Forcepoint Data Security Posture Management

Powered by Getvisibility

User Guide

Forcepoint

Report

Forcepoint
April 23, 2024

Table of Contents

Introduction

Forcepoint DSPM is an innovative software solution designed to simplify and automate the data governance and risk management process for organisations of all sizes. It delivers a comprehensive approach to data classification, policy creation, and implementation of security controls, leveraging cutting-edge technology to ensure data security and compliance with regulatory standards.

Challenges
Organisations face significant challenges when it comes to data governance. Many lack a clear starting point or a structured approach, resulting in "shelf-ware" policies that go unused or unenforced. The manual, time-consuming nature of conducting data classification workshops, generating asset inventories, and defining roles and controls leads to inefficient resource use and potential compliance risks.

- Lack of Clarity and Direction:
  - **Starting Point Confusion:** Companies often need an incomplete understanding of their data governance maturity and more insight into where to begin their data governance journey.
  - **Undefined Processes**: Organisations need a structured approach or clear methodologies to develop and maintain a data governance strategy.
- Resource Intensiveness and Inefficiency:
  - **Manual Efforts**: The reliance on manual processes for data classification, policy development, and role assignment leads to significant delays and high costs.
  - **Extended Timelines**: Tasks such as creating data asset inventories are tedious, taking weeks or even months to complete for each business unit, draining valuable time and staffing.
- Compliance and Regulatory Challenges:
  - **Complex Regulations**: Keeping up with varied and often changing regulations like GDPR, HIPAA, PCI DSS, CMMC, SAMA, Export Controls and many others from the data security and data governance standpoint is complex and proven to be not at a desired state even for mature multinational organisations.
  - **Policy Enforcement:** Even when policies exist, enforcing them consistently across departments and geographies remains a hurdle due to a lack of automated controls.
- Data Handling Inconsistencies:
  - **Variable Data Sensitivity:** Organisations struggle to establish and apply consistent data handling rules across different business units.
  - **Ineffective Control Measures**: Without a system to enforce data handling standards, sensitive information is often mishandled, leading to security breaches and non-compliance penalties.
- Lack of Engagement and Ownership:
  - **Unmanaged Data Assets:** A significant number of data assets remain without clear ownership, leading to accountability issues and increased risk exposure.
  - **Policy Awareness**: Employees often need more awareness of data governance policies, which leads to non-compliance.
- Technological Fragmentation:

- **System Disparities**: Organisations using multiple systems face challenges integrating data governance solutions, leading to fragmented and siloed data management efforts.
- **Limited Alerting and Monitoring**: Traditional methods provide limited capabilities for real-time alerting on policy violations, delaying response times and remediation efforts.

These complex challenges underscore the necessity for a comprehensive, user-friendly, and automated data governance tool like Forcepoint DSPM, which aims to equip organisations with the means to effectively manage their data governance challenges in an ever-evolving digital landscape.

How Forcepoint DSPM Helps Organisation

- **Streamlines Data Governance Processes**: Forcepoint DSPM replaces manual, error-prone methods with automated, machine learning-driven processes for gap analysis, data classification, and policy creation.
- **Improves Compliance and Reduces Risk**: Forcepoint DSPM helps organisations ensure they meet regulatory requirements and mitigate risks associated with data management by providing pre-built templates and custom policy generation.
- **Enhances User Experience**: Through its intuitive interface and real-time dashboards, Forcepoint DSPM aims to make complex data governance processes accessible to non-specialists and experts alike.
- **Integrates Seamlessly with Existing Systems**: By integrating with popular tools such as Jira and Slack, Forcepoint DSPM ensures that it augments and enhances current organisational workflows.
- **Provides Continuous Monitoring and Execution**: Forcepoint DSPM tracks policy acceptance and violations, assisting organisations in setting up and maintaining their data governance framework.
- **Enables Organisational Autonomy**: Forcepoint DSPM empowers organisations by providing them with the tools to identify unmanaged data assets, assign data owners, and enforce data security without continuous external support.

Use cases - Gap Analysis, Data Classification, and Information Handling Policy Setup

Forcepoint DSPM

The foundation of a robust data governance strategy begins with a comprehensive understanding of your organisation. Forcepoint DSPMs start with understanding organisational information, paving the way for a tailored data governance framework.

Forcepoint DSPM streamlines the collection process through a user-friendly interface that prompts representatives to input information efficiently. This interface includes forms tailored to extract all necessary details to establish a data governance framework that aligns with your organisational goals.

Compliance Hub

- Company
- Compliance Standards
- Classification Policy
- Taxonomy
- Data mapping
- Departments

The information garnered during this initial phase will serve as the foundation for subsequent steps in the Forcepoint DSPM setup process. It will help in customising the governance tools to fit your organisational needs, formulating policies that reflect your business operations, and ensuring compliance with all relevant legal and regulatory standards.

- **Company**: As users input their data in **Company**, Forcepoint DSPM's intelligent system analyses the information in real-time, offering immediate insights and recommendations tailored to your specific organisational context.

