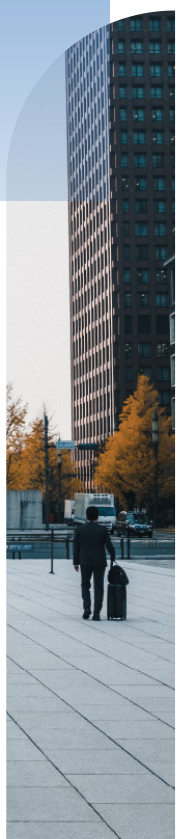
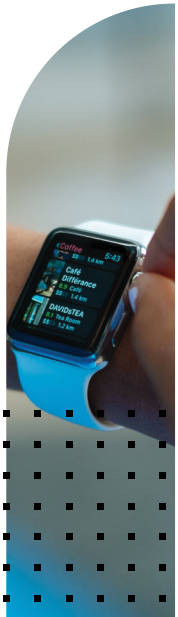
DEPLOYMENT GUIDE

FortiEDR Architecture and Deployment





Introduction

This document describes the FortiEDR architecture and deployment steps for the Software-as-a-Serivce (SaaS) solution on the Google Cloud Platform (GCP).

FortiEDR Components and Flow

The FortiEDR platform is a distributed architecture that collects and analyzes the flow of events to detect malicious activity. The message flow between FortiEDR components is as described below (Figure 1):

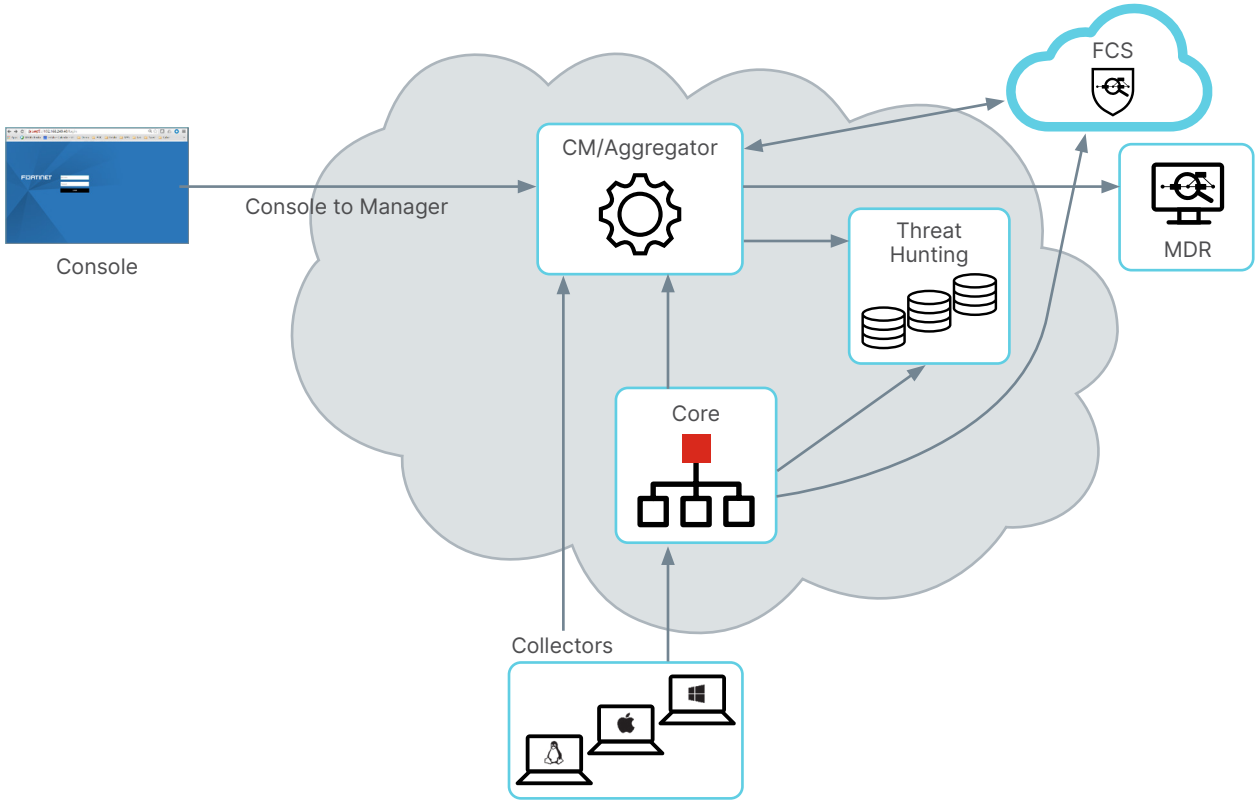


Figure 1: FortiEDR GCP architecture.

