proofpoint.

RESUMEN DE LA SOLUCIÓN

# Protección de los proveedores de atención sanitaria con Proofpoint

Proteja a las personas, los agentes de IA y los datos de los pacientes para garantizar la seguridad y la resiliencia de la atención sanitaria

## Descripción general

Con la creciente digitalización, distribución y automatización de la atención sanitaria, los proveedores de servicios de salud deben hacer frente a una superficie de ataque cada vez más amplia. Debido a la escasez de mano de obra, el personal suele estar demasiado ocupado para cumplir con los protocolos de seguridad. Los servicios cloud y los dispositivos médicos conectados añaden nuevos puntos de entrada para los ataques. Y los flujos de trabajo basados en IA introducen nuevas vulnerabilidades.

Los ciberdelincuentes han tomado buena nota de estos cambios y los están aprovechando. Saben que las filtraciones de datos sanitarios suelen tener su origen en personas o agentes de IA que actúan en su nombre. Por lo tanto, se centran en ataques basados en la identidad, la ingeniería social y el uso indebido de accesos legítimos.

Proofpoint ayuda a hospitales, sistemas sanitarios, clínicas y redes de proveedores integrados a proteger a sus médicos, personal, sistemas y pacientes. Protege todo el ecosistema de personas, agentes de IA y datos. Nuestras soluciones integradas de ciberseguridad y cumplimiento normativo reducen los riesgos de compromiso, protegen la información sensible y facilitan la prestación de una atención sanitaria resiliente e ininterrumpida.

## Objetivos de alto valor en el sector sanitario

Los proveedores de atención sanitaria se cuentan hoy entre los principales objetivos. Además de trabajar bajo una intensa presión, gestionan grandes volúmenes de datos muy sensibles, como:

- Información sanitaria como historias clínicas, resultados diagnósticos y datos de tratamiento
- Información de identificación personal
- Datos financieros, de facturación y de nóminas

Toda esta información tiene un gran valor para los ciberdelincuentes y su pérdida supone un coste muy elevado. Una fuga de datos puede dar lugar a sanciones reglamentarias, litigios, daños a la reputación y perturbaciones en la atención y la seguridad de los pacientes.

Los proveedores de atención sanitaria también se enfrentan a retos específicos relacionados con la prestación de cuidados:

- Los médicos necesitan un acceso rápido y sin interrupciones a los sistemas.
- Las comunicaciones suelen contener información sensible y urgente.
- Los equipos de atención médica colaboran con otros hospitales, clínicas y laboratorios, así como con terceros.
- Los controles jurídicos, las auditorías y las investigaciones son frecuentes.

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.

Las herramientas de colaboración por correo electrónico y en la nube son esenciales para coordinar la atención médica. Pero también constituyen los principales puntos de entrada de los ciberdelincuentes.

**Según el *informe de investigación 2025 sobre fugas de datos* de Verizon, en el 60 % de los incidentes interviene el factor humano.**

## Retos relacionados con la ciberseguridad para los proveedores de atención sanitaria

A medida que los proveedores de atención sanitaria modernizan sus operaciones, se enfrentan a riesgos cada vez mayores.

### Protección de los datos clínicos y de los pacientes

Los proveedores de servicios de atención sanitaria deben proteger la información sanitaria, la información de identificación personal y los datos financieros en lo que respecta al correo electrónico, las plataformas en la nube y los endpoints. Cualquier compromiso puede dar lugar a infracciones de las leyes HIPAA y HITECH, sanciones nacionales por infracciones de la privacidad, problemas de cumplimiento de la norma PCI DSS y costosos litigios.

### Gestión de los riesgos relacionados con los usuarios internos en entornos clínicos

El riesgo interno elevado está presente en todas partes. No solo la tasa de rotación del personal es elevada, sino que también existe una lista rotativa entre los miembros del personal, los contratistas y los residentes. Además, las historias clínicas electrónicas están disponibles para un amplio número de usuarios. La exposición accidental de datos, el uso compartido de credenciales y el uso indebido del acceso son factores que pueden dar lugar a compromisos y que deben comunicarse a las autoridades.

### Prevención del robo de identidad y la usurpación de cuentas

Los proveedores de atención sanitaria dependen de un complejo ecosistema de terceros: laboratorios, fabricantes de dispositivos médicos, proveedores de servicios, aseguradoras, organismos gubernamentales, etc. Para aprovecharse de estas relaciones de confianza, los ciberdelincuentes recurren a las estafa Business Email Compromise (BEC), a la suplantación de la identidad de proveedores y al phishing de credenciales. Los buzones de correo compartidos y las cuentas de servicio son objetivos especialmente atractivos.

