proofpoint.

RESUMEN DE LA SOLUCIÓN

Proofpoint Enterprise DLP

Transforme su programa y su arquitectura de seguridad de los datos

Ventajas principales

- Prevención de la pérdida de datos a través del correo electrónico, la nube, los endpoints y las aplicaciones de IA generativa.
- Aceleración de la resolución de incidentes, incluida la clasificación de alertas DLP, la investigación y la respuesta.
- Despliegue rápido, ampliación automática y mantenimiento sencillo.
- Cumplimiento de las normativas sobre la privacidad de los datos en Estados Unidos y otras regiones.

En la actualidad, los trabajadores ponen los datos en peligro de más formas que nunca. Utilizan dispositivos personales para acceder a aplicaciones cloud y compartir datos a través del correo electrónico, los endpoints y las herramientas de colaboración. Además, las herramientas de IA generativa no autorizadas suelen estar a un solo clic en el navegador. Los equipos de seguridad trabajan sin descanso para proteger la privacidad, garantizar el cumplimiento normativo y promover un uso responsable de la IA generativa. Las fugas de datos tienen cada vez mayores repercusiones económicas, reputacionales y en materia de auditoría.

Las organizaciones necesitan una mejor visibilidad de los datos sensibles. También deben observar cómo gestionan los usuarios estos datos en el correo electrónico, la nube, los endpoints y las aplicaciones de IA generativa. Sin embargo, las herramientas tradicionales de prevención de la pérdida de datos (DLP) suelen estar aisladas entre sí, son difíciles de actualizar no ofrecen una protección uniforme en los distintos canales. Tampoco son capaces de hacer frente a los riesgos emergentes relacionados con la IA.

Proofpoint Enterprise DLP fomenta un enfoque unificado y adaptativo de la prevención de la pérdida de datos (DLP). Ayuda a prevenir las pérdidas de datos provocadas por personas a través del correo electrónico, la nube, los endpoints y las aplicaciones de IA. Además, ayuda a los equipos de seguridad a trabajar de forma más eficaz.

Proofpoint identifica los contenidos sensibles y muestra cómo los utilizan los empleados. La consola unificada le ayuda a gestionar las alertas y a investigar los incidentes en todos los canales. Los análisis y la clasificación mediante IA ayudan a los equipos a evaluar los riesgos relacionados con los datos, a tomar mejores decisiones y a actuar con rapidez. La solución funciona en la nube, se actualiza automáticamente y es fácil de desplegar y gestionar. Además, cuenta con modernos controles de privacidad y un agente extremadamente estable.

Reduzca los riesgos para la seguridad de los datos en todos los canales

Una visión clara del comportamiento de los usuarios

Proofpoint supervisa cómo utilizan los empleados los datos en el correo electrónico, los dispositivos gestionados y no gestionados, las herramientas de IA generativa y las aplicaciones cloud (Microsoft 365, Google Workspace, Salesforce, etc.). Revela las intenciones de los usuarios y detecta y previene las filtraciones de datos. Por ejemplo, copiar archivos en una memoria USB no autorizada, subir archivos sensibles a una carpeta personal en la nube o compartir información confidencial a través de indicaciones de IA.

Proofpoint ayuda a las organizaciones a adoptar la IA generativa de forma segura. Detecta, bloquea y oculta los datos sensibles antes de que se compartan con aplicaciones de IA autorizadas o no autorizadas. Los equipos pueden aplicar políticas en las aplicaciones de IA tanto en el navegador como en el escritorio. Las medidas correctivas inteligentes y las experiencias de usuario guiadas ayudan a los usuarios a mantener su productividad.

Proofpoint supervisa y controla:

- Cargas de archivos a aplicaciones de IA
- Actividades de copiar y pegar que implican datos sensibles
- Prompts de IA que contienen información regulada o propietaria
- Archivos adjuntos confidenciales compartidos a través del correo electrónico y de herramientas de colaboración en la nube
- Comportamientos de riesgo de los usuarios en los endpoints y los servicios cloud

©Proofpoint, Inc. 2026

Proofpoint se integra con LDAP y Active Directory. Puede utilizar los grupos de estos directorios para definir y aplicar de forma dinámica políticas detalladas de cifrado del correo electrónico. Nuestra solución realiza un seguimiento de comportamientos como los siguientes:

- **Modificaciones en los archivos**, como cambiar el nombre de los archivos que contienen datos sensibles o modificar su extensión.
- **Uso inusual de sitios web y aplicaciones**, incluida la descarga de copias de seguridad de datos o herramientas de piratería
- **Acciones peligrosas de usuarios de alto riesgo**, incluida la manipulación del Registro de Windows para desactivar los controles de seguridad

