Forcepoint

Datasheet

Forcepoint Data Security Posture Management

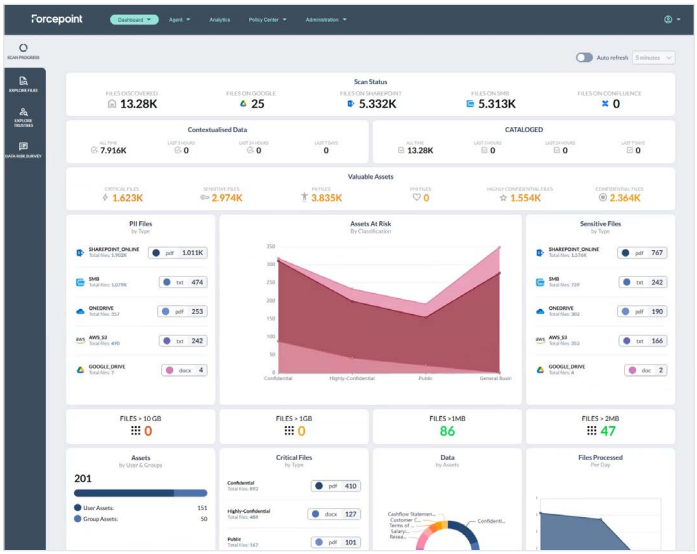
Key features and benefits:

- **AI and ML –** AI cataloging delivers unmatched accuracy and efficiency, continuously evolving through machine learning for ongoing enhancements.
- **Rapid discovery –** Run Forcepoint DSPM in the cloud and on-prem storage locations, as often as you like.
- **Real-time monitoring and risk assessment –** Check access permissions and other data risks.
- **Automated remediation –** Efficiently resolve issues in near real-time with minimal intervention.
- **Workflow orchestration –** Implement business priorities for stakeholders.

As more organizations migrate applications and data from on-premises to the cloud, they face the ongoing struggle of keeping track of where their sensitive data is, who can access it, and how it's used. The exponential growth of "dark data," which is concealed within cloud-based repositories or scattered across individual devices, poses a significant risk. It is estimated that up to 80 percent of an organization's data exists in this elusive "dark" state, beyond the reach of traditional oversight.

The consequence of this obscured data landscape is critical. Without clear visibility and management, organizations are exposed to heightened risks of breaches, with potentially devastating consequences across commercial, nonprofit and governmental sectors alike. In today's digital transformation era, the imperative to regain control of sensitive information has never been more urgent.

Forcepoint DSPM is designed to address those challenges. It delivers visibility across cloud and on-prem storage locations, leveraging AI-powered machine learning to continuously improve data discovery and classification accuracy. It also automates tasks such as remediation and reporting to streamline processes and reduce costs. With Forcepoint DSPM, organizations can improve productivity, reduce data security risks and ensure compliance with data privacy regulations.