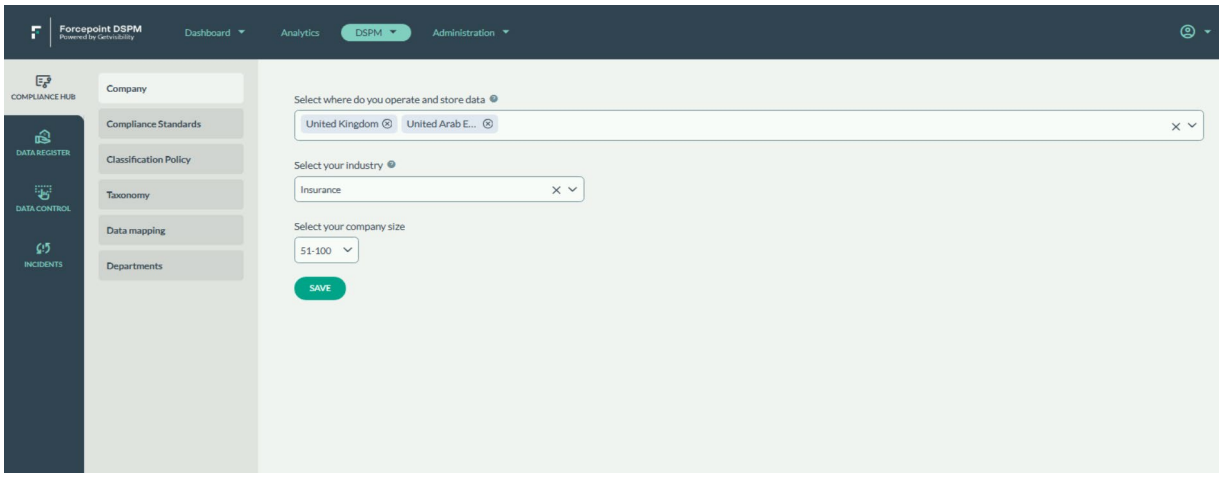

Figure 1.

- **Compliance Standards**: Based on the details provided, we can determine which **Compliance Standards** and regulatory frameworks are relevant to the customer. For instance, if a customer operates in the insurance sector within the United States, Ireland, and France, and services over 5,000 users, they would typically be subject to regulations like GDPR, HIPAA, and PCI DSS. In addition to these, we will identify and inform the customer of any other pertinent regulations that may apply to their specific situation.

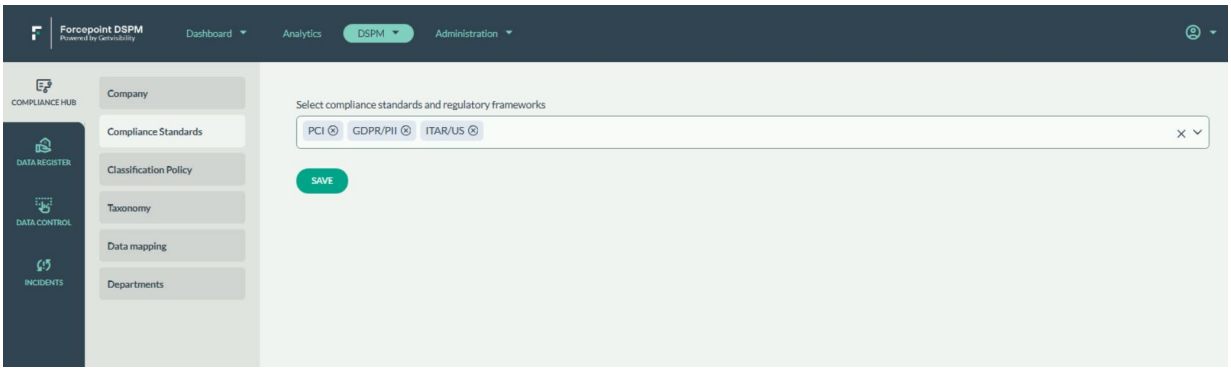

Figure 2.

- **Classification Policy**: In the event you lack an established policy, Forcepoint DSPM provides a robust policy template. This resource is designed to facilitate focused workshops for policy creation, offering a solid foundation that can be tailored to your specific needs. Alternatively, deploy our default policy to quickly meet compliance requirements with a comprehensive, ready-to-use solution.

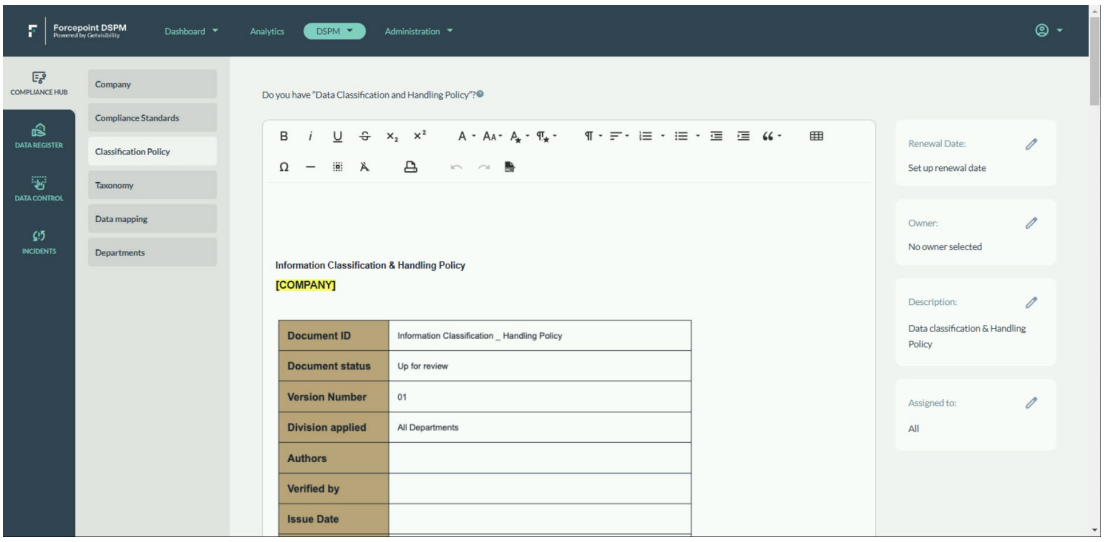

Figure 3.

