

# Forcepoint Data Security Posture Management

Powered by Getvisibility

Data Controls

**Forcepoint**

Report

Forcepoint  
April 23, 2024

# Table of Contents

<b>INTRODUCTION</b> .....	<b>2</b>
HOW TO SET A RULE .....	<b>2</b>

# 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.

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

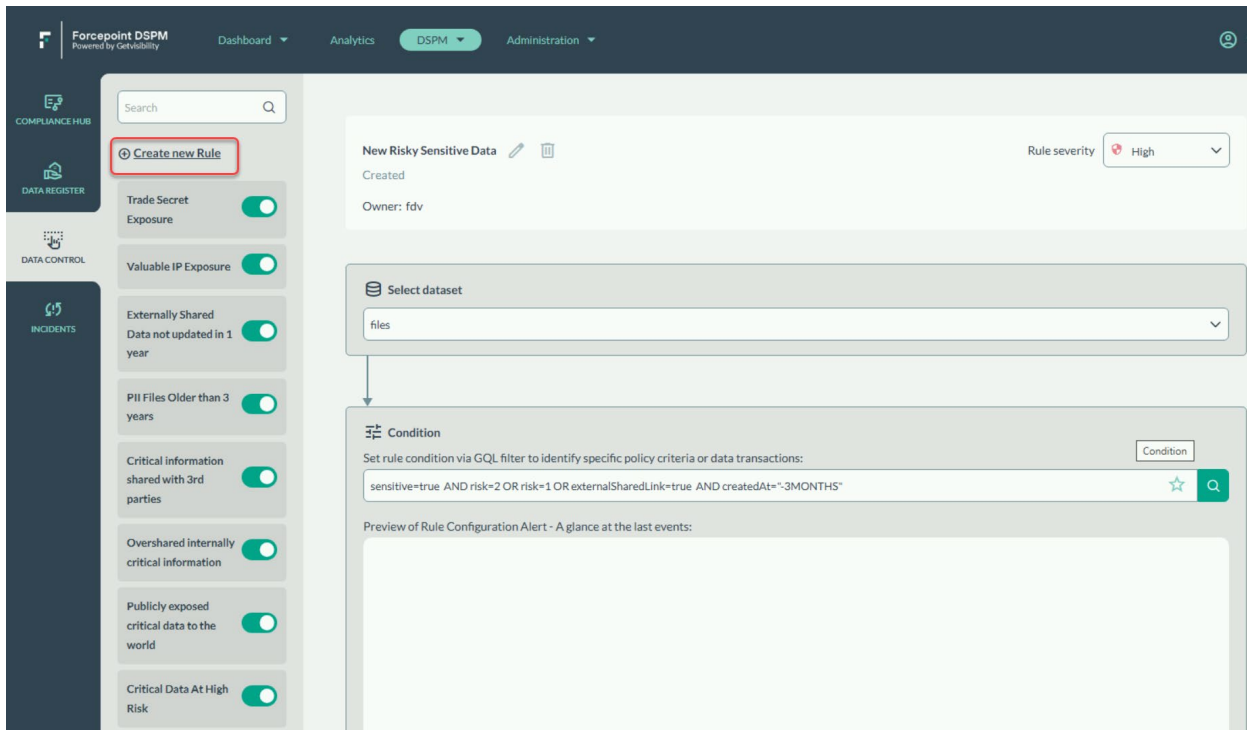
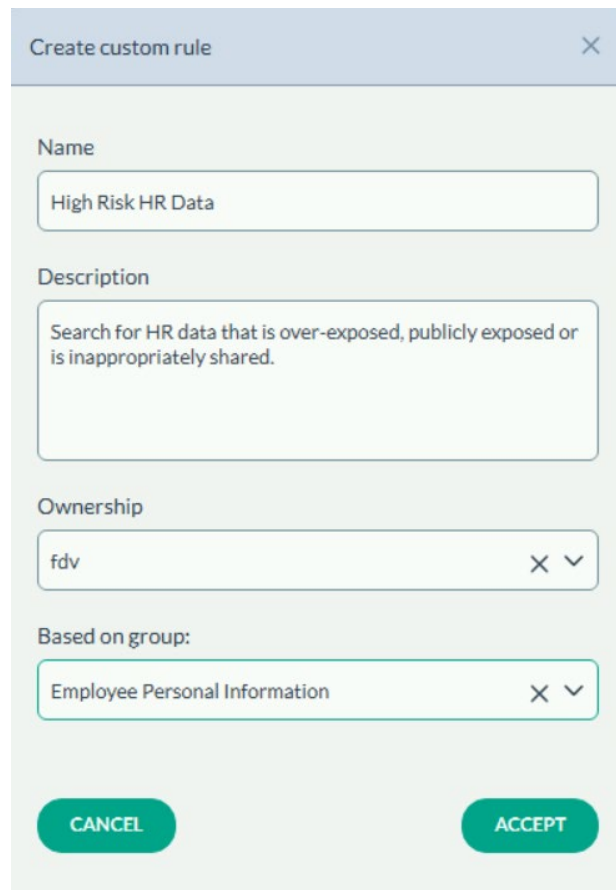


