Forcepoint Data Security Posture Management

Powered by Getvisibility

Analytics

Forcepoint

Report

Forcepoint
April 23, 2024

Table of Contents

Introduction

The Analytics page and its boards showcase various metrics, charts, and graphs that detail the findings from data scans, including overexposed files, sensitive data, and data at risk.

These are critical for understanding and managing the organisation's data security and compliance posture. It identifies potential vulnerabilities, risks, and compliance issues, enabling informed decision-making to mitigate threats and enhance data protection strategies.

The primary users of the Analytics page are CISOs (Chief Information Security Officers), security analysts, data protection officers, and IT administrators who are responsible for the organisation's data security and compliance. It provides these stakeholders with a comprehensive overview of the data security health of the organisation.

The Analytics page is fully populated after Forcepoint DSPM scans have been completed but it can be accessed during scan to view live information.

The Analytics page gathers its information through the Forcepoint DSPM platform's data discovery, classification, and risk assessment processes. The platform’s connectors are set up to scan the organisation's digital environment, identifying and classifying data across systems and repositories, and evaluating the risks based on various factors such as sensitivity, exposure, and compliance requirements. This data is then aggregated, analysed, and presented on the Analytics Boards in an easily digestible format.

The Analytics page is found within the Forcepoint DSPM platform's user interface under the dedicated "Analytics" section.

The Boards

Forcepoint DSPM comes with 20 preconfigured boards out-of-the-box. Here are brief descriptions of the use cases they cover.

- **Scan Status**: The Scan Status board provides real-time insights into the progress of ongoing data scans, allowing organisations to monitor the coverage and completeness of their data discovery and security efforts.
- **Databases**: This board offers a comprehensive overview of all databases within an organisation, highlighting potential vulnerabilities and ensuring databases are properly secured and monitored.
- **High Risk Users**: Identifies users with excessive permissions or abnormal access patterns, enabling organisations to mitigate insider threats and enforce least privilege access policies.
- **Classification Overview**: Provides a snapshot of data classification across the organisation, aiding in the identification of sensitive data and ensuring compliance with data protection regulations.
- **Data Risk Assessment**: Summarises the potential risks to an organisation's data, offering actionable insights for mitigating exposure and enhancing data security posture.
- **Key Data Overview**: Highlights critical data assets within the organisation, enabling focused protection efforts on the most valuable and sensitive information.
- **Executive Data At Risk**: Targets the specific data risks associated with executive-level information, ensuring high-profile data receives adequate security measures.
- **Financial Data At Risk**: Focuses on identifying and mitigating risks associated with financial data, essential for preventing fraud and ensuring regulatory compliance.

- **HR Data At Risk**: Highlights vulnerabilities within human resources data, protecting sensitive employee information from breaches and unauthorised access.
- **Data Ownership**: Clarifies data stewardship within the organisation, promoting accountability and facilitating effective data management and security practices.
- **Unprotected Data**: Identifies data lacking adequate security controls, allowing for quick remediation and the strengthening of data protection measures.
- **Data Compression Schedules**: Provides insights into data compression activities, optimising storage utilisation and enhancing data management efficiency.
- **Shadow Data**: Reveals unmanaged or unknown data residing outside of controlled environments, reducing risks associated with data sprawl and exposure.
- **ROT Data**: Identifies redundant, obsolete, or trivial (ROT) data that clutters systems and poses unnecessary risk, enabling effective data clean-up and policy enforcement.
- **Data Incidents**: Summarises past and present data security incidents, providing insights from past incidents and enhancing organisational resilience against future threats.
- **Ransomware Exposure**: Evaluates the organisation's vulnerability to ransomware attacks, facilitating proactive measures to protect critical data assets.
- **Agent Management**: Monitors the status and health of deployed security agents across the organisation's endpoints, ensuring comprehensive data protection coverage.
- **Duplicate Files**: Identifies and addresses issues of data redundancy, improving storage efficiency and data management practices.
- **Catalogued Files**: Offers a detailed inventory of all catalogued files. These are files that have not passed through the ML pipeline. This helps identify any data issues.
- **Endpoint Risk Management**: Provides a comprehensive view of endpoint security, enabling organisations to identify and mitigate risks associated with user endpoint data.

While the default boards provide excellent coverage for the most frequent data security and compliance use cases, it can be beneficial to edit some of the input parameters to suit some specific customer requirements.

The interface for editing the boards' widgets is designed for ease of use, incorporating GQL (Getvisibility Query Language) and graphical elements.

GQL Quick Guide

Basics:

- GQL: Query language for Forcepoint DSPM platform
- Based on: Apache Lucene
- Supports: Boolean, term, range queries
- Use: For custom queries without hard coding

Querying:

- Choose terms from specific dataset: Files, Trustees, Activity, Management
- Apply operations like AND, OR =, !=, >, <, >=, <= to filter data
- Form queries, e.g., `flow=classification AND risk>=1`.

Examples:

- Simple: `dataAttributeName=HR`
- Complex: `complianceTag=PII AND dataAttributeName=HR AND (dataAttributeName=Record OR dataAttributeName=Legal) AND (detectorHits="Health Insurance" OR detectorHits="Compliance report")`

Aggregation (Analytics):

- Use in widgets for counters, charts, maps.
- Aggregate terms for complex visualisations.

Editing Widgets Graphically

There are several widgets available and each of them have their own unique customisation options.

Counter

The widget's design aims to provide a customisable and at-a-glance view of specific data metrics, which can be particularly useful for quickly accessing the volume of data that matches certain criteria, such as sensitive files or risk levels.