- The FortiEDR Collectors sends registration and status information to the Aggregator. It also receives configuration from the Aggregator.
- Collectors sends compressed OS metadata and Threat Hunting data to Core.
- Core forwards Threat Hunting data to Threat Hunting Repository, and it also sends malicious activity and status information to Aggregator.
- Threat Hunting queries from Central manager are sent to Threat Hunting Repository.
- FortiEDR Aggregator acts as a proxy for Central Manager and aggregates information received from collectors and cores. It also distributes configurations from the Central manager to the cores and collectors. Usually, in most deployments Aggregator and Central Manager can be installed on the same server.
- Fortinet Cloud Services (FCS) performs deep threat analysis to classify security events.
- FCS helps in tuning of an environment by automatically creating security events exceptions if a triggered event is reclassified as Safe.
- Playbook actions configured on Central Manager are also triggered based on final classification of security event by FCS.

Initiating a Service

In the Google Cloud Marketplace, find the Fortinet FortiEDR service offering and select the plan and subscription period (Figure 2).

- FortiEDR Discover, Protect, and Respond
- FortiEDR Discover, Protect, and Respond with MDR

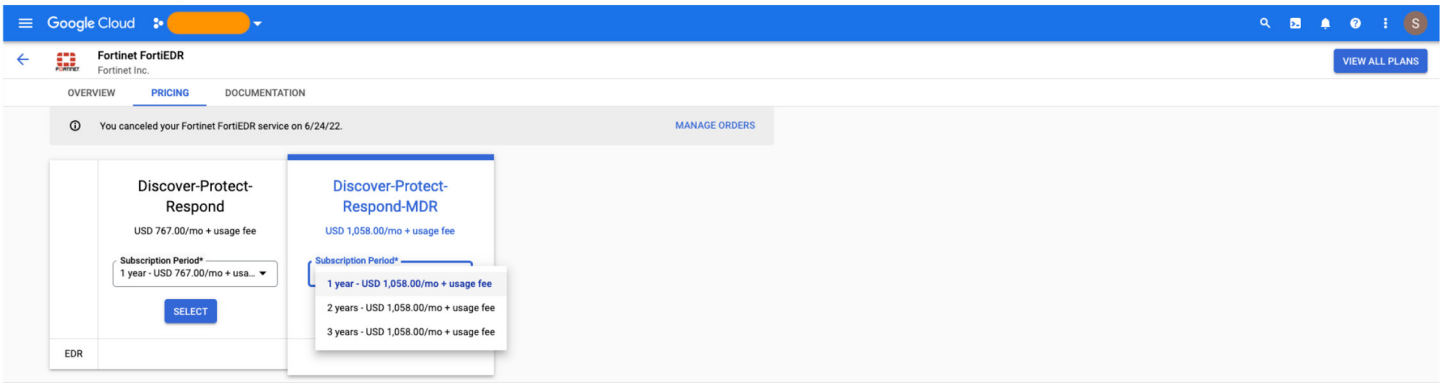


Figure 2: FortiEDR services on GCP.

Once customers subscribe to a specific plan, they get prompted to register and create a FortiCloud support account (Figure 3). To complete the registration process, the customer will get redirected to the forticloud.com portal hosted by Fortinet from the Google Cloud console.