Identificación precisa de los contenidos y clasificación mediante IA

Proofpoint mejora la precisión de la detección con más de 110 clasificadores listos para usar basados en IA. Estos identifican las categorías de documentos y añaden un contexto empresarial a las alertas de DLP. Funcionan con tecnologías de correspondencia de patrones, correspondencia exacta de datos (EDM), correspondencia de documentos indexados (IDM), reconocimiento óptico de caracteres (OCR) y análisis de huellas digitales. Esta combinación reduce los falsos positivos y mejora la protección en todos los canales.

La clasificación personalizada y autónoma de Proofpoint utiliza grandes modelos de lenguaje (LLM) para identificar los contenidos sensibles de cada empresa, y todo ello sin necesidad de ajustes manuales. Los equipos pueden localizar y proteger rápidamente los datos sensibles (código fuente, modelos financieros, documentos técnicos, expedientes de clientes, etc.). Esto simplifica la creación de políticas y reduce el tiempo necesario para obtener valor.

Los motores de detección compartidos y controlados por IA ofrecen una protección coherente en todos los canales DLP de la empresa. Las organizaciones pueden detectar y clasificar información se identificación personal, información sanitaria (PHI), datos del sector de las tarjetas de pago, credenciales, propiedad intelectual e información comercial confidencial. Las alertas enriquecidas con grandes modelos de lenguaje (LLM) aportan contexto para que los equipos puedan investigar y reaccionar con mayor rapidez.

