Data Security Posture Management

Data Security Posture Management (DSPM): la solución para la protección de datos

Bajo la premisa de que “los datos son el activo más valioso para las empresas”, todas las organizaciones son conscientes de que una adecuada seguridad de los datos es prioritaria para las áreas de seguridad de sus compañías. El problema surge ante el escenario que encuentran a la hora de implantarla: arquitecturas en constante cambio, datos fragmentados en multitud de aplicaciones, proveedores de SaaS, y entornos cloud que han modificado sustancialmente el funcionamiento de las empresas. El movimiento de los datos ahora es más sencillo y ágil que nunca, pero lo que es una ventaja a la hora de ser más eficientes, se convierte en un problema para las empresas, ya que aumenta el riesgo de exposición de los datos.

¿Qué es un DSPM?

Gartner identifica “**Data Security Posture Management**” (*Gestión de la Postura de la Seguridad de los Datos*) como una tecnología emergente: **DSPM** proporciona visibilidad sobre dónde se encuentran los datos sensibles, quién tiene acceso a estos, cómo son utilizados y cuál es la postura de seguridad de la aplicación o sistema donde se encuentran almacenados. Para ello, evalúa el estado actual de la seguridad de los datos, identifica posibles riesgos y vulnerabilidades, aplica controles de seguridad para mitigar estos riesgos y supervisa y actualiza periódicamente la postura de seguridad para garantizar que sigue siendo eficaz. Como resultado, permite a las empresas mantener la confidencialidad, integridad y disponibilidad de los datos sensibles.

La implantación de un DSPM en las compañías resuelve los problemas de seguridad en cualquier entorno mediante la automatización de las actividades de detección y protección de datos en un entorno dinámico y la conexión de datos, aplicaciones e identidades, proporcionando así una imagen completa de la postura de seguridad de una empresa.

DSPM se centra en la capa de datos confidenciales, desde su identificación hasta la monitorización e identificación de riesgos tales como accesos inapropiados, intercambio arriesgado, etc. pudiendo remediar esos problemas, eliminando de esta forma cualquier actividad que pudiese poner datos confidenciales en terceros inapropiados, ya sea internos o externos a la compañía.

DSPM vs CSPM

DSPM se encarga de la ”gestión de la postura de seguridad de los **datos**” mientras que en el caso de un CSPM hablamos de la “gestión de la postura de seguridad en la **nube**”

Un CSPM se centra en la infraestructura de la nube.Su función es proporcionar visibilidad de los activos en la nube y alertas sobre configuraciones erróneas, aborda problemas relacionados con la infraestructura: el cifrado insuficiente, administración incorrecta de claves u otros problemas de permisos de cuenta.

DSPM, en cambio, se centra en los datos y su contexto, y en la clasificación de los mismos en base a su sensibilidad. El descubrimiento de datos y la gestión de la postura no puede limitarse al contexto solo en la nube, sino que también deben incluir cualquier base de datos local, SaaS, … Un DSPM cubre la capa que faltaba en la seguridad en cualquier entorno: la protección de los datos sensibles.

Diferencias entre DSPM y la protección tradicional de seguridad de datos

En ocasiones, la forma en la que trabajan las empresas tradicionales de seguridad de datos es complementaria o trabaja bajo el *paraguas* de un DSPM.Una empresa que realiza cifrado de datos requerirá en muchas ocasiones de un DSPM previo para realizar el descubrimiento de los mismos. En otros casos hablamos de protección tradicional como la de proveedores de gobernanza o clasificación de acceso a datos que fueron diseñadas exclusivamente para datos locales por lo que serían ineficaces para las arquitecturas actuales de las empresas.

Las empresas que utilizan protecciones tradicionales se enfrentan habitualmente a problemas tales como que el descubrimiento de datos requiere que previamente haya que definir las reglas y políticas, conocer qué datos son sensibles, dificultad para manejar grandes volúmenes de datos o la dinámica de los entornos de nube; periodos largos de implantación o funcionamientos como una solución local.DSPM supera todos estos hándicaps ya que identifica de forma autónoma dónde pueden estar en riesgo los datos, derechos inapropiados, usos compartido arriesgados, y múltiples casuísticas sin necesidad de que las empresas escriban previamente las políticas.

DSPM es totalmente eficiente ya que trabaja con un modelo de implementación fácil, operando como una solución SaaS, basado en API, de fácil implementación, capaz de trabajar con datos estructurados y no estructurados y de manejar multitud de datos sin necesidad de la intervención de equipos de seguridad

Implantar un Data Security Posture Management ayuda a abordar los problemas de seguridad mucho mejor que los métodos de seguridad tradicionales ya que, por sí sola, es capaz por sí sola de definir qué datos son confidenciales, qué datos compartidos eran apropiados o no y de reportar sobre estos riesgos a los equipos de seguridad.

DSPM: protección adaptada a las nuevas arquitecturas

Las herramientas de seguridad de datos hasta el momento estaban diseñadas para entornos tradicionales. DSPM surge debido a la necesidad de las empresas de descubrir, monitorizar y proteger datos confidenciales en la nube sin limitaciones, ayudando a abordar desafíos complejos de seguridad de datos.

DSPM permite a las empresas manejar la seguridad de los datos conociendo qué datos se comparten con quién, monitorizando cómo se mueven, identificando los riesgos y alertando a los responsables de seguridad del dato para remediar esos posibles riesgos en el momento en el que ocurren.Todo ello adaptándose a las nuevas arquitecturas mediante enfoques y entornos actualizados que permiten el descubrimiento, la clasificación y la protección integral de datos de una manera integrándose de forma nativa con las características de la infraestructura y las API.

Arexdata DSP: la manera más simple de proteger tus datos

Arexdata te ofrece la Plataforma de Seguridad del Dato que: Audita, Clasifica y Protege el dato en las compañías, proporcionándote una Visibilidad y Trazabilidad Extremo-a-Extremo y de manera Centralizada.