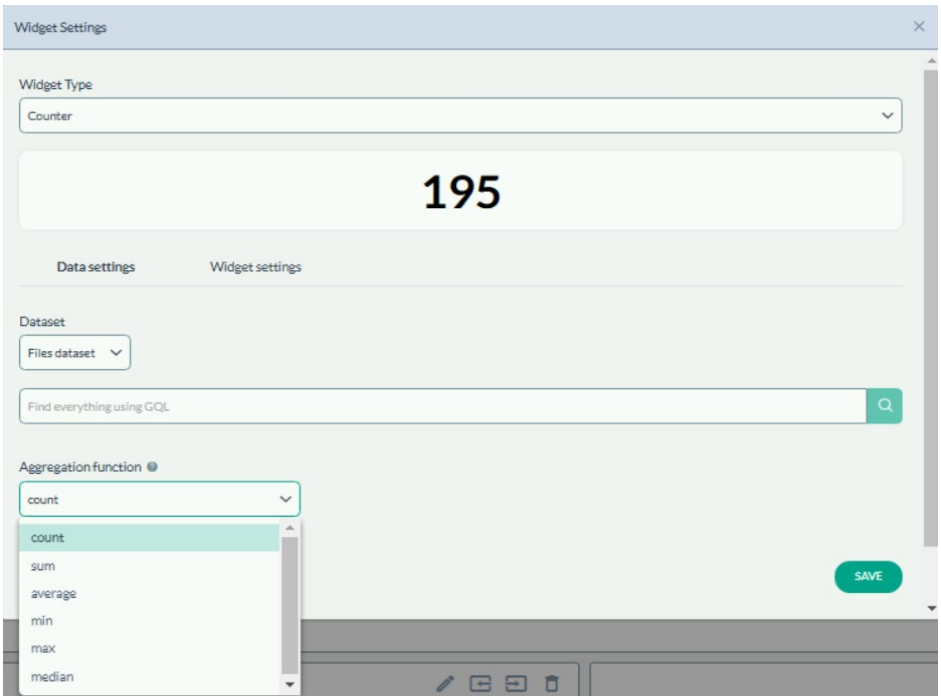

Figure 1.

Users can choose the dataset they wish to count from, like files, trustees, or agent activities. They can also employ GQL to refine their search and set the aggregation function (e.g., count, sum, average).

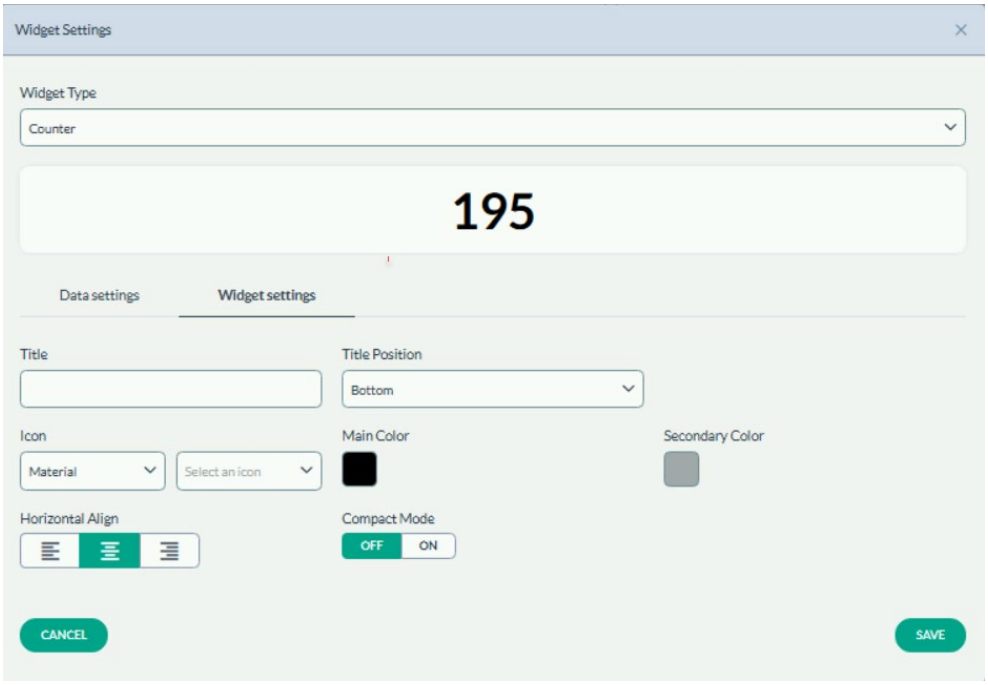

Figure 2.

This section allows users to add a descriptive title, position it, accordingly, select an icon to represent the data

visually, and choose primary and secondary colours for the widget's theme. Users can also toggle the compact mode to change the widget's display size.

Chart

These widgets are designed to help users tailor the display of data analytics to their preferences for better interpretation and presentation of data insights. They can have multiple types: Horizontal Bar, Vertical Bar, Line, Ares, or Pie.

