

Proofpoint Data Security Posture Management

Descubra y proteja los datos en plataformas SaaS, infraestructuras cloud y entornos locales

Ventajas principales

- **Los clasificadores de IA** identifican datos sensibles y propios del negocio sin necesidad de definir reglas manuales en entornos SaaS, en la nube y locales.
- **Data Risk Map** prioriza el riesgo utilizando la sensibilidad, el acceso, el impacto empresarial y el movimiento de los datos.
- **El gobierno del acceso a escala empresarial agiliza la corrección directa y delegada, así como la creación de políticas de DLP.**
- **La seguridad de datos integrada para la IA** identifica los datos sensibles expuestos a aplicaciones de IA y procesos de entrenamiento.
- Los paneles de cumplimiento evalúan la postura respecto a más de 25 marcos normativos y ofrecen informes que facilitan la toma de medidas.
- La seguridad de datos unificada comparte inteligencia entre DSPM, gobierno del acceso, DLP y seguridad de datos para la IA.

El crecimiento explosivo de los datos empresariales

El auge de la IA, las plataformas de bases de datos como servicio (DBaaS) y el almacenamiento en la nube han acelerado la dispersión de los datos en entornos SaaS, en la nube y locales. A medida que los datos sensibles se dispersan por distintos sistemas y flujos de datos, a los equipos les resulta difícil saber dónde se encuentran. Esto genera puntos ciegos, aumenta el riesgo de exposición y dificulta el cumplimiento normativo.

Acceso descontrolado a los datos por parte de personas y sistemas de IA

La falta de control sobre quién o qué puede acceder a los datos sensibles agrava aún más su dispersión. Los usuarios con privilegios, las herramientas no autorizadas y las prácticas de uso compartido poco seguras generan riesgos vinculados al factor humano. Los modelos de IA, los agentes y los flujos de trabajo automatizados crean nuevas vías de acceso sin intervención humana. Sin un gobierno sólido, las configuraciones incorrectas, el exceso de permisos y una supervisión insuficiente pueden provocar fugas de datos, usos indebidos e incumplimientos normativos.

55%

de las organizaciones afirman que entre el 21 y el 40 % de sus datos son sensibles.

Fuente: Proofpoint

68%

de las organizaciones afirman que el uso inadecuado de la IA ha provocado la exposición de datos sensibles.

Fuente: Proofpoint

Descubra, clasifique, gobierne y proteja los datos

Proofpoint Data Security Posture Management (DSPM) ayuda a los equipos a recuperar el control sobre los datos dispersos y reducir los accesos de riesgo por parte de personas y sistemas de IA. Descubra y clasifique los datos sensibles, identifique quién y qué puede acceder a ellos y evalúe el nivel de riesgo. Los equipos pueden corregir con mayor rapidez las exposiciones de datos y reforzar su seguridad.

Funciones únicas

Como parte de Proofpoint Data Security, DSPM integra el gobierno del acceso a los datos y comparte su marco de clasificación con Proofpoint Enterprise DLP y Proofpoint Data Security for AI. Los clasificadores de IA identifican categorías de documentos sensibles a partir del contexto y el significado, no solo de patrones. Esto mejora el descubrimiento y la clasificación de los datos. También ayuda a los equipos a gestionar el acceso, crear políticas de prevención de pérdida de datos (DLP) y proteger los datos en entornos SaaS, en la nube, locales y de IA.

DSPM detecta permisos excesivos, accesos de riesgo, configuraciones incorrectas, datos obsoletos y rutas de ataque. Data Risk Map muestra dónde se encuentran los datos sensibles, cuál es su grado de exposición y qué usuarios, aplicaciones y herramientas de IA pueden acceder a ellos. Los flujos de trabajo de gobierno del acceso a los datos permiten la corrección masiva y delegada. Con solo unos clics, los hallazgos de DSPM se convierten en reglas DLP. Estas capacidades ayudan a los equipos a reducir la exposición y aplicar el principio del mínimo de privilegios posible.

