint ZenGuide

Como a Proofpoint pode ajudar os prestadores de serviços de saúde

Com a confiança de 67% das empresas de saúde da Fortune 500, somente a Proofpoint oferece uma plataforma integrada que protege pessoas, agentes e dados.

Esta seção discute as várias maneiras pelas quais podemos ajudar.

Proteja-se contra ransomware e outras ameaças avançadas

O **Proofpoint Collaboration Security Prime** oferece uma abordagem abrangente para impedir ataques direcionados contra pessoas e agentes por e-mail, ferramentas de colaboração, aplicativos de nuvem, canais da Web e plataformas sociais. Respaldado pelo **Proofpoint Nexus®**, ele usa IA avançada, análise comportamental e inteligência sobre ameaças para bloquear ataques em todo o ciclo de vida da ameaça, desde a pré-entrega até o momento do clique.

Proteja comunicações críticas de e-mail e aplicativos

Os prestadores de serviços de saúde confiam nos e-mails gerados pelo sistema para fluxos de trabalho clínicos e operacionais essenciais, inclusive:

- Lembretes de consultas e notificações aos pacientes
- Coordenação de cuidados e alertas clínicos
- Extratos de cobrança e comunicações financeiras
- Mensagens de conformidade, de relatórios e administrativas. Essas comunicações geralmente são enviadas em grandes volumes por aplicativos confiáveis e devem ser:
  - Entregues de forma confiável
  - Autenticadas pelos destinatários e de confiança
  - Seguras e em conformidade

O **Proofpoint Secure Email Relay** permite que os prestadores de serviços de saúde enviem com segurança grandes volumes de e-mails gerados por aplicativos, protegendo pacientes, parceiros e a organização contra falsificação de identidade e fraude. O Proofpoint Secure Email Relay:

- Permite a entrega de e-mail compatível com DMARC a partir de aplicativos essenciais, como Epic, ServiceNow e outras plataformas clínicas e administrativas
- Protege os e-mails gerados pelo sistema contra falsificação e abuso de domínios parecidos
- Garante confiança e integridade nas comunicações operacionais e voltadas para o paciente
- Reduz o risco de e-mails de aplicativo comprometidos ou mal configurados

Ao proteger remetentes não humanos, o Proofpoint Secure Email Relay amplia o modelo de cibersegurança centrado em agentes da Proofpoint. Ele garante que as comunicações essenciais da área de saúde permaneçam confiáveis, em conformidade e resilientes.

Mantenha protegidos os dados dos pacientes

As soluções **Proofpoint Data Loss Prevention (DLP**) evitam a perda acidental ou maliciosa de dados por e-mail, nuvem e endpoints, oferecendo visibilidade profunda do conteúdo e do comportamento do usuário.

O **Proofpoint Adaptive Email DLP** usa IA comportamental para analisar os padrões normais de envio de e-mail e oferecer avisos contextuais em tempo real para médicos e funcionários. Ele evita exposição de dados e mensagens endereçadas incorretamente sem interromper a prestação de cuidados.

O **Proofpoint Data Security Posture Management (DSPM)** identifica onde os dados confidenciais estão localizados, quais pessoas e agentes podem acessá-los e onde existem permissões excessivas ou arriscadas. Isso permite que os profissionais de saúde reduzam a exposição e adotem com segurança a IA e a automação.

O **Proofpoint Satori™** estende o DSPM com governança de acesso a dados em tempo real para ambientes de saúde. O Proofpoint Satori monitora e controla continuamente o acesso a dados confidenciais do paciente. Ele faz isso em armazenamentos de dados na nuvem, plataformas de análise e pipelines de IA sem interromper fluxos de trabalho clínicos.

Com o Proofpoint Satori, os profissionais de saúde podem:

- Descobrir e classificar dados confidenciais de pacientes e dados clínicos em plataformas de nuvem
- Impor acesso com privilégios mínimos para médicos, funcionários, aplicativos e agentes de IA
- Detectar e corrigir acesso arriscado ou anômalo a dados em tempo real
- Aplicar controles baseados em política para proteger PHI e, ao mesmo tempo, viabilizar análises, pesquisas e inovação em IA.

Detecte comprometimento e uso indevido em grande escala

O **Proofpoint Account Takeover Protection** e o **Proofpoint Insider Threat Management** detectam comportamentos suspeitos, tanto em identidades humanas quanto de agentes. Eles identificam comprometimento de credenciais, abuso de privilégios, movimentação lateral e vazamento de dados. Ao correlacionar identidade, comportamento e movimentação de dados, a solução da Proofpoint viabiliza uma resposta mais rápida e precisa, antes que o atendimento ao paciente seja interrompido.

Mantenha-se em conformidade e pronto para litígios

As soluções **Proofpoint Digital Communications Governance** simplificam a conformidade com HIPAA, HITECH e requisitos de retenção. Elas garantem que comunicações clínicas e administrativas sejam capturadas, possam ser pesquisadas e estejam disponíveis para auditorias, investigações e desco-berta eletrônica.

