Forcepoint

Solution Brief

Forcepoint Data Classification

Challenge

- Effectively classifying large volumes of diverse data is complex. Maintaining consistency across different departments can be challenging and may lead to confusion, undermining the purpose of classification.
- Without automated tools or clear guidelines, classification often results in human errors, including over-classification, which can impact business operations, create an overly complex system, and hinder effective utilization and retrieval.

Solution

- Forcepoint Data Classification accurately and efficiently classifies data to enforce security and manage regulatory compliance.
- Forcepoint Data Classification streamlines the user experience through context-aware suggestions. AI-generated classification simplifies the initial categorization process and continuously learns, enabling customization to meet specific industry needs.

Outcome

- Increase productivity through rapid and accurate classification of unstructured data.
- Reduce risk through customizable sensitivity settings and user-specific detectors.
- Streamline audits and ensure compliance with global data protection laws like GDPR, HIPAA, and CCPA. Utilize AI Mesh for auditable and explainable adherence to AI and privacy regulations, such as the AI Act in the EU.

AI transformation has evolved from digital transformation; it's how organizations harness the power of AI to streamline operations and enhance decision-making processes. However, organizations are still grappling with how to safely implement AI applications while maintaining their data's safety. One of the first steps is to classify data properly and accurately.

Data classification provides significant value to businesses by enhancing security and compliance. By properly identifying and categorizing sensitive information, organizations effectively safeguard critical data, reducing the risk of breaches and ensuring compliance with regulations like GDPR and HIPAA. This proactive approach to data security minimizes legal and financial consequences, cultivating trust with customers and stakeholders.

