Guía del CISO para una seguridad de datos orientada hacia el futuro con DSPM impulsada por la IA

2025

Índice

Explorar el panorama moderno de la seguridad de datos

El crecimiento exponencial y la dispersión de datos en múltiples plataformas han aumentado la complejidad, los costos y los riesgos para muchas organizaciones. Ahora, los responsables de seguridad se enfrentan a importantes desafíos para comprender y controlar en profundidad sus datos críticos. A esta complejidad se suma la rápida adopción de la IA, que dispersa aún más los datos, y deja a las organizaciones más vulnerables a los riesgos relacionados con los datos y el cumplimiento normativo.

Para mitigar eficazmente los riesgos de seguridad y garantizar un cumplimiento normativo sólido, los equipos de seguridad de datos necesitan herramientas innovadoras que ofrezcan una comprensión integral y en tiempo real de todo su universo de datos. La gestión de la postura de seguridad de datos (DSPM) se ha consolidado como el enfoque moderno por excelencia, que permite a los responsables de la seguridad de datos lograr esta visibilidad y comprensión continuas mediante el uso de la IA y la automatización.

Este libro electrónico esencial profundiza en el potencial transformador de DSPM, y capacita a los líderes de seguridad y a sus equipos para proteger de los datos confidenciales manera proactiva. Diseñado específicamente para profesionales sénior de seguridad y gestión de riesgos, proporciona conocimientos prácticos para explorar+ las complejidades del panorama actual de la seguridad de datos. Como guía integral para elevar la postura de seguridad de datos de su organización, este recurso explora tendencias críticas, aborda desafíos apremiantes y revela estrategias innovadoras, destacando en última instancia, el papel indispensable de DSPM en la protección de sus activos de datos en la dinámica era de la IA.

El objetivo del CISO: Dominar la seguridad de los datos en la era de la IA

Para los responsables de seguridad de la información (CISO), la rápida adopción de la IA y las tecnologías en la nube plantea un dilema profundo. Si bien ofrece oportunidades sin precedentes para el ahorro de costos, la mejora de los resultados empresariales y el aumento notable de la productividad, esta transformación digital introduce simultáneamente un panorama complejo de desafíos para la seguridad de datos.

El panorama del aumento masivo de datos

El punto central de este desafío reside en la explosión de datos empresariales. La información valiosa y confidencial ya no está confinada; está cada vez más fragmentada y dispersa en diversos entornos: ecosistemas de IA, SaaS, PaaS, implementaciones multinube, arquitecturas de nube híbrida e infraestructura local tradicional. Esta proliferación es escalofriante: IDC prevé un crecimiento de datos a una tasa anual compuesta de 21.2 %, y que se disparará a más de 221,000 exabytes para 2026.

Explorar la complejidad y el riesgo

Esto genera una enorme complejidad para los CISO, quienes ahora deben gestionar la seguridad de los datos en un entorno cada vez más extenso y efímero. Los datos se crean, comparten y almacenan constantemente en cientos de sistemas y aplicaciones diversos en toda la empresa, lo que dificulta enormemente su protección integral.

Principales riesgos de seguridad de datos en la era de la IA:

- **Vulnerabilidad y riesgos de cumplimiento:** La dispersión y fragmentación de los datos aumenta significativamente el riesgo de violaciones de datos e incumplimiento normativo. Garantizar el cumplimiento de las normativas de privacidad y gobernanza de datos cambiantes (como el RGPD, la CCPA, etc.) se convierte en una tarea titánica.
- **La amenaza de los datos redundantes, obsoletos y triviales (ROT):** La proliferación descontrolada de datos ocultos (copias de datos desconocidas o no autorizadas) y datos abandonados (datos desactualizados u olvidados) crea vulnerabilidades críticas. Estas suelen provocar importantes fallas de seguridad y amplían exponencialmente la superficie de ataque.
- **Desafíos de la inteligencia artificial generativa (GenAI) y la seguridad de los LLM:** El auge de la IA generativa y los modelos de lenguaje extensos (LLM) introduce una nueva ola de riesgos altamente especializados. Estos incluyen la IA oculta, la fuga de datos (exposición involuntaria de información confidencial), problemas de permisos dentro de los sistemas de IA y nuevas vías para las infracciones normativas. La seguridad de la IA y la gobernanza de datos de los LLM son fundamentales.

Abordar estos desafíos multifacéticos en materia de seguridad de datos requiere un enfoque estratégico y proactivo por parte de los CISO, centrado en una gobernanza de datos sólida, soluciones avanzadas de protección de datos y marcos de seguridad de IA integrales para proteger la información confidencial en esta era dinámica.

Riesgo de perder datos valiosos

Ante la creciente ola de ataques dirigidos y un entorno regulatorio en constante cambio, se ha vuelto crucial que los CISO prioricen la seguridad de estos entornos. Aproximadamente el 44 % de las empresas sufrieron una violación de datos en su entorno de nube en los últimos 12 meses.[1] Una violación de datos puede tener graves consecuencias, como la pérdida de datos, daños a la reputación y pérdidas financieras. A medida que el panorama de amenazas relacionadas con la IA y la nube se vuelve más complejo, el rol del CISO adquiere mayor importancia.

US$4.44M

El costo medio global de una violación de datos en 2025[2]

1. Revista Infosecurity, **Las violaciones en la nube afectan a casi la mitad de las organizaciones**, 25 de junio de 2024.
2. **Informe de IBM sobre el costo de una violación de datos, 2025**

Para gestionar estos riesgos y garantizar el cumplimiento de las normativas, los responsables de seguridad deben comprender a fondo sus entornos de datos. Sin embargo, a menudo el volumen, la variedad y la velocidad de los datos hacen que sea difícil protegerlos. Los líderes no suelen tener las respuestas a estas preguntas:

- ¿Dónde están los datos?
- ¿Qué almacenes de datos contienen datos valiosos o confidenciales?
- ¿Quién, qué o qué herramientas de IA tienen acceso a esos almacenes?
- ¿Cómo se accede o se comparten los datos con herramientas de IA?
- ¿Qué valor tienen los datos?
- ¿Cómo se gestionan los datos y cómo afectan el cumplimiento normativo?

Más allá de los límites: ¿Por qué la seguridad de datos tradicional falla en la era de la IA?

