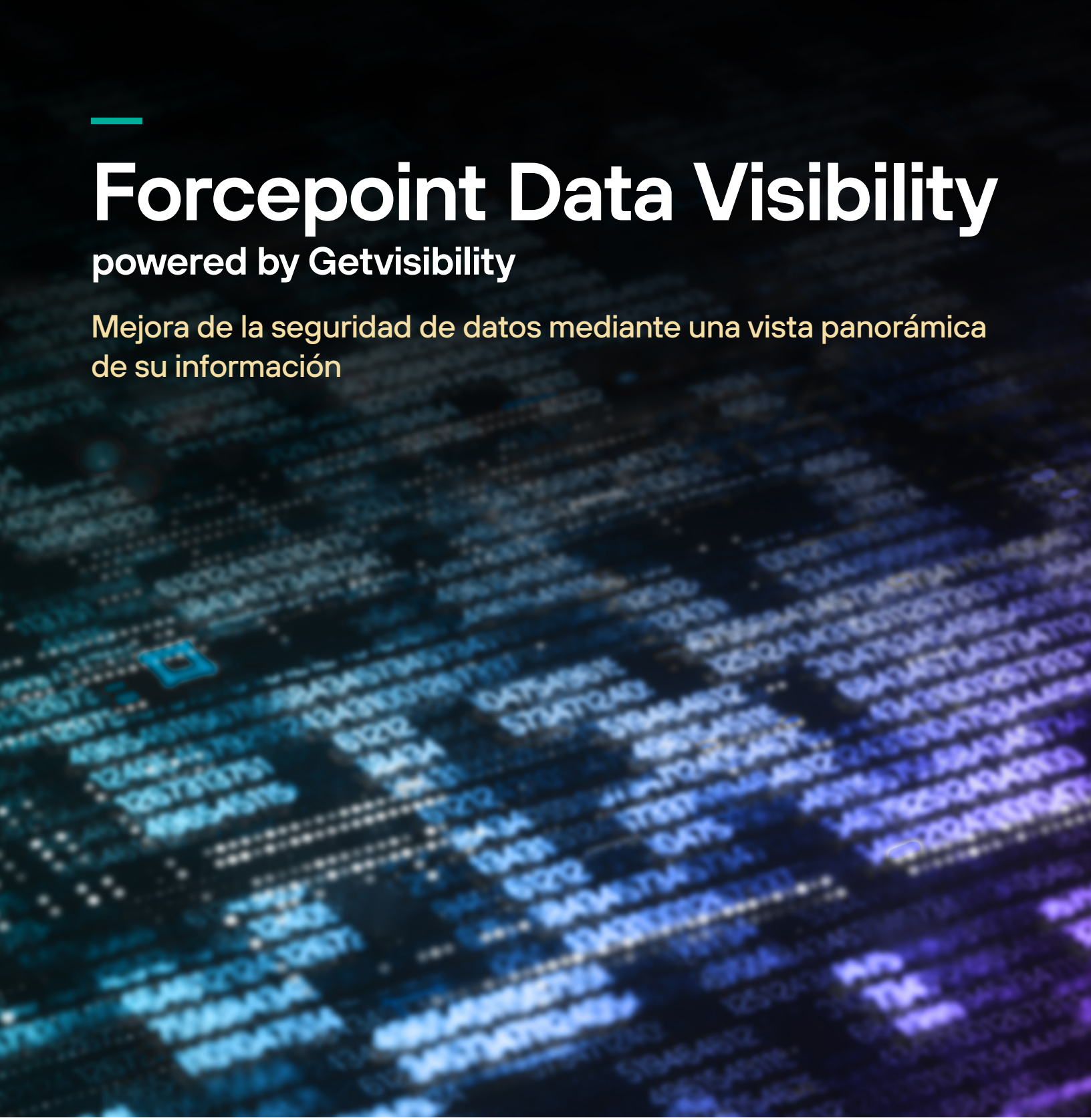


Forcepoint Data Visibility

powered by Getvisibility

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

Forcepoint

Folleto

Sus datos están en todas partes y es solo el comienzo del problema. Es muy probable que sus datos estén también aislados en distintas centrales de datos, varias nubes y muchas computadoras portátiles, lo que hace que el problema de los datos sea todavía más grande. ¿Está al tanto de exactamente qué datos tiene, dónde están ubicados y, lo que es más importante, qué nivel de riesgo generan todos estos 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 el riesgo y los costos resultantes. Las organizaciones de todo tipo y tamaño deben dedicarle atención continua.

