Zscaler Data Security Posture Management (DSPM)

Resumen de la solución

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

Los desafíos de proteger grandes cantidades de datos comerciales en entornos multinube incluyen la gestión de la complejidad y la escala de la protección de datos, la gestión de amenazas internas, infracciones de datos, acceso de terceros y proveedores y riesgos de la cadena de suministro, y el cumplimiento de las regulaciones de datos. Las organizaciones luchan por inventariar, clasificar, controlar y proteger activos de datos críticos mientras los protegen de diversas amenazas. Esta complejidad se ve agravada por una multitud de ubicaciones de datos, roles y permisos fragmentados en diferentes entornos.

Entornos complejos	Volumen de datos	Ataques sofisticados y dirigidos	Acceso sobreprivilegiado
El 82 % de las infracciones implicaron datos almacenados en la nube[1]	Se estima que 175 ZB de datos se almacenarán en la nube en 2025[2]	4,88 millones de dólares estadounidenses: el coste medio mundial de una filtración de datos en 2024[3]	El 80 % de las organizaciones han sufrido infracciones de identidad[4]

Desafortunadamente, se ha demostrado que las soluciones heredadas de protección de datos no están diseñadas para entornos multinube dinámicos. Mientras tanto, los proveedores puntuales de DSPM ofrecen enfoques aislados que no logran integrarse correctamente en los programas de protección de datos existentes. Las organizaciones necesitan un enfoque nuevo y 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) totalmente integrada y sin agentes.

¿Qué es DSPM?

"Data Security Poture Management (DSPM) proporciona visibilidad sobre dónde se encuentran los datos confidenciales, quién tiene acceso a dichos 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, al tiempo que complementa muchas otras soluciones en la pila de seguridad de una organización.

Específicamente, DSPM implica la supervisión, evaluación y optimización continuas de los controles de seguridad para proteger datos confidenciales en plataformas multinube. Al automatizar la identificación de datos confidenciales, vulnerabilidades potenciales asociadas, errores de configuración e infracciones de cumplimiento, DSPM garantiza que las organizaciones aborden de manera proactiva el riesgo de exposición de datos. Al hacerlo, DSPM les ayuda a fortalecer la postura general de seguridad de datos, minimizar el riesgo de infracciones de datos y cumplir con 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

¿Por qué DSPM?

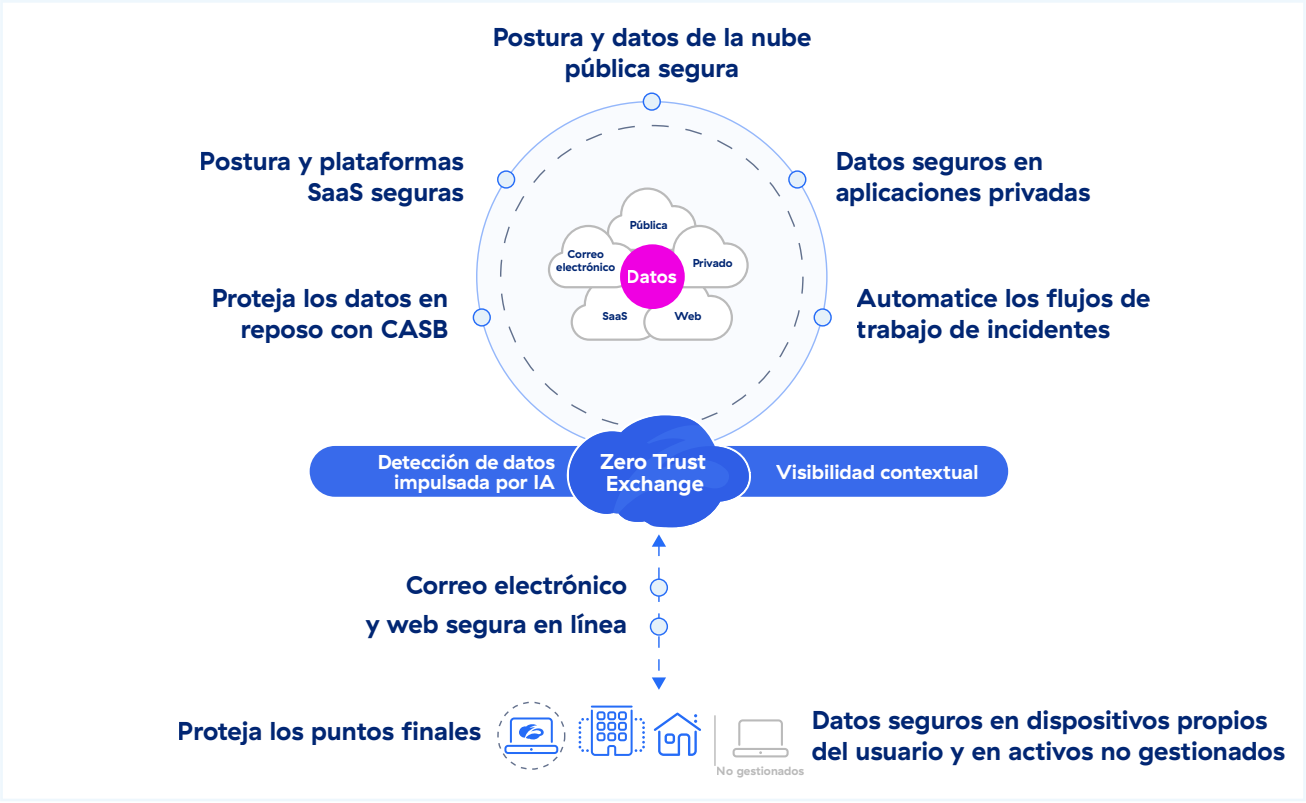
El enfoque principal de las herramientas DSPM es evaluar y gestionar el estado de seguridad del entorno de datos de una organización mediante la búsqueda de debilidades, la supervisión de configuraciones de seguridad y la identificación de amenazas potenciales a datos confidenciales. DSPM va más allá de la mera política y analiza los datos reales.

