proofpoint.

RESUMEN DE LA SOLUCIÓN

Protección del sector sanitario frente al ransomware con Proofpoint

Prevenga los ataques dirigidos a personas, defiéndase contra las estafas basadas en la IA y proteja sus datos contra la extorsión

Esta suite de soluciones forma parte de la plataforma integrada Human-Centric Security de Proofpoint, que protege a las personas y los datos en los entornos de trabajo agénticos.

Descripción general

El ransomware es una de las amenazas más graves a las que se enfrentan hoy en día las organizaciones de atención sanitaria. Estos ataques ya no se limitan al cifrado de los sistemas. Ahora combinan el robo de credenciales de acceso, la filtración de datos y la extorsión para maximizar el impacto operativo y financiero. Para los hospitales y los proveedores de atención sanitaria, las consecuencias van mucho más allá de las simples interrupciones del servicio y afectan directamente a la atención prestada a los pacientes, a su seguridad y a la confianza que se deposita en ellos.

La mayoría de los ataques de ransomware comienzan con un correo electrónico dirigido a una persona concreta, una cuenta comprometida o un mensaje engañoso que incita al usuario a actuar. Los correos electrónicos, las aplicaciones cloud y las plataformas de colaboración siguen siendo los principales puntos de entrada, y los ciberdelincuentes se aprovechan del comportamiento humano para obtener acceso inicial.

La IA está acelerando ahora esta amenaza. Los adversarios utilizan la IA para crear mensajes de phishing muy convincentes, suplantar la identidad de personas de confianza y ampliar los ataques contra las organizaciones de atención sanitaria. Al mismo tiempo, los proveedores de atención sanitaria están adoptando flujos de trabajo basados en la IA y la automatización, lo que da lugar a nuevas identidades de máquina e interacciones automatizadas que los ciberdelincuentes también pueden aprovechar.

Proofpoint ayuda a las organizaciones de atención sanitaria a combatir el ransomware evitando que los usuarios caigan en la trampa, detectando estafas basadas en la IA y protegiendo los datos sensibles contra la filtración y la extorsión.

Impacto del ransomware en la atención a los pacientes

Los ataques de ransomware no son meros incidentes de TI; afectan directamente a la seguridad de los pacientes.

Cuando los sistemas no están disponibles o los datos se ven comprometidos, las consecuencias son inmediatas y tienen repercusiones considerables.

- Acceso retrasado o con dificultades a los historias clínicas electrónicas
- Derivación de los casos de urgencias a otros centros
- Alteraciones en la atención a los pacientes en cuidados intensivos y en los flujos de trabajo clínicos
- Imposibilidad de acceder a los sistemas de diagnóstico, a los resultados de laboratorio ni a las pruebas de imagen
- Divulgación de datos sensibles de pacientes, lo que provoca una pérdida de confianza

1,2 M$

Importe medio de los rescates pagados en el sector sanitario[1].

Desafíos que plantea el ransomware en el sector sanitario

El ransomware en el sector sanitario es especialmente devastador, ya que afecta tanto al funcionamiento de los centros como a la atención a los pacientes. Los ciberdelincuentes atacan deliberadamente entornos en los que las interrupciones del servicio son inaceptables.

Estos ataques siguen un patrón predecible. Los ciberdelincuentes utilizan el phishing o la ingeniería social para robar credenciales, acceder a los sistemas y desplazarse lateralmente dentro de la organización.

Una vez dentro, identifican los sistemas y los datos de gran valor, filtran información confidencial y, a continuación, despliegan ransomware para maximizar su capacidad de presión y, en última instancia, paralizar las operaciones.

Lo que ha cambiado es la forma en que se llevan a cabo estos ataques. Las campañas de ransomware presentan ahora las siguientes características:

- Muy específicas y dirigidas a perfiles concretos, como médicos, equipos financieros y altos directivos.
- Optimizadas mediante IA, lo que permite suplantaciones de identidad más convincentes y una preparación más rápida de los ataques.
- Basadas en datos, que dan prioridad a la protección contra el robo de datos de pacientes e información operativa por encima del cifrado.
- Ampliadas a todos los ecosistemas, gracias a la colaboración con proveedores, partners y plataformas compartidas.