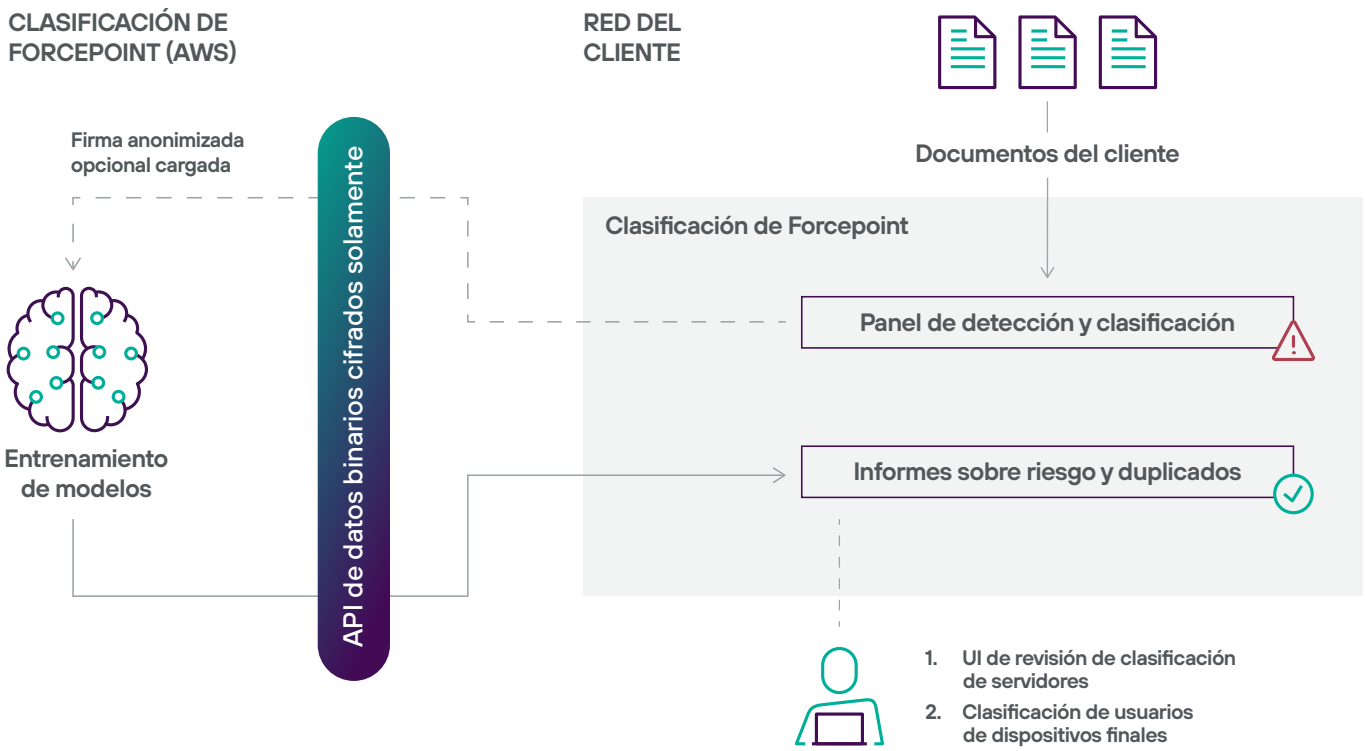
La minimización del riesgo comienza por ver los datos donde sea que residen, en las instalaciones o en la nube. Forcepoint Data Visibility powered by Getvisibility le brinda una vista panorámica de los datos de su organización. La visibilidad de datos es parte esencial del enfoque de Forcepoint respecto 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 la pérdida de datos, eliminar el riesgo de cumplimiento y, en última instancia, ahorrarle costos enormes resultado de fugas de datos y falta de cumplimiento.

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 90 % 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 datos[5] 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, febrero de 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, enero de 2022
5 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



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

Forcepoint Data Visibility supera estos desafíos mediante la aplicación de IA y AA 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 la solución se basa en un modelo de 50 dimensiones entrenado con cientos de millones de archivos de datos del mundo real de muchas organizaciones en las principales industrias. A medida que el motor la solución ingiere datos, su aprendizaje continúo basado en IA hace sugerencias de clasificación de datos en lenguaje claro, con categorización de datos, detección de información de identificación personal (PII) y calificación de riesgo de cumplimiento de datos altamente precisas.

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

La visibilidad de quién puede ver su información más sensible.

¿Está seguro de que desea que contratistas de tiempo parcial vean PII de los clientes o información confidencial de ventas? Muchas organizaciones experimentan un "aumento furtivo de los privilegios", con frecuencia otorgando 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 entre empresas que están tratando de establecer principios de seguridad de confianza cero. Los usuarios con demasiados privilegios pueden, a fin de cuentas, costarle a las empresas enormes sumas de dinero en fugas y falta de cumplimiento.[6] Una práctica recomendada para Zero Trust es el Principio del mínimo privilegio (POLP). El objetivo del POLP es limitar el acceso a solo los archivos y archivos compartidos que los usuarios necesitan estrictamente para hacer su trabajo.