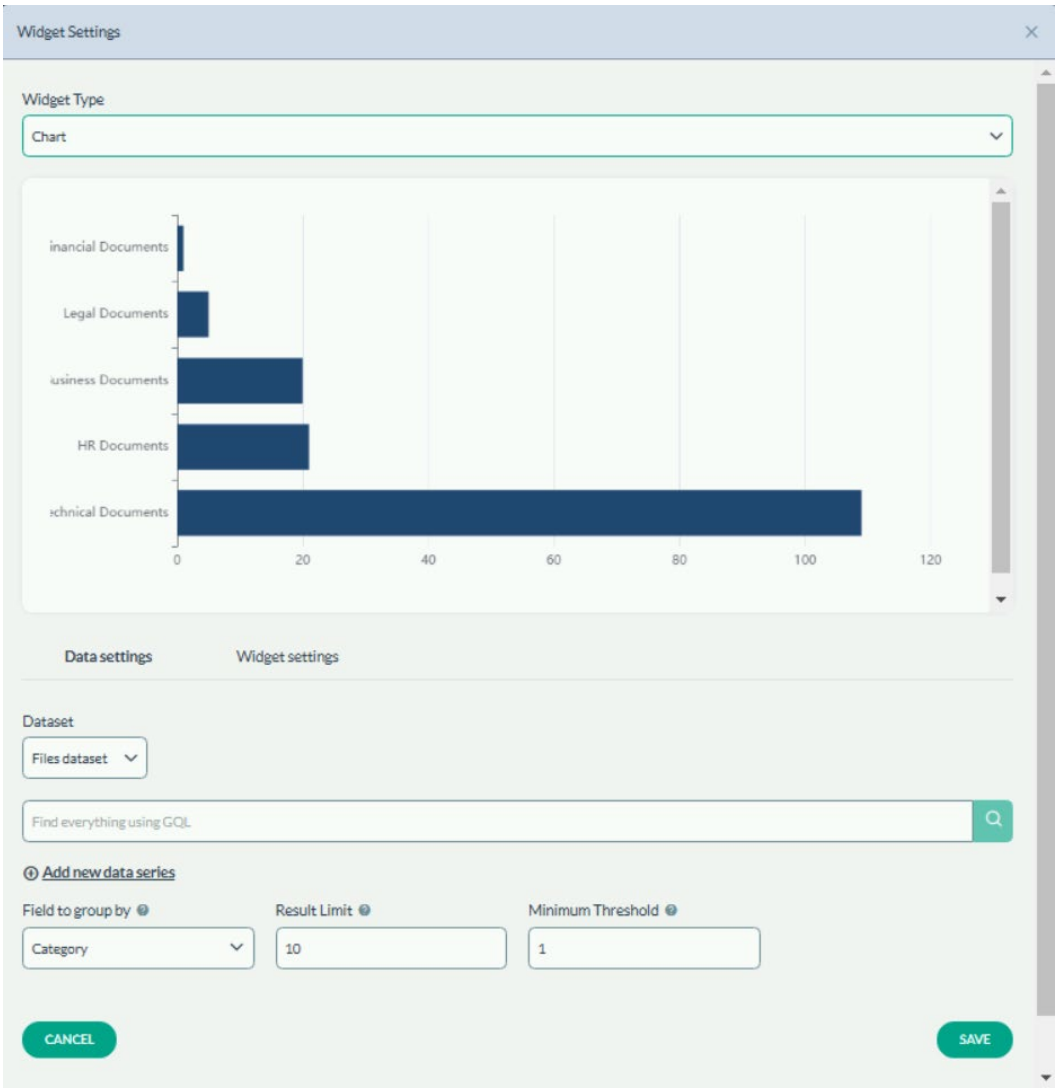

Figure 3.

This tab allows users to select the type of dataset to visualise (e.g., files or trustees) and use GQL for specific queries. The 'Field to group by' feature is used to categorise data, with adjustable limits on the results displayed and thresholds for inclusion in the visualisation.

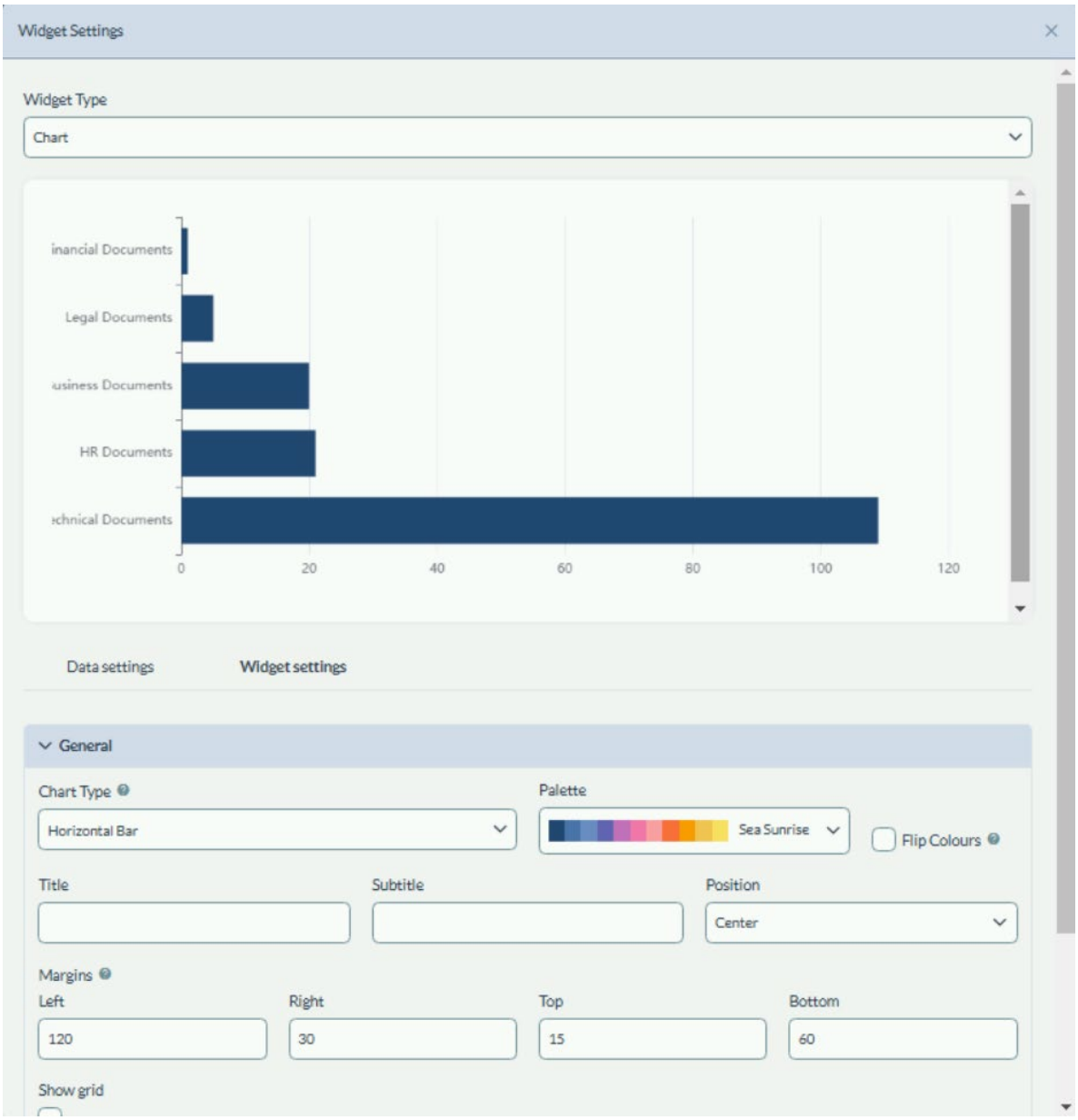

Figure 4.

Users can adjust general settings like chart type, add a title, adjust margins for clarity, and choose a colour palette for the chart. Options for additional customisations such as enabling grid lines or flipping colours for visual differentiation are also present.

