

Proofpoint Cloud DLP

Disfrute de visibilidad y control sobre los datos sensibles en las aplicaciones cloud

Ventajas principales

- Obtenga visibilidad sobre las amenazas en la nube, los movimientos sospechosos de datos, la exposición de los datos en la nube y el uso de riesgo de las aplicaciones cloud.
- Proteja los datos sensibles mediante funciones de prevención de la pérdida de datos (DLP) que abarcan tanto el contenido como el comportamiento y la telemetría de amenazas.
- Simplifique las operaciones de DLP en la nube, el correo electrónico, la web y los endpoints gracias a un gestor de alertas unificado.
- Protéjase contra la apropiación de cuentas, el uso indebido de aplicaciones OAuth, los accesos persistentes y los ataques basados en archivos.
- Detecta los riesgos internos relacionados con la nube mediante modelos de aprendizaje automático diseñados para detectar descargas, usos compartidos y filtraciones de datos inusuales.
- Acelera la corrección con acciones automatizadas que eliminan los recursos compartidos, limitan los permisos, bloquean las cuentas, revocan el acceso OAuth y neutralizan los riesgos.

Proofpoint Cloud DLP adopta un enfoque centrado en las personas para proteger los datos sensibles y a los usuarios frente a las amenazas en la nube. Esto permite realizar un seguimiento de la exposición de datos, gobernar el uso de aplicaciones SaaS y controlar el acceso de aplicaciones OAuth de terceros.

La seguridad en la nube comienza por proteger las aplicaciones autorizadas por el departamento de TI que albergan sus datos más valiosos, como Microsoft 365, Google Workspace, Salesforce y Box. Proofpoint Cloud DLP ofrece una visibilidad centrada en las personas sobre las amenazas en la nube, la exposición de datos, el comportamiento de los usuarios y el movimiento de los datos. Esto ayuda a las organizaciones a crear y mantener una postura sólida de seguridad en la nube.

Como parte de la plataforma de seguridad de datos dev Proofpoint, Cloud DLP correlaciona las amenazas con el comportamiento de los usuarios y aplica políticas de DLP coherentes en aplicaciones, correo electrónico, la web y endpoints.

Proofpoint Cloud DLP le ayuda a detener el intercambio excesivo y la pérdida de datos sensibles, reducir el riesgo interno y reducir el comportamiento de riesgo del usuario. Gracias a esta solución, podrá protegerse contra los ataques de suplantación de cuentas, los archivos maliciosos y el uso indebido de OAuth.

Ampliación de la visibilidad centrada en las personas a las aplicaciones cloud

Proofpoint Cloud DLP le ofrece visibilidad sobre las amenazas en la nube y el correo electrónico. Le ayudamos a identificar a las personas más atacadas, Very Attacked People™ (VAP) y proteger sus datos y cuentas cloud. Puede identificar los archivos que incumplen las normas DLP, así como a los usuarios que son sus propietarios y a todos aquellos que los descargan, los comparten y los modifican. Sus potentes herramientas de análisis y controles adaptativos le ayudan a conceder los niveles de acceso adecuados a los usuarios y a las aplicaciones OAuth de terceros en función de los factores de riesgo que considere más importantes.

Protección de los usuarios, las aplicaciones y los datos frente a las amenazas en la nube

Proofpoint Cloud DLP combina el contexto del usuario con la inteligencia sobre amenazas multicanal de Proofpoint Behavior Graph. El aprendizaje automático y la correlación de amenazas le ayudan a detectar cuándo una cuenta cloud ha sido comprometida y se está utilizando para actividades sospechosas: por ejemplo, el envío o la transferencia de correos electrónicos o la filtración de datos.

El panel de control intuitivo de Proofpoint Cloud DLP le permite examinar las alertas relacionadas con conexiones sospechosas, actividades relacionadas con archivos y funciones de administración. Puede exportar datos forenses a una solución de administración de información y eventos de seguridad (SIEM) para su análisis detallado, manualmente o con las API REST.

Gracias a las políticas rigurosas, las alertas en tiempo real y las respuestas automatizadas de Proofpoint Cloud DLP, podrá:

- Proteger su entorno contra la usurpación de cuentas cloud y suspender las cuentas comprometidas.
- Implementar una autenticación basada en el riesgo y controles de acceso adaptativos.
- Prevenir el robo de datos y el uso indebido de aplicaciones OAuth mediante la identificación y la revocación de los accesos de terceros que supongan un riesgo.

- Detectar y poner en cuarentena los archivos maliciosos.
- Eliminar los permisos y los recursos compartidos de archivos inadecuados.
- Limitar el acceso a contenidos sensibles.
- Bloquear las cuentas de usuario y automatizar los flujos de corrección.
- Analizar y neutralizar las actividades sospechosas en las cuentas cloud.

