Forcepoint DSPM



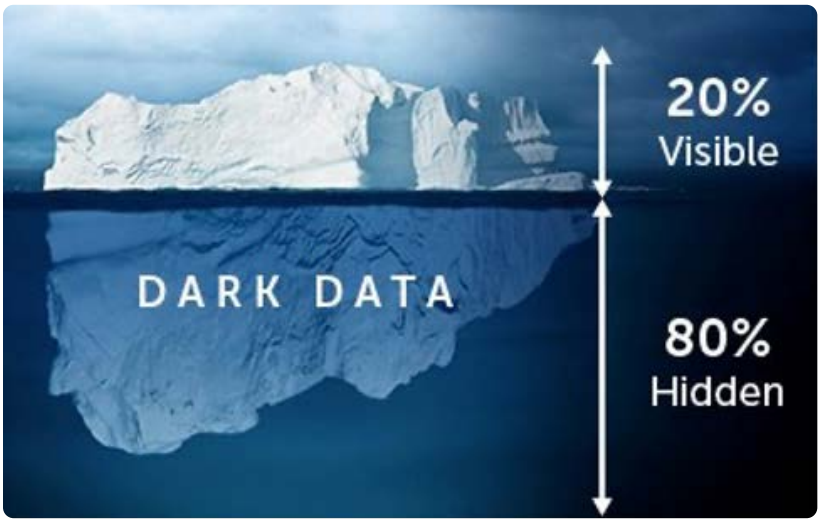
Forcepoint

Brochure

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

¿Están sus datos seguros en esta nueva era?

Las organizaciones de todos los sectores están lidiando con la transformación de la IA, impulsada por la promesa de aumentar drásticamente la productividad. Esta era potenciada por la IA se caracteriza por iniciativas para incorporar servicios empresariales de IA, gestionar el uso no autorizado de IA y mitigar los riesgos asociados con la actividad de agentic AI. En general, una prioridad clave que sustenta estos esfuerzos es la visibilidad y el control sobre cómo se utilizan los datos sensibles. Sin embargo, prácticamente todas las organizaciones tienen dificultades para lograr una visibilidad consistente, y mucho menos control, de sus datos a gran escala. Es como un iceberg, donde solo vemos una pequeña fracción en la superficie, mientras que la gran mayoría es imperceptible por debajo de ella. Esto suele denominarse "datos oscuros" (dark data): permanecen invisibles y desconocidos, pero contienen cantidades importantes de información sensible de la cual la organización es directamente responsable. Ahora, las organizaciones están tratando de descubrir cómo permitir que los usuarios aprovechen la IA de forma segura mientras garantizan la protección de sus datos sensibles, pero el propio uso de la IA está empeorando el problema, ya que ayuda a crear más datos a una velocidad sin precedentes.



Data Security Posture Management (DSPM) ofrece un enfoque integral para proteger tu información contra el acceso no autorizado, la divulgación, la alteración o la destrucción de datos. A diferencia de otros métodos de seguridad de datos que se centran en aplicaciones y dispositivos específicos, DSPM puede ver y controlar la totalidad de los datos de una organización, ya sea en la nube o en redes privadas, garantizando el cumplimiento normativo y mitigando el riesgo de filtraciones de datos.



Porcentaje de organizaciones que informaron una brecha relacionada con la IA y que carecían de controles de acceso adecuados a la IA.[1]



Ahorro de costos por el uso extensivo de la IA en las operaciones de seguridad. Los equipos de seguridad que utilizan ampliamente la IA y la automatización redujeron sus tiempos de contención de brechas en 65 días y disminuyeron sus costos promedio en USD 1.93 millones en comparación con aquellos que no utilizaron estas soluciones.[1].