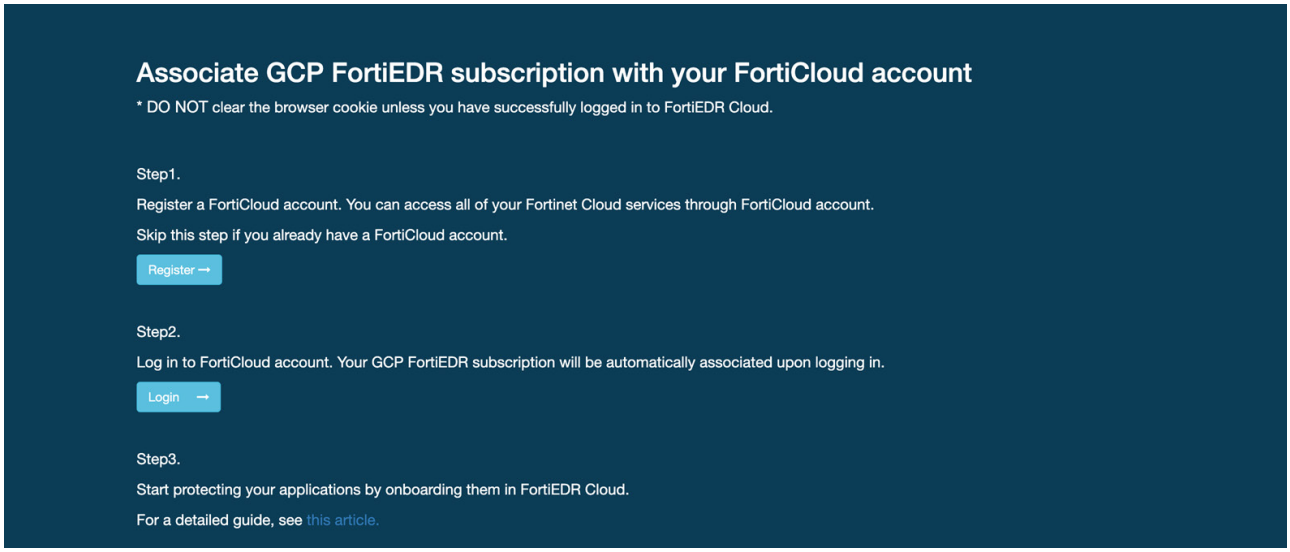


Figure 3: FortiCloud registration page.

Once the customer registers with the forticloud.com portal, the Fortinet support team will start working on setting up the customer environment. It can take up to one business day for service activation. Once the service is activated, the customer will see a checkmark with the status listed as "Active" for their FortiEDR subscription (Figure 4). The customer will also receive an email with the URL to access the FortiEDR manager console, an IP address of the FortiEDR Aggregator, and access credentials.

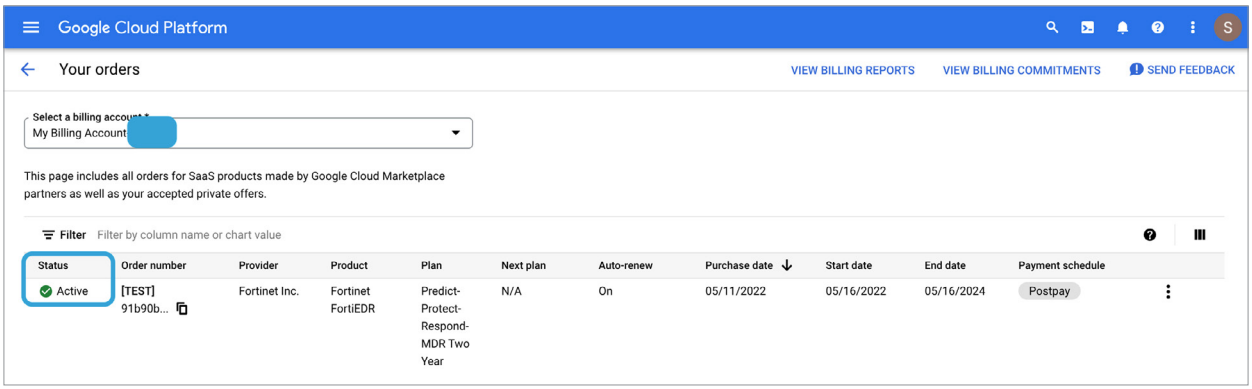


Figure 4: FortiEDR order status.

FortiEDR Collector Installation inside GCP

The collector installation process inside the Google Cloud is a little different when compared to regular FortiEDR deployments. Fortinet has automated most of the FortiEDR collector installation process using either OS-policy (recommended) or guest-policy methods available on GCP, but customers need to take care of some prerequisites inside their GCP projects for successful collector installation. Below is the list of parameters that customers need to set before initiating a script to install FortiEDR collectors:

1. Ensure users have the following IAM permissions:
   - osconfig.guestPolicies.create
   - osconfig.guestPolicies.delete
   - osconfig.guestPolicies.get
   - osconfig.guestPolicies.list
   - storage.buckets.create
   - storage.buckets.get
   - storage.objects.create
   - storage.objects.delete
2. Enable OS Configuration Management API and Compute API inside Google Cloud (GCP).
3. Enable OS configuration attributes for the specific project where one needs to deploy FortiEDR collectors (Figure 5).
   - enable-osconfig – TRUE
   - enable-oslogin – TRUE
   - enable-guest-attribute – TRUE