Proofpoint Cloud DLP también permite identificar los riesgos internos en la nube. Unos modelos de aprendizaje automático especializados detectan los comportamientos que suelen asociarse a las amenazas internas y a los empleados que abandonan la empresa. Podemos citar, por ejemplo, descargas anómalas, uso compartido excesiva, patrones inusuales de acceso a los datos o incluso la posible filtración de datos, en comparación con la actividad habitual a nivel de los usuarios o de la empresa en su conjunto.

El módulo complementario (add-on) SaaS Isolation también le permite proteger a los usuarios, aplicar reglas de DLP a los dispositivos no gestionados e integrar tu solución de gestión de identidades mediante la autenticación SAML (Security Assertion Markup Language).

Normas de DLP unificadas en todos los canales

Proofpoint Cloud DLP comparte los clasificadores DLP con otras soluciones de seguridad de datos de Proofpoint. Entre ellos se incluyen identificadores inteligentes integrados, diccionarios, reglas, plantillas y clasificadores autónomos personalizados (ACC) que utilizan grandes modelos de lenguaje (LLM) para detectar y clasificar automáticamente el contenido sensible específico de la organización.

Esta función compartida le ayuda a identificar y proteger los datos sensibles más rápidamente. En el marco de la plataforma de seguridad de datos de Proofpoint, puede implementar reglas de DLP coherentes en aplicaciones SaaS, correo electrónico, la web y los endpoints.

Combinamos datos de análisis de contenido, de comportamientos y de amenazas de estos canales.

Esto le ayuda a determinar si el usuario que activó la alerta de DLP ha sido víctima de un ataque, o bien si actúa de manera negligente o malintencionada. Del mismo modo, puede unificar la gestión de las alertas de DLP en varios canales.

Más de 240 clasificadores integrados abarcan los datos sujetos a la norma PCI, al RGPD y a la normativa sobre datos de identificación personal e información sanitaria. Las tecnologías avanzadas de detección le permiten crear controles personalizados, como la correspondencia exacta de datos y políticas contextuales. Además, puede restringir el acceso a los datos desde dispositivos no gestionados, impedir la descarga de archivos confidenciales a aplicaciones cloud no autorizadas y limitar los permisos de uso compartido excesivos. También puede identificar los archivos sensibles que están muy expuestos y relacionar las actividades de conexión sospechosas con los incidentes de DLP.

Administración de aplicaciones cloud y de terceros

Proofpoint Cloud DLP detecta las aplicaciones de TI no autorizadas (Shadow IT) e identifica las aplicaciones cloud que se utilizan en su empresa. Nuestro catálogo cuenta con 46 000 apps. Cada aplicación tiene más de 50 atributos. Y puede clasificar las aplicaciones cloud por tipo y puntuación de riesgo. Esto le permite identificar riesgos de seguridad, vulnerabilidades que pueden provocar pérdidas de datos e incumplimientos normativos. Puede bloquear las aplicaciones que presentan riesgos o conceder a los usuarios acceso de solo lectura a ellas.

También detectamos y evaluamos los permisos OAuth para aplicaciones de terceros, y los scripts que acceden a sus servicios cloud principales, aprobados por el departamento de TI. Su función de análisis permite identificar las aplicaciones que presentan riesgos y reducir tu superficie de ataque. Puede definir o automatizar acciones según la puntuación de riesgo y el contexto.

Despliegue rápido

Nuestra arquitectura multimodal le permite rentabilizar su inversión más rápidamente. En menos de cuatro semanas, puede integrar la solución con API en la nube, herramientas híbridas de gestión de identidades y productos de orquestación de la seguridad (entre ellos, Proofpoint Threat Response).

Esta integración le permitirá detectar automáticamente las amenazas, contenerlas y proteger los datos. La autenticación SAML basada en el riesgo y la función SaaS Isolation ayudan a bloquear el acceso no autorizado a las aplicaciones de la empresa y son compatibles con las estrategias BYOD.

Las ventajas de Proofpoint Cloud DLP

Proofpoint Cloud DLP combina, en una única solución, la protección de datos, la defensa frente a amenazas en la nube, la detección de riesgos internos, la visibilidad de la exposición de los datos en la nube y los controles adaptativos centrados en las personas. Al integrar la actividad en la nube, el comportamiento de los usuarios, la inteligencia sobre amenazas y la telemetría de DLP, las organizaciones pueden proteger mejor la información confidencial y, al mismo tiempo, reducir la complejidad operativa.

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 responsabilizar a sus empleados, al tiempo que adoptan la IA de forma segura y con
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