El panorama de la seguridad de datos ha cambiado radicalmente. Para muchos CISO y sus equipos, la respuesta convencional ante las crecientes amenazas ha sido acumular una amplia variedad de herramientas de seguridad dispares. Sin embargo, estas herramientas tradicionales de seguridad de datos están demostrando ser cada vez más insuficientes, ya que no proporcionan la información ni las protecciones esenciales que realmente se necesitan en el entorno dinámico actual.

Los desafíos no resueltos de la seguridad de la IA: Una deficiencia importante de las soluciones heredadas radica en su incapacidad para abordar los comportamientos únicos, los nuevos modos de fallas y los requisitos especializados de gobernanza de datos de las tecnologías emergentes. En concreto, resultan insuficientes a la hora de proteger los LLM, los agentes de IA generativa y otros modelos fundamentales. Estos nuevos riesgos de la IA exigen un enfoque radicalmente diferente.

La necesidad imperiosa de un nuevo paradigma de seguridad

Este panorama de amenazas emergentes no solo exige nuevas soluciones, sino un enfoque holístico e integrado para la gobernanza y la seguridad de los datos en la era de la IA. Hablamos de un cambio de paradigma donde la seguridad de la IA no es una consideración secundaria, sino un componente esencial de su estrategia general de ciberseguridad.

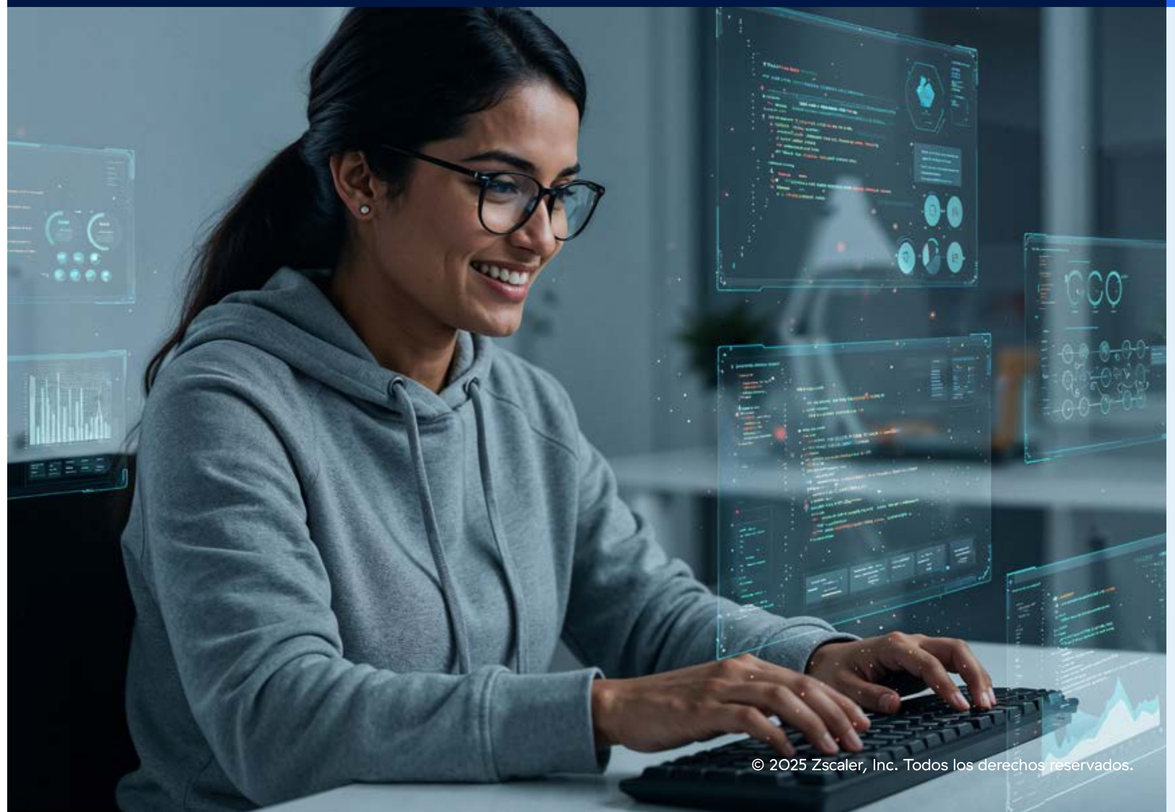
Optimización de inversiones con presupuestos más ajustados

A estos desafíos se suman los presupuestos de seguridad cada vez más limitados, lo que obliga a los responsables de seguridad a evaluar y optimizar sus inversiones. El enfoque se centra ahora en reducir la complejidad operativa y minimizar los costos, al tiempo que se mejoran las defensas de ciberseguridad y se cierran las brechas de seguridad críticas. Paradójicamente, esta inversión estratégica a menudo incluye el uso de soluciones de seguridad sofisticadas basadas en la IA. Estas herramientas avanzadas no solo forman parte del problema, sino que son potentes facilitadoras de una mayor visibilidad, una detección de riesgos más rápida y una respuesta a incidentes más eficiente, lo que en última instancia fortalece toda la postura de seguridad frente a las amenazas de la era de la IA.

3. Informe de IBM sobre el costo de una violación de datos 2025

97 %

de las organizaciones que informaron de una violación de seguridad relacionada con la IA carecían de controles de acceso adecuados a la IA.



