Zscaler Data Security Posture Management (DSPM)

Resumen de la solución

Descripción general: Protección de datos en un mundo centrado en la nube

Los desafíos que plantea la protección de grandes cantidades de datos empresariales en entornos de múltiples nubes incluyen la gestión de la complejidad y la escala de la protección de datos; hacer frente a las amenazas internas, las violaciones de datos, el acceso de terceros y proveedores, y los riesgos de la cadena de suministro; y cumplir las normativas en materia de datos. Las organizaciones tienen dificultades para inventariar, clasificar, controlar y proteger los activos de datos críticos al tiempo que los protegen de diversas amenazas. Esta complejidad se ve agravada por una gran variedad de ubicaciones de datos, funciones y permisos fragmentados en distintos entornos.

Entornos complejos	Volumen de datos	Ataques sofisticados y dirigidos	Acceso con privilegios excesivos
el 82 % de las violaciones afectan a datos almacenados en la nube.	Se estima que 175 ZB de datos se almacenarán en la nube en 2025[2]	4.88 millones de dólares – El costo promedio mundial de una violación de datos en 2024[3]	El 80 % de las organizaciones han sufrido violaciones de identidad[4]

Lamentablemente, las soluciones de protección de datos heredadas no se diseñaron para entornos dinámicos de múltiples nubes. Al mismo tiempo, los proveedores de DSPM puntuales están ofreciendo enfoques aislados que no se integran perfectamente en los programas de protección de datos existentes. Las organizaciones necesitan un nuevo enfoque unificado para proteger sus datos en la nube.

Zscaler resuelve estos desafíos de seguridad de datos en entornos multinube con una solución de gestión de la postura de seguridad de datos (DSPM) sin agentes y totalmente integrada.

¿Qué es DSPM?

"Data security posture management (DSPM) ofrece visibilidad sobre dónde están los datos confidenciales, quién tiene acceso a esos datos, cómo se han utilizado y cuál es la postura de seguridad de los datos almacenados o de la aplicación". —Gartner®

A veces se hace referencia a DSPM como seguridad que prioriza los datos, invirtiendo el modelo de protección adoptado por otras tecnologías y prácticas de ciberseguridad. En lugar de proteger los dispositivos, sistemas y aplicaciones que albergan, mueven o procesan datos, DSPM se centra en proteger los datos directamente, sin dejar de complementar muchas otras soluciones de la pila de seguridad de una organización.

Más concretamente, la DSPM implica la supervisión, evaluación y optimización continuas de los controles de seguridad para proteger los datos confidenciales en todas las plataformas multinube. Al automatizar la identificación de los datos confidenciales, así como de cualquier vulnerabilidad potencial, error de configuración o violación de la normativa, DSPM permite a las organizaciones abordar de manera proactiva el riesgo de exposición de los datos. Al hacerlo, DSPM les ayuda a reforzar la postura general de seguridad de los datos, minimizar el riesgo de violaciones de datos y satisfacer los requisitos de cumplimiento normativo.

1. https://www.informationweek.com/cyber-resilience/data-breaches-just-keep-piling-up
2. https://www.forbes.com/sites/tomcoughlin/2018/11/27/175-zettabytes-by-2025/
3. https://www.ibm.com/reports/data-breach
4. https://www.darkreading.com/cybersecurity-operations/identity-related-breaches-last-12-months

Why DSPM?

El principal objetivo de las herramientas DSPM es evaluar y gestionar el estado de seguridad del entorno de datos de una organización mediante la búsqueda de puntos débiles, la supervisión de los ajustes de seguridad y la identificación de posibles amenazas a los datos confidenciales. La DSPM va más allá de la mera política para examinar los propios datos.

