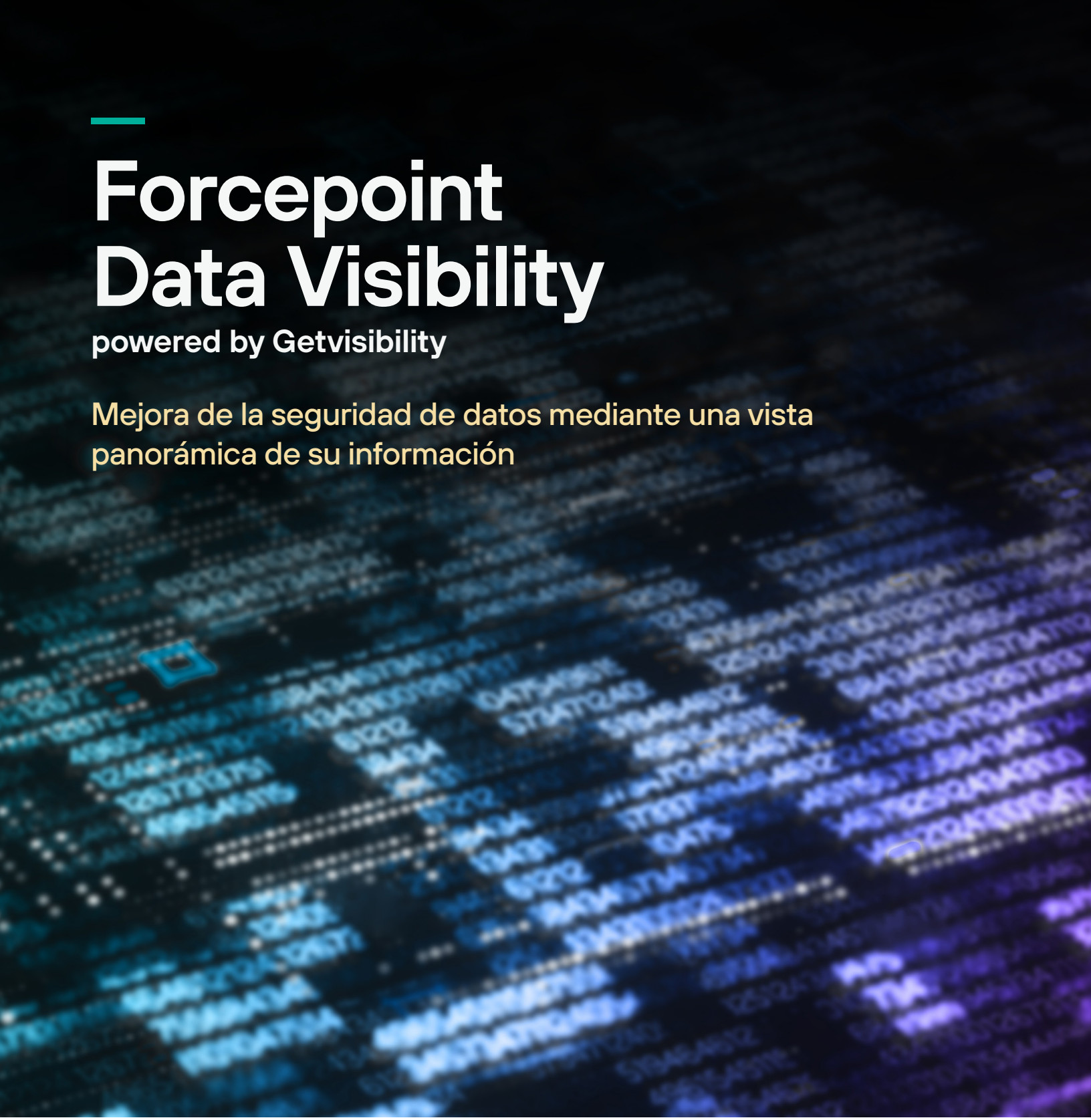


Forcepoint Data Visibility

powered by Getvisibility

Mejora de la seguridad de datos mediante una vista panorámica de su información

Forcepoint

Brochure

Sus datos están en todas partes, y eso es solo el comienzo de sus problemas. Es muy probable que sus datos también estén aislados en distintos centros de datos, varias nubes y muchas computadoras portátiles, lo que hace que el problema de los datos sea aún mayor. ¿Está al tanto de exactamente qué datos tiene, dónde están ubicados y, lo que es más importante, qué riesgos le generan todos esos datos a su empresa en este momento? IDC estimó que el 80 % de los datos de todo el mundo no están estructurados y que el 90 % de esos datos no han sido analizados[1]. En otras palabras, se trata de datos que no son conocidos y que no forman parte del trabajo cotidiano de una organización. Literalmente, esos datos son invisibles. A medida que las organizaciones enfrentan exigencias