proofpoint.

RESUMEN DE LA SOLUCIÓN

Proofpoint Data Loss Prevention

Transforme su programa y arquitectura de seguridad de datos

Ventajas principales

- Prevención de la pérdida en datos en el correo electrónico, la nube y los endpoints.
- 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.

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 trabajadores actuales ponen en peligro los datos de formas cada vez más variadas. Utilizan cada vez más herramientas de productividad no aprobadas, como la IA generativa (GenAI). También utilizan dispositivos personales para acceder a las aplicaciones cloud de sus organizaciones. Los equipos de seguridad de datos tienen más dificultades para seguir el ritmo, ya que se les exige garantizar la privacidad con menos recursos. Al mismo tiempo, las consecuencias empresariales de las fugas de datos son cada vez más costosas. Estas incluyen pérdidas económicas, daños a la reputación y el incumplimiento de normativas. Las organizaciones deben mejorar la visibilidad de los datos que circulan por el correo electrónico, la nube y los endpoints, además de comprender mejor el comportamiento de los usuarios. Sin embargo, las herramientas tradicionales de prevención de la pérdida de datos (DLP) no satisfacen estas necesidades. Y lo que es peor, a menudo están aisladas, son costosas, difíciles de mantener y de ampliar.

Las soluciones Proofpoint Data Loss Prevention (DLP) le permiten transformar su programa y arquitectura de seguridad de datos. Nuestras soluciones permiten implementar un enfoque adaptable para la prevención de la pérdida de datos. Como resultado, puede hacer frente a la pérdida de datos provocada por las personas en sus canales de correo electrónico, nube y endpoints de forma más eficaz y eficiente.

Proofpoint identifica con precisión los contenidos sensibles y proporciona una visibilidad exhaustiva del comportamiento de los usuarios. 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. Nuestras soluciones 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.

Reduzca los riesgos para la seguridad de los datos en el correo electrónico, la nube y los endpoints

Visibilidad profunda del comportamiento de los usuarios

Proofpoint supervisa el modo en que sus trabajadores interactúan con los datos a través del correo electrónico, los endpoints gestionados y no gestionados y las aplicaciones cloud, como Microsoft 365, Google Workspace y Salesforce. Proporcionamos información sobre la intención del usuario que le ayuda a responder adecuadamente al riesgo asociados a los datos, y detectamos e impedimos la filtración de datos confidenciales. Algunos ejemplos son la copia de archivos en una unidad USB no autorizada o el intento de subirlos a una carpeta personal en la nube.

Mediante integraciones con LDAP y Active Directory, Proofpoint le ayuda a definir y aplicar dinámicamente políticas granulares de cifrado de correo electrónico. También recopilamos telemetría sobre los siguientes comportamientos:

- **Manipulación de archivos**: cambiar el nombre de los archivos con datos sensibles o cambiar su extensión.
- **Uso de sitios web y aplicaciones**: descargar copias de seguridad de datos de la web e instalarlas.
- **Comportamientos peligrosos de los usuarios de mayor riesgo**: manipular el registro de Windows para desactivar los controles de seguridad.

