proofpoint.

RESUMEN DE LA SOLUCIÓN

Protección de datos sanitarios con Proofpoint

Proteja los datos de los pacientes frente a amenazas internas, la pérdida de datos y los riesgos de la nube

Ventajas principales

- Identifique y reduzca los riesgos asociados a usuarios internos negligentes, comprometidos y maliciosos.
- Garantice una protección escalable en todos los elementos de la superficie de ataque a medida que crece su huella digital.
- Prevenga la pérdida de datos en el correo electrónico, la nube y los endpoints.

10 %

de todos los ataques de ransomware de los últimos dos años afectaron al sector de la asistencia sanitaria.

Fuente: SC Media

Las organizaciones de asistencia sanitaria han estado históricamente en el punto de mira de los ciberdelincuentes. Estas organizaciones manejan muchos tipos de datos, como propiedad intelectual, datos de ensayos clínicos, información sanitaria (PHI) y detalles financieros personales. Los ciberdelincuentes tienen muchas opciones para sacar provecho económico de un ataque contra estos datos. Con la adopción de la nube, el trabajo remoto y la telemedicina, las instituciones sanitarias están ampliando su superficie de exposición a posibles amenazas. Además, el elevado nivel de estrés al que están sometidos muchos profesionales del sector aumenta el riesgo de incidentes, tanto por acciones malintencionadas como por errores involuntarios que pueden derivar en incidentes de seguridad.

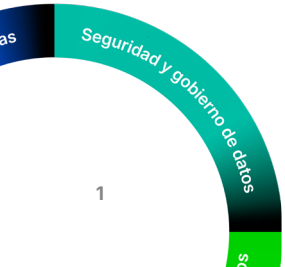
Proofpoint apuesta por una protección centrada en las personas para defender los datos sensibles en redes sanitarias distribuidas. Nuestras soluciones de seguridad ofrecen una visibilidad y control excepcionales sobre los datos sensibles. Le ayudamos a proteger a su equipo y sus datos frente a filtraciones accidentales, ataques maliciosos y amenazas internas. Nuestra cobertura abarca servicios cloud, correo electrónico, dispositivos y recursos compartidos de archivos locales, permitiendo a su organización gestionar mejor los riesgos para los datos y, al mismo tiempo, optimizar tiempo y costes operativos.

Una amenaza creciente

Al igual que muchas empresas, las organizaciones de asistencia sanitaria almacenan información sobre tarjetas de pago y otros datos financieros. Pero también gestionan enormes volúmenes de información sanitaria (PHI) sobre pacientes y datos de investigación clínica. Incluso gestionan datos relacionados con subvenciones públicas, lo que las convierte en un objetivo especialmente lucrativo para los ciberdelincuentes.

Al mismo tiempo, la huella digital de las instituciones sanitarias se vuelve cada vez más compleja: el sector aloja una creciente variedad de servicios en la nube y el número de dispositivos del Internet de la Cosas Médicas (IoMT) no deja de aumentar, ampliando así la superficie de ataque. La expansión de opciones de telesalud implica que los datos sensibles circulan cada vez más allá del perímetro tradicional de la red, y el trabajo híbrido permite que muchos empleados teletrabajen.

Por desgracia, los atacantes también han seguido a sus objetivos fuera de ese perímetro. En los dos últimos años, el sector sanitario sufrió el 10 % de todos los ataques de ransomware, y los ciberataques dirigidos a este sector aumentaron un 32 %[1], cifras notablemente superiores a las de otros sectores.



1. Shaun Nichols (*SC Media*). "Cyberattacks targeting medial organizations up 32% in 2024" (Los ciberataques contra organizaciones de asistencia sanitaria aumentaron un 32 % en 2024), febrero de 2025.

32 %

Los ciberataques contra el sector médico aumentaron un 32 % en los últimos dos años.

