Proteja los datos de la nube y detenga las infracciones con DSPM de Zscaler

Defina una sola vez y aplique en todas partes con la plataforma de protección de datos más completa y totalmente integrada del mundo

Sus datos en la nube son el nuevo objetivo

El 82 %

El 82 % de las filtraciones de datos han involucrado datos almacenados en entornos de nube

227

El tiempo medio para identificar una infracción de datos es de 227 días

4,45 millones

El coste promedio global de una violación de datos es de 4,45 millones de dólares estadounidenses

"INFORME SOBRE EL ESTADO DE LA GOBERNANZA Y EL EMPODERAMIENTO DE LOS DATOS" ESG, 2022
"INFORME SOBRE EL COSTE DE UNA VULNERACIÓN DE DATOS 2023" IBM SECURITY - 2023

"Para 2026, más del 20 % de las organizaciones implementarán tecnología DSPM [Data Security Protection Management], debido a la apremiante necesidad de identificar y localizar depósitos de datos previamente desconocidos y mitigar los riesgos de seguridad y privacidad asociados".

– Gartner

GARTNER NO RESPALDA A NINGÚN PROVEEDOR, PRODUCTO O SERVICIO DESCRITO EN LAS PUBLICACIONES DE SU INVESTIGACIÓN Y NO RECOMIENDA A LOS USUARIOS DE TECNOLOGÍA QUE SELECCIONEN EXCLUSIVAMENTE AQUELLOS PROVEEDORES CON CALIFICACIONES MÁS ALTAS U OTRA DESIGNACIÓN. LAS PUBLICACIONES DE INVESTIGACIÓN DE GARTNER CONSISTEN EN OPINIONES DE LA ORGANIZACIÓN DE INVESTIGACIÓN DE GARTNER Y NO DEBEN INTERPRETARSE COMO DECLARACIONES DE HECHO. GARTNER RENUNCIA A TODAS LAS GARANTÍAS, EXPRESAS O IMPLÍCITAS, CON RESPECTO A ESTA INVESTIGACIÓN, INCLUIDA CUALQUIER GARANTÍA DE COMERCIABILIDAD O IDONEIDAD PARA UN PROPÓSITO PARTICULAR.

Dificultades de proteger los datos en el mundo centrado en la nube

Los entornos multinube son intrínsecamente complejos y requieren muchos recursos. La gran cantidad de datos que se envían a la nube, combinada con una gran cantidad de usuarios que acceden a diferentes plataformas, cuentas y servicios en la nube, dificulta que las organizaciones comprendan y controlen lo que sucede en la nube.

Los profesionales de la seguridad se enfrentan a cuatro importantes desafíos cuando se trata de proteger los datos en un entorno multinube:

01 LA NUBE ES ÁGIL

La tecnología y los servicios de nube modernos y ágiles ofrecen a los desarrolladores la flexibilidad de colaborar y compartir datos con facilidad, lo que puede resultar en pérdidas de visibilidad y control sobre datos confidenciales.

02 LA NUBE ES COMPLEJA

Se calcula que la cantidad total de datos en la nube aumentará de los 33 ZB actuales a 175 ZB en 2025. Con una dispersión de datos en múltiples plataformas, cuentas y servicios en la nube, las organizaciones luchan por comprender qué servicios, regiones y cuentas en la nube consumen y almacenan datos.

03 DERECHOS EXCESIVOS

Además de los desafíos de descubrir y clasificar datos, los equipos de seguridad también luchan por comprender el acceso a los datos y, simultáneamente, lograr y mantener el cumplimiento de los requisitos de soberanía de los datos, lo que genera enormes brechas de seguridad.

04 FALTA DE CONTEXTO DE DATOS

La sobrecarga de alertas en torno a configuraciones erróneas y vulnerabilidades sin una priorización basada en el contexto de los datos confidenciales genera una mayor fatiga de los recursos y las infracciones de seguridad.