Forcepoint DSPM's policy management tool enhances your data protection framework:

- **Policy Acceptance Tracking**: Instantly monitor policy engagement with a dashboard that displays acceptance rates, ensuring your team is informed and compliant.
- **Annual Review Reminders**: Keep your policies up-to-date effortlessly with automatic reminders, prompting timely reviews and maintaining policy effectiveness.
- **Audit Trail Accessibility**: Gain insight into your policy's history with an extensive audit trail that records policy amendments, user acceptances, and review dates, thereby enhancing transparency and accountability.

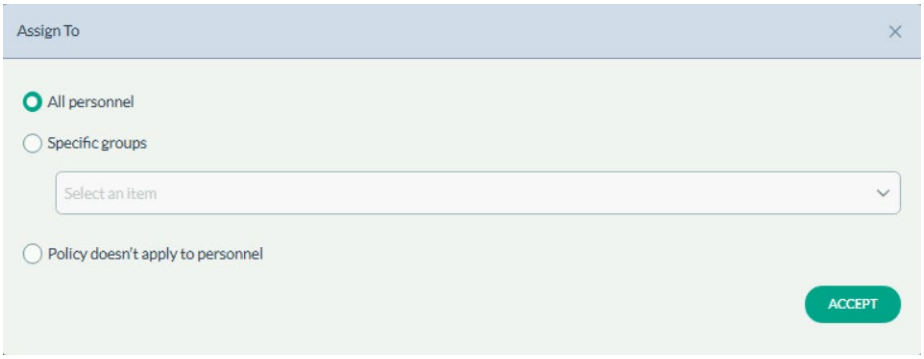

Figure 4.

- **Taxonomy**: This section allows organisations to set their classification sensitivity levels such as Public, Internal, Confidential, and Secret, among others, ensuring that data handling aligns precisely with their company's security protocols.

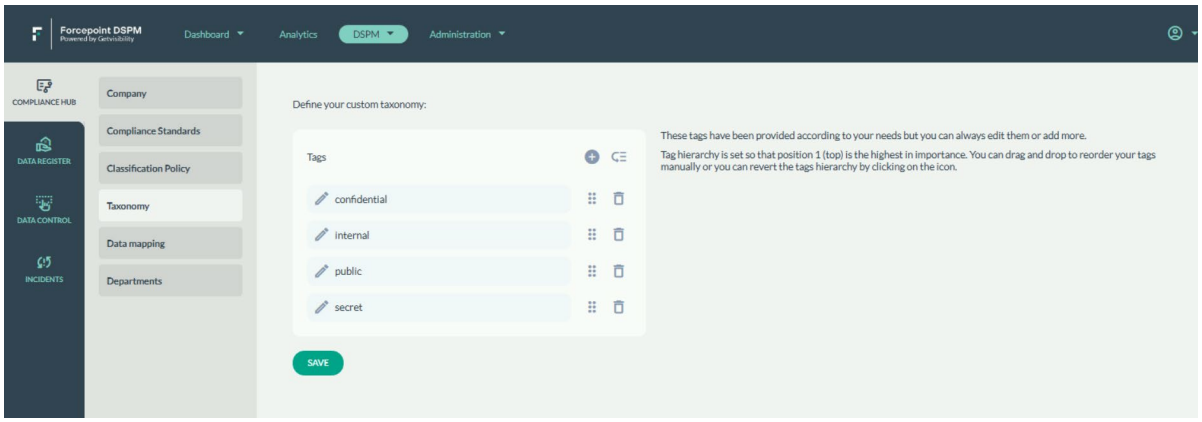

Figure 5.

- **Data mapping**

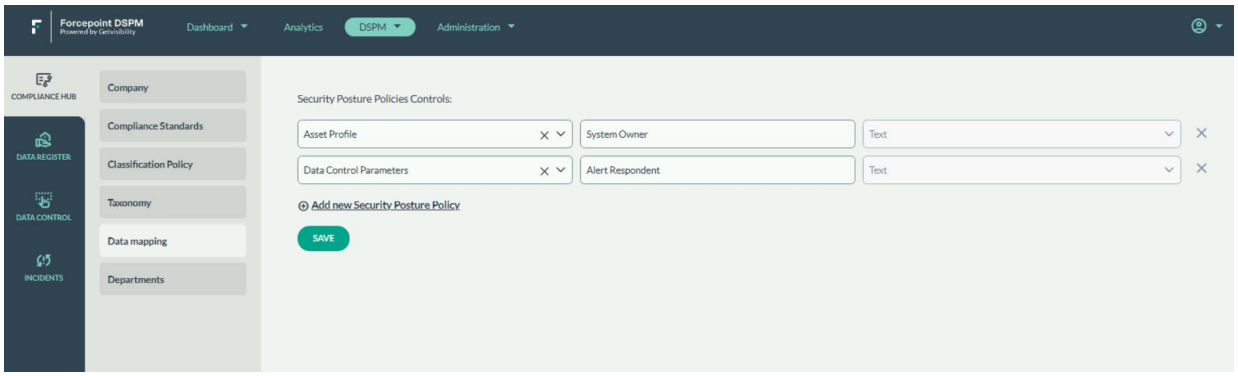

Figure 6.

- **Departments**: Defining the company's **Departments** and assigning department representatives, effectively mirroring organisational hierarchy within the system. This feature enables:
    - **Streamlined Communication**: Department heads or business unit representatives are designated as primary points of contact.
    - **Engagement with Data Governance**: These appointed individuals will receive notifications prompting them to log into Forcepoint DSPM and undertake an inventory of data assets specific to their business unit or department.