de cumplimiento cada vez mayores y más fugas de datos[2], es imperativo obtener visibilidad de todos los datos para minimizar los riesgos y los costos resultantes. Las organizaciones de todo tipo y tamaño deben dedicarle atención continua a esta cuestión.

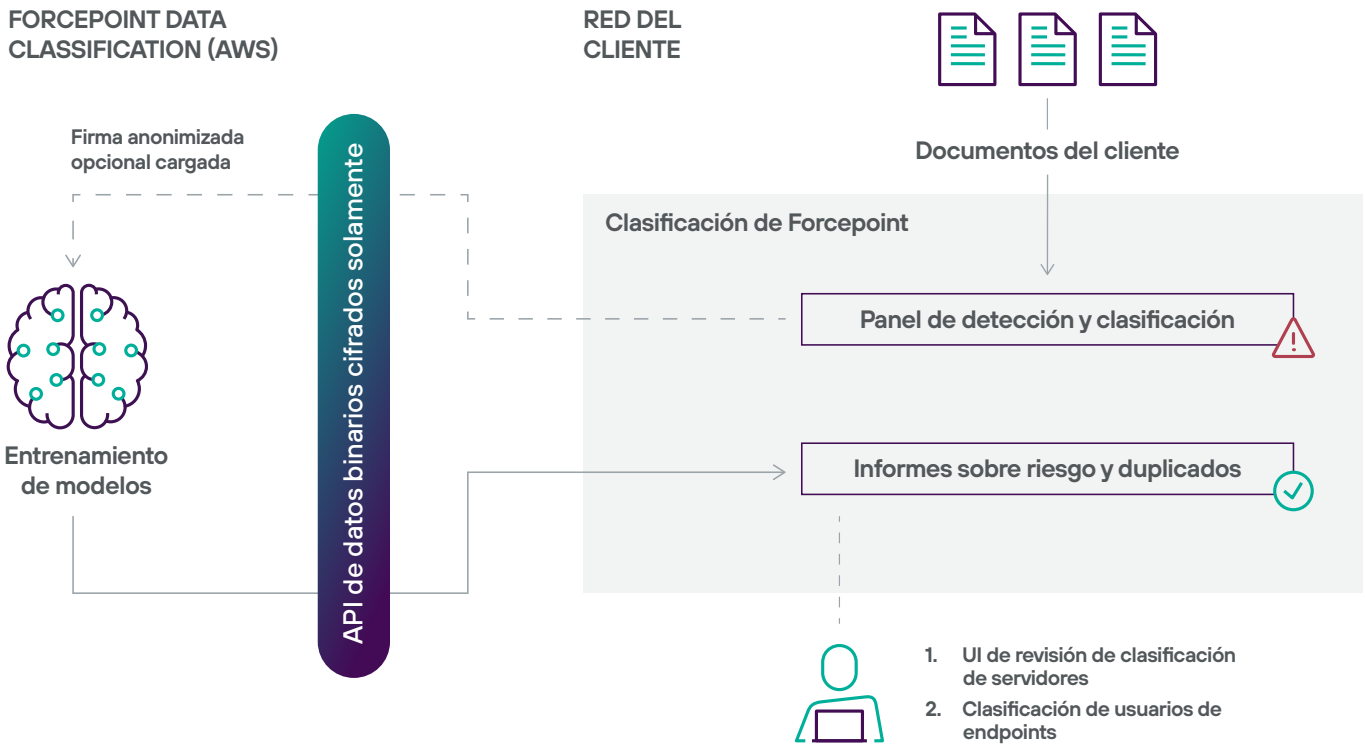
La minimización de los riesgos comienza por ver los datos donde sea que estén alojados, ya sea en sus instalaciones o en la nube. Forcepoint Data Visibility proporciona una vista panorámica de los datos de su organización. La visibilidad es una parte esencial del enfoque de Forcepoint respecto de la seguridad de datos, lo que permite a los clientes detectar, clasificar, monitorear y proteger todos sus datos de manera continua. La vista de 360° de Forcepoint Data Visibility puede reducir drásticamente las pérdidas de datos, eliminar los riesgos de cumplimiento y, en última instancia, ahorrarle los costos enormes que generan las fugas de datos y los incumplimientos.