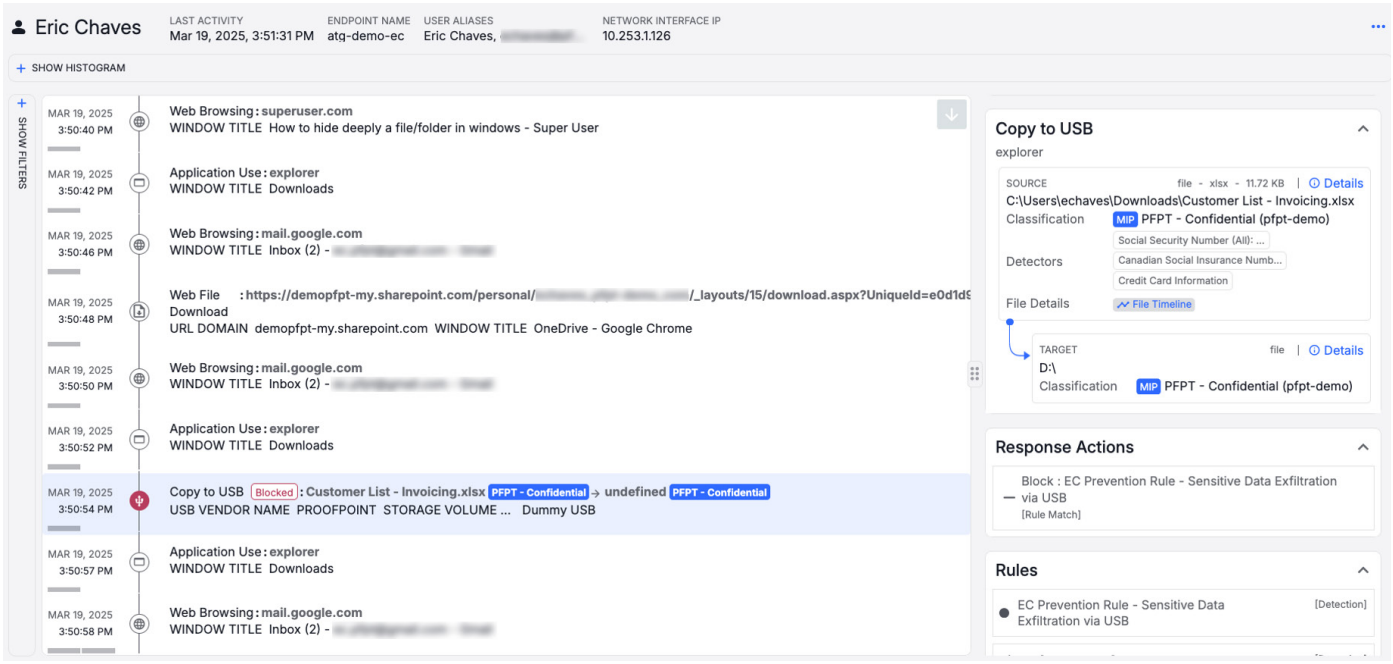


Figura 1. En esta captura de pantalla de la consola de Data Security Workbench, un usuario visita un sitio web titulado "How to hide deeply a file/folder in Windows" (Cómo ocultar profundamente un archivo/carpeta en Windows). A continuación, el usuario descarga un archivo de la unidad SharePoint de la empresa. Por último, copia un archivo confidencial llamado "Lista de clientes - facturación.xlsx" en una unidad USB. La cronología de las actividades del usuario y la identificación de contenido sensible indican a un analista que el usuario está intentando eludir las normas de la empresa y que es necesario seguir investigando.

Identificación precisa de contenido

Proofpoint utiliza métodos avanzados de identificación de contenidos para proteger sus datos. Por ejemplo, en la nube, la coincidencia exacta de datos y el reconocimiento óptico de caracteres (OCR) pueden detectar números de historias clínicas en imágenes. Esto podría ayudar a un proveedor de servicios de atención sanitaria, por ejemplo, a reducir los falsos positivos y negativos.

Puede crear políticas de DLP que tengan clasificadores de grandes modelos de lenguaje (LLM). Esto protege los contenidos sensibles de recién creado sin necesidad de clasificación previa, y le ahorra tiempo. Además, la combinación de los clasificadores de grandes modelos de lenguaje con la comparación de patrones, le permitirá reducir los falsos positivos.

Las alertas LLM ayudan a categorizar los documentos. Por ejemplo, si la coincidencia de patrones para números de DNI activa una alerta, Proofpoint puede identificar si el documento es una declaración de la renta, un formulario de paciente o una solicitud de crédito. Esto acelera las tareas de clasificación y las investigaciones.

Aplicación de políticas adaptable

Con información sobre el comportamiento de los usuarios y el movimiento de datos confidenciales, puede responder con mayor precisión a los riesgos asociados a los datos. Proofpoint evita la pérdida de datos sensibles a través de prompts de IA generativa. Nuestras soluciones forman a los usuarios para que sean capaces de modificar sus comportamientos y adoptar un uso aceptable de la IA. Actúan automáticamente para controlar el uso compartido excesivo de archivos en aplicaciones cloud. También solicita al usuario una justificación cuando copia de datos confidenciales a una carpeta en la nube o a una unidad de red.

