Forcepoint Data Security Posture Management

v3.209.0

Release Notes

Report

Forcepoint
April 23, 2024

Table of Contents

Summary

- **Revoke Permissions**: New capability to easily revoke permissions from files, both individually and in bulk, enhancing data security.

- **Improved Data Asset Visibility**: Introduction of Data Asset, Department, and Owner columns on the File Explorer page for comprehensive oversight of sensitive company assets.

- **User Interface Enhancements**

  o Expanded row details in the sidebar UI to show up to 10 chips before collapsing, with a new tooltip for easier row expansion.

  o Moved the language selector to the top menu for more accessible and streamlined navigation.

  o Removed checkboxes from the data register and data mapping sections to simplify data handling.

- **Workflow Optimisation**: Optimised table column ordering to prioritise the most frequently used information like file paths and classifications.

- Fixed search functionality within the table widget to efficiently filter through available columns.

- **Improved Alerting**: Email alert configuration for real-time notifications about important data control activities.

Overview of New Updates

Major Enhancements for Data Security and Management

Revoke of Permission for SMB and SharePoint Online

You can elevate your data security with our new permission revocation capabilities. You can now easily revoke access rights for files in SMB and SharePoint Online, either individually or in bulk. This powerful feature, integrated with RBAC, allows for tighter control over data access, significantly improving your organisation's data risk posture.

Previously, managing permissions for files stored in SMB and SharePoint Online could be more convenient and secure, especially when needing to revoke access in bulk. This led to potential data breaches and overexposed sensitive information. Our new permission revocation feature allows you to swiftly revoke access rights for these files, either individually or in bulk, directly enhancing your data security posture. Integrated with RBAC, this functionality ensures only authorised users can manage permissions, thereby tightening control over data access.

Navigate by Trustees: Gain the ability to control access at an individual account or group level by navigating through trustees. This feature is critical for managing permissions based on user roles or specific groups, ensuring only authorised access is maintained.

Why It's Important for You

- **Before**: You might have faced challenges in quickly revoking permissions for sensitive files, potentially leading to security vulnerabilities.
  After: You can now efficiently manage access rights, significantly reducing the risk of unauthorised data access and improving compliance with data protection regulations.

Use Case & Value

- It's possible that not everyone is aware of the ability to view all files associated with a user, a feature that offers significant insight and control over data access. Discovering all files a particular user or group can access

provides a powerful tool for auditing and managing permissions effectively. Compliance officers can now regularly review and adjust permissions to sensitive files, ensuring that only relevant personnel have access. This proactive approach to data management significantly mitigates the risk of data breaches.

- With these advancements, managing user access becomes more intuitive and effective. Whether dealing with a staff departure or restricting access for an untrusted user, you can now:

- Navigate to the trustee's profile, see all associated files, and precisely revoke permissions as needed. This level of control is invaluable for maintaining strict data security and ensuring that sensitive information remains protected.

- By enabling precise control over who can see and access specific files, you can safeguard your data against unauthorised access and potential security risks. This feature is particularly useful for quickly adjusting permissions in scenarios such as staff turnovers, ensuring that access rights are always up to date and reflective of current roles and trust levels.
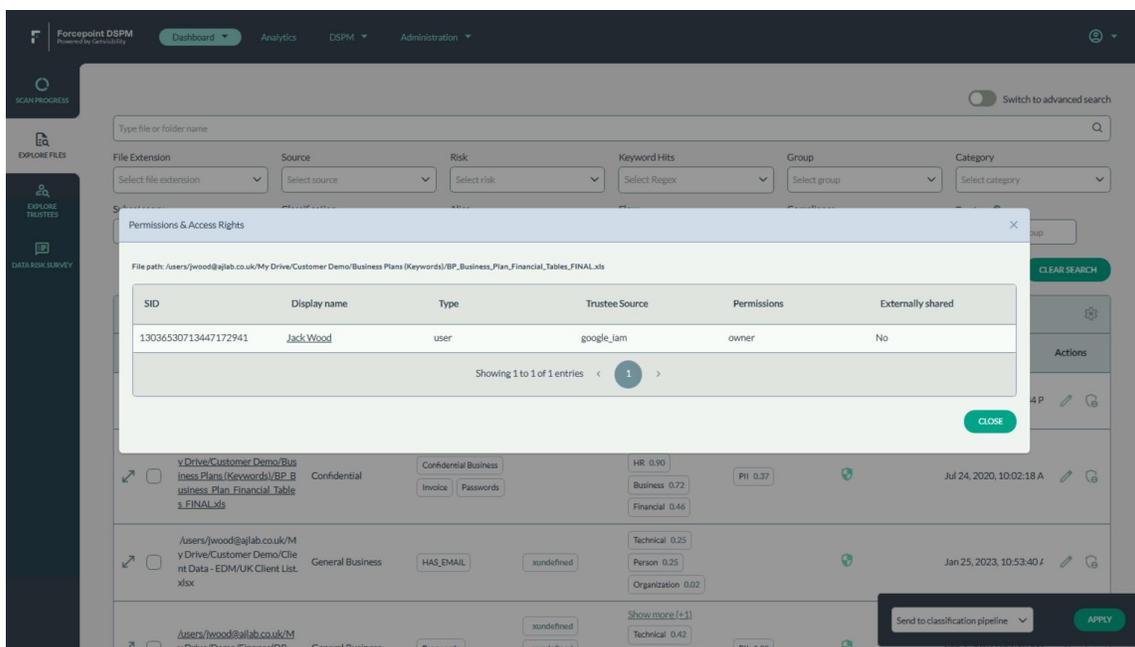

