La guía del CISO para garantizar la seguridad de los datos a futuro con DSPM impulsado por IA

2025

Índice

Navegar por el actual panorama de seguridad de datos

El crecimiento exponencial y la dispersión de datos en múltiples plataformas han aumentado la complejidad, los costes y los riesgos para muchas organizaciones. Los responsables de seguridad se enfrentan ahora 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, dejando 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 seguridad de datos lograr esta visibilidad y comprensión continuas mediante el uso de IA y automatización.

Este libro electrónico esencial profundiza en el potencial transformador de DSPM, capacitando a los líderes de seguridad y a sus equipos para proteger de forma proactiva los datos confidenciales. Diseñado específicamente para profesionales sénior de seguridad y gestión de riesgos, proporciona información práctica para desenvolverse en las complejidades del panorama actual de la seguridad de datos. Como guía integral para mejorar la postura de seguridad de datos de su organización, este recurso explora tendencias críticas, aborda desafíos apremiantes y revela estrategias innovadoras; en última instancia pone de relevancia el papel indispensable de la gestión de la seguridad de datos (DSPM) en la protección de sus activos de datos en la dinámica era de la IA.

El imperativo 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 profundo dilema. Si bien ofrece oportunidades sin precedentes para el ahorro de costes, la mejora de los resultados empresariales y el aumento notable de la productividad, esta transformación digital introduce al mismo tiempo un panorama complejo de desafíos en materia de seguridad de datos.

El panorama de datos en expansión

El núcleo de este desafío reside en el crecimiento de datos empresariales. La información valiosa y confidencial ya no está confinada; cada vez está 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 asombrosa: IDC prevé un crecimiento de datos a una tasa anual compuesta del 21,2 % que aumentará a más de 221 OOO exabytes para 2O26.

Navegando por la complejidad y el riesgo

Esto genera una enorme complejidad para los CISO, que ahora deben gestionar la seguridad de los datos en un entorno de datos efímero y en constante expansión . Se crean, comparten y almacenan datos constantemente en cientos de sistemas y aplicaciones diversos en toda la empresa, lo que dificulta enormemente la protección integral de los mismos.

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 filtraciones e incumplimiento normativo. Garantizar el cumplimiento de las normativas de privacidad y gobernanza de datos en constante evolución (como el RGPD, la CCPA, etc.) se convierte en una tarea titánica.
- **La amenaza de los datos obsoletos:** 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 fallos de seguridad y amplían exponencialmente la superficie de ataque.
- **Inteligencia artificial generativa y desafíos de 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 en la sombra, la filtración de datos (exposición involuntaria de información confidencial), problemas de permisos dentro de los sistemas de IA y nuevas vías para infracciones normativas. La seguridad de la IA y la gobernanza de datos de los LLM son fundamentales.

Abordar estos desafíos plurales en materia de seguridad de datos requiere un enfoque estratégico y proactivo por parte de los CISO; se debe centrar en una gobernanza de datos sólida, soluciones avanzadas de protección de datos y marcos de seguridad de IA integrales para salvaguardar 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 convertido en algo fundamental que los CISO prioricen la seguridad de estos entornos. Aproximadamente el 44 % de las empresas sufrieron una filtración de datos en su entorno de nube en los últimos 12 meses.[1] Una filtración de datos puede tener graves consecuencias, como la pérdida de datos, daños a la reputación y pérdidas financieras. A medida que el panorama de amenazasrelacionadas con la IA y la nube se vuelve más complejo, el rol del CISO adquiere mayor importancia.

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

4,44 millones de dólares estadouni denses

El coste promedio global de una infracción de datos en 2025[2]

Para gestionar estos riesgos y garantizar el cumplimiento de las regulaciones, los líderes de seguridad deben comprender completamente 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 con frecuencia carecen de 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 esas tiendas?
- ¿Cómo se accede o se comparten los datos con herramientas de IA?
- ¿Qué valor tienen los datos?
- ¿Cómo se gestionan los datos y cuál es el impacto en el cumplimiento normativo?

Más allá de los límites: ¿Por qué fracasa la seguridad de datos tradicional 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 gama 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 cruciales que realmente se necesitan en el entorno dinámico actual.

Los desafíos no resueltos de la seguridad de la IA : una importante deficiencia de las soluciones heredadas radica en su incapacidad para abordar los comportamientos únicos, los nuevos modos de fallo y los requisitos especializados de gobernanza de datos de las tecnologías emergentes. En concreto, resultan insuficientes a la hora de proteger el aprendizaje automático, 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 exige no solo 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.