Figure 1.

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.



The screenshot shows a 'Create custom rule' dialog box with the following fields and values:

- Name:** High Risk HR Data
- Description:** Search for HR data that is over-exposed, publicly exposed or is inappropriately shared.
- Ownership:** fdv
- Based on group:** Employee Personal Information

At the bottom of the dialog are two buttons: **CANCEL** and **ACCEPT**.

Figure 2.

3. Select **Accept**.

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

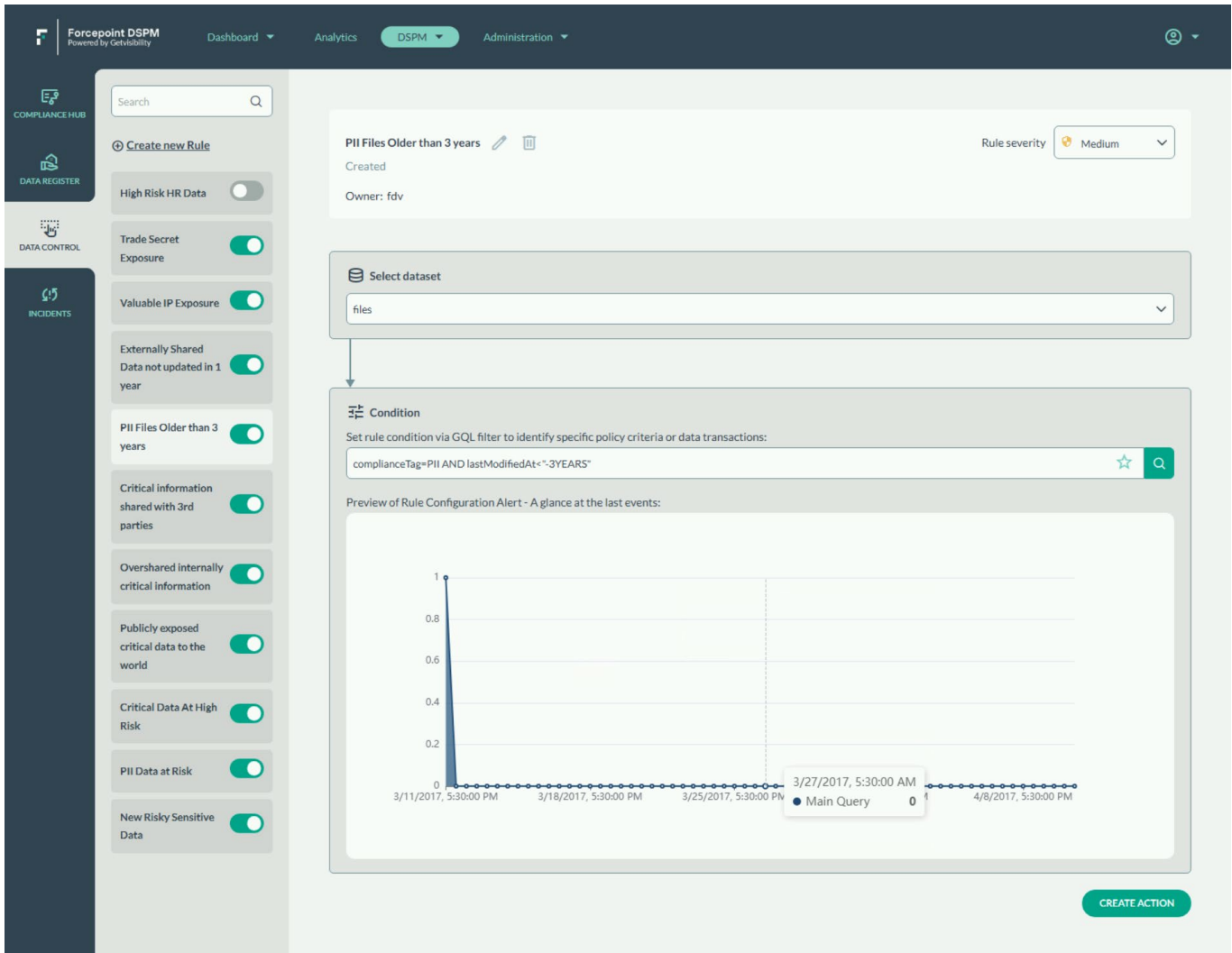


Figure 3.

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
  - o **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

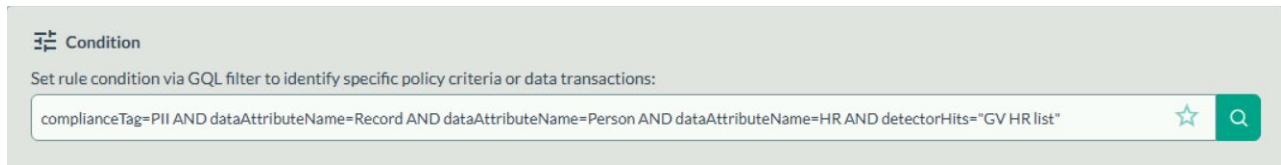


Figure 4.

