

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

🗄 Google Cloud 🔹 🦲 🚽			९ 🗷 🗍 🛛 🗄 🔞
Fortinet FortiEDR			VIEW ALL PLANS
OVERVIEW PRICING DOCUMENTAT			
You canceled your Fortinet FortiEDR service	e on 6/24/22.	MANAGE ORDERS	
Discover-Protect- Respond USD 767.00/mo + usage fee Subacription Period* 1 year - USD 767.00/mo + usa_ • SELECT	Discover-Protect- Respond-MDR USD 1,058.00/mo + usage fee Subscription Pariod* 1 year - USD 1,058.00/mo + usage fee 2 years - USD 1,058.00/mo + usage fee 3 years - USD 1,058.00/mo + usage fee		

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.

Associate GCP Fo	rtiEDR subscription with your FortiCloud account	
* DO NOT clear the browser cool	tie unless you have successfully logged in to FortiEDR Cloud.	
Step1.		
Register a FortiCloud account. Yo	u can access all of your Fortinet Cloud services through FortiCloud account.	
Skip this step if you already have	a FortiCloud account.	
Register →		
Step2.		
Log in to FortiCloud account. You	r GCP FortiEDR subscription will be automatically associated upon logging in.	
Login →		
Step3.		
Start protecting your applications	by onboarding them in FortiEDR Cloud.	

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.

≡ Google	Cloud Platfor	m								۹ ک.	•	0		
← Your orders VIEW BILLING REPORTS VIEW BILLING COMMITMENTS									rs 🧣	SEND	FEEDBAC	ск		
Select a billing account My Billing Account This page includes all orders for SaaS products made by Google Cloud Marketplace partners as well as your accepted private offers. Filter Filter by column name or chart value									Ø					
Status	Order number	Provider	Product	Plan	Next plan	Auto-renew	Purchase date 🛛 🕹	Start date	End date	Payment sched	ule			
Active	[TEST] 91b90b Г	Fortinet Inc.	Fortinet FortiEDR	Predict- Protect- Respond- MDR Two Year	N/A	On	05/11/2022	05/16/2022	05/16/2024	Postpay		:		

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 guestpolicy 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

=	Google Cloud Platform	*	Q Search metadata	× v	>	.	?	: (S)
۲	Compute Engine	Metadata 🖋 EDIT	C refresh					
Virtua	machines ^	All instances in this project inherit th	ese key-value pairs. <u>Learn more</u>					
B	VM instances	METADATA SSH KEYS						
	Instance templates							
8	Sole-tenant nodes	Metadata						
	Machine images	Key 1 * enable-osconfig	Value 1 TRUE					
2	TPUs	_ Key 2 *						
1%1	Committed use discounts	enable-guest-attributes	TRUE					
۹	Migrate for Compute Engi	Key 3 * enable-oslogin	Value 3 TRUE					
Storag	e ^							

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.

=	Google Cloud Platform	*	Q Search secret manag	x •)	2 · • · : 🌘							
0	Security	Secret Manager + CREATE SECRET			C SHOW INFO PANEL							
58	Security Command Center	SECRETS LOGS										
0	reCAPTCHA Enterprise											
C	BeyondCorp Enterprise	Secret Manager lets you store, manage, and secure access to your application secrets. Learn more										
٩	Policy Troubleshooter for Be	= Filter (fed- 0) Enter property name or value										
æ	Identity-Aware Proxy	□ Name ↑ Location Encryption	Labels Created E	xpiration Actions								
\odot	Access Context Manager	fedr-ip Automatically replicated Google-mana	ed None 5/7/22, 3:59 PM	:								
۲	VPC Service Controls	fedr-org Automatically replicated Google-mana	ed None 5/7/22, 4:00 PM	1								
Ø	Binary Authorization	fedr-port Automatically replicated Google-mana	ed None 5/7/22, 3:59 PM									
M	binary Autionzation	fedr-pwd Automatically replicated Google-mana	ed None 5/7/22, 3:59 PM	1								
ø	Data Loss Prevention	No secrets selected										
٢	Key Management											
0	Certificate Authority Service											
[]	Secret Manager											

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:

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

\equiv Google Cloud Platform	n 🛊 🦲 👘	Q Search	h Products, resources, docs (/)	Manage labels		×
Compute Engine	← Edit instance-8 instance			Labels entered here will be assigned at the instance may be edited on the instance det	time of instance creation. Labels for an existing alls page.	
Virtual machines	Basic information			Key 1 product	Value 1 fortiedr	
VM instances	Name	instance-8				
Instance templates	Instance ID			+ ADD LABEL		
(iii) instance templates	Status	Running				
Sole-tenant nodes	Creation time	May 23, 2022, 4:17:59 PM UTC-05:00				
	Zone	us-east1-b				
Machine images	Reservation	Automatically choose				

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



www.fortinet.com

Copyright © 2022 Fortinet, Inc., All rights reserved. Fortinet*, FortiGate*, FortiGate* 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 neutrics 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 waranies, whether express or implied, except to the extent Fortine tenters a binding written contract, signal dy Fortinets General Coursel, 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 darity, any such warranty will be limited to performance in the same ideal conditions as in Fortinets is 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