DSPM permite adoptar la IA de forma más segura. Identifica datos sensibles expuestos a copilotos, grandes modelos de lenguaje (LLM) y aplicaciones de IA.

En conjunto, Proofpoint DSPM con gobierno del acceso a los datos, Proofpoint Enterprise DLP y Proofpoint Data Security for AI permiten a los equipos descubrir, gobernar y proteger los datos sensibles durante todo su ciclo de vida.

Clasifique de forma autónoma documentos críticos para el negocio

Proofpoint DSPM ofrece una clasificación de datos líder del mercado. Utilice expresiones regulares, procesamiento del lenguaje natural (NLP) y grandes modelos de lenguaje (LLM) para optimizar el rendimiento y reducir el consumo de recursos.

Proofpoint Autonomous Custom Classification (ACC) identifica documentos específicos de la organización sin necesidad de reglas manuales ni entrenamiento. Esto ayuda a los equipos a descubrir datos propios de la empresa, eliminar puntos ciegos y mejorar la detección de riesgos y la aplicación de políticas.

Proofpoint DSPM también puede aplicar etiquetas de confidencialidad de Microsoft Information Protection (MIP) basándose en clasificadores de IA. Esto ayuda a los equipos a aplicar políticas de gobierno, favorecer el cumplimiento normativo y proteger los datos de Microsoft frente a accesos no autorizados o usos indebidos.

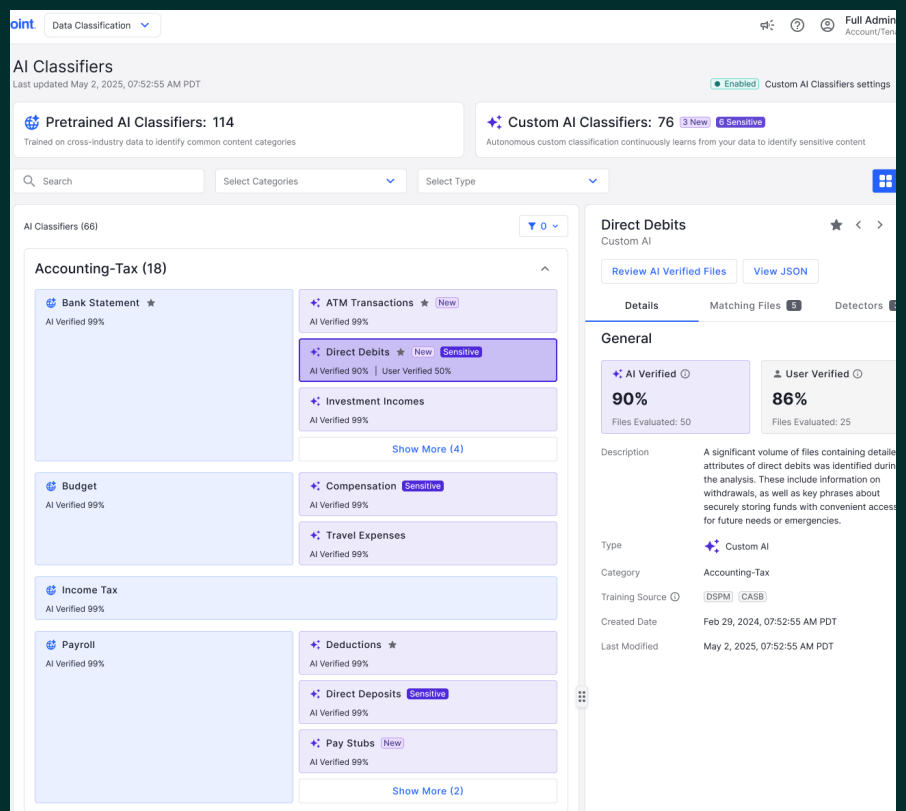


Figura 1. Los clasificadores de IA autónomos y preentrenados de DSPM identifican documentos habituales y propios del negocio, como contratos, registros financieros, código fuente y expedientes de empleados.