### Respuesta rápida a las amenazas avanzadas

Los equipos de seguridad se enfrentan a un número abrumador de alertas. Además, no siempre es fácil adaptar las verificaciones manuales, especialmente cuando los ataques afectan a cientos de usuarios o provienen de identidades de confianza que parecen legítimas.

### Preparación para un entorno de atención sanitaria basado en la nube

Los médicos acceden cada vez más a los sistemas de forma remota y suelen utilizar sus dispositivos personales para ello. Ya no tiene sentido someter todo el tráfico a controles de seguridad locales. Para implementar una seguridad eficaz, los equipos deben poder determinar quién accede a los datos sensibles, cómo y por qué.

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

Juntos, las personas y los agentes conforman ahora la superficie operativa de la prestación de asistencia sanitaria. Aunque los médicos y el personal son responsables de implementar los procesos profesionales y de atención, también cuentan con asistencia. Muchas tareas ahora son realizadas por agentes no humanos, entre ellas:

- Buzones de correo compartidos y cuentas de servicio
- Identidades y API en la nube
- Flujos de trabajo de automatización y sistemas basados en IA
- Dispositivos médicos conectados
- Aplicaciones clínicas y profesionales como Epic.

Por eso, los ciberataques actuales no solo se dirigen contra la tecnología. Explotan a personas y agentes de confianza.

Desafortunadamente, las herramientas de seguridad tradicionales basadas en el perímetro son incapaces de distinguir entre acciones legítimas y comportamientos maliciosos. Esto es especialmente cierto cuando los ciberdelincuentes utilizan identidades comprometidas en lugar de malware para llevar a cabo sus actividades fraudulentas.

Proofpoint protege este entorno correlacionando identidades, comportamientos y accesos a los datos, tanto para personas como para agentes. Este enfoque permite eliminar los ángulos muertos que los ciberdelincuentes explotan activamente.

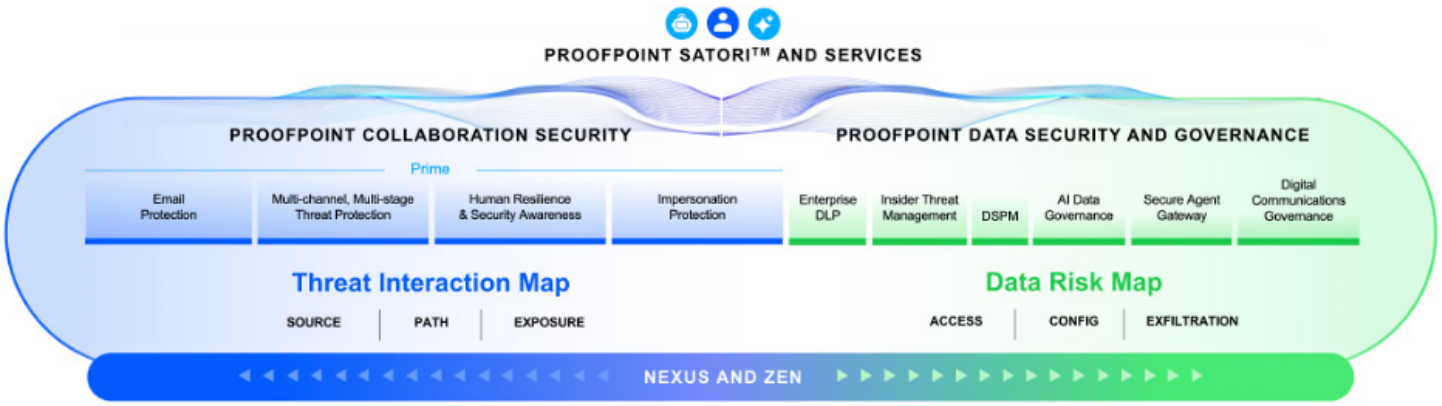



**Figura 1.** Las soluciones de Proofpoint protegen todo el ecosistema formado por personas, agentes de IA y datos.

### Productos

- Proofpoint Collaboration Security Prime
- Proofpoint Secure Email Relay
- 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 Digital Communications Governance
- Proofpoint ZenGuide

## Cómo puede Proofpoint ayudar a los proveedores de atención sanitaria

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.

