COHESITY

GUÍA DEL COMPRADOR

NAVEGUE ENTRE DATOS Y EL RIESGO DE LA IA CON LA SOLUCIÓN DE DSPM ADECUADA

Resumen ejecutivo

Ahora los datos confidenciales se distribuyen en plataformas en la nube, SaaS, bases de datos, copias de seguridad, infraestructuras híbridas, NAS y más. Es probable que ya tenga más datos de los que puede controlar fácilmente. Sin embargo, es difícil entender en dónde se encuentran sus datos más confidenciales, qué tan ampliamente están expuestos, quién tiene acceso a ellos y si el acceso es apropiado.

Esto crea una tormenta perfecta que amplifica el riesgo empresarial al nivel de la junta directiva. Y el desafío es cada vez mayor: incluso a medida que las personas acceden, alteran y mueven esos datos, los agentes de IA están introduciendo un nuevo y creciente riesgo.

Estas brechas de seguridad y protección son el motivo por el que la gestión de la postura de seguridad de los datos (DSPM) se ha convertido en una prioridad estratégica para los líderes empresariales modernos.

El 89 % **de los directores de seguridad indican que el estado actual de la seguridad de datos en su empresa es un problema.**

El 39 % **de los directores de seguridad indican que las tecnologías tradicionales son insuficientes para los requisitos actuales.**

El 60 % **de las empresas carecen de visibilidad en al menos la mitad de su patrimonio de datos.**[1]

[1]Documento técnico de Omdia: Cómo lograr la resiliencia cibernética con inteligencia de información accionable

Una solución de DSPM moderna debería ayudarlo a hacer mucho más que inventariar datos. Eso debería ayudarle a reducir activamente el riesgo, reforzar la resiliencia cibernética y responder preguntas críticas durante la respuesta a incidentes, simulacros de seguridad o auditorías:

- ¿Dónde están y cuáles son nuestros datos confidenciales?
- ¿Quién o qué tiene acceso a ellos?
- ¿Qué debemos resolver primero?
- ¿Cómo reducir el riesgo sin desacelerar la innovación y el crecimiento de la empresa?
- ¿Están protegidos los datos y pueden recuperarse de manera rápida, segura y normada?

Para los directores de seguridad, esto significa pasar de la visibilidad a una reducción de riesgos accionable antes y después de que ocurra un ataque.

Esta guía es para los equipos humanos que evalúan soluciones de DSPM, de modo que usted pueda seleccionar la más adecuada a sus necesidades.

El inventario no es suficiente.

La verdadera pregunta de compra no es si una solución puede mostrarle en dónde están los datos. Sino ver si la solución puede identificar y mostrar *por qué* es de alto riesgo y qué puede hacer usted ahora para remediar ese riesgo.

Lo que la DSPM resuelve

Uno de los errores más comunes que cometen las organizaciones al evaluar la DSPM es tratarla como una simple herramienta de exploración. Una solución de DSPM es mucho más que visibilidad. La solución correcta debería ayudarle a resolver problemas relacionados con la postura de riesgo de sus datos.

Estos son cinco problemas que su solución de DSPM debería ayudarle a resolver:

