

RESUMEN DE LA SOLUCIÓN

Seguridad de los datos de Proofpoint

Protección unificada contra la filtración y exposición de datos, y las amenazas internas



Ventajas principales

- Protección integral con la primera solución de seguridad de los datos unificada del sector
- Reducción del riesgo de seguridad de los datos con prevención de pérdida de datos omnicanal, gestión de amenazas internas y gestión de la postura de seguridad de los datos
- Optimización de las operaciones de seguridad, rentabilización más rápida y menor coste de propiedad
- Agilidad empresarial, gracias al uso seguro de la IA y a la productividad de los usuarios

Este conjunto de soluciones forma parte de la plataforma Human-Centric Security, que mitiga las cuatro principales áreas de riesgo asociado a las personas.

Los datos no se pierden por arte de magia

Actualmente el riesgo de seguridad de los datos depende del comportamiento humano. Los empleados modernos ponen los datos en riesgo de multitud de formas, ya sea por error, de manera intencionada o debido al compromiso de cuentas. Según las investigaciones de Proofpoint de 2024, los usuarios negligentes han provocado el 71 % de los incidentes de pérdida de datos. Los empleados que dejan la empresa representan el 87 % de los incidentes de filtración de archivos en la nube.¹

La dispersión de los datos supone hoy día un problema importante. Los trabajadores del conocimiento almacenan datos en nubes públicas, servicios de intercambio de archivos y bases de datos locales. Además, aportan datos a los grandes modelos de lenguaje (LLM). Esta fragmentación genera puntos ciegos para los equipos de TI y de seguridad. Una de cada tres fugas de datos está relacionada con este tipo de datos no controlados por la empresa (o *shadow data*) y supone un coste por incidente un 16 % superior a la media.²

Muchas herramientas de seguridad de datos no tienen en cuenta el comportamiento humano ni la intención. Esto implica que no pueden distinguir la actividad segura de los intentos de robo de datos, lo que da lugar a falsas alertas y largas investigaciones, y afecta a la eficiencia de los equipos de seguridad. Según Gartner, para 2027, el 70 % de los directores de seguridad de la información (CISO) de las grandes empresas adoptarán un enfoque consolidado capaz de afrontar tanto los riesgos internos como la filtración de datos.³

Reducción de riesgos, disminución de costes y aumento de la agilidad empresarial

Proofpoint transforma la seguridad de los datos con una estrategia adaptable y centrada en las personas, que ya ayuda a 53 de las empresas Fortune 100 a reducir el riesgo de ciberseguridad, recortar costes y promover la agilidad empresarial.

Nuestra solución unificada protege contra los usuarios negligentes, maliciosos y comprometidos, con una precisión inigualable. Analiza el contenido y el comportamiento en el correo electrónico, los endpoints, las aplicaciones de software como servicio (SaaS) y los almacenes de datos en la nube y locales. Sus controles adaptables y automatizados responden a los riesgos emergentes en tiempo real. De esta forma, obtiene una defensa en profundidad contra filtraciones y exposición de los datos, así como frente a amenazas internas.

70 %

de los CISO adoptarán un enfoque consolidado para afrontar los riesgos internos y la filtración de datos para 2027.

Fuente: Gartner

1. Proofpoint. *Data Loss Landscape Report*. 2024.
2. IBM y Ponemon Institute. *Cost of Data Breach Report*. 2025.
3. Gartner. *Market Guide for Data Loss Prevention*. 2025.

Productos

- Proofpoint Enterprise DLP
- Proofpoint Data Security Posture Management
- Proofpoint Insider Threat Management
- Proofpoint Adaptive Email DLP

Reducción del riesgo de seguridad de los datos

La solución de seguridad de los datos de Proofpoint unifica la prevención de pérdida de datos (DLP), la gestión de la postura de seguridad de los datos (DSPM) y la gestión de amenazas internas (ITM). Gracias a estos componentes unificados, puede identificar, supervisar y mitigar los riesgos para los datos con más eficacia. Con nuestra solución, puede:

• Transformar su programa de DLP.