Las políticas adaptables permiten una supervisión más precisa de los usuarios con mayor nivel de riesgo. Esto le proporciona un contexto más profundo y una mejor comprensión de la intención de sus usuarios. En lugar de ajustar las políticas manualmente, puede automatizar las respuestas ante comportamientos de riesgo. Gracias a estas políticas dinámicas, es posible recoger metadatos adicionales y pruebas visuales sobre la actividad del usuario al generarse una alerta. Con una mayor visibilidad e inteligencia procesable, puede acelerar el proceso de investigación y reducir el coste total de propiedad.

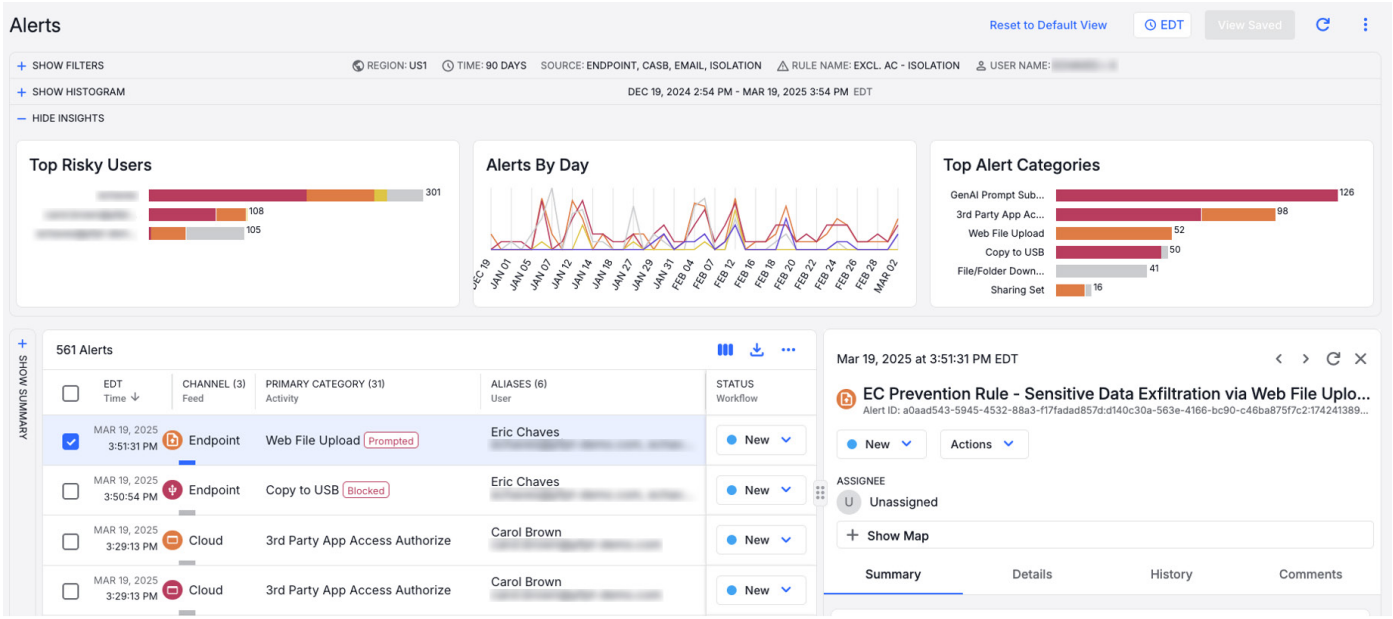


Figura 2. La consola Data Security Workbench agiliza la gestión de alertas en el correo electrónico, la nube y los endpoints, para que no tenga que cambiar entre varias consolas. En este ejemplo, un analista ha filtrado alertas para un usuario específico. La consola muestra que el usuario cargó datos confidenciales en su cuenta de correo electrónico corporativo y, a continuación, intentó copiar un archivo en una unidad USB antes de ser bloqueado.

