Forcepoint Data Security Posture Management

Powered by Getvisibility

Detectors

Report

Forcepoint
April 23, 2024

Table of Contents

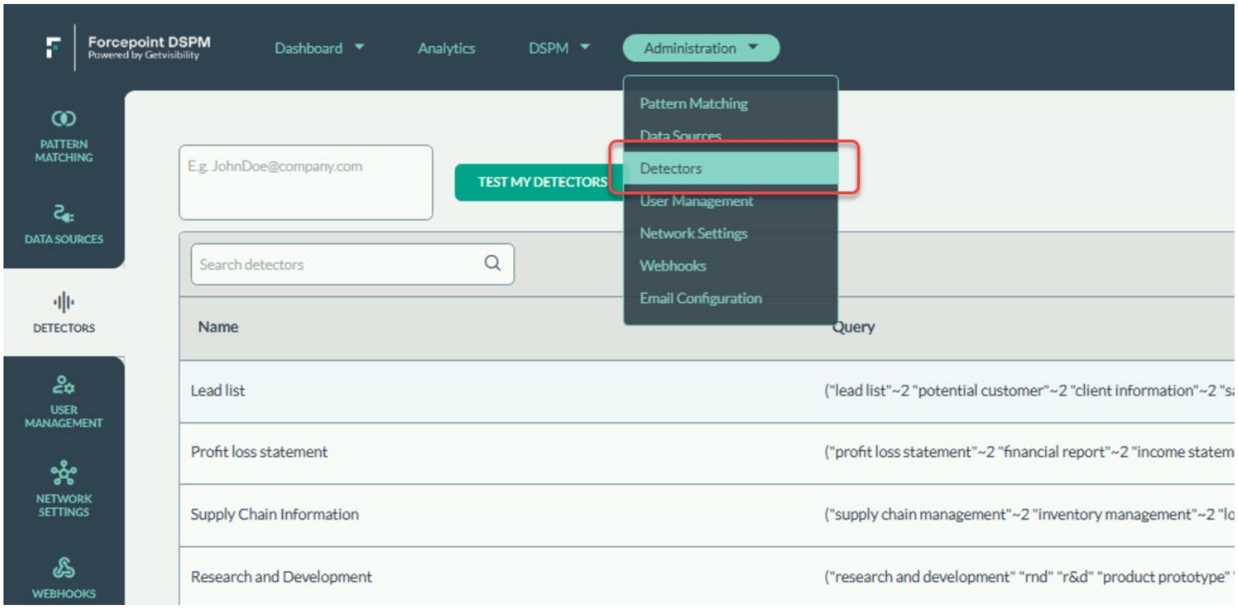
Introduction

Detectors are features that allow users to set up alerts for certain parameters during a classification search. A user can set up a Detector to search for keywords within the entire contents of a document or file, as well as search for keyword hits within the file's pathname. It uses advanced AI and ML search techniques such as Fuzzy Word Search and Percolation to search through documents much more quickly than a traditional pattern-matching search, such as using Regular Expressions.

How do I Set Up a Detector?

An example of a Detector that a user could set up is **Employee Salary**. A user might want to ensure that documents that contain this information are not publicly shared or shared internally throughout an organisation.

1. To set this up, a user should click on **Administration -> Detectors** to bring them to the **Detectors** page.



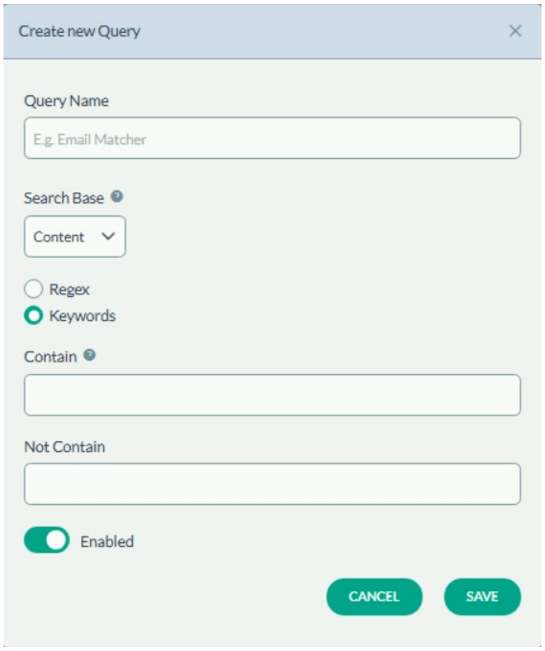
Name	Query
Lead list	("lead list"~2 "potential customer"~2 "client information"~2 "s
Profit loss statement	("profit loss statement"~2 "financial report"~2 "income statem
Supply Chain Information	("supply chain management"~2 "inventory management"~2 "lo
Research and Development	("research and development" "rnd" "r&d" "product prototype"

Figure 1.

