proofpoint.

RESUMO DA SOLUÇÃO

Proteção do setor de saúde contra ransomware com a Proofpoint

Evite ataques direcionados a seres humanos, defenda-se de golpes impulsionados por IA e proteja os dados contra extorsão

Visão geral

O ransomware é uma das ameaças mais perturbadoras que as organizações de saúde enfrentam atualmente. Tais ataques não se restringem apenas à criptografia de sistemas. Eles agora combinam roubo de credenciais, vazamento de dados e extorsão para maximizar os impactos operacional e financeiro. Para hospitais e prestadores de serviços de saúde, as consequências vão muito além da inatividade, afetando diretamente o atendimento ao paciente, a segurança e a confiança.

A maioria dos ataques de ransomware começa com um e-mail direcionado, uma conta comprometida ou uma mensagem enganosa que induz o usuário a realizar uma ação. E-mail, aplicativos de nuvem e plataformas de colaboração continuam sendo os principais pontos de entrada, onde atacantes exploram o comportamento humano para obter acesso inicial.

A IA está acelerando essa ameaça. Os adversários usam IA para criar mensagens de phishing altamente convincentes, passando-se por indivíduos confiáveis e ampliando ataques em organizações de saúde. Ao mesmo tempo, os prestadores de serviços de saúde estão adotando fluxos de trabalho e automação impulsionados por IA, introduzindo novas identidades de máquina e interações automatizadas que os atacantes também podem explorar.

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

A Proofpoint ajuda as organizações de saúde a combater o ransomware prevenindo o comprometimento de pessoas, detectando golpes impulsionados por IA e protegendo dados confidenciais contra vazamento de dados e extorsão.

Impacto do ransomware no atendimento ao paciente

Os ataques de ransomware não são apenas incidentes de TI; são eventos de segurança do paciente.

Quando sistemas se tornam indisponíveis ou dados são comprometidos, o impacto é imediato e de longo alcance.

- Atrasos ou interrupções no acesso a registros eletrônicos de saúde (EHR)
- Encaminhamento de pacientes de emergência para outras instalações
- Interrupções na prestação de cuidados críticos e fluxos de trabalho clínicos
- Incapacidade de acessar sistemas de diagnóstico, resultados de laboratório ou exames de imagem
- Exposição de dados confidenciais dos pacientes (PHI), o que resulta em perda de confiança

US$ 1,2M

Pagamento médio de resgate na área de saúde.[1]

Desafios do ransomware na área de saúde

O ransomware na área da saúde é particularmente prejudicial porque visa tanto as operações quanto os resultados dos pacientes. Os atacantes concentram-se deliberadamente em ambientes onde a inatividade é inadmissível.

Esses ataques seguem um padrão previsível. Perpetradores de ameaças usam phishing ou engenharia social para roubar credenciais, obter acesso a sistemas e movimentar-se lateralmente pela organização.

Uma vez dentro, eles identificam sistemas e dados de alto valor, extraem informações confidenciais e, em seguida, implantam ransomware para maximizar seu impacto e, potencialmente, interromper operações.

O que mudou é a forma como esses ataques são executados. As campanhas de ransomware atualmente são:

- Altamente direcionadas, com foco em pessoas em funções específicas, como clínicos, equipes financeiras e executivos
- Potencializadas por IA, possibilitando uma imitação mais convincente e um desenvolvimento de ataque mais acelerado
- Orientadas por dados, priorizando o roubo de dados de pacientes e de informações operacionais antes da criptografia
- Estendidas por ecossistemas, explorando fornecedores, parceiros e plataformas compartilhadas

Ao mesmo tempo, as organizações de saúde devem proteger não apenas usuários, mas também agentes de IA, fluxos de trabalho automatizados e identidades não humanas que interagem com sistemas e dados confidenciais.

Essa convergência de riscos humanos, ameaças impulsionadas por IA e exposição de dados é o que torna o ransomware moderno tão eficaz e tão difícil de deter com controles tradicionais.

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

Os ataques cibernéticos atuais não visam apenas a tecnologia. Eles exploram pessoas e agentes confiáveis. Para combater o ransomware, é necessário mudar a abordagem de segurança, da etapa final da criptografia aos estágios iniciais da cadeia de ataque.

Como o ransomware geralmente é entregue por meio de interação humana (ao clicar em um link, abrir um arquivo ou responder a uma mensagem), a defesa mais eficaz é prevenir o comprometimento antes que os atacantes obtenham acesso.