Mapa de riesgos de acceso a los datos

El mapa de riesgos de datos muestra dónde se encuentran los datos sensibles en entornos SaaS y sistemas locales. Muestra hasta qué punto se comparten los datos y qué usuarios, aplicaciones o herramientas de IA pueden acceder a ellos. Combine la clasificación mediante IA con información sobre el acceso a los datos y su uso.

Los equipos de seguridad pueden localizar datos sobreexpuestos, clasificar los riesgos, validar las correcciones y garantizar que el acceso siga siendo adecuado a medida que aumenta el uso de la IA. Los hallazgos sobre riesgos para los datos se basan en su grado de sensibilidad, los

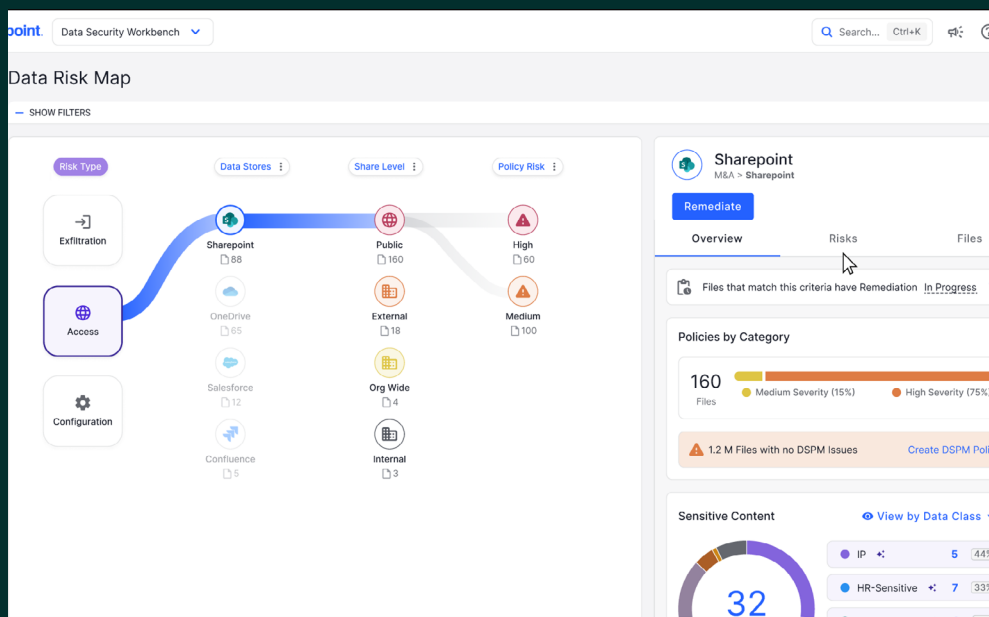


Figura 2. El mapa de riesgos de datos muestra qué repositorios contienen datos sensibles, hasta qué punto se comparten y qué usuarios, aplicaciones y herramientas de IA pueden acceder a ellos.

Priorice los riesgos según el valor económico de los datos

Los equipos de seguridad de datos deben proteger numerosos repositorios. Sin embargo, no todos los repositorios tienen el mismo valor ni presentan el mismo nivel de riesgo. Proofpoint DSPM utiliza tecnología de valoración de datos para estimar el coste de una fuga de datos en cada repositorio. Esto ayuda a los equipos a centrarse en lo que más importa. Proofpoint DSPM también incluye más de 200 hallazgos predefinidos sobre acceso y exposición, con detección de combinaciones tóxicas. Esta matriz de riesgos permite identificar los repositorios que presentan un riesgo elevado y un gran impacto financiero.