La consola con un solo agente unificada para Proofpoint DLP y Proofpoint ITM emplea IA para identificar con precisión la información sensible, detecta comportamientos de riesgo mediante el análisis del contenido y el contexto, y aplica controles adaptables para evitar la filtración de datos y los riesgos internos en los endpoints, el correo electrónico y la nube.

• Gestionar los riesgos internos.

Proofpoint ITM ajusta la supervisión y los controles según el riesgo que presenta cada usuario. Para agilizar las investigaciones, obtiene pruebas claras del comportamiento del usuario.

• Reducir el riesgo de exposición de datos.

Proofpoint DSPM usa análisis in situ para descubrir y clasificar los datos sensibles en entornos cloud e híbridos. Esta solución ayuda a obtener visibilidad de la dispersión de datos y a reducir su exposición eliminando el exceso de privilegios con solo un clic.

• Proteger contra la pérdida de datos por correo electrónico.

Proofpoint Adaptive Email DLP usa la IA para detectar y bloquear mensajes enviados a la persona equivocada o a una cuenta no autorizada o con archivos adjuntados por error.

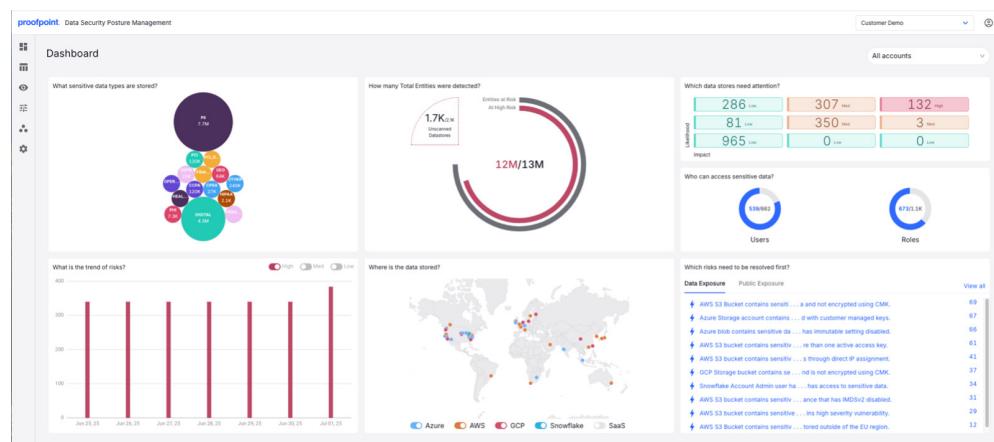


Figura 1: El panel de DSPM muestra tipos de datos valiosos o sensibles, su valor monetario y su riesgo, así como quién tiene acceso a ellos.

Detección precisa impulsada por IA y rentabilización más rápida

- Gracias a su **anificador sin agente impulsado por IA**, DSPM ofrece la clasificación de datos más precisa del mercado. Mediante la combinación de validación con expresiones regulares, procesamiento del lenguaje natural (PLN) y LLM, optimiza el rendimiento y minimiza el uso de recursos.
- Los **clasificadores de Proofpoint Nexus** AI identifican con precisión las categorías de documentos, como código fuente, o contenido legal, de contabilidad o de RR.HH. De esta forma, la información esencial de la empresa queda protegida.
- La **detección de anomalías** identifica cambios en archivos y actividades de usuarios inusuales en la nube y los endpoints. Así se evita la pérdida de datos, las amenazas internas y los compromisos de cuentas cloud.
- La **IA basada en el comportamiento** de Proofpoint Adaptive Email DLP impide que se filtren datos a cuentas no autorizadas, se envíen mensajes a la dirección equivocada y se adjunten archivos por error, lo que no permiten las soluciones de DLP por correo electrónico basadas en reglas.
- La **investigación asistida por IA** usa PLN para simplificar las búsquedas y agilizar el proceso.

Más eficiencia, menos costes operativos

Con Proofpoint, puede mejorar la eficiencia y la agilidad de las operaciones de seguridad de los datos y de protección contra amenazas internas. De esta forma se disminuye el plazo de rentabilización de la seguridad y se reduce el coste total de propiedad.