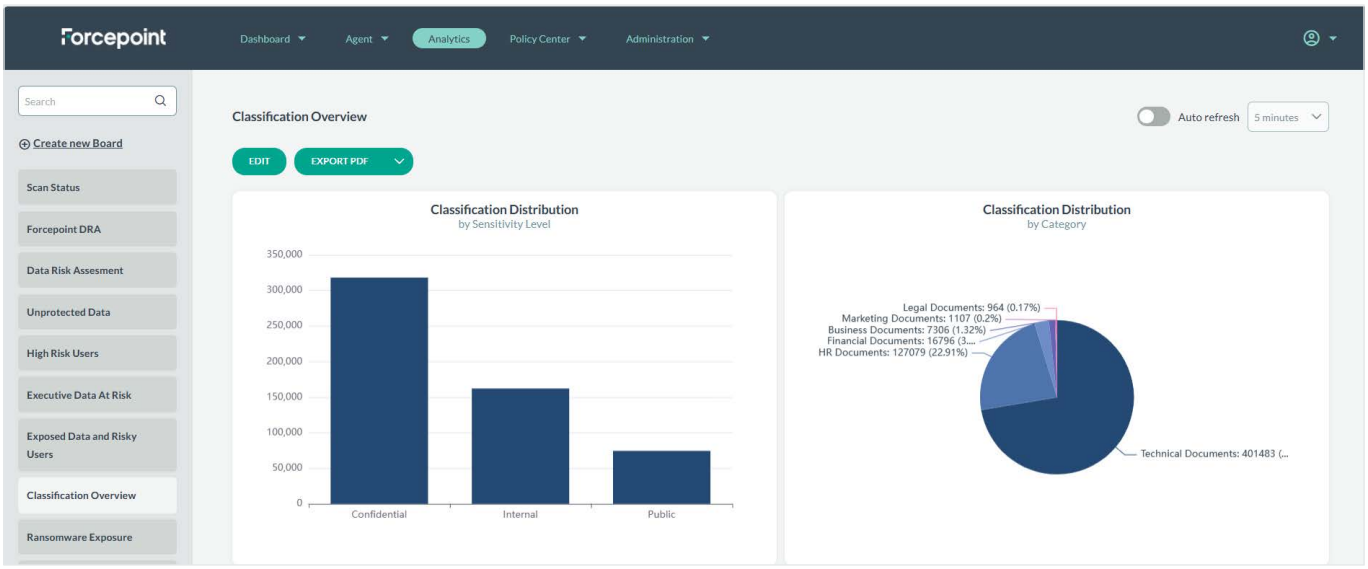


Fast, comprehensive discovery

With a multitude of connectors, Forcepoint DSPM efficiently locates sensitive data across diverse storage environments, whether in the cloud or on-premises, scanning approximately one million files per hour across major platforms such as Amazon (AWS S3 and IAM), Microsoft (Azure AD, OneDrive, SharePoint Online) and Google (Google Drive and IAM), as well as local LDAP and SharePoint systems.