Reduzca los costes operativos y acelere la resolución de incidentes

Operaciones de DLP eficientes en todos los canales

Los equipos de seguridad que utilizan herramientas de DLP aisladas o de generaciones anteriores pueden experimentar tiempos de investigación prolongados y pasar por alto infracciones de las políticas. Proofpoint recopila datos de telemetría de aplicaciones cloud, endpoints y correo electrónico para ofrecerle una visibilidad multicanal completa de los riesgos de los datos de forma centralizada. Esto agiliza la clasificación de alertas en todos los canales y acelera las investigaciones y la respuesta a incidentes. La consola Data Security Workbench proporciona potentes análisis, visualizaciones intuitivas y flujos de trabajo eficaces para ayudarle a:

- Investigar las interacciones de los usuarios con los datos dentro de una vista cronológica para determinar sus intenciones y su nivel de riesgo (Figura 1).
- Clasificar y correlacionar alertas (Figura 2).
- Rastrear el ciclo de vida de un archivo (creación, modificación, compartición).
- Coordinar la respuesta a incidentes.
- Utilizar informes resumidos listos para usar para demostrar la eficacia y la cobertura, y generar informes personalizados con fines de auditoría.
- Implementar y gestionar políticas de DLP y controles de administrador coherentes para el acceso a los datos y la confidencialidad en todos los canales.

Seguridad proactiva de los datos

La consola Data Security Workbench ofrece funciones avanzadas de búsqueda y filtrado. Le ayuda a crear exploraciones personalizadas para que pueda gestionar de forma proactiva los riesgos asociados a los datos. Puede buscar intentos de filtración de datos y otras actividades de riesgo, como el uso de aplicaciones de IA generativa no aprobadas. La cronológica de las actividades de los usuarios le ayuda a conocer todos los detalles ("quién, qué, dónde, cuándo y porqué") de cada incidente de seguridad.

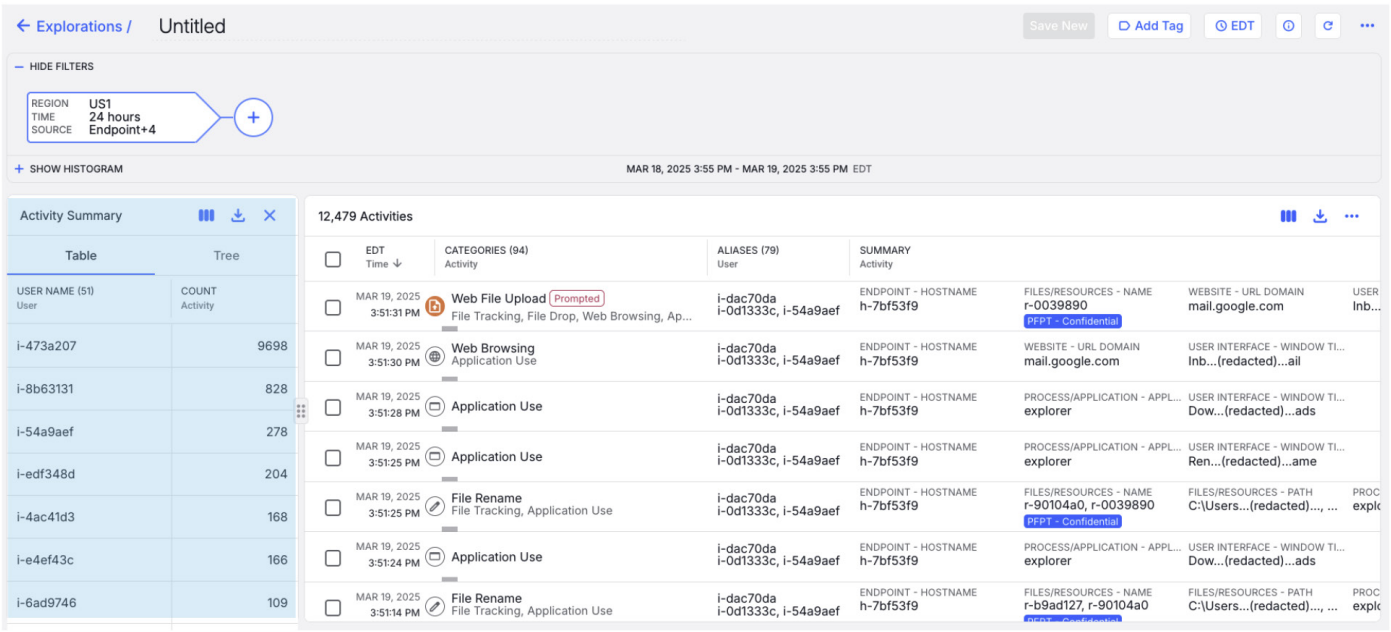


Figura 3. Como se puede ver en la captura de pantalla, la consola anonimiza los nombres de usuario. Esto protege la privacidad de los usuarios investigados y elimina el sesgo de los analistas.