¿Qué impulsa la necesidad de un DSPM integral?

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 perfectamente en los programas de protección de datos existentes. Está claro que las organizaciones necesitan un enfoque nuevo y unificado para proteger sus datos en la nube.

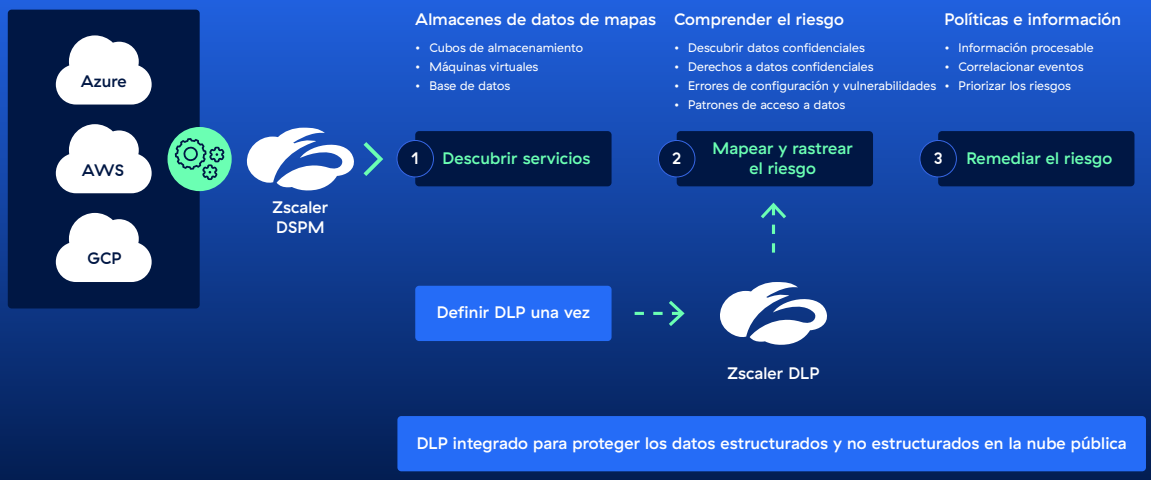
Conozca Data Security Posture Management (DSPM) de Zscaler

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

Como parte de la plataforma Zscaler, Zscaler Data Security Posture Management (DSPM) extiende la seguridad más potente de su clase a sus datos 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, lo que permite a las organizaciones y a los equipos de seguridad prevenir y remediar las filtraciones de datos de la nube a escala.

Utiliza un motor DLP único y unificado para ofrecer una protección de datos uniforme 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.

GESTIÓN DE LA POSTURA DE SEGURIDAD DE DATOS DE ZSCALER



¿Por qué DSPM de Zscaler?

01 UNA PLATAFORMA DE SEGURIDAD DE DATOS UNIFICADA

Zscaler DSPM se integra perfectamente con la plataforma Zscaler AI Data Protection, diseñada específicamente en torno a un motor DLP centralizado que permite a los equipos de seguridad obtener la mejor seguridad de datos de su clase para web, SaaS, aplicaciones locales, terminales, dispositivos propios del usuario y nube pública.

02 DESCUBRIMIENTO AUTOMÁTICO DE DATOS MEDIANTE IA

Nuestro enfoque sin agente descubre, clasifica e identifica datos automáticamente sin ninguna configuración y, al mismo tiempo, acelera drásticamente la implementación y las operaciones.

03 EQUIPOS EMPODERADOS Y OPERACIONES SIMPLIFICADAS

Reduzca significativamente las sobrecargas de alertas con una potente correlación de amenazas que descubre riesgos ocultos y rutas de ataque críticas, lo que permite a su equipo centrarse en los riesgos más importantes.