Adoptar DSPM: El objetivo moderno para la seguridad de los datos de IA

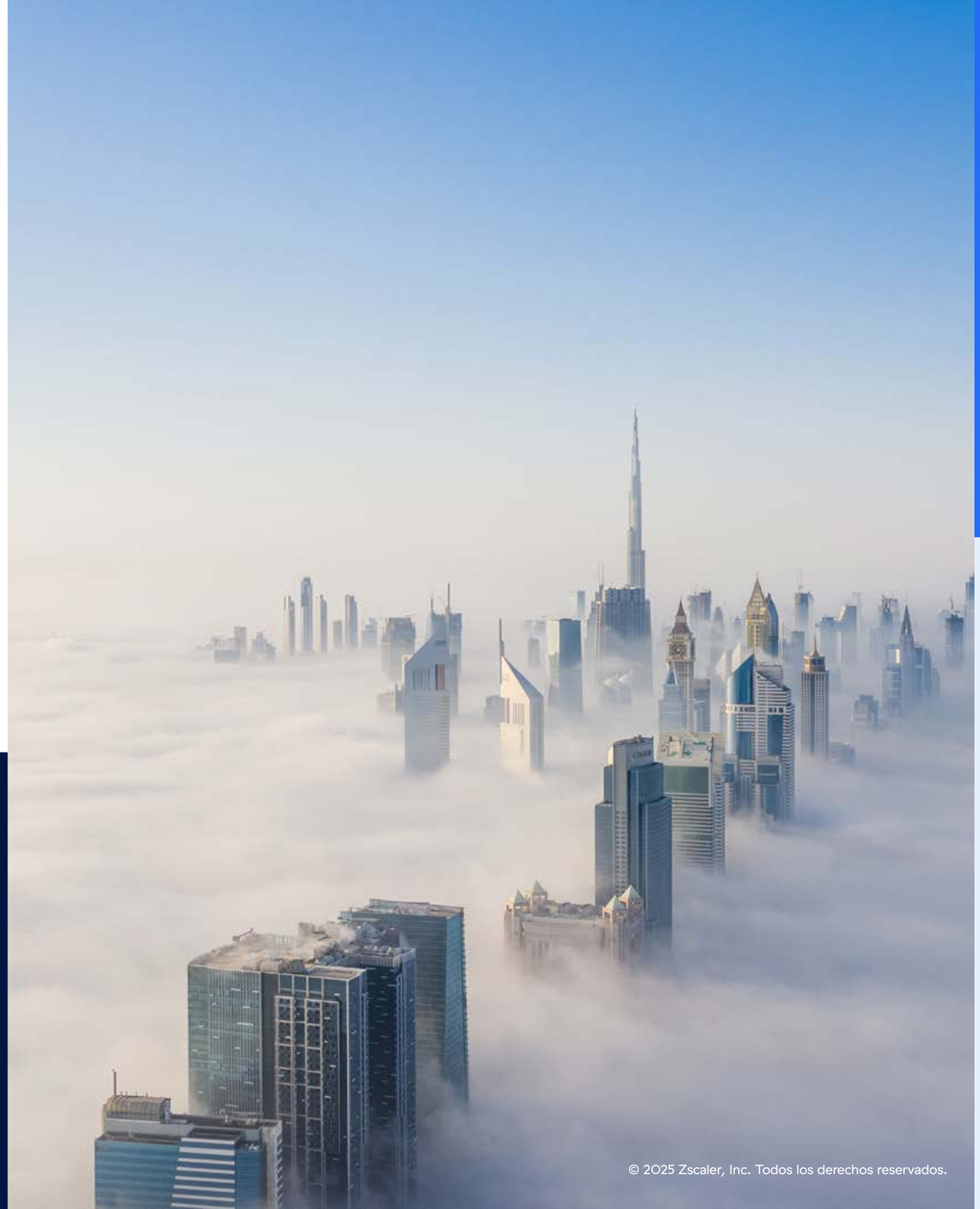
Ante los riesgos sin precedentes de la IA y las reconocidas limitaciones de las herramientas de ciberseguridad tradicionales, un enfoque verdaderamente moderno de la seguridad de los datos no solo es beneficioso, sino esencial. Es aquí donde la gestión de la postura de seguridad de datos (DSPM) surge como una solución fundamental e indispensable.

La DSPM ofrece el contexto y la automatización necesarios para explorar satisfactoriamente las complejidades de los entornos de datos modernos. Al adoptar una metodología innovadora, los CISO pueden comprender mejor sus datos, garantizar el cumplimiento de las normativas y reducir los riesgos asociados con el uso de la IA.

4. Ibid.

US$1.9M

El ahorro promedio para las organizaciones que utilizan ampliamente la IA y la automatización en seguridad[4]



Cómo los CISO pueden mejorar la postura de seguridad de datos utilizando DSPM integrada

A continuación, se presentan algunas de las maneras en que los CISO pueden utilizar eficazmente IA, ML y correlación de riesgos para mejorar la postura de seguridad de los datos:

Abordar los problemas de la IA oculta, los datos y los datos abandonados

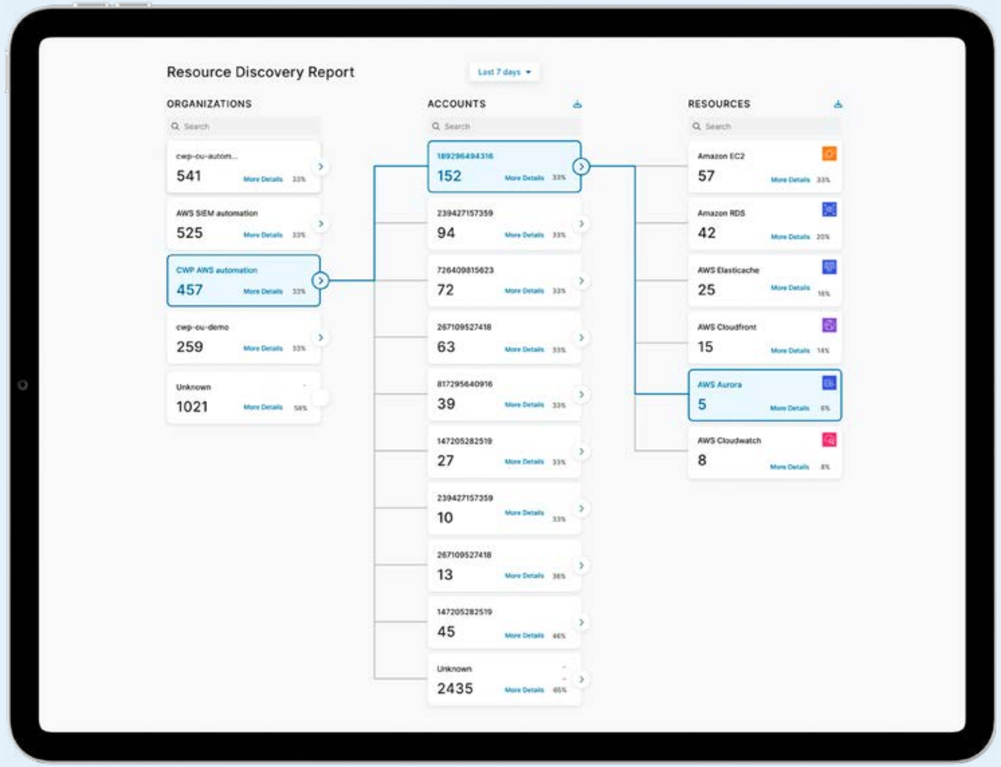
Datos ocultos Los datos ocultos y los datos abandonados presentan riesgos de seguridad sustanciales, ya que con frecuencia operan fuera del alcance de los protocolos de seguridad de TI y los marcos de gobernanza de datos. Según IBM, el 35 % de las violaciones de datos involucraron datos ocultos, y estas violaciones generaron un costo promedio del 16 % mayor. Además, las violaciones que involucraron datos ocultos tardaron un 26.2 % más en identificarse y un 20.2 % más en contenerse[5]. Los datos ocultos pueden encontrarse en archivos no estructurados, bases de datos estructuradas, almacenamiento en la nube o en dispositivos personales sin la supervisión adecuada, mientras que los datos abandonados, sin una gestión de su ciclo de vida, pueden convertirse en un problema.
Las soluciones DSPM aprovechan la IA para descubrir permanentemente los almacenes de datos, mejorando la visibilidad general del panorama de datos. La IA puede ayudar a catalogar datos oscuros y ocultos, aumentando la visibilidad de los mismos. También alerta a los equipos de seguridad sobre posibles riesgos y minimiza los riesgos de violación. Puede supervisar anormalidades en el acceso a datos, patrones, detectar anomalías y predecir posibles violaciones de seguridad.