Al analizar y categorizar los datos, ayuda a las organizaciones a comprender completamente dónde se encuentran los datos confidenciales y cómo se utilizan. También ayuda a priorizar los problemas identificados y evita alertas abrumadoras que podrían hacer que se pasen por alto dichos problemas.

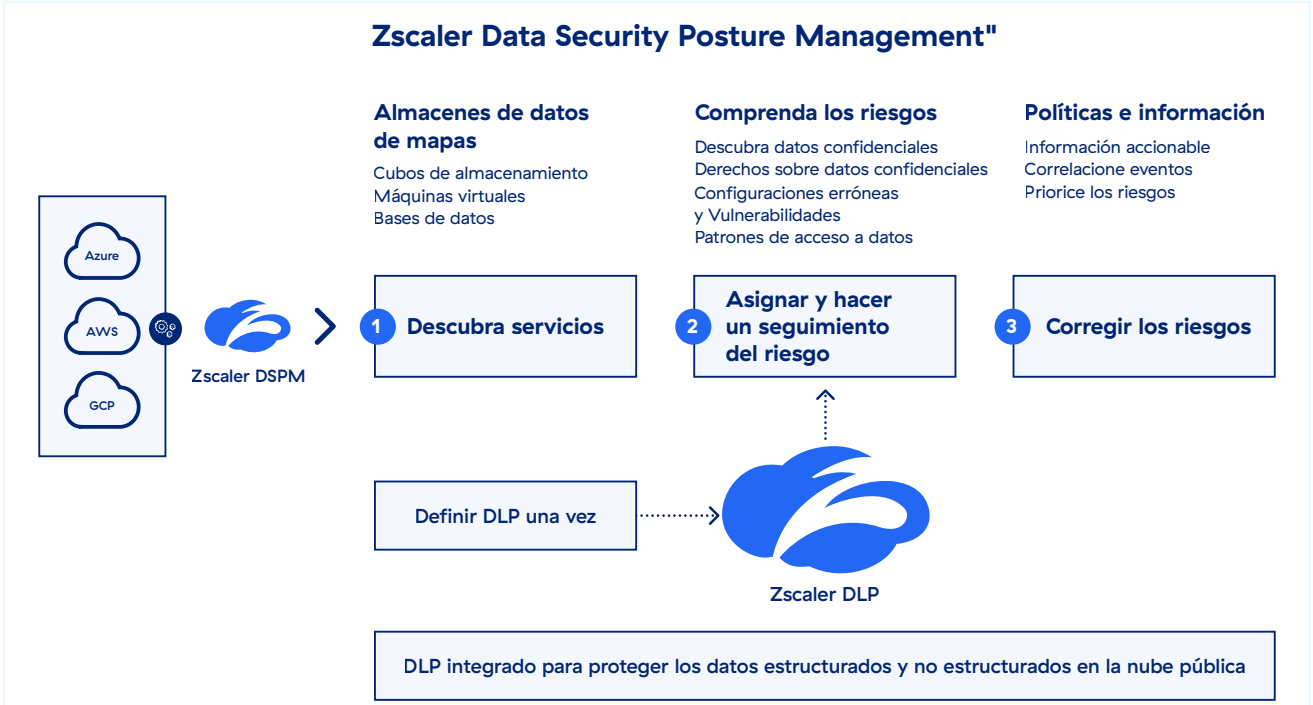
Los casos de uso prácticos de DSPM incluyen la detección de vulnerabilidades de seguridad (como el cifrado) en entornos de nube, la aplicación de políticas de acceso y el suministro de alertas y capacidades de investigación para la gestión de incidentes.

