Forcepoint

Datasheet

Forcepoint Data Security Posture Management

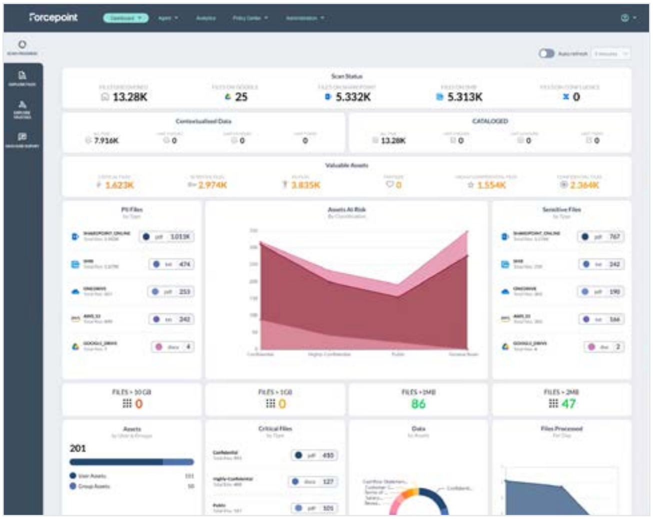
Key features and benefits:

- **AI Mesh Classification –** Highly accurate and efficient networked classification architecture using GenAI, predictive AI and data science capabilities.
- **Rapid discovery –** Run Forcepoint DSPM in the cloud and on-prem storage locations, as often as you like.
- **Real-time risk assessment –** Check access permissions and other data risks.
- **Workflow orchestration –** Implement business priorities for stakeholders.

Digital transformation has evolved into AI transformation, driven by the integration of AI technologies, particularly GenAI applications, into business processes. Coupled with data sprawl from organizations migrating applications and data from on-premises to the cloud and utilizing GenAI tools such as ChatGPT, Copilot, and Gemini, 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," hidden within cloud-based repositories or spread across individual devices and now Gen AI applications presents a substantial risk. It is estimated that as much as 80 percent of an organization's data exists in this obscure "dark" state, evading 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's AI Mesh empowers organizations with superior data classification accuracy. Its networked AI architecture, leveraging a GenAI Small Language Model (SLM) and advanced data and AI components, efficiently captures context from unstructured text. Customizable and efficient, it ensures rapid, accurate classification without extensive training, enhancing trust and compliance.