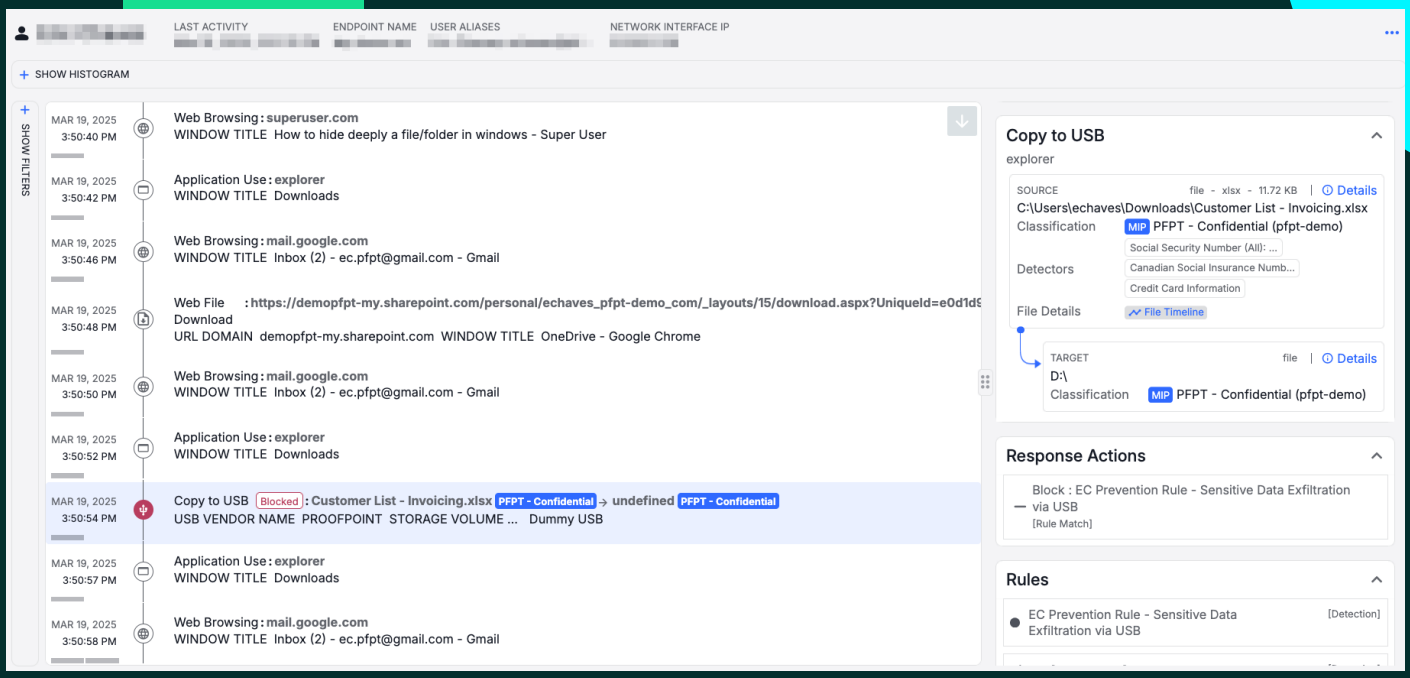

Figura 1: Este ejemplo de Data Security Workbench muestra una secuencia de acciones de los usuarios que entraña un riesgo. El usuario busca formas de ocultar un archivo, descarga un archivo confidencial de SharePoint e intenta copiarlo en una memoria USB. Las acciones y la cronología asociada apuntan a una posible elusión de las políticas, lo que requiere un análisis más detallado.

©Proofpoint, Inc. 2026

Aplicación adaptativa de las políticas y corrección guiada

Proofpoint ofrece una aplicación común de las políticas en todos los canales de DLP. Los equipos pueden definir las políticas una sola vez y aplicarlas de forma coherente.

Las políticas adaptativas ayudan a los equipos a supervisar a los usuarios de alto riesgo, a comprender sus intenciones y a automatizar las respuestas. Cuando aparece una alerta, estas políticas recopilan más metadatos y pruebas visuales. Una información más clara ayuda a los analistas a investigar más rápidamente y a reducir el coste total de propiedad.

Proofpoint también evita las pérdidas de datos confidenciales a través de prompts generados por IA. Nuestra solución ayuda a los usuarios a utilizar la IA de forma más segura. Corrige automáticamente el uso compartido ampliado de archivos en las aplicaciones cloud. Asimismo, pide a los usuarios que justifiquen la copia de datos sensibles en una carpeta en la nube o en una unidad de red.

Reduzca los costes operativos y acelere la resolución de incidentes

Operaciones de DLP eficaces en todos los canales

Los equipos que utilizan herramientas de DLP tradicionales y aisladas suelen enfrentarse a investigaciones lentas, una visibilidad fragmentada y la detección tardía (o incluso la omisión) de infracciones de las políticas. Proofpoint centraliza la detección, las políticas y los controles de gobierno en todos los canales de DLP. Data Security Workbench también centraliza la telemetría y las alertas. Esto ayuda a los equipos a clasificar, investigar y reaccionar con mayor rapidez.

La consola Data Security Workbench ofrece las siguientes ventajas :

- Vistas cronológicas de las interacciones de los usuarios con datos sensibles (véase la figura 1)
- Gestión unificada de alertas y configuración DLP (ver figura 2)
- Investigaciones relacionadas con el correo electrónico, la nube, los endpoints y las aplicaciones de IA
- Seguimiento de la trazabilidad de los archivos a medida que se crean, se modifican y se comparten
- Caza de amenazas para detectar e investigar los riesgos con mayor antelación
- Paneles para directivos e informes de auditoría

Seguridad proactiva de los datos

Data Security Workbench le permite buscar y filtrar los riesgos relacionados con los datos. Puede crear vistas personalizadas para gestionar estos riesgos antes de que se agraven. Puede detectar intentos de filtración de datos y otras actividades de riesgo, como el uso de aplicaciones de IA generativa no autorizadas. El historial de los usuarios muestra quién ha hecho qué, dónde, cuándo y por qué.

