Forcepoint Data Visibility

powered by Getvisibility

Enhancing data security through a panoramic view of your data

Forcepoint

Brochure

Your data is everywhere, and that's just the beginning of your problems. Very likely your data is also siloed across datacenters, multiple clouds and a lot of laptops, making your data problem even bigger. Are you aware exactly what data you have, where it's located and even more importantly, what risks all of this data is bringing to your company at this moment? IDC has estimated that 80 percent of data globally is unstructured and 90 percent of that data is not analyzed[1] – in other words, it is data that is not part of an organization's daily work and is not known. That data is literally unseen. As organizations face growing compliance demands and more data breaches[2], getting visibility into all your data to minimize your risk and resulting costs is imperative. This issue demands continuous attention by organizations of all types and sizes.

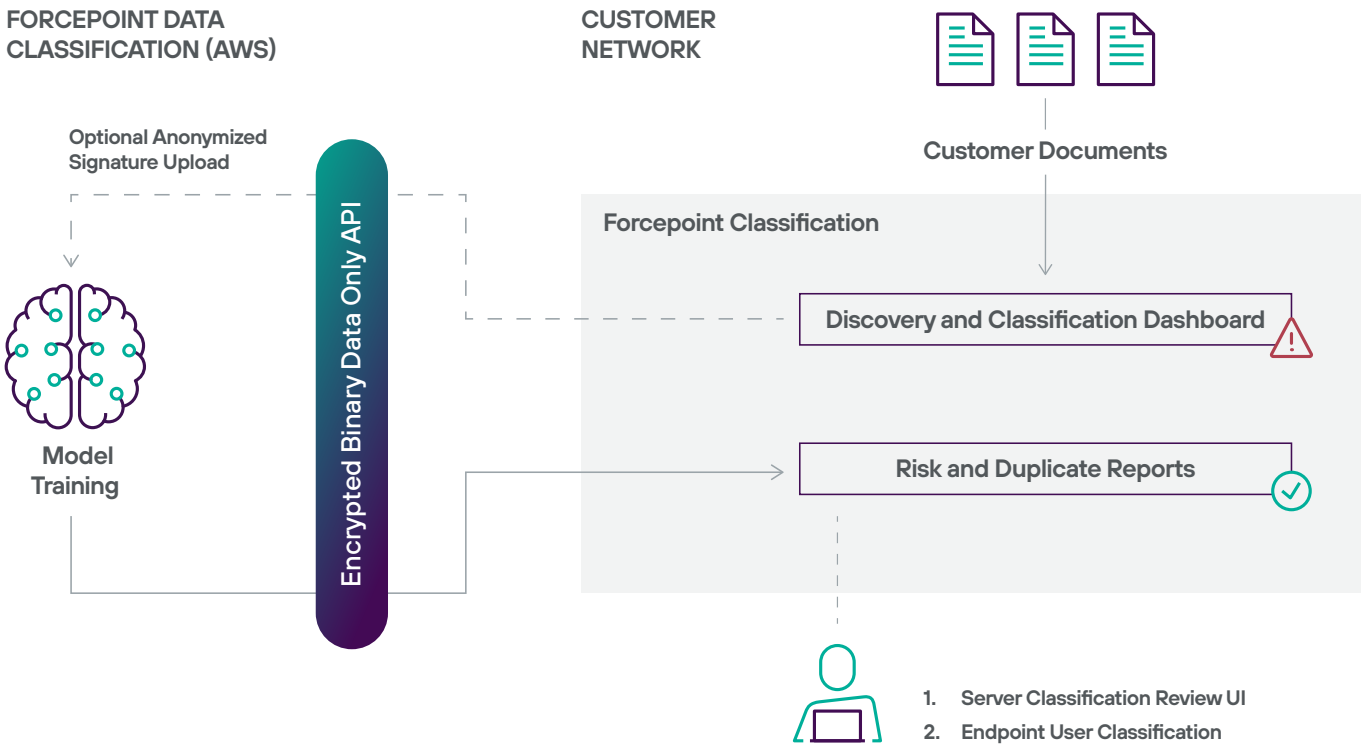
Minimizing risk starts with seeing your data wherever it resides – on-premises or in the cloud. Forcepoint Data Visibility provides a panoramic view of your organization's data. Data Visibility is a core part of Forcepoint's approach to data security, which enables customers to continuously discover, classify, monitor and protect all their data. The 360° view provided by Forcepoint Data Visibility can dramatically reduce data loss, remove compliance risk and ultimately save you the enormous costs that come with data breaches and non-compliance.