Problema	Cómo lo resuelve la DSPM
No sé dónde están mis datos confidenciales.	Pocas organizaciones pueden responder con confianza en dónde residen sus datos regulados o de mayor valor en entornos de nube, SaaS e híbridos. ¿Por qué es este el estado de las cosas? Las herramientas tradicionales de seguridad de los datos se limitan a tipos específicos de información, a ciertos modelos de implementación o a casos de uso específicos. Incluso cuando se tiene algún inventario, este suele estar incompleto, desactualizado o desconectado del contexto de riesgo. Se requiere una arquitectura moderna, nativa de la nube, para mantenerse al día con el volumen y la amplitud de los datos.
No sé quién o qué está accediendo (o puede acceder) a mis datos.	El empleado típico interactúa con aproximadamente 36 servicios de nube cada día, en más de 200 herramientas de colaboración. La información confidencial se distribuye entre plataformas y a menudo se comparte fuera de los controles de gobernanza establecidos. Los datos confidenciales se vuelven aún más riesgosos cuando están sobreexpuestos, se conceden permisos en exceso, se comparten de forma demasiado amplia, se almacenan en un lugar equivocado o están accesibles para más identidades (humanas y no humanas) de las previstas. Su solución de DSPM deberá ayudarle a comprender qué datos están en riesgo, no solo qué datos coinciden con una política de clasificación.
No sé qué riesgos de los datos debería priorizar para la remediación.	La mayoría de los entornos empresariales contienen grandes cantidades de datos confidenciales. Sin embargo, no todos los riesgos de datos tienen la misma urgencia. Los equipos humanos necesitan una forma de distinguir el ruido de fondo de la exposición significativa. La solución correcta deberá ayudarle a enfocarse en los problemas con el mayor impacto potencial en la empresa, en función de la sensibilidad, el acceso, la exposición, el entorno y el contexto empresarial aprendido.
No puedo remediar los riesgos de los datos de forma rápida o automática.	El contexto de los datos, combinado con una integración profunda a la cadena de herramientas de seguridad, es esencial para reducir el tiempo medio hasta la respuesta (MTTR) al remediar datos que están en alto riesgo. Los métodos tradicionales de seguridad de los datos dependen en gran medida de patrones y etiquetas, lo que abruma a los equipos humanos con alertas ruidosas que a menudo carecen de credibilidad. Las soluciones de DSPM deben promover la acción. Los hallazgos deberán ser comprensibles, asignables y rastreables. Los equipos de seguridad y de TI deberán poder actuar sobre ellos con confianza.
Cuando necesito recuperar datos, el proceso es lento, riesgoso y costoso.	Los datos secundarios (por ejemplo, copias de seguridad) son críticos cuando se trata de la respuesta a incidentes y la recuperación. Estos datos también pueden introducir riesgos y posibles incumplimientos normativos que será necesario atender. Las soluciones de DSPM modernas deberán reforzar los resultados de resiliencia cibernética y alimentar la inteligencia de datos para ayudar a asegurar que se apliquen los niveles de protección adecuados. Los datos confidenciales deben priorizarse y recuperarse de manera normada durante la respuesta a incidentes.

Qué aspecto tiene lo “bueno”

Antes de evaluar a los proveedores, debe decidir cómo se ve “lo bueno”. Estas son cinco áreas en las que toda solución de DSPM moderna deberá sobresalir:

Implementar rápidamente y escalar sin problemas ni límites

Un buen descubrimiento deberá ayudarle a obtener rápidamente una visión más completa de su exposición sin necesidad de un ciclo de implementación largo y pesado, antes de que aparezca el valor.

Las organizaciones deberán esperar un escaneo continuo de cientos de petabytes, sin poner en riesgo el rendimiento. El proveedor ideal ofrecerá un amplio soporte en los entornos clave, como almacenes de datos en la nube, aplicaciones de SaaS, sistemas de archivo y bases de datos locales, cuando corresponda.

Elimine puntos ciegos con descubrimiento y clasificación precisos

Un buen descubrimiento ayuda a evitar que los resultados deficientes contaminen todos los resultados ulteriores. Si la herramienta de DSPM pasa por alto ubicaciones críticas, clasifica erróneamente la información confidencial o requiere demasiados ajustes manuales, los hallazgos serán menos útiles o incluso irrelevantes.

La solución de DSPM ideal revela puntos ciegos adaptándose a su entorno y clasifica los datos automáticamente (incluidos la IP y los datos particularmente relevantes para su negocio).

Priorice el riesgo real, no el ruido

El tiempo es limitado; ningún equipo humano puede remediar todo a la vez. Una buena solución de DSPM combina exposiciones y contexto para enfocarse en los mayores peligros. Dicha solución deberá priorizar el riesgo a partir de datos altamente confidenciales y con exposiciones amplias.

Esto requiere capacidades avanzadas para correlacionar la sensibilidad de los datos, el propósito empresarial, las identidades, la actividad de acceso y la exposición para sacar a la luz el riesgo real para la empresa.

Automatice la remediación a escala

Las soluciones de DSPM modernas necesitan ayudar a las organizaciones a reducir la exposición, no solo a observarla. Las organizaciones deberán buscar soluciones de DSPM que ofrezcan remediaciones listas para aplicar. Por ejemplo, las mejores soluciones ofrecen controles con un solo clic para revocar el acceso, enmascarar datos, activar flujos de trabajo predefinidos y encauzar los problemas directamente a los responsables de los datos, todo con el contexto necesario para resolver rápidamente los problemas.