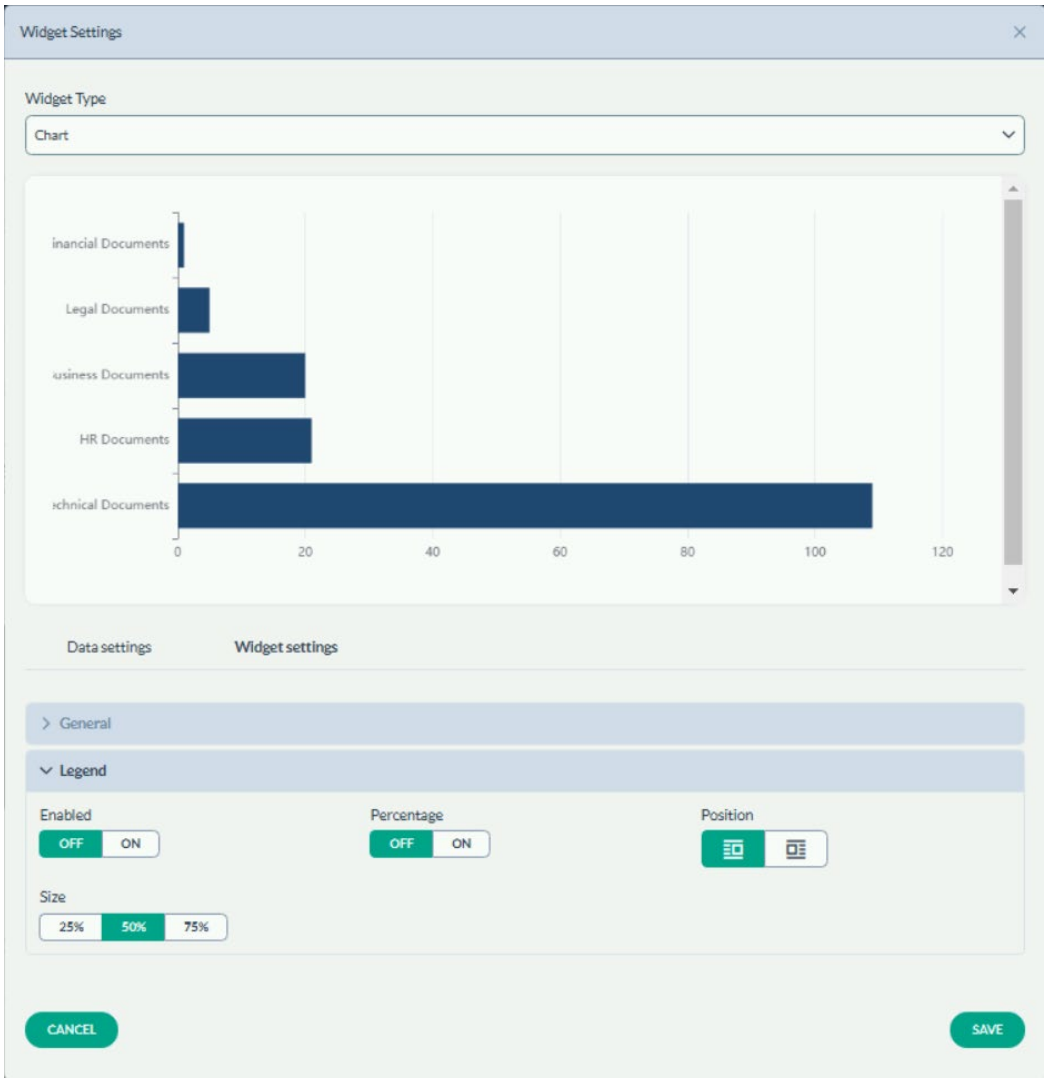

Figure 5.

The Legend section has toggles for enabling a legend display and showing percentages, with adjustments for size and positioning on the chart.

Map

The map widget is an interactive element that displays geographical data. It is configurable to show specific information based on user-defined criteria. Geographic location can be added during scan set up and is crucial in discovering data sovereignty violations.

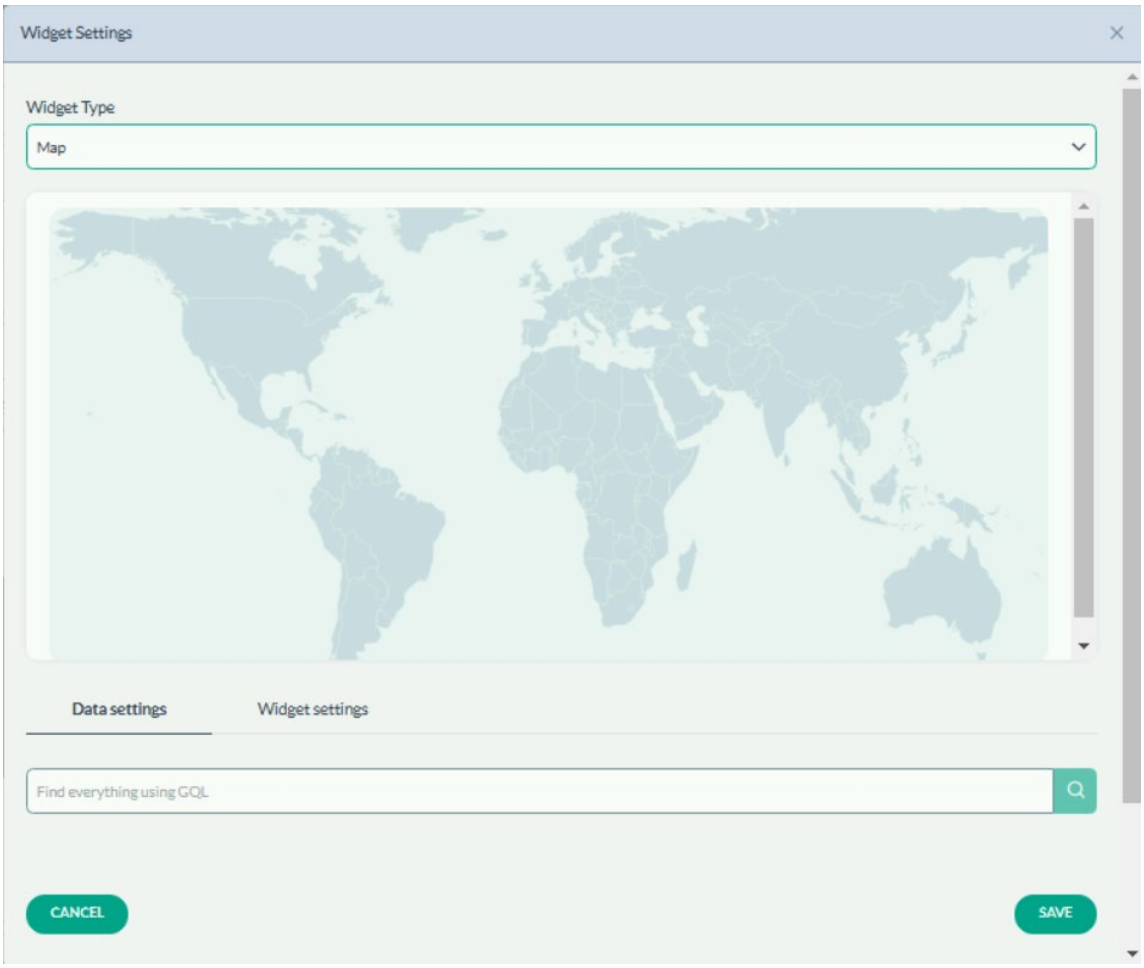

Figure 6.

This interface allows you to use GQL to query and filter the data that will be displayed on the map. Enter your query in the search bar and click "SAVE" to apply the filters or "CANCEL" to exit without making changes.