IA oculta Al igual que la TI oculta, IA oculta se refiere principalmente al uso de herramientas de IA no autorizadas para interactuar con datos confidenciales de la empresa, lo que puede tener consecuencias de gran alcance para la seguridad de los datos y el cumplimiento normativo. A medida que estas herramientas de IA se vuelven más accesibles y productivas, los empleados las adoptan sin supervisión del departamento de TI. Si bien puede parecer inofensivo, puede generar riesgos en cadena imposibles de abordar por los marcos de seguridad tradicionales con solo prohibir las herramientas de IA.

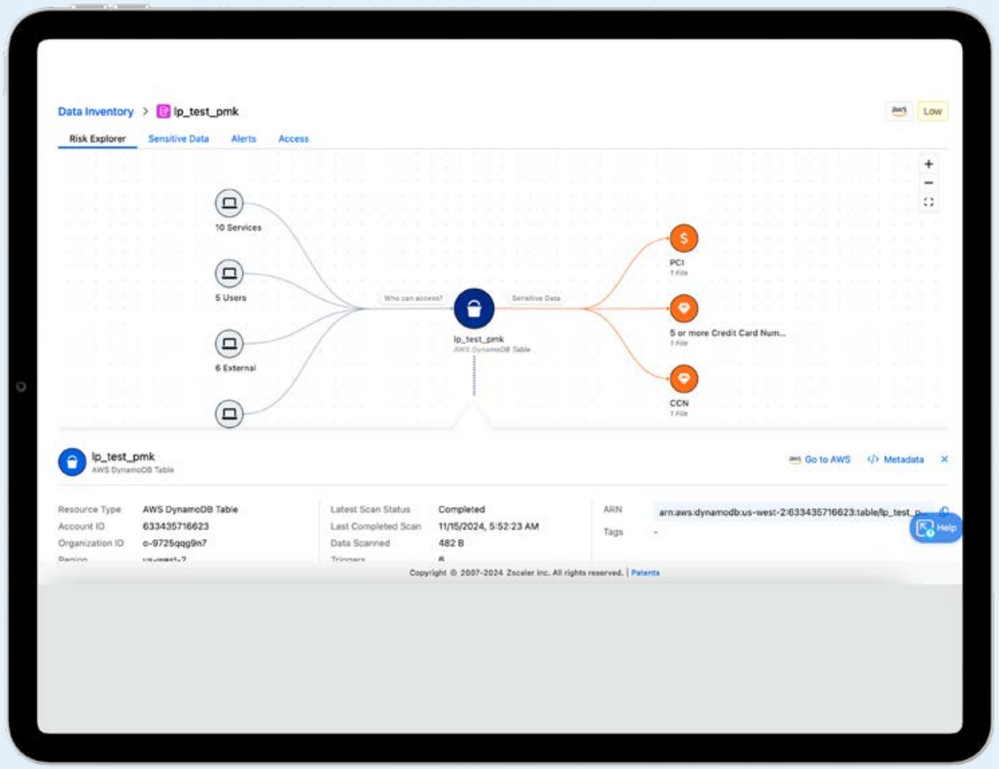
Con la DSPM, las organizaciones pueden aprovechar los beneficios de la IA. En lugar de bloquear o prohibir las herramientas de IA, las organizaciones pueden gestionar los riesgos de la IA oculta con DSPM al tiempo que aprovechan los beneficios de la IA. La capacidad de seguridad de IA integrada de DSPM ayuda a los equipos a obtener visibilidad y control de extremo a extremo sobre los datos y los modelos de IA para protegerse contra los riesgos de la IA de manera proactiva. Ayuda a

- Obtenga una visión de 360 grados de sus modelos, agentes y servicios de IA
- Identifique y proteja los datos de entrenamiento de la IA contra el envenenamiento de datos, las configuraciones erróneas y la exposición
- Adáptese a los nuevos y emergentes marcos de cumplimiento de IA

Con DSPM, los líderes de seguridad pueden transformar el caos en materia de seguridad en una innovación controlada, proporcionando una detección de datos unificada, una evaluación de riesgos contextual y una gobernanza automatizada en cada interacción con la IA.