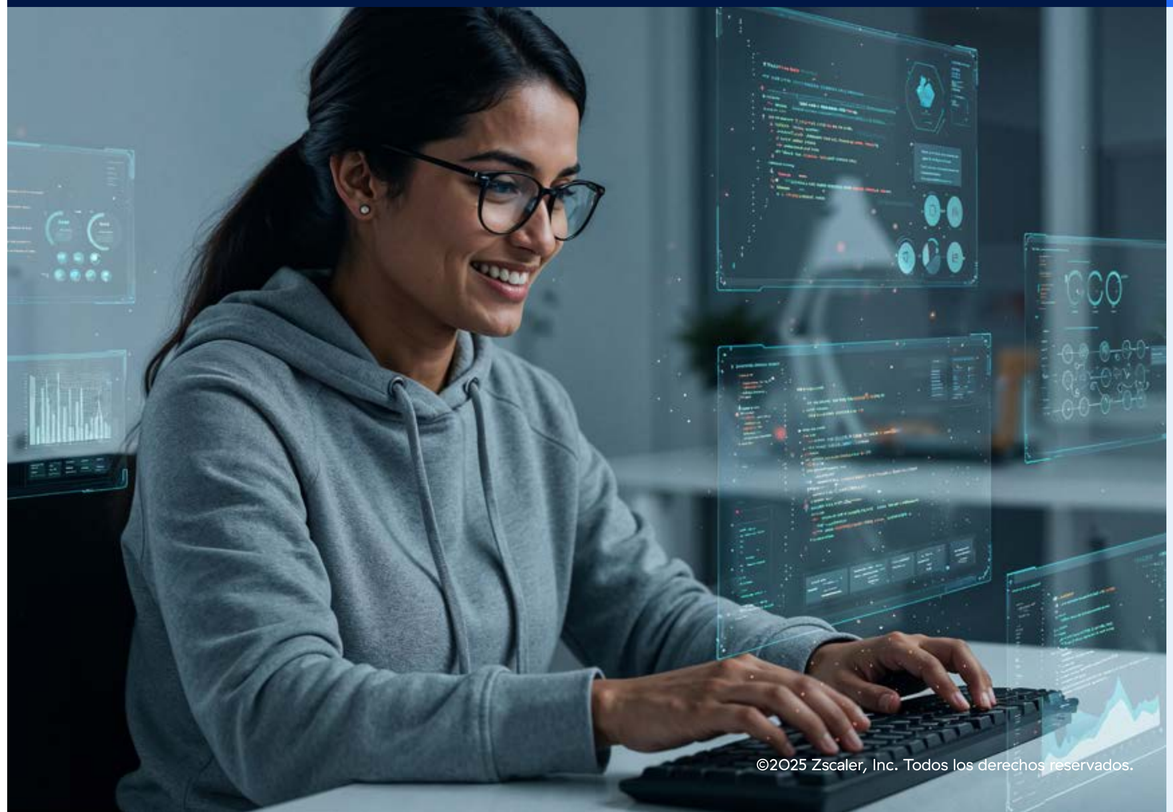
Optimización de inversiones con presupuestos más ajustados

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 costes, 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 IA. Estas herramientas avanzadas no solo forman parte del problema, sino que propician en gran medida 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 coste de una infracción de datos 2025

97 %

de las organizaciones que informaron de una brecha de seguridad relacionada con la IA carecían de controles de acceso adecuados a la IA[3]