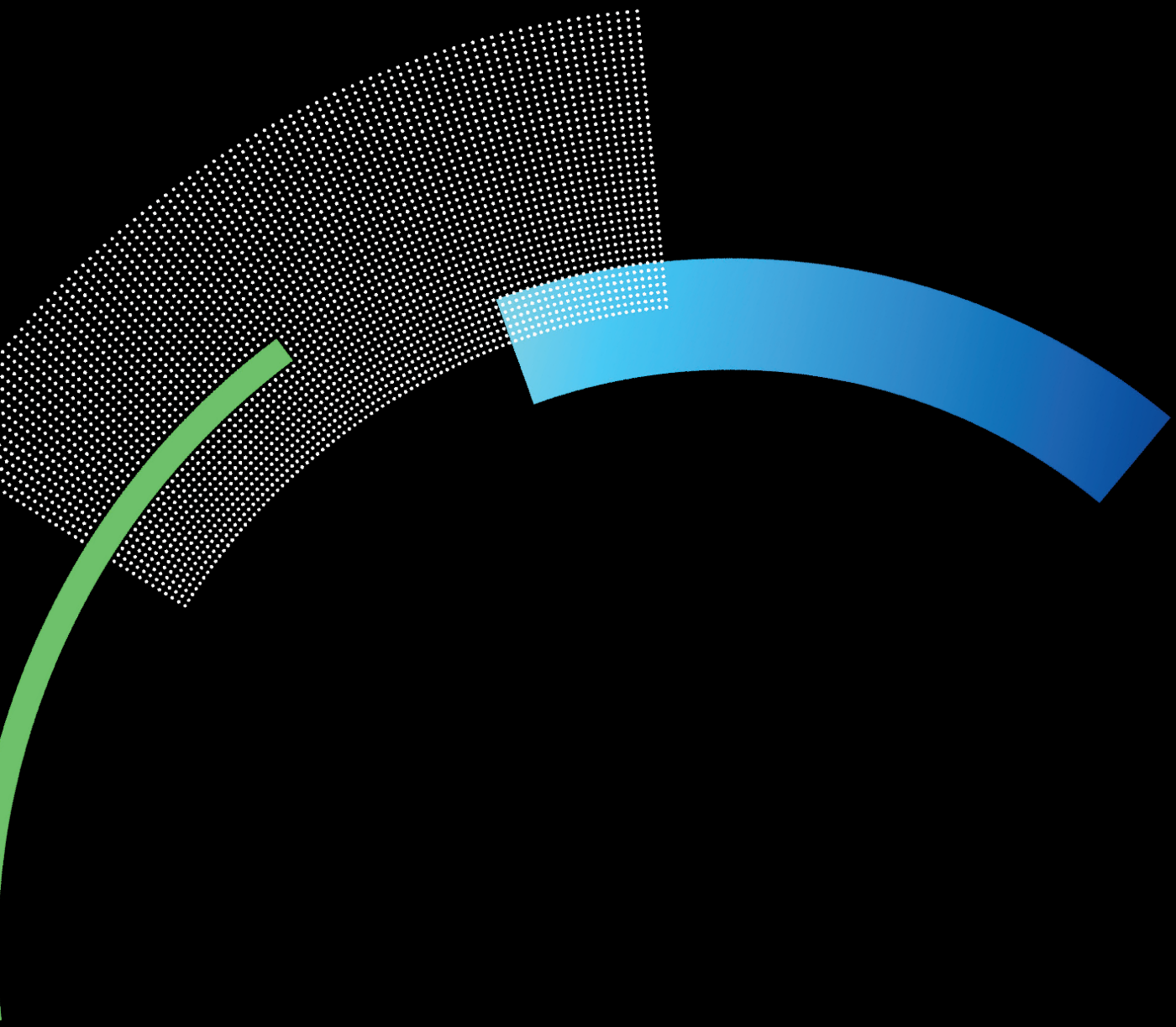
Reduza o risco por meio de mudança comportamental

O **Proofpoint ZenGuide™** oferece treinamento de conscientização de segurança baseado em funções e orientado por riscos, personalizado para médicos e funcionários. Ele reforça comportamentos seguros usando cenários reais de ameaças à assistência de saúde sem atrasar a prestação de cuidados.

Conclusão

A Proofpoint sempre protegeu as pessoas. Agora, nossa plataforma de segurança centrada em pessoas e agentes estende essa proteção a todas as interações entre pessoas, dados e agentes de IA. Ela oferece controle, conformidade e a liberdade de adotar inovações.

Com a Proofpoint, os profissionais de saúde podem reduzir o risco de violações, proteger os dados dos pacientes, manter a conformidade e oferecer cuidados resilientes e ininterruptos em um cenário complexo de ameaças.



proofpoint.

Sobrea Proofpoint, Inc. 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 empresas e milhões de organizações menores, ajudando a combater ameaças, evitar perda de dados e construir resiliência entre pessoas e fluxos de trabalho de IA. A plataforma de segurança de colaboração e dados da Proofpoint ajuda organizações de todos os tamanhos a proteger e capacitar suas equipes enquanto adotam a IA de forma segura e confiante. Saiba mais em www.proofpoint.com.

Conecte-se à Proofpoint: LinkedIn

DESCUBRA A PLATAFORMA DA PROOFPOINT →