5. Ibid.



Clasificación de datos impulsada por la IA

La clasificación de datos es un aspecto fundamental de una seguridad de datos sólida. La identificación proactiva de datos confidenciales y su relación con los riesgos asociados es esencial para evitar posibles exposiciones causadas por configuraciones erróneas o prácticas inseguras. Los enfoques convencionales, que a menudo dependen de procedimientos manuales o de un reconocimiento de patrones simplista, son susceptibles a altos niveles de resultados falsos positivos y a una asignación subóptima de recursos de seguridad. Con frecuencia, las organizaciones dependen en gran medida de soluciones basadas en expresiones regulares, un enfoque rígido y plagado de falsos positivos, que ha demostrado ser frágil e ineficiente. Incluso los enfoques actuales basados en productos puntuales no logran integrar la clasificación dentro de una plataforma centralizada y unificada, lo que genera alertas inconsistentes y visibilidad fragmentada, especialmente porque los datos se mueven a través del ecosistema de una organización.

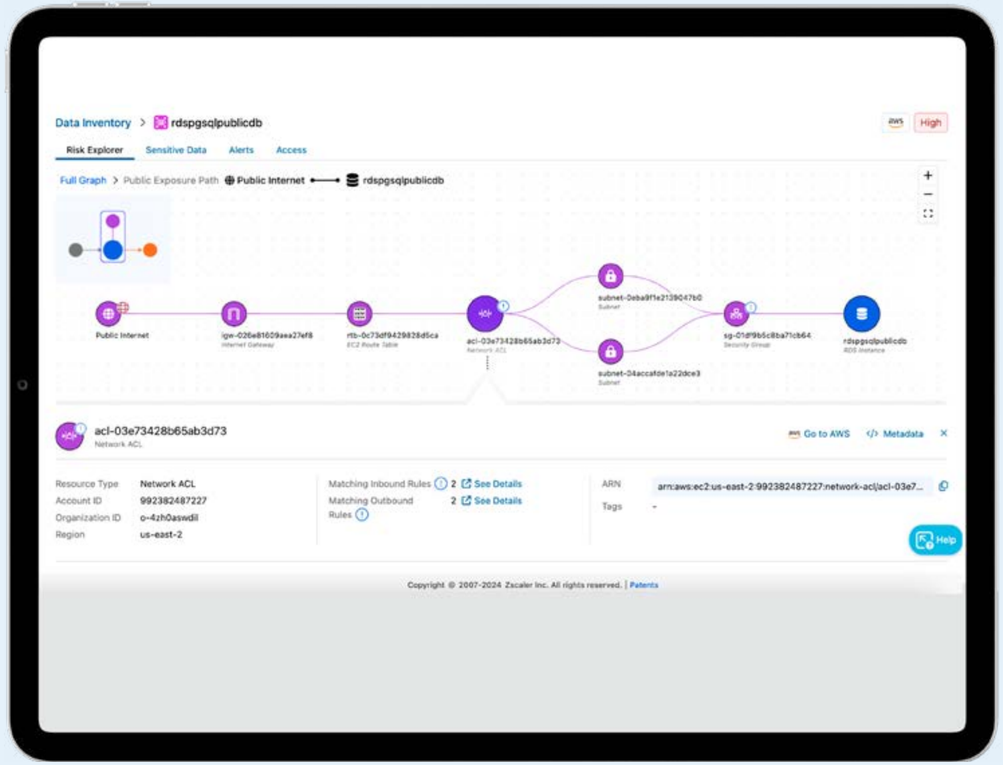
Los responsables de seguridad pueden aprovechar la DSPM con la clasificación LLM impulsada por la IA que mejora el funcionamiento de los tradicionales flujos de trabajo con expresiones regulares, brindando una visibilidad y flexibilidad increíbles que les permiten proteger datos confidenciales conocidos y desconocidos como nunca antes. A diferencia de las técnicas dependientes de palabras clave, la clasificación LLM permite una identificación de contenido más profunda. Utiliza procesamiento avanzado del lenguaje para la clasificación de datos con el fin de comprender la intención y el contexto del contenido, sin necesidad de patrones o palabras clave predefinidos. Esto permite a las organizaciones no solo mejorar sus prácticas existentes, sino también descubrir y proteger nuevos tipos de datos confidenciales que antes pasaban desapercibidos o eran imposibles de detectar.

Gestión proactiva de riesgos

Para controlar eficazmente el riesgo de seguridad y garantizar el cumplimiento, los líderes de seguridad necesitan una manera proactiva de gestionar su postura de seguridad de datos. Una de las aplicaciones más interesantes de la IA en la seguridad de datos es el enfoque de seguridad proactivo y el análisis predictivo. AI analizar y correlacionar datos, los algoritmos de IA pueden predecir posibles riesgos de seguridad. Este enfoque proactivo permite a las organizaciones estar un paso por delante de las amenazas y los riesgos críticos

La DSPM aprovecha la IA y las técnicas de correlación avanzada que ayudan a identificar patrones y tendencias en los datos que pueden indicar incidentes de seguridad inminentes. Además, puede priorizar los almacenes de datos en función de su valor (gravedad del riesgo), garantizando así que los esfuerzos de seguridad se destinen a los activos más críticos. Asimismo, al automatizar numerosos procesos de seguridad, reduce la carga de trabajo de los profesionales de seguridad, permite un enfoque de seguridad proactivo y mejora la eficiencia operativa general.

Por ejemplo, la correlación avanzada de Zscaler DSPM puede conectar puntos de manera proactiva y detectar riesgos ocultos, lo que permite priorizar los esfuerzos de seguridad en los datos más críticos.



49 %

de las organizaciones que invierten en seguridad tras una violación de seguridad[6]

6. Informe de IBM sobre el costo de una violación de datos 2025

Optimizar el cumplimiento con la gobernanza de datos en tiempo real

Mantener el cumplimiento de las normativas cambiantes y los protocolos de seguridad internos es una piedra angular de la seguridad de los datos y la IA, desde el RGPD hasta la SEC. Las organizaciones de la actualidad deben sortear no solo las normativas establecidas, como el RGPD y la HIPAA, sino también los marcos que surgen específicamente para la IA, incluida la Ley de IA de la UE, la NIST AI 600 y otras. La seguridad y el riesgo de cumplimiento comparten un vínculo inquebrantable, compenetrándose profundamente y moldeando la trayectoria de una organización. Las violaciones pueden conllevar sanciones por incumplimiento, lo que puede tener graves repercusiones, multas considerables y manchar la reputación de una organización. Por el contrario, adoptar las normativas puede servir de escudo, fortificando la IA y los datos contra las vulnerabilidades y amenazas a la seguridad.