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

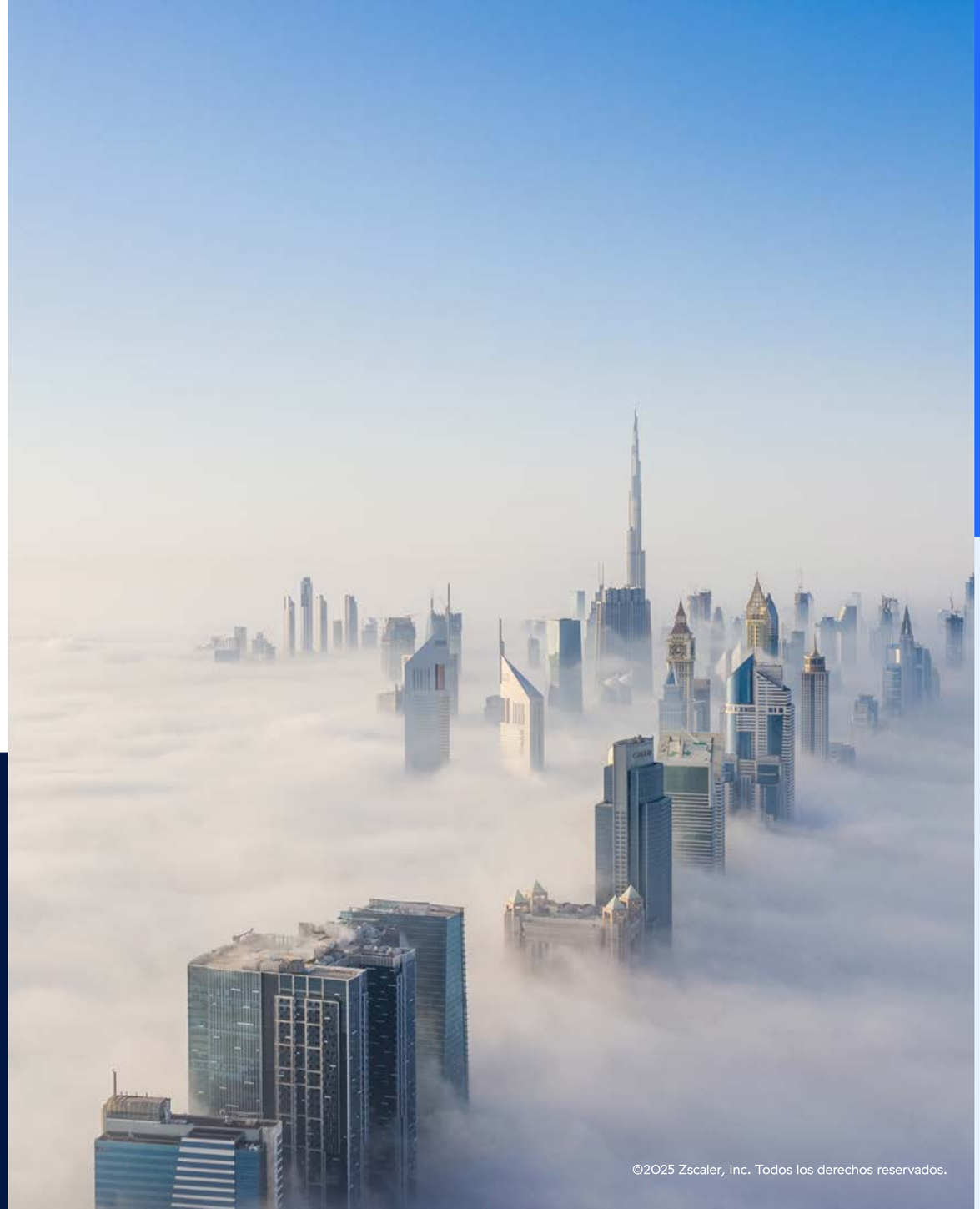
Ante los riesgos sin precedentes de la IA y las reconocidas limitaciones de las herramientas de ciberseguridad tradicionales, un enfoque verdaderamente moderno de la seguridad de los datos no solo es beneficioso, sino esencial. Es aquí donde la Gestión de la Postura de Seguridad de Datos (DSPM) emerge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

DSPM ofrece el contexto y la automatización necesarios para navegar con destreza por 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 al uso de la IA.

4. Ibid.

1,9 millones de dólares estadounidenses

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



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

A continuación figuran algunas de las formas en que los CISO pueden utilizar de manera eficaz la IA para mejorar la postura de seguridad de los datos:

Aborde las preocupaciones sobre la IA en la sombra, los datos y los datos abandonados

Datos en la sombra Los datos en la sombra 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 filtraciones de datos involucraron datos ocultos y estas filtraciones generaron un costo promedio un 16 % mayor. Además, se tardó un 26,2 % más en indentificar y un 20,2 % más en contener las filtraciones que involucraron datos en la sombra[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 y clasificar 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 infracciones. Puede supervisar irregularidades en el acceso a datos, patrones, detectar anomalías y predecir posibles infracciones de seguridad.

