Forcepoint ONE Integrated with Microsoft Sentinel Configuration Guide

Forcepoint

Table of Contents

About This Document

This document describes in detail the configuration steps needed to integrate Forcepoint ONE with Microsoft Sentinel, as logs generated from Forcepoint ONE will be sent to Microsoft Sentinel via REST APIs.

Forcepoint Overview

Forcepoint is the leading user and data security cybersecurity company, entrusted to safeguard organizations while driving digital transformation and growth. Forcepoint solutions adapt in real time to how people interact with data, providing secure access while enabling employees to create value.

Microsoft Overview

Microsoft Corporation is an American multinational technology corporation headquartered in Redmond, Washington. Microsoft's best-known software products are the Windows line of operating systems, the Microsoft Office suite and the Internet Explorer and Edge web browsers.

Audience

This guide is for network administrators, endpoint and IT administrators and security analysts responsible for deploying, monitoring and managing enterprise security systems. This document is targeted to those interested in learning details of how Forcepoint ONE and Microsoft Sentinel interact, as well as providing guidance for integration of the two solutions.

Forcepoint ONE and Microsoft Solutions Introduction

Forcepoint ONE Overview

Forcepoint ONE is an all-in-one SSE platform that makes it easy to adopt Zero Trust, protect against threats and prevent the theft or loss of sensitive data and intellectual property on the web (SWG), in the cloud (CASB) and in internal private applications (ZTNA). It allows organizations to manage one set of policies, in one console, with one endpoint agent. Unique features include 99.99 percent verified uptime since 2015, more than 300 points of presence worldwide, ability to support inline proxy of highly latency sensitive apps like Slack, SWG with integrated smart RBI with CDR, and distributed SWG policy enforcement. The solution contains an agentless CASB and ZTNA option for private web applications. The options for Cloud and SaaS Security Posture Management (CSPM and SSPM) flag and optionally auto-remediate risky tenant security settings.

Microsoft Sentinel Overview

Microsoft Sentinel is a scalable, cloud-native, Security Information and Event Management (SIEM) and Security Orchestration, Automation and Response (SOAR) solution. Microsoft Sentinel delivers intelligent security analytics and threat intelligence across the enterprise, providing a single solution for attack detection, threat visibility, proactive hunting and threat response.

Microsoft Sentinel acts like a bird’s-eye view across the enterprise, alleviating the stress of increasingly sophisticated attacks, increasing volumes of alerts and long resolution time frames.

Microsoft Sentinel helps organizations to a) collect data at cloud scale, b) detect previously undetected threats and minimize false positives, c) investigate threats with artificial intelligence and d) respond to incidents rapidly with built-in orchestration and automation of common tasks.

Integration Introduction

Integration Architecture

Every user-initiated transaction that traverses Forcepoint ONE generates a corresponding log message. These log messages are retained by Forcepoint ONE for a specific limited period, and customers can view and search these logs using the dashboards and log menus of Forcepoint ONE.

Forcepoint ONE includes REST APIs to export these logs to third-party solutions for further processing and to deliver additional capabilities around user and application transactions. Forcepoint ONE provides different types of logs, listed as follows:

- Cloud (API): Logs generated by cloud apps as seen on the **Analyze > Logs > API** dashboard page.
    - Cloud Summary: Displays the current status of the files in the applications.
    - Cloud Audit: Displays every scan result for each file in your corporate account.
- Access (Proxy): Logs generated by application activity as seen on the **Analyze > Logs > Proxy** dashboard page.
- Admin: All admin events within the admin portal as seen on the **Analyze > Logs > Admin** dashboard page.
- SWG Web: Logs generated from general web traffic from users using the SmartEdge agent, pulls logs from the **Analyze > Logs > Web** dashboard page.
- SWG DLP: Logs generated from DLP specific policy actions under the Web Browsing Policy actions as seen on the **Analyze > Logs > Web DLP** dashboard page.
- Health: The Health dashboard allows admins to identify if issues that users encounter are brought on by Forcepoint ONE or the destination application (e.g., Google, Exchange, Salesforce, etc.). You can access the System and Proxy Health Logs by navigating to **Analyze > Logs > Health**.
- ZTNA: The ZTNA Logs page is where all the ZTNA events by the end users are displayed. You can access the ZTNA Logs page by navigating to **Analyze > Logs > ZTNA**.

Using Microsoft Sentinel Codeless Connector Platform (CCP), we will create Data Connectors to retrieve access logs from Forcepoint ONE without any requirements for additional service installations. These data connectors include health monitoring and are fully supported by Microsoft Sentinel.

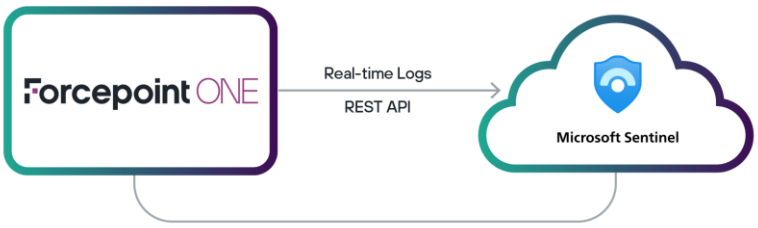

Figure 1. High-level Integration Architecture

Prerequisites

As both Forcepoint and Microsoft solutions are pure SaaS cloud-native solutions, there are minimal prerequisites:

- Active Forcepoint ONE tenant with any or all three modules enabled (SWG, CASB, ZTNA)
- Active Azure subscription

Configuration Steps

Forcepoint ONE
In this section, we will list all the steps to perform on the Forcepoint ONE side to integrate the two solutions together.