Esto es particularmente importante a escala empresarial, donde participan muchos equipos humanos. Los equipos de seguridad identifican a menudo el problema, pero la remediación puede depender de diferentes grupos, por ejemplo, administradores de almacenamiento, responsables de datos, equipos humanos de identidad o los inversores de la empresa. Cuanto más claramente respalde una solución ese traspaso, más probable será que impulse resultados significativos que mejoren su postura de seguridad.

Refuerce la seguridad antes y después de los incidentes

Ya cubrimos la reducción proactiva del riesgo antes de que ocurra una brecha. La solución de DSPM adecuada también puede ofrecer la inteligencia de datos y el contexto necesarios para reforzar los esfuerzos de recuperación, asegurando que el personal de seguridad y de protección de datos comprenda en dónde residen los datos confidenciales, qué activos son los más delicados y si se han aplicado protecciones adecuadas a las joyas de la corona de la organización.

Con una visión clara de los datos más confidenciales y delicados para la empresa, la DSPM deberá informar y mejorar las estrategias de protección de datos que son la base de la resiliencia cibernética. Esto le ayudará a priorizar los datos más importantes durante la recuperación, acelerar la respuesta a incidentes con un mejor contexto, y reducir el costo y la complejidad al identificar y eliminar datos obsoletos, redundantes o de bajo valor.

El resultado es un bucle de retroalimentación continuo entre visibilidad, protección, respuesta y recuperación. Con la solución de DSPM adecuada, deberá poder conectar estas funciones para pasar de los esfuerzos de seguridad aislados, a una estrategia más holística e integral de seguridad de los datos y resiliencia cibernética.

Kit de evaluación de proveedores

Preguntas críticas que debe hacer a los proveedores

Las siguientes preguntas le ayudarán a evaluar su lista de productos de DSPM preseleccionados.

Sobre descubrimiento y cobertura:

- ¿Qué entornos de nube, SaaS, IA, de bases de datos o híbridos admiten actualmente?
- ¿Cómo identifican y clasifican los datos confidenciales en los diferentes tipos de datos? ¿Cuánto tiempo suele tardar eso?
- ¿Cómo manejan los datos estructurados y no estructurados? ¿Tiene usted mejor soporte para uno u otro?
- ¿Qué nivel de ajuste se requiere antes de que los resultados sean utilizables?
- ¿Cómo ayuda usted a los clientes a validar la cobertura y la confianza de manera oportuna?

Sobre los controles de exposición y acceso:

- ¿Cómo determina usted si los datos confidenciales están sobreexpuestos? ¿Puede mostrar qué identidades, grupos o usuarios tienen acceso a los datos confidenciales?
- ¿Cómo identifica usted el acceso amplio, excesivo o riesgoso?
- ¿Cómo conecta usted el contexto de acceso con la sensibilidad de los datos?
- ¿Puede usted bloquear cuáles datos confidenciales entran o salen de los modelos y sistemas de IA?
- ¿Puede demostrar cómo es que su solución destaca los problemas de mayor riesgo?

Sobre la priorización y la remediación de riesgos:

- ¿Cómo clasifica o prioriza usted los hallazgos? ¿Qué factores influyen en la gravedad o la puntuación del riesgo?
- ¿Puede mostrar cómo es que los equipos humanos pasan de muchos hallazgos a un plan de acción manejable?
- ¿Cómo es que su solución orienta la remediación?
- ¿Se pueden asignar los hallazgos a los equipos humanos o responsables correctos?
- ¿Se pueden incluir hallazgos sin problemas en las plataformas de protección de datos y ofrecer mejores resultados de seguridad y recuperación?

Sobre el tiempo hasta el valor y la implementación:

- ¿Qué es lo que la implementación inicial requiere de nuestro equipo humano?
- ¿Con qué rapidez podemos esperar hallazgos útiles?
- ¿Cómo deberá verse el éxito en los primeros 30, 60 y 90 días?

Señales de alerta a las que debe estar atento

Visibilidad limitada del riesgo de acceso

El acceso a datos confidenciales es el mayor riesgo. Si un proveedor no puede demostrar claramente quién (o qué) puede acceder a los datos y qué riesgos existen, esa es una limitación seria.