According to IDC, 80% of data globally is unstructured and 90% of that data is not analyzed, also referred to as "dark data." [3]

94% of organizations are storing data in multiple cloud environments.[4]

Equifax settled a $1.4B lawsuit for its data breach[5] exacerbated by hackers accessing a shared drive storing multiple copies of employee usernames and passwords. The company lacked tools to detect and identify redundant and outdated files.

1 The Unseen Data Conundrum, Forbes, February 2022
2 2022 Data Breach Investigations Report, Verizon, May 2022
3 The Unseen Data Conundrum, Forbes, February 2022
4 Dark Data: The Cloud's Unknown Security and Privacy Risk, Forbes, June 2023
5 Equifax agrees $1.38bn data breach lawsuit settlement, Finextra, January 2020



Fast visibility leveraging the power of Artificial Intelligence (AI)

With organizations that are storing data in multiple cloud environments, including on-prem, relying on a cloud provider that can only provide visibility into data within its own cloud service severely limits data security efficacy. Second, typical discovery and classification tools require manual admin intervention to deliver results; even those that make limited use of Machine Learning (ML) need someone to step in to make training decisions.

Forcepoint Data Visibility overcomes these challenges by applying self-learning AI and Large Language Models (LLMs) to automate the process of finding, categorizing and classifying data, regardless of whether the data is stored in the cloud or on-premises. Forcepoint's powerful pre-trained discovery and classification model is based on a 50-dimensional model trained by hundreds of millions of real-world data files from many organizations across all major industries. This innovative approach generates high-quality synthetic data for unparalleled classification accuracy and continuous improvement, without compromising data privacy associated with real data. As the Forcepoint engine ingests data, its AI-powered continuous learning makes data classification suggestions in natural language, with highly accurate data categorization,

PII detection and data compliance risk scoring.

Forcepoint provides this information through high-fidelity dashboards and reporting. These dashboards also reveal the IP address, path and in-depth permissions on every file discovered. Our classification accuracy improves with use over time, and when combined with Forcepoint Data Loss Prevention (DLP), brings greater visibility for the highest level of data security.

- **AI-powered accuracy:** Ditch slow, manual data hunts. Forcepoint's self-learning AI automatically finds, categorizes and classifies all your data, even across clouds and on-prem, saving time and boosting accuracy.
- **No more data blind spots:** Get crystal-clear dashboards with deep file details, including location, permissions and risk scores. Make informed decisions faster with intuitive data visualizations.
- **Smarter security:** Forcepoint's AI continuously learns and adapts, suggesting plain-language data classifications and detecting sensitive PII – all to proactively prevent data breaches and non-compliance.

Visibility into who can see your most sensitive information.

Do you really want part-time contractors to see customer PII or confidential sales information? Many organizations experience "privilege creep," often allowing access permissions far beyond what's needed for employees to do their job. Controlling access to the most sensitive information is often overlooked and mismanaged, even among companies that are trying to establish Zero Trust security principles. Overprivileged users can ultimately cost companies huge amounts of money in breaches and non-compliance.[6]

Forcepoint Data Visibility allows you to inspect permissions for all files and users. Data admins can see which individuals have access to a file or file shares across the organization. Through regular scanning, privilege creep can be stopped, dramatically reducing the opportunity for data breaches. With a single click, you can immediately view permissions for all files that are scanned. You can then apply the proper level of permissions necessary for users to do their work.

- **Stop "privilege creep":** Ensure users only access the data they need, preventing insider threats and accidental leaks. One click reveals permissions for all scanned files, allowing you to apply the right level of access at lightning speed.
- **Comply with regulatory mandates:** Avoid costly litigation and penalties by gaining visibility into permissions for all files and users.
- **Reduce data breach risk:** Eliminate overprivileged users, a prime target for attackers. Regular scans detect and stop privilege creep in its tracks, dramatically lowering the potential for data breaches.

Clearing out ROT to reduce data liability

Is your company a hoarder when it comes to how they managing data? Popular TV shows feature people who can't throw anything away, depicting how they ultimately live in a mass of garbage that has become completely unmanageable. Many organizations hoard data, somehow believing that maintaining data is good and will even mitigate risk. The opposite is true.
Data can be an asset, but it also can be a liability. The outcome to organizations hanging on to data is that they have amassed a large amount of ROT (redundant, obsolete or trivial) data. Instead of making companies compliant, it can leave them extremely vulnerable to data breaches and even greater non-compliance with the growing number of data regulations. A closer look at what is ROT:

- **Redundant data** is a large number of copies or versions of files stored in multiple locations in the cloud or on-prem. Organizations may mistakenly avoid deletion in case users rely on that specific copy or fear that deletion can create risk of non-compliance.
- **Outdated data** is information that is either no longer accurate or no longer in use. Typically, obsolete data has already been replaced with current, useful data.
- **Trivial data** is information that just isn't necessary to store. Trivial data provides no current benefit to the organization.