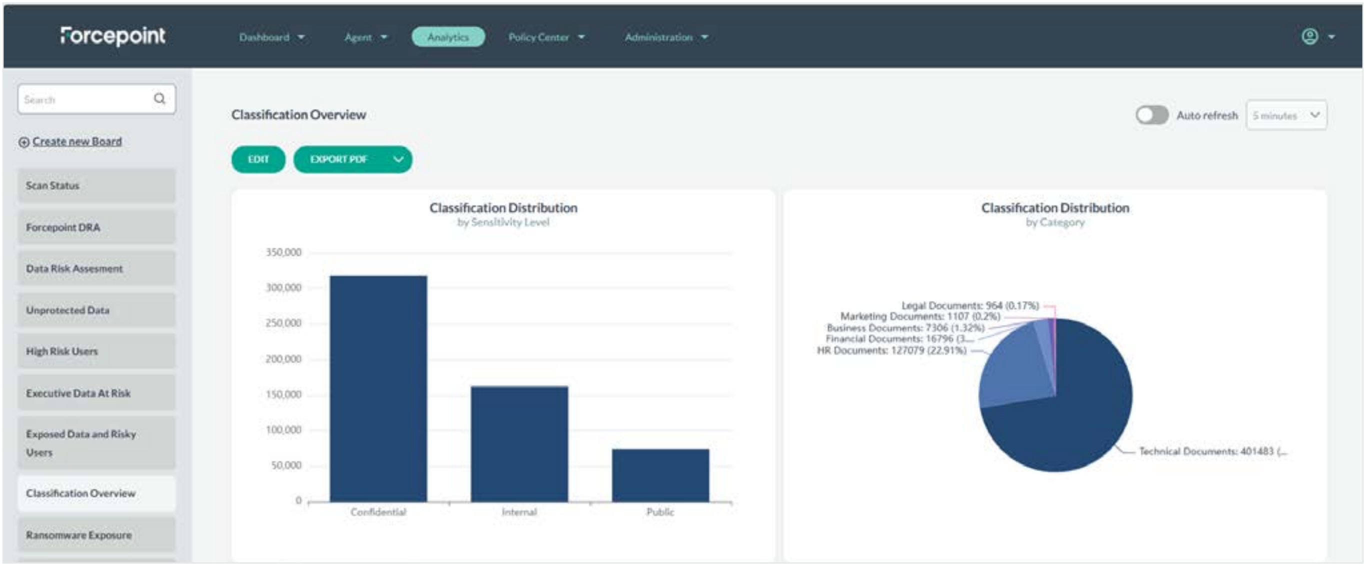


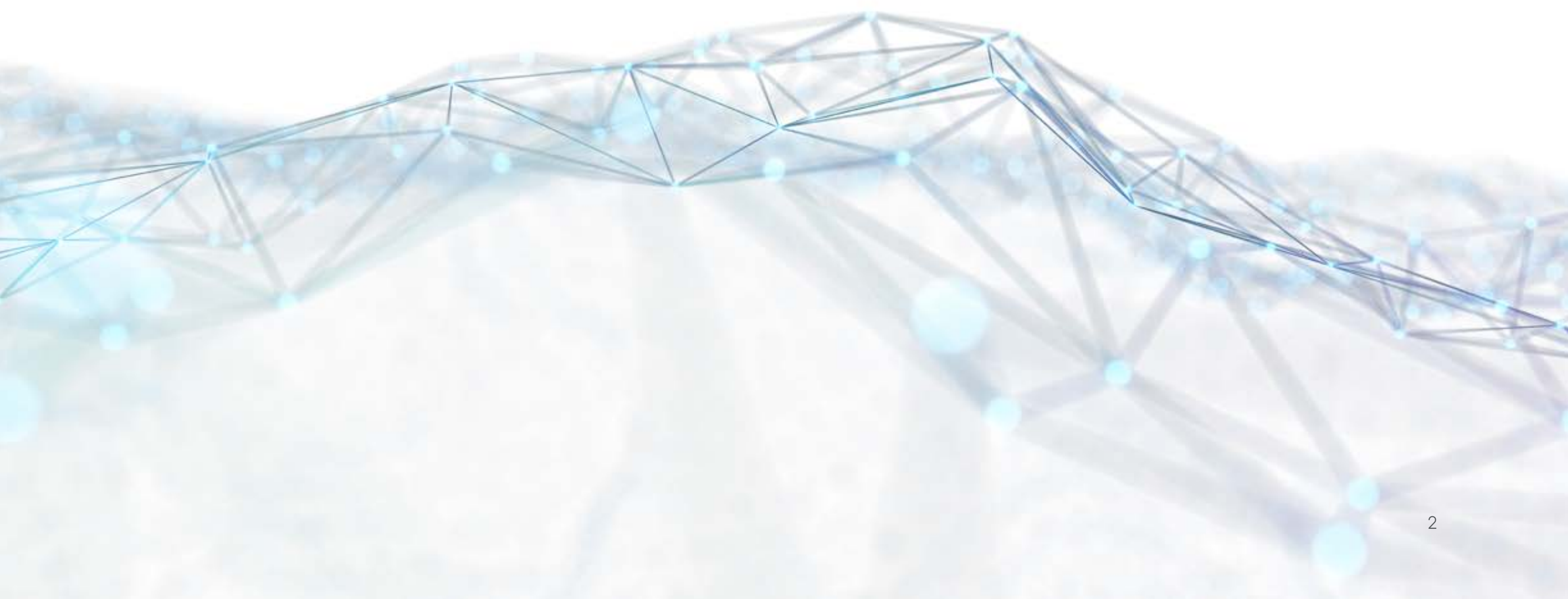
Fast, comprehensive discovery

With a multitude of connectors, Forcepoint DSPM efficiently locates sensitive data across diverse storage environments, whether in the cloud or on-premises, scanning 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 Mesh enabled accuracy