Muchas normativas se reducen a conocer la IA y los datos confidenciales, limitar quién puede acceder a ellos y supervisar continuamente el riesgo. Aunque esto pueda parecer simple, la complejidad de los entornos de IA y de datos puede convertirlo en un desafío. Además, las regulaciones evolucionan constantemente, impulsadas por las nuevas tecnologías, las cambiantes preocupaciones sobre la privacidad y la creciente interconexión de la economía global. Este terreno regulatorio en constante cambio exige vigilancia y adaptación constantes por parte de las organizaciones que desean mantener el cumplimiento. Los enfoques tradicionales de cumplimiento normativo, con sus visiones fragmentadas, evaluaciones manuales y respuestas reactivas, tienen dificultades para brindar claridad y eficiencia.

La DSPM puede agilizar los procesos de cumplimiento con capacidades de gobernanza y cumplimiento de datos en tiempo real. La solución DSPM proporciona a las organizaciones una visión amplia del estado de cumplimiento de los datos, análisis exhaustivos, evaluación comparativa, remediación y generación de informes para actuar con rapidez ante sus brechas de cumplimiento. Esto es especialmente importante en sectores altamente regulados, donde es esencial comprender claramente el estado de los datos y mitigar los riesgos. Desde pasos de remediación guiados hasta flujos de trabajo automatizados, el panel de control de cumplimiento permite a los equipos de seguridad actuar con rapidez y eficacia. La aplicación de la IA en la gobernanza de datos se asegura de que las organizaciones puedan cumplir con las exigencias regulatorias al tiempo que mantienen medidas de seguridad sólidas.

63 %

de las organizaciones carecen de políticas de gobernanza de la IA[7]

7. https://newsroom.ibm.com/2025-07-30-ibm-report-13-of-organizations-reported-breaches-of-ai-models-or-applications,-97-of-which-reported-lacking-proper-ai-access-controls

Conseguir acceso con privilegios mínimos

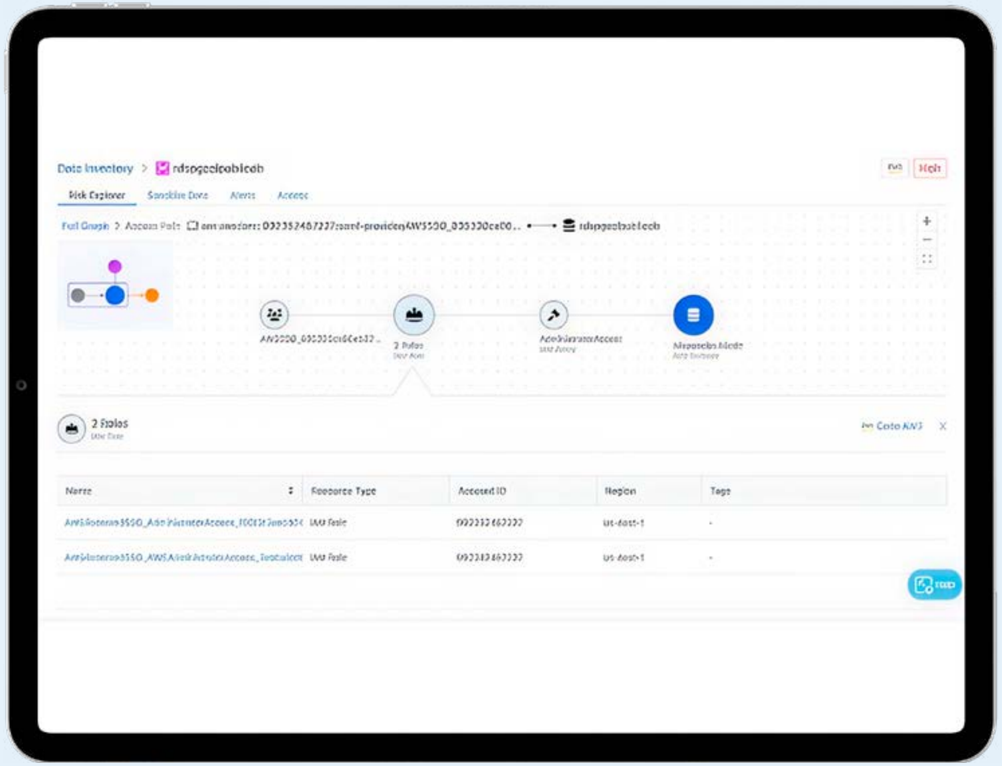
Debido al enorme volumen de usuarios, aplicaciones y recursos, los entornos de datos conllevan un riesgo significativo de controles de acceso inadecuados, proliferación de identidades y almacenes huérfanos. Aproximadamente el 90 % de las organizaciones sufrieron violaciones de seguridad relacionadas con la identidad, lo que ocasionó costosos incidentes de seguridad.

Además, los modelos de IA y las herramientas basadas en LLM introducen riesgos adicionales relacionados con el acceso no autorizado a los datos. Entre los riesgos clave se incluyen las divulgaciones involuntarias o no autorizadas de datos confidenciales, la exfiltración de datos (donde se roban datos confidenciales a través de los resultados de la IA) y los ataques sofisticados, donde las identidades comprometidas explotan los sistemas de IA para obtener acceso no autorizado.

Por eso, garantizar el acceso con privilegios mínimos a los almacenes de datos es un principio fundamental de la seguridad de los datos. La gobernanza del acceso a los datos resulta más compleja debido a la proliferación de datos, la proliferación de permisos y las complejas arquitecturas de la IA y multinube. Sin embargo, sigue siendo un componente esencial de la seguridad de los datos, ya que la exposición no autorizada de datos confidenciales suele ser el primer paso de un ataque sofisticado.

La DSPM ofrece un enfoque unificado para la gobernanza del acceso a los datos con una supervisión continua de la postura de seguridad de los datos y el comportamiento del usuario. La DSPM examina las funciones, los permisos y los atributos relacionados con la gestión de la identidad y el acceso a los datos para identificar rápidamente las vías riesgosas de acceso a los almacenes de datos. La DSPM admite datos estructurados, no estructurados y en entornos locales, multinube y SaaS, lo que permite a las organizaciones identificar y abordar los riesgos de acceso de manera uniforme y aplicar políticas de acceso en diversos conjuntos de datos y ecosistemas de IA. Al proporcionar información detallada sobre los patrones de acceso y las vulnerabilidades potenciales, los equipos de seguridad de datos pueden aplicar el acceso con privilegios mínimos de manera más eficaz. Este enfoque reduce el riesgo de acceso no autorizado y mejora la seguridad general del entorno de datos.