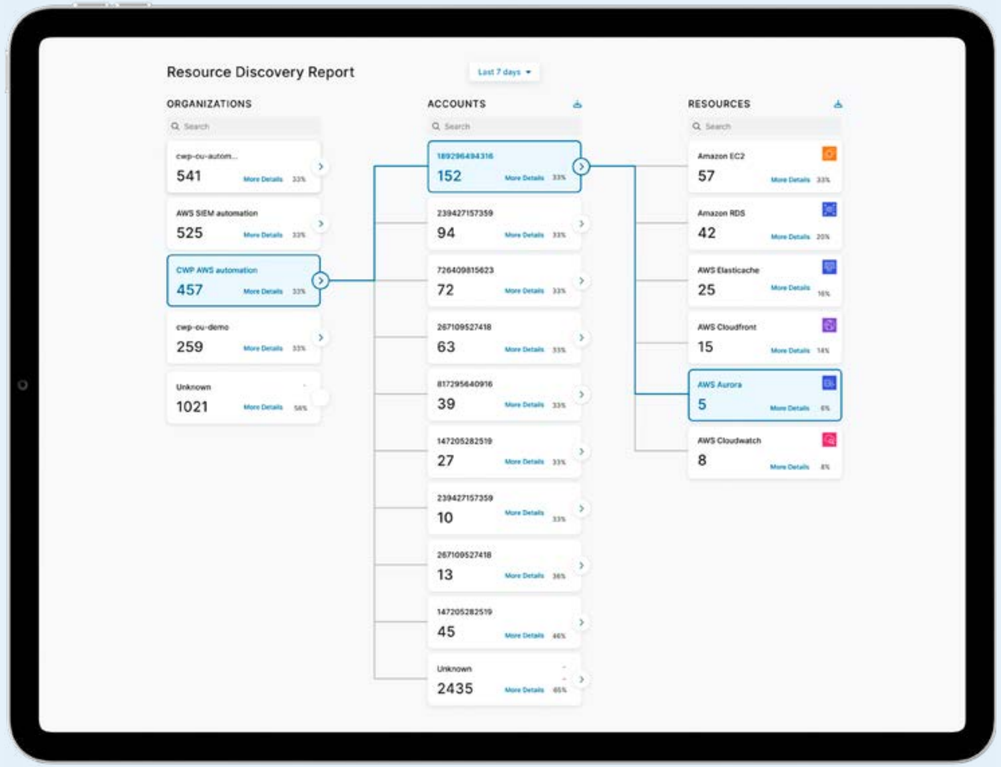
IA en la sombra La IA en la sombra, al igual que la TI en la sombra, se refiere principalmente al uso de herramientas de IA no autorizadas para interactuar con datos confidenciales de la empresa, lo que puede tener consecuencias de gran alcance para la seguridad de los datos y el cumplimiento normativo. 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 esto puede parecer inofensivo, puede generar riesgos en cadena que los marcos de seguridad tradicionales no pueden abordar simplemente prohibiendo las herramientas de IA.

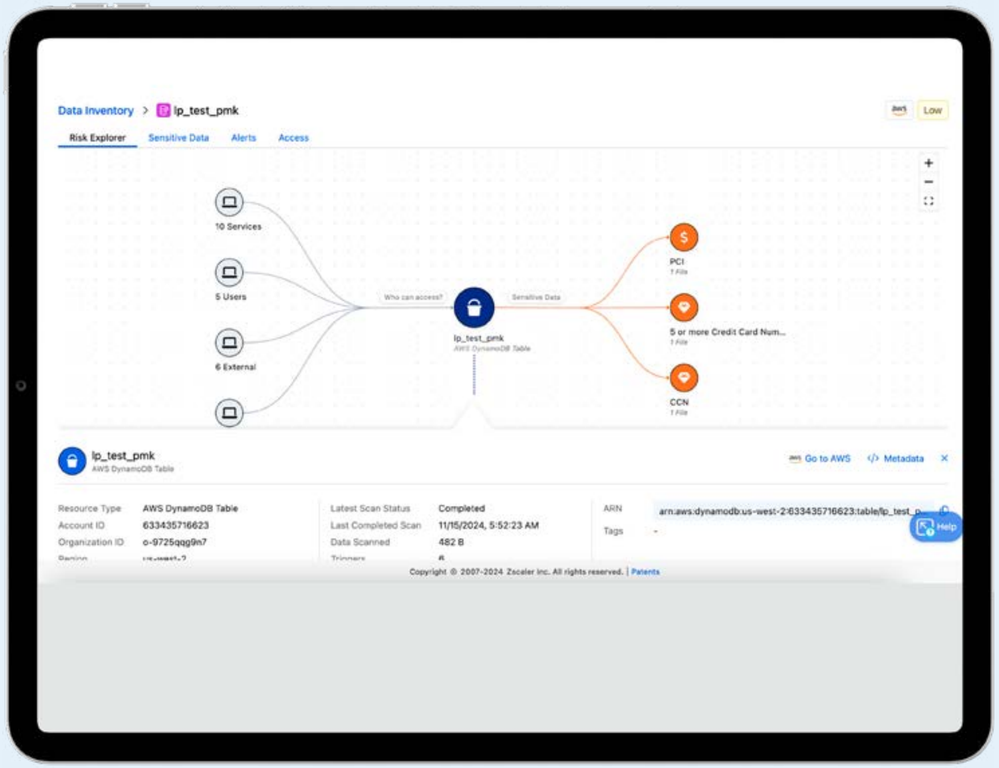
Con DSPM, las organizaciones pueden aprovechar los beneficios de la IA. En lugar de bloquear o prohibir las herramientas de IA, las organizaciones pueden gestionar los riesgos de la IA en la sombra con DSPM al tiempo que aprovechan los beneficios de la IA. La capacidad de seguridad de IA integrada de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

- Obtenga una vista de 360 grados de sus modelos, agentes y servicios de IA
- Identifique y proteja los datos de entrenamiento de IA frente a envenenamiento de datos, errores de configuración y exposición
- Alinee su organización con los nuevos y emergentes marcos de cumplimiento para IA.