Al mismo tiempo, las organizaciones de atención sanitaria deben garantizar la seguridad no solo de los usuarios, sino también de los agentes de IA, los flujos de trabajo automatizados y las identidades no humanas que interactúan con los sistemas y los datos sensibles.

Es precisamente esta convergencia entre los riesgos humanos, las amenazas potenciadas por la IA y la exposición de los datos lo que hace que el ransomware moderno sea tan eficaz y tan difícil de detener con los controles tradicionales.

Un enfoque centrado en las personas y los agentes para garantizar la seguridad de la atención sanitaria

Los ciberataques actuales no se dirigen únicamente a la tecnología. Se aprovechan de las personas y de los agentes de confianza. Para hacer frente al ransomware, debe reorientar su estrategia de seguridad y centrarse en las primeras etapas de la cadena de ataque, en lugar de en la fase final de cifrado.

Dado que el ransomware suele propagarse a partir de una acción humana (hacer clic en un enlace, abrir un archivo o responder a un mensaje), la mejor defensa consiste en detener el ataque antes de que los ciberdelincuentes accedan al sistema.

Esto requiere un enfoque de seguridad que:

- Comprenda quiénes son los objetivos.
- Detecte estafas en correos electrónicos y servicios cloud.
- Proteja las interacciones basadas en IA y los procesos automatizados.
- Proteja los datos sensibles contra la

1. Ponemon Institute, *Study on Cyber Insecurity in Healthcare (Estudio sobre la ciberseguridad en el sector sanitario)*, 2025.

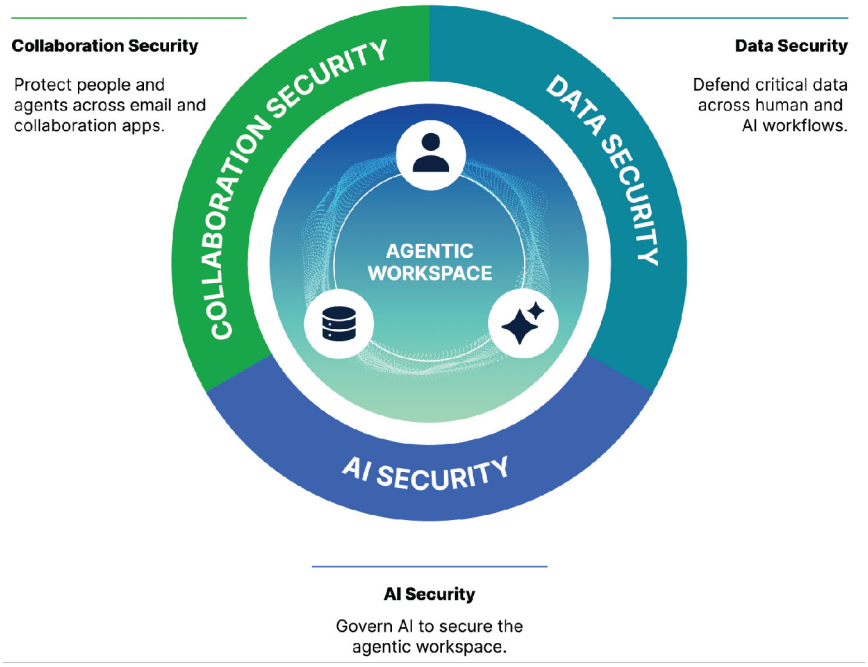

Figura 1. Un enfoque basado en una plataforma que bloquea el ransomware a lo largo de todo el ciclo de vida del ataque.

Productos

- 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

Cómo puede ayudarle Proofpoint

Adoptado por el 67 % de las empresas de atención sanitaria Fortune 500, Proofpoint es el único proveedor que ofrece una plataforma integrada que protege tanto a las personas como a los agentes y los datos.