Here they can see the list of pre-defined common Detectors that they may want to set up. In our instance, we want to set up a new one.

2. Click on the Create button on the top right corner of the screen.

   This brings us to a **Detector Creation Screen**.



Create new Query

Query Name

E.g. Email Matcher

Search Base

Content

○ Regex

● Keywords

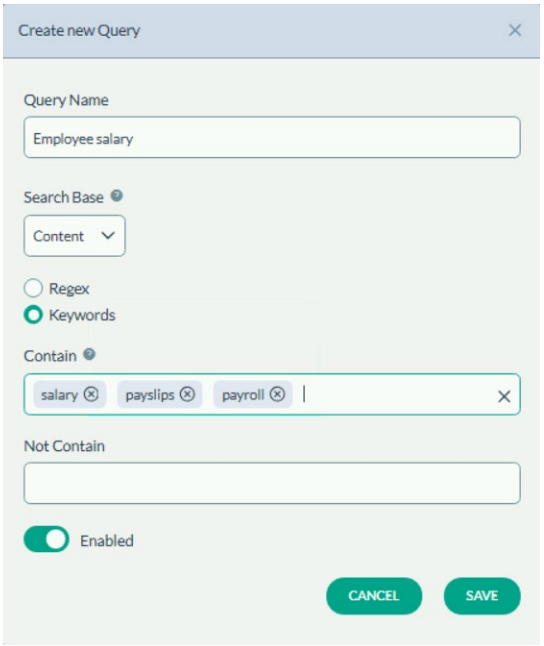
Contain

Not Contain

Enabled

Figure 2.

3. The Detector can be set up using following simple steps:
   a) The user will need to provide a Query Name (an easy to remember name that you can identify in the list of detectors). Let's call this one Employee Salaries
   b) They need to define where the Search Base of the Detector will look (i.e. search through the contents of a file or the file path). Here we want to search through the full document contents to look for certain salary-related keywords, so we'll select Content.
   c) What keywords do you want the Detector to look for? Here we'll set up a few salary-related keywords that might trigger a detector hit in a potentially sensitive document, so we'll add "Salary" "Compensation Package" "Payslip" "Payroll" "Compensation Structure" "OTE"
   d) You can also add terms that you want the Detector to ignore in the "Not Contain" field.
   e) Once you're done, click the Enabled button and Save your Detector.



Query Name: Employee salary

Search Base: Content

○ Regex
● Keywords

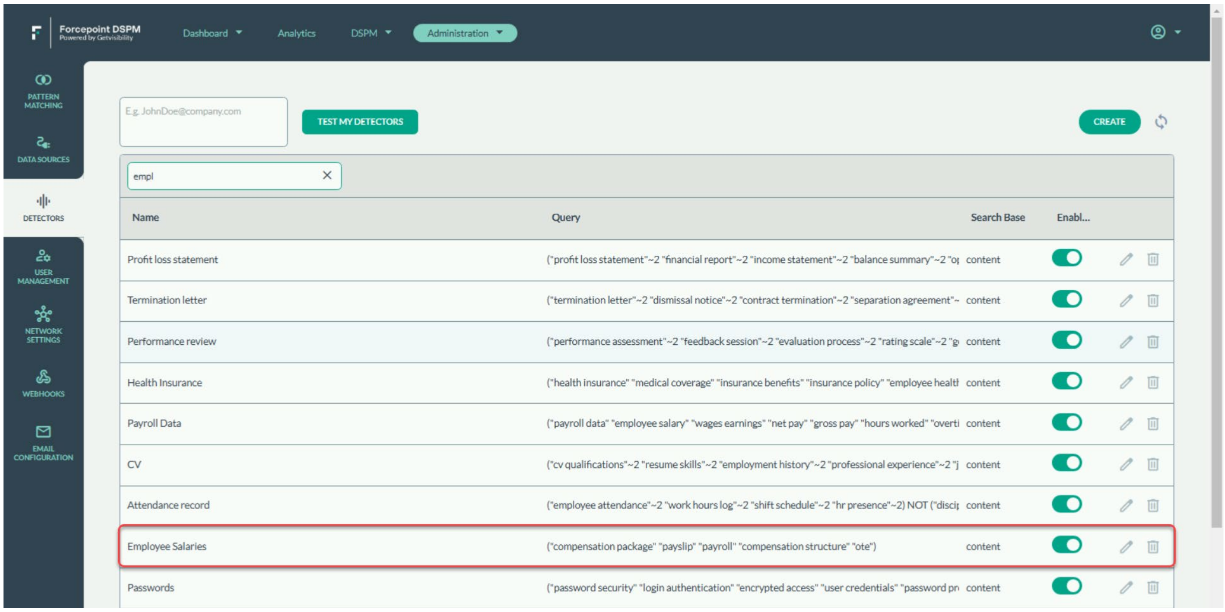
Contain: salary ⊗ payslips ⊗ payroll ⊗

Not Contain:

Enabled

Figure 3.