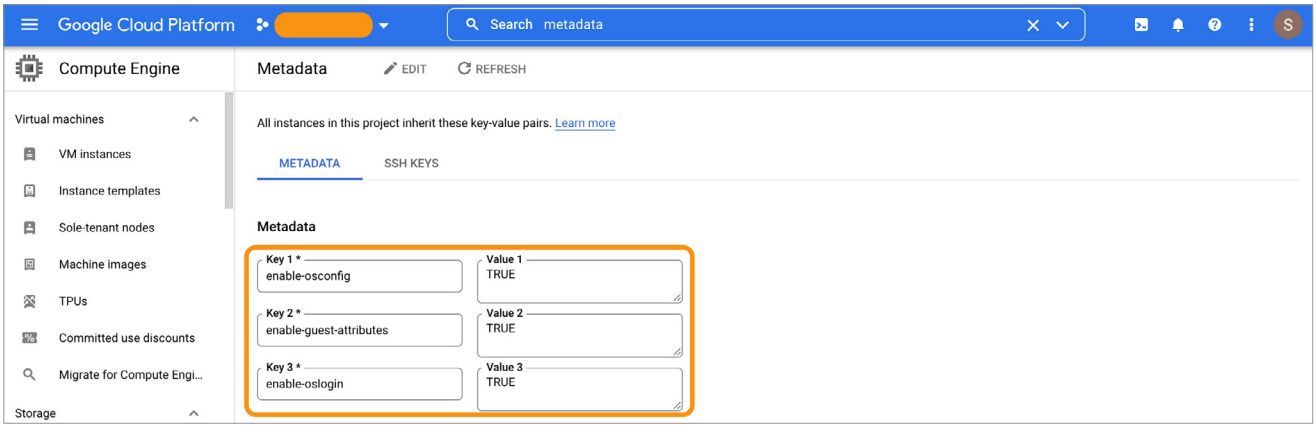


Figure 5: Required OS metadata attributes.

4. Add the FortiEDR Aggregator IP, Password, Port (default is 8081), and Organization inside the customer's Google Cloud Secret Manager with the values provided by the Fortinet in the activation email. The customer should use the same naming convention as shown in the below-given screenshot (Figure 6), as FortiEDR collector installation scripts will use these field names as variables to fetch the values from Secret Manager needed for collector installation.
5. To access the values from Secret Manager, the Compute Engine default service account (or service account of the target VM) should have read access to all of the secrets mentioned above.

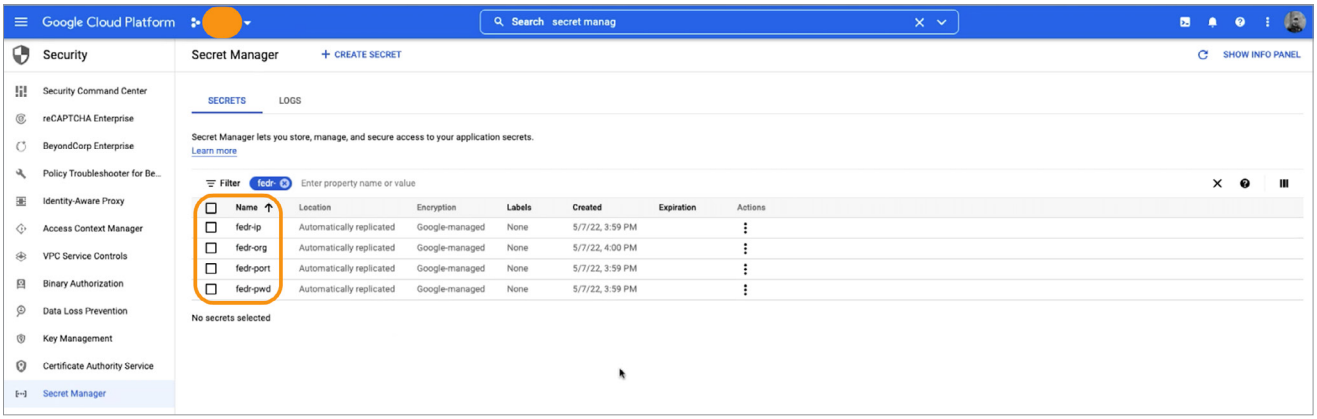


Figure 6: Fields with values to be added to Secret Manager.