Según IDC, el 80 % de los datos de todo el mundo no están estructurados y el 90 % de esos datos no han sido analizados, por lo que se los denomina "datos oscuros". [3]

El 94 % de las organizaciones almacena datos en múltiples entornos en la nube.[4]

Equifax aceptó un acuerdo por USD 1400 M en una demanda por su fuga de datos5 exacerbada por hackers que accedieron a una unidad compartida que almacenaba varias copias de nombres de usuarios y contraseñas de empleados. La empresa no contaba con las herramientas para detectar e identificar archivos redundantes y desactualizados.

1 The Unseen Data Conundrum (El enigma de los datos invisibles), Forbes, february 2022
2 2022 Data Breach Investigations Report (Informe sobre investigaciones de fugas de datos 2022), Verizon, mayo de 2022
3 The Unseen Data Conundrum (El enigma de los datos invisibles), Forbes, febrero de 2022
4 Dark Data: The Cloud's Unknown Security and Privacy Risk (Los datos oscuros: el riesgo de privacidad y seguridad desconocido de la nube), Forbes, junio de 2023
5 Equifax agrees $1.38bn data breach lawsuit settlement (Equifax acepta acuerdo por USD 1380 M en demanda por fuga de datos), Finextra, enero 2020


FORCEPOINT DATA CLASSIFICATION (AWS)
RED DEL CLIENTE
Firma anonimizada opcional cargada
API de datos binarios cifrados solamente
Documentos del cliente
Clasificación de Forcepoint
Panel de detección y clasificación
Informes sobre riesgo y duplicados
Entrenamiento de modelos
1. UI de revisión de clasificación de servidores
2. Clasificación de usuarios de endpoints

Visibilidad rápida que aprovecha el poder de la inteligencia artificial (IA)

Dado que las organizaciones almacenan datos en múltiples entornos en la nube, incluso en sus instalaciones, confiar en un proveedor de servicios en la nube que solo pueda brindar visibilidad sobre los datos dentro de su propio servicio limita drásticamente la eficacia de la seguridad de datos. Además, las herramientas de detección y clasificación típicas requieren la intervención manual de un administrador para lograr resultados; incluso aquellas que hacen un uso limitado del Machine Learning (ML) necesitan que alguien tome las decisiones de entrenamiento.

Forcepoint Data Visibility supera estos desafíos mediante la aplicación de IA y modelos de lenguaje grandes (LLM) de aprendizaje autónomo para automatizar el proceso de encontrar, categorizar y clasificar los datos, sin importar dónde estén almacenados en la nube o en las instalaciones. El poderoso modelo de detección y clasificación previamente entrenado de Forcepoint se basa en un modelo de 50 dimensiones entrenado con cientos de millones de archivos de datos reales de muchas organizaciones de las principales industrias. Este enfoque innovador genera datos sintéticos de alta calidad para ofrecer una precisión de clasificación y una mejora continua sin precedentes, sin comprometer la privacidad de los datos asociados con los datos reales. A medida que el motor de Forcepoint procesa los datos, su aprendizaje continúo impulsado por la IA hace sugerencias con respecto a la clasificación de los datos en lenguaje natural, con una categorización sumamente precisa.

Carga opcional de firmas anónimas Clasificación de Forcepoint RED DEL CLIENTE FORCEPOINT DATA CLASSIFICATION (AWS) Panel de detección y clasificación Informes sobre riesgos y duplicados Entrenamiento del modelo Documentos del cliente 1. UI de revisión de clasificación de servidores 2. Clasificación de usuarios de endpoints API de datos binarios cifrados únicamente Detección de información de identificación personal (PII) y calificación de los riesgos de cumplimiento de los datos.

Forcepoint proporciona esta información mediante informes y paneles de alta fidelidad. Estos paneles también revelan la dirección IP, la ruta y los permisos detallados de cada archivo detectado. La precisión de nuestra clasificación mejora con el uso y el tiempo, y cuando se combina con Forcepoint Data Loss Prevention (DLP), ofrece una mayor visibilidad para proporcionar el nivel de seguridad de datos más alto.

