Forcepoint

Datasheet

Forcepoint Data Security Posture Management

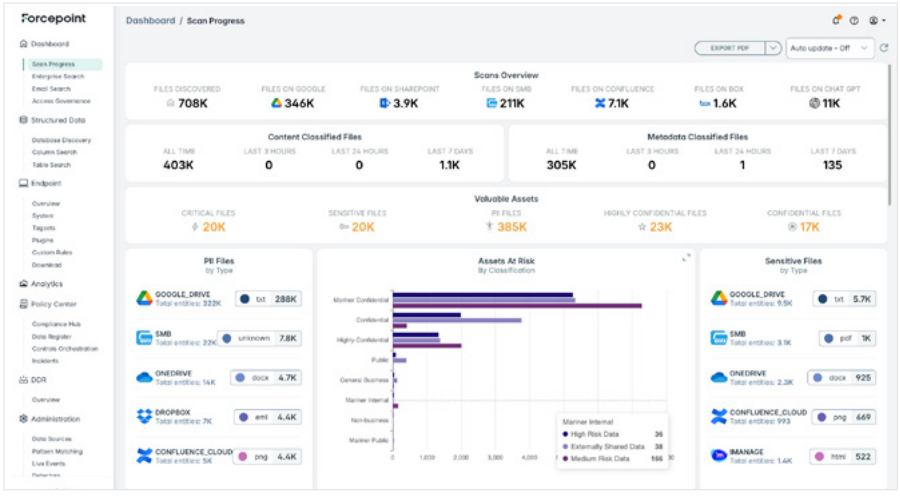
Características y beneficios clave:

- **Clasificación de AI Mesh:** Arquitectura de clasificación altamente precisa y eficiente que utiliza IA generativa, IA predictiva y capacidades de ciencia de datos.
- **Descubrimiento rápido:** ejecute Forcepoint DSPM en la nube y en ubicaciones de almacenamiento on-prem, con la frecuencia que desee.
- **Evaluación de riesgos en tiempo real:** Revise los permisos de acceso y otros riesgos de datos.
- **Orquestación del flujo de trabajo:** implemente prioridades empresariales para las partes interesadas.

La transformación digital ha evolucionado hacia la transformación de la IA, impulsada por la integración de las tecnologías de IA, en particular las aplicaciones de IA generativa, en los procesos empresariales. Junto con la dispersión de datos de las organizaciones que migran aplicaciones y datos desde on-premises a la nube y utilizan herramientas de IA generativa como ChatGPT, Copilot y Gemini, se enfrentan a la lucha continua de mantener un registro de dónde están sus datos confidenciales, quién puede acceder a ellos y cómo se utilizan. El crecimiento exponencial de los "datos oscuros", ocultos en repositorios basados en la nube o repartidos entre dispositivos individuales y, ahora, en aplicaciones de IA generativa, supone un riesgo sustancial. Se estima que hasta el 80 por ciento de los datos de una organización existen en este estado "oscuro" oculto, evadiendo la supervisión tradicional.

La consecuencia de este panorama de datos ocultos es crítica. Sin una visibilidad y una administración claras, las organizaciones están expuestas a un mayor riesgo de fugas, con consecuencias potencialmente devastadoras en los sectores comercial, gubernamental y sin fines de lucro. En la actual era de transformación digital, el imperativo de recuperar el control de la información confidencial nunca ha sido más urgente.

Forcepoint DSPM descubre y clasifica rápidamente datos confidenciales a escala, y cubre datos estructurados y no estructurados. Su AI Mesh único ofrece velocidad y explicabilidad con una arquitectura de Small Language Model (SLM) altamente eficiente. Este AI Mesh también permite la personalización sin un extenso reentrenamiento del modelo y garantiza una clasificación rápida y precisa para una confianza y un cumplimiento mejorados.