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

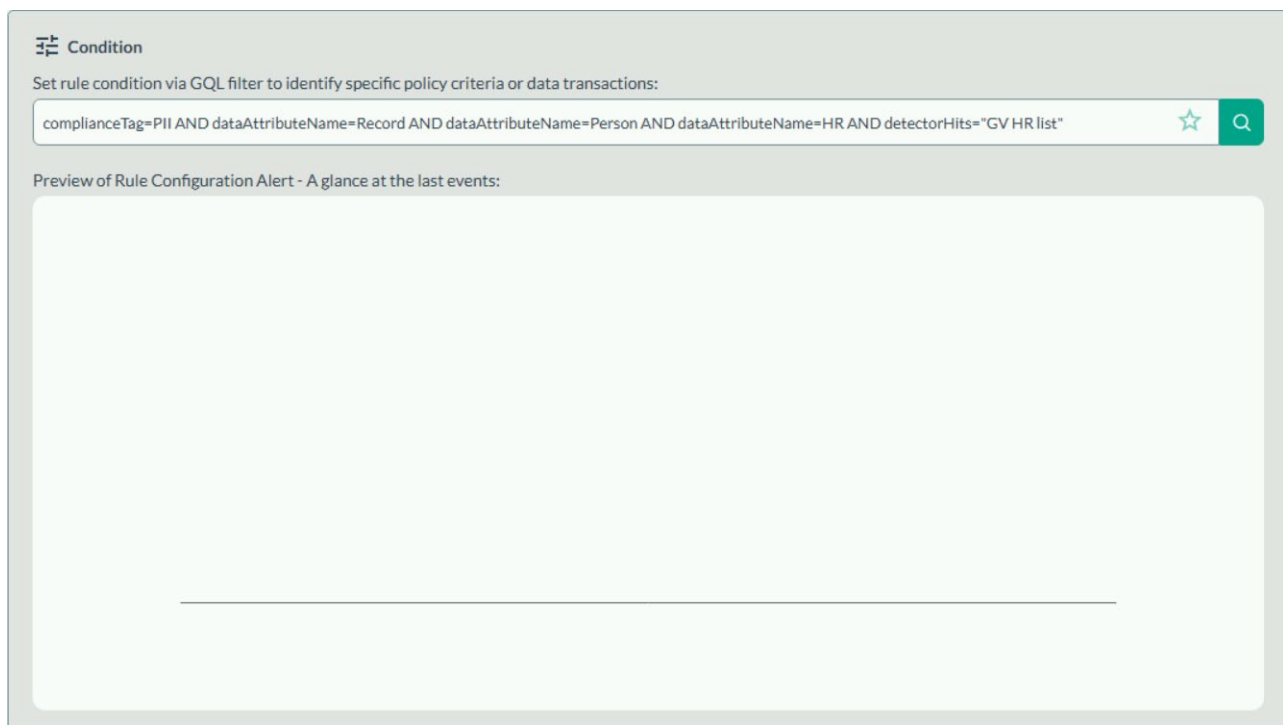


Figure 5.

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.