Los hallazgos no se relacionan con el riesgo y el contexto empresarial individual

Cada empresa es diferente. El riesgo que representan los datos confidenciales o la propiedad intelectual expuesta puede variar según lo que sea importante para la organización. Los hallazgos deberán basarse en el contexto y los clasificadores aprendidos para ofrecer recomendaciones precisas de remediación de riesgos.

Incapacidad para vincular el riesgo de los datos con los resultados de resiliencia cibernética

Optimizar la postura de riesgo de los datos y la IA es fundamental para la resiliencia cibernética. Deberá recurrirse a la inteligencia de datos para orientar la seguridad proactiva de los datos y permitir que haya mejores resultados de recuperación. Los hallazgos no deben quedar aislados, en especial porque la remediación suele involucrar equipos interdisciplinarios.

El valor depende de un esfuerzo manual excesivo

Un producto que requiera amplios ajustes, interpretaciones o diseño de procesos del cliente puede agregar costos operativos y complejidad continuos.

Tabla comparativa de proveedores

Utilice esta tabla para comparar proveedores lado a lado, en función de las capacidades principales necesarias para una estrategia de DSPM eficaz. Al revisar cada fila, considere no solo si existe una característica, sino qué tan bien funciona en la práctica.*

Para que las comparaciones de proveedores sean más uniformes y objetivas, cada capacidad se puede evaluar mediante un modelo de puntuación simple de 0 a 5.

Esta estrategia ayuda a los equipos humanos a ir más allá de una comparación básica en la que se marcan casillas, y a evaluar la fortaleza relativa, la madurez y la utilidad práctica de cada capacidad. Un puntaje alto deberá indicar que la capacidad no solo está disponible, sino que también está lista para la empresa, es operativamente eficiente y se ha demostrado que ofrece valor a escala.

Puntaje	Definición
5	La mejor capacidad de su clase, totalmente implementada, altamente automatizada, escalable y bien integrada
4	Capacidad sólida con funcionalidad robusta y brechas menores
3	Capacidad adecuada que cumple con los requisitos principales, pero con limitaciones en profundidad, escala o facilidad de uso
2	Soporte básico o parcial con brechas notorias, esfuerzo manual o aplicabilidad limitada
1	Capacidad mínima, funcionalidad en las etapas tempranas o soporte muy limitado
0	No compatible o sin evidencias significativas

Categoría	Proveedor 1	Proveedor 2	Proveedor 3	Notas
Arquitectura nativa de la nube para una implementación rápida y sin agentes				
Descubrimiento continuo de datos a escala y velocidad				
Clasificación de datos basada en la IA				
Contextualización de datos				
Riesgos mapeados según las regulaciones				
Controles y vigilancia del cumplimiento de acceso adaptable				
Detección de datos y respuesta en tiempo real				
Alertas contextualizadas				
Flujos de trabajo de remediación integrados				
Integración perfecta con plataformas de protección de datos				
Total				

**Los puntajes deberán basarse en lo que está disponible hoy en general, no en las afirmaciones del mapa de ruta. Cada puntaje deberá validarse mediante demostraciones de productos, referencias de clientes, documentación, requisitos de implementación y pruebas de la profundidad de integración.*

Conclusión

Seleccionar una solución de DSPM es más que una simple decisión de selección de herramientas. Hay demasiado en juego. Los datos continúan proliferando y dispersándose a velocidad alarmante, y las estrategias manuales o la tecnología tradicional no pueden seguirles el paso. La solución de DSPM adecuada le ayudará a crear claridad, enfocar la atención de sus equipos, reducir el riesgo y reforzar tanto los resultados de seguridad de los datos, como los de resiliencia cibernética. Esta solución rendirá dividendos a largo plazo, ya que le ayudará a proteger y asegurar los datos que sustentan sus modelos, sistemas y agentes de IA.

Obtenga más información sobre nuestra solución de DSPM y cómo puede optimizar su postura ante los riesgos para sus datos y la IA. O bien, contáctenos hoy mismo.

COHESITY

cohesity.com
1-855-926-4374
2625 Augustine Drive, Santa Clara, CA 95054

4500066-001-ES 5-2026