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

5. Ibid.





Clasificación de datos impulsada por 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 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 fracasan a la hora de integrar la clasificación dentro de una plataforma centralizada y unificada. Esto genera alertas inconsistentes y visibilidad fragmentada, especialmente cuando los datos se mueven a través del ecosistema de una organización.

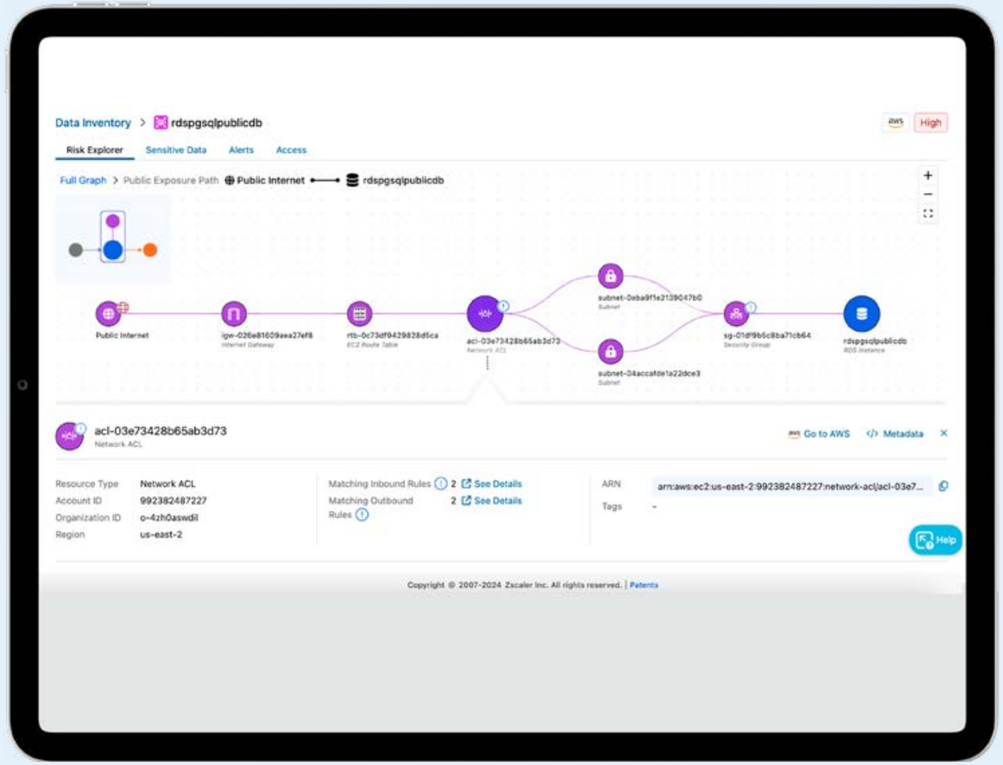
Los responsables de seguridad pueden aprovechar DSPM con la clasificación LLM impulsada por IA que mejora el funcionamiento en torno a los flujos de trabajo tradicionales de expresiones regulares. Con ello, se brinda una visibilidad y flexibilidad increíbles que les permiten proteger datos confidenciales conocidos y desconocidos como nunca antes. A diferencia de las técnicas dependientes de contraseñas, 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 contraseñas 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 responsables de seguridad necesitan una forma 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. Al analizar y correlacionar datos, los algoritmos de IA pueden predecir posibles riesgos de seguridad. Este enfoque proactivo permite a las organizaciones mantenerse un paso por delante de las amenazas y los riesgos críticos.

DSPM aprovecha la IA y técnicas de correlación avanzadas 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 dirijan 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 y detectar riesgos ocultos de forma proactiva, lo que permite priorizar los esfuerzos de seguridad en los datos más críticos.



49 %

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

6.Informe de IBM sobre el coste de una filtración de datos 2025

Optimice el cumplimiento con gobernanza en tiempo real

Mantener el cumplimiento de las regulaciones y los protocolos de seguridad internos es una de las piedras angulares de la IA y la seguridad de los datos, desde el RGPD hasta la SEC. Hoy en día, las organizaciones deben explorar y cumplir no solo las normativas establecidas, como el RGPD y la HIPAA, sino también los marcos emergentes dirigidos específicamente a 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, se influyen profundamente entre sí y dan forma a la trayectoria de una organización. Las infracciones pueden desencadenar sanciones por incumplimiento, lo que genera graves repercusiones y multas importantes empañando con ello la reputación de una organización. Por el contrario, adoptar regulaciones puede servir como escudo, fortificando los datos contra vulnerabilidades y amenazas de seguridad.

