proofpoint.

RESUMO DA SOLUÇÃO

Proteção de dados de saúde com a Proofpoint

Proteja dados de pacientes contra ameaças internas, perda de dados e riscos na nuvem

Principais vantagens

- Identifique e mitigue riscos associados a elementos internos negligentes, comprometidos ou maliciosos
- Assegure uma proteção expansível em todos os elementos da superfície de ataque para acomodar o aumento da pegada digital
- Evite perda de dados em e-mail, nuvem e endpoints

10%

de todos os ataques de ransomware nos últimos dois anos atingiram o setor de saúde.

Fonte: SC Media

Há muito que as organizações de saúde são alvos preferenciais de criminosos cibernéticos. Essas organizações manuseiam diversos tipos de dados, como propriedade intelectual (PI), dados de testes clínicos, informações protegidas de saúde (PHI) e dados financeiros pessoais. Os atacantes têm várias opções para faturar com ataques contra cada um desses tipos de dados. Conforme as instituições de saúde adotam a nuvem, o trabalho remoto e o atendimento à distância, elas também aumentam sua superfície exposta a ataques. E como os funcionários do setor atuam sob níveis de estresse cada vez mais elevados, as organizações enfrentam riscos maiores associados a elementos internos, tanto maliciosos quanto bem intencionados.

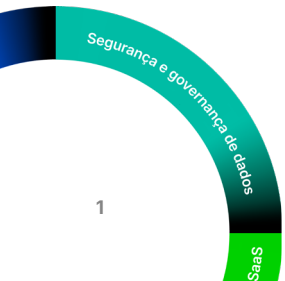
A Proofpoint oferece uma abordagem centrada em pessoas para a proteção de dados confidenciais em redes de atendimento médico distribuídas. Nossas soluções de segurança de dados proporcionam visibilidade e controle de dados confidenciais inigualáveis. Nós ajudamos você a defender o seu pessoal e seus dados confidenciais contra divulgação acidental, ataques maliciosos e risco interno. Nosso escudo protetor estende-se a serviços de nuvem, e-mail, endpoints e compartilhamentos de arquivos no local. A sua organização pode gerenciar melhor o risco aos dados além de também poupar tempo e reduzir custos operacionais.

Uma ameaça crescente

Como muitas empresas, as organizações de saúde armazenam dados de cartões de pagamento e outras informações financeiras. Porém, elas também manuseiam grandes quantidades de dados de pesquisas clínicas e informações protegidas de saúde. Elas armazenam até dados relacionados a subsídios governamentais. Tudo isso as torna um alvo lucrativo para criminosos cibernéticos.

Ao mesmo tempo, as pegadas digitais das instituições de saúde estão se tornando mais complexas. O setor hospeda atualmente uma variedade crescente de serviços na nuvem. Um número cada vez maior de dispositivos salvadores de vidas da Internet das coisas médicas (IoMT) está aumentando sua superfície exposta a ataques. Opções expandidas de atendimento remoto de saúde também fazem com que dados confidenciais trafeguem cada vez mais fora do perímetro de rede. Atualmente, devido a regras de trabalho híbrido, os funcionários não raro trabalham remotamente.

Infelizmente, os atacantes seguiram seus alvos além do perímetro. Nos dois últimos anos, o setor de saúde foi atingido por 10% de todos os ataques de ransomware e os ataques cibernéticos contra o setor de saúde cresceram 32%.[1] Esses percentuais são bem maiores que os de outros setores e segmentos de atividade. As violações de dados também são mais onerosas no setor de saúde do que em qualquer outro setor.



1. Shaun Nichols (*SC Media*). "Cyberattacks targeting medial organizations up 32% in 2024" (Os ataques cibernéticos contra organizações médicas aumentaram 32% em 2024). Fevereiro de 2025.

32%

Os ataques cibernéticos contra o setor de saúde aumentaram 32% nos dois últimos anos.

Fonte: SC Media

US$ 9,77 M

Em 2024, uma violação de dados no setor de saúde custava, em média, US$ 9,77 milhões.

Fonte: Ponemon Institute e IBM

Em 2024, uma violação de dados de saúde custava, em média, US$ 9,77 milhões.[2] Esse custo podia incluir resgates pagos, correções de sistemas, multas por falta de conformidade, litígio e perda de prestígio da marca. Inatividade de sistemas ou integridade de dados comprometida também podem ter resultados negativos na área de saúde. Podem até resultar em perda de vidas.

Desafios de segurança de dados

Para hospitais, clínicas, provedores de planos de saúde e empresas de biotecnologia, a segurança dos dados deve ter prioridade máxima. Essas instituições precisam proteger seus próprios dados de pesquisa e propriedade intelectual. No entanto, elas também precisam proteger informações de saúde dos pacientes (PHI), informações de identificação pessoal (PII) e dados de cartões de pagamento. Elas enfrentam muitos desafios. Esta seção descreve apenas alguns deles.