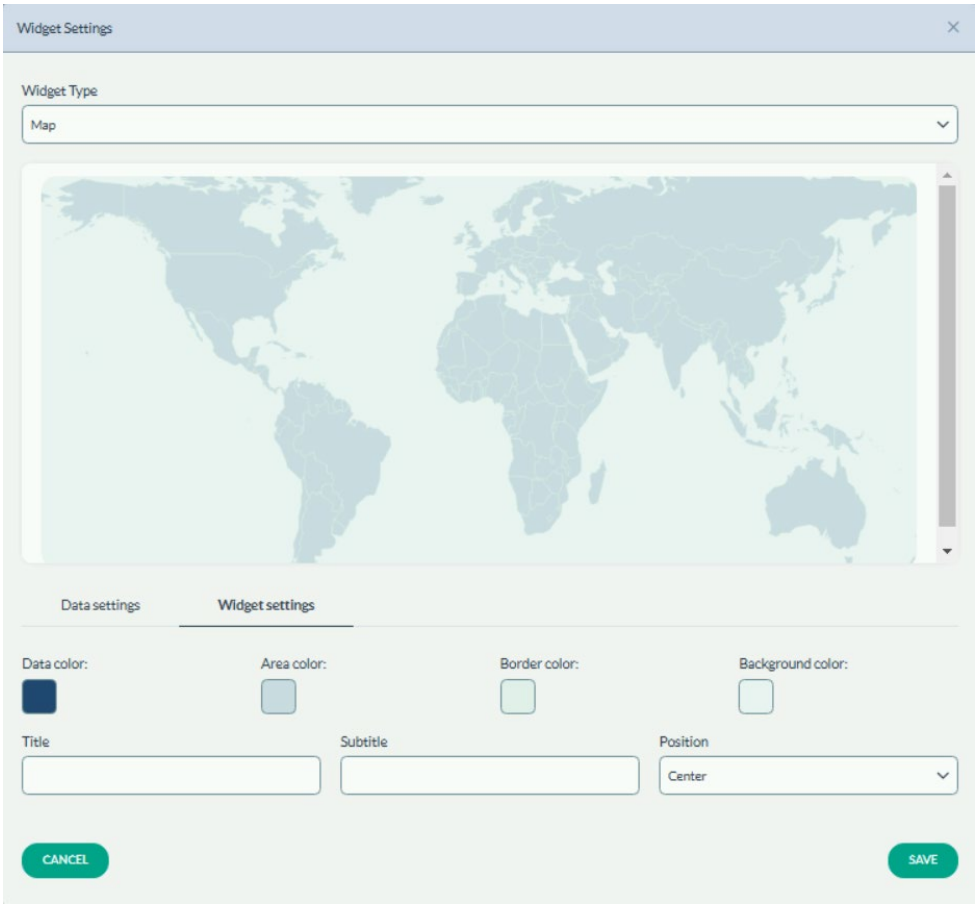

Figure 7.

Here, you can customise the map's appearance. Adjust the data, area, border, and background colours using the colour selection tools, and add a title or subtitle as needed.

Text

The text widget allows for rich text creation and editing. Users can format the text with the various styling options provided.

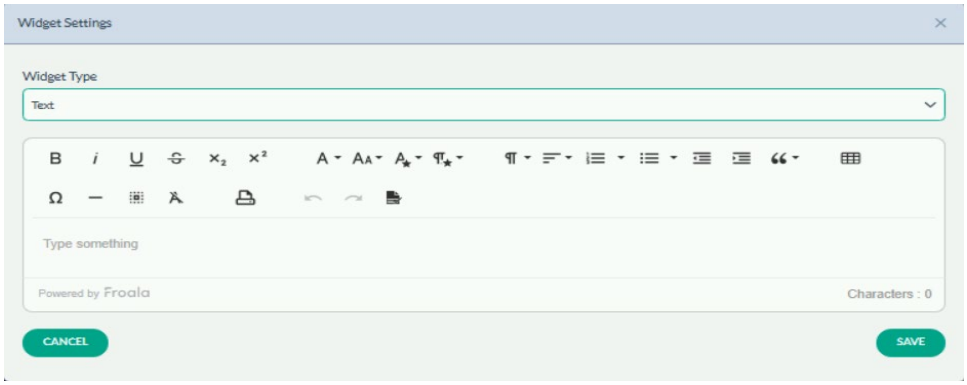

Figure 8.

The toolbar has options like bold, italic, underline, subscript, superscript, and various list, and alignment tools. Users can enter and format their text in the area below the toolbar.

Table

The table widget displays data in a structured format.

