Forcepoint Data Classification

Combining AI Mesh and Small Language Model to deliver highly accurate data classification for Forcepoint Data Security and Forcepoint Enterprise DLP

Forcepoint

Brochure

Fundamental Challenge to Data Security

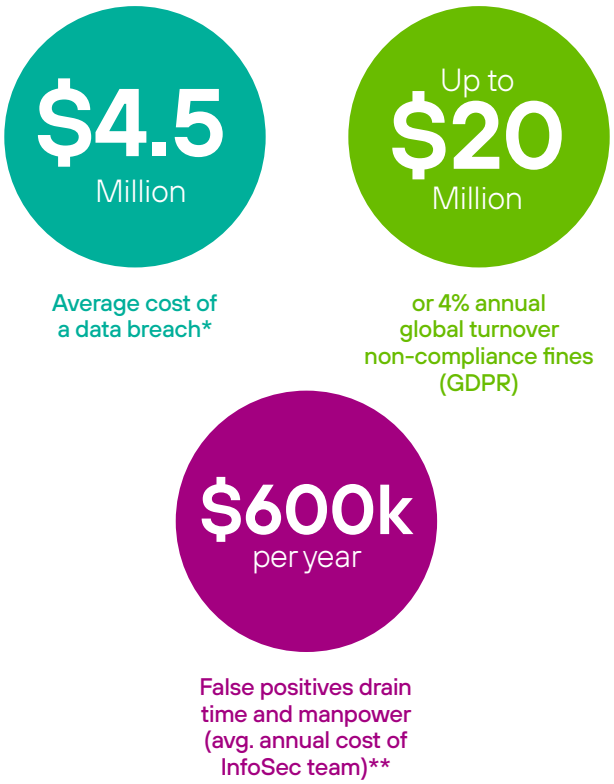
When it comes to an organization preventing the loss of data, the common phrase, "you can't protect what you can't see," speaks to the very foundation of data security.

Organizations that lack an effective method for identifying the various types of data that they have are ultimately unable to prevent the loss of that data. Traditional classification methods are highly manual, largely depending solely on users to make critical classifications decisions about the value of data. Inaccurate data classification generates large volumes of false positives and false negatives in Data Loss Prevention (DLP) policy enforcement. This results in wasted time and resources. It also impacts an organization's ability to keep sensitive data from being exfiltrated and leaves it open to security threats from both outside (malware, ransomware) and within the organization (malicious insiders, misuse, error, mistaken classification).

Leveraging AI Mesh to Gain Sight into All of Your Data

Forcepoint's AI Mesh feature excels at empowering today's organizations with superior data classification accuracy. It offers a multi-node, connected AI architecture, leveraging a GenAI Small Language Model (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 rapid classification within 200 milliseconds. High accuracy is achieved without extensive ML training, reducing maintenance costs. Moreover, the AI Mesh ensures auditable and explainable adherence to AI and privacy regulation requirements, such as the AI Act in the EU.

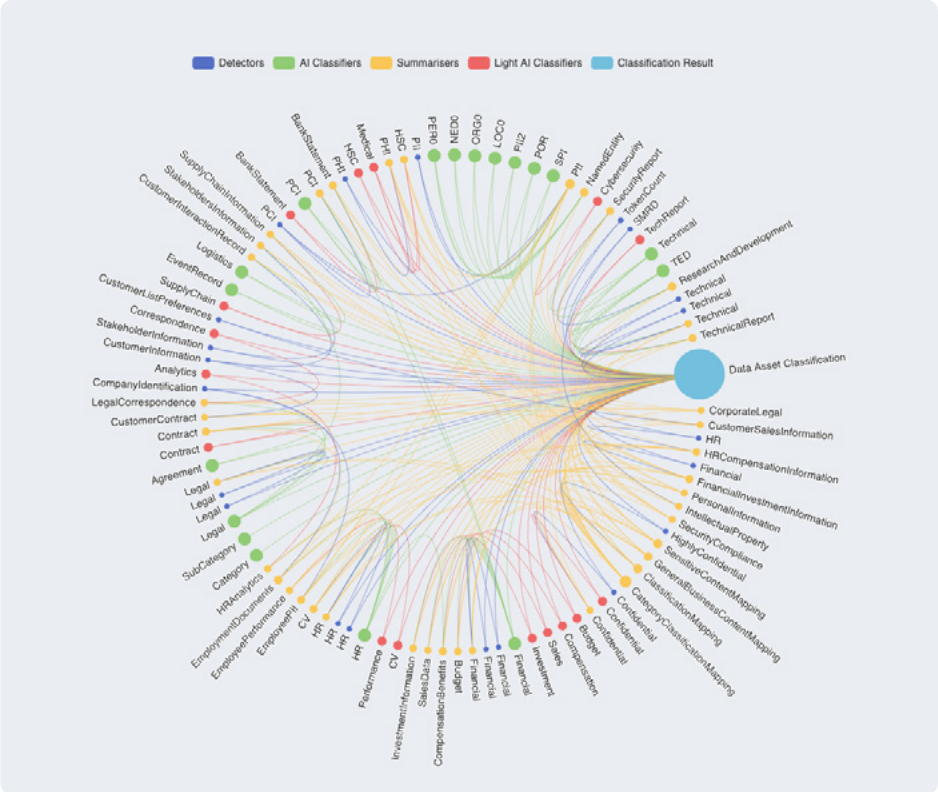
Impact of Inaccurate Data Classification