You should now see your new Detector named Employee Salaries in the list of Detectors.



empl

Name	Query	Search Base	Enabl...
Profit loss statement	("profit loss statement"~2 "financial report"~2 "income statement"~2 "balance summary"~2 "o	content	✓
Termination letter	("termination letter"~2 "dismissal notice"~2 "contract termination"~2 "separation agreement"~	content	✓
Performance review	("performance assessment"~2 "feedback session"~2 "evaluation process"~2 "rating scale"~2 "g	content	✓
Health Insurance	("health insurance" "medical coverage" "insurance benefits" "insurance policy" "employee healt	content	✓
Payroll Data	("payroll data" "employee salary" "wages earnings" "net pay" "gross pay" "hours worked" "overti	content	✓
CV	("cv qualifications"~2 "resume skills"~2 "employment history"~2 "professional experience"~2 "j	content	✓
Attendance record	("employee attendance"~2 "work hours log"~2 "shift schedule"~2 "hr presence"~2) NOT ("disci	content	✓
Employee Salaries	("compensation package" "payslip" "payroll" "compensation structure" "ote")	content	✓
Passwords	("password security" "login authentication" "encrypted access" "user credentials" "password pr	content	✓

Figure 4.

A user must now perform a new scan to detect for Employee Salaries.

Operations: Each token that is added to a detector is related to the other tokens like an OR condition. AND conditions are not available detectors, but this functionality can be configured indirectly through the data asset registry or directly through RegEx pattern matching.

Why is it Different to Pattern Matching?

Detectors work differently to Pattern Matching in several ways. Firstly, they can scan the entire contents of a document and path name for keywords while a traditional regex search is limited to searching through the first X number of words across all documents. Detectors leverage advanced AI and ML techniques such as Fuzzy Word Search and Percolation Search to search for phrases across an entire document in a fraction of the time it would take to search with Pattern Matching.

Feature	Detectors	Pattern Matching
Whole File Scan	Yes	No
Negative keywords	Yes	No
Specify distance between words	Yes	No
File processing	In database	In classification pipeline

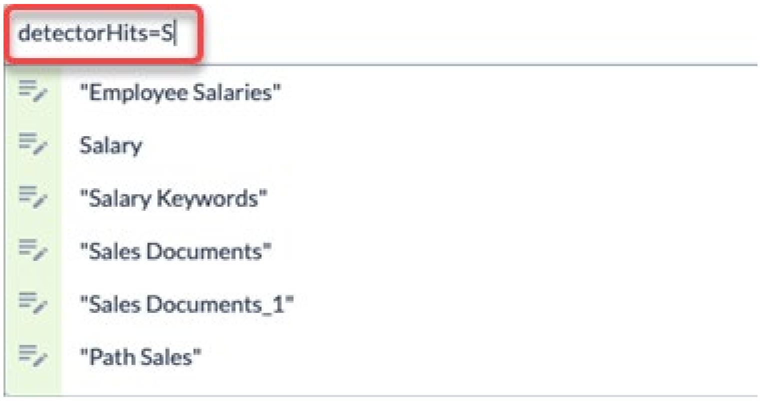
Usages

Defining Data Assets

An important feature of Forcepoint DSPM is the ability to identify data assets that are important to the organisation and assign those assets in the inventory. Detectors are a powerful method that work in conjunction with the AI Mesh to find critical, sensitive, and regulated data during scans.

GQL Queries

Once Detectors are configured and scans are underway, users can access them for describing queries in GQL. Use the detectorHits value as shown below. GQL will give suggestions to help speed up filtering.



detectorHits=S

"Employee Salaries"

Salary

"Salary Keywords"

"Sales Documents"

"Sales Documents_1"

"Path Sales"

Figure 5.

Analytics

Detectors are used along with the AI Mesh to analyse data and visually present findings in the Analytics Dashboard. Detector as associated with various data assets and types can be found through the out-of-the-box and play a crucial role in helping to identify specific important data.

Create Employee Lists

To identify employee data during scans it can be useful to add all employee names to a detector. This means a detector that helps identify HR data located throughout the data estate.

Overall, detectors give users a better understanding of their data and help them define very specific attributes as well as broad categories of data assets.

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 Detectors]
[Status]23 Apr. 24