- **Precisión impulsada por la IA:** olvídese las búsquedas de datos manuales y lentas. La IA de aprendizaje autónomo de Forcepoint encuentra, categoriza y clasifica automáticamente todos sus datos, incluso en las nubes y en sus instalaciones, lo que ahorra tiempo y aumenta la precisión.
- **No más puntos ciegos de datos:** obtenga paneles sumamente claros con información detallada de los archivos, como la ubicación, los permisos y las calificaciones de riesgos. Tome decisiones informadas más rápido con visualizaciones de datos intuitivas.
- **Seguridad más inteligente:** la IA de Forcepoint aprende y se adapta continuamente, sugiere clasificaciones de datos en lenguaje sencillo y detecta PII confidencial para prevenir de manera proactiva las filtraciones de datos y los incumplimientos.

La visibilidad de quién puede ver su información más sensible.

¿Está seguro de que desea que contratistas accedan a la PII de los clientes o a información confidencial de ventas? Muchas organizaciones experimentan una "acumulación de privilegios", y, a menudo, otorgan permisos de acceso que exceden lo necesario para que los empleados realicen su trabajo. El control del acceso a la información más confidencial suele pasarse por alto o estar mal administrado, incluso en las empresas que buscan establecer principios de seguridad Zero Trust. Los usuarios con demasiados privilegios pueden, a fin de cuentas, costarles a las empresas enormes sumas de dinero en fugas y falta de cumplimiento.

Forcepoint Data Visibility le permite inspeccionar los permisos de todos los archivos y usuarios. Los administradores de datos pueden ver qué personas tienen acceso a un archivo o a archivos compartidos en toda la organización. La acumulación de privilegios se puede detener mediante análisis periódicos, lo que reduce drásticamente las posibilidades de fugas de datos. Con un solo clic, puede ver instantáneamente los permisos de todos los archivos examinados. Luego, puede aplicar el nivel de permisos adecuado necesario para que los usuarios hagan su trabajo.

- **Detenga la acumulación de privilegios:** asegúrese de que los usuarios solo tengan acceso a los datos que necesitan para evitar amenazas internas y fugas accidentales. Con un solo clic, puede ver los permisos de todos los archivos examinados, lo que le permite aplicar los niveles de acceso adecuados a la velocidad de la luz.
- **Cumpla con las obligaciones normativas:** evite litigios y sanciones costosos obteniendo visibilidad de los permisos de todos los archivos y usuarios.
- **Reduzca los riesgos de fugas de datos:** elimine a los usuarios con demasiados privilegios, que son uno de los objetivos principales de los atacantes. Los análisis periódicos permiten detectar y evitar la acumulación de privilegios, lo que reduce drásticamente las posibilidades de fugas de datos.

Limpiando datos ROT para reducir el problema de los datos

¿Su empresa es acaparadora en lo que respecta a la administración de datos? Existen programas de TV populares sobre personas que no se deshacen de nada y terminan viviendo en medio de un basural imposible de manejar. Muchas organizaciones actúan de esta manera con respecto a los datos, con la idea de que conservar datos es algo bueno e incluso contribuye a mitigar los riesgos. Sin embargo, lo que realmente ocurre es lo opuesto. Los datos pueden ser un recurso, pero también un problema. Lo que sucede con las organizaciones que acumulan datos es que acaparan grandes cantidades de datos redundantes, obsoletos o triviales (ROT, por sus siglas en inglés). En lugar de hacer que las empresas estén en cumplimiento, las dejan sumamente vulnerables a las fugas de datos y susceptibles a incumplimientos incluso mayores en relación con el creciente número de reglamentaciones sobre datos. Demos un vistazo más de cerca a lo que son los datos ROT:

- **Datos redundantes:** se refiere a grandes cantidades de copias o versiones de archivos almacenadas en distintas ubicaciones en la nube o las instalaciones. Las organizaciones erróneamente evitan eliminarlos en caso de que los usuarios dependan de esa copia específica o temen que deshacerse de ellos pueda crear riesgo de falta de cumplimiento.
- **Datos desactualizados:** se trata de información que ya no es correcta o ya no se utiliza. Normalmente, los datos obsoletos ya fueron reemplazados por datos actuales y útiles.
- **Datos triviales:** se refiere a información que no es necesario almacenar. Los datos triviales no brindan un beneficio actual a la organización.