Operaciones eficientes en varios canales

La solución integral y adaptable de Proofpoint, impulsada por IA y automatización inteligente, incrementa la eficiencia de su programa de seguridad de los datos. La amplia visibilidad, el contexto detallado y los análisis avanzados eliminan las alertas de falsos positivos. Su equipo de seguridad tiene más tiempo para centrarse en iniciativas estratégicas.

- La seguridad centrada en las personas de Proofpoint combina telemetría de datos con inteligencia de amenazas y conocimiento del comportamiento y la intención de los usuarios. Así puede distinguir entre las actividades con datos que son seguras y las que son maliciosas, y responder a los riesgos de manera eficaz.

- El motor de políticas unificado de Proofpoint implementa las políticas de manera coherente en DLP, DSPM e ITM. Las políticas adaptables se ajustan a medida que cambia el nivel de riesgo del usuario.
- Para facilitar la priorización de los riesgos, DSPM evalúa el valor de los datos, la probabilidad y las rutas de posibles ataques, y los accesos con un exceso de privilegios. La posibilidad de corregir con un clic el exceso de privilegios evita la exposición de datos.
- Proofpoint Data Security Workbench ayuda a buscar amenazas antes de que se conviertan en fugas de datos.

Figura 2: En esta captura de la consola de Data Security Workbench, un usuario visita un sitio web con el título "How to hide deeply a file/folder in Windows" (Cómo ocultar bien una carpeta/archivo en Windows) y, a continuación, descarga un archivo de la unidad de SharePoint de la empresa. Por último, copia un archivo confidencial "Customer List – invoicing.xlsx" con la lista de clientes y facturas, en una unidad USB. La cronología del comportamiento del usuario y la identificación del contenido confidencial indica al analista que este usuario intenta sortear la política de la empresa y que requiere una investigación más a fondo.

58 %

Proofpoint reduce los costes de administración de DLP un 58 %.

Fuente: Enterprise Strategy Group

182 %

Proofpoint Enterprise DLP ofrece una rentabilidad de la inversión del 182 % en tres años.

Fuente: Enterprise Strategy Group

Plazo de rentabilización y coste de propiedad inigualables

Según el informe [Economic Validation of Proofpoint Enterprise DLP](#) de 2025 elaborado por Enterprise Strategy Group, Proofpoint reduce los costes de administración de DLP un 58 % y ofrece una rentabilidad de la inversión del 182 %.⁴ Esto es posible gracias a las siguientes ventajas:

- El servicio nativo de la nube de Proofpoint optimiza el despliegue, la integración y la administración.

- La seguridad de datos impulsada por IA con información del comportamiento de los usuarios reduce el tiempo para obtener valor de meses a semanas, en comparación con las soluciones tradicionales.
- La solución unificada de Proofpoint es más rentable y eficiente que un conjunto de herramientas dispares.
- DSPM identifica y elimina los datos redundantes y las copias de seguridad e instantáneas del sistema (snapshots) abandonadas. De esta forma se reducen la superficie de ataque y los costes del almacenamiento en la nube.