Fuente: SC Media

9,77 M$

En 2024, una fuga de datos sanitarios costó de media 9,77 millones de dólares.

Fuente: Ponemon Institute e IBM

Además, las fugas de datos resultan más costosas en el sector sanitario que en cualquier otro sector: en 2024, el coste medio de una fuga de datos sanitarios fue de 9,77 millones de dólares[2], incluyendo rescates, corrección, sanciones, litigios y daños reputacionales. La interrupción de sistemas o la alteración de la integridad de los datos puede tener consecuencias graves para la atención sanitaria, llegando incluso a poner en peligro vidas humanas.

Desafíos de seguridad de los datos

Para hospitales, clínicas, aseguradoras de salud y empresas biotecnológicas, la seguridad de los datos debe ser una prioridad absoluta. Estas instituciones no solo están obligadas a proteger sus propios datos de investigación y propiedad intelectual, sino que también deben proteger la información sanitaria (PHI) de los pacientes, los datos de identificación personal (PII) y la información de tarjetas de pago. Se enfrentan a numerosos desafíos. En esta sección se describen solo algunos de ellos.

Prevención del espionaje de historias clínicas electrónicas

Las organizaciones sanitarias se encuentran entre los lugares de trabajo más estresantes. Esto significa que tienen un mayor riesgo de amenazas internas.

Por ejemplo, para relajarse, un empleado curioso podría consultar las historias clínicas de un paciente famoso. Esto se conoce como espionaje de historias clínicas electrónicas, y representa un riesgo serio para la institución si llegara a hacerse pública la información de un paciente con grandes recursos económicos. Empleados bien intencionados, pero sobrecargados, podrían abrir correos electrónicos de phishing o enviar accidentalmente correos con datos sensibles a destinatarios equivocados. El estrés emocional podría incluso estar en el origen de amenazas internas maliciosas contra un empleador. Si se compromete la cuenta de un usuario de confianza debido a un robo de credenciales, las consecuencias pueden ser muy graves antes de que alguien advierta lo ocurrido. Prevenir este tipo de amenazas requiere un enfoque proactivo.

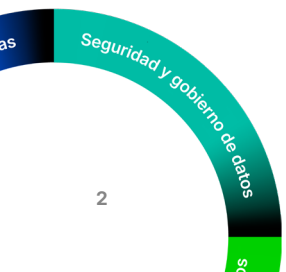
Gestión de riesgos de seguridad de la IA generativa

Las organizaciones de atención sanitaria están descubriendo cada vez más aplicaciones para la inteligencia artificial generativa (GenAI). Entre sus usos destacan el aumento de la productividad de los profesionales, la mejora de la interacción y el compromiso con pacientes y asegurados, y la optimización de tareas administrativas. Además, la IA generativa permite optimizar la calidad y la prestación de la asistencia, y va más allá de las aplicaciones clínicas tradicionales para mejorar la experiencia global del paciente. Sin embargo, el uso de la inteligencia artificial también conlleva riesgos. Más allá de los problemas derivados de resultados inexactos o sesgados, los proveedores de asistencia sanitaria deben asegurarse de que los modelos de IA no expongan ni utilicen de forma indebida información sanitaria (PHI). Esto puede suceder, por ejemplo, cuando la IA procesa datos no estructurados, como notas clínicas. Por otra parte, la integración de la IA generativa en la práctica clínica suele enfrentarse a complejos desafíos normativos que dificultan su adopción y despliegue seguro.

Cobertura de una superficie de ataque cada vez mayor durante la migración a la nube

Muchas organizaciones de asistencia sanitaria tardaron en adoptar la nube. Sin embargo, en la actualidad, prácticamente todas ellas disponen de múltiples servicios en nubes públicas, privadas e híbridas. Esto ha mejorado la atención al paciente al poner la información a disposición de los profesionales en tiempo real. También ha ayudado a las organizaciones a optimizar sus operaciones y a reducir la necesidad de grandes inversiones en infraestructura tecnológica. No obstante, estas mejoras han ampliado considerablemente la superficie de ataque.

