Protección de la información sanitaria con Proofpoint

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

Productos

- Proofpoint Cloud App Security Broker
- Proofpoint Email Data Loss Prevention
- Proofpoint Endpoint Data Loss Prevention
- Proofpoint Insider Threat Management
- Proofpoint Web Security
- Proofpoint Zero Trust Network Access
- Servicios gestionados de protección de la información de Proofpoint

Ventajas principales

- Identificación y reducción de los riesgos asociados a usuarios negligentes, comprometidos y maliciosos.
- Prevención de la pérdida de datos en el correo electrónico, la nube y los endpoints.
- Ampliación de la protección evolutiva a un número cada vez mayor de servicios cloud ampliamente distribuidos.

El sector de la atención sanitaria ha sido durante mucho tiempo objetivo de preferencia de los ciberdelincuentes, y la pandemia de COVID-19 no ha hecho sino agravar la situación. Los ciberdelincuentes han redoblado esfuerzos para conseguir datos de valor como información sobre ensayos con las vacunas, información sanitaria confidencial, y datos financieros. Y por su parte, las instituciones de atención sanitaria han aumentado su superficie de ataque por la adopción de la nube, y porque permiten a más empleados y pacientes conectarse de forma remota. Estas instituciones también se enfrentan a riesgos asociados tanto a usuarios internos maliciosos como bienintencionados.

Proofpoint proporciona un enfoque centrado en las personas para proteger los datos sensibles de redes de atención sanitaria ampliamente distribuidas. Nuestras soluciones de protección de la información son fáciles de desplegar y de mantener. Puede utilizarlas para crear una arquitectura de seguridad SASE (Secure Access Service Edge) o SSE (Security Service Edge). Le ayudamos a proteger a sus empleados y sus datos confidenciales frente a los errores accidentales, los ataques y los riesgos internos. Nuestro escudo de protección se extiende a los servicios cloud, el correo electrónico, los endpoints y los recursos compartidos de archivos locales.

Una amenaza creciente

Un incidente de seguridad puede provocar sanciones por incumplimiento de normativas, litigios y el deterioro de la imagen de marca de las instituciones de atención sanitaria, e incluso la pérdida de vidas. Según el Departamento de Salud y Servicios Humanos de EE. UU, se produjo un aumento del 50 % en el número de incidentes de seguridad relacionados con la atención sanitaria en la primera mitad de 2020. Y en 2021, se duplicó el número total de ataques de ransomware. Ese año, la atención sanitaria se convirtió en uno de los sectores más atacados.

El número creciente de dispositivos IoT (Internet of Things) médicos permite salvar vidas, pero también aumenta la complejidad. Y la COVID-19 ha llevado a más proveedores a recurrir a los servicios de teleasistencia. Algunos incluso proporcionan estos servicios desde sus hogares, y no desde una clínica u hospital.

No sorprende que Moody's Investors Service descubriera que el ciberriesgo seguirá siendo alto en el sector de la atención sanitaria en el corto plazo. Tras hacer frente a casi dos años de una crisis existencial, las organizaciones de atención sanitaria deben permanecer en guardia.

Desafíos asociados a la protección de la información

Frente a un panorama de amenazas poco prometedor, los hospitales, las clínicas, las compañías de seguros médicos y las empresas biotecnológicas deben hacer de la protección de la información una prioridad absoluta. Deben proteger la información sanitaria confidencial, de identificación personal y de tarjetas de crédito de los pacientes. Los desafíos a los que se enfrentan son múltiples.

Precención del espionaje de historias médica electrónicas

Los empleados de atención sanitaria son los héroes de la pandemia. Han desarrollado su trabajo bajo el estrés y la urgencia, día tras día, incluso cuando no se vislumbraba un final. Ese nivel de estrés puede aumentar el riesgo de amenazas internas. Para relajarse, los empleados curiosos podrían, por ejemplo, sentirse tentados a curiosear las historias clínicas de un paciente famoso. Este "espionaje" de historias clínicas electrónicas puede presentar un riesgo mayor para una institución en caso de divulgación de información de un paciente acaudalado.

Empleados bienintencionados pero desbordados también podrían hacer clic en un mensaje de phishing que habrían sido capaces de identificar en otras circunstancias. El estrés emocional podría incluso estar en el origen de amenazas internas maliciosas contra un empleador. Un enfoque proactivo es por tanto esencial para impedir todos estos tipos de amenazas.

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

Muchas organizaciones de atención sanitaria tardaron en adoptar la nube. Sin embargo, en la actualidad, prácticamente todas ellas disponen de múltiples servicios en nubes públicas y privadas, lo que les ha permitido mejorar su eficacia operativa y evitar tener que invertir para dotarse de una infraestructura de TI. Pero la migración a la nube también ha aumentado la superficie de ataque de las instituciones.

