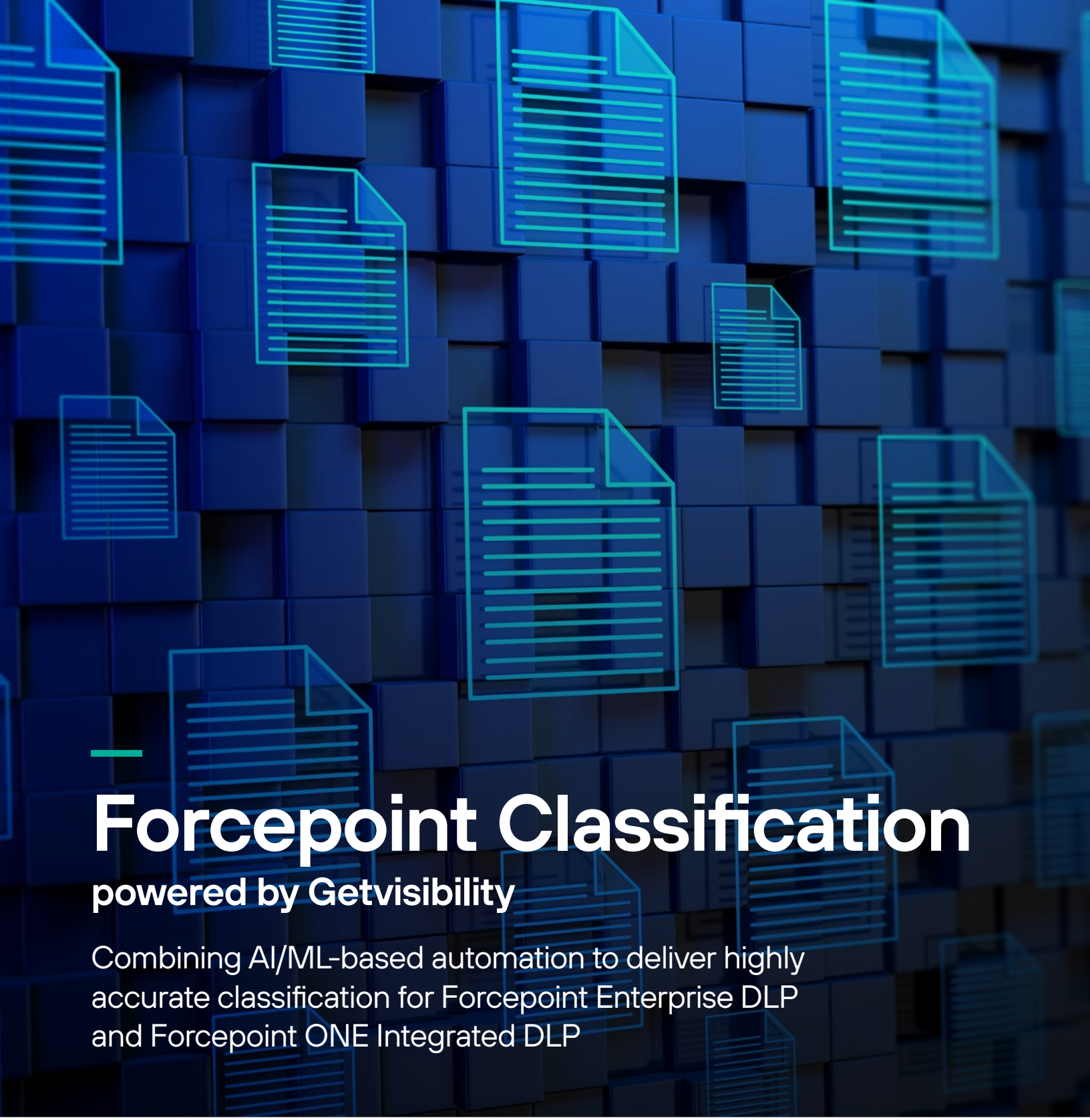


Forcepoint Classification

powered by Getvisibility

Combining AI/ML-based automation to deliver highly accurate classification for Forcepoint Enterprise DLP and Forcepoint ONE Integrated 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 or "seeing" all the types of data that they have are ultimately unable to prevent the loss of that data. However, typical classification methods are highly manual, largely depending solely on individuals to make important decisions on 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 them open to security threats from both outside (malware, ransomware) and within the organization (malicious insiders, misuse, error, mistaken classification).