Figure 1.

Data Assets Visibility

Achieve seamless stakeholder alignment with Data Assets Visibility. This update catalyses strong stakeholder alignment and facilitates the establishment of comprehensive security policies.

By centralising the view of Data Asset, Department, and Owner information, organisations can now collaboratively identify and define what defines most sensitive business data (we call it data assets). This is the crucial step toward implementing rigorous data controls.

The Process Transforms Data Asset Management:

- **Collaborative Asset Definition**: Stakeholders define what constitutes a data asset, ensuring all parties have a unified understanding.

- **Policy Creation**: Develop tailored policies for each data asset, allowing for nuanced governance that reflects the asset's unique characteristics.

Specify where data should reside, how long we should store it, and how data should be protected.

- **Data Ownership:** Assign clear ownership to each data asset, ensuring accountability and fostering a sense of responsibility.

- **Control Implementation**: Create controls aligned with your business needs and defined data assets. We put your policies on immediate monitoring with our data controls. Once Forcepoint DSPM finds any policy violation, it will alert the right data owner.

- **Ownership Assignment**: **Risk & Gap Analysis**: Perform detailed risk and gap analyses, allowing for targeted security strategies that address specific vulnerabilities.

- **Ongoing Management**: Continually adapt and refine the controls and policies as data assets evolve and new threats emerge.

Why It's Important for You

- **Before**: Locating, classifying, and managing data assets was often disjointed, leading to inefficiencies and security oversights.

- **After**: With unified views and agreed-upon definitions, your organisation can proactively manage data assets with controls and policies that contribute to a robust security posture.

Use Case & Value: This strategic initiative enables the company to define internal policies and quickly respond to business needs and external regulatory demands. When a company defines an asset, immediate action can be taken to protect it, ensuring security measures are effective and in line with broader organisational goals.
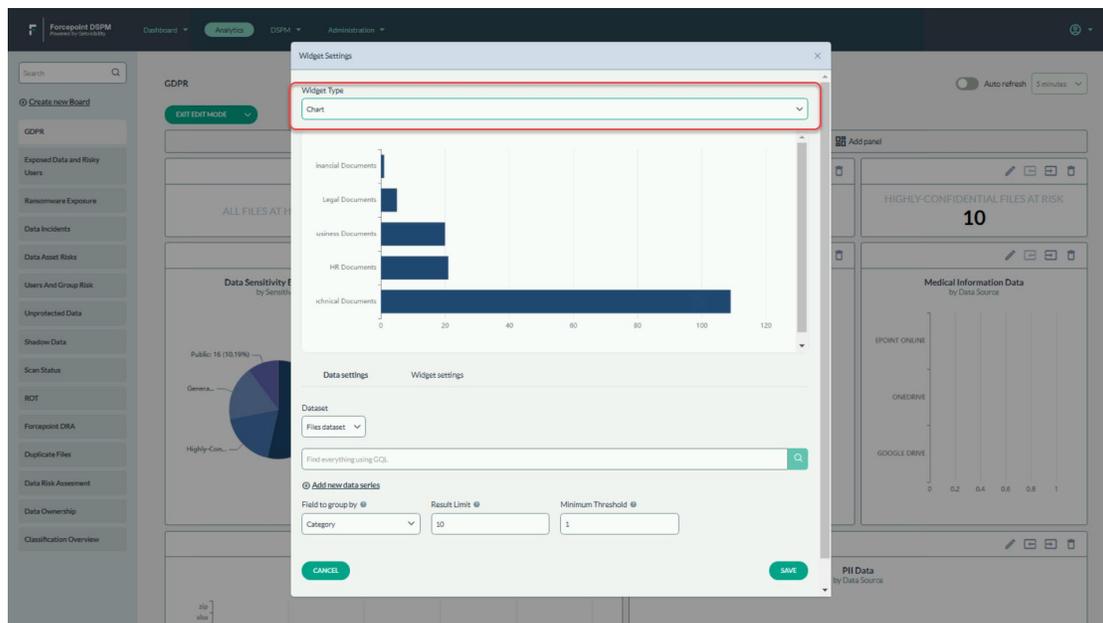
Figure 2.

