Forcepoint

Hoja de datos

Forcepoint Data Security Posture Management

Características y beneficios clave:

- **AI Mesh y aprendizaje automático:** la catalogación delAI Mesh ofrece una precisión y eficiencia inigualables, evolucionando continuamente a través del aprendizaje automatizado para mejoras continuas.
- **Descubrimiento rápido:** ejecute Forcepoint DSPM en la nube y en ubicaciones de almacenamiento on-prem, con la frecuencia que desee.
- **Monitoreo y evaluación de riesgos en tiempo real:** compruebe 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.

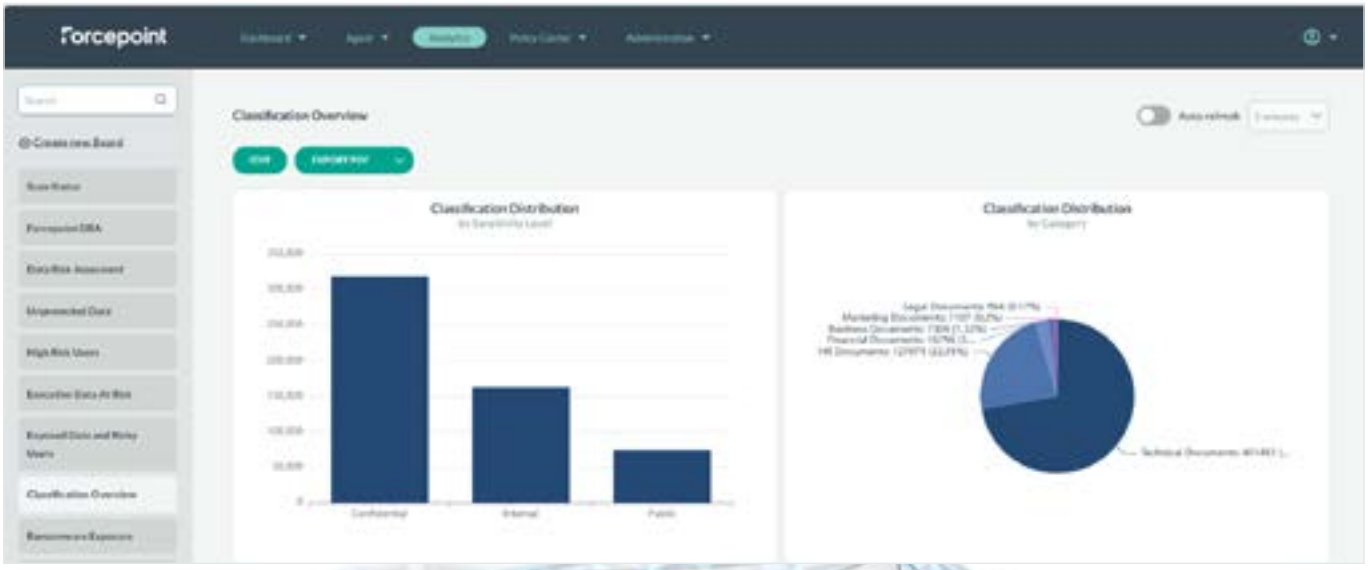
El AI Mesh de Forcepoint DSPM empodera a las organizaciones con una precisión superior de clasificación de datos. Su arquitectura de IA en red, que aprovecha un modelo de lenguaje pequeño (SLM) de GenAI, así como datos avanzados y componentes de la IA, captura de manera eficiente el contexto del texto 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.

Descubrimiento rápido y completo

Con una multitud de conectores, Forcepoint DSPM localiza de manera eficiente los datos confidenciales a través de diversos entornos de almacenamiento, ya sea en la nube u on-premises, escaneando aproximadamente un millón de archivos por hora a través de las principales plataformas como Amazon (AWS S3 y IAM), Microsoft (Azure AD, OneDrive, SharePoint Online) y Google (Google Drive y IAM), así como sistemas locales de LDAP y SharePoint.