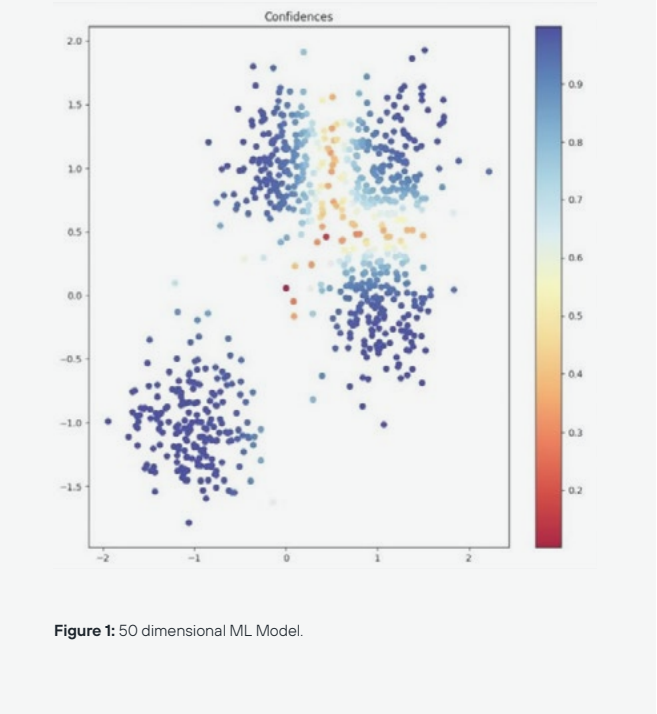


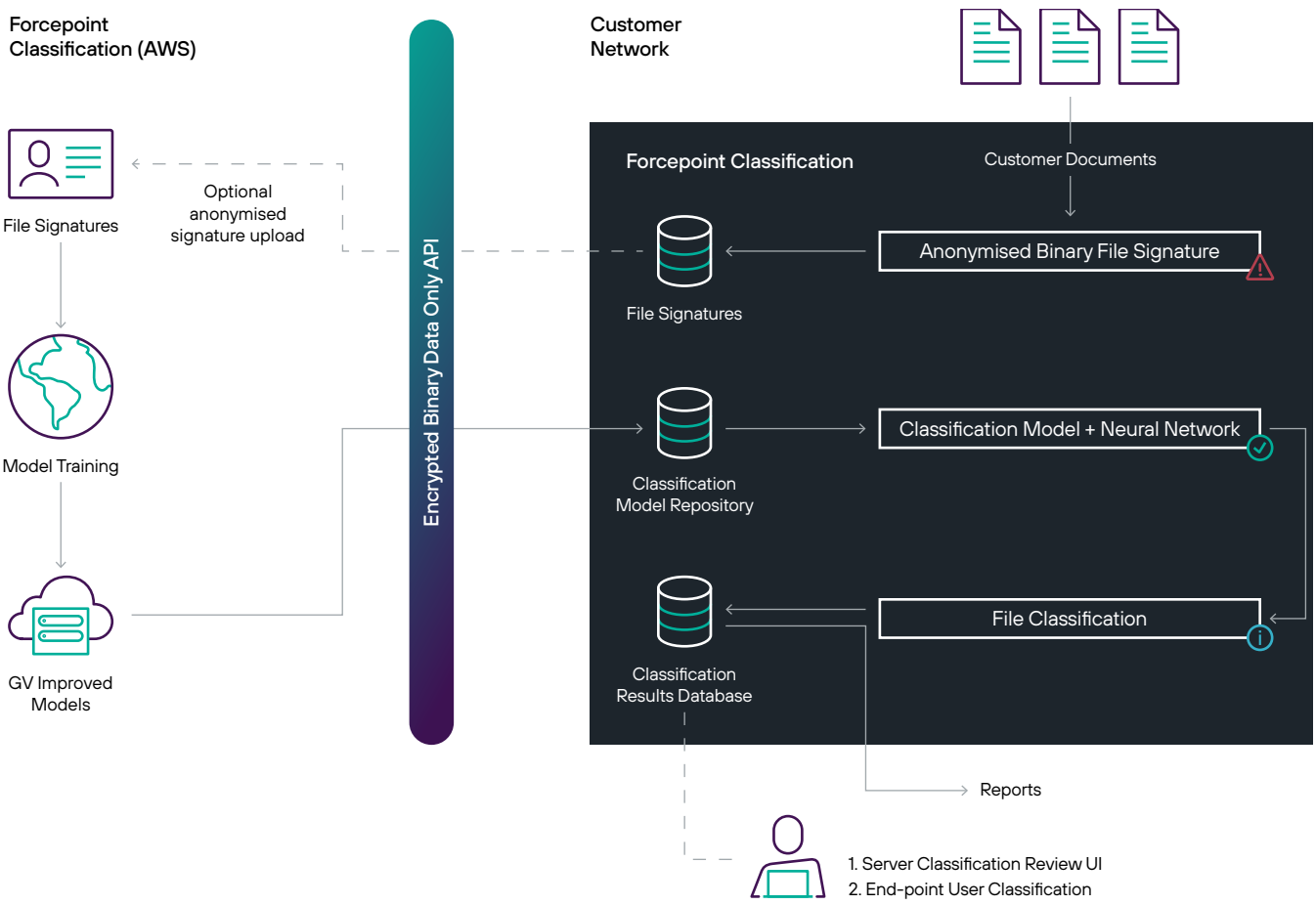
Figure 1: 50 dimensional ML Model.