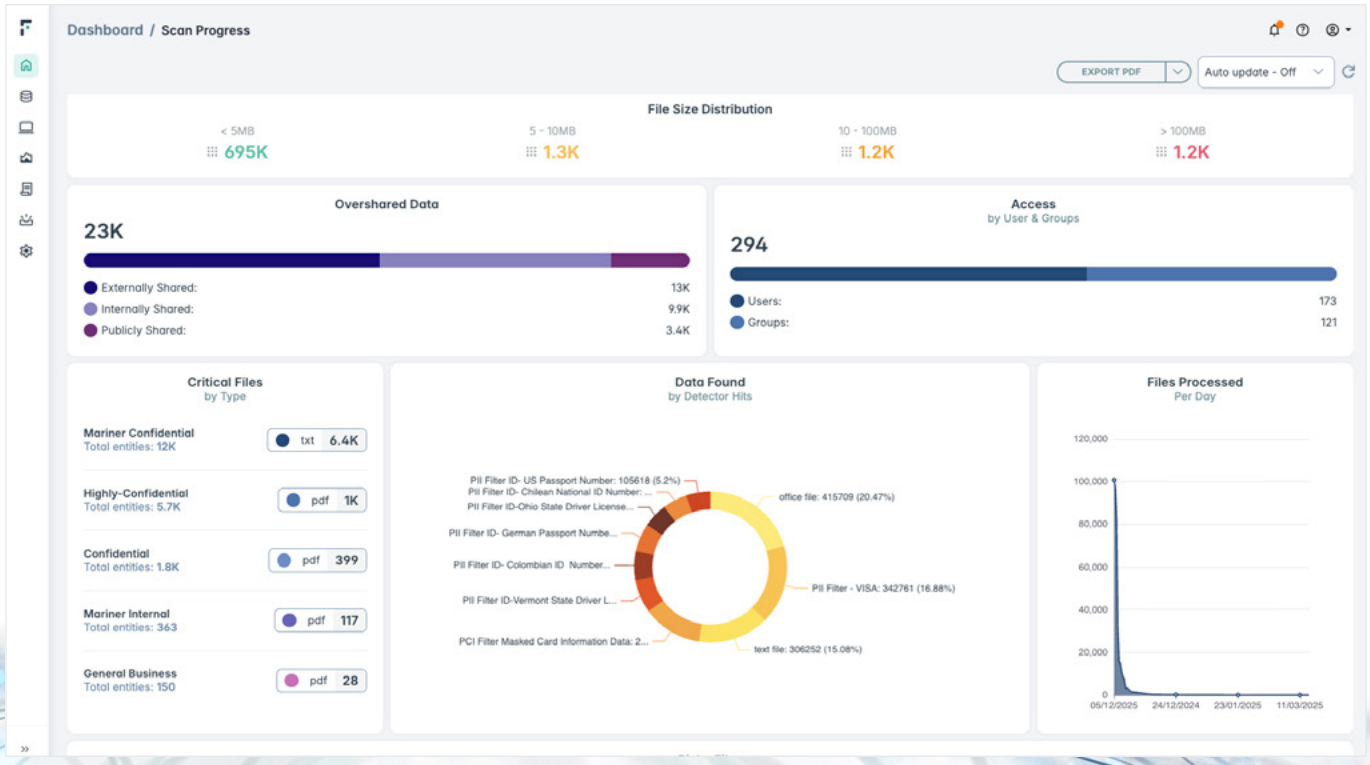


Descubrimiento rápido y completo

Con una multitud de conectores, Forcepoint DSPM localiza de manera eficiente los datos confidenciales en diversos entornos de almacenamiento, ya sea en la nube u on-premises, ya sean datos estructurados o no estructurados, escaneando en plataformas importantes como Amazon (AWS S3 e IAM), Microsoft (Azure AD, OneDrive, SharePoint Online) y Google (Google Drive e IAM), así como sistemas locales de LDAP y SharePoint.