En esta sección se examinan las numerosas formas en que podemos ayudar.

### Protección contra el ransomware y otras amenazas avanzadas

**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: antes de la entrega, después de la entrega y al hacer clic.

### Protección de las comunicaciones críticas por correo electrónico y a través de aplicaciones

Los proveedores de atención sanitaria tienden a depender de los correos electrónicos generados por el sistema para flujos de trabajo clínicos y operativos esenciales, por ejemplo:

- Notificaciones a pacientes y recordatorios de citas
- Coordinación de cuidados y alertas clínicas
- Extractos de facturación y comunicaciones financieras
- Cumplimiento normativo, informes y mensajes administrativos

Estas comunicacionessuelen enviarse en grandes cantidades a través de aplicaciones de confianza y deben ser:

- Entregadas de forma fiable
- Autenticadas y aprobadas por los destinatarios
- Seguras y conformes

**Proofpoint Secure Email Relay** permite a los proveedores de atención sanitaria enviar de forma segura grandes volúmenes de correos electrónicos generados por aplicaciones, al tiempo que protege a sus pacientes, partners y sus organizaciones contra la suplantación de la identidad y el fraude. Proofpoint Secure Email Relay:

- Permite la distribución de correos electrónicos que cumplen con el estándar DMARC desde aplicaciones críticas como Epic, ServiceNow y otras plataformas clínicas y empresariales.
- Protege los correos electrónicos generados por el sistema contra la suplantación de dominio y el uso indebido de dominios parecidos.
- Garantiza la confianza y la integridad de las comunicaciones operativas y con los pacientes.
- Reduce los riesgos asociados a los correos electrónicos procedentes de aplicaciones comprometidas o mal configuradas.

Al garantizar la seguridad de los remitentes no humanos, Proofpoint Secure Email Relay amplía el modelo de ciberseguridad centrado en los agentes de Proofpoint. Garantiza que las comunicaciones esenciales en materia de atención sanitaria sigan siendo fiables, conformes y resilientes.

### Protección de datos de pacientes

**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, ofreciendo 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 normales de envío de correo electrónico y proporcionar alertas contextuales en tiempo real a los médicos y al personal. Evita que los mensajes se envíen al destinatario equivocado y que los datos queden expuestos, sin perturbar la atención prestada.

**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 constantemente el acceso a los datos sensibles de los pacientes, especialmente en lo que respecta a las bases de datos en la nube, las plataformas de análisis y los procesos de IA, sin alterar los flujos de trabajo clínicos.

Gracias a Proofpoint Satori, los proveedores pueden:

- Identificar y clasificar los datos clínicos y de pacientes sensibles en las plataformas cloud.
- 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.

### Detección de compromisos y usos indebidos a gran escala

**Proofpoint Account Takeover Protection** y **Proofpoint Insider Threat Management** detectan comportamientos sospechosos relacionados con las identidades de personas y agentes. Detectan el compromiso de credenciales, el uso indebido de privilegios, los desplazamientos laterales y la filtración de datos. Al 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.

### Cumplimiento normativo y preparación para posibles litigios

**Las soluciones Proofpoint Digital Communications Governance** simplifican el cumplimiento de las leyes HIPAA y HITECH y los requisitos de retención. Se aseguran de que las comunicaciones clínicas y profesionales se recopilen, puedan consultarse y estén disponibles para auditorías, investigaciones y descubrimiento electrónico (e-Discovery).