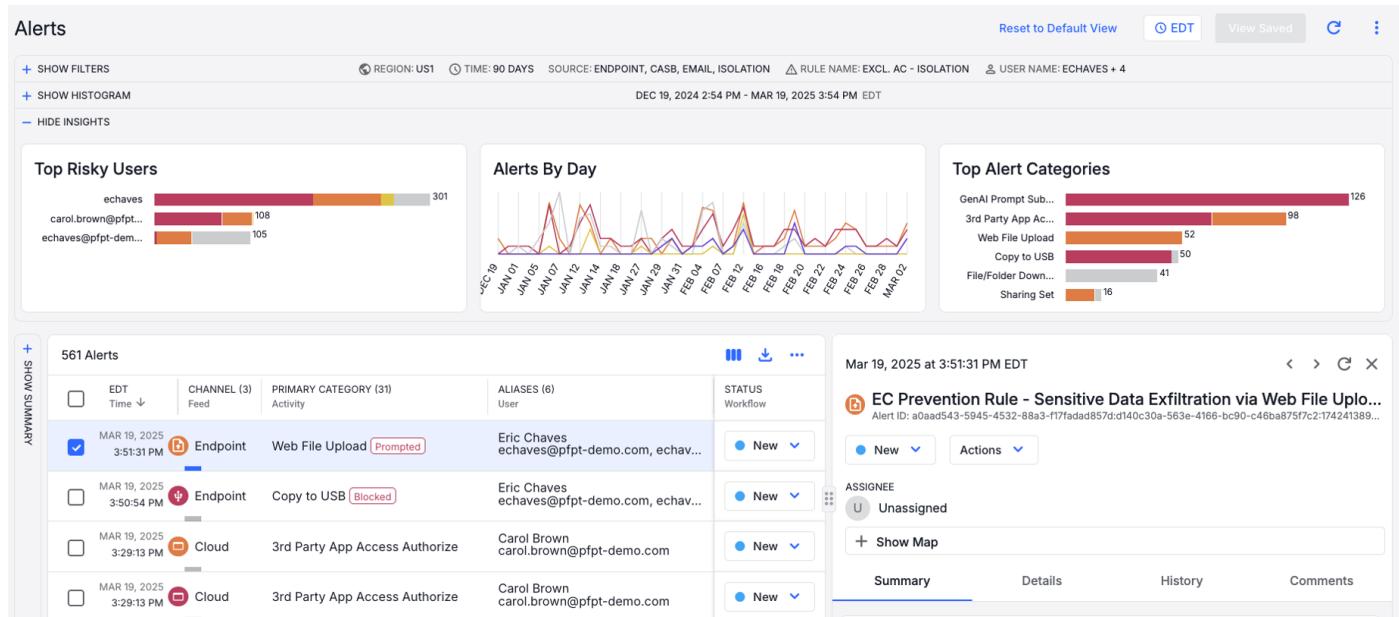


Figura 3: Data Security Workbench optimiza la gestión de alertas en el correo electrónico, la nube y los endpoints, sin necesidad de usar varias consolas. En este ejemplo, un analista filtra las alertas para un usuario concreto. El panel muestra que el usuario cargó datos sensibles en su cuenta de correo electrónico de empresa e intentó copiar un archivo en una unidad USB antes de que lo bloquearan.

4. Enterprise Strategy Group. *Analyzing the Economic Value of Proofpoint Enterprise DLP*. Junio de 2025.

Agilidad en entornos empresariales cambiantes

Cuando su organización lleve a cabo una restructuración, se expanda a otras regiones o adopte nuevas tecnologías, la información sensible estará protegida con la solución de seguridad de los datos de Proofpoint. Con Proofpoint, puede:

- **Facilitar los cambios en la organización**, reduciendo los riesgos para la propiedad intelectual, la información confidencial y demás datos sensibles. Esto incluye información asociada a fusiones, adquisiciones o restructuraciones empresariales. Con visibilidad de los entornos de las organizaciones adquiridas, puede cerrar cualquier brecha en la seguridad heredada. Nuestra automatización permite aplicar e implementar políticas y estándares de seguridad. Las políticas adaptables se ajustan a la fluctuación de los riesgos en tiempo real.
- **Garantizar un uso de la IA seguro y conforme a las normativas**, evitando compartir datos sensibles con herramientas de IA generativa públicas, grandes modelos de lenguaje (LLM) y agentes de IA. Limite la información protegida que se puede incluir en los prompts de IA generativa a través de navegadores o apps instaladas. Evite el uso de datos confidenciales al entrenar LLM personalizados.

- **Promocione la productividad del usuario**, mejorando el rendimiento de los endpoints y garantizando el acceso a las aplicaciones. Gracias al agente único ligero en modo usuario para DLP e ITM, se evitan las incompatibilidades de software, los fallos del sistema y la disminución del rendimiento de los endpoints que conlleva el uso de agentes en modo de kernel. En lugar de bloquear globalmente las aplicaciones, puede proporcionar a los usuarios pequeñas recomendaciones, por ejemplo, un recordatorio en tiempo real de que no se debe incluir información sensible en un prompt de ChatGPT. También puede solicitar a los usuarios una justificación cuando copian datos confidenciales.