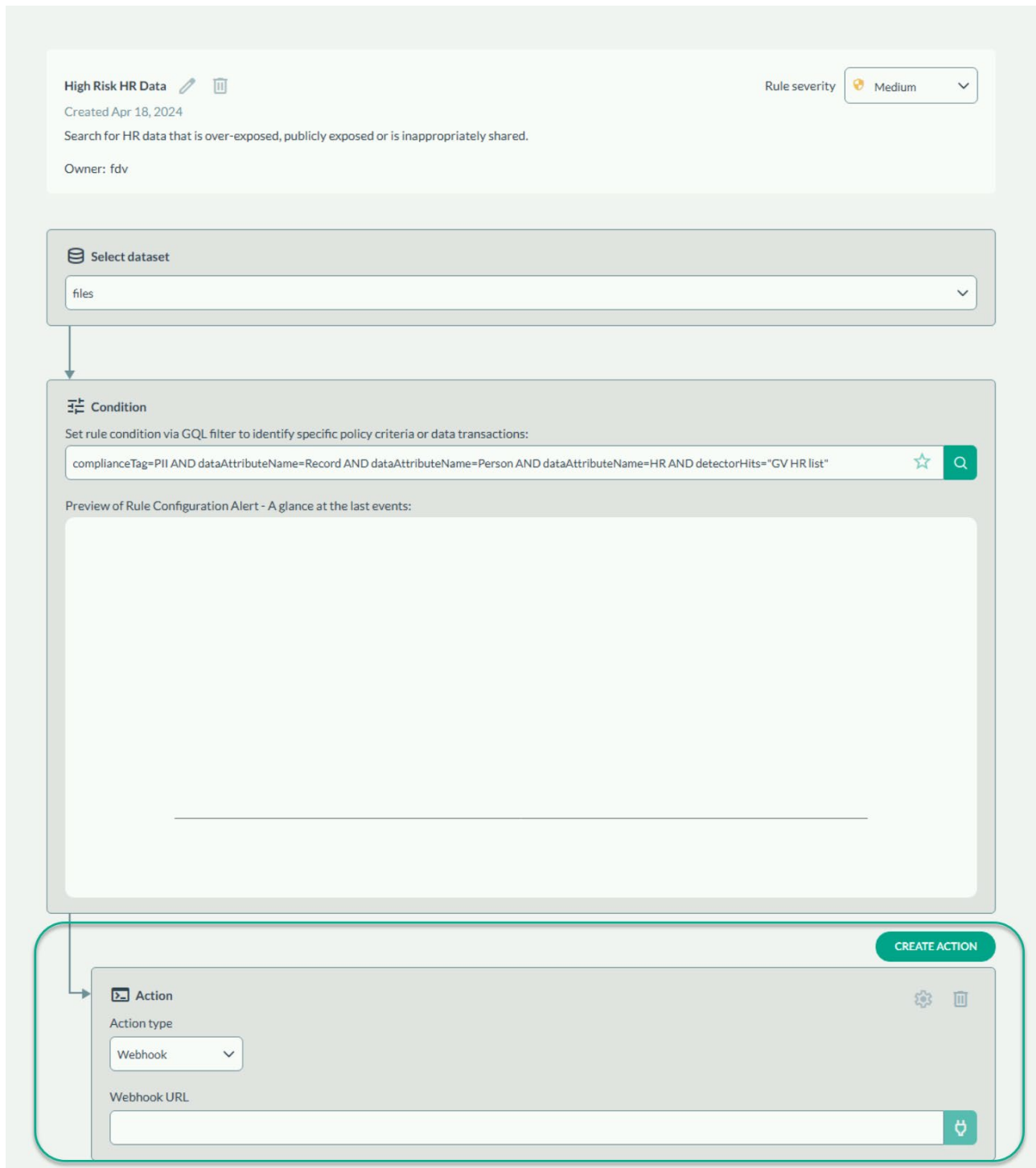


Figure 6.

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.

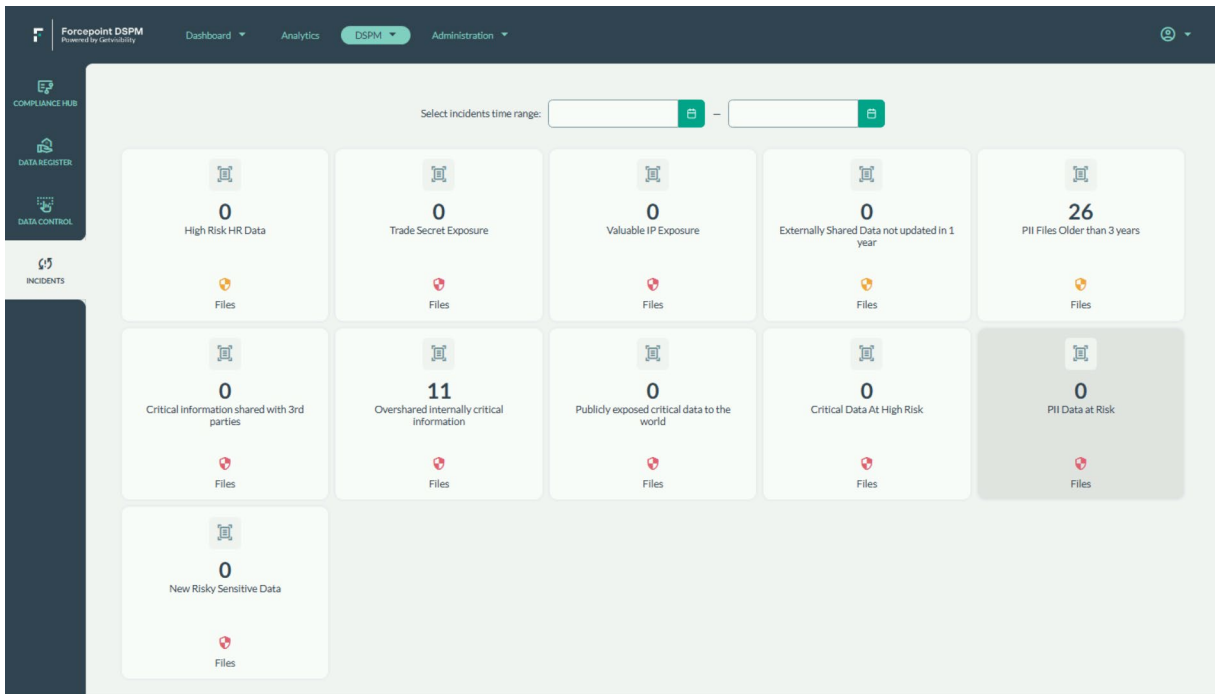


Figure 7.





[forcepoint.com/contact](https://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](https://www.forcepoint.com), [Twitter](#) and [LinkedIn](#).