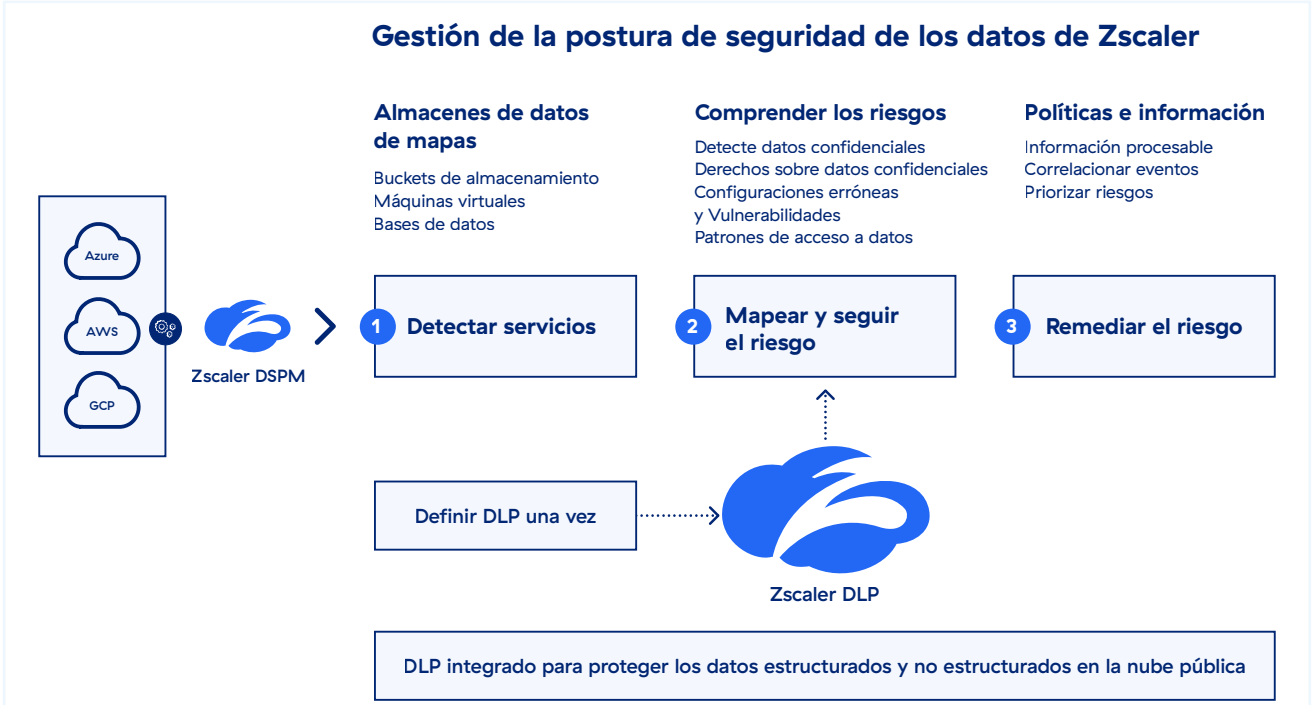
Al escanear y categorizar los datos, ayuda a las organizaciones a comprender plenamente dónde se encuentran los datos confidenciales y cómo se están utilizando. También ayuda a priorizar los problemas identificados y evita la acumulación de alertas que podrían llevar a pasar por alto dichos problemas.

Los casos prácticos de uso de DSPM incluyen la detección de vulnerabilidades de seguridad (como el cifrado) en entornos de nube, la aplicación de políticas de acceso y la provisión de alertas y capacidades de investigación para la gestión de incidentes.

Le presentamos Zscaler DSPM

Zscaler AI Data Protection es la plataforma de protección de datos más completa y totalmente integrada del mundo. Protege tanto los datos estructurados como los no estructurados en la web, los servicios basados en SaaS, los entornos de nube pública (AWS, Azure), las aplicaciones privadas, el correo electrónico y los puntos finales.

Como parte de la plataforma Zscaler, Zscaler DSPM extiende una seguridad de datos robusta, la mejor de su clase, a la nube pública. Proporciona visibilidad granular de los datos de la nube, clasifica e identifica los datos y el acceso, y contextualiza la exposición de los datos y la postura de seguridad, facultando a los equipos de seguridad para prevenir y remediar las violaciones de datos de la nube a escala.



Utilizando un único motor DLP unificado, Zscaler DSPM ofrece una protección de datos uniforme en todos los canales. Al realizar un seguimiento de todos los usuarios en todas las ubicaciones y controlar los datos tanto en uso como en reposo, garantiza que los datos confidenciales estén perfectamente protegidos y que se cumpla la normativa.

Capacidades principales de Zscaler DSPM

Detección, clasificación e inventario de datos
Los métodos de escaneado tradicionales son caros y requieren un esfuerzo significativo para producir resultados útiles. Zscaler DSPM, con un acceso mínimo a los recursos en entornos de nube (AWS, Azure y GCP), escanea los almacenes de datos, detecta los datos confidenciales y clasifica los datos con precisión. Ayuda con lo siguiente:

- **Detección exhaustiva de datos:** Zscaler DSPM supervisa constantemente los entornos de nube para detectar automáticamente nuevos almacenes de datos a medida que se instancian en entornos de datos cambiantes para ahorrar tiempo y eliminar los puntos ciegos de datos.
- **Clasificación precisa de los datos:** Zscaler DSPM utiliza motores y diccionarios DLP predefinidos para la clasificación de datos. Ofrece visibilidad sobre qué tipo de datos confidenciales se almacenan en los recursos de la nube, la región, los archivos que contienen datos confidenciales, la gravedad del riesgo asociado a los datos confidenciales, etc. También ofrece flexibilidad a las organizaciones para crear o replicar las políticas existentes que estén disponibles.
- **Inventario de datos preciso:** Zscaler DSPM crea un mapa y un inventario precisos de los activos de datos, lo que ayuda a los equipos de seguridad a localizar los datos confidenciales y a comprender quién tiene acceso a ellos y cómo se están utilizando.