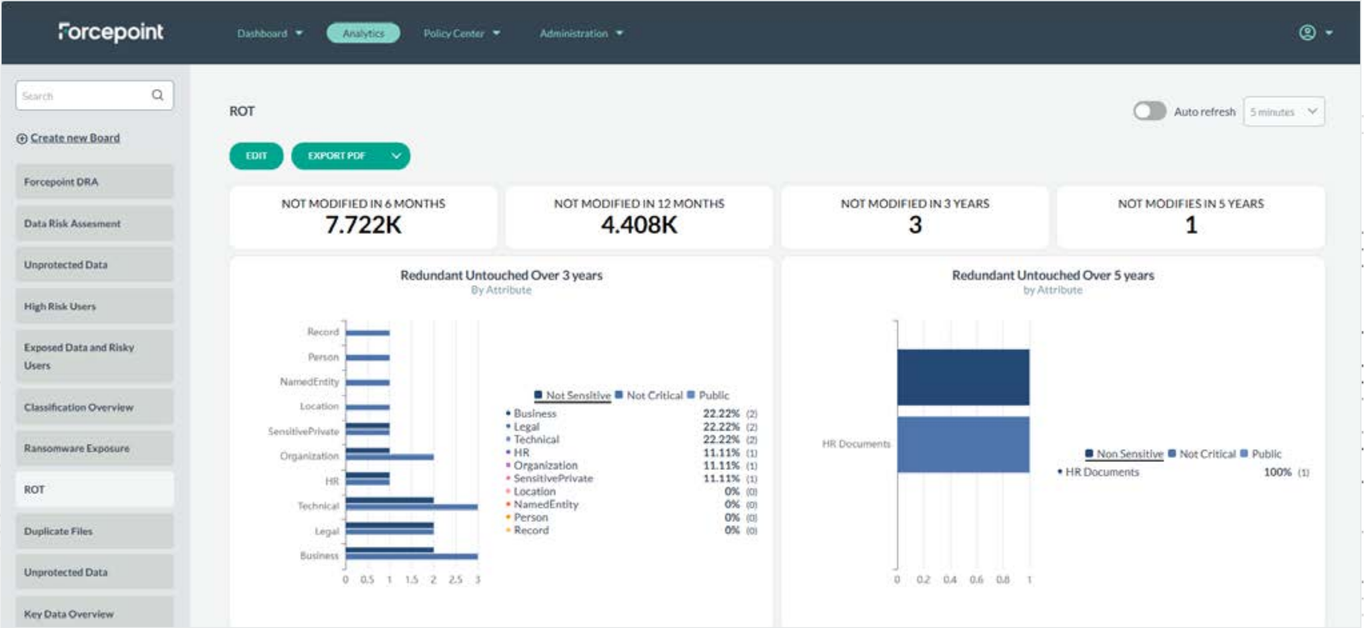
Forcepoint DSPM's AI Mesh feature excels at empowering today's organizations with superior data classification accuracy. Unlike other DSPM solutions, it offers a multi-node, connected AI architecture, leveraging a GenAI SLM and a network of advanced data and AI components. This structure efficiently captures context and transforms unstructured text into precise document classifications. The AI Mesh is customizable, tailoring to industry needs and regulatory environments. It runs efficiently on standard compute resources without requiring GPUs while providing high performance classification. High accuracy is achieved without extensive ML training, reducing maintenance costs. The explainability of the AI Mesh enhances trust and compliance, ensuring a highly secure data posture and adherence to privacy regulations.





High performance 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.



ROT

NOT MODIFIED IN 6 MONTHS	NOT MODIFIED IN 12 MONTHS	NOT MODIFIED IN 3 YEARS	NOT MODIFIES IN 5 YEARS
7.722K	4.408K	3	1

Redundant Untouched Over 3 years
By Attribute

■ Not Sensitive ■ Not Critical ■ Public

• Business	22.22% (2)
• Legal	22.22% (2)
• Technical	22.22% (2)
• HR	11.11% (1)
• Organization	11.11% (1)
• SensitivePrivate	11.11% (1)
• Location	0% (0)
• NamedEntity	0% (0)
• Person	0% (0)
• Record	0% (0)

Redundant Untouched Over 5 years
by Attribute

■ Non Sensitive ■ Not Critical ■ Public

• HR Documents	100% (1)

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 secure their data posture 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. 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.
Connects to important data sources	Robust visibility into unstructured data by offering a range of data source connectors.
Overexposed data analysis	Identify overexposed data that is publicly shared, shared externally with 3rd parties, and overshared internally.
View and remediate permissions	View access for each file and remediate to establish principle of least privilege (POLP) zero trust security.
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 Mesh Data Classification

FEATURE	BENEFIT
AI Mesh classification of unstructured data	Highly accurate AI classification for unstructured data.
Custom model training	Organizations can tailor the AI Mesh model to suit unique data needs (e.g., IP, trade secrets, etc.), for highly accurate data classification, reducing DSPM and DLP false positives/negatives.
Able to map tags to the Microsoft Purview IP tagging.	Provides additional layer of classification granularity, complementing the MIP tags. Able to correct MIP tagging.
Data tagging	Tags all scanned and classified files with persistent labels that are readable by DLP with standard tagging (classified, highly 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 with Forcepoint DLP to utilize DSPM AI Mesh 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 security 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 regulation 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, incident tracking for data control violations and many more.
Ransomware exposure analysis	Identify critical data that could be exposed to a ransomware attack.
No-code reporting and analytics builder	Easily create custom use cases and analytics reporting with no coding skills 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.

Forcepoint

forcepoint.com/contact

[FP-Data Security Posture Management Datasheet-EN] 03Jan2025