Incluso cuando las historias clínicas electrónicas se almacenan localmente, algunos detalles de estos registros se consultan, comparten y almacenan en otros lugares. Pensemos en dispositivos móviles, endpoints remotos, dispositivos IoMT y sistemas de correo electrónico en la nube. Y cuanto más lejos viajan los datos sanitarios, más difícil resulta garantizar su seguridad.



2. Ponemon Institute e IBM. "Cost of a Data Breach Report 2024" (Informe sobre el coste de una fuga de datos en 2022).

Soluciones

- 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

El crecimiento de la presencia en la nube también incrementa el riesgo de robo de credenciales. Cada vez más aplicaciones de oficina y funciones de colaboración se proporcionan a través de servicios cloud como Microsoft 365 y Google Workspace. Esto ha aumentado el interés de los ciberdelincuentes por estos servicios.

Unificación de la seguridad de los datos en todos los canales y plataformas

Las instituciones sanitarias actuales utilizan múltiples métodos para comunicarse y transferir datos. Estos pueden incluir sistemas de historias clínicas electrónicas como Epic, sistemas de correo electrónico en la nube y locales, otros sistemas de mensajería y servicios para compartir archivos. Además, cuentan con una amplia variedad de endpoints: ordenadores en el punto de atención, cientos de tipos de dispositivos médicos, ordenadores de sobremesa, portátiles y dispositivos móviles. Muchos trabajadores utilizan varios dispositivos en un solo día. Los datos sensibles se almacenan tanto en servidores del centro de datos como en la nube, y circulan habitualmente entre ambos entornos.

A medida que la superficie de ataque se amplía y la infraestructura se complica, resulta aún más esencial contar con una seguridad integrada. En el caso de la seguridad de los datos, esto implica disponer de herramientas integradas de prevención de la pérdida de datos (DLP) en los endpoints, el correo electrónico y la nube.

Un enfoque centrado en las personas

Los enfoques tradicionales de seguridad de los datos solo se centran en los propios datos. Sin embargo, los datos no se pierden por arte de magia: detrás del incidente siempre hay una persona, ya actúe de manera accidental o malintencionada. En cualquiera de los casos, en materia de ciberseguridad, la visibilidad es esencial, por lo tanto, resulta fundamental identificar a las personas asociadas a los mayores riesgos. Un enfoque centrado en las personas permite comprender la dinámica de los usuarios que interactúan con los datos.

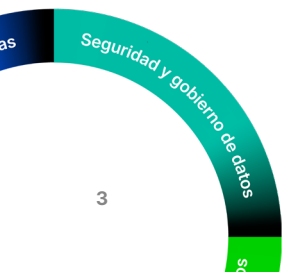
Cómo puede ayudarle Proofpoint

Las soluciones de protección de los datos centradas en las personas de Proofpoint le ofrecen una visibilidad inigualable. Gracias a una interfaz nativa para la nube, puede proteger su información sensible centrándose en las personas que interactúan con ella. Nuestras soluciones tienen en cuenta el contenido, las amenazas y los comportamientos. Combinan protección de la información en cliente (local) con seguridad para la nube. Esto garantiza que su personal, los trabajadores clínicos y los pacientes estén protegidos, con independencia de por dónde circulen sus datos.

Los componentes clave de nuestra solución unificada de seguridad de datos son los siguientes:

Proofpoint Adaptive Email DLP

Proofpoint Adaptive Email DLP emplea IA basada en el comportamiento para evitar pérdidas de datos, ya sean accidentales o intencionadas, a través del correo electrónico. Analiza más de 12 meses de datos de correo electrónico para conocer los comportamientos habituales de envío de correo electrónico de sus empleados, sus relaciones de confianza y la forma en que gestionan los datos sanitarios confidenciales. Este análisis permite a Proofpoint Adaptive Email DLP identificar el comportamiento anómalo en el correo electrónico cuando se produce. Cuando sospecha que se está enviando un mensaje de correo electrónico a la persona equivocada, un archivo mal adjuntado o se está produciendo una filtración de datos, muestra al usuario un mensaje de advertencia contextual, que le permite corregir y prevenir el incidente de pérdida de datos en tiempo real, sin intervención del administrador.