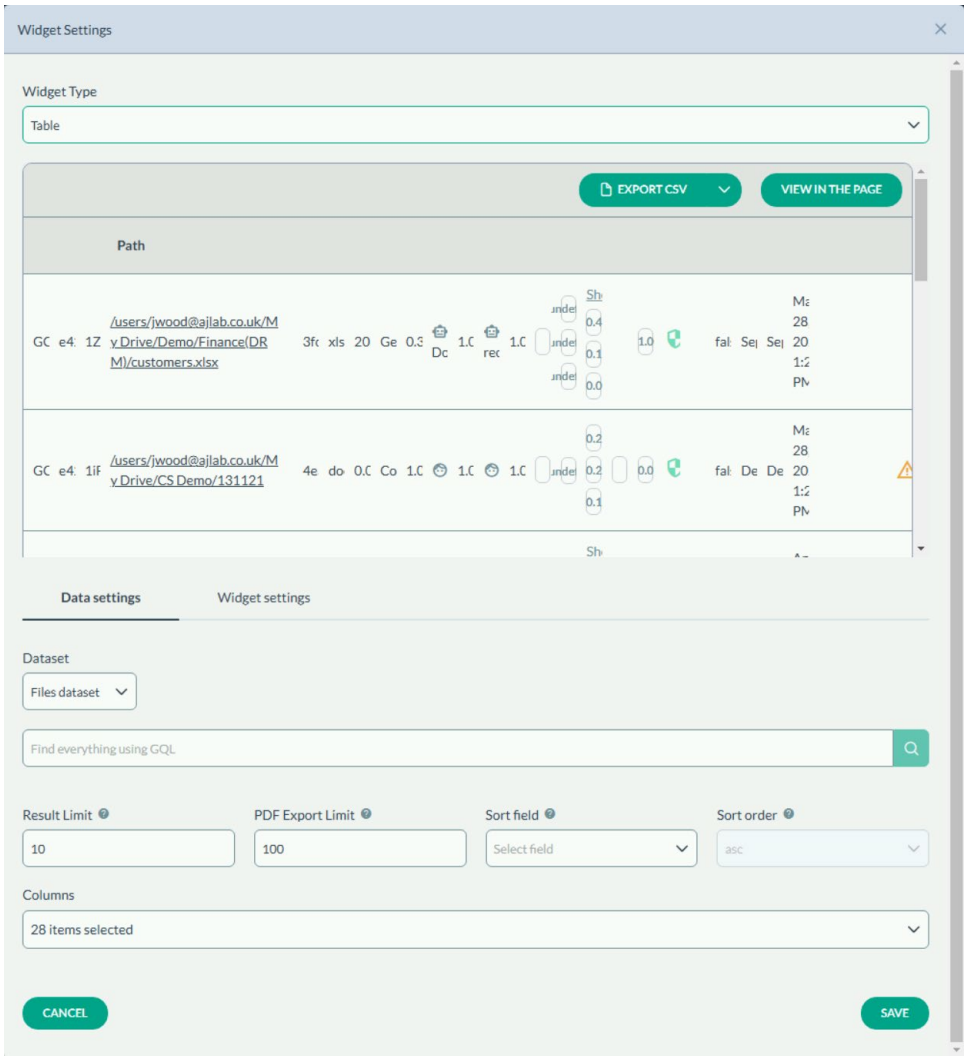

Figure 9.

This interface shows the selection of a data source (SharePoint Online) and the path to specific files within that source. The use of GQL is available to further query and refine the data. Options to export the data as a CSV file or view the table on the page will be provided. Users can set the result limit, PDF export limit, sorting field and order, and select which columns to display before saving.

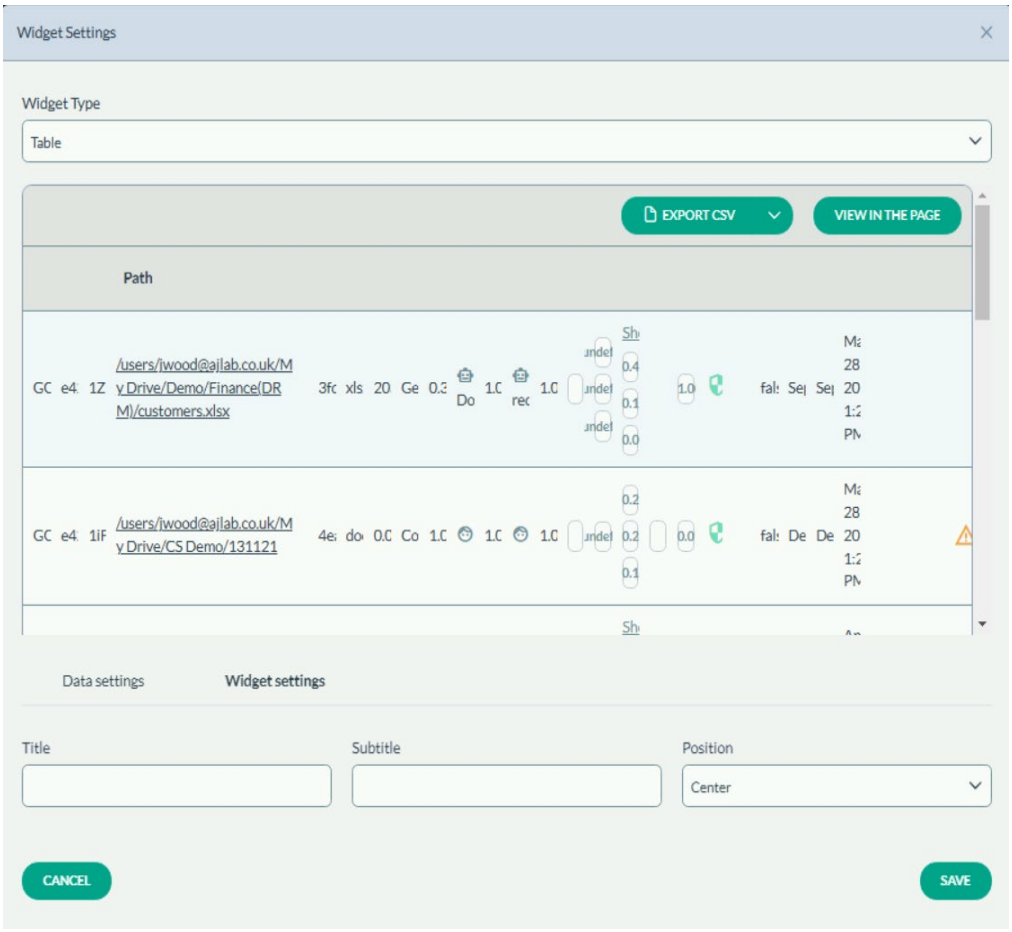

Figure 10.

In this settings panel, you can add a title and subtitle for the table, and choose their alignment on the page (e.g., left, center, right).

DSPM Rule Violations

This widget is designed to monitor and report on pre-configured data compliance issues, focusing on various data security and management rules.

