Forcepoint

Forcepoint Data Classification

Powered by Getvisibility

Best Practices Document

Forcepoint

Report

Forcepoint
15 July, 2024
Forcepoint Proprietary

forcepoint.com

Table of Contents

Introduction

With state-of-the-art machine learning algorithms, GetVisibility combines natural language processing with neural networks. This allows us to classify unstructured data across organizations with unparalleled accuracy and speed.

Using machine learning rather than traditional pattern matching (regular expressions) and dictionary lookup methods allows GetVisibility to understand the context of a document, thereby increasing accuracy. As the neural network does most of the work, organizations no longer must embark on the laborious and expensive task of creating rules and regex hits per department and document type. GetVisibility customisable tag set enables users to apply company-specific classification to their unstructured data, which the neural network learns with increasing accuracy. Training of the neural network can be done through our user-friendly interface, eliminating the need for the highly qualified engineers and data scientists associated with traditional methods.

The GetVisibility classification tool is built on sophisticated machine learning algorithms to enable organizations to discover, classify, and secure their most sensitive data. The GetVisibility platform combines smart agent technology and machine learning to provide a uniquely powerful solution for data classification and tagging. This is the first solution to enable automated, historical, and manual classification with one deployment. This is unique but it also has a significant value dramatically improving the quality of the manual classification process by leveraging the advanced AI model and understanding of historically created data.

Data Classification Overview

Data classification is a foundational step in cybersecurity threat management. It entails identifying what information is being processed and saved in various data systems. Additionally, it involves deciding the sensitivity of this information and the probable impact should the information confront compromise, loss, or abuse. To ensure successful threat management, organizations must aim to categorise data by working backwards in the contextual usage of their information. It must also generate a categorisation scheme that takes into consideration whether a specified use-case contributes to significant impact to a company operation (for example: if information remains confidential, must have ethics, and be accessible).

Data Classification Value

Data classification has been used for decades to help businesses make determinations for protecting sensitive or critical data with proper levels of protection. Irrespective of whether the information is stored or processed on-premises or in the cloud, data classification is a beginning point for determining the right number of controls to the confidentiality, integrity, and accessibility of information based on danger to your business. Data classification permits organizations to assess data based on sensitivity and business effect. This helps the organization evaluate risks related to various kinds of information. Each information classification level should be related to a recommended baseline set of safety controls that offer security against vulnerabilities, threats, and risks connected with the designated protection degree.

It is essential to be aware of the dangers of over classifying data. Occasionally, organizations may widely misclassify large sets of information by assigning the data with the highest or top classification level. This over-classification can incur unnecessary costs by introducing too many expensive security controls, affecting business operations. This strategy may also divert data visibility on less crucial datasets and restrict business use of their data via unnecessary compliance demands because of over classification.

Forcepoint powered by Getvisibility products

Forcepoint Data Classification is designed to help your organization classify and project your data in use, new data, and data in motion. The solution works for in-cloud and on-prem applications.

Forcepoint Data Visibility enables automated, accurate and timely legacy data discovery and classification of both new and legacy data. This solution gives organisations an overview of all their data, tailored to how they want that data to be displayed and monitored.

These products are offers contextual classification, empowering the data with appropriate metadata, and enhancing the usage of that data throughout the organization.

Components

- → Data classification levels (for example: levels, descriptions, data examples)
- → Risks
- → Data Access and Control
- → Transmission
- → Storage
- → Documented Backup and Recovery Procedures
- → Documented Data Retention Policy
- → Audit Controls

Typical levels

- → Public
- → Internal
- → Restricted or Sensitive
- → Confidential
- → Regulated or Protected (Optional)

Data Classification Typical levels

Public

Such data is available for anyone to see.

Examples:

- → Brochures
- → White paper/Public Standard

Internal

Such data is available to all staff and students.

Examples:

- → Internal correspondence
- → Committee papers and meeting minutes
- → Internal policies and procedures

Restricted or Sensitive

Accessible by restricted members of staff or students on a need-to-know basis. Often containing sensitive personal data, loss of such data results in legal action, reputational damage, or financial loss.

Examples:

- → Personal/Employee Data
- → Business/Financial Data
- → Academic/Research Information (that is: unpublished, confidential research, or funding information)

Confidential

Accessible only to designated or relevant members of staff due to its potential impact on the organization that could result in legal action, reputational damage, or financial loss.

Examples:

→ Payrolls, salaries info

→ HR personnel records

→ Credit card and financial account information

→ Internal investigation information

→ Intellectual property

→ All legal and attorney-client communications

→ Medical records

→ Detailed budgets or financial reports

Protected or Regulated

This is a special category to represent multiple regulations, for example as HIPAA or ITAR. Loss of such data results in a major legal action and a massive financial loss. Protection of such information is required by law/regulation or required by the government to self-report.

Examples:

→ Sensitive personal data (for example: physical or mental health, criminal convictions).