Reduzca los datos obsoletos

En entornos SaaS y sistemas locales, Proofpoint DSPM localiza y elimina los archivos a los que no se ha accedido recientemente. Los clasificadores de IA ayudan a los equipos a conservar los datos críticos para el negocio durante el tiempo necesario. Esto incluye datos en la sombra, duplicados y abandonados, como copias de seguridad e instantáneas obsoletas.

Esto reduce los costes de almacenamiento y la superficie de ataque, además de simplificar la gestión de los datos. Los equipos conservan únicamente los datos relevantes que siguen en uso.

Aplique el principio del mínimo de privilegios posible

Proofpoint DSPM ayuda a aplicar el principio del mínimo de privilegios posible al identificar usuarios con permisos excesivos, accesos no utilizados y cuentas de riesgo en todos los repositorios de datos. Esto refuerza el gobierno del acceso a los datos y el modelo Zero Trust.

La solución analiza las funciones de gestión de identidades y accesos (IAM), las autorizaciones, los derechos de acceso a las bases de datos y otros controles de acceso para identidades humanas y máquinas. Muestra casi en tiempo real quién puede acceder a los datos sensibles. Los equipos pueden revocar los permisos innecesarios y reducir la exposición.

Proofpoint DSPM también identifica las cuentas que no cuentan con protección suficiente en entornos SaaS y de plataforma como servicio (PaaS). Entre los ejemplos se incluyen usuarios con acceso a datos sensibles sin autenticación multifactor (MFA), cuentas inactivas y aplicaciones con privilegios de administrador excesivos.

Detecte rutas de ataque en entornos de nube

DSPM Proofpoint recopila información sobre los recursos informáticos y de red, así como sobre los servicios PaaS y SaaS, de todos los proveedores de servicios en la nube. Detecta errores de configuración y vulnerabilidades en esos recursos. El gráfico muestra las rutas que un atacante podría seguir para acceder a datos sensibles. La supervisión casi en tiempo real ayuda a los equipos a detectar cambios que aumentan la exposición.

La información sobre la sensibilidad de los datos, los patrones de acceso y el riesgo también sirve de base para las herramientas de prevención de la pérdida de datos (DLP) y de detección y respuesta de datos (DDR).

Gobierne el acceso directamente o mediante delegación

En entornos SaaS y sistemas locales, los flujos de trabajo de Proofpoint DSPM convierten la información sobre la exposición en medidas concretas. A medida que herramientas de IA como Microsoft Copilot amplifican las consecuencias de compartir información en exceso, resulta fundamental reducir los accesos excesivos. Los administradores pueden revocar enlaces públicos, recursos compartidos con usuarios externos y accesos concedidos a todos

los usuarios del dominio en Google Workspace y Microsoft 365. Esto permite realizar correcciones a escala empresarial.

Los equipos de seguridad no pueden determinar cuál es el nivel de acceso adecuado para cada archivo. Los flujos de trabajo de gobierno del acceso a los datos permiten delegar las revisiones de acceso en los propietarios del contenido. Las campañas automatizadas, los recordatorios y el seguimiento facilitan un gobierno continuo.

La integración con Enterprise DLP amplía la protección, que ya no se limita a los datos en reposo. Los datos sensibles clasificados y los riesgos priorizados por Proofpoint DSPM pueden vincularse a las políticas de DLP. Esto permite aplicar una protección uniforme y correcciones automatizadas en el correo electrónico, los endpoints, la nube y los canales de colaboración.

En entornos IaaS y PaaS, los análisis y las recomendaciones prácticas ayudan a los equipos a reducir rápidamente la exposición. Las integraciones con plataformas de gestión de tickets, notificaciones y automatización permiten a los equipos de seguridad colaborar con los de DevOps e ingeniería de plataformas mediante los flujos de trabajo que ya utilizan.