Trustees Visibility: Clear Oversight on User Data Access

Gain crucial insights into individual or group access across your organisation's data landscape with our new Trustees Visibility feature. This enhancement to the Forcepoint Data Visibility platform provides a comprehensive view of all files associated with a user or group, empowering you with the means to conduct thorough access reviews and adjust permissions

accurately and efficiently. It is easy to find risky users who such as admins with an outdated password and remediate permissions.

Empowering Data Governance

- **Centralised Access Overview**: Quickly view and manage the data access of individual trustees or groups from a single, intuitive interface.

- **Simplified Trustee Management**: With just a few clicks, you can review a trustee's access to various files and make informed decisions about permission revocations or adjustments.

- **Identification of Risky Users:** We have prepared new dashboards that have prebuilt use cases for:

- Users with **Outdated passwords**

- **Inactive Admins**

- **Admins with Outdated passwords**

- **Inactive** users

Why It's Important for You

- **Before**: Gaining visibility into what files a user or group could access was a manual and scattered process, often leading to oversight gaps and potential security risks. No easy way to find inactive users, or users with outdated passwords that violated compliance policies.

- **After**: With immediate visibility into all files associated with a user, you can proactively manage data access, ensuring that only the right eyes see sensitive information.

Use Case & Value: Secure Data on Staff Changes

- In the event of staff turnover or when dealing with an untrusted user, Trustees Visibility comes to the forefront of your data security strategy.

- Navigate to a trustee's profile to see all the files they have access to.

- Revoke permissions with precision, ensuring ex-employees or risky accounts don't retain access to sensitive data.

- Maintain a high standard of data security and ensure compliance with internal policies and external regulations.

- This proactive approach is invaluable for data security officers, IT administrators, and compliance teams, providing a robust tool to quickly react to changes in staff status or to tighten security controls.

		Requiring Remediation		
OUTDATED PASSWORDS	INACTIVE ADMIN		ADMIN OUTDATED PASSWORDS	IN ACTIVE
97	7		14	3.404K

Figure 3.

New Features to Stay Informed and In Control

Email Alerting

Our new email configuration design makes it easier than ever to stay on top of essential data control activities. Enabling email notifications with just an API key and Endpoint details ensures you're always informed.

Direct, real-time notifications made staying informed about critical data control activities easier. Our new email alerting feature lets you set up email notifications easily with an API key and Endpoint details, ensuring you're always

informed of important events and actions within your data ecosystem.

Why It's Important for You

- **Before**: Important alerts and notifications could be missed, delaying response times to critical events.
- **After**: Immediate email notifications keep you informed in real-time, allowing for swift action and enhanced data control.

Use Case & Value: IT security teams can now receive alerts for unauthorised access attempts or changes to sensitive data, enabling rapid response to potential security incidents.

User Interface and Experience Improvements

Streamlined Navigation with Sidebar UI Enhancements

Access more information with fewer clicks thanks to the expanded row details in the sidebar UI, now showing up to 10 chips before collapsing. Additionally, a new tooltip makes expanding row details straightforward, enhancing your ability to analyse data quickly.

Why It's Important for You

- **Before**, Users found it cumbersome to access detailed information quickly, which impacted productivity. After, the Enhanced sidebar UI allows immediate access to detailed data asset information, improving efficiency.

Use Case & Value: Data analysts can quickly assess details of data assets without leaving their workflow, enhancing analysis speed and accuracy.