Proofpoint Enterprise DLP

Las soluciones DLP líderes de Proofpoint utilizan una estrategia adaptable y centrada en las personas de la prevención de la pérdida de datos. Ofrecen una visibilidad profunda de los comportamientos de los usuarios y los contenidos, lo que permite detectar y prevenir eficazmente los riesgos de incidentes importantes de pérdida de datos. Integramos en estrategias DLP tradicionales la protección del correo electrónico, la nube y tanto los endpoints gestionados como los no gestionados. Nuestras soluciones DLP se basan en una arquitectura nativa para la nube con modernos controles de privacidad y un agente extremadamente estable. Se amplían automáticamente y son fáciles de desplegar y de mantener.

Una única consola unificada le ayuda a gestionar las alertas e investigar las incidencias en todos los canales. Esto permite a los analistas evaluar rápidamente los riesgos para los datos, llegar a veredictos muy fiables y adoptar las medidas adecuadas.

Proofpoint Email DLP

Proofpoint Email DLP reduce sus riesgos de pérdida de datos confidenciales a través del correo electrónico y garantiza el cumplimiento de normativas aplicando la prevención basada en políticas y cifrado. Es fácil de desplegar con seguridad del correo electrónico o como parte de una estrategia unificada de DLP empresarial. Proofpoint Email DLP automatiza el cumplimiento normativo con políticas integradas para leyes y reglamentos como PCI, PII, SOX, HIPAA y RGPD. También puede utilizar diccionarios personalizados, incluida la clasificación basada en IA, para identificar y proteger datos exclusivos de su organización.

Proofpoint Email Encryption

Proofpoint Email Encryption protege automáticamente los mensajes y adjuntos con total transparencia. A diferencia de los servicios de cifrado del correo electrónico tradicionales, todo se realiza en segundo plano; los usuarios no tienen que hacer nada manualmente. Con Proofpoint Email Encryption, puede proteger los mensajes de correo electrónico confidenciales garantizando al mismo tiempo que sus filiales, partners comerciales y usuarios puedan seguir accediendo sin problema a los mensajes protegidos desde sus ordenadores o dispositivos móviles.

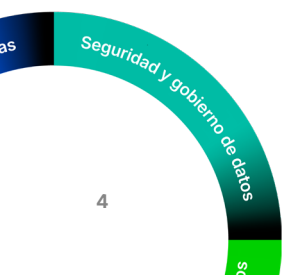
Proofpoint Insider Threat Management

Proofpoint Insider Threat Management (ITM) correlaciona las actividades de los usuarios y el movimiento de los datos. Permite a los equipos de seguridad detectar, analizar y neutralizar las amenazas internas con conocimiento de los comportamientos basado en las personas. Proporciona funciones de detección y respuesta en tiempo real en caso de filtración de datos, abuso de privilegios, uso inapropiado de aplicaciones, acceso no autorizado, actividades accidentales peligrosas o comportamientos anómalos. Esto le ayuda a detectar, prevenir y responder a amenazas como el espionaje de historias clínicas electrónicas, gracias a vistas y a análisis cronológicos.

Cuando se identifica una amenaza interna, Proofpoint ITM proporciona flujos de trabajo y pruebas irrefutables de acciones maliciosas para acelerar la respuesta a incidentes. Esta inteligencia se recopila mediante sensores de endpoints ligeros. A continuación se analiza dentro de una arquitectura moderna para garantizar la escalabilidad, la seguridad y la privacidad. También puede desplegarse mediante modelos SaaS o en cliente.