6. Below are the steps to automate FortiEDR Collector installation using the OS configuration agent. (GCP documentation)

   6.1 Installation process utilizing OS policy:

   a. Download YAML files from the Google Cloud storage bucket, which will be used to create operating system policy for FortiEDR Collector images. Following are the links to download YAML files:

      i. https://storage.googleapis.com/fortiedr_bucket/OS-Policy/fedr-centos-os-policy.yml

      ii. https://storage.googleapis.com/fortiedr_bucket/OS-Policy/fedr-ubuntu-os-policy.yml

      iii. https://storage.googleapis.com/fortiedr_bucket/OS-Policy/fedr-windows-os-policy.yml

b. Download the shell script from below-given link and run it in the appropriate project to begin collector installation. It will create OS policy in all zones for a project that includes an inclusion-filter label “product: fortiedr” (Figure 7).

iii. https://storage.googleapis.com/fortiedr_bucket/OS-Policy/install_linux_collectors_all_zones.sh

iv. Make sure that new and existing VMs have the “product: fortiedr” label.

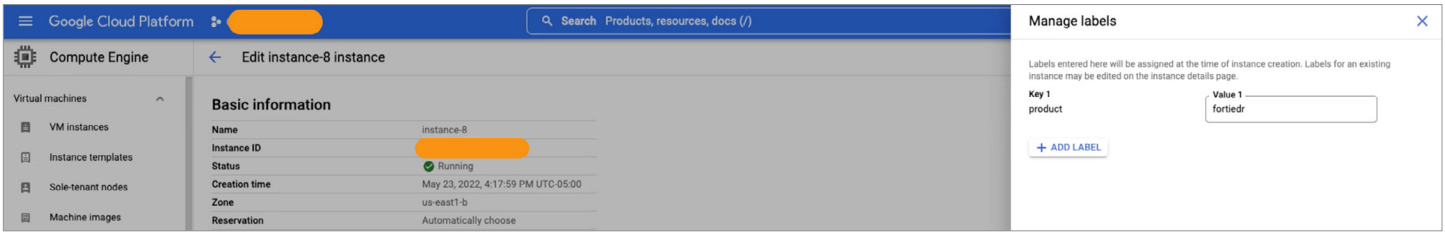


Figure 7: Product label.

6.2 Installation process using guest policy:

a. Download YAML files from the Google Cloud storage bucket, which will be used to create guest policy for FortiEDR Collector images. Below are the links to download YAML files:

i. https://storage.googleapis.com/fortiedr_bucket/Guest-Policy/fedr-centos-guest-policy.yml

ii. https://storage.googleapis.com/fortiedr_bucket/Guest-Policy/fedr-ubuntu-guest-policy.yml

b. Run below Google Cloud commands to install the guest policy:

i. gcloud beta compute os-config guest-policies create fedr-centos-guest-policy --file=fedr-centos-guest-policy.yml

ii. gcloud beta compute os-config guest-policies create fedr-ubuntu-guest-policy --file=fedr-ubuntu-guest-policy.yml

Resources

- Deploying Security Agents on GCP
- Permission to create OS Policy on GCP
- Viewing VM Manager Audit Logs
- Guest Policies:
  - https://cloud.google.com/compute/docs/os-config-management/create-guest-policy
  - https://cloud.google.com/compute/docs/os-config-management/manage-guest-policy

Copyright © 2022 Fortinet, Inc. All rights reserved. Fortinet®, FortiGate®, FortiCare® and FortiGuard®, and certain other marks are registered trademarks of Fortinet, Inc., and other Fortinet names herein may also be registered and/or common law trademarks of Fortinet. All other product or company names may be trademarks of their respective owners. Performance and other metrics contained herein were attained in internal lab tests under ideal conditions, and actual performance and other results may vary. Network variables, different network environments and other conditions may affect performance results. Nothing herein represents any binding commitment by Fortinet, and Fortinet disclaims all warranties, whether express or implied, except to the extent Fortinet enters a binding written contract, signed by Fortinet’s General Counsel, with a purchaser that expressly warrants that the identified product will perform according to certain expressly-identified performance metrics and, in such event, only the specific performance metrics expressly identified in such binding written contract shall be binding on Fortinet. For absolute clarity, any such warranty will be limited to performance in the same ideal conditions as in Fortinet’s internal lab tests. Fortinet disclaims in full any covenants, representations, and guarantees pursuant hereto, whether express or implied. Fortinet reserves the right to change, modify, transfer, or otherwise revise this publication without notice, and the most current version of the publication shall be applicable.

August 29, 2022 4:48 PM

1617944-0-0-EN