Muchas regulaciones 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 la IA y los entornos de datos puede convertirlo en todo 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 internacional. Este terreno regulatorio en constante cambio exige vigilancia y adaptación constantes por parte de las organizaciones que desean seguir cumpliendo la normativa. Los enfoques tradicionales de cumplimiento normativo, con sus visiones fragmentadas, evaluaciones manuales y respuestas reactivas, fracasan a la hora de brindar claridad y eficiencia.

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 amplia perspectiva del estado de cumplimiento de los datos, análisis exhaustivos, evaluación comparativa, corrección y generación de informes para actuar con rapidez ante sus deficiencias 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 garantiza 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 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

Consiga acceso con privilegios mínimos

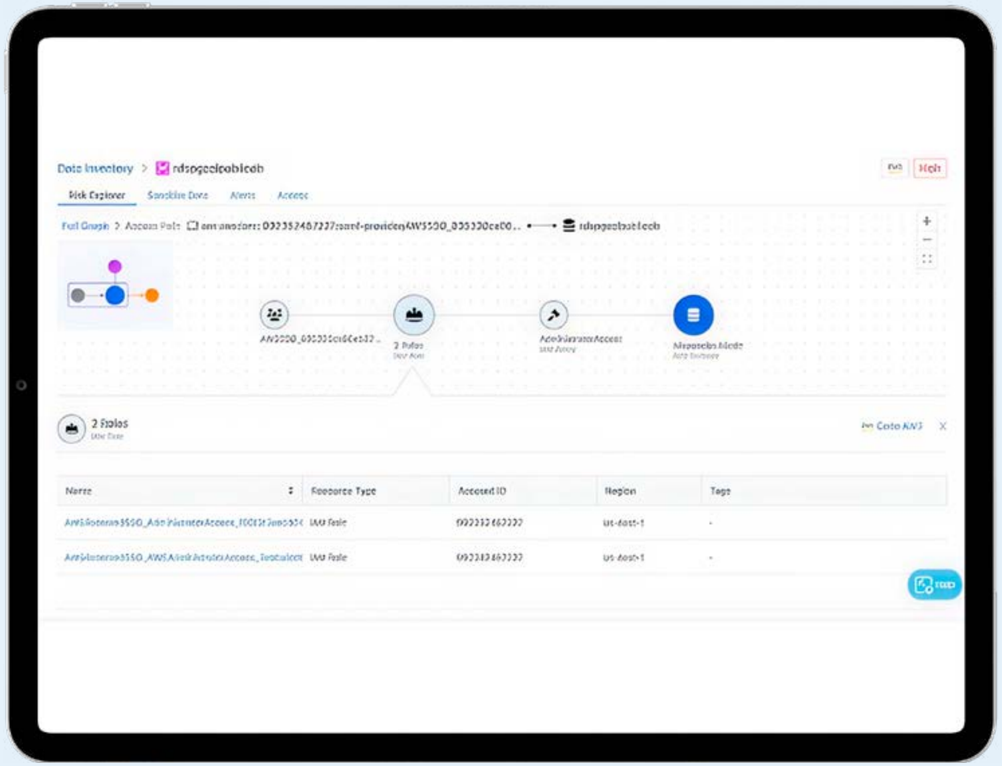
Debido al enorme volumen de usuarios, aplicaciones y recursos, los entornos de datos conllevan un riesgo significativo de controles de acceso inadecuados, proliferación de identidades y almacenamiento de datos huérfanos. Aproximadamente el 90 % de las organizaciones sufrieron brechas de seguridad relacionadas con laidentidad, 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 la divulgación involuntaria o no autorizada de datos confidenciales , la exfiltración de datos (donde se roban datos confidenciales a través de los resultados de la IA) y los ataques sofisticados, en los que las identidades comprometidas explotan los sistemas de IA para obtener acceso no autorizado.

Por ello, garantizar el acceso con mínimos privilegios 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, el aumento de permisos y las complejas arquitecturas de 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.

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. DSPM analiza minuciosamente los roles, permisos y atributos relacionados con la gestión de identidades y acceso a datos para identificar rápidamente las rutas de acceso arriesgadas a los almacenes de datos. DSPM admite datos estructurados, no estructurados y en entornos locales, multinube y SaaS, lo que permite a las organizaciones identificar y abordar de forma consistente los riesgos de acceso 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 posibles vulnerabilidades, los equipos de seguridad de datos pueden aplicar el acceso con menos privilegios de forma más efectiva. Este enfoque reduce el riesgo de acceso no autorizado y mejora la seguridad general del entorno de datos.