Proofpoint Data Security Posture Management

Proofpoint Data Security Posture Management (DSPM) aborda la causa principal de muchas fugas de datos (los puntos ciegos en los entornos de datos), y prioriza la reducción de los riesgos centrados en las personas en la seguridad de los datos. Al identificar dónde reside la información sensible y valiosa, quién tiene acceso a ella y qué riesgos representan la mayor amenaza, Proofpoint DSPM permite a las organizaciones de asistencia sanitaria corregir las vulnerabilidades, reducir la superficie de ataque y automatizar el cumplimiento de normativas. Proofpoint DSPM también permite la adopción segura de herramientas de IA identificando los datos sensibles, aplicando políticas de protección de datos y proporcionando análisis de sensibilidad en tiempo real para flujos de trabajo de IA.



Proofpoint Applied Services for Data Security

El sector sanitario se enfrenta desde hace muchos años a una importante escasez de personal. Esta situación ha dificultado la prestación de una asistencia de calidad a los pacientes. Con menos profesionales capacitados para encargarse de la seguridad, muchas organizaciones de asistencia sanitaria están optando por servicios gestionados para cubrir sus necesidades de seguridad. Con los servicios Proofpoint Applied Services for Data Security, puede utilizar nuestro equipo mundial de expertos en seguridad de datos para reforzar su equipo. Nuestras décadas de experiencia nos permiten crear mejores prácticas y modelos de madurez para optimizar su programa. Incluimos administración de aplicaciones, definición del ámbito y políticas, filtrado de eventos, gestión de incidentes, generación de informes y análisis. De esta forma su organización estará protegida frente al robo de propiedad intelectual y las fugas de datos de pacientes. Nuestros expertos diseñan, implementan y ejecutan un programa adaptado a sus necesidades de seguridad y cumplimiento. Las soluciones DLP e ITM de Proofpoint utilizan aprendizaje automático avanzado y el análisis humano para garantizar la seguridad de sus datos sanitarios. Inspeccionamos y gestionamos las alertas de seguridad, y respondemos de forma rápida ante intentos de vulneración de la seguridad de los datos. Déjenos ayudarle a mejorar su seguridad y dé a su equipo más tiempo para dedicarse a otros problemas.

Conclusión

En los últimos años, instituciones de asistencia sanitaria como la suya han tenido que enfrentarse a desafíos sin precedentes. Esta situación de inestabilidad persiste mientras intentan recuperar la normalidad frente a recortes presupuestarios, disminución de reembolsos, escasez de personal, etc. En lo que se refiere a infraestructura, la superficie de ataque se ha ampliado considerablemente. La necesidad de proteger los datos ha dejado de limitarse al data center y ahora abarca múltiples entornos cloud. Los accesos remotos, tanto de empleados como de pacientes, siguen siendo elevados. Además, el número de dispositivos IoMT (Internet de las Cosas Médicas) en el perímetro de la red continúa creciendo. Durante casi dos décadas, las organizaciones han centrado sus esfuerzos en proteger el perímetro. Sin embargo, las tendencias actuales demuestran que el perímetro tradicional ya no existe. Hoy en día, cada empleado es el nuevo perímetro, y el nuevo límite de la red. Con las soluciones de seguridad de los datos de Proofpoint, obtiene información en tiempo real sobre los riesgos para los datos. También puede priorizar y responder a los incidentes y prevenir la pérdida de datos. La plataforma le ofrece asimismo una amplia variedad de funciones de cumplimiento de normativas, como el descubrimiento, la clasificación y el cifrado. De esta forma podrá satisfacer los requisitos normativos y los estándares de la industria. Si protege a los empleados con acceso a información sensible, estará protegiendo su institución.

proofpoint.

DESCUBRA LA PLATAFORMA DE PROOFPOINT →

0207-005-06-04 6/25