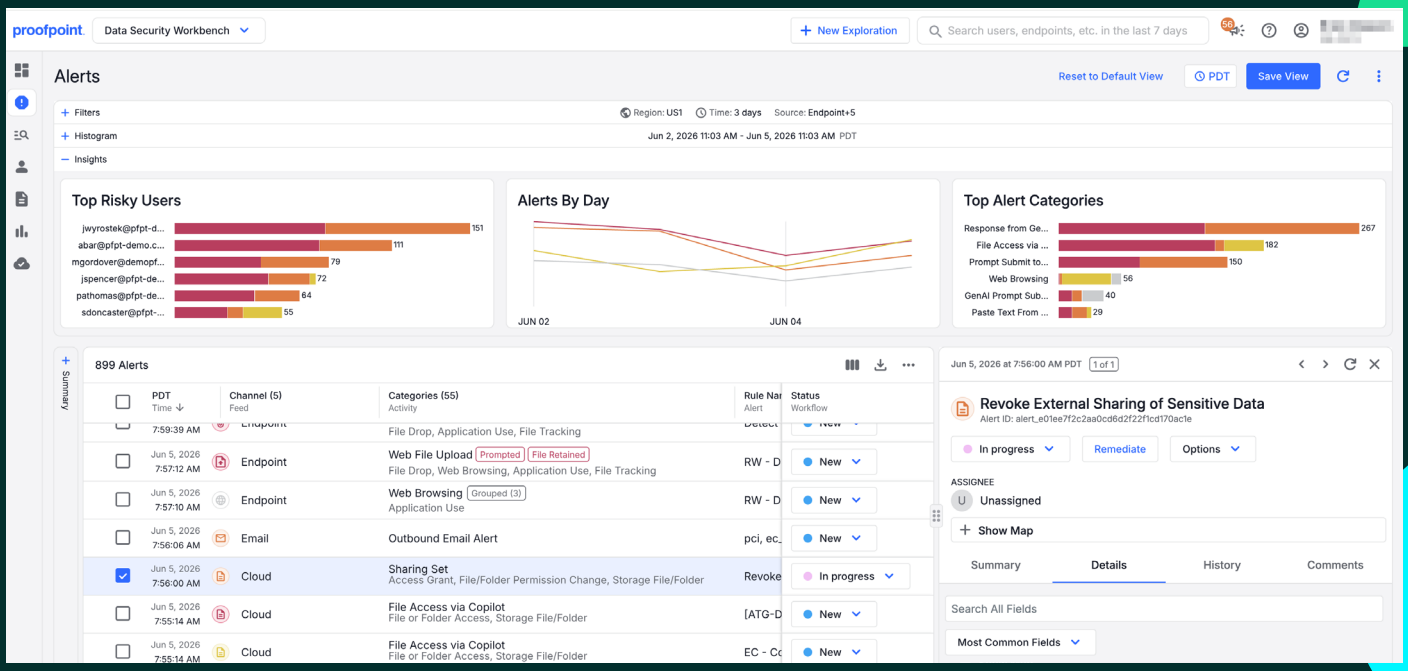

Figura 2: En el Data Security Workbench, puede crear exploraciones personalizadas de riesgos asociados a los datos.

©Proofpoint, Inc. 2026

Mejore la agilidad con una arquitectura moderna

Las soluciones de Proofpoint se ofrecen en forma de servicios, lo que le permite ahorrar un tiempo muy valioso. Se despliegan rápidamente, escalan automáticamente y facilitan el mantenimiento. Son modulares y utilizan servicios cloud compartidos. Nuestras soluciones nativas en la nube admiten múltiples inquilinos y API. Están diseñadas para evolucionar. Pueden admitir cientos de miles de usuarios por inquilino. La plataforma Proofpoint se integra con partners como Microsoft, Okta, Splunk y ServiceNow.

Controles granulares de privacidad de datos

Proofpoint ofrece una consola global nativa para la nube y puede almacenar datos en varias regiones. Los controles de acceso basados en atributos limitan quién puede consultar las alertas y las investigaciones según su rol, función o región. El enmascaramiento de los datos y la anonimización de los usuarios (véase la figura 3) contribuyen al cumplimiento de normativas regionales en materia de privacidad y residencia de los datos.

Agente de endpoint extremadamente estable

Nuestro agente ligero en modo usuario es estable y rápido de desplegar. Es único en su forma de detectar pérdidas de datos y posibles amenazas internas. Puede modificar el comportamiento del agente actualizando las políticas en la plataforma. A diferencia de los agentes en modo kernel, el agente de Proofpoint ofrece una experiencia de usuario fiable. Esto puede reducir el número de tickets de asistencia y ahorrar tiempo a los administradores.

Menor plazo de amortización gracias a nuestra experiencia

La prevención de la pérdida de datos requiere conocimientos técnicos y sobre productos, así como sólidas competencias en materia de gobierno de datos. Los servicios de Proofpoint Applied le ayudan a sacar más partido a su inversión, a garantizar la continuidad de las operaciones y a hacer evolucionar su programa de protección de datos.