8. Security Today, 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 organizaciones han sufrido un incidente relacionado con la identidad[8]

Optimice los costes de almacenamiento y consumo

Los equipos de datos necesitan optimizar los costos de almacenamiento y consumo identificando repositorios de datos duplicados o desatendidos que pueden 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 DSPM pueden resolver este problema al brindar información sobre almacenes de datos duplicados o abandonados, lo que permite a las organizaciones tomar las medidas adecuadas. De igual manera Zscaler DSPM proporciona una vista integral de los almacenes de datos duplicados o abandonados, lo que permite a los equipos identificar aquellos datos que se pueden eliminar o migrar de forma segura.

Con información impulsada por 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, mantener políticas de seguridad de datos consistentes en diversos entornos supone un enorme desafío. Las soluciones DSPM pueden superar esta dificultad al ofrecer un enfoque unificado para la seguridad de los datos en entornos multinube, 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 integral de los datos en la nube y agilizando el proceso de identificación y resolución de riesgos. Al utilizar información impulsada por IA/ML, las organizaciones pueden reducir el riesgo de infracciones de datos y cumplir mejor las reglas de protección de la información.

Respuesta rápida a incidentes

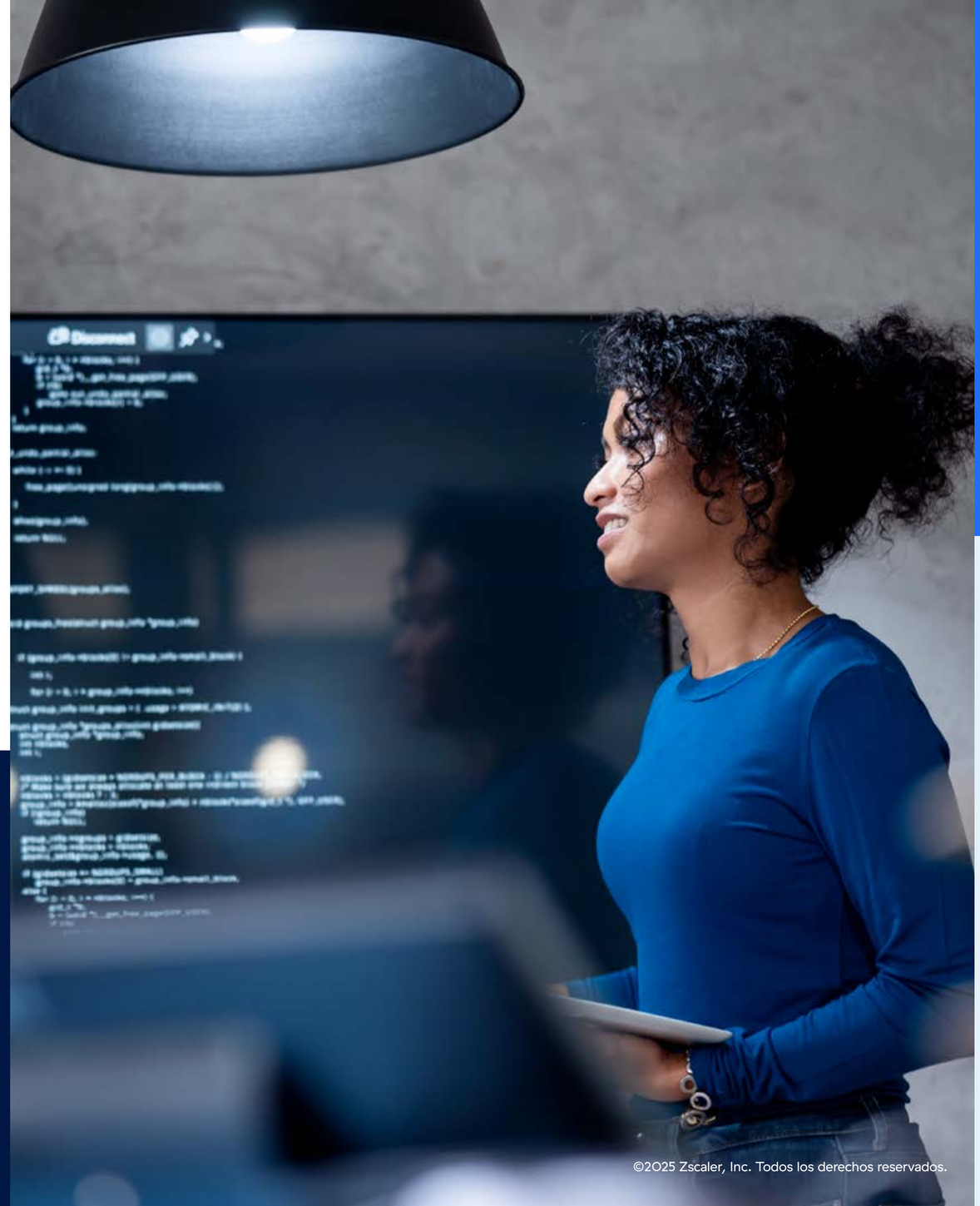
Identificar y mitigar riesgos son tareas fundamentales para los profesionales de la seguridad de datos. La velocidad a la que evolucionan las amenazas requiere respuestas en tiempo real. Sin embargo, las metodologías convencionales pueden fallar ante un entorno de amenazas dinámico promovido por la IA.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

