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

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

Los datos en la nube son el nuevo objetivo

82 %

El 82 % de las violaciones de datos han incluido datos almacenados en entornos de nube

227

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

4.45 millones

El costo promedio global de una violación de datos es $4.45 millones

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

"Para 2026, más del 20 % de las organizaciones implementarán la tecnología DSPM [Gestión de la Protección de la Seguridad de los Datos], debido a los urgentes requisitos para identificar y localizar repositorios de datos previamente desconocidos y mitigar los riesgos de seguridad y privacidad asociados."

– Gartner®

GARTNER® NO PATROCINA A NINGÚN PROVEEDOR, PRODUCTO O SERVICIO DESCRITO EN SUS PUBLICACIONES DE INVESTIGACIÓN, Y NO ACONSEJA A LOS USUARIOS DE TECNOLOGÍA QUE SELECCIONEN ÚNICAMENTE A LOS PROVEEDORES CON LAS CALIFICACIONES MÁS ALTAS U OTRA DESIGNACIÓN. LAS PUBLICACIONES DE INVESTIGACIÓN DE GARTNER® CONSISTEN EN LAS OPINIONES DE SU ORGANIZACIÓN DE INVESTIGACIÓN 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.

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

Los entornos multinube son intrínsecamente complejos y dependen muchos recursos. La enorme cantidad de datos que se envían a la nube, junto con el elevado número de usuarios que acceden a diferentes plataformas, cuentas y servicios en la nube, dificulta a las organizaciones la comprensión y el control de lo que ocurre en la nube.

Los profesionales de la seguridad se enfrentan a cuatro desafíos principales 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 proliferación de datos en múltiples plataformas, cuentas y servicios en la nube, las organizaciones tienen dificultades para comprender qué servicios en la nube, regiones y cuentas están consumiendo y almacenando datos.

03 DERECHOS EXCESIVOS

Además de los desafíos que supone descubrir y clasificar los datos, los equipos de seguridad también se esfuerzan por comprender el acceso a los datos y, al mismo tiempo, lograr y mantener el cumplimiento de los requisitos de soberanía de los datos, lo que da lugar a enormes brechas de seguridad.

04 FALTA DE CONTEXTO DE LOS DATOS

La sobrecarga de alertas en torno a configuraciones erróneas y vulnerabilidades sin una priorización basada en el contexto de los datos confidenciales conduce a un mayor agotamiento de los recursos y las brechas de seguridad.

¿Qué impulsa la necesidad de una DSPM integral?

Lamentablemente, 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 están ofreciendo 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.

Le presentamos Zscaler Data Security Posture Management (DSPM)

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

Como parte de la plataforma Zscaler, Zscaler Data Security Posture Management (DSPM) extiende la seguridad sólida y mejor de su clase para sus datos a la nube pública. Proporciona una 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, facultando a las organizaciones y a los equipos de seguridad para prevenir y remediar las violaciones de datos en 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 LOS DATOS DE ZSCALER

¿Por qué Zscaler DSPM?

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, puntos finales, dispositivos BYOD y nube pública.

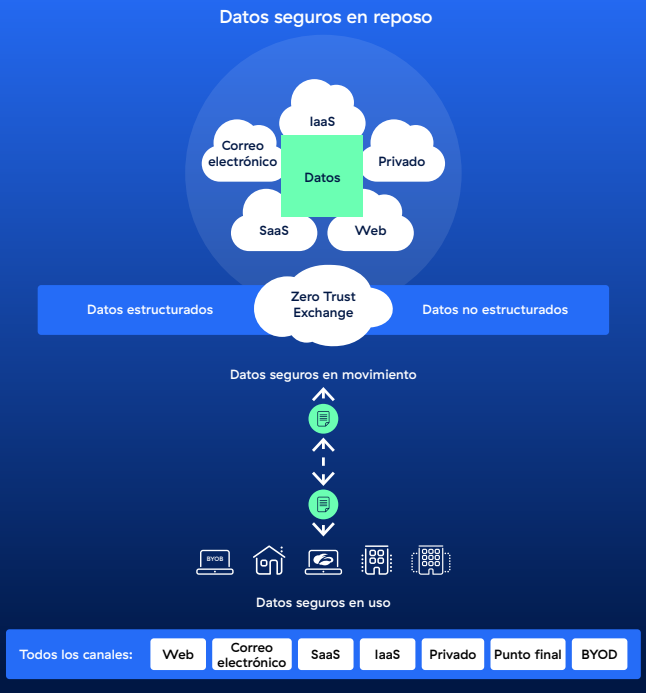
02 DESCUBRIMIENTO AUTOMÁTICO DE DATOS CON IA