Conozca Zscaler DSPM

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



Como parte de la plataforma Zscaler, Zscaler DSPM extiende la seguridad de datos sólida y de primera clase a la nube pública. Proporciona visibilidad granular de los datos en la nube, clasifica e identifica los datos y el acceso, y contextualiza la exposición de los datos y la postura de seguridad, lo que permite a los equipos de seguridad prevenir y remediar las infracciones de datos en la nube a gran escala.



Al utilizar un único motor DLP unificado, Zscaler DSPM ofrece protección de datos consistente en todos los canales. Al seguir a todos los usuarios en todas las ubicaciones y controlar los datos en uso y en reposo, se garantiza que los datos confidenciales estén perfectamente protegidos y se logre el cumplimiento.

Capacidades básicas de Zscaler DSPM

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

- **Descubrimiento integral de datos:** Zscaler DSPM supervisa constantemente los entornos de nube para descubrir automáticamente nuevos almacenes de datos a medida que se instancian en entornos de datos en constante cambio para ahorrar tiempo y eliminar puntos ciegos de datos.
- **Clasificación precisa de 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 con los datos confidenciales, etc. También ofrece flexibilidad a las organizaciones para crear o replicar las políticas existentes que están disponibles.
- **Inventario de datos preciso:** Zscaler DSPM crea un mapa preciso y un inventario de activos de datos, lo que ayuda a los equipos de seguridad a localizar datos confidenciales y comprender quién tiene acceso a ellos y cómo se utilizan.

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 administrar y mejorar la postura de seguridad de datos de entornos multinube, que abarcan capas complejas de SaaS, PaaS, IaaS y bases de datos.

Exposición de datos de mapas y seguimiento

Los servicios y configuraciones en la nube cambian con frecuencia, lo que puede dar lugar a exposición de datos. Es fundamental corregir estas brechas de seguridad antes de que los actores maliciosos puedan explotarlas. Zscaler DSPM detecta recursos expuestos públicamente, así como las vulnerabilidades o configuraciones incorrectas en los diferentes componentes (grupo de seguridad de red, balanceador de carga, red virtual, etc.) asociados al recurso de datos. Esto ayuda con:

- **Análisis de exposición:** determine la exposición pública, las configuraciones erróneas y las vulnerabilidades de los servicios y almacenes de datos.
- **Evaluación de riesgos:** se calcula 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 el ruido y priorizar los incidentes según el riesgo y la gravedad.
- **Correlación de amenazas avanzada:** correlacione amenazas, factores de riesgo y rutas de ataque ocultas para minimizar el riesgo.
- **Inteligencia de acceso adaptativa:** obtenga una vista granular, basada en riesgos y centrada en el usuario de todas las rutas de acceso a datos y configuraciones de misión crítica.

Corrección de riesgos

DSPM agiliza la gestión de riesgos con corrección guiada basada en el contexto, lo que permite a los equipos de seguridad solucionar fácilmente problemas e infracciones en el 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 afrontar 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 perfecta** para una fácil integración con herramientas y plataformas ITSM, SIEM o ChatOps existentes para alertas, corrección, orientación y flujos de trabajo.

Experimente Zscaler DSPM

Solicite una demostración
Vea 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 el DSPM adecuado para su organización.

Descargar ahora

Para obtener más información, visite: zscaler.com/es/dspm.

Apéndice

Glosario de términos

- Gestión de la postura de seguridad de los 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 demanda

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

+1 408.533.0288 Zscaler, Inc. (HQ) • 120 Holger Way • San Jose, CA 95134 zscaler.com/es