Isso requer uma abordagem de segurança que:

- Identifique quem está sendo visado
- Detecte golpes em vários canais de e-mail e nuvem
- Proteja processos automatizados e interações impulsionadas por IA
- Proteja dados confidenciais contra vazamento de dados

A Proofpoint oferece isso através de uma plataforma unificada, centrada em pessoas e agentes, que correlaciona comportamento, identidade e acesso a dados para deter o ransomware ao longo de todo o ciclo de vida do ataque.

1. Ponemon Institute. *Estudo sobre insegurança cibernética na área de saúde.* 2025.

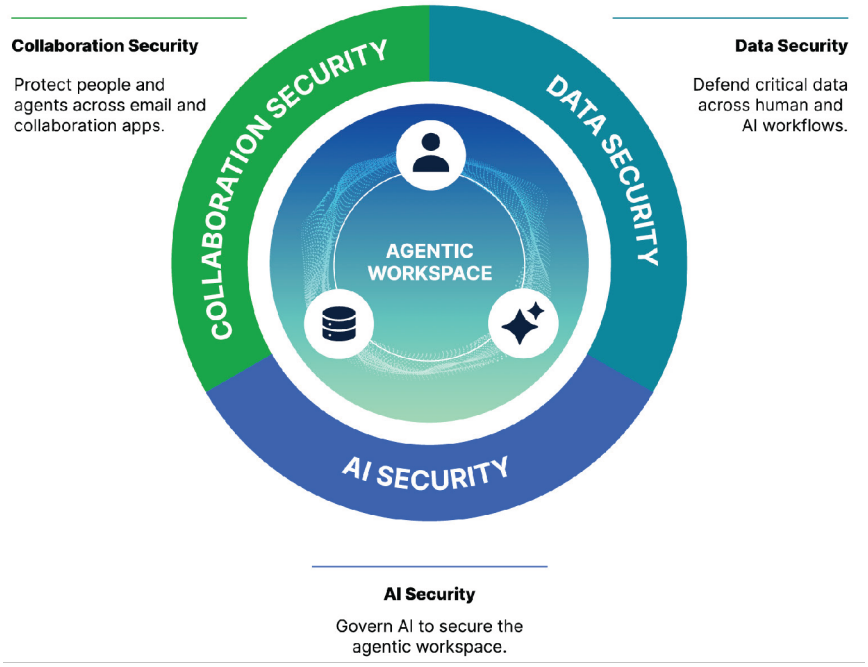

Figura 1. Uma abordagem de plataforma que interrompe o ransomware ao longo de todo o ciclo de vida do ataque.

Produtos

- Proofpoint Collaboration Security Prime
- Proofpoint Nexus
- 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 ZenGuide

Como a Proofpoint pode ajudar

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

Evite o comprometimento inicial

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.

Defenda-se de sequestro de contas e golpes impulsionados por IA

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

Mantenha os dados do paciente seguros

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

O Proofpoint Adaptive Email DLP utiliza IA comportamental para analisar padrões normais de envio de e-mails e fornecer alertas contextuais em tempo real a clínicos e funcionários, evitando o envio equivocado de mensagens e a exposição de dados sem interromper a prestação de cuidados.

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

O Proofpoint Satori™ estende aos ambientes da área de saúde o DSPM com governança de acesso a dados em tempo real. O Proofpoint Satori monitora e controla continuamente o acesso a dados confidenciais de pacientes em armazenamentos de dados na nuvem, plataformas de análise e pipelines de IA sem interromper fluxos de trabalho clínicos.

Com o Proofpoint Satori, os provedores de saúde podem: Descobrir e classificar dados confidenciais clínicos e de pacientes em plataformas de dados na nuvem

- Impor acesso com privilégios mínimos para clínicos, funcionários, aplicativos e agentes de IA
- Detectar e corrigir acessos arriscados ou anômalos a dados em tempo real
- Aplicar controles baseados em política para proteger PHI e, ao mesmo tempo, viabilizar análises, pesquisas e inovação em IA.

Reduza o risco humano por meio de mudança comportamental

O Proofpoint ZenGuide oferece treinamento de conscientização de segurança baseado em funções e orientado por riscos, personalizado para clínicos e funcionários. Ele reforça comportamentos seguros por meio de cenários reais de ameaças na área da saúde, sem comprometer a prestação de cuidados.

Conclusão

Os ataques de ransomware na área de saúde são inevitáveis, mas o êxito dos ataques não. Ao se concentrar nas fases iniciais da cadeia de ataque e abordar as causas fundamentais, as organizações de saúde podem deter o ransomware antes que ele interrompa a prestação de cuidados.

A Proofpoint possibilita que as organizações de saúde evitem ataques, protejam dados de pacientes e mantenham a resiliência operacional com uma abordagem moderna e centrada em pessoas e agentes para a defesa contra ransomware.

proofpoint.