6 Worldwide Digital Loss Technologies Market Shares, 2020: (Participaciones en el mercado de tecnologías de pérdida digital en todo el mundo de 2020: La DLP ha muerto, ¡larga vida a la DLP!), IDC, octubre de 2021

7 Worldwide Digital Loss Technologies Market Shares, 2020: (Participaciones en el mercado de tecnologías de pérdida digital en todo el mundo de 2020: La DLP ha muerto, ¡larga vida a la DLP!), IDC, octubre de 2021

Los datos ROT son un problema porque suelen contener información confidencial. Sin visibilidad de los datos que deben eliminar, las empresas quedan susceptibles a fugas de datos y posibles sanciones regulatorias. Un ejemplo de un caso en el que los datos ROT terminaron siendo costosos es el de la fuga de datos de Equifax, que terminó en un acuerdo judicial por un valor de 1380 mil millones de dólares.8 El origen de esta fuga fue una unidad compartida en la que los empleados guardaban múltiples copias de nombres de usuario y contraseñas, pensando que así estaban haciendo que su trabajo fuera más eficiente. Una vez que los hackers lograron acceder a la unidad compartida, esas copias facilitaron su trabajo. Equifax no contaba con las herramientas para detectar e identificar copias de archivos redundantes y desactualizados.

"Hasta un tercio de los datos empresariales pueden considerarse datos ROT (y otro 52 % son datos oscuros de valor desconocido)"

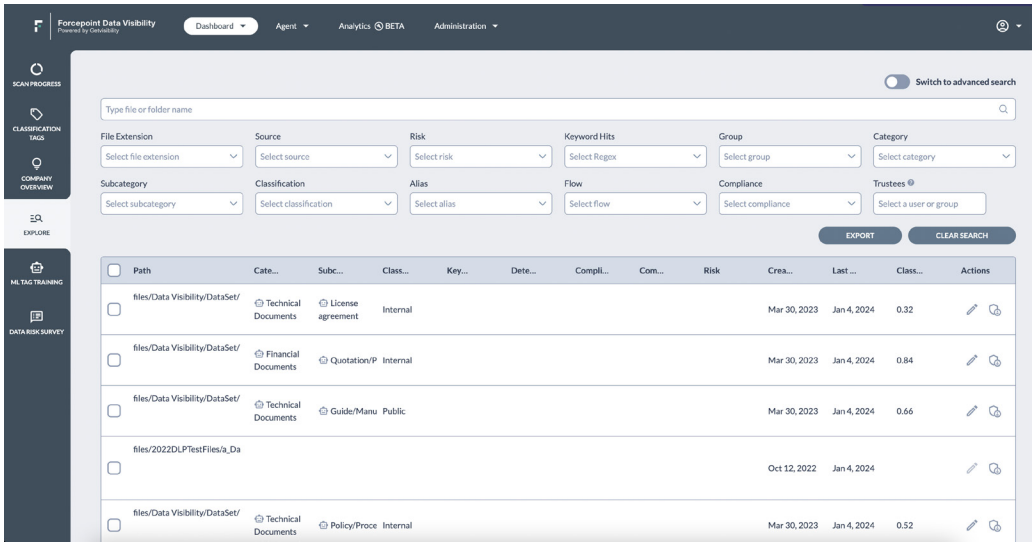
Cómo evitar tener datos ROT en la nube, Forbes, enero de 2023

Para eliminar el riesgo de tener datos ROT, se requiere automatización e información detallada. Forcepoint Data Visibility comienza por proporcionar capacidades de detección y clasificación que permiten examinar rápidamente todos sus datos, independientemente de dónde se encuentren. La precisión impulsada por la IA le brinda claridad absoluta respecto de la duplicación de archivos, la fecha de creación y el último uso de cada archivo, así como su clasificación y riesgos de incumplimiento. El panel de Forcepoint Data Visibility permite a los usuarios analizar estas distintas áreas, ver detalles de cada archivo y ejecutar informes sobre los duplicados. Con esta información, puede eliminar de forma eficaz los datos ROT. Las organizaciones que utilizan Forcepoint Data Visibility pueden realizar análisis de datos completos e informes de riesgos con la frecuencia que sea necesaria sin costos adicionales, lo que les permite abordar de manera proactiva sus problemas de datos ROT.