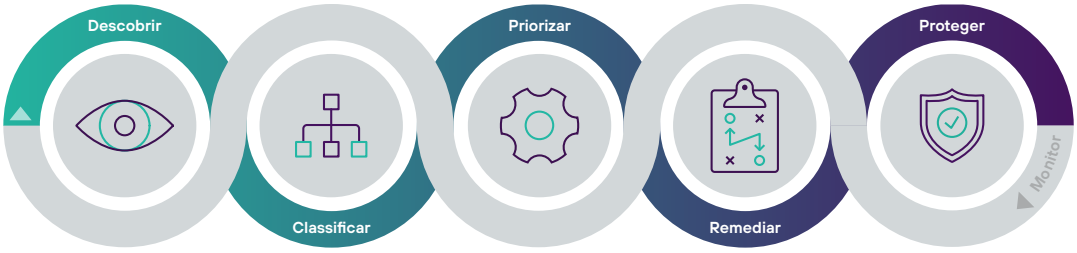
AT&T acordó un pago de $177 millones para resolver una demanda colectiva vinculada a dos brechas de seguridad ocurridas en 2024. La primera brecha expuso datos, incluidos números de Seguro Social, de 73 millones de clientes actuales y anteriores, y la segunda implicó el acceso no autorizado a un espacio de trabajo que contenía información sensible de clientes alojada en un entorno de nube sin la supervisión adecuada[2].

1 IBM's Cost of a Data Breach Report 2026
2 Top Class Actions **acuerdo de la demanda colectiva por la filtración de datos de AT&T**

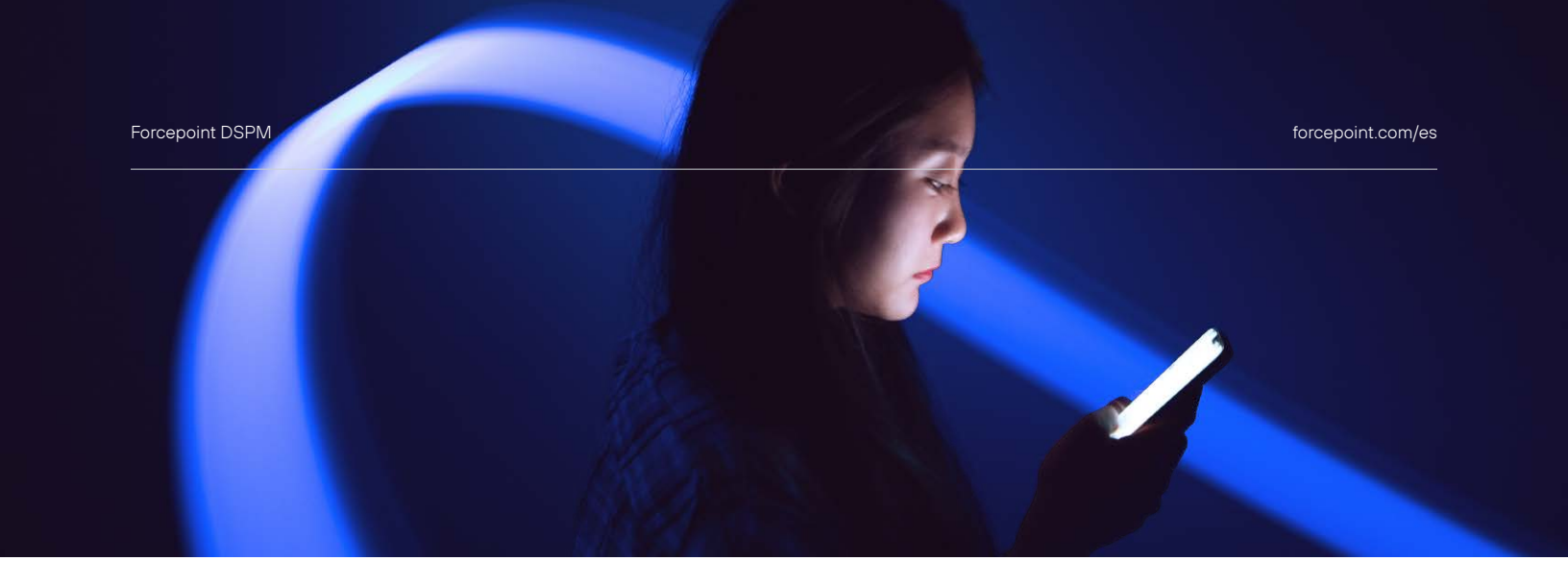
¿Qué aborda DSPM?