POTENTE CLASIFICACIÓN: TODO TIPO DE DATOS, UBICACIONES Y CANALES

Casos de uso de DSPM

CARACTERÍSTICA	VENTAJA	VENTAJAS
Descubra y clasifique datos	Analice y descubra datos confidenciales en varias plataformas y servicios en la nube en tiempo real o casi en tiempo real. Categorice, etiquete e inventaríe con precisión datos confidenciales en función de políticas predefinidas o personalizadas. Obtenga una clasificación de datos precisa basada en IA respaldada por la plataforma Zscaler que supervisa miles de millones de transacciones diariamente.	Obtenga visibilidad exclusiva de la expansión de los datos en la nube y descubra datos confidenciales, incluso donde no sabía que los tenía.
Asignación y seguimiento de la exposición	Obtenga una vista unificada de la seguridad, el inventario y el cumplimiento de los datos confidenciales en su entorno multinube. Obtenga una vista granular, basada en riesgos y centrada en el usuario de todas las rutas de acceso a los activos de datos de misión crítica y su configuración. Analice riesgos ocultos como configuraciones incorrectas, permisos excesivos y vulnerabilidades.	Comprenda el radio de explosión de datos de los activos de datos comprometidos, el acceso, las rutas de ataque ocultas y las amenazas sofisticadas en curso.
Remedie el riesgo	Priorice el riesgo según la gravedad. Solucione fácilmente problemas e infracciones desde el origen con una solución guiada basada en el contexto.	Minimice el riesgo de exposición y vulneración de datos.
Mantenga una postura constante	Aplique la mejor seguridad de datos consistente en todas partes, desde terminales, correo electrónico, SaaS, nube pública, etc.	Mejore la postura general de seguridad y supere las amenazas.
Mantenga el cumplimiento continuo	Asigne continuamente la postura frente a los puntos de referencia regulatorios para identificar y remediar las infracciones de cumplimiento. Aproveche un panel de cumplimiento integral que simplifica la colaboración de seguridad entre equipos multifuncionales.	Controle las infracciones, simplifique las auditorías y evite pérdidas financieras y de reputación.
Integre flujos de trabajo	Integre perfectamente con su ecosistema de seguridad existente, servicios de terceros, herramientas nativas para priorización de riesgos y aplicaciones de colaboración en equipo.	Minimice el coste y la complejidad de proteger datos confidenciales.

Componentes clave de DSPM de Zscaler

Descubrimiento de datos	Descubre almacenes de datos estructurados y no estructurados	Incluido en el SKU de DSPM
Clasificación de datos	Detecta y clasifica automáticamente datos confidenciales con detección lista para usar y reglas personalizadas	Incluido en el SKU de DSPM
Control de acceso a datos	Asigna y rastrea el acceso a recursos de datos	Incluido en el SKU de DSPM
Evaluación de riesgos	Detecta y prioriza el riesgo según la gravedad y el impacto utilizando IA, ML y correlación de amenazas avanzada	Incluido en el SKU de DSPM
Remediación de riesgos	Ofrece solución guiada paso a paso con contexto completo	Incluido en el SKU de DSPM
Gestión de cumplimiento	Asigna automáticamente la postura de seguridad de los datos con respecto a los puntos de referencia de la industria y los estándares de cumplimiento, como RGPD*, CEI, NIST y PCI DSS*	Incluido en el SKU de DSPM

*CAPACIDADES DE HOJA DE RUTA DEL PRODUCTO

Experimente DPSM de Zscaler

Programe una demostración

Experimente el poder de la plataforma DSPM de Zscaler con una demostración guiada.

SOLICITAR UNA DEMOSTRACIÓN

Vea el último evento de lanzamiento

Explore cómo DSPM elimina la complejidad y ofrece una mejor protección de datos contra los sofisticados ataques y amenazas actuales, lo que permite a los equipos de seguridad maximizar la eficiencia.

VEA EL EVENTO DE LANZAMIENTO

Para más información, visite:
www.zscaler.es/dspm