6 Worldwide Digital Loss Technologies Market Shares, 2020: DLP is Dead, Long Live DLP, IDC, October 2021
7 Worldwide Digital Loss Technologies Market Shares, 2020: DLP is Dead, Long Live DLP, IDC, October 2021

ROT data is a liability because it often contains sensitive information. Without visibility into the data they should delete, companies open themselves up to potential data breaches and regulatory penalties. An expensive example of ROT is the Equifax breach that resulted in a $1.38B lawsuit settlement.[8] At the heart of the breach was a shared drive on which copies of usernames and passwords were saved by employees, who believed they were making business more efficient through making multiple copies of usernames and passwords. Once hackers were able to get into the share, the multiple copies of usernames and passwords made the hackers' work easy. Equifax lacked tools to detect and identify redundant as well as outdated copies of the files.

"As much as a third of enterprise data can be considered ROT (and another 52% is dark data with unknown value)"

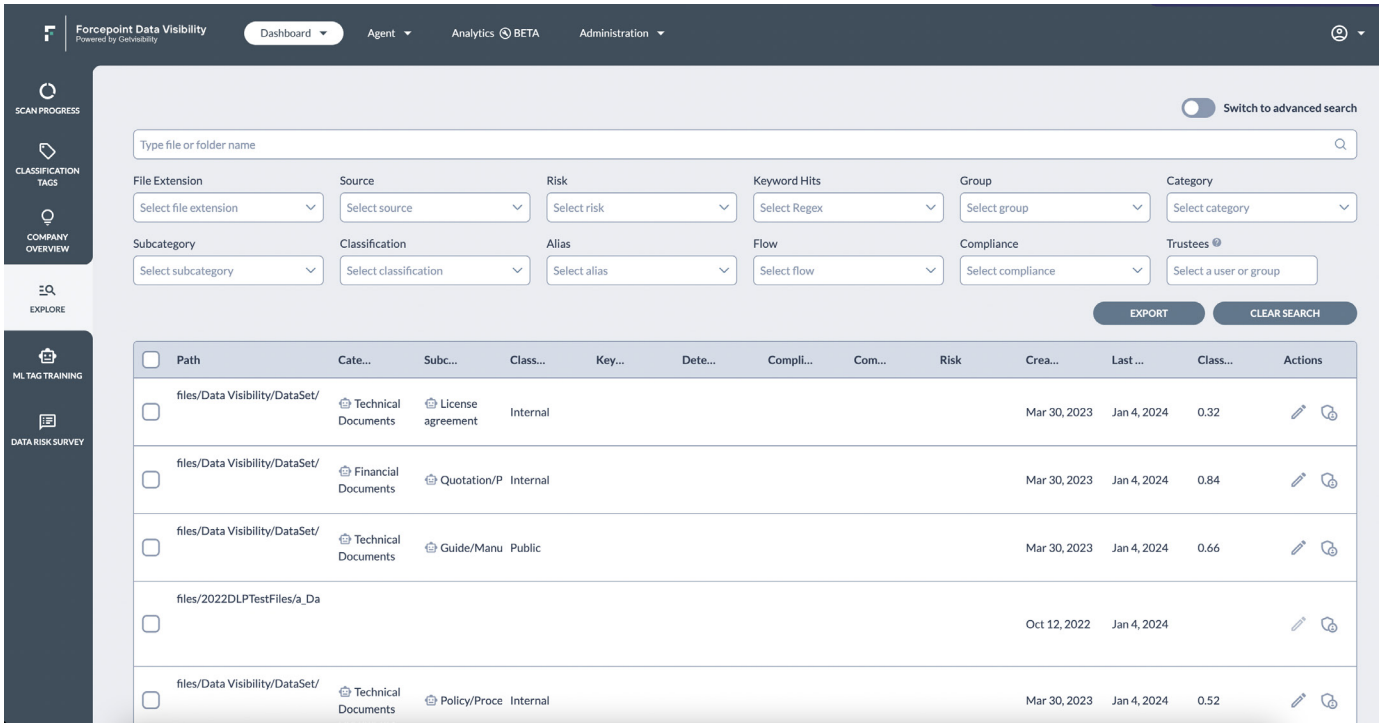
How To Keep Your Data From ROT-Ing In The Cloud, Forbes, January 2023