Language Selector Accessibility

Moving the language selection to the top menu enhances accessibility. It allows for quicker and more convenient language changes, ensuring that users can easily navigate the platform in their preferred language without disrupting their workflow.
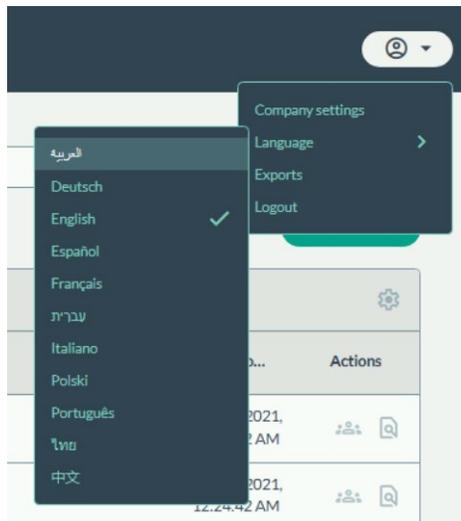

Figure 4.

Simplified Data Handling

By removing checkboxes from the data register and data mapping sections, we've simplified the user interface,

making it more intuitive and reducing confusion. This change allows users to focus on their data management tasks without unnecessary clutter or complexity.

Workflow Optimisation

Table Columns Reordering

Finding the most relevant data quickly is crucial for efficient data analysis and management. We've optimised table columns to display the most frequently used information, like file paths and classifications, at the forefront, reducing the time you spend searching for key data.
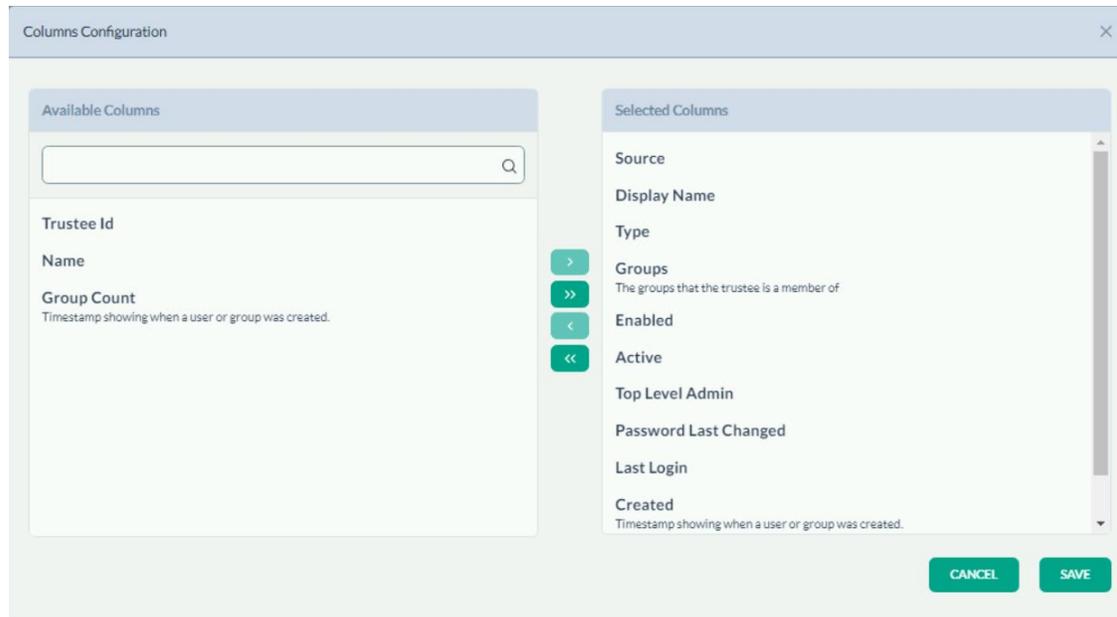
Figure 5.

Resolved Issues

- Default order for table columns now prioritises the most used information for improved navigation.

- Added a tooltip to expand row details in the Sidebar UI for enhanced user clarity.

- Added view-groups permissions to the User Management table, aligning with DSPM product requirements.

- Fixed the search functionality in the Analytics - Table widget, ensuring column search works as expected.

- Removed Beta label from Detectors, marking the official transition to General Availability.

- Set the default interval to 24 hours for the Chart widget to enhance data analysis consistency.

- Removed checkboxes on data register & data mapping sections to reduce user confusion.

- Moved language select to the top menu for better accessibility.

- Increased the default number of visible chips in row details before collapsing to improve information display.

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.