Mejore la agilidad con una arquitectura moderna

Disponibles en forma de servicios, nuestras soluciones le ahorrarán un tiempo valioso. Se despliegan rápidamente, evolucionan automáticamente y son fáciles de mantener. Son modulares y ofrecen servicios compartidos basados en la nube. Nuestras soluciones multiinquilino nativas para la nube se basan en API y son muy escalables. Pueden admitir cientos de miles de usuarios por inquilino. La plataforma de Proofpoint admite integraciones API con partner del ecosistema como Microsoft, Okta, Splunk y ServiceNow.

Controles granulares de privacidad de datos

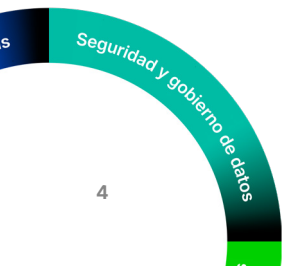
Aunque Proofpoint ofrece una consola global nativa para la nube, puede almacenar datos en varias regiones. Puede utilizar controles de acceso basados en atributos para gestionar alertas e investigaciones a través de roles y funciones regionales. También puede ocultar datos sensibles y anonimizar la información que identifica a los usuarios (Figura 3). Esto le ayudará a cumplir los requisitos de localización y confidencialidad de datos específicos de cada región del mundo.

Agente de endpoint extremadamente estable

Nuestro agente ligero en modo usuario es estable y rápido de desplegar. Puede detectar pérdidas de datos y mejorar la visibilidad de posibles amenazas internas. Ajustando las políticas en la plataforma, puede modificar el comportamiento del agente. A diferencia de los agentes en modo kernel, el agente de Proofpoint ofrece una experiencia de usuario fiable. Esto reduce el número de solicitudes de asistencia y ahorra tiempo a los administradores.

Cortos períodos de rentabilización gracias a nuestra experiencia

Evitar las filtraciones de datos no es tarea fácil. Requiere conocimientos técnicos y de producto, así como una comprensión profunda del gobierno y la administración de datos. Proofpoint puede convertirse en su partner de confianza para garantizar el éxito de su programa DLP. Nuestros servicios Applied le ofrecen una experiencia que le ayuda a optimizar su inversión en tecnología, facilitar la continuidad de sus operaciones y madurar su estrategia de protección de datos.



Características principales de las soluciones Proofpoint DLP

Compare nuestras soluciones para encontrar la que mejor se adapte a su organización.

CARACTERÍSTICAS PRINCIPALES	PROOFPOINT DLP TRANSFORM	PROOFPOINT DLP TRANSFORM – ADVANCED	MÓDULOS COMPLE-MENTARIOS (ADD-ON)
Contexto detallado de usuarios y archivos	✓	✓	
Caza de amenazas para una detección/investigación proactiva	✓	✓	
Agente único configurable en modo usuario para amenazas internas y DLP	✓	✓	
Detecciones DLP enriquecidas (RegEx, OCR, IDM, EDM) y clasificación MIP	✓	✓	
Supervisión y detección de movimientos de archivos y linaje de datos	✓	✓	
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 con ecosistemas de seguridad (SIEM/SOAR/Teams)	✓	✓	
Detección y análisis de los datos sensibles en mensajes y adjuntos de correo electrónico.		✓	
Cifrado dinámico de correo electrónico externo e interno		✓	
Análisis de huellas digitales de documentos sensibles en el correo electrónico		✓	
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			✓

proofpoint.

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: LinkedIn

DESCUBRA LA PLATAFORMA DE PROOFPOINT →