Manténgase alineado con los marcos de cumplimiento

Proofpoint DSPM detecta deficiencias de privacidad y seguridad en más de 25 marcos de cumplimiento normativo. Entre ellos figuran la Ley de IA de la UE, el GDPR, la HIPAA, el NIST, la CMMC y SOC 2, entre otros.

Los incumplimientos se etiquetan tanto por marco como por control, para que los analistas puedan evaluar su impacto en el cumplimiento normativo.

Los informes muestran el estado de cumplimiento de toda la infraestructura, con vistas por cuenta, recurso y marco normativo. Esto ayuda a los equipos a corregir vulnerabilidades, prepararse para las auditorías y garantizar el cumplimiento normativo.

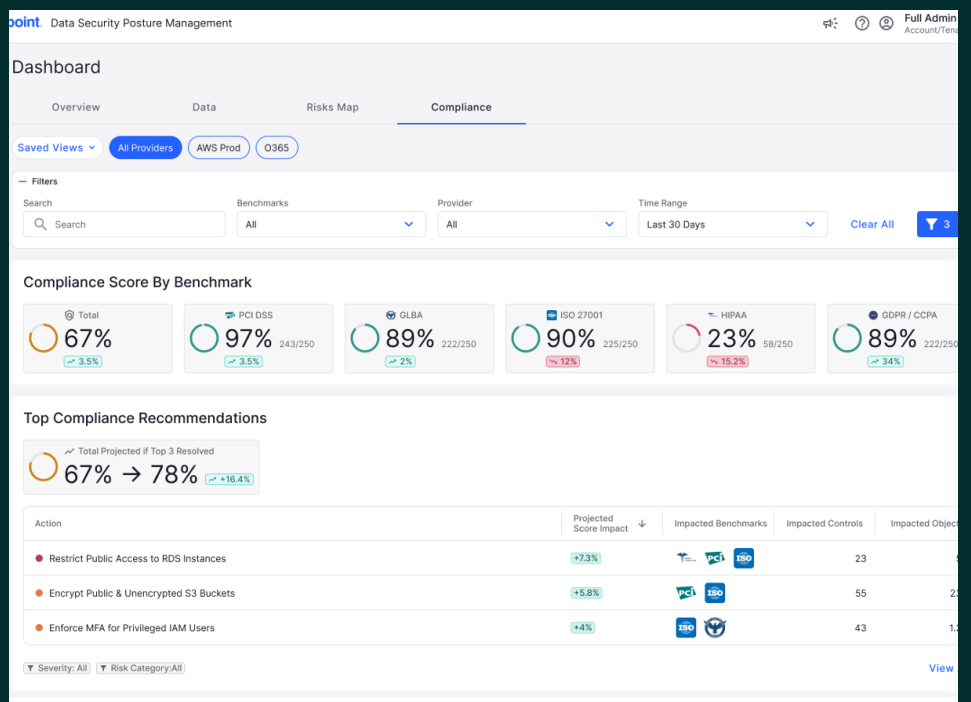


Figura 3. Panel con una vista destacada del estado de cumplimiento.

Reduzca los riesgos de exposición de los datos a la IA

Proofpoint DSPM ayuda a las organizaciones a ampliar el uso de la IA al localizar los datos sensibles a los que pueden acceder las aplicaciones y los flujos de trabajo de IA.

Proofpoint DSPM proporciona al panel de control de Proofpoint Data Security for AI información sobre la exposición. El panel ofrece una visión centralizada de los riesgos para los datos en aplicaciones de IA autorizadas y no autorizadas. Proofpoint DSPM también supervisa las aplicaciones de IA para detectar errores de configuración y ayuda a los equipos a corregirlos. Esto reduce el riesgo de fugas, fortalece el gobierno de los datos de IA y apoya la adopción segura.

Proofpoint DSPM protege los LLM personalizados y las aplicaciones de IA desplegadas en plataformas como AWS Bedrock y Azure ML. Detecte los datos sensibles incorporados a modelos base, modelos personalizados y flujos de trabajo de generación aumentada por recuperación (RAG).