Creating Admin Role
The "Admin Roles" page is where Forcepoint ONE admins can create different and unique admin roles to assign to users or groups. The role permissions can allow users to perform Edit, View or Disabled (i.e., hidden) actions to each individual tab and the sub-component within the tab.

1. Go to Identity & Access Management (IAM) menu
2. Click on “Admin Roles”
3. Click “Add”
4. Name the new Admin Role with a relevant name, i.e., “API Role”
5. Make sure the “View” check is selected for all the components under every section
6. Click “Save”

Creating API User
The “User and Groups” page is where Forcepoint ONE admins manage everything related to their organization’s domain, users, groups and authentication. This is where we will create the new API user and assign it to the Admin Role we have just created.

1. Go to Identity & Access Management (IAM) menu
2. Click on “Users and Groups”
3. Under “All Users”, click “Add”
4. Select “Add a User Manually” and click “Continue”
5. Enter the mandatory fields, like: “username,” “First Name,” “NetBios Domain,” “SAMAccountName”
6. Make sure to select the “Admin Role” we created in the previous section, i.e., “API Role”
7. Click “Set password and activate user”
8. Set the account password and confirm it
9. Click “Create”

Microsoft Sentinel

In this section, we will list all the steps to perform on the Microsoft Azure side to integrate the two solutions together.

Onboarding Microsoft Sentinel

The following steps assume you don't have an existing Microsoft Sentinel service running already or any existing workspaces created and that this is the first time to onboard this service on your Microsoft Azure portal.

Creating Log Analytics Workspace

On your Azure portal https://portal.azure.com, under "Azure Services," click "Microsoft Sentinel." If you can't find it in the main screen, you can search for it in the search bar on top of the portal.

1. Click "+ Create"
2. On the "Add Microsoft Sentinel to a workspace" page, click "+ Create a new workspace"
3. Select your Azure subscription you want to host this service under
4. Under the "Resource Group" section, click "Create new"
5. Name it a relevant name, i.e., "FP-RG"
6. Click "OK"
7. Under the "Instance details" section, name the new workspace with a relevant name, i.e., "FP-WS"
8. Select the relevant "Region"
9. Click "Review + Create"
10. Upon successful validation, click "Create"

Enabling Microsoft Sentinel

Once the workspace has been created successfully, go to the main Azure portal page.

1. Click "Microsoft Sentinel" again
2. Click "+ Create"
3. Now, select the workspace you have just created, i.e., "FP-WS," and click "Add"

Creating Codeless Data Connector

1. On the Azure portal main page, search for "Deploy a custom template"
2. Click "Build your own template in the editor"
3. Delete the preloaded text, and paste the text from the relevant attached json file:
    - For CASB Data Connector, use file: "FONE-CASB-Connector.json"
    - For SWG Data Connector, use file: "FONE-WEB-Connector.json"
4. Click "Save"
5. Select the proper Resource Group, i.e., "FP-RG"
6. Enter the proper Log Analytics Workspace Name, i.e., "FP-WS"
7. Click "Review + create"
8. Upon successful validation, click "Create"

9. Once the connector is successfully created, go to “Microsoft Sentinel” from Azure portal main page
10. Select the proper workspace, i.e., “FP-WS”
11. Choose “Data connectors”
12. Click “Refresh” to make sure the newly created Data Connector is listed
13. Search for the newly created Data Connector using the relevant name:
    - For CASB Data Connector, search for: “Forcepoint ONE (CASB) Connector”
    - For SWG Data Connector, search for: “Forcepoint ONE (WEB) Connector”
14. Now, click on the name of the Data Connector, and click “Open connector page”
15. On the Data Connector page, under the “Configuration” section, enter the username and password of the API user that was created on Forcepoint ONE
16. Click “Connect”

Checking Logs Reception

According to Microsoft, please note that the first log lines may take up to 15-20 minutes until they reach Microsoft Sentinel.

To make sure that Forcepoint ONE logs are now available on Microsoft Sentinel:

1. Click on “Microsoft Sentinel” on the main Azure portal page
2. Select the proper workspace, i.e., “FP-WS”
3. Click on “Logs”
4. In the query window, enter the relevant table name, followed by “| take 10”
    - For CASB logs, the table name is: “ForcepointONECASBconnector_CL”
    - For SWG logs, the table name is: “ForcepointONEWEBconnector_CL”
5. Click “Run”

In the “Results” section, you should see an entry with 10 log lines from the relevant table. This is a proof that now Forcepoint ONE logs are reaching Microsoft Sentinel, and we are ready for the next step of creating workbooks.

Creating Workbooks

Admins can create dashboards as needed in workbooks; Forcepoint is including two initial workbooks to present sample dashboards on both CASB & SWG logs. To create Microsoft Sentinel workbooks:

1. Click on “Microsoft Sentinel” on the main Azure portal page
2. Select the proper workspace, i.e., “FP-WS”
3. Click on “Workbooks”
4. Click “+ Add workbook”
5. Click “Edit”
6. Click the “Advanced Editor” button
7. Clear all preloaded text in the template
8. Paste the relevant text from the workbook file attached to this guide:

9. Click “Apply”
10. Click “Done Editing”
11. Click “Save”
12. Give the new workbook a relevant name, i.e., “Forcepoint ONE - CASB”
13. Select the proper Resource Group, i.e., “FP-RG”
14. Click “Apply”

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.

[FP ONE Integrated with Microsoft Sentinel Configuration Guide] 22Sept2023