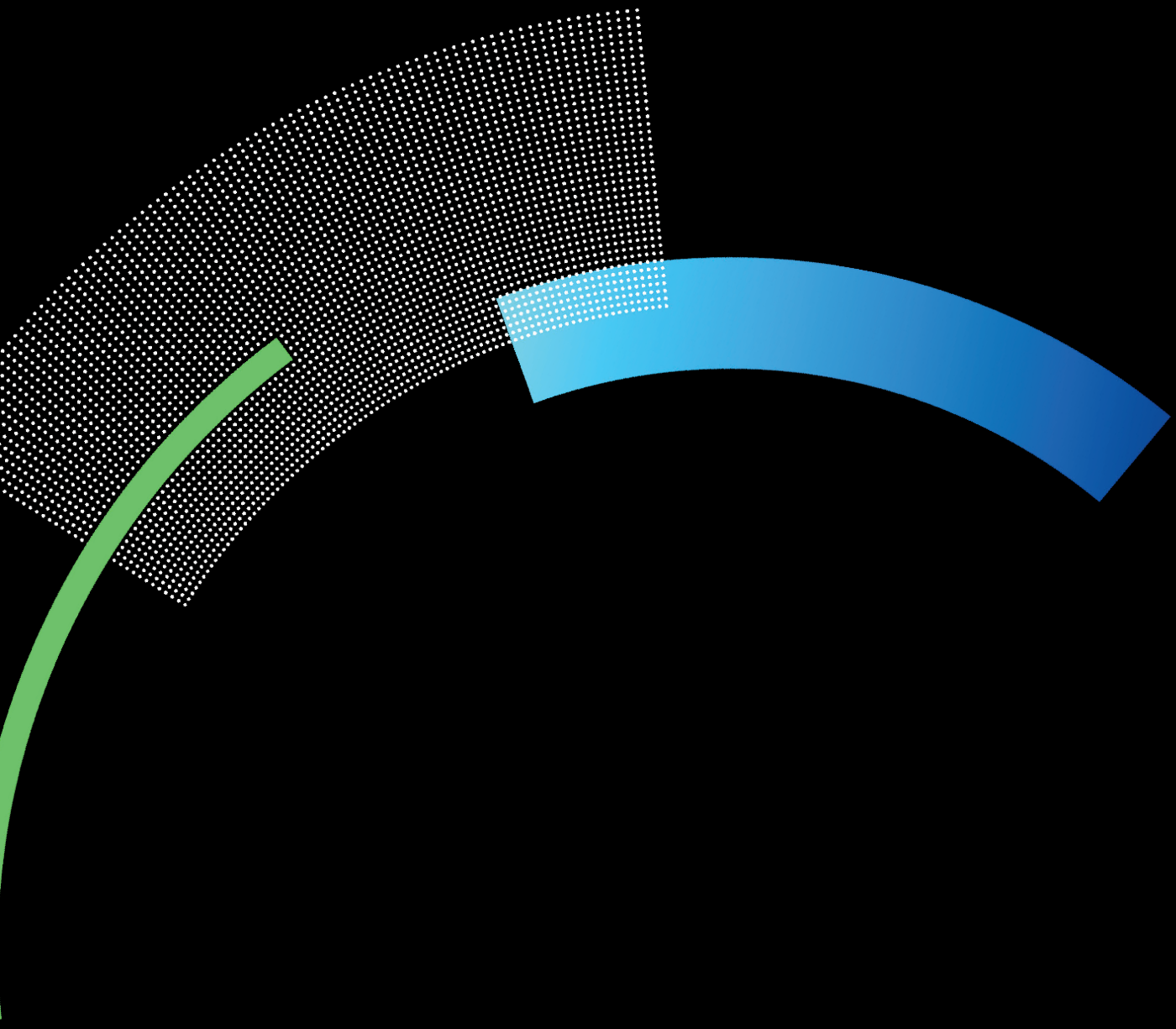
### Reducción de riesgos mediante un cambio de comportamiento

**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

Proofpoint siempre ha protegido a las personas. Y ahora nuestra plataforma de seguridad centrada en las personas y los agentes amplía la protección a cada interacción entre los empleados, los datos y los agentes de IA. De este modo, garantiza el control, el cumplimiento normativo y la libertad para adoptar la innovación.

Gracias a Proofpoint, los proveedores de atención sanitaria pueden reducir el riesgo de comprometer la seguridad, proteger los datos de los pacientes, mantener el cumplimiento normativo y proporcionar una atención resiliente e ininterrumpida en un panorama de amenazas complejo.



proofpoint.

**Acerca de Proofpoint, Inc.** Proofpoint, Inc. es líder mundial en ciberseguridad centrada en las personas y los agentes, que protege la forma en que las personas, los datos y los agentes de IA se conectan a través del correo electrónico, la nube y las herramientas de colaboración. Proofpoint es partner de confianza para más de 80 empresas Fortune 100, más de 10 000 grandes empresas y millones de pequeñas organizaciones. Les ayuda a bloquear amenazas, prevenir la pérdida de datos y reforzar la resiliencia de las personas y los flujos de trabajo de IA. La plataforma de colaboración y seguridad de datos de Proofpoint ayuda a organizaciones de todos los tamaños a proteger y empoderar a su personal mientras adoptan la IA de forma segura y con confianza. Para obtener más información, consulte www.proofpoint.com/es.

Conecte con Proofpoint: LinkedIn



**DESCUBRA LA PROOFPOINT PLATAFORMA →**