Evitar espionagem de registros médicos e outras ameaças de elementos internos

As organizações de saúde estão entre os locais de trabalho mais estressantes. Isso significa que há um risco maior de ameaças por parte de elementos internos.

Durante um intervalo de turno, por exemplo, um funcionário curioso pode olhar os registros médicos de um paciente famoso. Isso é o que chamamos de espionagem de registros médicos eletrônicos (EHR). É um risco grave para uma instituição que as informações de um paciente abastado sejam expostas publicamente. Funcionários bem intencionados, mas sobrecarregados, podem abrir e-mails de phishing ou enviar acidentalmente e-mails com dados confidenciais para os destinatários errados. O estresse emocional pode levar a ameaças de elementos internos maliciosos contra um empregador. Se a conta de um usuário confiável for comprometida por roubo de credenciais, as consequências podem ser graves, antes que alguém perceba o que aconteceu. Evitar esses tipos de ameaças requer uma abordagem proativa.

Lidar com os riscos de segurança inerentes à inteligência artificial generativa

As organizações de saúde estão descobrindo uma lista cada vez maior de usos para a inteligência artificial generativa (GenAI). Isso inclui, por exemplo, aumentar a produtividade dos clínicos, melhorar o engajamento entre o paciente e os funcionários e simplificar a eficiência administrativa. Também podemos citar otimização da qualidade do atendimento prestado, bem como expansão além das aplicações clínicas para melhorar as interações com os pacientes em geral. Contudo, a inteligência artificial apresenta riscos. Fora os perigos associados a resultados imprecisos ou tendenciosos, os provedores de serviços de saúde precisam assegurar que os modelos de inteligência artificial não exponham ou utilizem indevidamente informações de saúde dos pacientes. Isso pode ocorrer, por exemplo, quando a inteligência artificial manipula dados não estruturados, como anotações clínicas. Além disso, a integração de GenAI na prática clínica frequentemente esbarra em complexidades regulatórias.

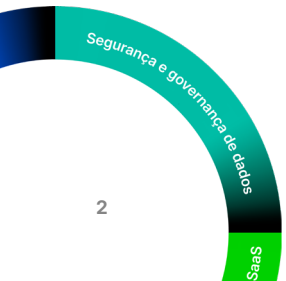
Cobrir uma superfície de ataque crescente conforme o setor de saúdo adota a nuvem

Muitas organizações de saúde demoraram a adotar a nuvem. Agora, porém, praticamente todas têm múltiplos serviços em nuvens públicas, privadas e híbridas. Ao disponibilizar informações aos provedores em tempo real, o atendimento aos pacientes melhorou. Isso ajudou as organizações a simplificar operações e a reduzir a necessidade de custeio de TI. Porém, também expandiu a superfície de ataque.

Mesmo quando os registros médicos são guardados no local, detalhes desses registros costumam ser acessados, compartilhados e armazenados em outros lugares. Por exemplo, em dispositivos móveis, endpoints remotos, dispositivos IoMT e sistemas de e-mail baseados em nuvem. Conforme os dados de saúde transitam por geografias mais amplas, a proteção desses dados torna-se um desafio muito maior.

Uma presença maior na nuvem acarreta um risco maior de roubo de credenciais. Cada vez mais funções de colaboração e de software de escritório são fornecidas por meio de serviços de nuvem, como Microsoft 365 e Google Workspace. Como resultado, criminosos cibernéticos exploram cada vez mais esses serviços.

2. Ponemon Institute e IBM. "Cost of a Data Breach Report 2024" (Relatório sobre o custo de uma violação de dados em 2024).



Produtos

- Proofpoint Adaptive Email DLP
- Proofpoint Enterprise DLP
- Proofpoint Email DLP
- Proofpoint Email Encryption
- Proofpoint Insider Threat Management
- Proofpoint Data Security Posture Management
- Proofpoint Applied Services for Data Security

Unificar a segurança de dados em todos os canais e plataformas

As instituições de saúde de hoje utilizam muitos modos de se comunicar e transferir dados. Estes incluem sistemas de EHR, como o Epic, sistemas de e-mail no local e baseados em nuvem, outros sistemas de mensagens e serviços de compartilhamento de arquivos. As instituições também possuem uma grande malha de endpoints. Estes incluem PCs no ponto de atendimento, centenas de tipos de dispositivos médicos, computadores desktop, laptops e dispositivos móveis. Muitos trabalhadores utilizam vários dispositivos no mesmo dia. Os seus dados confidenciais são armazenados em servidores, tanto no data center quanto na nuvem. Eles trafegam regularmente entre ambos.