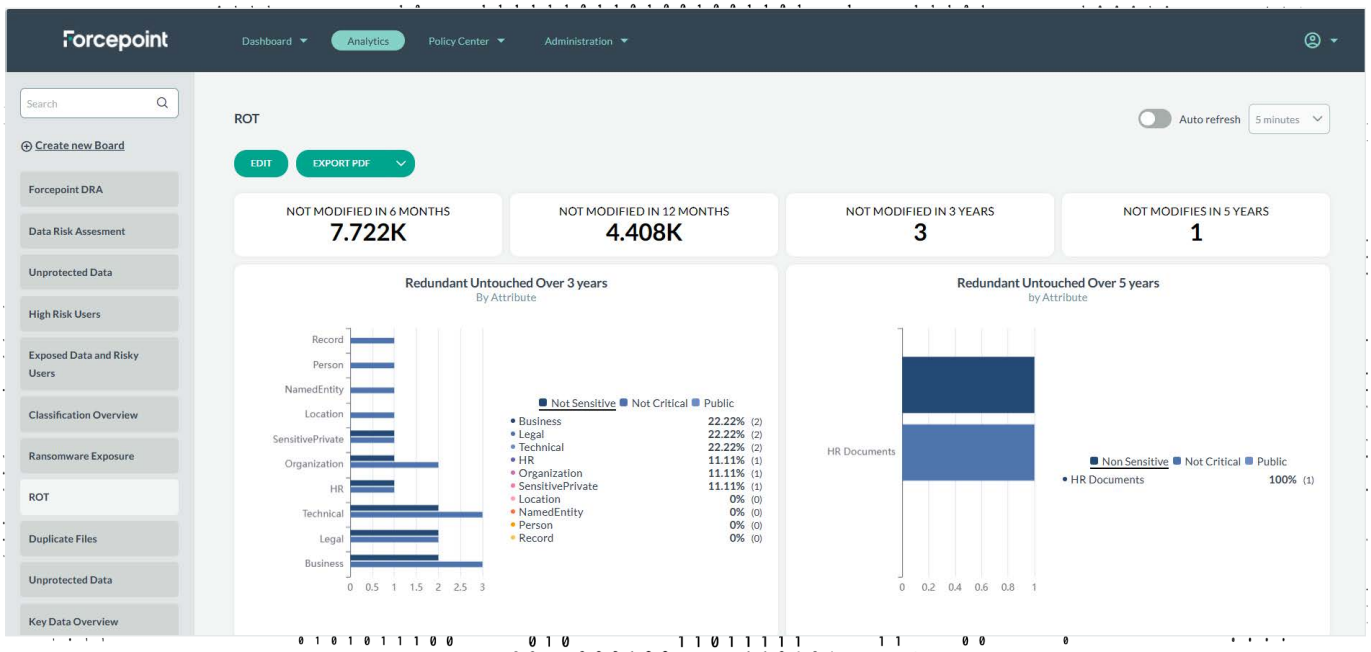
AI-powered data classification

Forcepoint DSPM applies a cloud-based AI model trained by LLM synthetic data and domain-specific GenAI with ML training. It accurately classifies data and can learn to differentiate between sensitive and non-sensitive data, surpassing simple pattern matching to safeguard valuable assets such as intellectual property. Our AI model can be trained to create custom classifications based on your specific needs. For example, it has been used to distinguish between valuable IP formulas and recipes from common ingredient lists to ensure that intellectual property is protected without triggering false alerts.



Real-time monitoring and data risk assessment

As Forcepoint DSPM scans and discovers data, it delivers detailed information such as the number of internally shared files containing critical information, the quantity of PII files at risk, and the count of redundant, outdated, and trivial data (ROT) files.

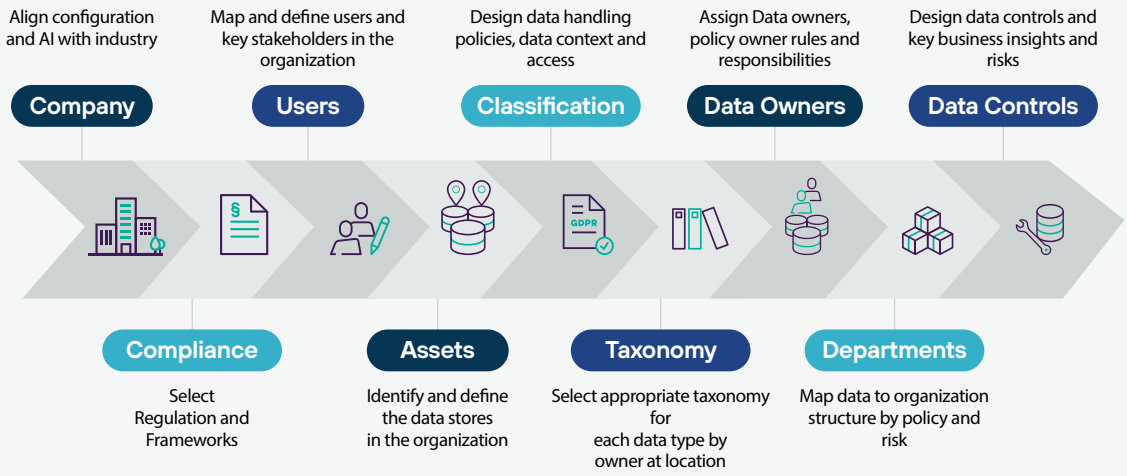


Automated remediation

Forcepoint DSPM goes beyond just detecting potential problems; it quickly resolves them with automated remediation. It performs tasks such as deduplication, permission repair, quarantining, and file relocations without requiring additional costly add-on tools.

Workflow orchestration

Streamline data security governance effortlessly with Forcepoint DSPM. Its intuitive workflow orchestration ensures efficient tracking of data ownership and accountability. By breaking down silos and facilitating collaboration among stakeholders, it aligns responsibilities, enhancing operational efficiency and fostering clarity across the organization.



Implementing a robust DSPM solution is crucial for organizations aiming to streamline their data estate and safeguard sensitive information across cloud and on-premises data storage locations. By utilizing Forcepoint DSPM, organizations can boost productivity by enhancing the reliability of data access and sharing, fostering innovation and encouraging collaboration. Moreover, organizations can lower costs through comprehensive automation, reducing the time and resources required for investigation and remediation efforts. Simultaneously, they can mitigate risk by proactively identifying and addressing improper usage of sensitive data, thus preventing data breaches. Ultimately, organizations can streamline compliance efforts by attaining genuine visibility and control over sensitive data across all environments.

