

Forcepoint DSPM



Forcepoint

Brochure

La transformación de la IA es la próxima evolución de la transformación digital

¿Están sus datos seguros en esta nueva era?

La mayoría de las organizaciones que han experimentado la transformación digital ahora se están preparando para la próxima evolución: la transformación de la inteligencia artificial (IA). Esta nueva era de la IA está impulsada por los muchos beneficios que ofrecen las aplicaciones de inteligencia artificial generativa (GenAI), como ChatGPT, Copilot, Gemini y otras. A partir de sus experiencias de transformación digital, las organizaciones han aprendido que la seguridad de los datos debe ser una prioridad. Sin embargo, para muchas organizaciones, los datos de hoy en día son como un iceberg gigante, con su mayoría oculta bajo la superficie. A menudo llamados "datos oscuros" o "datos en la sombra", permanecen invisibles y desconocidos, pero contienen cantidades sustanciales de información confidencial de la que las organizaciones son responsables directamente. Actualmente, las organizaciones están lidiando con cómo permitir a los usuarios aprovechar las aplicaciones de GenAI de manera segura para mejorar la productividad y la eficiencia, a la vez que garantizan la protección de sus datos confidenciales.



DSPM (Data Security Posture Management) ofrece un enfoque integral para proteger su información frente al acceso, divulgación, alteración o destrucción no autorizada de datos. A diferencia de otros tipos de métodos de seguridad de datos que se centran en sistemas y dispositivos, DSPM se centra en la totalidad de los datos de una organización, ya sean estructurados o no estructurados, ya sean propiedad intelectual o datos regulados, ya sea en la nube o en redes privadas, garantizando el cumplimiento y mitigando el riesgo de fugas de datos.



Según IDC, globalmente, el 80% de los datos no están estructurados y el 90 % de esos datos no ha sido analizado; a estos¹ también se los conoce como "datos oscuros".¹



El 94% de las organizaciones almacenan datos en múltiples entornos de nube.²



Equifax resuelve una demanda de \$ 1,4 mil millones por su violación de datos³, exacerbada por piratas informáticos que accedieron a una unidad compartida en la que se almacenaban varias copias de nombres de usuario y contraseñas de empleados. La compañía carecía de herramientas para detectar e identificar archivos redundantes y obsoletos.

¹ El enigma de datos invisibles, Forbes, febrero de 2022

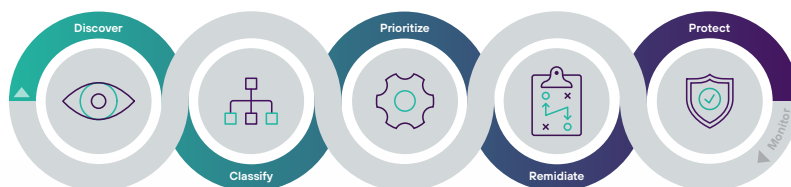
² Datos oscuros: el riesgo desconocido de la seguridad y privacidad de la nube, Forbes, junio de 2023

³ Equifax acepta una conciliación por una demanda por violación de datos de \$1,38 mil millones, Finextra, enero de 2020

¿Qué aborda DSPM?

- **Viaje de transformación de la IA:** Desencadene el potencial de la IA con Forcepoint DSPM, que protege sus datos en todas partes mediante nuestra avanzada tecnología de AI Mesh. Con una visibilidad centralizada y remediación desde Forcepoint DSPM y controles de bloqueo en tiempo real desde Forcepoint DLP, protegemos tu información confidencial en canales clave, incluidas aplicaciones de IA generativa como ChatGPT, Copilot, Gemini y muchas otras, lo que potencia la innovación audaz mientras aumentas la productividad y reduces el riesgo.
- **Identificación de datos confidenciales:** DSPM ayuda a las organizaciones a identificar datos confidenciales en múltiples entornos y servicios en la nube, así como en ubicaciones on-prem, incluyendo datos estructurados y no estructurados. Esto incluye comprender dónde residen los datos confidenciales, cómo se accede a ellos y quién tiene permisos para interactuar con ellos.
- **Evaluación de vulnerabilidad y riesgo:** DSPM reduce la vulnerabilidad de los datos confidenciales a las amenazas de seguridad y al riesgo de incumplimiento normativo. Al analizar la postura de seguridad de los datos, las organizaciones pueden abordar los riesgos potenciales proactivamente.
- **Centrarse en los datos en la fuente:** A diferencia de otras herramientas de seguridad de datos que protegen principalmente dispositivos, sistemas y aplicaciones, DSPM se centra directamente en la protección de la totalidad de los datos de una organización. Su objetivo es prevenir las violaciones de datos y garantizar el cumplimiento mediante la protección de los datos en su núcleo.
- **Abordar datos oscuros y datos redundantes, obsoletos y triviales (ROT):** DSPM aborda directamente datos oscuros (datos que actualmente no se ven ni se usan en procesos comerciales normales). Del mismo modo, DSPM puede abordar datos ROT, que también tienden a proliferar en las organizaciones a medida que las empresas continúan reteniendo grandes cantidades de datos, por varios motivos, pensando que les ayudará a mantenerse en cumplimiento. En realidad, crea un riesgo de datos aún mayor, y DSPM ayuda a administrar este riesgo.
- **Aborda datos con permisos excesivos o sobreexpuestos:** Debido a la forma en que los datos proliferan mediante el copiado y la edición de nuevas versiones de datos, los permisos a los datos a menudo también pueden explotar en usuarios, grupos y hasta la organización entera. DSPM ayuda a implementar el concepto de Zero Trust del "principio de mínimo privilegio" (POLP), el cual reduce drásticamente los datos con permisos excesivos como una forma de prevenir violaciones de datos.
- **Entornos de nube múltiple e híbrida:** A medida que las organizaciones adoptan entornos de nube múltiple e híbrida, el riesgo de violaciones de datos aumenta drásticamente. DSPM proporciona visibilidad y control sobre datos confidenciales en estos diversos entornos informáticos, además de ubicaciones on-premises.
- **Monitoreo continuo de riesgos:** El complemento Forcepoint Data Detection and Response (DDR, Detección y Respuesta de Datos) permite a Forcepoint DSPM detectar y remediar nuevos riesgos de datos a medida que ocurren. No es necesario esperar al próximo análisis completo de DSPM, identifique dinámicamente los riesgos para su postura de seguridad de datos para remediarlos.