Incluso si las historias clínicas electrónicas se almacenan una infraestructura local, inevitablemente, algunos detalles de esos registros se consultan, comparten y almacenan en otros lugares, concretamente en dispositivos móviles, endpoints remotos, dispositivos IoT médicos y sistemas de correo electrónico basados en la nube. Cuanto más aumentan los canales de circulación de datos médicos, más complicado es protegerlos.

Además, la extensión de la nube viene acompañada de un riesgo mayor de robo de credenciales. Servicios cloud como Microsoft 365 y Google Workspace proporcionan cada vez más software de oficina y funciones de colaboración. Pero estos servicios son vulnerables a ciberamenazas. Para complicar todavía más las cosas, los ciberdelincuentes utilizan cada vez más estos recursos compartidos de archivos reconocidos para distribuir sus exploits.

Protección del personal médico y de los pacientes remotos a medida que evolucionan los modelos de prestación

Algunos de los cambios repentinos del entorno de trabajo provocados por la pandemia a principios de 2020 han sido temporales. Sin embargo, para muchos otros, el impacto se dejará notar todavía durante varios años. En el sector de la atención sanitaria, la tendencia cada vez mayor es la de recurrir a la teleasistencia. Un estudio ha demostrado que en febrero de 2021, el uso de la teleasistencia era todavía 38 veces superior a la cifra de referencia de 2019. Esta situación genera un aumento considerable del número de pacientes que acceden de forma remota a recursos de las instituciones de atención sanitaria.

Además, una gran cantidad de los empleados siguen teletrabajando, al menos a tiempo parcial. Muchos de ellos gestionan historias clínicas electrónicas, información financiera de pacientes y datos de investigaciones. El creciente volumen de conexiones remotas aumenta el riesgo de ataques contra las personas con funciones específicas dentro de una organización.

Adopción de un enfoque centrado en las personas

Las soluciones tradicionales de protección de la información se ocupan exclusivamente de los datos. Sin embargo, los datos no se pierden por arte de magia: siempre hay una persona detrás del incidente, ya sea de manera accidental o maliciosa. En matera de ciberseguridad, la visibilidad es la clave. 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.

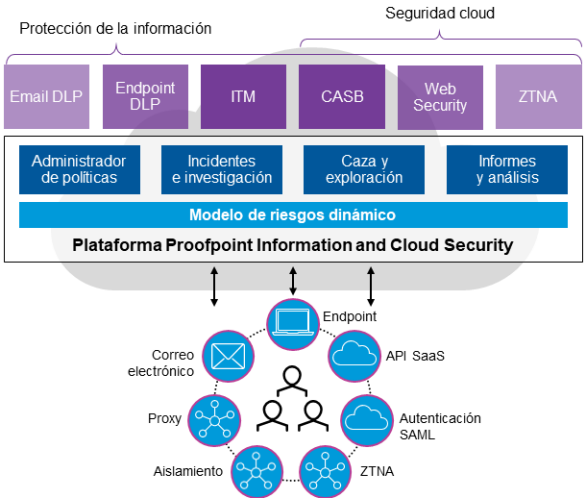

Figura 1: Plataforma Proofpoint Information and Cloud Security.

Cómo puede ayudarle Proofpoint

La plataforma Proofpoint Information and Cloud Security puede ayudarle a proteger sus datos sensibles centrándose en las personas que los administran.

Proofpoint Cloud App Security Broker

Proofpoint Cloud App Security Broker (CASB) protege a los usuarios contra las amenazas en la nube. Protege los datos sensibles y administra las aplicaciones cloud y OAuth en Microsoft 365, Google Workspace y más de 900 aplicaciones cloud aprobadas y autorizadas por el departamento de TI. Amplía la visibilidad de Proofpoint de sus VAP (Very Attacked People™, o personas muy atacadas) a sus servicios basados en la nube. Esto le permite proteger de manera más eficaz las cuentas y los datos en la nube. Proofpoint CASB ofrece una vista granular del acceso a la nube, del comportamiento de los usuarios y del tratamiento de datos sensibles (por ejemplo, información sanitaria confidencial), para ayudarle a garantizar el cumplimiento de normativas y la seguridad de los datos.