Conforme a sua superfície de ataque cresce e a sua infraestrutura fica mais complexa, é ainda mais importante que a sua proteção de segurança seja integrada. No caso da segurança de dados, isso significa ter ferramentas integradas de prevenção de perda de dados (DLP) em endpoints, e-mail e nuvem.

Uma abordagem centrada em pessoas

As abordagens tradicionais de segurança de dados examinam apenas os dados. Porém, as informações não se perdem sozinhas. Pessoas permitem que a perda de dados aconteça. Elas podem fazer isso acidentalmente ou maliciosamente. De uma forma ou de outra, na cibersegurança a visibilidade é fundamental. Você precisa compreender as personalidades com maior probabilidade de trazer risco. Uma abordagem centrada em pessoas atua para compreender a dinâmica dos indivíduos que interagem com os seus dados.

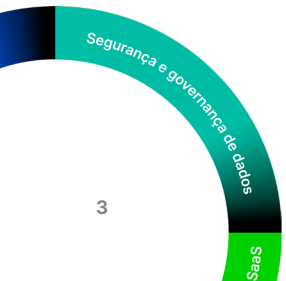
Como a Proofpoint pode ajudar

A solução unificada de segurança de dados centrada em pessoas da Proofpoint oferece a você uma visibilidade inigualável. Com uma interface nativa em nuvem, você pode proteger as suas informações confidenciais concentrando-se nas pessoas que interagem com elas. Nossas soluções levam em consideração o conteúdo, o comportamento e a ameaça. Elas combinam proteção de informações no local com segurança de nuvem. Isso assegura que a sua equipe, os funcionários clínicos e os pacientes sejam protegidos, não importando onde seus dados trafeguem.

Os componentes fundamentais da sua solução unificada de segurança de dados são os seguintes:

Proofpoint Adaptive Email DLP

O Proofpoint Adaptive Email DLP utiliza inteligência artificial comportamental para evitar perda de dados acidental ou intencional por e-mail. Ele analisa mais de 12 meses de dados de e-mail para aprender os comportamentos de envio normais dos funcionários, seus relacionamentos confiáveis e como eles lidam com dados confidenciais de saúde. Com essa análise, o Proofpoint Adaptive Email DLP pode identificar comportamentos anômalos no e-mail quando estes ocorrem. Quando suspeita que um e-mail foi endereçado incorretamente, um arquivo foi anexado indevidamente ou um evento de vazamento de dados está ocorrendo, ele mostra ao usuário uma mensagem de advertência contextual no mesmo instante. Isso permite que o usuário corrija e evite o incidente de perda de dados em tempo real, sem a participação de um administrador.



Proofpoint Enterprise DLP

As soluções de DLP líderes de mercado da Proofpoint promovem uma abordagem adaptável e centrada em pessoas para prevenção de perda de dados. Elas oferecem visibilidade detalhada do conteúdo e do comportamento do usuário, viabilizando uma detecção e prevenção efetiva de riscos significativos de perda de dados. A Proofpoint atualiza estratégias de DLP tradicionais integrando a proteção no e-mail, na nuvem e em endpoints, tanto gerenciados quanto não gerenciados. Nossas soluções de DLP baseiam-se em uma arquitetura nativa de nuvem, com controles de privacidade modernos e um agente altamente estável. Essas se expandem automaticamente e são de fácil implantação e manutenção.

Um console único e unificado ajuda você a gerenciar alertas e a investigar incidentes em todos os canais. Com análises poderosas, você pode avaliar rapidamente o risco para os dados, chegar a vereditos de alta fidelidade e tomar as providências apropriadas.

Proofpoint Email DLP

O Proofpoint Email DLP reduz os seus riscos de perda de dados confidenciais por e-mail e assegura conformidade aplicando criptografia e prevenção com base em políticas. Ele é fácil de distribuir com segurança de e-mail ou como parte de uma abordagem de DLP corporativa unificada. O Proofpoint Email DLP automatiza a conformidade regulatória com políticas predefinidas para PCI, PII, GDPR, SOX, HIPAA e mais. Você também pode utilizar dicionários personalizados — inclusive classificação com inteligência artificial — para identificar e proteger dados específicos da sua organização.

Proofpoint Email Encryption

O Proofpoint Email Encryption protege mensagens e anexos automaticamente e com total transparência. Diferentemente de serviços de e-mail criptografado tradicionais, tudo acontece em segundo plano — os usuários nada precisam fazer manualmente. Com o Proofpoint Email Encryption, você pode proteger mensagens de e-mail confidenciais enquanto assegura que os seus afiliados, parceiros comerciais e usuários têm acesso contínuo a mensagens protegidas em computadores ou dispositivos móveis.

