# Forcepoint Data Security Posture Management

Powered by Getvisibility

**Data Controls** 



Report

Forcepoint April 23, 2024

## Table of Contents

NTRODUCTION	2
How TO SET A RULE	2

## Introduction

Data Controls enable organisations to apply security and compliance conditions on the data assets in their systems and apply actions on those rules when they are identified.

They are important for security and regulatory compliance as they help orchestrate the data handling within an organisation while ensuring stakeholders and data owners are involved.

They are set up during the configuration of the system and refined as the Forcepoint DSPM journey proceeds. They are used by data owners, CISOs, and other stakeholders throughout an organisation.

The data control rules are set using GQL, this can granularly define the files, users, or other assets that exist within the organisation and specify under which conditions the rule should activate. A graphical display of any recent condition-activations can be viewed as well. Automated actions can be applied to the rule where users can choose to alert use messaging apps or webhooks.

The rules are configured in the Forcepoint DSPM platform under Data Controls. Simply select Create New Rule and follow the below instructions. The rules will be triggered during a scan of the particular dataset the rule applies to.

#### How to Set a Rule

In this example we will create a rule to find HR related data that is at high risk. We will assign ownership and set up a slack message to alert a specific channel.

Force Powered	apoint DSPM Dashboard 🔻	Analytics DSPM  Administration	<b>@</b> ·
	Search Q		
Data Register	<u>Create new Rule</u> Trade Secret	New Risky Sensitive Data 🧷 🏢 Rule severity 🔮 Hi Created	ligh 🗸
DATA CONTROL	Exposure Valuable IP Exposure		
(15 Incidents	Externally Shared Data not updated in 1	Select dataset	~
	PII Files Older than 3 years	王 Condition	
	Critical information shared with 3rd parties	Set rule condition via GQL filter to identify specific policy criteria or data transactions:           sensitive=true_AND risk=2 OR risk=1 OR externalSharedLink=true_AND createdAt=".3MONTHS"	Condition Q
	Overshared internally critical information	Preview of Rule Configuration Alert - A glance at the last events:	
	Publicly exposed critical data to the world		
	Critical Data At High Risk		

1. On the Data Controls page of Forcepoint DSPM, select Create new rule.

Figure 1.

- 2. Enter the following data to create the rule
  - Name To identify the rule amongst many that can be created
  - Description Useful for others to understand the intention of the rule
  - Ownership The person who is responsible for the rule and its consequences
  - **Based on group** The data asset that this rule is associated with. These are granularly defined in the Data Asset Registry.

Create custom rule	×
Name	
High Risk HR Data	
Description	
Search for HR data that is over-exposed, p is inappropriately shared.	publicly exposed or
Ownership fdv	× ~
Based on group:	
Employee Personal Information	× ~
CANCEL	АССЕРТ



#### 3. Select Accept.

This screen allows you to further refine the rule and set the actions.

Force Powered	point DSPM Dashboard 🔻	Analytics DSPM  Administration	© •
Es? COMPLIANCE HUB	Search Q		
പ്പ	⊕ <u>Create new Rule</u>	PII Files Older than 3 years 🧷 🔟 Rule severity 😯 Medium Created	~
DATA REGISTER	High Risk HR Data	Owner: fdv	
DATA CONTROL	Trade Secret Exposure	Select dataset	
<b>۲:5</b> Incidents	Valuable IP Exposure	files	~
	Externally Shared Data not updated in 1		
	PII Files Older than 3 years	국는 Condition Set rule condition via GQL filter to identify specific policy criteria or data transactions: complianceTag=PII AND lastModifiedAt<"-3YEARS" ☆	Q
	Critical information shared with 3rd parties	Preview of Rule Configuration Alert - A glance at the last events:	-
	Overshared internally critical information	1	
	Publicly exposed critical data to the world	0.6	
	Critical Data At High Risk	0.4	
	PII Data at Risk	0 3/17/2017, 5:30:00 PM 3/18/2017, 5:30:00 PM 3/25/2017, 5:30:00 PM	
	New Risky Sensitive Data	3/11/2017, 5:30:00 PM 3/18/2017, 5:30:00 PM 3/25/2017, 5:30:00 PM Main Query 0 4/8/2017, 5:30:00 PM	
		CREATE	ACTION

Figure 3.