Proofpoint CASB puede desplegarse de modos distintos, en función de los casos de uso. Para garantizar una visibilidad en tiempo real y una reducción del plazo de rentabilización, Proofpoint CASB se integra con conectores API de sus aplicaciones cloud y de registros de su infraestructura. Para disponer de acceso y controles de datos en tiempo real, puede utilizar autenticación SAML basada en los riesgos, el aislamiento y funciones de proxy de reenvío en línea. Como en una verdadera arquitectura SSE, puede integrar Proofpoint CASB con Proofpoint Web Security y Proofpoint Zero Trust Network Access (ZTNA) para conectar y proteger a sus empleados remotos en las aplicaciones web y cloud.

Proofpoint Data Loss Prevention

Proofpoint Data Loss Prevention adopta un enfoque centrado en las personas de las prevención de la pérdida de datos (DLP). Combina contenido, comportamientos y amenazas, y proporciona información contextual sobre los tres aspectos. Esta información se presenta de una forma cronológica moderna, que le proporciona una comprensión más completa y detallada de cada evento. Esta información puede ayudarle a comprender si un usuario ha sido víctima de un compromiso, tiene intenciones maliciosas o sencillamente es negligente.

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. Ofrece concienciación sobre los comportamientos centrada 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. La inteligencia se recopila mediante sensores de endpoints ligeros. A continuación se analiza dentro de una arquitectura moderna para garantizar la escalabilidad, al seguridad y la privacidad. Proofpoint ITM también puede desplegarse mediante modelos de distribución locales o SaaS (Software-as-a-Service).

Proofpoint Web Security

La mayor parte de los empleados se conectan desde fuera del perímetro de red. Proofpoint Web Security protege a sus empleados distribuidos contra las amenazas avanzadas y cuando visitan la web garantizando una navegación segura. Gracias a la inspección de todo el tráfico SSL, Proofpoint Web Security detecta y bloquea amenazas como el ransomware y los ataques de phishing de día cero. La solución impide además que los empleados accedan a contenido peligroso y no conforme.

Proofpoint Zero Trust Network Access

Con la migración de aplicaciones a la nube, los profesionales de la sanidad son cada vez más móviles. Por lo tanto, es absolutamente necesaria una alternativa más eficaz a las VPN para proteger el acceso. Proofpoint ZTNA utiliza un perímetro definido por software para cada usuario. De esta forma los usuarios disponen de acceso remoto seguro a través de la nube a los recursos del centro de datos y de la nube.

A cada usuario se le concede acceso a aplicaciones específicas. El resto de la red permanece oculta. Proofpoint ZTNA valida a los usuarios antes de que accedan a la red, lo que permite reforzar la seguridad y la visibilidad.

Servicios gestionados de protección de la información de Proofpoint

Los servicios gestionados de protección de la información refuerzan su equipo con nuestros expertos mundiales en seguridad de los datos. 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 está protegido 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 Proofpoint DLP, CASB (Cloud Access Security Broker) e ITM aprovechan el aprendizaje automático avanzado y un análisis humano para garantizar la protección de la información sanitaria.

Las alertas se analizan y los equipos pueden intervenir rápidamente a los intentos de compromiso. Déjenos ayudarle a mejorar su seguridad y dé a su equipo más tiempo para dedicarse a otros problemas.

Conclusión

Las instituciones de atención sanitaria como la suya han tenido que adaptarse a los enormes cambios en el entorno de trabajo provocados por la pandemia de COVID-19. Las superficies de ataque han aumentado. La protección de la información se extiende ahora a múltiples nubes. Las conexiones de empleados y pacientes desde ubicaciones remotas aumentan a diario, al igual que el número de dispositivos IoT médicos en el perímetro de red.

Desde hace 20 años, las empresas se han esforzado en proteger su perímetro. La reciente explosión del uso de servicios cloud y la expansión del teletrabajo han convertido a los teletrabajadores en el nuevo perímetro.

Estos cambios rápidos necesitan una arquitectura de seguridad emergente, a menudo conocida como arquitectura SSE (el componente de seguridad de una arquitectura SASE). Una arquitectura así ofrece a los usuarios el acceso seguro que necesitan a todos los servicios cloud a través de los centros de datos cloud. Es en esta arquitectura donde se realiza el acceso de red de confianza cero o Zero Trust y la gestión de identidades, y donde los administradores supervisan los accesos mediante controles centralizados.

Puede aprovechar la plataforma Proofpoint Information and Cloud Security para crear una arquitectura SSE o SASE robusta. También puede proteger el acceso y garantizar la protección contras las amenazas cuando los usuarios acceden a las aplicaciones y a los datos, independientemente de dónde se encuentren y de los dispositivos que utilicen. Si protege a los empleados con acceso a información sensible, estará protegiendo su institución.

MÁS INFORMACIÓN

Para obtener más información, visite **proofpoint.com/es**.