* Source: IBM Security: Cost of a Data Breach Report 2023
** The Quest for a Single Set of Unified DLP Policies (IDC)

Forcepoint Data Classification achieves unparalleled accuracy by using the latest AI Mesh and SLM innovations:

- **Leveraging the GenAI SLM** and a network of advanced data and AI components efficiently captures context and transforms unstructured text into precise document classification.
- **AI Mesh is customizable,** tailoring to industry needs and regulatory environments.



Visual Representation of AI Mesh

During file creation, Forcepoint Data Classification enables you to add visual labels and metadata, giving you the option of selecting your own classification or using the AI-generated recommendation.

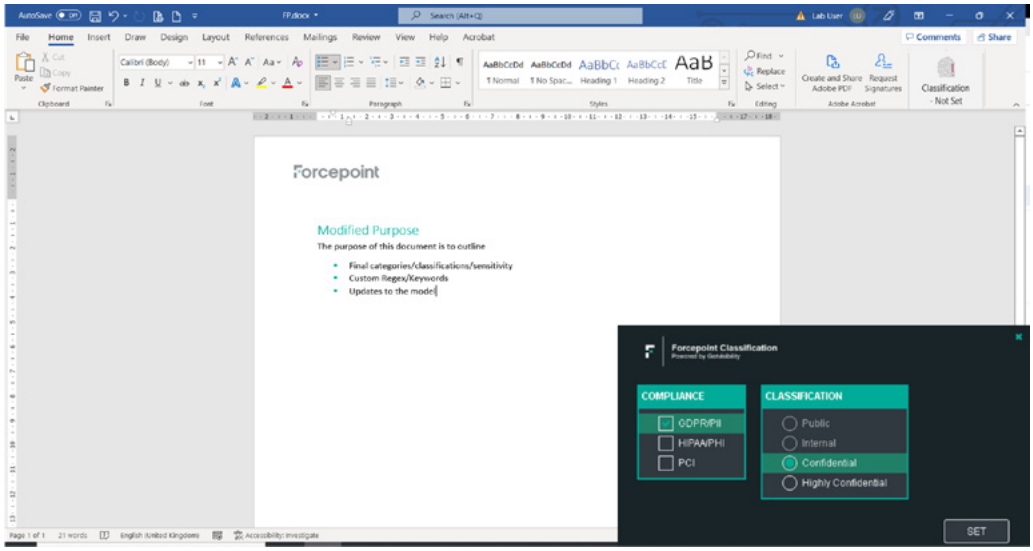
Each recommendation is delivered with a confidence level based on the data within the file compared with the AI model to help make highly accurate classification decisions. The decision then enables you to add visual labels and metadata to facilitate policy enforcement and regulation compliance. As the tool is used, it continues to learn and improve. The customization configuration wizard options include:

› Compliance
› Classification
› Enforcement rules
› Visual labeling
› Email sharing rules
› Exceptions

The result is that Forcepoint Data Classification delivers real-time classification of newly created data, no matter where your people work. Through continual learning and improvement, it delivers the most accurate classification tailored to your business needs, all while requiring minimal effort to deploy and ensuring a low Total Cost of Ownership (TCO).

- **AI-powered** for industry-leading accuracy and efficiency
- **Minimal maintenance** with AI Mesh's low maintenance requirements, organizations save time and resources. It eliminates the need for extensive retraining, ensuring sustained accuracy without constant intervention.
- **Efficient data classification,** AI Mesh rapidly and accurately classifies data within milliseconds, streamlining processes and reducing manual effort. This efficiency allows teams to focus on higher-value tasks.