8 Equifax agrees $1.38bn data breach lawsuit settlement (Equifax acepta acuerdo por USD 1380 M en demanda por fuga de datos), Finextra, enero de 2020

El primer paso en una estrategia de seguridad de datos Zero Trust es descubrir y clasificar toda la información existente y determinar rápidamente qué tiene valor y es necesaria para el cumplimiento normativo. Todo lo demás está podrido y se puede eliminar de manera defendible.

Un panel fácil de usar para obtener una vista panorámica de sus datos



Forcepoint Data Visibility ofrece a los administradores un panel de control fácil de usar en el que pueden realizar búsquedas y aplicar filtros y clasificaciones de acuerdo con sus necesidades. Hay opciones para verificar los resultados del modelo de IA, cambiar la categoría y la subcategoría y ajustar la presencia de PII dentro de un documento, que se puede actualizar en el modelo de IA tanto de forma automática como manual. Estos resultados se pueden exportar a un formato procesable para corregirlos o realizar otras tareas con el fin de abordar las áreas de riesgo, lo que permite optimizar aún más las operaciones de seguridad.

La utilización de este modelo de IA de entrenamiento impulsado por el usuario proporciona un aprendizaje autónomo continuo para aumentar la personalización y la precisión de la organización.

Un modelo de aprendizaje autónomo para mayor personalización y precisión

Forcepoint Data Visibility utiliza el poder de la IA generativa y de múltiples modelos de lenguaje grande líderes para mejorar la seguridad de datos de varias maneras:

- → **Precisión mejorada:** nuestros modelos de IA avanzados están entrenados previamente y aprenden de un amplio repositorio de cientos de millones de archivos de diversas empresas e industrias. Este enfoque integral garantiza una clasificación precisa de los datos al comprender los matices de diversos entornos organizacionales, lo que hace que las clasificaciones sean significativas y procesables.
- → **Datos sintéticos de alta calidad:** representan un enfoque innovador en el que generamos datos sintéticos precisos a partir de nuestro modelo de IA, lo que garantiza una precisión de clasificación y una mejora continua sin precedentes, sin comprometer los problemas de privacidad o seguridad asociados con los datos reales.
- → **Modelo de IA personalizado:** nuestro modelo de IA está centrado en el usuario y se mejora continuamente, lo que le brinda una solución para el panorama de sus datos adaptada a las necesidades de su organización y su industria específicas, y proporciona mayor personalización y precisión.

Todos estos elementos funcionan a la perfección en conjunto para ofrecer una precisión de clasificación del 98 % en más de 70 campos de clasificación, lo que le brinda una mejor visibilidad de sus datos en toda la organización. Esto se traduce en menos falsos positivos de DLP, así como en una defensa más sólida contra las fugas de datos y las exfiltraciones.