Proofpoint DSPM también ofrece API especializadas en la seguridad de los LLM. Estas API analizan en tiempo real los datos sensibles que entran y salen de los LLM. También ofrecen funciones de gobierno y visibilidad del uso de los datos, y se integran en los flujos de trabajo de los clientes.

Plataformas y tecnologías compatibles

Proofpoint DSPM localiza y clasifica datos en numerosas plataformas y servicios. Es compatible con una amplia variedad de repositorios de datos, desde bases de datos relacionales y NoSQL hasta almacenes de clave-valor. Esto proporciona a los equipos visibilidad sobre los datos estructurados, no estructurados y semiestructurados.

Es compatible con las principales plataformas de nube y SaaS. Entre los ejemplos figuran AWS, Azure, Google Cloud Platform (GCP), Snowflake, Salesforce, ServiceNow, Workday, los LLM y los copilotos.

El marco común de descubrimiento y clasificación permite a Proofpoint ofrecer rápidamente compatibilidad con nuevos repositorios de datos.

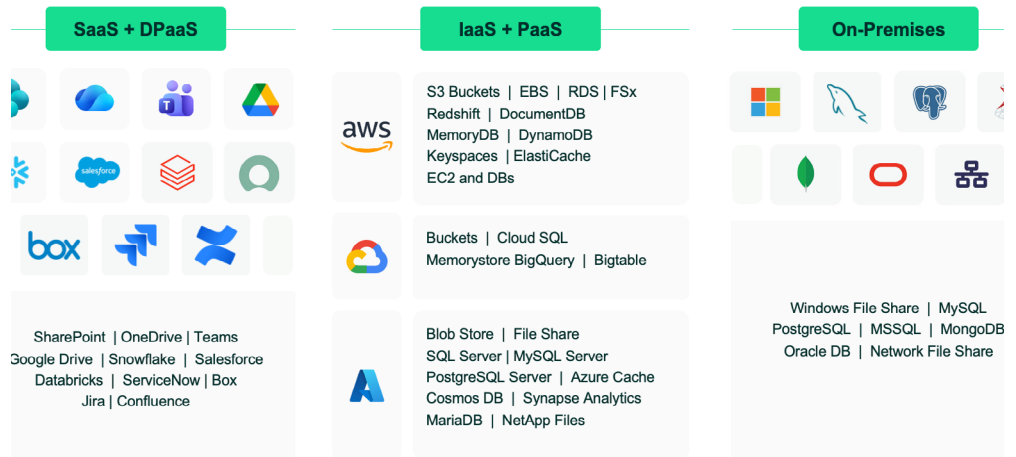


Figura 4. Proofpoint DSPM localiza y clasifica datos en una amplia variedad de plataformas y servicios.

Conclusión

A medida que las organizaciones adoptan la IA y aumenta el volumen de datos que gestionan, necesitan saber dónde se encuentran sus datos sensibles, quién puede acceder a ellos y cómo se utilizan. Proofpoint DSPM reduce la exposición al clasificar los datos sensibles, priorizar los riesgos, detectar accesos excesivos y aplicar el principio del mínimo de privilegios posible en entornos de nube, SaaS, locales y de IA.

Como parte de Proofpoint Data Security, Proofpoint DSPM funciona conjuntamente con Proofpoint Enterprise DLP. Juntos, ayudan a los equipos a localizar, clasificar, gobernar y proteger los datos sensibles. Las organizaciones pueden reforzar el cumplimiento normativo, adoptar la IA de forma segura, reducir el riesgo y proteger su información más valiosa.

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 responsabilizar a sus empleados, al tiempo que adoptan la IA de forma segura y con total confianza. Más información en www.proofpoint.com/es.

Conecte con Proofpoint: [LinkedIn](#)

Proofpoint es una marca registrada o nombre 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