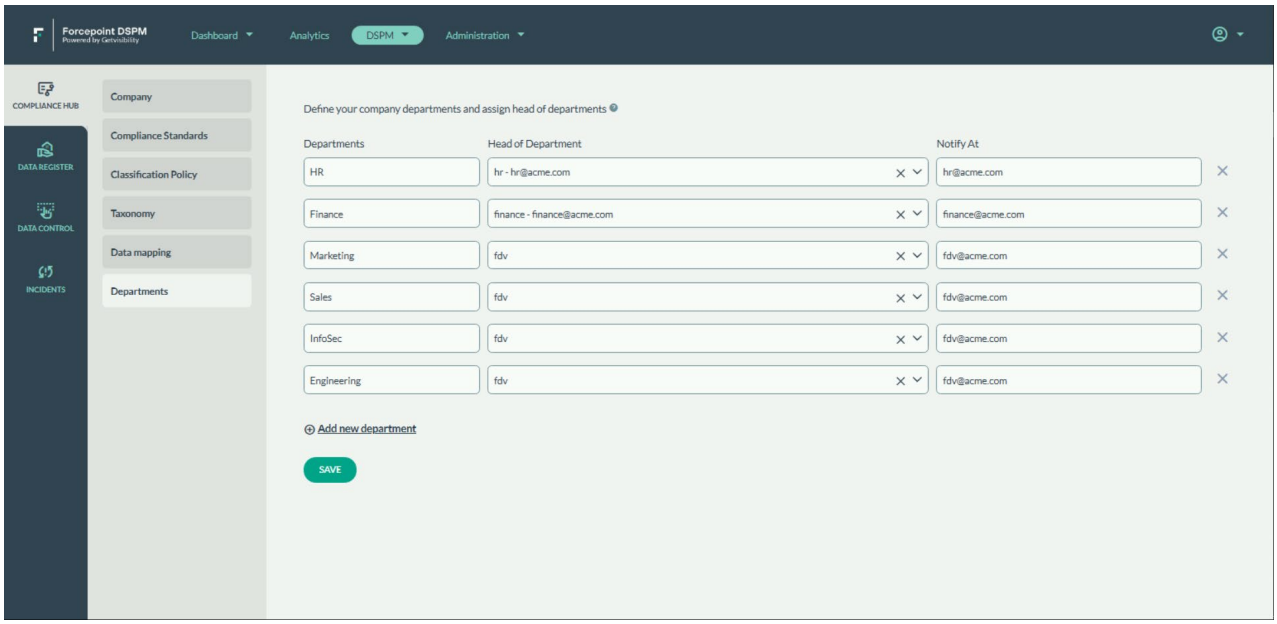

Figure 7.

Outcomes: Forcepoint DSPM ensures that data governance becomes an integrated part of business operations, with responsibilities clearly delineated along existing organisational lines. It also translates to enhanced data management as every department's key stakeholder becomes a custodian of their data, thereby building up a culture of data stewardship across the organisation. For a business unit or department representative, this means having the authority and responsibility to oversee data practices, ensuring that their segment of the organisation aligns with overall data protection and compliance standards.

Use case - Manage the organisation’s data asset inventory

Data Register

1. Security Posture Policies
2. Data Asset Inventory
3. Review Status

The data asset register is a dynamic entity, expected to evolve with your organisation's changes throughout the years. The steps provided in this interface guide you on how to correctly populate it:

- **Review the Pre-Populated List**: Start with the suggested list of data assets based on your organisational profile.
- **Edit as Necessary**: Use the provided fields and drop-down menus to make any required changes or updates to the list.
- **Assign Ownership**: For each asset, assign an owner who will be responsible for managing and updating its information.
- **Apply Security Controls**: Implement the necessary security measures for each data asset in accordance with regulatory requirements and organisational policies.

To guarantee the uniformity of data handling across various departments, Forcepoint DSPM provides:

- **Templates**: Pre-defined templates tailored to common data types and department-specific assets.
- **Examples**: Illustrative examples that demonstrate best practices for asset handling and classification.
- **Support**: In-app guidance and tooltips to assist users in making informed decisions about their data management strategies.

By using "**Security Posture Policies**" and thoroughly defining how each policy is to be managed, your organisation will enhance its security posture, promote regulatory compliance, and promote a culture of accountability in data handling. Forcepoint DSPM's systematic approach ensures that you have a robust framework for protecting your information assets.