Forcepoint DSPM está diseñado para la organización moderna que necesita una visibilidad y un control robustos de sus datos confidenciales. Proporciona visibilidad en varios entornos y servidores en la nube para evitar fugas de datos y reducir el riesgo de incumplimiento de las regulaciones de privacidad. Forcepoint ofrece visibilidad y control completos en todo el ciclo de vida de los datos, proporcionando Data Security Everywhere al combinar la **detección proactiva de riesgos de datos** (DSPM) con **controles activos sobre cómo se utilizan los datos** (DLP), al tiempo que **se adapta continuamente a las acciones de cada usuario** (Risk-Adaptive Protection). Obtenga un descubrimiento dinámico de los riesgos de los datos con monitoreo continuo (Forcepoint DDR) para evitar las fugas de datos y proteger su postura de seguridad de datos.



Descubrimiento, clasificación y orquestación impulsados por la IA



Unifique la visibilidad y el control sobre su entorno de datos con Forcepoint DSPM

Administrar y proteger los datos de tu organización nunca ha sido tan complejo. Forcepoint DSPM ofrece una solución potente para obtener visibilidad y control completos sobre tus datos, independientemente de la ubicación. Con velocidades de descubrimiento y capacidades avanzadas de clasificación de datos de AI Mesh líderes en la industria, Forcepoint DSPM te permite tomar decisiones informadas sobre tu postura de seguridad de datos y abordar potenciales riesgos de manera proactiva.

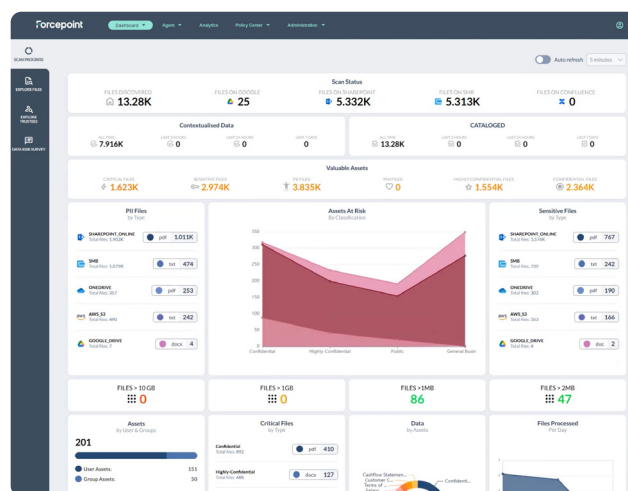
Los beneficios clave de Forcepoint DSPM incluyen:

Detección rápida e integral: En múltiples nubes y on-prem, Forcepoint DSPM es capaz de escanear rápidamente archivos y bases de datos. No es raro que las organizaciones tengan muchos terabytes e incluso algunas tengan petabytes de datos, con organizaciones muy grandes que incluso tienen exabytes de datos bajo su responsabilidad. Con el descubrimiento de alto rendimiento, Forcepoint permite a las organizaciones obtener una vista rápida de los datos en un entorno de datos masivo, incluido ChatGPT Enterprise. A diferencia de otros proveedores de DSPM, Forcepoint no cobra por los escaneos de descubrimiento: los clientes pueden ejecutar escaneos de detección con la frecuencia que deseen sin cargos adicionales.