8. La seguridad actual, Estudio: **El 90 por ciento de las organizaciones experimentaron un incidente relacionado con la identidad el año pasado**, 5 de junio de 2024.



90 %

de las organizaciones han sufrido un incidente relacionado con la identidad[8]

Optimizar los costos de almacenamiento y consumo

Los equipos de datos necesitan optimizar los costos de almacenamiento y consumo identificando repositorios de datos duplicados o desatendidos que puedan eliminarse o transferirse a soluciones de almacenamiento más rentables. Los métodos convencionales suelen ser insuficientes para identificar y gestionar estos datos, lo que genera gastos de almacenamiento superfluos.

Las soluciones de DSPM pueden hacer frente a este problema proporcionando información sobre los almacenes de datos duplicados o abandonados, lo que permite a las organizaciones tomar las medidas adecuadas. Del mismo modo, Zscaler DSPM proporciona una visión completa de los almacenes de datos duplicados o abandonados, lo que permite a los equipos identificar los datos que se pueden eliminar o migrar de manera segura.

Gracias a los conocimientos basados en la IA, las organizaciones pueden reducir los gastos excesivos de almacenamiento y garantizar la gestión y protección adecuadas de la información confidencial.

Aplique políticas unificadas en todos los entornos de datos

Con los métodos tradicionales, el desafío de mantener políticas de seguridad de datos uniformes en diversos entornos es formidable. Las soluciones de DSPM pueden superar esto ofreciendo un enfoque unificado de la seguridad de los datos en entornos de múltiples nubes, lo que permite a las organizaciones aplicar políticas uniformes en todos los entornos de datos.

Zscaler DSPM presenta una estrategia unificada para la seguridad de datos. Permite a las organizaciones establecer políticas uniformes en todos los entornos de datos, garantizando una vigilancia exhaustiva sobre los datos en la nube y agilizando el proceso de identificación y resolución de riesgos. Mediante el uso de conocimientos detallados, las organizaciones pueden reducir el riesgo de violación de datos y seguir mejor las normas de protección de datos.

Respuesta rápida a incidentes

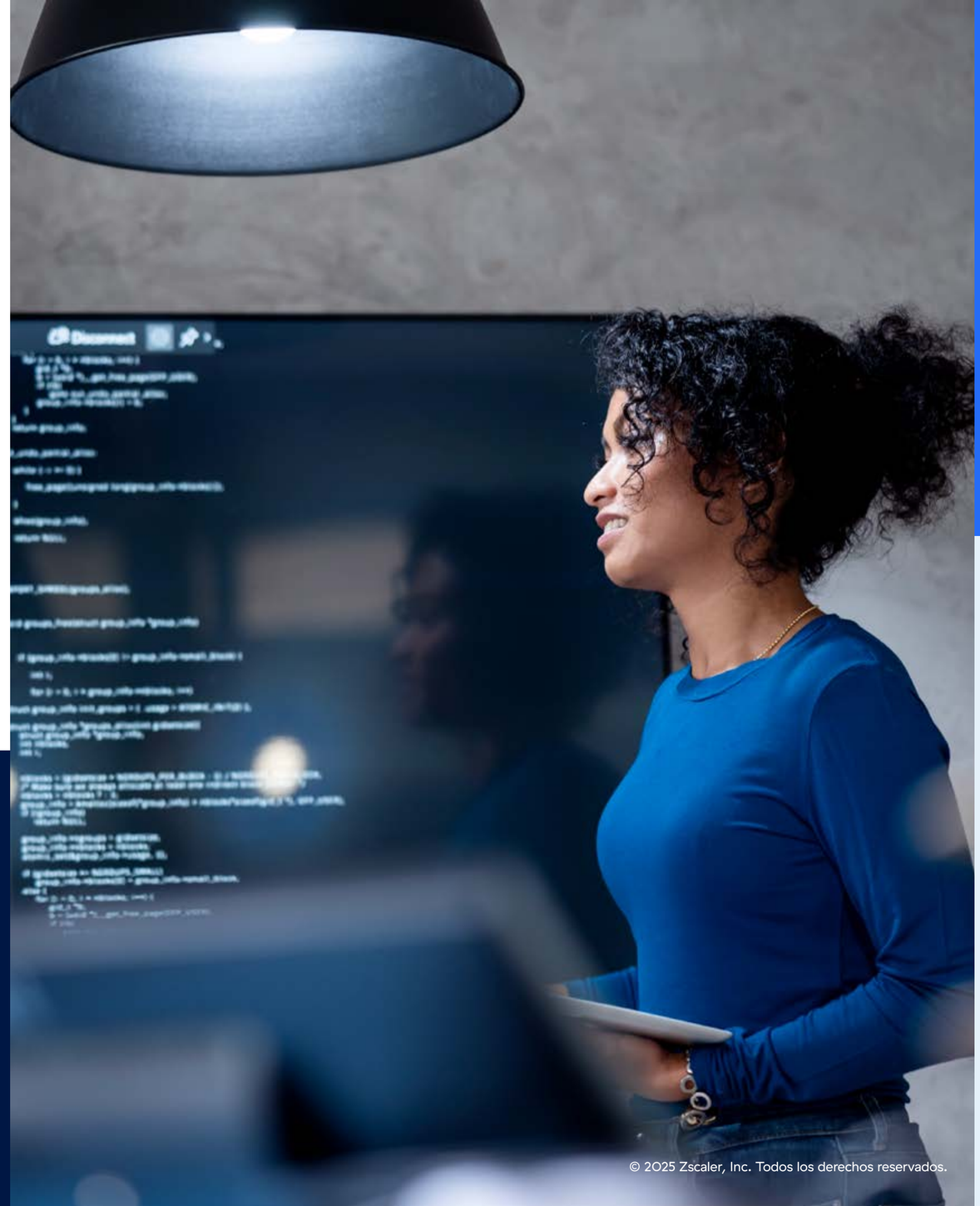
La identificación y mitigación de los riesgos son tareas fundamentales para los profesionales de la seguridad de los datos. La velocidad a la que evolucionan las amenazas requiere respuestas en tiempo real. Sin embargo, las metodologías convencionales pueden fallar en un entorno de amenazas dinámico impulsado por la IA. La automatización de la seguridad impulsada por la IA es la respuesta a este desafío.