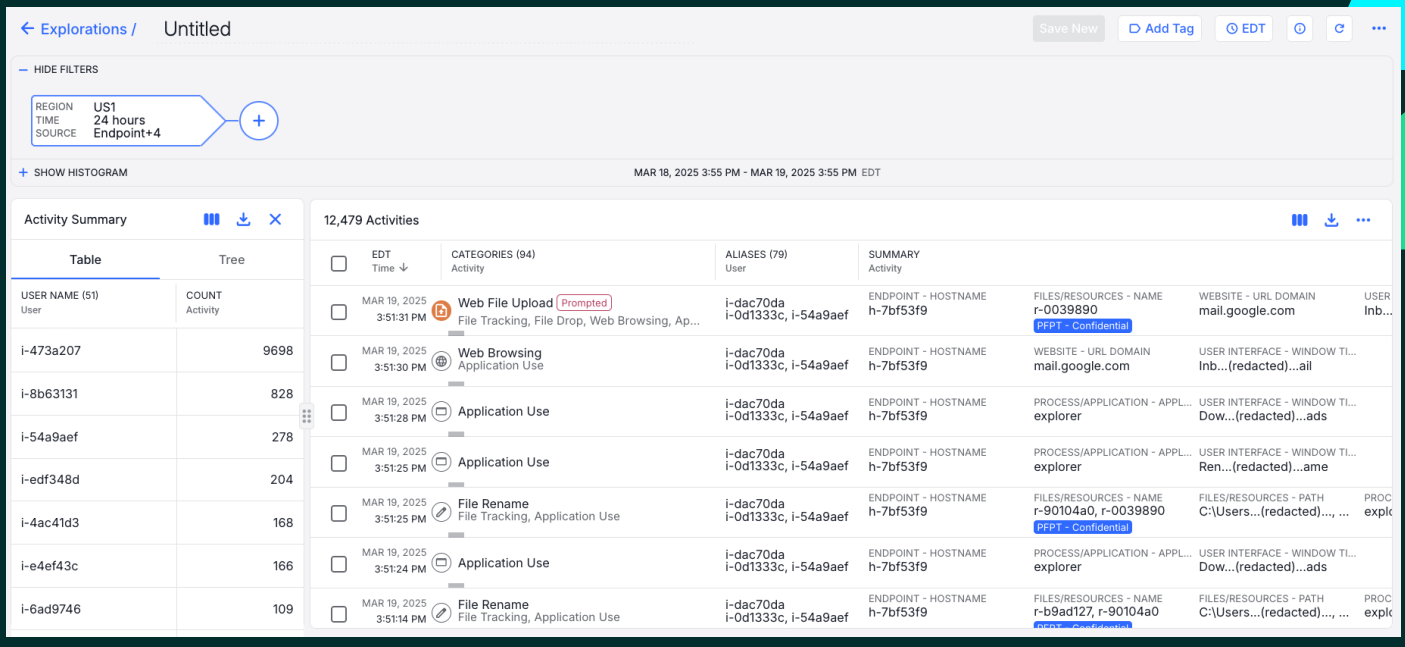

Figura 3: La consola puede anonimizar la información de los usuarios durante las investigaciones. Esto protege su privacidad y contribuye a reducir el sesgo de los analistas.

©Proofpoint, Inc. 2026

Características principales	Proofpoint DLP Transform nivel 1	Proofpoint DLP Transform nivel 2	Módulos complementarios (Add-on)
Contexto detallado de usuarios y archivos	✓	✓	
Caza de amenazas para detectar e investigar antes	✓	✓	
Agente único configurable en modo usuario para amenazas internas y DLP	✓	✓	
Detectores DLP enriquecidos (RegEx, OCR, IDM, EDM) y clasificación MIP	✓	✓	
IA lista para usar y clasificadores autónomos controlados por IA	✓	✓	
Linaje de datos para supervisar y detectar los movimientos de los archivos	✓	✓	
API, proxy de reenvío e inverso	✓	✓	
Detectores ampliados para aplicaciones cloud	✓	✓	
Gestión unificada de alertas y configuración DLP	✓	✓	
Privacidad de los datos y controles de acceso granulares	✓	✓	
Integración al ecosistema de seguridad (SIEM/SOAR/Teams)	✓	✓	
Detección y análisis de datos sensibles en mensajes y adjuntos de correo electrónico		✓	
Cifrado dinámico de los correos electrónicos externos o internos		✓	
Análisis de la huella digital de los documentos confidenciales en los correos electrónicos		✓	
Prevención impulsada por IA de la pérdida de datos accidental o intencionada a través del correo electrónico.			✓
Descubrimiento y clasificación de almacenes de datos			✓
Detección y corrección de riesgos de exposición en almacenes de datos			✓
Captura visual de amenazas internas			✓

Más información

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

Acerca de Proofpoint, Inc. Proofpoint, Inc. es un 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 un partner de confianza para más de 80 de las empresas Fortune 100, más de 10 000 grandes empresas y millones de pequeñas organizaciones. Les ayuda a bloquear las 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 inteligencia artificial de forma segura y con confianza. Más información en www.proofpoint.com/es

Conecte con Proofpoint: LinkedIn

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

proofpoint.