

RESUMEN DE LA SOLUCIÓN

Proofpoint Data Security Posture Management para Snowflake

Proteja su entorno DPaaS (Data Platforms-as-a-Service) en plena expansión

Ventajas principales

- Visibilidad de datos a gran escala
- Aplicación del principio de privilegios mínimos
- Reducción de la superficie de ataque
- Cumplimiento continuo

Snowflake ha transformado la forma en que las empresas gestionan las cargas de trabajo de Big Data. Les ayuda a recopilar, almacenar y analizar grandes volúmenes de datos de forma más rentable. Sin embargo, para los equipos responsables de la seguridad y los datos, Snowflake dificulta la gestión del movimiento, la clasificación y el acceso a los datos. Estos retos aumentan el riesgo de compromiso y los problemas de gobierno.

Proofpoint Data Security Posture Management (DSPM) maximiza el valor de su inversión en Snowflake. Simplifica la forma en que los equipos de seguridad y datos proporcionan a los usuarios los datos que necesitan. Resuelve problemas como el rápido crecimiento de los datos,

la complejidad de su clasificación y los excesivos privilegios de acceso. También garantiza el cumplimiento y el gobierno continuos, algo que no ofrecen las herramientas inadecuadas de gestión de riesgos.

Además de su funcionalidad principal, Proofpoint DSPM se integra perfectamente con AI Data Cloud de Snowflake, lo que le permite aprovechar las capacidades de seguridad y cumplimiento de Snowflake Horizon. Proofpoint le ofrece un mayor control sobre su entorno Snowflake, que acelera la adopción de tecnologías de Snowflake y funciones avanzadas como la IA.

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

Gobierno del acceso

- Visibilidad y control

La necesidad de un gobierno permanente del acceso y la clasificación de datos a gran escala

Snowflake ofrece una flexibilidad y escalabilidad excepcionales. Sin embargo, estas ventajas también se traducen en una multiplicación de los movimientos de datos, estructuras de acceso complejas y un exceso de datos compartidos. Por ello, los equipos responsables de la seguridad y la protección de datos pueden enfrentarse a una serie de retos:

Conflicto entre la concesión de acceso y la prevención de riesgos: si los equipos de datos son responsables de conceder a los usuarios acceso a grandes conjuntos de datos, los equipos de seguridad deben garantizar que estos usuarios sólo acceden a los datos que están autorizados a ver y utilizar.

Incapacidad para clasificar los datos: la rápida afluencia de datos no estructurados dificulta enormemente la clasificación continua. Los equipos de seguridad se esfuerzan por aplicar controles de acceso y supervisar a los usuarios que podrían intentar acceder a datos estratégicos o sensibles.

Ocultación de datos estratégicos o sensibles: los datos no estructurados, como los blobs JSON y los resultados generados por IA, dificultan la identificación de la ubicación de datos estratégicos o sensibles, dificultando el acceso a los datos y su control.

Características exclusivas de Proofpoint DSPM

En los entornos Snowflake, las dificultades asociadas a la gestión del movimiento, la clasificación y el acceso a los datos aumentan el riesgo de que estos se vean comprometidos y los problemas de gobierno. Proofpoint DSPM resuelve estos retos con funciones exclusivas:

Identificación continua y clasificación precisa: obtenga visibilidad total de los datos críticos en todo momento. El análisis de un solo paso de Proofpoint DSPM permite una identificación rápida

y continua y una clasificación precisa de sus datos. No es necesario realizar ninguna configuración o ajuste manual.

Gobernanza del acceso: utilice gráficos dinámicos detallados para ver cómo acceden a los datos su personal y sus recursos. Determine quién tiene acceso a bases de datos específicas y determinar si dispone de las autorizaciones apropiadas. Identificar a los usuarios inactivos, mal configurados o sobreadicionados. Asegúrese de que los usuarios sólo tienen acceso a los datos que necesitan.

Gestión de las credenciales de inicio de sesión: identifique a los usuarios que tienen acceso a datos estratégicos y sensibles, pero que no están sujetos a determinadas medidas de seguridad esenciales (como la autenticación multifactor). Aplique reglas de autenticación más estrictas a estos usuarios.

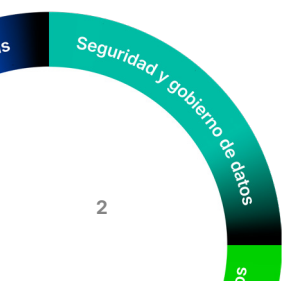
Gestión de riesgos: identifique las vías de ataque susceptibles de conducir a un compromiso o fuga de datos. Visualice gráficos en tiempo real que priorizan sus riesgos según el valor de los datos y la probabilidad de éxito de los ataques. Ponga un valor monetario a sus datos, con clasificaciones diseñadas para ayudar a los equipos de seguridad y datos a evaluar las consecuencias de posibles fugas de datos. Reduzca su superficie de ataque y recorte sus costes de almacenamiento identificando los datos abandonados. Supervise constantemente la actividad anómala, como picos inesperados en las descargas de datos o accesos desde lugares inusuales. Utilice esta información para resolver más rápidamente los problemas de alto riesgo.

Cumplimiento de datos: anticipése a los retos normativos y reduzca los riesgos con herramientas avanzadas diseñadas para admitir protocolos de cumplimiento rigurosos como ISO 27001, SOC 2 y PCI DSS, NIST CSF 2.0 y Snowflake CIS Benchmark.

Arquitectura de análisis in situ: confíe plenamente en la seguridad de sus datos. Proofpoint DSPM se ejecuta como una aplicación nativa de Snowflake y despliega escáneres dentro de su entorno. Esto garantiza que sus datos nunca salgan de su perímetro de seguridad.

Funciones únicas

- Contexto de datos
- Gobierno de acceso a los datos
- Cumplimiento de datos



Maximice el valor de su inversión en Snowflake

Al optimizar los flujos de trabajo de sus equipos de datos y seguridad, Proofpoint DSPM le ayuda a maximizar el valor de su inversión en Snowflake.

Uso optimizado de las tecnologías

Snowflake: Proofpoint DSPM hace que el uso de los datos sea más seguro para una amplia gama de usuarios en toda su organización. Esto permitirá a los clientes de Snowflake aprovechar mejor la pila tecnológica de Snowflake, incluidas sus capacidades de IA.

Reduzca el número de incógnitas:

Proofpoint DSPM elimina los puntos de fricción entre los datos y los equipos de seguridad al agilizar el proceso de concesión de niveles adecuados de acceso a los usuarios. Así puede estar seguro de que sus datos son accesibles y están protegidos.

Contextualización de Zero Trust y requisitos de cumplimiento:

Proofpoint DSPM admite la implementación del modelo Zero Trust (de confianza cero) y otros marcos de seguridad mediante la clasificación precisa de datos críticos y confidenciales y la gestión eficaz del acceso de los usuarios.

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](#)

Proofpoint es una 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 →