Evite el compromiso inicial

Proofpoint Collaboration Security Prime ofrece un enfoque integral para bloquear los ataques dirigidos a personas y agentes a través del correo electrónico, las herramientas de colaboración, las aplicaciones cloud, los canales web y las redes sociales. Optimizada por Proofpoint Nexus®, esta solución utiliza inteligencia artificial avanzada, análisis de comportamiento e inteligencia de amenazas para bloquear los ataques a lo largo de todo su ciclo de vida: desde antes de la entrega hasta después de hacer clic.

Protección contra las estafas y la usurpación de cuentas basada en la IA

Proofpoint Account Takeover Protection y Proofpoint Insider Threat Management detectan comportamientos sospechosos relacionados con las identidades de personas y agentes, en particular el robo de credenciales de inicio de sesión, el uso indebido de privilegios, los desplazamientos laterales y la filtración de datos. AI correlacionar identidades, comportamientos y desplazamientos de datos, Proofpoint permite intervenir de forma más rápida y precisa, antes de que se vea afectada la atención al paciente.

Garantice la seguridad de los datos de los pacientes

Las soluciones Las soluciones Proofpoint Data Loss Prevention (DLP) previenen las pérdidas de datos accidentales y maliciosas a través del correo electrónico, la nube y los endpoints, al ofrecer una amplia visibilidad del comportamiento de los usuarios y del contenido.

Proofpoint Adaptive Email DLP utiliza la IA basada en el comportamiento para analizar los patrones habituales de envío de correos electrónicos y proporcionar alertas contextuales en tiempo real a los médicos y al personal, evitando así que los mensajes se envíen a destinatarios equivocados y la exposición de datos, sin interrumpir la atención sanitaria.

Proofpoint Data Security Posture Management (DSPM) identifica la ubicación de los datos sensibles, las personas y los agentes que tienen acceso a ellos, así como los casos en los que se conceden autorizaciones excesivas o arriesgadas. De este modo, los proveedores pueden reducir el riesgo de exposición de los datos y adoptar con total seguridad la IA y la automatización.

Proofpoint Satori™ complementa Proofpoint DSPM al gestionar el control del acceso a los datos en tiempo real en entornos sanitarios. Proofpoint Satori supervisa y controla de forma continua el acceso a los datos sensibles de los pacientes en las bases de datos en la nube, las plataformas de análisis y los procesos de IA, sin alterar los flujos de trabajo clínicos.

Con Satori, los proveedores de atención médica pueden: Descubrir y clasificar datos sensibles de los pacientes y clínicos en plataformas de datos en la nube.

- Aplicar el principio de privilegios mínimos en materia de acceso para médicos, personal, aplicaciones y agentes de IA.
- Detectar y corregir en tiempo real los accesos de riesgo o anormales a los datos.
- Aplicar controles basados en políticas para proteger los datos médicos y, al mismo tiempo, promover el análisis, la investigación y la innovación en materia de IA.

Reduzca los riesgos asociados a los usuarios mediante el cambio de comportamiento

Proofpoint ZenGuide™ ofrece cursos de formación en seguridad basados en funciones y riesgos, diseñados a medida para médicos y personal sanitario. Refuerza los comportamientos seguros basándose en escenarios de amenazas reales para la atención sanitaria sin ralentizar la prestación de la misma.

Conclusión

Los ataques de ransomware en el sector sanitario son inevitables, pero eso no significa que su éxito esté garantizado. Al centrarse en las primeras etapas de la cadena de ataque y abordar las causas subyacentes, los centros sanitarios pueden evitar que el ransomware perturbe la prestación de la atención médica.

Proofpoint permite a las organizaciones de atención sanitaria prevenir los ataques, proteger los datos de los pacientes y mantener su resiliencia operativa gracias a un enfoque moderno y centrado en las personas y los usuarios en materia de protección contra el ransomware.

proofpoint.

DESCUBRA LA PLATAFORMA DE PROOFPOINT →