DSPM puede supervisar datos de forma continua, detectar anomalías y ayudar a responder a las amenazas. Las soluciones DSPM refuerzan la reducción de riesgos al ofrecer una sofisticada correlación de riesgos e inteligencia de acceso adaptativa. Algunas soluciones 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 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 brechas de datos en todo el mundo de 2017 a 2024**, consultado el 9 de diciembre de 2024.

194 días

El tiempo promedio para identificar una violación de datos es[9]



Seguridad de IA mejorada

Las organizaciones están adoptando aplicaciones de IA a un ritmo vertiginoso. Desafortunadamente, aplicaciones como la IA generativa y los grandes modelos de lenguaje (LLM) han introducido importantes riesgos de filtración de datos e incumplimiento normativo. Un informe reciente indicó que el 13 % de las organizaciones informaron de vulneraciones 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 la IA generativa en sus operaciones deben tomar medidas para evitar el uso inadvertido de datos confidenciales dentro de estos modelos. Los equipos de seguridad deben dar prioridad al marcado, el etiquetado y la clasificación de datos para garantizar que los equipos multifuncionales aprovechen la IA generativa de manera responsable.

DSPM mejora el control y la protección de datos en entornos de IA generativa gracias a sus capacidades integradas de gestión de postura de seguridad de la IA.

AI identificar y categorizar meticulosamente los datos, DSPM evita la transmisión de información confidencial a los sistemas de gestión de aprendizaje (LLM), reduciendo así el riesgo de filtraciones de datos e incumplimiento normativo. 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 el descubrimiento, la clasificación y la supervisión continua de los datos a lo largo de su ciclo de vida, DSPM ayuda a reducir 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 de gestión de postura de seguridad de la IA integradas 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 fiables 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

Aprovechamiento de DSPM para proteger un panorama de datos diverso

El uso estratégico de DSPM es fundamental en la búsqueda de una seguridad de datos más sólida. Estas tecnologías ofrecen el contexto y la automatización necesarios para gestionar eficazmente las complejidades de los entornos de datos modernos. Mediante una postura proactiva, los responsables de seguridad pueden proteger de manera más eficaz los datos confidenciales, garantizar el cumplimiento y reducir los riesgos asociados con tecnologías progresivas como la IA generativa.

"Para 2026 más del 20 % de las organizaciones implementarán tecnología DSPM, debido a la apremiante necesidad de identificar y localizar depósitos de datos previamente desconocidos y reducir los riesgos de privacidad y seguridad que conllevan".

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 de protección de datos integrada más completa del mundo que protege datos estructurados y no estructurados en la web en entornos SaaS, de nube pública (AWS, Azure, GCP), aplicaciones locales y terminales.

Zscaler DSPM 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.

Zscaler DSPM adopta un enfoque unificado impulsado por IA para garantizar una sólida higiene de datos en todos los almacenes de datos, incluidos IaaS, SaaS, locales, terminales y más. Integrada de forma nativa con la plataforma de seguridad de datos de Zscaler, le permite comprender y controlar completamente todos sus datos en una única plataforma.

La plataforma de segurida de datos de Zscaler utiliza un motor DLP único y unificado para ofrecer la mejor protección de datos consistente y de su clase en todos los canales. Al seguir a todos los usuarios en todas las ubicaciones y controlar los datos en uso y en reposo, garantiza que los datos confidenciales estén perfectamente protegidos y se logre el cumplimiento

Para más información, visite zscaler.com/es/dp/dspm.

Explore el recorrido interactivo del producto DSPM

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

Vea el seminario web a petición ⟶

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, resilientes y seguros. Zscaler Zero Trust Exchange™ protege a miles de clientes de ciberataques y de la pérdida de datos gracias a la conexión segura de usuarios, dispositivos y aplicaciones ubicados en cualquier lugar. Distribuida en más de 150 centros de datos en todo el mundo , Zero Trust Exchange™ basada en SSE es la mayor plataforma de seguridad en línea en la nube del mundo. Para obtener más información, visite **www.zscaler.com/es** o síganos en Twitter **@zscaler**.

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