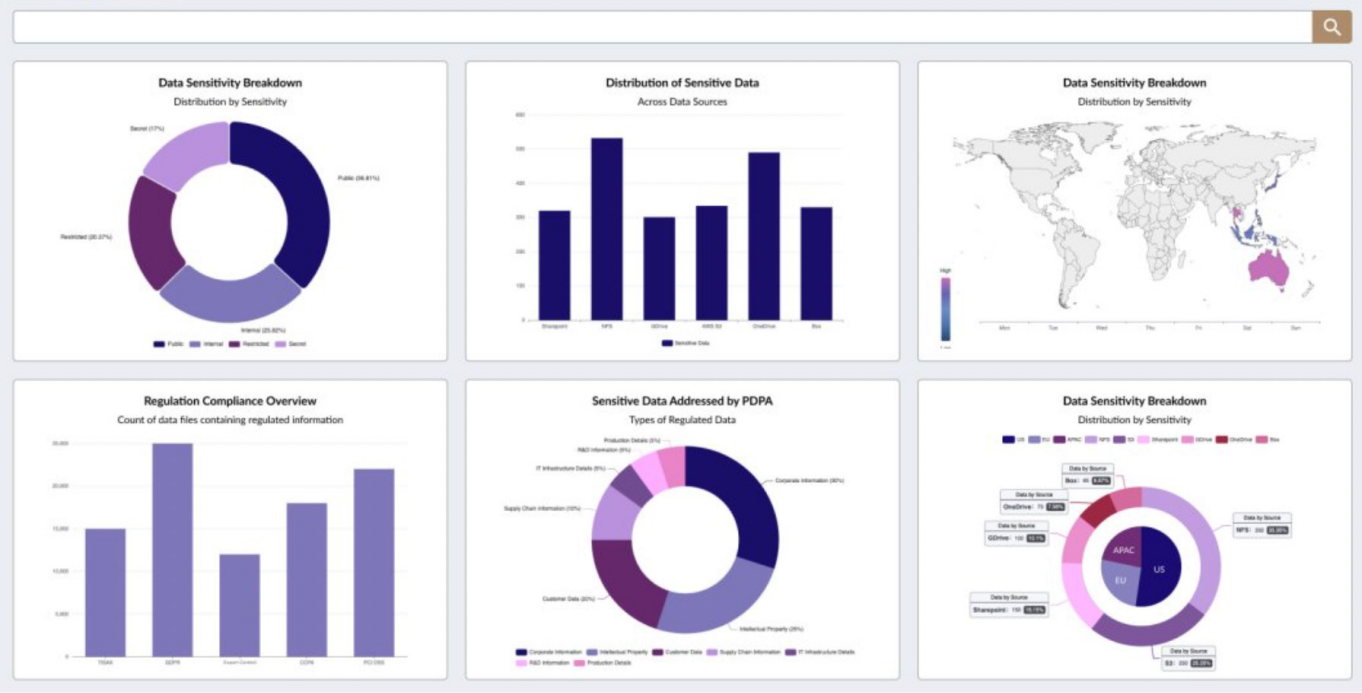
El acceso con privilegios mínimos refuerza su estrategia de Zero Trust

Un elemento clave que fortalece su estrategia de Zero Trust es el principio de acceso con privilegios mínimos. Al limitar estrictamente el acceso a los requisitos esenciales, creamos un entorno de datos más seguro. Este enfoque no solo mejora la visibilidad general de los datos, sino que también contribuye a una defensa sólida contra posibles amenazas, lo que ayuda a acelerar sus iniciativas de seguridad de Zero Trust.

El conjunto de informes de Forcepoint Data Visibility, que se encuentra en el panel de administración, permite generar informes con un solo clic, en función de cada caso de uso. Esto proporciona información sobre las áreas de riesgo clave en relación con los usuarios, los grupos y las contraseñas, y garantiza que se concedan los permisos de acceso adecuados.

Estos son algunos de los informes disponibles:

- → Archivos confidenciales
- → Permisos de acceso
- → Archivos duplicados
- → Datos redundantes, obsoletos o triviales (ROT)
- → Evaluaciones de riesgos de datos



Mediante el uso de modelos de IA y automatización avanzada, Forcepoint Data Visibility brinda visibilidad, clasificación y monitoreo continuo de los datos de forma más rápida y precisa que los métodos tradicionales. Puede identificar y distinguir fácilmente los datos de propiedad intelectual y la PII confidenciales de montones de archivos insignificantes. Puede garantizar el acceso con privilegios mínimos para evitar exfiltraciones mientras sus usuarios finales continúan siendo productivos sin inconvenientes. Dado que proporciona una vista panorámica de los datos de una amplia variedad de fuentes (servidores de archivos, Microsoft OneDrive, SharePoint, Google Drive, Box, Confluence, Azure y más), Forcepoint Data Visibility es un componente esencial de todo enfoque de seguridad de datos completo.

¿Está listo para pasar a la visibilidad de datos basada en IA?

Conozca más

Forcepoint

forcepoint.com/es/contact

Acerca de Forcepoint

Forcepoint simplifica la seguridad para las empresas y los gobiernos de todo el mundo. La plataforma todo en uno y realmente nativa en la nube de Forcepoint facilita la adopción de un enfoque de Zero Trust y evita el robo o la pérdida de datos confidenciales y propiedad intelectual sin importar desde donde trabajen las personas. Con sede en Austin, Texas, Forcepoint crea entornos seguros y confiables para los clientes y sus empleados en más de 150 países. Conéctese con Forcepoint a través de www.forcepoint.com/es, Twitter y LinkedIn.

[FP-Forcepoint Data Visibility Powered By Getvisibility-Brochure-ES] 24Jan2024