Nuestro enfoque sin agentes 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.

CLASIFICACIÓN POTENTE: TODOS LOS TIPOS DE DATOS, UBICACIONES Y CANALES



Casos de uso de DSPM

CARACTERÍSTICAS	VENTAJA	VENTAJAS
Descubra y clasifique datos	Escanee y descubra datos confidenciales en varias plataformas y servicios en la nube en tiempo real o casi en tiempo real. Clasifique, etiquete e haga un inventario preciso de los datos confidenciales basándose en 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 una visibilidad exclusiva de la proliferación de datos en la nube y descubra datos confidenciales, incluso donde no sabía que se encontraban.
Mapee y rastree 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 erróneas, permisos excesivos y vulnerabilidades.	Conozca el radio de explosión de los activos de datos comprometidos, el acceso, las vías de ataque ocultas y las sofisticadas amenazas en curso.
Remedie el riesgo	Priorice el riesgo según la gravedad. Solucione fácilmente problemas y violaciones desde el origen con una solución guiada basada en el contexto.	Minimice el riesgo de exposición y violaciones de datos.
Mantenga una postura uniforme	Aplique una seguridad de datos uniforme y de primera clase en todas partes, desde el punto final, el correo electrónico, SaaS, la nube pública, etc.	Mejore la postura general de seguridad y anticípese a las amenazas.
Mantenga el cumplimiento continuo	Mapee continuamente la postura frente a los puntos de referencia regulatorios para identificar y remediar las violaciones de cumplimiento. Utilice un panel de control de cumplimiento exhaustivo que simplifica la colaboración en materia de seguridad entre equipos multifuncionales.	Controle las violaciones, simplifique las auditorías y evite pérdidas financieras y de reputación.
Integre flujos de trabajo	Integre a la perfección su ecosistema de seguridad existente, los servicios de terceros, las herramientas nativas de priorización de riesgos y las aplicaciones de colaboración en equipo.	Minimice el costo y la complejidad de proteger los datos confidenciales.

Componentes clave de Zscaler DSPM

Descubrimiento de datos	Descubre almacenes de datos estructurados y no estructurados.	Incluido en el SKU de DSPM
Clasificación de datos	Detecta y clasifica automáticamente los datos confidenciales con detección automática y reglas personalizadas.	Incluido en el SKU de DSPM
Control de acceso a los datos	Mapea 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 mediante IA, aprendizaje automático y correlación de amenazas avanzada	Incluido en el SKU de DSPM
Remediación de riesgos	Ofrece una remediación guiada paso a paso con un contexto completo	Incluido en el SKU de DSPM
Gestión de cumplimiento	Mapea automáticamente la postura de seguridad de los datos frente a los puntos de referencia de la industria y las normas de cumplimiento, como GDPR*, CIS, NIST y PCI DSS*.	Incluido en el SKU de DSPM

*CAPACIDADES DE LA HOJA DE RUTA DEL PRODUCTO

Experimente Zscaler DPSM

Programe una demostración

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

SOLICITE UNA DEMOSTRACIÓN

Vea el evento de lanzamiento

Descubra cómo DSPM elimina la complejidad y ofrece una mejor protección de los datos frente a los sofisticados ataques y amenazas actuales, permitiendo a los equipos de seguridad maximizar la eficacia.

VEA EL EVENTO DE LANZAMIENTO

Para más información visite:
www.zscaler.com.mx/dspm