At the top of the screen: the name, description, and owner are visible, as well as the creation date. The option to assign rule severity is also available. As this rule, if it were breached, has the potential to incur severe consequences such as legal and financial penalties, we will set it as High.

- 4. In the select dataset dropdown, we need to define the entity types we are setting our conditions for. (In the backend this relates to separate databases). The choice will be for files, trustees, and activities.
  - o Files unstructured data classified during discovery
  - o Trustees the users and groups discovered during IAM scans
  - Activities the usage statistics of the endpoint agents (FDC)

We will select files in this example.

The condition section will be pre-loaded with a GQL if you have selected a Data Asset Group. Here it is simply path=HR and we can see that there are some recent files that match these criteria.

#### 5. We will refine the search further by adding the condition that the HR files found will be high risk. AND risk=2.

The platform has three levels of risk: low, medium, and high. Their respective values in GQL are: 0, 1, and 2

- Condition		
et rule condition via GQL filter to identify specific policy criteria or data transactions:		
complianceTag=PII AND dataAttributeName=Record AND dataAttributeName=Person AND dataAttributeName=HR AND detectorHits="GV HR list"	☆	a

Figure 4.

As can be seen, no files have yet to fall under this rule.

∃≟ Condition	
Set rule condition via GQL filter to identify specific policy criteria or data transactions:	
complianceTag=PII AND dataAttributeName=Record AND dataAttributeName=Person AND dataAttributeName=HR AND detectorHits="GV HR list"	\$ Q
Preview of Rule Configuration Alert - A glance at the last events:	

Figure 5.

We can create an action so that we can catch high risk HR files going forward.

6. Scroll to below the condition and select **Create Action**. In the Action type dropdown, you can choose a simple Webhook or a Slack Webhook. Here we will add a Slack Webhook that will notify a Slack channel when the data control is activated.

High Risk HR Data 🧷 🔟	Rule severity 🔗 Medium	~
Created Apr 18, 2024		
Search for HR data that is over-exposed, publicly exposed or is inappropriately shared.		
Owner: fdv		
Select dataset		
files		~
↓		
로 Condition Set rule condition via GQL filter to identify specific policy criteria or data transactions:		
complianceTag=PII AND dataAttributeName=Record AND dataAttributeName=Person AND dataAttri	ibuteName=HR AND detectorHits="GV HR list"	Q
Preview of Rule Configuration Alert - A glance at the last events:		
	CREATE A	_
Action		стюн
Action Action type Webhook		_
Action type		_



Multiple actions can be created for the same data control.

7. Select **UPDATE** to save the control, and that's it! Once scanning commences we will get notified in Slack, as well as on the Incidents page.

Forcepoint Powered by Getv	DSPM Dashboard ▼ Analytics elability	DSPM  Administration			e
		Select incidents time range:		e	
AREGISTER	[II]	(B)	jej	II	ĨĦĴ
	<b>O</b> High Risk HR Data	O Trade Secret Exposure	O Valuable IP Exposure	O Externally Shared Data not updated in 1 year	26 PII Files Older than 3 years
CIDENTS	Files	<b>O</b> Files	Files	<b>⊘</b> Files	<b>O</b> Files
	E)	(II)	[II]	jej	jiij
	O Critical information shared with 3rd parties	<b>11</b> Overshared internally critical information	O Publicly exposed critical data to the world	<b>O</b> Critical Data At High Risk	<b>O</b> PII Data at Risk
	<b>?</b> Files	<b>O</b> Files	Files	😯 Files	<b>?</b> Files
	الله الله				
	<b>O</b> New Risky Sensitive Data				
	😵 Files				

Figure 7.



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.

© 2024 Forcepoint. Forcepoint and the FORCEPOINT logo are trademarks of Forcepoint. All other trademarks used in this document are the property of their respective owners. [Forcepoint Data Security Posture Management Powered by GetVisibility Data Controls] [Status]23 Apr. 24