Leveraging AI to Gain Sight into All of Your Data

Forcepoint is delivering a new type of classification technique that leverages the power of artificial intelligence (AI) and machine learning (ML) in order to improve data classification accuracy, automating the classification process for both structured and unstructured data types.

ML has been applied by other classification solutions in the past, but typically relies on data security professionals to train the ML-based data classifier. With Forcepoint Classification powered by Getvisibility, TensorFlow is applied to mimic neural networks which build a classification engine that is predictive and self-learning. Forcepoint Classification works with natural language to suggest classifications. Using a 50-dimensional model, customer meta-data is ingested into the model and, through continuous learning, delivers high-accuracy suggestions.

To start, thousands of newly created files and emails are classified for customers. Each file is converted into a mathematical vector with a classification label that is anonymous and not able to be reverse engineered so that the information can be securely stored. In this way, Forcepoint Classification leverages data classification from customers across various industries to build and continuously improve the 50-dimensional model. As an individual organization deploys and runs Forcepoint Classification, they are also able to maintain their own 50-dimensional model that can learn based on their unique organizational classification requirements.



During file creation, Forcepoint Classification also 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 ML 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 labelling
- Email sharing rules
- Exceptions

The outcome is Forcepoint Classification delivers "Classification Everywhere," providing on-the-fly classification of newly created data everywhere your people work. Through usage, Forcepoint Classification provides the most accurate classification available for your specific business requirements. It also requires minimal effort to deploy and superior Total Cost of Ownership.

For more information schedule a demo today.

Appendix A - Key Features:

FEATURE	OVERVIEW
Data Classification	Windows & UNIX File Servers, Windows Unix & MacOS computers, Android and iOS mobile devices, NAS, Microsoft Online, DropBox, Box, and GDrive (uses AI-based 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 risks 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, dotx, xlsx, xlsm, xlst, pptx, potm, potx, ppsm, pptm, ppsx, vsdm, vsdx, vstx, vss, vssm,vst, vstm,vssx, odt, ott, oth, odm, dwg, dxf, jpg, jpeg, png, mp4, jpe, bmp, gif, tiff, csv, txt, log and other text MIME type, psd, msg, and zip.
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 Enterprise Data Loss Prevention (DLP) and Forcepoint ONE Integrated DLP. It also is able to be used with other leading DLP solutions in the industry.
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 & 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.

[FP-Forcepoint Classification-Brochure] 06Sept2022