→ Medical Research (HIPAA).

→ Academic research regulated by Export Controls (ITAR/EAR) export-related security controls on information that is subject to a Technology Control Plan.

→ Student information classified under FERPA.

→ Credit card information covered by PCI-DSS rules.

→ Court or national security orders that prohibit disclosure (for example: subpoenas, National Security Letters).

Data Access and Control

Classification	Public	Internal	Restricted or Sensitive	Confidential	Regulated or Protected
Access	No restrictions	Only staff and non-employees based on their duties	Only designated individuals with approved access and who is entitled to use it.	Only designated individuals with approved access. Dissemination is strictly limited to authorised personnel only.	Only a few individual users being entitled to see or use the data. Dissemination is strictly limited to authorised personnel only.
Transmission	No restrictions	Information may be placed in shared folders, company managed cloud storages and sent via internal email.	Should only be shared in folders with restricted access or transmitted securely via a protected electronic messaging system (e-mail).	Should only be transmitted electronically with encrypted format and/or within a dissemination list.	Should only be transmitted electronically with encrypted format or within a dissemination list.
Storage	No restrictions	Information should be stored in shared folders and in company managed cloud storages.	Should only be held in folders with restricted access.	Information should be held only in restricted areas of the organizations network.	Information should be held only in restricted areas of the organizations network.

Data Storage Example of a Guide

Service	Public	Internal	Restricted or Sensitive	Confidential	Regulated or Protected
Default Home (Z:) Drive	✓	✓	✓	✓	✓
Confluence/Wiki	✓	✓	✓	✗	✗
Email	✓	✓	✓	✓	✓
SharePoint	✓	✓	✓	✗	✗
Full Disk Encrypted Systems	✓	✓	✓	✓	✓
Unencrypted Workstations	✓	✓	✓	✗	✗
Enterprise Office 365	✓	✓	✓	✓	✓

Data Backup

Classification	Public	Internal	Restricted or Sensitive	Confidential	Regulated or Protected
Backup	Encouraged	Encouraged	Required (should be required by an internal policy)	Required (should be required by an internal policy)	Required (required by a regulation)

Data Retention

Classification	Public	Internal	Restricted or Sensitive	Confidential	Regulated or Protected
Retention	Encouraged	Encouraged	Required (should be required by an internal policy)	Required (should be required by an internal policy)	Required (required by a regulation)

Audit Controls

Classification	Public	Internal	Restricted or Sensitive	Confidential	Regulated or Protected
Audit controls	Not required	Encouraged	An organization must actively monitor and review their systems and procedures for potential misuse and unauthorized access.	An organization must actively monitor and review their systems and procedures for potential misuse and unauthorized access.	An organization must actively monitor and review their systems and procedures for potential misuse and unauthorized access.

Sample flowchart for determining Data Classification

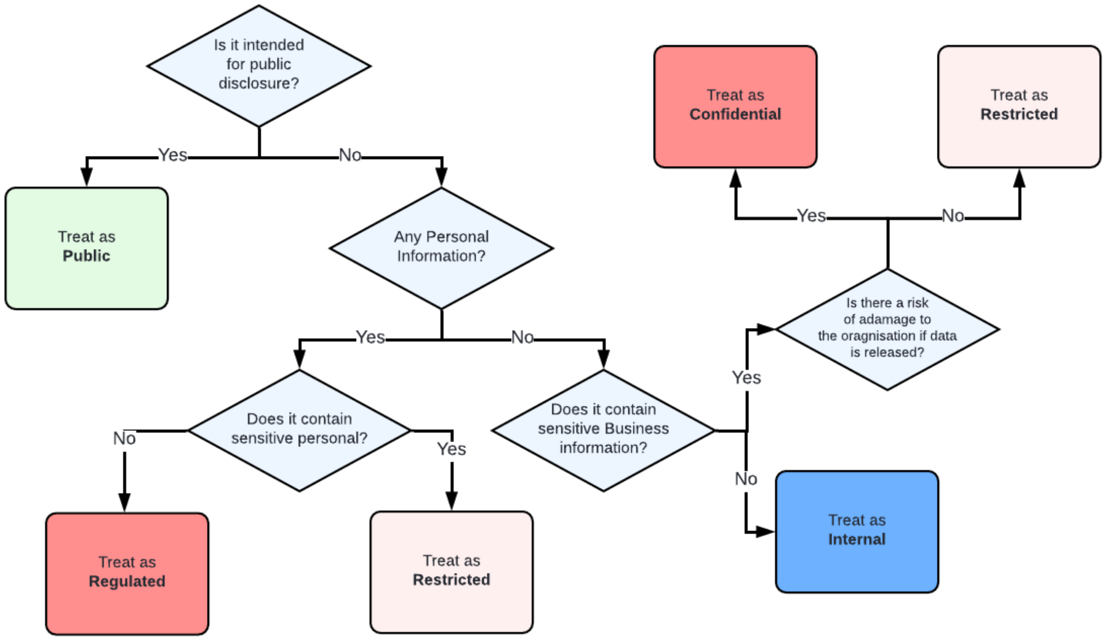
Is it intended for public disclosure?
Yes
No
Treat as **Public**
Any Personal Information?
Yes
No
Does it contain sensitive personal?
No
Yes
Treat as **Regulated**
Treat as **Restricted**
Does it contain sensitive Business information?
Yes
No
Is there a risk of adamage to the oragnisation if data is released?
Yes
No
Treat as **Confidential**
Treat as **Restricted**
Treat as **Internal**

figure 1.