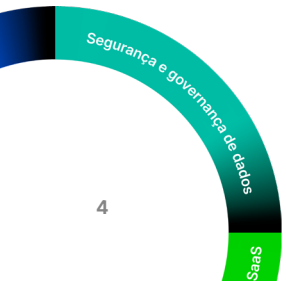
Proofpoint Insider Threat Management

O Proofpoint Insider Threat Management (ITM) correlaciona atividades de usuários com movimentação de dados. Ele permite que as suas equipes de segurança detectem, investiguem e respondam a ameaças internas em potencial com percepção comportamental centrada em pessoas. Além disso, ele oferece detecção e resposta em tempo real a vazamentos de dados, abuso de privilégios, má utilização de aplicativos, acesso não autorizado, ações acidentais arriscadas e comportamentos anômalos. Isso ajuda você a detectar, evitar e responder a ameaças, como espionagem de registros médicos, dentro de visualizações e análises cronológicas.

Quando uma ameaça interna é identificada, o Proofpoint ITM oferece fluxos de trabalho e evidências irrefutáveis de atos ilícitos para acelerar a resposta ao incidente. Essa inteligência é coletada por sensores leves em endpoints. Ela é, então, analisada dentro de uma arquitetura moderna que proporciona expansibilidade, segurança e privacidade. A implantação pode ser feita por meio de modelos de entrega no local ou SaaS.

Proofpoint Data Security Posture Management

O Proofpoint Data Security Posture Management (DSPM) ataca a causa-raiz de muitas violações — pontos cegos nos ambientes de dados — enquanto prioriza a redução de riscos centrados em pessoas na segurança de dados. Ao identificar onde residem os dados confidenciais e valiosos, quem tem acesso a eles e quais riscos constituem a maior ameaça, o Proofpoint DSPM capacita as organizações de saúde a fechar lacunas, reduzir a superfície de ataque e automatizar a conformidade. O Proofpoint DSPM também permite adotar ferramentas de inteligência artificial com segurança ao identificar dados confidenciais, impor políticas de proteção de dados e oferecer análises de confidencialidade em tempo real para fluxos de trabalho de inteligência artificial.



Proofpoint Applied Services for Data Security

Há muitos anos o setor de saúde enfrenta uma escassez de mão de obra. Oferecer um atendimento de qualidade aos pacientes tem sido um verdadeiro desafio. Com menos trabalhadores qualificados para gerenciar a segurança, mais organizações de saúde estão recorrendo a serviços gerenciados para ajudá-las a suprir suas necessidades de segurança. Com o Proofpoint Applied Services for Data Security, você pode contar com nossa equipe global de especialistas em segurança de dados para complementar a sua equipe. Temos décadas de experiência. Nesse tempo, desenvolvemos as melhores práticas e modelos de maturidade para otimizar o seu programa. Nós cobrimos gerenciamento de aplicativos, governança de política e escopo, triagem de eventos, gerenciamento de incidentes, relatórios e análises. Isso protege você contra roubo de propriedade intelectual e violações de dados de pacientes. Nossos especialistas desenvolvem, implementam e operam um programa adequado às suas necessidades de segurança e conformidade. Da DLP ao ITM, nós utilizamos autoaprendizagem avançada e análise das pessoas envolvidas para proteger os seus dados de saúde. Nós inspecionamos e atuamos com base nos alertas. E oferecemos uma resposta rápida a tentativas de violação. Deixe-nos ajudar a aprimorar a sua segurança e a aproveitar a sua equipe, para que você possa se concentrar em outras coisas.

Conclusão

Instituições de saúde como a sua enfrentaram desafios sem precedentes nos últimos anos. Essa turbulência continua enquanto você tenta voltar a uma situação de estabilidade diante de cortes de custos, queda de reembolsos, escassez de mão de obra e mais. No aspecto da infraestrutura, as superfícies de ataque cresceram.
A necessidade de segurança de dados expandiu-se do data center para múltiplas nuvens. Logins efetuados de localizações remotas, tanto por funcionários quanto por pacientes, continuam numerosos.
E a quantidade de dispositivos de IoMT na borda da rede continua crescendo. Durante quase duas décadas as organizações se concentraram na proteção do perímetro. Porém, tendências recentes sinalizam que o perímetro tradicional perdeu seu significado. Nos dias de hoje, o trabalhador individual é o perímetro — e a borda. Com as soluções de segurança de dados da Proofpoint, você pode obter insights em tempo real sobre risco de dados. Você também pode priorizar e responder a incidentes e evitar perda de dados. A plataforma também oferece uma variedade de recursos regulatórios e de conformidade, inclusive descoberta, classificação e criptografia de dados. Estes ajudam você a cumprir requisitos regulatórios e padrões do setor. Você estará protegendo a sua instituição ao proteger as pessoas que trabalham com as suas informações confidenciais.

proofpoint.

DESCUBRA A PLATAFORMA DA PROOFPOINT →

0207-005-07-04 6/25