- **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



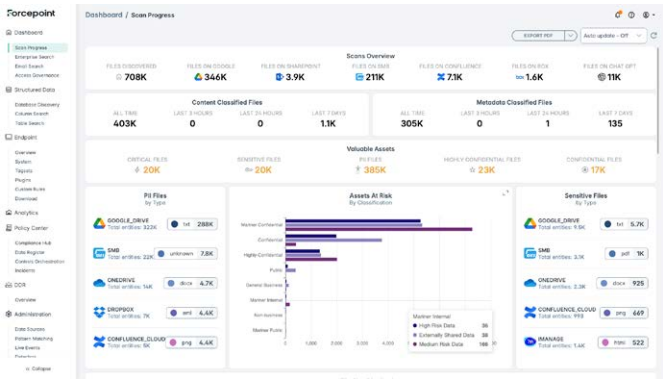
Unifique la visibilidad y el control sobre su entorno de datos con Forcepoint DSPM

Gestionar y proteger los datos de tu organización nunca ha sido tan complejo. Forcepoint DSPM ofrece una solución potente para obtener visibilidad y control integrales sobre tus datos, sin importar su ubicación. Con una clasificación de datos líder en la industria que utiliza inspección de contenido completo impulsada por AI Mesh de Forcepoint y clasificadores DLP avanzados, Forcepoint DSPM te permite tomar decisiones informadas sobre tu postura de seguridad de datos y abordar los riesgos potenciales de forma proactiva.

Los beneficios clave de Forcepoint DSPM incluyen:

Detección rápida e integral: Forcepoint DSPM ofrece un escaneo rápido y de alto rendimiento de archivos y bases de datos en entornos multi cloud y on-premises, realizando una inspección de contenido completo en lugar de depender del simple etiquetado de metadatos o de enfoques de muestreo. Esta profundidad de análisis garantiza que los datos sensibles se identifiquen con precisión, no que solo se estimen. El descubrimiento y la clasificación de alto rendimiento de Forcepoint permiten a las organizaciones obtener una visibilidad rápida e integral de su panorama de datos a gran escala, abarcando tanto repositorios estructurados como no estructurados, incluidos los datos alojados en plataformas de IA generativa como ChatGPT Enterprise, Anthropic Claude y Microsoft Copilot, para ayudar a los equipos de seguridad a anticiparse a los riesgos emergentes de exposición de datos impulsados por la IA.

Precisión habilitada por AI Mesh: Forcepoint DSPM descubre datos en fuentes de nube y de red, y clasifica automáticamente esos datos utilizando un motor de clasificación de IA avanzado. El AI Mesh de Forcepoint DSPM ofrece a las organizaciones una precisión de clasificación de datos superior. Su arquitectura de IA en red, que aprovecha un GenAI Small Language Model (SLM) y los clasificadores DLP de Forcepoint, confiables desde hace mucho tiempo y cuidadosamente seleccionados, captura de manera eficiente el contexto de texto no estructurado. Personalizable y eficiente, garantiza una clasificación rápida y precisa sin necesidad de un entrenamiento extenso, lo que aumenta la confianza y el cumplimiento normativo. En última instancia, esta alta precisión ha permitido que organizaciones que tenían dificultades con otros métodos de clasificación populares reduzcan drásticamente los falsos positivos y negativos, protegiendo con éxito su propiedad intelectual y ahorrando grandes cantidades 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 qué personas tienen acceso a archivos y bases de datos 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, r educir 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

forcepoint.com/contact

About Forcepoint

Forcepoint impulsa Self-Aware Data Security, un enfoque nativo de IA que ayuda a empresas y gobiernos a conocer sus datos en todas partes, adaptarse a los riesgos y regulaciones cambiantes en tiempo real, y proteger a gran escala con un marco de política única y unificada. Con sede en Austin, Texas, Forcepoint crea entornos seguros y confiables para clientes y sus empleados en más de 150 países. Conéctate con Forcepoint en www.forcepoint.com/es, LinkedIn, Instagram and YouTube.

©2026 Forcepoint. Forcepoint y el logotipo de FORCEPOINT son marcas registradas de Forcepoint. Todas las demás marcas registradas que se utilizan en este documento son propiedad de sus respectivos propietarios.
[FP-DSPM-Brochure-ES] 21Aug2026