Precisión habilitada por la malla de la IA: Forcepoint DSPM descubre datos en fuentes de nube y red, y los clasifica automáticamente mediante el uso de un motor de clasificación de IA avanzado. La malla de IA de Forcepoint DSPM empodera a las organizaciones con una precisión superior de clasificación de datos. Su arquitectura de IA en red, que aprovecha un modelo de lenguaje pequeño (SLM) de GenAI, así como datos avanzados y componentes de la IA, captura de manera eficiente el contexto del texto no estructurado. Personalizable y eficiente, garantiza una clasificación rápida y precisa sin la necesidad de capacitaciones intensivas, lo que aumenta la confianza y el cumplimiento. En última instancia, esta alta precisión ha permitido a organizaciones que tenían problemas con otros métodos populares de clasificación reducir drásticamente los falsos positivos y negativos, lo cual ha resultado en una protección exitosa de su propiedad intelectual y un ahorro considerable en términos de tiempo y recursos.

Visibilidad de datos en todo el entorno de datos:

Forcepoint DSPM le permite inspeccionar los permisos de todos los archivos y usuarios. Los administradores de datos pueden ver quiénes tienen acceso a un archivo o a los archivos compartidos en toda la organización. Con un solo clic, puede ver inmediatamente los permisos para todos los archivos que se escanean. Forcepoint DSPM proporciona un panel de control con amplios detalles que ofrecen una vista panorámica de los datos oscuros, así como una evaluación general de riesgos de datos para ayudarle a comprender las áreas de mayor riesgo de datos.



Orquestación de flujo de trabajo: Defina fácilmente la propiedad y la responsabilidad para diferentes conjuntos de datos para optimizar el proceso de obtener la alineación de las partes interesadas. Esto permite flujos de trabajo más eficientes en torno a las acciones que se realizan en cada fuente de datos y activo. Una remediación eficaz requiere una amplia aceptación y colaboración, más allá de la organización de seguridad, del director de datos o el grupo de gobernanza, riesgo y cumplimiento (GRC), así como de funciones como marketing, finanzas, DevOps y muchas otras. Forcepoint DSPM considera la postura ante la seguridad de los datos no solo como un problema de seguridad, sino como una prioridad comercial.

Forcepoint DDR: Un poderoso complemento de Forcepoint DSPM y una solución clave para abordar las fugas de datos. Proporciona una detección de amenazas continua y visibilidad mejorada de los riesgos de los datos, lo que garantiza que las organizaciones puedan ver de forma eficaz los cambios en los datos que probablemente estén llevando a fugas mientras ocurren. Al aprovechar respuestas impulsadas por IA, Forcepoint DDR ofrece una neutralización precisa de las amenazas, lo que ayuda a las organizaciones a mantener medidas de seguridad sólidas. Su amplia visibilidad en la nube y los dispositivos finales, combinada con el seguimiento del linaje de datos, la convierte en una herramienta esencial para proteger información confidencial, reducir las pérdidas financieras y mantener la confianza del cliente.



No permita que el riesgo de datos paralice su negocio. ¡Forcepoint puede ayudar!

En la era digital actual, los datos son el activo más valioso de una organización, pero también pueden ser una responsabilidad importante si no se administran adecuadamente. Forcepoint DSPM ofrece un enfoque proactivo para proteger sus datos confidenciales, mitigar riesgos de violaciones de datos y garantizar el cumplimiento normativo. Al implementar Forcepoint DSPM, puede obtener una visibilidad completa del panorama de datos, identificar y abordar vulnerabilidades y proteger proactivamente a su organización de daños financieros y reputacionales causados por violaciones de datos e incumplimientos normativos, todo mientras protege sus datos en aplicaciones de GenAI. Tome el control de su postura de seguridad de datos hoy. Comience a explorar cómo DSPM puede proteger su valiosa información. Vaya a www.forcepoint.com/es/dspm para solicitar una demo o regístrese para obtener un data risk assessment gratuito en la que un ingeniero de seguridad puede proporcionarle una muestra de sus propios datos para ver qué tipos de riesgos de datos enfrenta en este momento.



[forcepoint.com/contact](https://www.forcepoint.com/contact)

Acerca de Forcepoint

Forcepoint simplifica la seguridad para empresas y gobiernos globales. La plataforma todo en uno y verdaderamente nativa de la nube de Forcepoint facilita la adopción de Zero Trust y evita el robo o la pérdida de datos confidenciales y de propiedad intelectual sin importar desde dónde trabajen las personas. Con sede en Austin, Texas, Forcepoint crea entornos seguros y confiables para clientes y sus empleados en más de 150 países. Interactúe con Forcepoint en www.forcepoint.com, Twitter y LinkedIn.