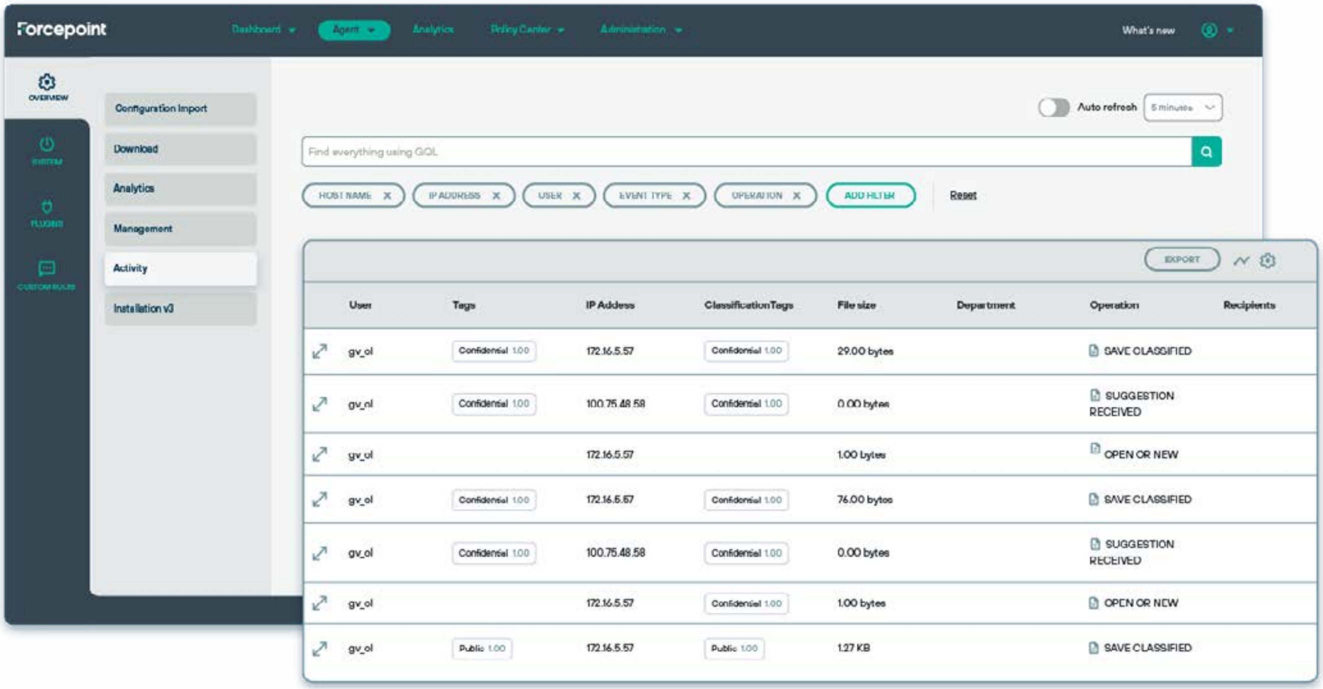
Solution Overview

Forcepoint Data Classification is engineered to classify your organization's unstructured data accurately and efficiently according to your unique requirements, ensuring that appropriate control levels are implemented and consistent data classification is enforced throughout the organization. Rather than using traditional pattern matching (regular expressions) and dictionary lookup methods, its networked AI architecture leverages a GenAI SLM and advanced data and AI components, enabling it to understand the context of a document and thereby increasing accuracy. Customizable and efficient, it ensures rapid classification without extensive training, improving trust and compliance.

Forcepoint Data Classification delivers a streamlined user experience through context-aware suggestions powered by networked AI architecture. Users benefit from AI-generated classifications that simplify the initial categorization process and can be easily reviewed and adjusted for improved accuracy and security efficacy. Its classification tags can be used by Forcepoint ONE Data Security (Cloud DLP) and Forcepoint Enterprise DLP (on-prem DLP) to make data security operations more efficient, streamlined and compliant.

Key Benefits:

- → **Increase Productivity:** Harness the industry's first AI Mesh technology to accurately and efficiently determine how data should be classified, dramatically increasing data classification accuracy. This is achieved through pre-trained models tailored to multiple vertical industries and compliance regulations.
- → **Reduce Cost:** Optimized resource allocation and reduced false positives mitigate the risk of data-related incidents, cutting down on costs. Achieve accuracy without extensive ML training, thereby reducing maintenance costs.
- → **Reduce Risk:** Rapidly and accurately classify unstructured data and ensure proper data controls and measures are implemented. Customize sensitivity settings and utilize user-specific detectors to mitigate potential data security threats.
- → **Streamline Compliance:** Avoid non-compliance fines with out-of-the-box key regulations and the broadest coverage of data types in the industry. Seamless integration with a wide array of apps, including Microsoft 365, enables effortless deployment without needing user training.



Auto refresh 5 minutes

Find everything using GQL

	User	Tags	IP Address	ClassificationTags	File size	Department	Operation	Recipients
↗	gv_ol	Confidential 1.00	172.16.5.57	Confidential 1.00	29.00 bytes		SAVE CLASSIFIED	
↗	gv_ol	Confidential 1.00	100.75.48.58	Confidential 1.00	0.00 bytes		SUGGESTION RECEIVED	
↗	gv_ol		172.16.5.57		1.00 bytes		OPEN OR NEW	
↗	gv_ol	Confidential 1.00	172.16.5.57	Confidential 1.00	76.00 bytes		SAVE CLASSIFIED	
↗	gv_ol	Confidential 1.00	100.75.48.58	Confidential 1.00	0.00 bytes		SUGGESTION RECEIVED	
↗	gv_ol		172.16.5.57	Confidential 1.00	1.00 bytes		OPEN OR NEW	
↗	gv_ol	Public 1.00	172.16.5.57	Public 1.00	1.27 KB		SAVE CLASSIFIED	

Forcepoint Data Classification Enables Your Organization to:

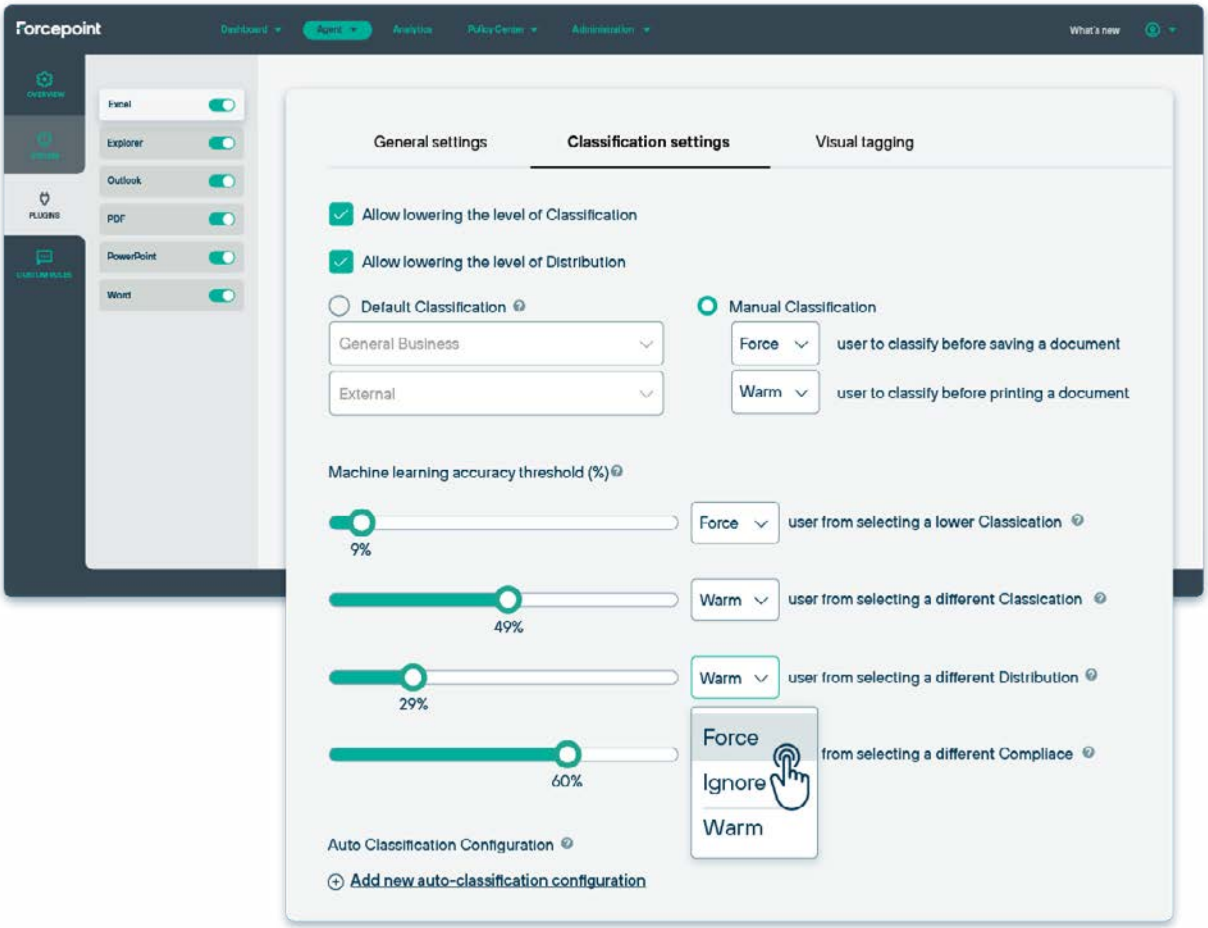
→ **Safely Use GenAI Applications:** Increase user productivity with GenAI apps such as Chat GPT Enterprise and Microsoft Copilot while enforcing DLP policies through accurate data classification and categorizing.

→ **Comply With Regulatory Mandates:** Navigate the complex landscape of global data protection laws and regulations with ease. Automate the identification and categorization of sensitive data to ensure your organization complies with data protection laws such as GDPR, HIPAA and CCPA. Reduce the risk of human error and avoid fines and penalties for non-compliance by accurately classifying vast amounts of data.

→ **Reduce Data Risks:** By accurately classifying data based on sensitivity, you can ensure the proper DLP polices are enforced. Apply the appropriate security controls and access restrictions, reducing the risk of data breaches and exfiltration.

→ **Control and Manage Data Lifecycle:** Accurate data classification is a critical component of data lifecycle management, ensuring organizations implement consistent data retention and disposal policies to streamline controls. Automated data classification suggestions leverage machine learning capabilities to adapt and improve over time.