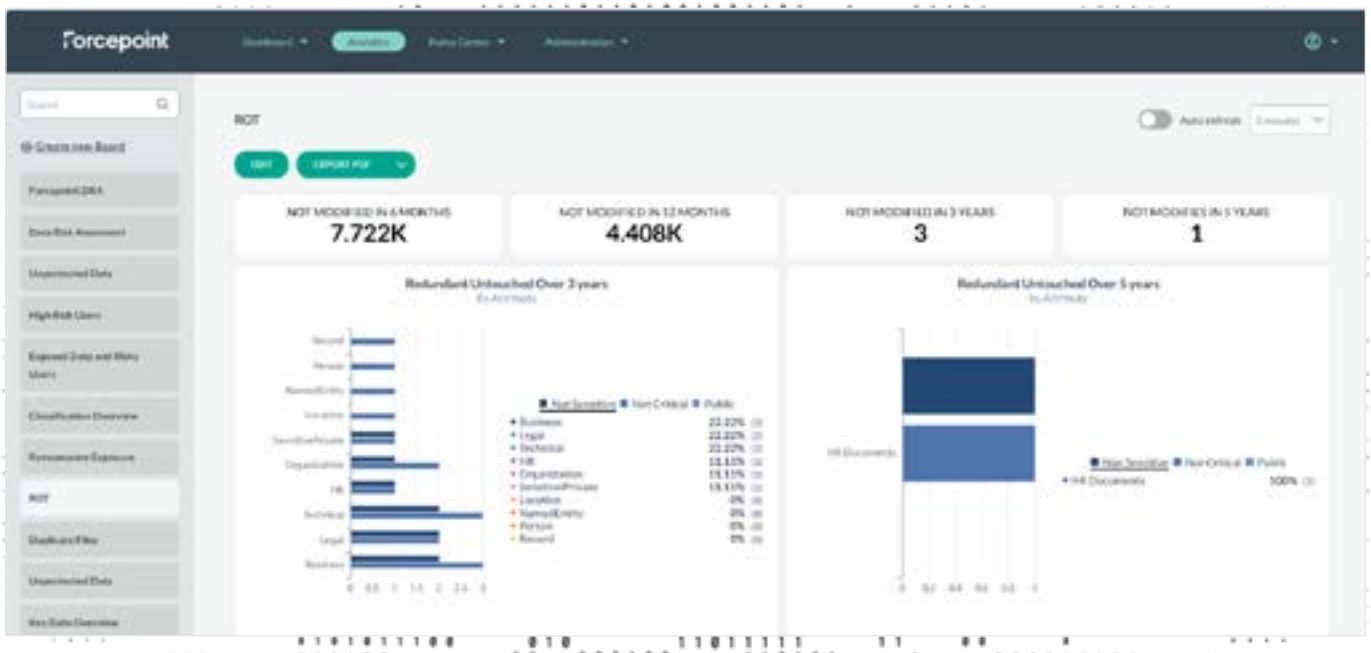
Precisión habilitada para el AI Mesh

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 no estructurado 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 y evaluación de riesgos en tiempo real

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 sólida es crucial para las organizaciones que pretenden optimizar su patrimonio 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 recursos de datos no estructurados, organizándolos en un formato fácil de digerir.
Amplios conectores de fuentes de datos	Visibilidad sólida de más datos no estructurados al ofrecer una amplia 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.
Ver los permisos de cada archivo de datos no estructurados	Vea el acceso individual de los usuarios para cada archivo y vea los usuarios con acceso a la mayoría de los archivos.
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 del AI Mesh y el aprendizaje automatizado de los datos no estructurados existentes	Sugerencias de clasificación de alta precisión recomendadas para los datos no estructurados existentes que se escanean.
Capacitación personalizada del modelo	Las organizaciones pueden personalizar el modelo de AI Mesh para adaptarlo a necesidades de datos únicas (por ejemplo, propiedad intelectual, secretos comerciales, etc.) y, mediante el aprendizaje automatizado, puede mejorarse con el tiempo para obtener una mayor precisión.
Capaz de asignar etiquetas al etiquetado de IP de Microsoft Purview.	Proporciona una capa adicional de granularidad de clasificación, que complementa las etiquetas MPIP. Capaz de corregir el etiquetado MPIP.
Etiquetado de datos	La optimización de la implementación de DLP mejora la eficacia de DLP al colocarle a todos los archivos escaneados y clasificados etiquetas legibles por DLP - con etiquetas típicas (clasificadas, altamente clasificadas, públicas), así como catalogación/etiquetado empresarial (RRHH, marketing, finanzas, desarrollo, con subetiquetas como currículums, pedidos, etc.).
Se integra con Forcepoint DLP	Puede integrarse para utilizar el etiquetado de archivos de AI Mesh de DSPM (clasificación) para crear políticas sólidas.

Monitoreo y evaluación de riesgos en tiempo real

CARACTERÍSTICA	BENEFICIO
Evaluaciones de riesgos de datos (DRA)	Las evaluaciones de riesgo de datos gratuitas están disponibles para analizar la postura actual de riesgo de datos de una organización a través de múltiples categorías.
Panel interactivo detallado	Vea todos los detalles de los archivos en una sola pantalla. 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 las regulaciones 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 sobreexposición y ransomware, duplicación de datos críticos, detección de usuarios riesgosos, retención de datos, datos extraviados, evaluación del riesgo de los datos, soberanía y seguimiento de incidentes por infracciones del control de datos.
Análisis de la exposición al ransomware	Identifique los datos críticos que están expuestos a un ataque de ransomware.
Generador de informes y análisis sin código	Cree fácilmente casos de uso personalizados e informes de analítica sin necesidad 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.

Orquestación del flujo de trabajo

CARACTERÍSTICA	BENEFICIO
Propiedad de los datos	Define la responsabilidad con facilidad y logra la alineación de las partes interesadas.
Administrador de tareas	Asigna tareas a los custodios y propietarios de los datos, lo que permite el seguimiento de las estadísticas de DSPM (como los tickets abiertos, resueltos y cerrados, el tiempo de resolución).