La DSPM puede supervisar datos de manera continua, detectar anomalías y ayudar a responder a las amenazas. Las soluciones DSPM refuerzan la mitigación de riesgos al ofrecer una sofisticada correlación de riesgos e inteligencia de acceso adaptativa. Algunas soluciones de DSPM, como Zscaler DSPM, incorporan inteligencia de amenazas de Zscaler ThreatLabz, una meticulosa remediación guiada y una implementación de seguridad acelerada. Mediante una sofisticada correlación de amenazas basada en la IA, las organizaciones pueden descubrir riesgos latentes y vectores de ataque clave, lo que permite concentrar los esfuerzos en los riesgos más críticos.

9. Statista, **Tiempo medio para identificar y contener las violaciones de datos en todo el mundo de 2017 a 2024**, consultado el 9 de diciembre de 2024.

194 días

El tiempo medio para identificar una violación de datos[9]



Seguridad mejorada de la IA

Las organizaciones están adoptando aplicaciones de IA a un ritmo vertiginoso. Lamentablemente, aplicaciones como la IA generativa (GenAI) y los grandes modelos de lenguaje (LLM) han introducido importantes riesgos de violación de datos e incumplimiento normativo. Un informe reciente indicó que el 13 % de las organizaciones denunciaron violaciones de modelos o aplicaciones de IA[10], lo que pone de manifiesto que la IA se está convirtiendo en un objetivo de alto valor.

Las organizaciones que integran GenAI en sus operaciones deben tomar medidas para evitar el uso inadvertido de datos confidenciales dentro de estos modelos. Los equipos de seguridad deben priorizar la señalización, el etiquetado y la clasificación de los datos para garantizar que los equipos multifuncionales utilicen la GenAI de manera responsable.

La DSPM mejora el control y la protección de datos en entornos de GenAI gracias a sus capacidades integradas de gestión de procesos AI-SPM.

Al identificar y categorizar meticulosamente los datos, la DSPM evita que la información confidencial se transmita a los LLM, reduciendo así el riesgo de violaciones de datos e incumplimiento normativo. La DSPM adopta un enfoque centrado en los datos, priorizando la seguridad de la información que alimenta la IA, en lugar de solo la infraestructura. Mediante la detección, clasificación y supervisión continua de los datos a lo largo de su ciclo de vida, la DSPM ayuda a mitigar riesgos de seguridad específicos de la IA, como el envenenamiento de datos, la exposición de datos confidenciales y el robo de modelos.

La adopción de DSPM con capacidades integradas de AI-SPM puede capacitar a las organizaciones para generar confianza en sus aplicaciones de IA. Al hacerlo, no solo protegen sus datos importantes, sino que también hacen que las aplicaciones de IA sean más confiables y seguras.

10. https://newsroom.ibm.com/2025-07-30-ibm-report-13-of-organizations-reported-breaches-of-ai-models-or-applications,-97-of-which-reported-lacking-proper-ai-access-controls

Aprovechar DSPM para proteger un entorno de datos diverso

El uso estratégico de DSPM es primordial en la búsqueda de una seguridad de datos más sólida. Estas tecnologías ofrecen el contexto y la automatización necesarios para gestionar con eficacia las complejidades de los entornos de datos modernos. A través de una postura proactiva, los líderes de seguridad pueden salvaguardar más eficazmente los datos confidenciales, garantizar el cumplimiento y mitigar los riesgos asociados con tecnologías progresivas como GenAI.

"Para 2026, más del 20 % de las organizaciones implementarán tecnología DSPM, debido a la necesidad apremiante de identificar y localizar repositorios de datos hasta ahora desconocidos y de mitigar los riesgos de seguridad y privacidad asociados."

Gartner®, Perspectiva sobre innovación: Gestión de la postura de seguridad de datos,
Brian Lowans, Joerg Fritsch, Andrew Bales,
28 de marzo de 2023

Zscaler DSPM

Zscaler DSPM es la plataforma integrada de protección de datos más completa del mundo para asegurar los datos estructurados y no estructurados a través de SaaS, entornos de nube pública (AWS, Azure, GCP), aplicaciones en las instalaciones locales y puntos finales.

Zscaler DSPM 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.

Zscaler DSPM adopta un enfoque unificado impulsado por la IA para garantizar una sólida higiene de datos en todos los almacenes, incluidos IaaS, SaaS, locales, puntos finales. etc. Su integración con la plataforma de seguridad de datos de Zscaler de manera nativa, le permite comprender y controlar completamente todos sus datos en una única plataforma.

La plataforma de seguridad de datos de Zscaler utiliza un motor DLP único y unificado para ofrecer una protección de datos uniforme y de primera clase en todos los canales. Mediante el seguimiento de todos los usuarios en todas las ubicaciones y el control de los datos en movimiento y en reposo, garantiza que los datos confidenciales estén perfectamente protegidos y que se cumpla la normativa

Para obtener más información, visite zscaler.com/mx/dp/dspm.

Explore la visita interactiva de producto de DSPM

¿Por qué la DSPM debe ser parte su estrategia de protección de datos?

Vea el seminario web a pedido ⟶

Escanee el código QR para acceder a recursos útiles de DSPM:

zscaler™ | Experience your world, secured.™

Acerca de Zscaler

Zscaler (NASDAQ: ZS) acelera la transformación digital para que los clientes puedan ser más ágiles, eficientes, resistentes y seguros. Zscaler Zero Trust Exchange protege a miles de clientes de ciberataques y pérdida de datos al conectar de manera segura usuarios, dispositivos y aplicaciones en cualquier ubicación. Distribuido en más de 150 centros de datos en todo el mundo, Zero Trust Exchange basado en SSE es la plataforma de seguridad en la nube en línea más grande del mundo. Obtenga más información en **zscaler.com/mx** o síganos en Twitter **@zscaler**.

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