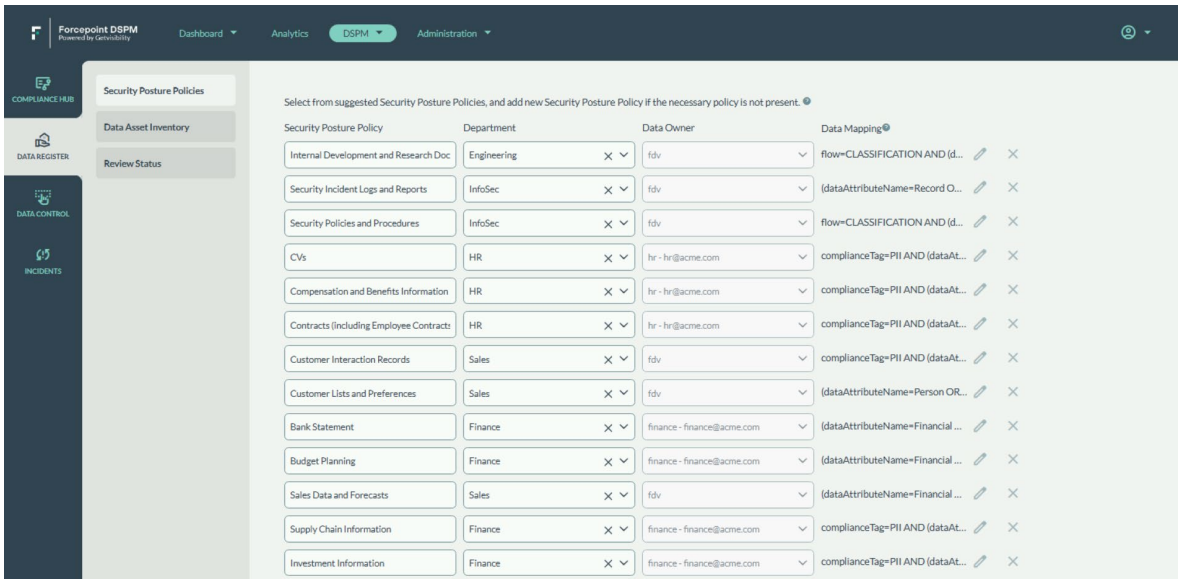

Figure 8.

Using "**Data Asset Inventory**" to assign data owners, you're not just assigning a task; you're creating a culture of accountability and proactive data governance.

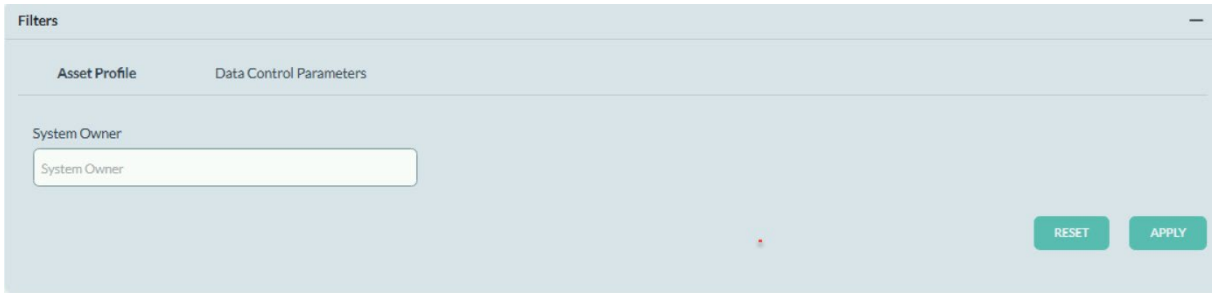

Figure 9.

Forcepoint DSPM empowers organisations to assign specific data owners to each data source, which is critical for maintaining data security and compliance. This feature helps to:

- **Identify Unmanaged Data Assets**: Quickly pinpoint data assets without an assigned owner, highlighting areas that require attention and reducing the risk of data being neglected or mismanaged.

- **Enable Targeted Alerts for Policy Violations**: Data owners receive immediate notifications if there are any policy violations regarding their assets. This ensures that the right person is informed and can take swift action to resolve the issue.

For a Chief Information Security Officer (CISO), this feature is indispensable as it ensures:

- **Accountability**: By assigning data owners, accountability for data security and compliance is clear, making it easier to enforce policies.
- **Efficiency**: Ensuring the right individual is alerted to issues reduces response times and improves the efficiency of your security operations.
- **Control**: CISOs ensured that data assets are continuously monitored and managed by designated personnel, streamlining compliance efforts.

Automated Suggestions of Data Assets

For instance, let's consider Joe, who has been identified as the Head of InfoSec during the initial steps. When Joe logs into Forcepoint DSPM, the system recognises his role and context: InfoSec department lead, with an organisation size of 5,000 users, spread across the US, Ireland, and France, in the Insurance industry, and under the jurisdiction of GDPR, HIPAA, and PCI compliance standards.

Forcepoint DSPM then provides Joe with a suggested inventory of data assets typical for his department and industry, such as security audit reports and vulnerability scan results. These suggestions are informed by benchmark data from similar organisations, allowing for a quicker and more relevant starting point.

Department-Specific Guidance

Each department within your organisation will receive a customised flow based on their role and the data types they typically handle. This personalised approach ensures that every team, from Cybersecurity to Human Resources, is equipped with relevant data asset suggestions and guided through the management process with precision. User Interaction with Suggested Data Assets

- **Agree or Disagree:** Users can review each suggested data asset and confirm its relevance to their department or flag it for removal.
- **Modify**: Any aspect of the data assets that doesn't perfectly align with the user's reality can be modified, ensuring a bespoke fit to the organisation's actual data landscape.
- **Finalise and Work**: Users can finalise their tailored list of data assets, begin working on them, and apply the necessary data governance policies and controls.

