

Take command of your security in the cloud

How to use Cloud Security Command Center to prevent, detect, and respond to threats in your Google Cloud environment



Table of Contents

Introduction	01
Improve your cloud security posture with Cloud Security Command Center.....	02
Find and fix misconfigurations in your Google Cloud resources with Security Health Analytics	09
Catch web app vulnerabilities before they hit production with Cloud Web Security Scanner.....	12
Detect and remediate security anomalies with Cloud Anomaly Detection	15
Detect and respond to high-risk threats in your logs with Event Threat Detection.....	18
Stop data exfiltration with Cloud Data Loss Prevention.....	22

Introduction

How to use Cloud Security Command Center to prevent, detect, and respond to threats in your GCP environment

Traditionally, organizations have looked to the public cloud for cost savings, or to augment private data center capacity. However, with the cost of data breaches and the complexity of managing heterogeneous infrastructure constantly on the rise, organizations are now looking to the public cloud for security. After all, providers can invest more in people and processes to deliver secure infrastructure and applications than most individual organizations currently can.

Google Cloud provides a modern security infrastructure from the user, to the device, to the application, to the platform. This includes:

- A secure global platform to build and run applications with GCP
- Applications to collaborate in a secure environment and protect data with GSuite
- A single console to easily manage users, devices, and apps with Cloud Identity
- Secure endpoints and access platforms with Chrome and Android

At Google Cloud, we're committed to doing our part in keeping your data secure, but security is a shared responsibility and requires collaboration. Part of how we help you manage your portion of that responsibility is by providing best practices, templates, products, and solutions. This eBook will focus on Cloud Security Command Center (Cloud SCC), a built-in security control that can help you prevent, detect, and respond to threats in your GCP resources.

In this eBook, you'll find in-depth explanations of how to use Cloud Security Command Center and the security products that integrate into it. We take you step-by-step through important security issues—like how you can identify security misconfigurations or respond to threats in your logs—so you can take action before these issues result in business damage, data loss, or worse. We hope you enjoy this eBook, and look forward to talking with you about how Cloud Security Command Center can help you improve your cloud security posture.

Improve your cloud security posture with Cloud Security Command Center

One of the great benefits of cloud-based services is how easy they are to deploy. However, this ease of deployment can make it so your organization isn't always aware of exactly what services you're running.

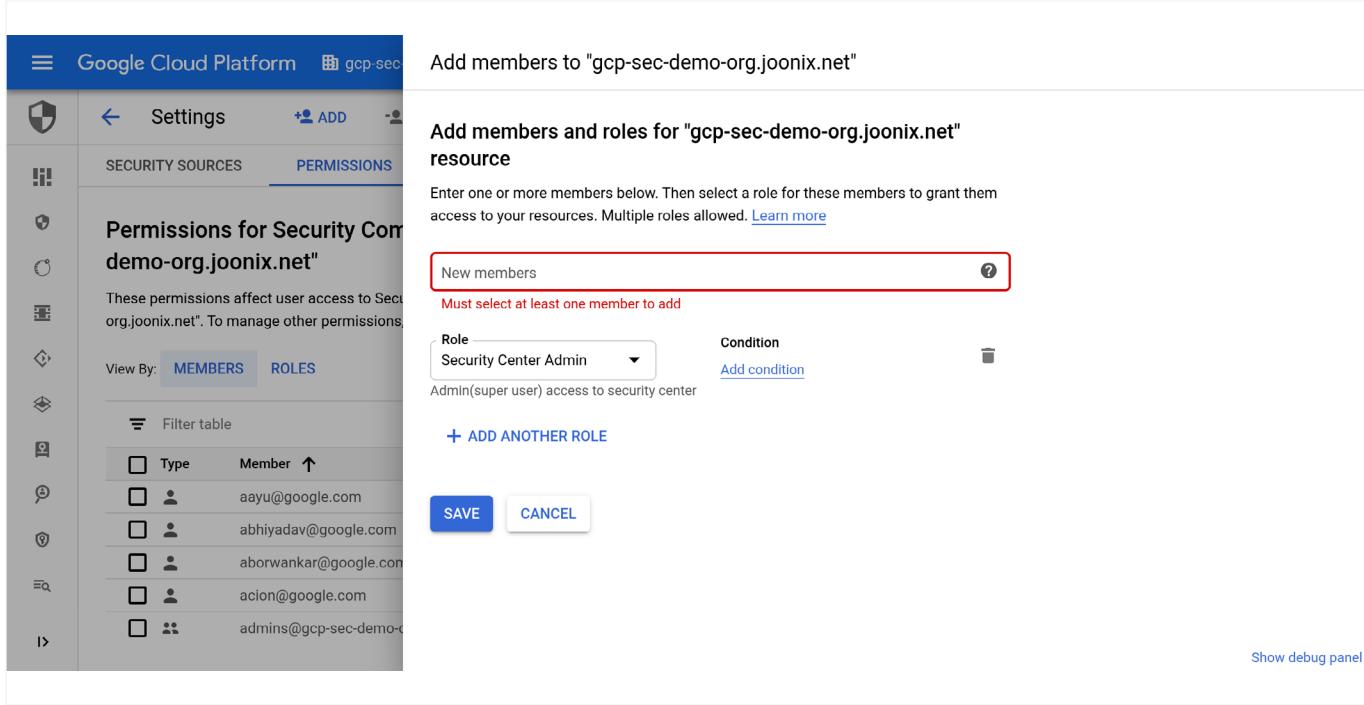
When you combine this with the increasing volume of cyber attacks, it becomes clear that you need to be able to see what resources you're running, the vulnerabilities and threats present, and how to fix them before they can result in damage or loss.