Robust Discovery

FEATURE	BENEFIT
Rapid discovery and cataloguing	It runs on multiple sources to scan greater volumes of files per second/hour and synthesizes details about unstructured data assets, organizing them into an easy-to-digest format.
Extensive data source connectors	Robust visibility into more unstructured data by offering a wide range of data source connectors.
Overexposed data analysis	Identify overexposed data that is publicly shared, shared externally with 3rd parties, and overshared internally.
View permissions for every unstructured data file	View individual user access for each file and see users with access to the most files.
Eliminate risk due to ROT (redundant, outdated, trivial) data	Identify and eliminate files that are redundant, outdated, or trivial (ROT).
Visibility into access and permissions	Integrations with Active Directory and other IRM solutions enhance access security within organizations.

AI-powered Data Classification

FEATURE	BENEFIT
AI/ML classification of existing unstructured data.	Highly accurate classification suggestions recommended for existing unstructured data that is scanned.
Custom model training	Organizations can tailor the AI model to suit unique data needs (e.g., IP, trade secrets, etc.), and through machine learning, it can improve over time for greater accuracy.
Able to map tags to the Microsoft Purview IP tagging.	Provides additional layer of classification granularity, complementing the MPIP tags. Able to correct MPIP tagging.
Data tagging	Streamlining the DLP rollout enhances DLP efficiency by tagging all scanned and classified files with labels that are readable by DLP with typical tags (classified, highl y classified, public) as well as business cataloging/tagging (HR, marketing, finance, devops - with sub tags such as resumes, POs, etc.).
Integrates with Forcepoint DLP	Can be integrated to utilize DSPM AI-powered tagging of files (classification) to build strong policies against.

Real-time Monitoring and Risk Assessment

FEATURE	BENEFIT
Data Risk Assessments (DRA)	Free Data Risk Assessments are available to analyze an organization's current data risk posture across multiple categories.
Detailed interactive dashboard	View comprehensive file details on one screen. Drill down for crucial file data like risk level, permissions, and locations (IP address, path).
Reporting function	Generate reports that show both general compliance readiness as well as for specific privacy regulations.
Advanced alerting system	Provides sophisticated data controls and alerts found during scans for any anomalies or potential breaches.
Data Subject Access Request (DSAR) search	Simplify generation of a DSAR to quickly comply with privacy regulations requests.
Analytics suite	Experience an advanced analytics suite for easy access to security and classification insights at a glance. Select from various predefined dashboards or craft your own, and effortlessly export PDF snapshots with just one click. Predefined dashboards include overexposure and ransomware analysis, critical data duplication, risky user detection, data retention, misplaced data, data risk assessment, sovereignty, and incident tracking for data control violations.
Ransomware exposure analysis	Identify critical data that is exposed to a ransomware attack.
No-code reporting and analytics builder	Easily create custom use cases and analytics reporting with no coding required.
Risky user identification	Identify users with elevated risk profiles who have access to significant amounts of critical information.
Data control incident	Provides a clear view on any data control violations and a status of incident resolution.

Automated Remediation

FEATURE	BENEFIT
Remediations for permissions	Receive automated notification of data security governance incidents or compliance issues, streamlines tracking and managing with existing ITSM and productivity tools, that includes alerts for overexposed data.
Remediation for data de-duplication	DSPM's de-duplication feature identifies and eliminates redundant data, reducing storage needs and costs, optimizing resource allocation. It deletes automatically according to customizable data controls.
Remediation for file quarantine/move/delete	Provide automated remediation actions for mislocated data, either quarantining, moving to a sanctioned location, or deleting based on data controls.

Workflow Orchestration

FEATURE	BENEFIT
Advanced data controls	Flexibility to define custom data control rules tailored to specific organizational needs or choose from a variety of predefined rules commonly used.
Data ownership	Defines accountability with ease and achieves stakeholder alignment. Facilitating effective remediation.
Task manager	Assigns tasks to data custodians and owners, allowing tracking of DSPM statistics (such as open, resolved, and closed tickets, resolution time).