Seamless Industry-Leading Precision and Efficiency



Forcepoint Data Classification is an industry-leading solution that seamlessly sits in the Microsoft application ribbon, providing easy access to the current document classification status. Upon selection, users receive prompts to choose classifications with AI-powered suggestions. After saving, the chosen classification level is automatically applied and embedded in the document's metadata.

Accuracy

Forcepoint Data Classification uses advanced AI Mesh and SLM to suggest classifications to users, dramatically increasing accuracy and reducing human error.

Automation

Automate the classification and protection of your data in real-time as your teams work and collaborate on apps anywhere.

Visual Labeling

Customizable visual labeling allows you to add custom headers, footers or extra text fields, based on your organization's policies.

User Activity Reporting

Gain deep insights into end-user activity through granular analytics, including insights into the top users, number of incidents per day, incident types, and much more.

Compatibility

Seamless integration with a popular business applications including Microsoft Office Suite. Pair with Forcepoint Data Security and Forcepoint Enterprise DLP, to immediately enable AI-powered data classification upon deployment.

Streamline Compliance

Forcepoint Data Classification makes it easy for organizations to meet compliance standards with efficient customization and transparent classification. By customizing AI Mesh to specific industry sectors, regulatory requirements, and user preferences, organizations can better align with privacy regulations. Adjustable sensitivity settings and user-specific detectors ensure precise data handling, reducing compliance risks. AI Mesh also provides transparent classification with explainable outcomes achieved through a limited number of signals, enhancing trust and facilitating compliance audits. Its ability to operate with smaller datasets simplifies verification of adherence to privacy regulations without compromising sensitive information.

- Out-of-the-box key regulations simplifying compliance
- Continuous data monitoring ensures ongoing adherence to evolving regulations
- Granular policy controls allow you to tailor-fit to specific compliance needs
- Streamlines compliance with the broadest coverage of data types in the industry

For more information schedule a demo today.

Appendix A - Key Features:

FEATURE	OVERVIEW
Data Classification	Windows and UNIX File Servers, Windows Unix and MacOS computers, Android and iOS mobile devices, NAS, Microsoft Online, DropBox, Box and GDrive (uses AIbased classifier).
Personal Identifiable Information (PII) Identification	AI named entity recognition models which identify PII based on the text content, offering the best PII identification accuracy available on the market.
Email Control	AI for email content and attachments classification. Allows keeping track of communication that involves sensitive subjects.
Monitoring	Monitoring and recording of events related to file activities and changes to active directory AI anomaly detection.
Reporting	Widgets provide a high-level overview with the ability to drill down and conduct detailed forensic investigations. All the findings can be exported in various formats. Generates management executive reports with high-level overview of data risk posture.
File Type Support	Supports more than 50 file types (including Microsoft Office file types) including the following standard files types: pdf, doc, dot, xls, xlt, ppt, pps, docx, docm, dotm, dotx, xlsx, xlsm, xlst, xlsb, pptx, potm, potx, ppsm, pptm, ppsx, vsdm, vsdx, vstx, vss, vssm, vst, vstm, vssx, dwg, dxf, jpg, jpeg, png, mp4, jpe, bmp, wav, mov, avi, m4p, m4v, gif, tiff, tif, zip, mpp.
Internet Dependency	Staff can classify and tag documents using the same rules as when they are online with the same warnings, blocking of risky activities and help assistance to explain the reasoning for the restrictions. While the ML classification suggestions are only available when online, the pattern-based suggestions are continuously available offline as well as online.
Integration Capabilities	Out-of-the-box integration with Forcepoint Data Security and Forcepoint Enterprise DLP.
Rights Management Partner Integration	Out-of-the-box integration is available with the main RMS providers. This includes Microsoft Azure RMS, Seclore, SealPath and Ionic.
Visual Marking Customization	Visual marking and metadata is fully customizable supporting different attributes and variables.
Existing Header/Footer Management	Visual markings are flexible in terms of position. Values can be inserted in existing headers/footers or can replace old headers/footers if needed. Watermarks are also supported.
Comprehensive Reporting	Reporting does not require additional resources to be enabled on the client machine that could lead to reduction in performance. Logging is stored on a centralized server. Forcepoint Classification will provide reports on user activity, data at risk, risk scoring and risk by department.
Email Subject Marking	Fully supports subject marking on emails.
Content Checking on Embedded and Attachment Files	Fully supports content checking on embedded as well as attachment files including ZIP files.

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.

©2025 Forcepoint. Forcepoint and the FORCEPOINT logo are trademarks of Forcepoint.
All other trademarks used in this document are the property of their respective owners.
[FP-Data Classification-Brochure] 06Aug2025