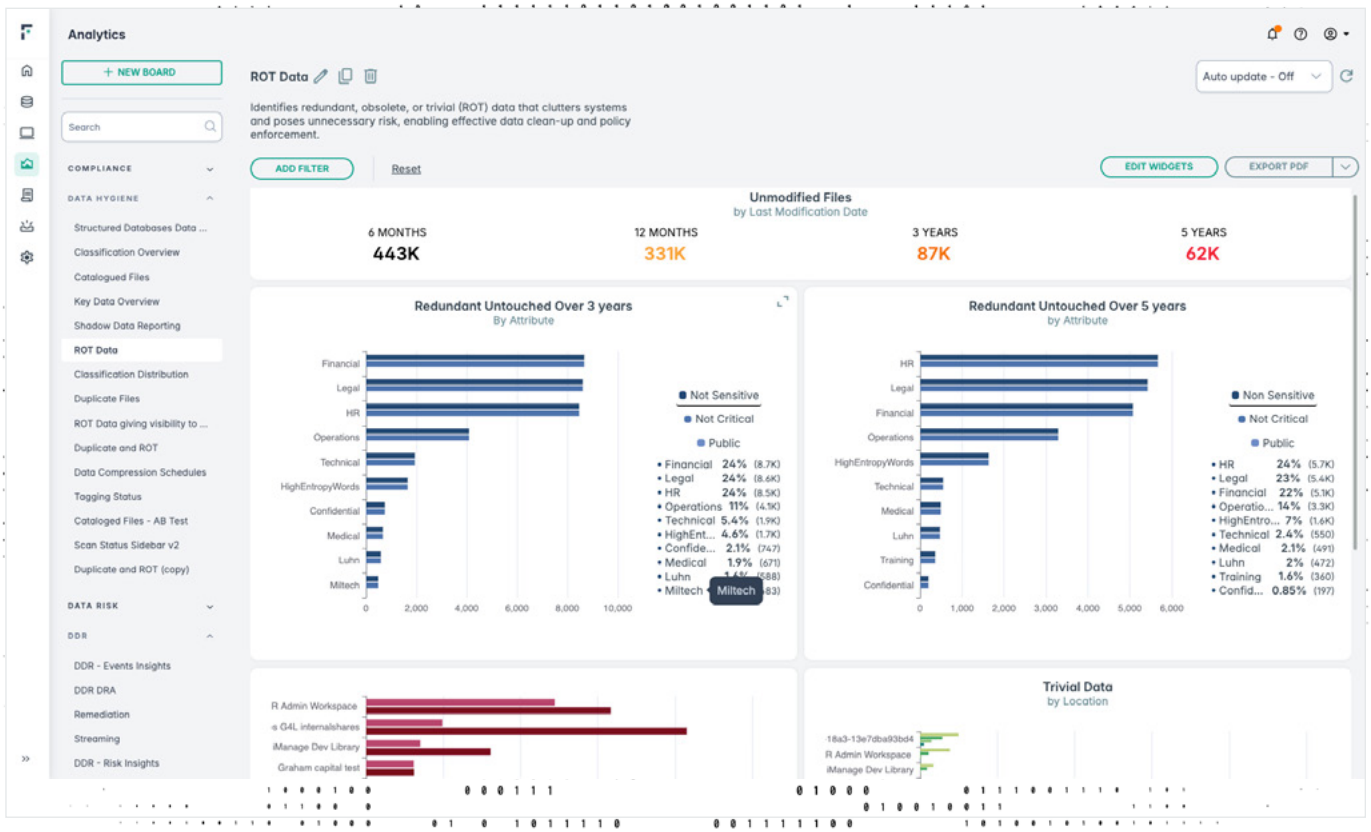
Precisión habilitada para el AI Mesh

La función AI Mesh de Forcepoint DSPM se destaca por empoderar a las organizaciones actuales con una precisión superior de clasificación de datos. A diferencia de otras soluciones de DSPM, ofrece una arquitectura de IA conectada de múltiples nodos, que aprovecha un SLM de IA de GenAI y una red de datos y componentes de IA avanzados. Esta estructura captura de manera eficiente el contexto y transforma el texto en clasificaciones precisas de documentos. AI Mesh es personalizable, adaptándose a las necesidades del sector y a los entornos regulatorios. Se ejecuta de manera eficiente en recursos informáticos estándar sin necesidad de GPU y proporciona a la vez una clasificación de alto rendimiento. Se logra una alta precisión sin una amplia capacitación en aprendizaje automático, lo que reduce los costos de mantenimiento. La explicabilidad de AI Mesh aumenta la confianza y el cumplimiento, lo que garantiza una postura de datos de alta seguridad y el cumplimiento de las regulaciones de privacidad.



Monitoreo de alto rendimiento y evaluación de riesgos de datos

A medida que Forcepoint DSPM escanea y descubre datos, proporciona información detallada como el número de archivos compartidos internamente que contienen información crítica, la cantidad de archivos PII en riesgo y el recuento de archivos de datos redundantes, obsoletos y triviales (ROT).



Orquestación del flujo de trabajo

Optimice la gobernanza de seguridad de datos sin esfuerzo con Forcepoint DSPM. Su intuitiva orquestación del flujo de trabajo garantiza un seguimiento eficaz de la propiedad y la responsabilidad de los datos. Al romper los silos y facilitar la colaboración entre las partes interesadas, alinea las responsabilidades, mejorando la eficiencia operativa y fomentando la claridad en toda la organización.

La implementación de una solución de DSPM robusta es crucial para las organizaciones que tienen como objetivo proteger su postura de datos y proteger la información confidencial en las ubicaciones de almacenamiento de datos en la nube y on-premises. Al utilizar Forcepoint DSPM, las organizaciones pueden impulsar la productividad mejorando la fiabilidad del acceso y el uso compartido de datos, fomentando la innovación y alentando la colaboración. Al mismo tiempo, pueden mitigar el riesgo identificando y abordando de forma proactiva el uso inadecuado de datos confidenciales, evitando así las fugas de datos. En última instancia, las organizaciones pueden optimizar los esfuerzos de cumplimiento de normativas al obtener una visibilidad y un control auténticos de los datos confidenciales en todos los entornos.