Eliminating ROT risk requires automation and granular insights. Forcepoint Data Visibility starts by providing discovery and classification capabilities that can rapidly scan all of your data anywhere it is located. AI-powered accuracy gives you crystal clarity into the duplication of files, creation and last used dates of each file, and classification and compliance risk of each file. The Forcepoint Data Visibility dashboard lets users drill down into these different areas, see details about each file and run reports on duplicates. Armed with this information, you can do the work of successfully clearing out ROT. Organizations with Forcepoint Data Visibility can conduct complete data scans and risk reporting as often as needed without additional costs, allowing them to proactively address their data ROT issues.

8 Equifax agrees $1.38bn data breach lawsuit settlement, Finextra, January 2020

The first step in a Zero Trust data security strategy is to discover and classify all existing information and quickly determine what has value and is needed for regulatory compliance. Everything else is ROT and can be defensibly deleted.

User-friendly dashboard for a panoramic view of your data



Forcepoint Data Visibility gives administrators a user-friendly dashboard that can be easily searched, filtered and sorted according to the administrator's needs. There are options to verify results from the AI model, change the category and subcategory, and adjust the presence of PII within a document, which can be updated in the AI model both automatically and manually. Further streamlining security operations, these results can be exported in an actionable format for remediation or other tasks to address areas of risks.

Utilizing this user-driven training AI model provides continuous self-learning for increased personalization and accuracy for the organization.

Continuous self-learning model for increased personalization and accuracy

Forcepoint Data Visibility utilizes the power of generative AI and multiple leading Large Language Models (LLMs) to enhance data security in several ways:

- → **Improved accuracy:** Our advanced AI models are pre-trained and learn from an extensive repository of hundreds of millions of files from diverse companies and industries. This comprehensive approach ensures accurate classification of data by understanding the nuances of various organizational landscapes, making classifications meaningful and actionable.
- → **High-quality synthetic data:** This represents an innovative approach in which we generate precise synthetic data from our AI model, ensuring unparalleled classification accuracy and continuous improvement without compromising privacy or security concerns associated with real data.
- → **Personalized AI model:** Our AI model is user-driven and continuously improving, delivering a solution that is tailored to your specific organizational and industry needs for your data landscape, providing better personalization and accuracy.

All these elements work together seamlessly to deliver 98%+ classification accuracy across 70 classification fields, giving you better visibility over your data across the organization. This means fewer DLP false positives, along with a stronger defense against data breaches and exfiltration.

Least privileged access strengthens your Zero Trust strategy

A key element that strengthens your Zero Trust strategy is the principle of least privileged access. By strictly limiting access to only the essential requirements, we create a more secure data environment. This approach not only enhances overall data visibility but also contributes to a robust defense against potential threats, helping to accelerate your Zero Trust security initiatives.

The Forcepoint Data Visibility reporting suite sits within the administrator dashboard and allows for one-click, use case-specific report generation. This provides information on key areas of risk regarding users, groups and passwords and ensures correct access permissions.

Available reports include but are not limited to:

- → Sensitive Files
- → Access Permissions
- → Duplicate Files
- → Redundant Obsolete or Trivial (ROT)
- → Data Risk Assessments

Using AI models and advanced automation, Forcepoint Data Visibility delivers faster and more accurate data visibility, classification and continuous monitoring than traditional methods. You can easily identify and distinguish between sensitive intellectual property, PII and piles of meaningless files. You can ensure least privileged access to prevent exfiltration while your end users stay productive with ease. By providing a panoramic view of data across a wide range of sources (file servers, Microsoft OneDrive, SharePoint, Google Drive, Box, Confluence, Azure and more), Forcepoint Data Visibility is an essential component of a complete data security approach.

Are you ready to move to AI-based Data Visibility?

Learn More

Forcepoint

forcepoint.com/contact

About Forcepoint

Forcepoint simplifies security for global businesses and governments. Forcepoint's all-in-one, truly cloud-native platform makes it easy to adopt Zero Trust and prevent the theft or loss of sensitive data and intellectual property no matter where people are working. Based in Austin, Texas, Forcepoint creates safe, trusted environments for customers and their employees in more than 150 countries. Engage with Forcepoint on www.forcepoint.com, Twitter and LinkedIn.

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