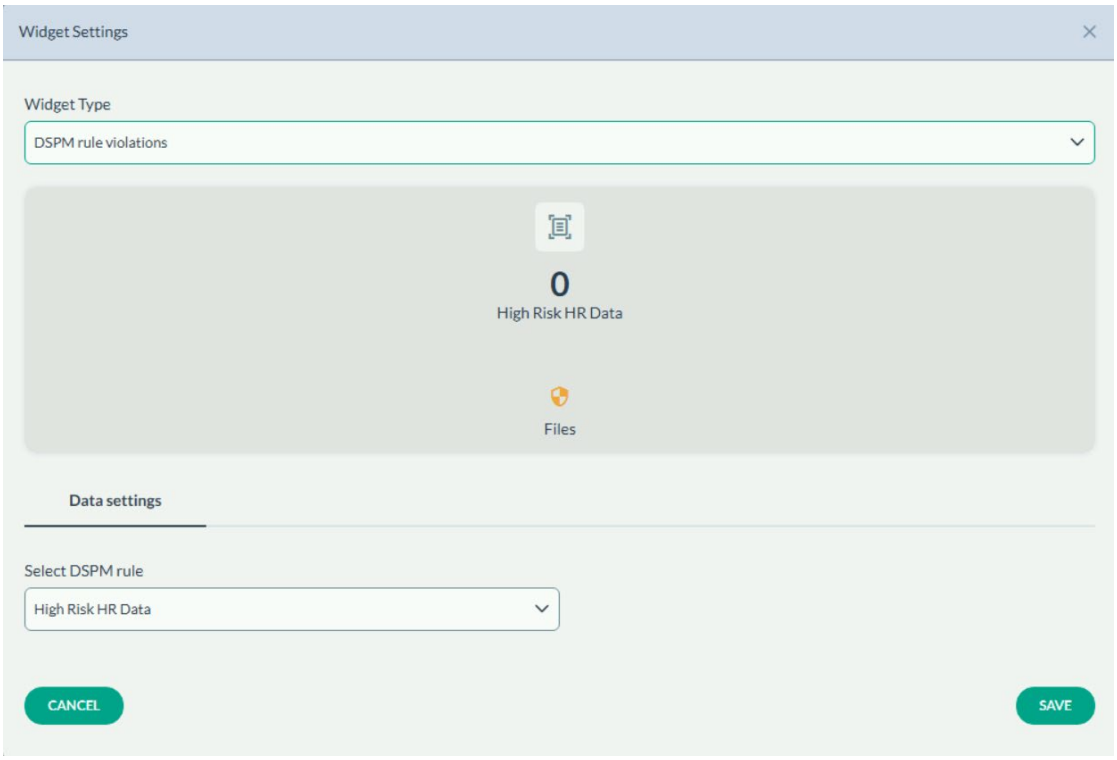

Figure 11.

Users can select a specific DSPM rule from a dropdown menu to focus on. The widget displays the count of rule violations and the corresponding files affected.

Dual Data Grouping

The Dual Data Grouping widget is used to organise and visualise complex datasets by multiple attributes simultaneously. It enables detailed analysis of complex data sets by allowing an examination of two separate data attributes concurrently. This enhances the understanding of the relationships within data.

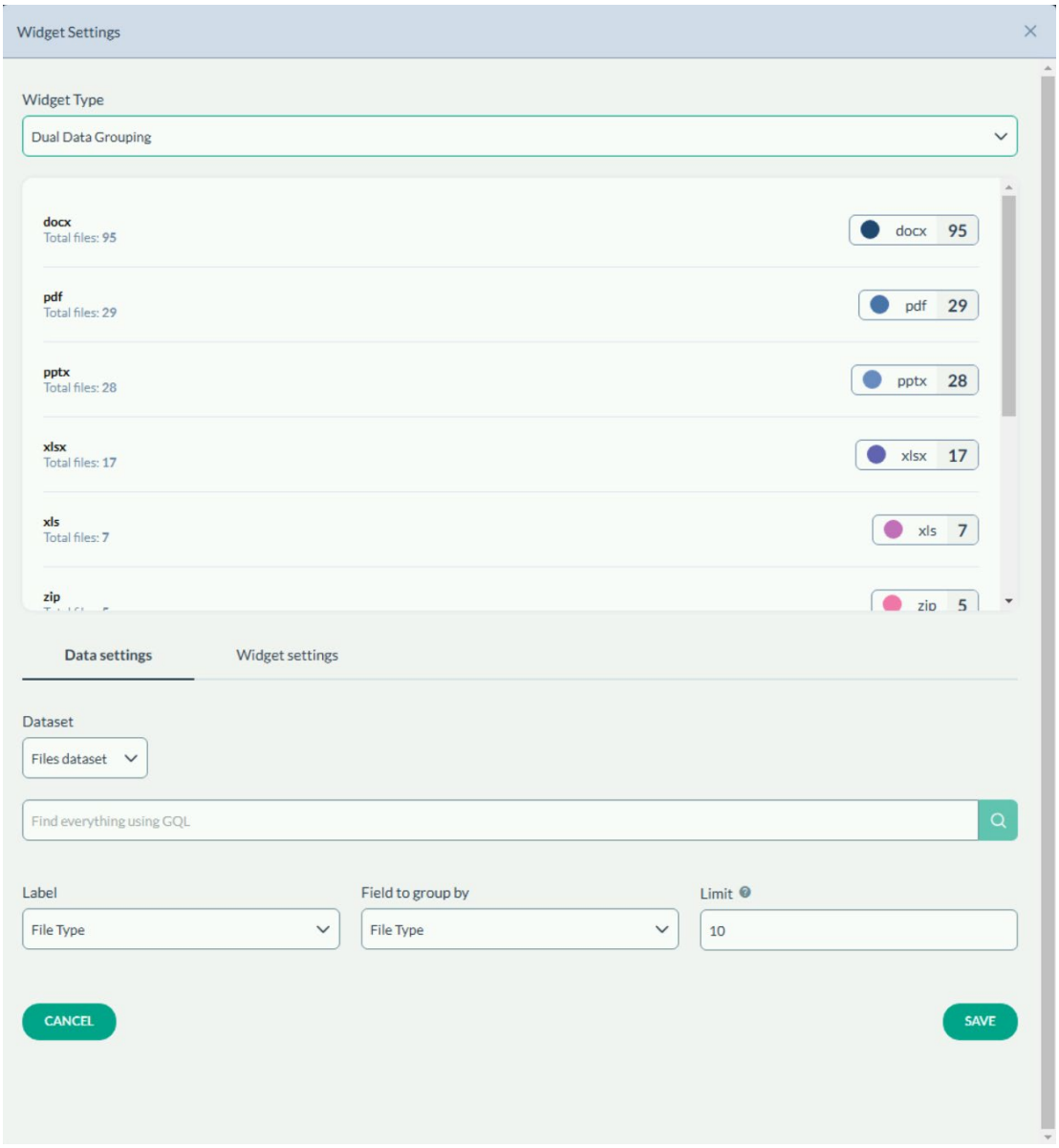

Figure 12.

The settings allow you to define the 'Label' and the 'Field to group by', which in this case is 'Data Attribute Name' and set a display limit for these groupings. Use the GQL search bar to refine your data set. After setting up, click "SAVE" to update the widget or "CANCEL" to discard changes.