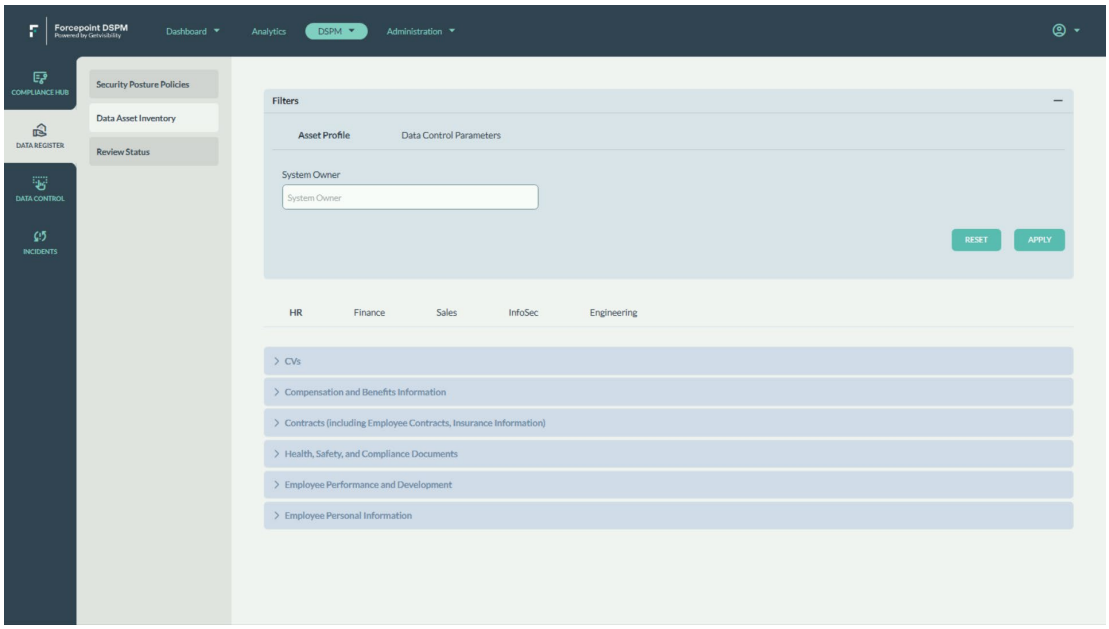

Figure 10.

After department representatives and data asset owners have detailed the handling procedures for each data asset within the Forcepoint DSPM platform, the next step is to go to **Review Status** to assign a reviewer. This stage is designed to ensure accuracy, completeness, and compliance with organisational and regulatory standards.

The review process is not merely a formality but a vital component of Forcepoint DSPM's governance capabilities. It provides an opportunity for a holistic assessment of how information assets are managed across the organisation, ensuring that:

- **Security Measures** are adequate and effectively mitigate risks.
- **Regulatory Requirements** are met, and the organisation remains compliant with relevant laws and standards.
- **Operational Efficiencies** are maintained, and data handling processes are optimised for performance without compromising security.

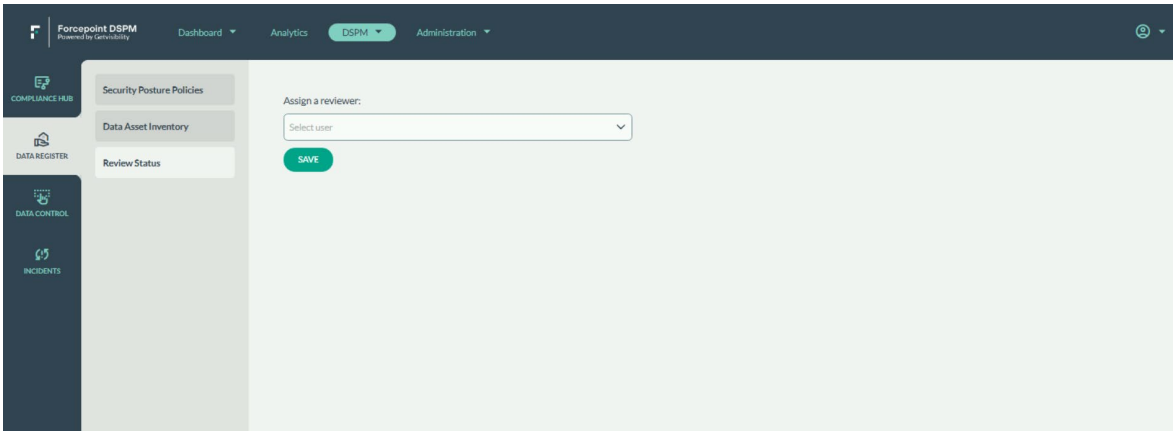

Figure 11.

Procedure for Review:

- **Submission**: Once the data handling details are inputted, users will submit their entries through Forcepoint DSPM's secure submission portal, automatically notifying the program manager or designated review authority.
- **Notification**: The program manager receives an alert indicating that a data asset handling specification is ready for review. This notification system ensures timely evaluations and maintains the workflow's momentum.
- **Evaluation**: The program manager, leveraging governance experts will carefully examine each submission. They will verify that all information is accurate, consistent with other assets, and aligned with security protocols.
- **Feedback Loop**: Should any discrepancies or areas requiring clarification emerge, the program manager will use Forcepoint DSPM's integrated communication tools to provide specific feedback directly to the responsible parties.
- **Amendments**: Department heads or data owners can then make any necessary changes promptly within the system, ensuring a dynamic and responsive review process.
- **Approval**: Once the program manager is satisfied that all criteria have been met and that the data assets are handled appropriately, they will approve the submission. This formal acceptance is logged within Forcepoint DSPM's audit trail for accountability and traceability.

Closing the Loop:

Upon the completion of the review and approval, the program manager will finalise the data asset registry, making it an official document that guides the organisation's data handling practices. Regular reviews and updates are scheduled to keep the registry current with any changes in data assets or handling requirements.

Use Case - Understand Data Controls and Incidents

Data Control

The last step of the data governance journey within Forcepoint DSPM is the conversion of detailed asset information into "Data Controls". This process converts data policies from the data assets inventory into enforceable rules that protect digital assets.

Let's consider this Scenario

John, is the CISO at ACME, is responsible for the integrity and confidentiality of vulnerability scan reports. Jane is the GRC Director, is tasked with overseeing the proper custody of these documents. The reports are stored in SharePoint under the directory "InfoSec/Vulnerability Scans" and are classified as confidential.