Define actions within Forcepoint ONE Data Security



Excel ●
Explorer ●
Outlook ●
PDF ●
PowerPoint ●
Word ●

☑ Allow lowering the level of Classification

☑ Allow lowering the level of Distribution

○ Default Classification
General Business
External

● Manual Classification
Force user to classify before saving a document
Warm user to classify before printing a document

Machine learning accuracy threshold (%)

9% — Force user from selecting a lower Classication

49% — Warm user from selecting a different Classication

29% — Warm user from selecting a different Distribution

60% — Force / Ignore / Warm from selecting a different Compliace

Auto Classification Configuration

⊕ Add new auto-classification configuration

Forcepoint Data Classification Types

CLASSIFICATION	PUBLIC	INTERNAL	RESTRICTED OR SENSITIVE	CONFIDENTIAL	REGULATED OR PROTECTED (OPTIONAL)
Access	No restrictions	Restricted to staff and non-employees based on their roles	Restricted to individuals with approved access and who are approved to use it	› Restricted to individuals with approved access › Distribution is strictly limited to authorized personnel only	› Restricted to only a few individual users being entitled to see or use the data › Distribution is strictly limited to authorized personnel only
Example	Marketing collateral	Internal policies and procedures	› Personal/Employee Data › Business/Financial Data	› Payrolls, salary info › Intellectual property › Detailed budgets or financial reports	› Medical research (HIPAA) › Credit card information covered by PCI-DSS rules › Academic research regulated by export controls (ITAR/EAR)

Key Features:

→ **AI Mesh-Powered Classification and ML Contextual Suggestions:** AI Mesh with GenAI SLM enables rapid and accurate classification of unstructured data, usually within milliseconds, streamlining classification processes and reducing manual effort. They enhance trust and compliance by providing customizable classification without extensive training, while simplifying user experience through context-aware suggestions developed through ML during classification.

→ **User Correction:** With user correction and automated classification of pre-defined data categories, users can easily review and adjust AI-suggested classifications for enhanced accuracy.

→ **Automated Classification of Pre-defined and Well-known Data Categories for Ease of Use:** Admins can choose between pre-defined classifications based on industry or specific business classification needs to reduce false positives/negatives.

→ **Granular Reporting:** Gain deeper insights into end-user activity and granular analytics through easy-to-read dashboards. View the top ten users by activity to ensure authorized data classification. Monitor endpoint distribution by OS to verify software updates and minimize classification vulnerabilities. Save time and increase productivity by focusing on organizational priorities, viewing incidents per day, incident type and user. Spot current trends with the latest incident data.

→ **Intuitive Administrator UI:** Expert Mode User Interface simplifies the setup process with an intuitive UI that offers comprehensive and customizable policy management control, along with user-friendly guidance through tooltips, helpful error messages and detailed documentation, thereby reducing the need for extensive training.

Key Sectors Around the World Choose Forcepoint Data Classification Because We Help Them Achieve Better Data Security Operations:

→ **Healthcare:** Healthcare organizations can ensure they remain compliant with HIPAA data regulatory requirements by accurately identifying and categorizing patient records and other sensitive information. Forcepoint Data Classification reduces the risk of data breaches and unauthorized access, protecting patient privacy and maintaining trust.

→ **Telecommunications:** In the telecommunications sector, Forcepoint Data Classification can ensure the General Data Protection Regulation (GDPR) and other data regulatory regulations are adhered to by accurately and rapidly classifying vast amounts of data. By classifying customer information based on sensitivity, telecom companies can apply appropriate data security measures to reduce risk and exfiltration.

→ **Retail:** Retail businesses operate with vast amounts of customer information such as credit card and personal data. Forcepoint Data Classification ensures proper classification to meet the Payment Card Industry Data Security Standard (PCI DSS). This ensures retailers manage their data more effectively and streamlines audits.

→ **Finance:** Operating within a highly regulated sector, financial institutions are required to adhere to many regulatory mandates such as the GDPR and USA's Sarbanes-Oxley Act (SOX). By classifying and securing customer account information and transaction details, they ensure regulatory compliance and mitigate risks that can lead to fines and penalties.

→ **Government:** Global government agencies benefit from data classification solutions by categorizing information based on sensitivity and regulatory requirements. This enhances data security, prevents unauthorized access and ensures compliance with specific standards. Automatic tagging of datasets facilitates audits and transparency in handling sensitive information. This structured approach improves operational efficiency, enabling quick retrieval and informed decision-making across departments.

Forcepoint AI Mesh Overview

Central to Forcepoint Data Classification is its classification pipeline powered by the industry's first AI Mesh. At the heart of this classification pipeline lies an artificial intelligence classification service designed to work on unstructured text. Once the text is extracted from files sourced through various connectors, it undergoes classification by diverse machine learning algorithms.