Descubrimiento sólido

CARACTERÍSTICA	BENEFICIO
Descubrimiento y catalogación rápidos	Se ejecuta en múltiples fuentes para escanear mayores volúmenes de archivos por segundo/hora y sintetiza detalles sobre activos de datos no estructurados y estructurados, organizándolos en un formato fácil de digerir.
Se conecta a fuentes de datos importantes	Visibilidad sólida de datos no estructurados y estructurados al ofrecer una gama de conectores de fuentes de datos.
Análisis de datos sobreexpuestos	Identifique los datos sobreexpuestos que se comparten públicamente, externamente con terceros, e internamente más de lo intencionado.
Vea y corrija permisos	Vea el acceso para cada archivo y corrija para establecer la seguridad de Zero Trust con el principio de mínimo privilegio (POLP).
Eliminar el riesgo debido a los datos ROT (redundantes, obsoletos y triviales)	Identifique y elimine los archivos redundantes, obsoletos o triviales (ROT).
Visibilidad del acceso y los permisos	Las integraciones con Active Directory y otras soluciones de IRM mejoran la seguridad de acceso en las organizaciones.

AI Mesh Data Classification

CARACTERÍSTICA	BENEFICIO
Clasificación de AI Mesh de datos no estructurados y estructurados	Clasificación de IA de alta precisión para datos no estructurados y estructurados.
Capacitación personalizada del modelo	Las organizaciones pueden adaptar el modelo de AI Mesh para adaptarse a las necesidades de datos únicas (por ejemplo, IP, secretos comerciales, etc.), para una clasificación de datos de alta precisión, reduciendo los falsos positivos/negativos de DSPM y DLP.
Capaz de asignar etiquetas al etiquetado de IP de Microsoft Purview	Proporciona una capa adicional de granularidad de clasificación, que complementa las etiquetas MIP. Capaz de corregir el etiquetado de MIP.
Etiquetado de datos	Etiquete todos los archivos escaneados y clasificados con etiquetas persistentes que son legibles por DLP con etiquetado estándar (clasificado, altamente clasificado, público), así como catalogación/etiquetado de negocios (RRHH, marketing, finanzas, devops, con subetiquetas como currículums, POs, etc.).
Se integra con Forcepoint DLP	Se puede integrar con Forcepoint DLP para utilizar el etiquetado de archivos de DSPM AI Mesh para crear políticas sólidas contra ellos.

Monitoreo y evaluación de riesgos en tiempo real

CARACTERÍSTICA	BENEFICIO
Evaluaciones de riesgos de datos (DRA)	Data Risk Assessments gratuitos disponibles para analizar la postura de seguridad de datos actual de una organización en múltiples categorías.
Panel interactivo detallado	Ve los detalles completos del archivo y la base de datos en una solución. Desglose los datos cruciales de los archivos, como el nivel de riesgo, los permisos y las ubicaciones (dirección IP, ruta).
Función de generación de informes	Genere informes que muestren tanto la preparación general para el cumplimiento como para regulaciones de privacidad específicas.
Sistema avanzado de alertas	Proporciona sofisticados controles de datos y alerta de las anomalías o posibles fugas detectadas durante los escaneos.
Búsqueda de solicitudes de acceso de sujetos de datos (DSAR)	Simplifique la generación de una DSAR para cumplir rápidamente con las solicitudes de regulación de privacidad.
Programas de analítica	Descubra programas de analítica avanzada para acceder fácilmente a información sobre seguridad y clasificación. Seleccione entre varios paneles predefinidos o elabore los suyos propios, y exporte instantáneas en PDF sin esfuerzo con un solo clic. Los paneles predefinidos incluyen análisis de ransomware y sobreexposición, duplicación de datos críticos, detección de usuarios de riesgo, retención de datos, datos perdidos, evaluación de riesgos de datos, soberanía, seguimiento de incidentes para violaciones de control de datos y muchos más.
Análisis de la exposición al ransomware	Identifique los datos críticos que podrían estar expuestos a un ataque de ransomware.
Generador de informes y análisis sin código	Cree fácilmente casos de uso personalizados e informes de análisis sin necesidad de habilidades de codificación.
Identificación de usuarios riesgosos	Identifique a los usuarios con perfiles de riesgo elevados que tienen acceso a cantidades significativas de información crítica.
Incidencia en el control de datos	Proporciona una visión clara de cualquier infracción del control de datos y un estado de la resolución de incidentes.

Remediación

FUNCIONALIDAD	BENEFICIO
Corrección de permisos	Reciba notificaciones sobre incidentes de gobernanza de seguridad de datos o problemas de cumplimiento, optimice el seguimiento y la gestión con las herramientas ITSM y de productividad existentes, incluidas alertas para datos sobreexpuestos.
Corrección mediante deduplicación de datos	La función de deduplicación de DSPM identifica y elimina datos redundantes, reduce las necesidades de almacenamiento y los costos, y optimiza la asignación de recursos. La eliminación se realiza automáticamente según controles de datos personalizables.
Archivos de Sustitución	Cree automáticamente stubs de archivos para mantener los procesos de negocio documentando los cambios de ubicación de los archivos cuando se mueven mediante DSPM.