- Data Classification and Rule Creation:
  - John inputs the classification details of the vulnerability scan report into Forcepoint DSPM flow 2.
  - Forcepoint DSPM automatically creates a set of rules to monitor the reports based on their classification as confidential, their storage location, and the assigned access permissions.
- Real-time Monitoring and Violation Detection:
  - Forcepoint DSPM constantly scans ACME's digital environment.

    - It identifies a file named "Vulnerability_Report_Q1" stored outside the designated SharePoint folder and marked as internal instead of confidential.
- Alert and Notification:
    - Forcepoint DSPM immediately sends an alert to John and Jane through their preferred communication channels, Slack and email, respectively.
- Incident Response and Resolution:
    - John reviews the alert and collaborates with Jane to investigate the issue.
- Documentation and Compliance Tracking:
    - Forcepoint DSPM logs the incident and the steps taken for resolution in an audit trail.
    - This incident report is available for future audits to demonstrate proactive compliance efforts.

Ensuring Compliance Through Continuous Monitoring:

Forcepoint DSPM's control system operates on a continuous monitoring principle, where data assets are perpetually scanned against the established rules. This relentless vigilance:

- **Mitigates Risks** by identifying and responding to violations immediately.
- **Maintains Standards** via continuous checks to ensure that data handling remains in line with the corporate policies and regulatory mandates.
- **Enhances Data Hygiene** via regular monitoring and automated alerts that help to maintain a clean and compliant data environment.

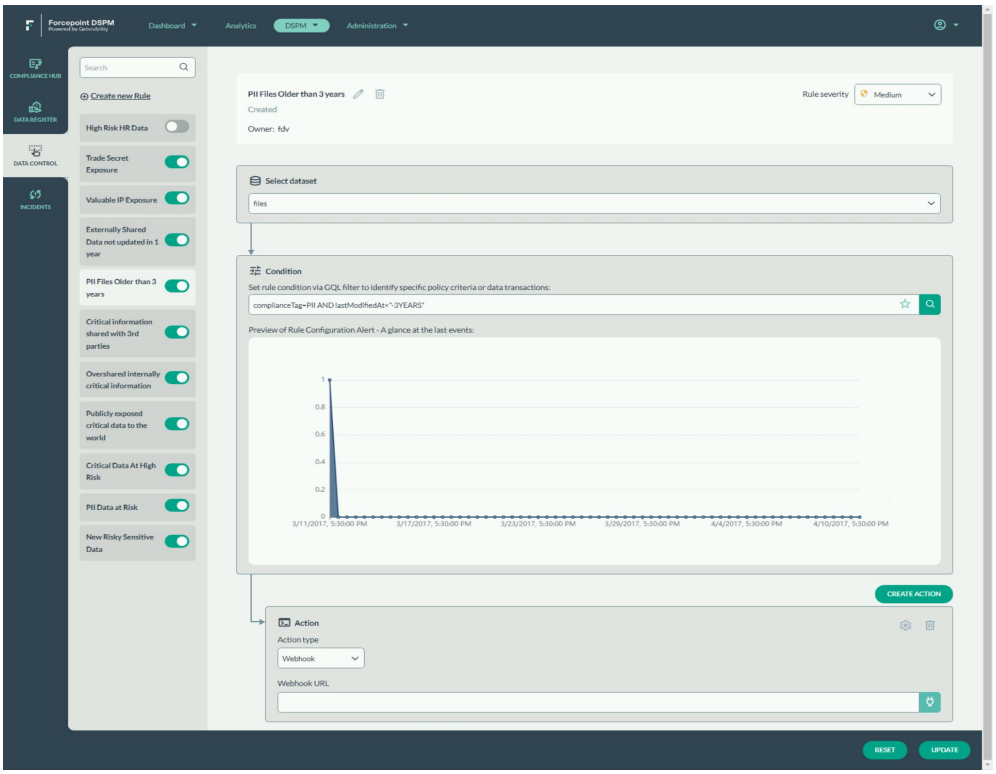

Figure 12.

Incidents

Forcepoint DSPM's incident management dashboard serves as the command centre for tracking and resolving data governance incidents.

Unified "**Incident**" Overview:

The dashboard presents a comprehensive view of all incidents, with real-time updates on:

- **Incident Details**: Clear descriptions of each incident, including the specific control violated and the data asset involved, are provided for immediate context.
- **Ticket Integration**: Integration with ticketing systems like Jira or ServiceNow and other ticketing management tools allow for seamless creation and tracking of tickets associated with each incident.
- **Resolution Tracking**: The dashboard displays the status of each ticket, from initial detection through to resolution, offering complete visibility into the remediation process.

Proactive Compliance Management:

This dynamic tracking capability enables organisations to manage their compliance with precision and agility:

- **Prioritisation**: Incidents can be sorted and prioritised based on severity, type, or other custom parameters, allowing teams to address the most critical issues first.
- **Accountability**: With each incident ticket linked to a responsible party, there is a clear line of accountability, ensuring that tasks are not overlooked.
- **Efficiency**: The streamlined interface reduces the complexity of managing multiple incidents across various systems and departments, enhancing operational efficiency.

Continuous Monitoring and Execution:

Forcepoint DSPM's monitoring system is not static; it adapts to new threats and evolving data landscapes, providing:

- **Automated Alerts**: Notifications for new incidents are dispatched immediately, reducing response times and potential exposure.
- **Actionable Insights**: The dashboard offers insights into patterns and trends, helping to inform strategic decisions and preventive measures.
- **Compliance**: At any moment, stakeholders can gauge their compliance posture, observing how the automated systems and organisational responses maintain adherence to policies and regulations.