The classification process utilizes an AI Mesh – a network composed of different AI and data components.

Key Components of the AI Mesh:

→ **Small Language Model (SLM):** This GenAI model is specifically designed for data classification. Unlike general-purpose Large Language Models (LLMs), the SLM is tailored to handle data classification tasks efficiently, transforming unstructured text into salient document vectors. It is 1/10th the size of the smallest LLMs, making it far more efficient and less resource-intensive.

→ **Deep Neural Network Classifiers:** These AI technologies perform sentiment analysis to gain qualitative assessments from written text, understanding emotions, opinions and attitudes. Their compact size ensures rapid processing.

→ **Bag-of-Words Models:** A fundamental technique in Natural Language Processing, this model performs topic detection to enhance classification accuracy.

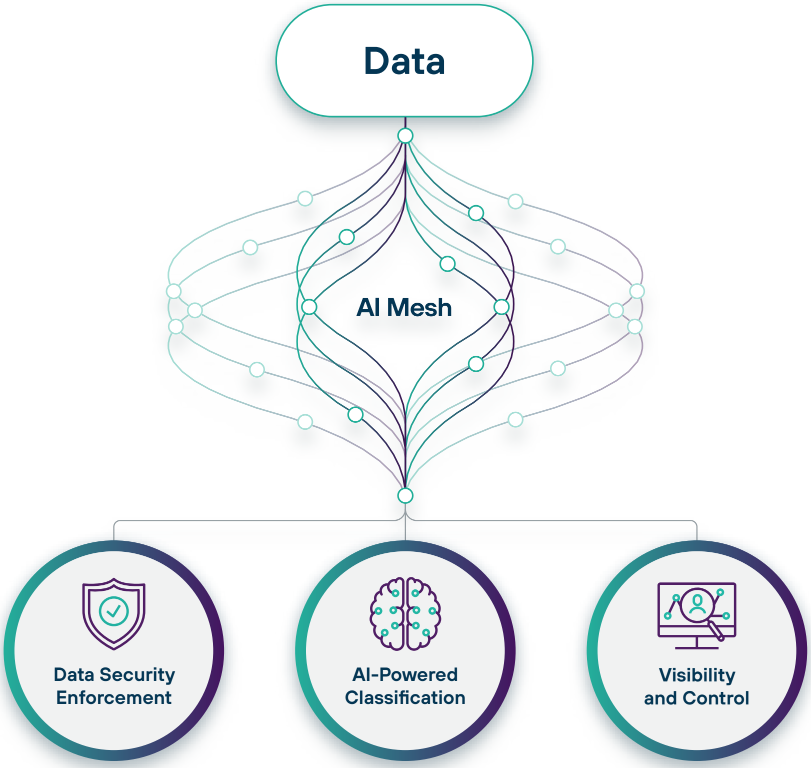
→ **Filters and Evaluators:** Utilizing regular expressions, fuzzy text searches and Python code segments, these components contribute to the mesh's effectiveness.

→ **Mapping Models:** Bayesian inference, a powerful ML and AI technique, is applied to make predictions by updating prior knowledge based on new evidence using Bayes' theorem. It combines inputs into a more refined classification conclusion.

Advantages of AI Mesh:

- **Customizable:** The AI Mesh can be tailored to meet an organization's industry needs and regulatory environments. It can also be adjusted to solve for very complex classification issues (e.g., product codes that may have the same format as government-issued IDs).
- **Efficiency and Cost-Effectiveness:** It runs efficiently on standard compute resources without requiring GPUs, providing rapid classification within 200 milliseconds.
- **Lower Maintenance:** High accuracy is achieved without extensive ongoing training, reducing maintenance costs.
- **Explainable and Trustworthy AI:** The explainability of the AI Mesh enhances trust among users and compliance with AI regulations, ensuring a highly secure data posture.

Classify Data using AI Mesh



Securing your organization's data is complex. Forcepoint simplifies the task by providing an innovative approach to data classification. Forcepoint Data Classification enables organizations to accurately and efficiently classify data using the latest AI technology, so appropriate security policies can be enforced whenever and wherever data is used, making operations more efficient and streamlining compliance.

Connect with an expert today to discover how Forcepoint can solve your specific data security challenges.

Forcepoint.com/contact