Recientemente, la Corte Suprema delos EE. UU. emitió un fallo (VanBuren contra los Estados Unidos) en el que una persona pudo realizar una investigación de antecedentes sobre un amigo a cambio de un pago (USD 5000).[7] Se imputó a la persona de "acceder intencionalmente a una computadora sin acceso autorizado o superando el acceso autorizado", según la Ley de Fraude y Abuso Informático (CFAA).Sin embargo, la Corte Suprema sostuvo que la persona no podía ser imputada según la CFAA dado que la organización le había otorgado acceso legítimamente. No ocurrió acceso indebido dado que tenía permisos para acceder a tales archivos. Este fallo muestra que todas las organizaciones deben administrar los permisos de todos sus archivos y los permisos de cada usuario.

Forcepoint Data Visibility le permite administrar los permisos de todos los archivos y usuarios. Los administradores de datos ven qué personas tienen acceso a un archivo o archivo compartido en toda una organización. A través de la examinación regular es posible evitar el aumento furtivo de los privilegios, lo que reduce drásticamente la oportunidad de fugas de datos. Con un solo clic, puede ver instantáneamente permisos para todos los archivos examinados. Luego, puede aplicar el nivel de permisos adecuado necesario para que los usuarios hagan su trabajo.

Limpiando datos ROT para reducir el problema de los datos

¿Es su empresa una acumuladora en lo que respecta a cómo administran los 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 respecto de los datos, creyendo que conservar datos es algo bueno e incluso mitiga el riesgo. Sin embargo, lo que realmente ocurre es lo opuesto.

Los datos pueden ser un activo, pero también un problema. El resultado de las organizaciones que acumulan datos es que acaparan grandes cantidades de datos redundantes, obsoletos o triviales (ROT). En lugar de hacer que las empresas estén en cumplimiento, las dejan sumamente vulnerables a las fugas de datos y susceptibles a un incumplimiento incluso mayor en relación con el creciente número de reglamentaciones de 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 representan un problema. Sin visibilidad de los datos que deben eliminar, las empresas quedan susceptibles a fugas de datos y sanciones regulatorias potenciales. Un ejemplo costoso de datos ROT es la fuga de Equifax que tuvo como resultado un acuerdo legal deUSD 1380 millones.[8] La fuga de datos se centró en una unidad compartida en la que los empleados guardaban copias de nombres de usuario y contraseñas, creyendo que hacían más eficiente a la empresa al crear copias múltiples de los nombres de usuario y las contraseñas. 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.

> "Las empresas creen que retener todos los datos los ayudará a mitigar posibles riesgos; sin embargo, lo que realmente ocurre es lo opuesto. Cuántos más datos desconocidos tenga una empresa, mayor será el riesgo de ser víctima de un ataque cibernético. Cuando desconoce los datos que tiene, no es capaz de notar si falta algo."
>
> The Dangers of Obsolete and Redundant Data (Los peligros de los datos obsoletos y redundantes), eWeek Editors, abril de 2022

Eliminar el riesgo de datos ROT requiere de automatización y perspectivas granulares. Forcepoint Data Visibility comienza por proporcionar capacidades de detección y clasificación que pueden examinar rápidamente todos sus datos, independientemente de dónde se encuentren. La precisión mediante IA le brinda claridad absoluta respecto de la duplicación de archivos, las fechas de creación y último uso de cada archivo, y la clasificación y el riesgo respecto del cumplimiento de cada archivo. El panel de Forcepoint Data Visibility permite a los usuarios analizar estas distintas áreas y ver detalles de cada archivo y ejecutar informes sobre los duplicados. Armado con esta información, puede realizar el trabajo de eliminar con éxito los 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 de Zero Trust es detectar y clasificar toda la información existente y determinar rápidamente qué tiene valor y se necesita para cumplir con las reglamentaciones. Todo lo demás son datos ROT y pueden eliminarse con justificación.

Mediante el uso de modelos de IA y automatización avanzada, Forcepoint Data Visibility brinda visibilidad de datos, clasificación y monitoreo continuo más rápidos y precisos que los métodos tradicionales. Puede identificar y distinguir fácilmente entre propiedad intelectual confidencial, PII y pilas de archivos insignificantes. Puede garantizar el acceso con mínimo privilegio para evitar la exfiltración mientras sus usuarios finales continúan siendo productivos sin inconvenientes. Al brindar una vista panorámica de los datos de distintas fuentes, Forcepoint Data Visibility es un componente esencial de un 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, Twitter y LinkedIn.

[FP-Forcepoint Data Visibility Powered By Getvisibility-Brochure-ES] 01Nov2022