Con Zscaler DSPM, los equipos de seguridad obtienen una mayor visibilidad de los datos dentro de la infraestructura de la nube. Esto hace que sea mucho más fácil gestionar y mejorar la postura de seguridad de los datos de los entornos multinube, que abarcan capas complejas de SaaS, PaaS, IaaS y bases de datos.

Mapa y seguimiento de exposiciones de datos

Los servicios en la nube y las configuraciones cambian con frecuencia, lo que puede provocar la exposición de los datos. Es esencial solucionar estas brechas de seguridad antes de que los malintencionados puedan explotarlas. Zscaler DSPM detecta los recursos expuestos públicamente así como las vulnerabilidades o configuraciones erróneas en los diferentes componentes (grupo de seguridad de red, equilibrador de carga, red virtual, etc.) asociados al recurso de datos. Esto ayuda con lo siguiente:

- **Análisis de la exposición:** Determine la exposición pública, las configuraciones erróneas y las vulnerabilidades de los almacenes y servicios de datos.
- **Evaluación de riesgos:** Calcule el nivel general de riesgo combinando el impacto y la probabilidad. Esto implica clasificar los riesgos en niveles alto, medio o bajo.
- **Priorización de riesgos:** Ayude a los equipos de seguridad a filtrar y priorizar los incidentes en función del riesgo y la gravedad.
- **Correlación avanzada de amenazas:** Correlacione las amenazas, los factores de riesgo y las rutas de ataque ocultas para minimizar el riesgo.
- **Inteligencia de acceso adaptable:** Obtenga una visión granular, basada en los riesgos y centrada en el usuario de todas las rutas de acceso a los datos y configuraciones de misión crítica.

Remediación de riesgos

Zscaler DSPM agiliza la gestión de riesgos con una corrección guiada basada en el contexto, lo que permite a los equipos de seguridad solucionar fácilmente los problemas y las violaciones en su origen, evitando futuras interrupciones. Las capacidades incluyen:

- **Investigación y respuesta eficaces** para ayudar a los equipos de seguridad a comprender rápidamente las posibles causas fundamentales durante las investigaciones de eventos de seguridad de datos.
- **Remediación guiada en profundidad** para ayudar a los equipos multifuncionales con flujos de trabajo automatizados y orientación paso a paso con contexto completo para abordar el riesgo de seguridad de los datos y remediarlo de manera efectiva.
- **Tiempo de seguridad más rápido**, que permite a los equipos configurar alertas personalizadas en tiempo real para mantenerse al día con los cambios rápidos en los datos y su entorno, acelerando la investigación y la respuesta.
- **Integración sin fisuras** para una integración sencilla con las herramientas y plataformas ITSM, SIEM o ChatOps existentes para alertas, corrección, orientación y flujos de trabajo.

Descubra Zscaler DSPM

Solicite una demostración
Conozca Zscaler DSPM en acción con una demostración guiada.

Solicitar una demostración

Descargue la Guía del comprador de DSPM
Conozca los 5 requisitos principales a tener en cuenta al seleccionar la DSPM adecuada para su organización.

Descargar ahora

Para más información, vaya a zscaler.com/mx/dp/dspm.

Anexo

Glosario de términos

- Gestión de la postura de seguridad de datos (DSPM)
- Plataforma de protección de aplicaciones nativas de la nube (CNAPP)
- Cloud Security Posture Management (CSPM)
- Gestión de derechos de infraestructura en la nube (CIEM)

Más información

Escanee el código QR para acceder a los recursos de DSPM

Sesiones a la carta

- Ponencia principal: Sesión Zenith Live '24, Zscaler DSPM: Asegure los datos de la nube con una plataforma totalmente integrada. Conozca la experiencia de Inter&Co con DSPM.
- Seminario web: "¿Por qué la DSPM debe ser parte su estrategia de protección de datos?"

+1 408.533.0288 Zscaler, Inc. (Oficinas centrales) • 120 Holger Way • San José, CA 95134 zscaler.com/mx