Best Practices for Configuration Wizard

1. Configure Compliance screen with the required Compliance standards:

   GetVisibility comes with out of the box compliance standards shown in the agent.

   Organizations can customize the classification options which appear on the end-user agent to align with internal policies or already implemented data loss prevention solutions.

   This is an optional feature, if you do not wish to show compliance standards in the agent, simply tick the **Disable Compliance** option.

2. Classification TAGS: Which classification tags will the end user be able to view and select?
3. Which Plugins will be active for the end-user?
4. Enforcement rule related to MS WORD, MS EXCEL, and MS POWERPOINT.

   Enforcement rules determine the necessity for end-users to classify a document before saving or printing. The enforcement options available are:

   → Enforce (or Force)

   → Warn

   → Log and Ignore

Review all available options in drop-down list (like Force, Warn, Log, and Ignore).

Keep the checkbox of **User lowers classification level of a classified document** un-checked. This will not allow the end-user to later lower the classification of the document after saving.

5. Visual Tagging and Labelling for MS WORD, MS POWERPOINT and MS EXCEL

   Visual labelling refers to the visual changes made to a document once classified. This includes customized:

   → Headers: (You can change the text to Forcepoint {classification})

   → Footers: (You can change the text to Forcepoint {classification})

   → Watermarking: (You can change the text to (<span>Forcepoint {classification}</span>))

6. Outlook Policies:

   The Data Classification will sit within the ribbon of your Microsoft Outlook application. Organizations can configure how they want this agent to work within their application, customizing enforcement rules and visual markings. There is an option **Inherit minimal classification from classified attachment**, this means for example: if an attached document is classified as Internal, the end-user may classify the email as Internal or Confidential but not as Public.

   Same as above for MS Word, Excel, and PowerPoint, we follow Enforcement and Visual tagging rule for MS Outlook now.

7. Enforcement rules

   Enforcement rules determine the necessity for end-users to classify an email before sending or printing. The enforcement options available are:

   → Enforce

   → Warn

   → Log and Ignore

8. Outlook Visual Tagging

   Visual labelling refers to the visual changes made to an email once classified. This includes customized:

   → Headers: (You can change the text to Forcepoint {classification} or anything of your choice)

   → Footers: (You can change the text to Forcepoint {classification} or anything of your choice)

9. Sharing restrictions: Configure PUBLIC emails

   → Sharing restrictions can be configured through the wizard and enforced through Outlook. Sharing rules are configured depending on the classification level of the email.

   → This enforces sharing rules for end-users, depending on the classification level of the email. These options are:

- Allow
- Warn
- Block

10. Exceptions

    This is an optional feature which allows administrators to create a whitelist of email addresses that will be exempt from the sharing restrictions enforced above. This is a useful feature in ensuring restrictions do not negatively impact daily operations, while still maintaining at least privileges approach to data sharing.

11. Configure INTERNAL Emails:

    Select the **BLOCK** option and create an exception for the internal domain under **Allowed** emails. You can add any internal domain like **forcepoint.com** or **forcegv.com.**

12. Configure CONFIDENTIAL Email

    If you select **WARN** option and create exception for Internal domains under **Allowed** emails and for non-trusted domain (like gmail.com) under blocked emails. You can add **forcepoint.com** and **forcegv.com** under allowed emails list and add **gmail.com** under blocked email list.

    The expected behaviour for this rule would be:

    Always **WARN** user when a **CONFIDENTIAL** classified email is sent out, except allow when **CONFIDENTIAL** email is sent to **forcepont.com** and **Block** when **CONFIDENTIAL** classified email is sent to **gmail.com**.

13. Click on **NEXT** and **FINISH.**
14. Now click on **RESTART** to restart the machine**.**

forcepoint.com/contact

About Forcepoint

Forcepoint is the leading user and data protection cybersecurity company, entrusted to safeguard organizations while driving digital transformation and growth. Forcepoint's humanly-attuned solutions adapt in real-time to how people interact with data, providing secure access while enabling employees to create value. Based in Austin, Texas, Forcepoint creates safe, trusted environments for thousands of customers worldwide.

[Forcepoint Data Classification Powered by Getvisibility Best Practices Document]
[Status]15 Jul. 24