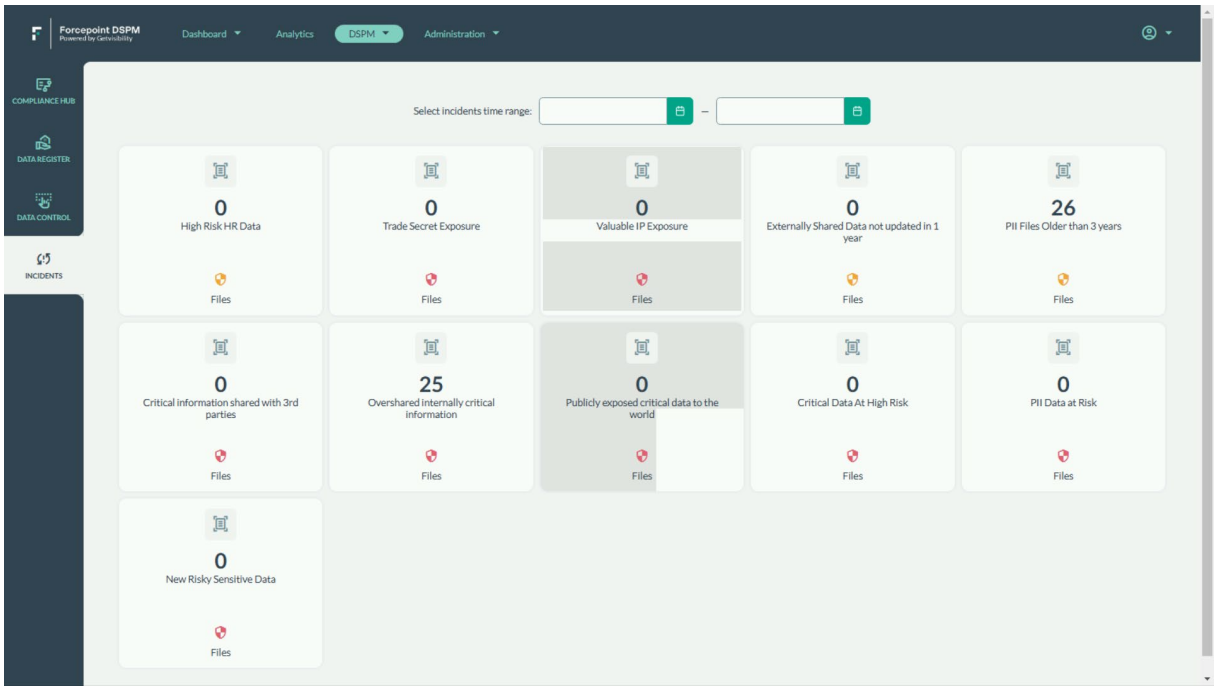

Figure 13.

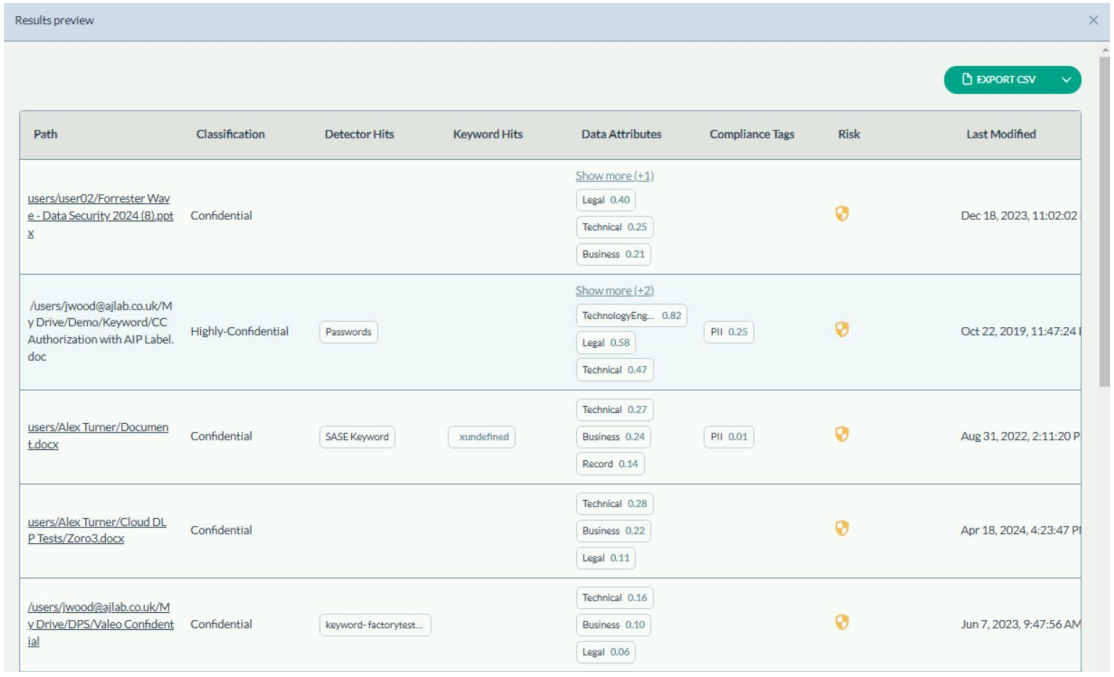

Figure 14.

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.

[Forcepoint Data Security Posture Management Powered by GetVisibility User Guide]
[Status]23 Apr. 24