Maximice el impacto de los programas de seguridad de los datos y protección contra amenazas internas

En calidad de partner estratégico, Proofpoint se ha comprometido a ayudar a que su programa dé resultados en cuanto a personas, procesos y tecnología. Los servicios Premium de Proofpoint pueden ayudarle a optimizar y madurar sus programas de seguridad de datos y protección contra amenazas internas. Ya se trate de consultoría, asesoría técnica u orientación sobre operaciones, así como gestión práctica de la seguridad de los datos, Proofpoint le proporciona la experiencia que necesita, en el momento adecuado.



Figura 4: El panel de Proofpoint Adaptive Email DLP muestra estadísticas de detección y prevención de pérdida de datos por correo electrónico. Incluye cifras de errores de entrega de mensajes, mensajes filtrados, aplicación de políticas personalizadas y de los usuarios que tienen un comportamiento más anómalo.

Niveles de la solución de seguridad de los datos de Proofpoint

Ofrecemos la solución de seguridad de los datos de Proofpoint en tres niveles: Data Security Core, Data Security Core Plus y Data Security Complete. Esta tabla incluye las funciones clave y la descripción de estos niveles de la solución.

FUNCIONES CLAVE Y DESCRIPCIÓN	DATA SECURITY CORE	DATA SECURITY CORE PLUS	DATA SECURITY COMPLETE
Contexto detallado de usuarios y archivos	✓	✓	✓
Caza de amenazas para una detección y investigación proactivas	✓	✓	✓
Agente único en modo usuario para amenazas internas y DLP	✓	✓	✓
Detecciones de DLP enriquecidas (RegEx, OCR, IDM, EDM) y clasificación MIP	✓	✓	✓
Supervisión y detección de movimientos de archivos y linaje de datos	✓	✓	✓
Detectores ampliados de aplicaciones en la nube	✓	✓	✓
Gestión unificada de alertas y configuración de DLP	✓	✓	✓
Privacidad de los datos y controles de acceso granulares	✓	✓	✓
Integración con ecosistemas de seguridad (SIEM/SOAR/Teams)	✓	✓	✓
Detección y un análisis de los datos sensibles en mensajes y adjuntos de correo electrónico.	✓	✓	✓
Cifrado dinámico de mensajes externos e internos	✓	✓	✓
Ánalisis de huellas digitales de documentos sensibles en el correo electrónico	✓	✓	✓
Descubrimiento y clasificación de almacenes de datos		✓	✓
Detección y corrección de la exposición a riesgos en almacenes de datos		✓	✓
Prevención mediante IA de la pérdida de datos accidental o intencionada a través del correo electrónico.			✓



Proofpoint, Inc. es una compañía líder en ciberseguridad y cumplimiento de normativas que protege el activo más importante y de mayor riesgo para las organizaciones: las personas. Gracias a una suite integrada de soluciones basadas en cloud, Proofpoint ayuda a empresas de todo el mundo a detener las amenazas dirigidas, a salvaguardar sus datos y a hacer a los usuarios más resilientes frente a ciberataques. Organizaciones líderes de todos los tamaños, entre las que se encuentran el 85 % de las empresas Fortune 100, confían en las soluciones de Proofpoint para su seguridad centrada en las personas y su cumplimiento normativo, mitigando los riesgos más críticos en sus sistemas de correo electrónico, cloud, redes sociales y web. Encontrará más información en www.proofpoint.com/es.

Conecte con Proofpoint: [X](#) | [LinkedIn](#) | [Facebook](#) | [YouTube](#)

Proofpoint es una marca comercial o marca comercial registrada de Proofpoint, Inc. en Estados Unidos y/o en otros países. Todas las demás marcas comerciales son propiedad exclusiva de sus respectivos propietarios. ©Proofpoint, Inc. 2025

DESCUBRA LA PLATAFORMA DE PROOFPOINT →