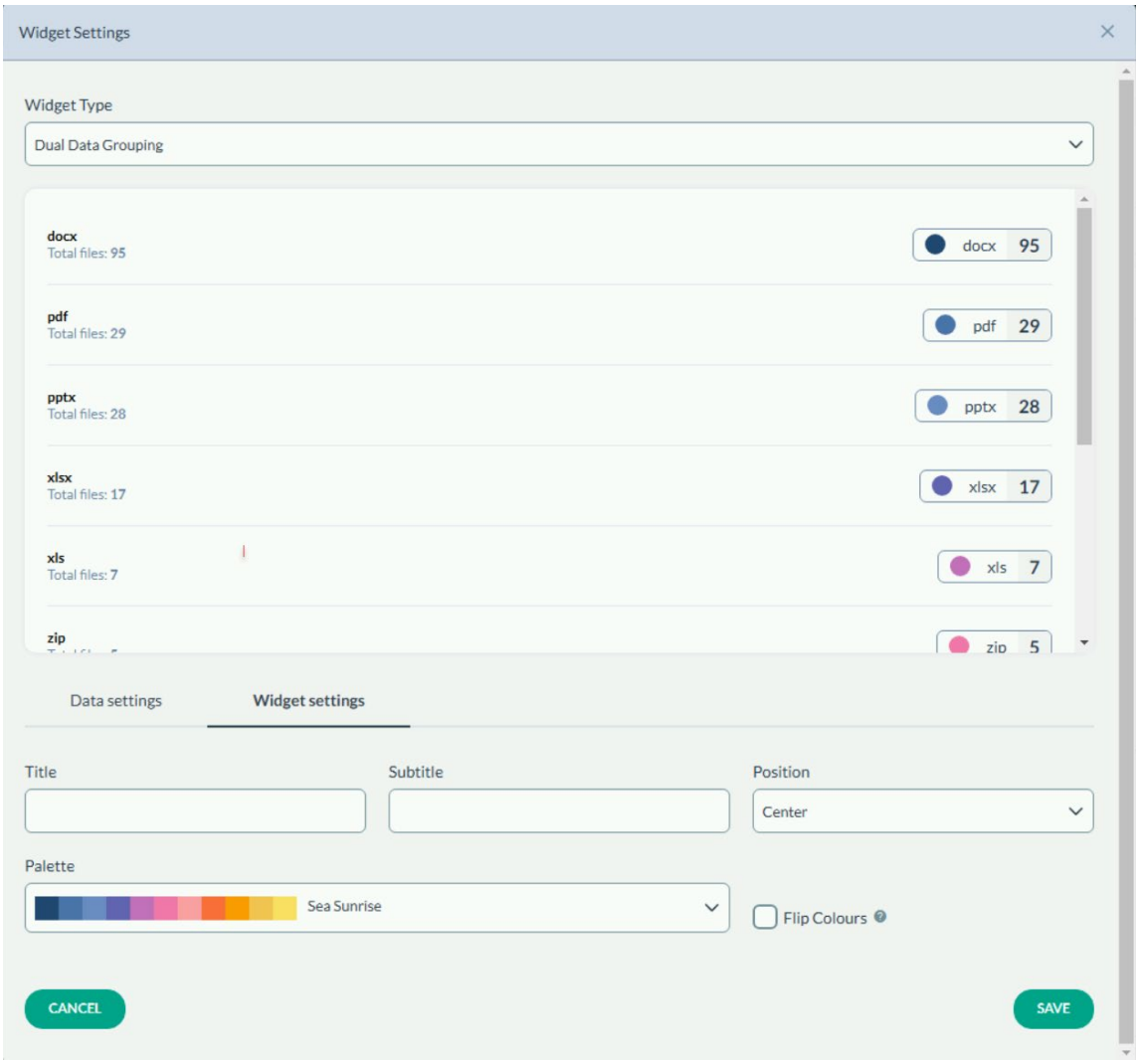

Figure 13.

You have the option to title the widget and choose a colour palette, to visually distinguish the different groupings. You can also decide whether to 'Flip Colours' for the display, to improve visual contrast or accessibility. The 'Position' dropdown allows you to align the title and subtitle.

Multi Counter

The Multi Counter widget is designed to track and display counts for multiple items or categories within a dataset, useful for monitoring and comparing quantities briefly.

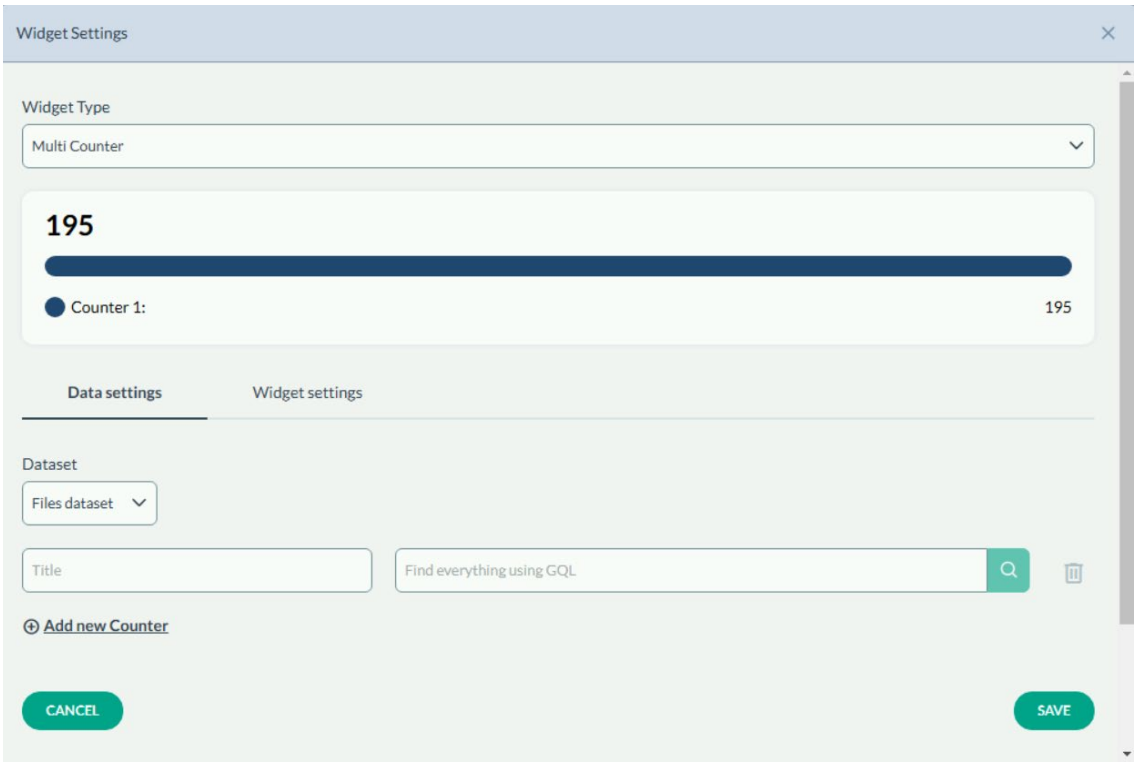

Figure 14.

Each counter can be set to track a different field. Users can customise the criteria for each counter using the search fields provided and add additional counters if needed.

Forcepoint DSPM Analytics presents essential data insights through its interface, offering a practical snapshot of data security and compliance statuses. This straightforward overview assists those in charge of data security with the necessary information to make quick, informed decisions to protect their organisation's data.

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 Analytics]
[Status]23 Apr. 24