[Cloud Security Command Center](#) (Cloud SCC) helps you with all of these tasks by providing a centralized dashboard to help you prevent, detect, and respond to threats in your GCP environment. Once you've installed Cloud SCC, there are a number of great features available that you can use to improve your security posture in many ways, as we'll see in the other chapters of this book. Let's first get Cloud SCC ready to go, in five easy steps.



Step 1 / Set up Cloud IAM permissions

To use Cloud Security Command Center, someone in your organization needs to have the Security Center IAM role. This role provides access to Cloud SCC and ensures that users with the role assigned have the right level of permissions to complete their tasks.



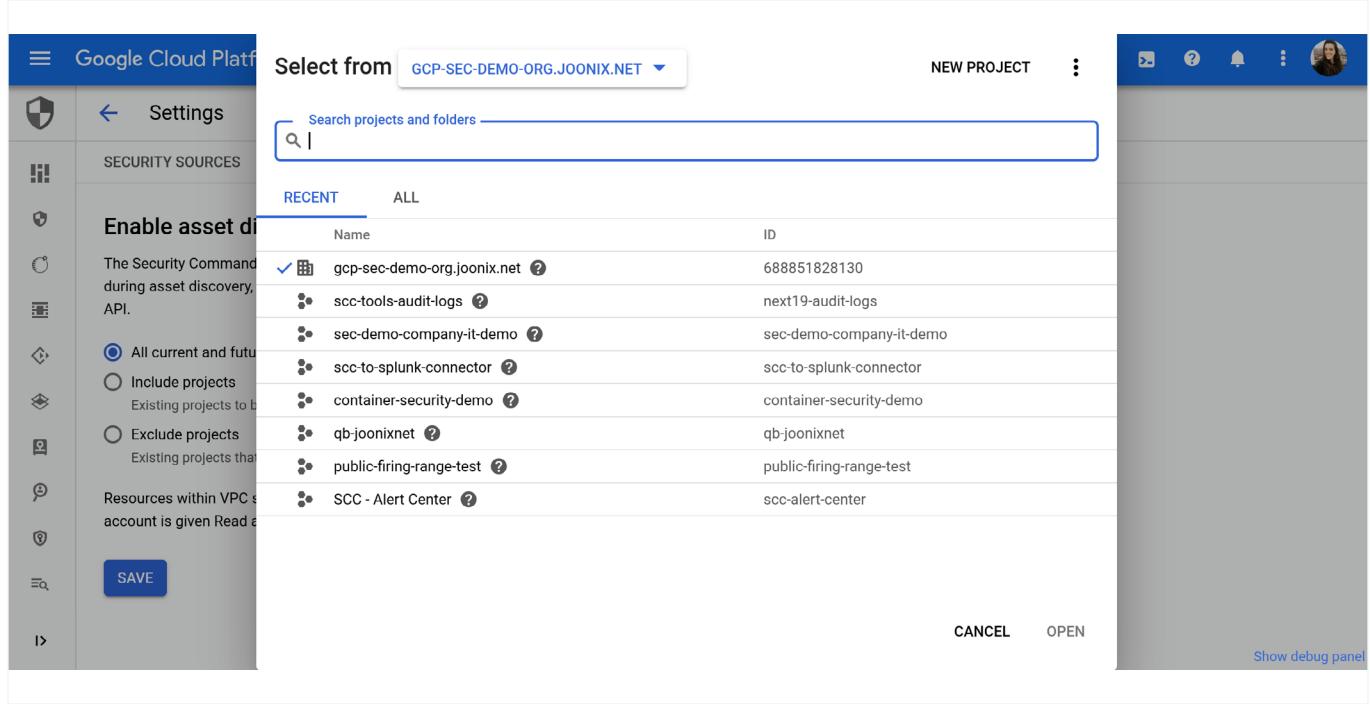
The screenshot shows the Google Cloud Platform IAM Permissions page for a security center resource. The left sidebar has a shield icon and lists various security-related services. The main panel title is "Add members to 'gcp-sec-demo-org.joonix.net'". It says "Add members and roles for 'gcp-sec-demo-org.joonix.net' resource". Below that, it says "Enter one or more members below. Then select a role for these members to grant them access to your resources. Multiple roles allowed." A red box highlights the "New members" input field, which contains "Must select at least one member to add". To the right of the input field are "Role" (set to "Security Center Admin") and "Condition" (with a link to "Add condition"). Below the input field, it says "Admin(super user) access to security center". At the bottom are "SAVE" and "CANCEL" buttons, and a link to "Show debug panel". On the far left, under "View By:", "MEMBERS" is selected. The table below lists members:

Type	Member
<input type="checkbox"/>	aayu@google.com
<input type="checkbox"/>	abhiyadav@google.com
<input type="checkbox"/>	aborwankar@google.com
<input type="checkbox"/>	acion@google.com
<input type="checkbox"/>	admins@gcp-sec-demo-

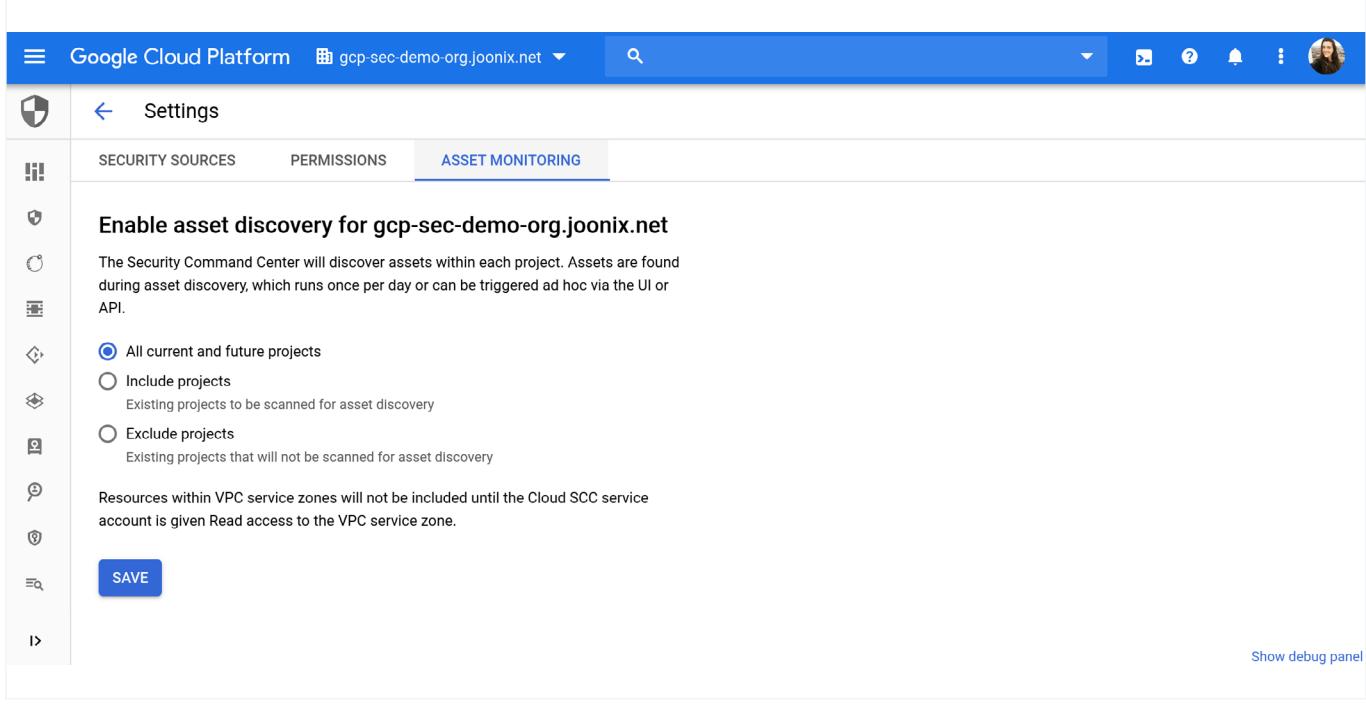
Set up Cloud IAM permissions

Step 2 / Enable Cloud Security Command Center

Cloud Security Command Center is not enabled by default, giving you the flexibility to choose where you want to use it. We recommend that you enable Cloud SCC for organizations running development, testing, and production workloads.



To enable Cloud SCC, you'll also need to turn on Asset Monitoring. This allows Cloud SCC to discover what GCP assets—our term for resources—you're running in Google Cloud.



The screenshot shows the Google Cloud Platform Security Command Center Asset Monitoring settings page. The top navigation bar includes the Google Cloud logo, the project name "gcp-sec-demo-org.joonix.net", a search bar, and various status icons. On the left, there's a sidebar with icons for different security features. The main content area has tabs for "SECURITY SOURCES", "PERMISSIONS", and "ASSET MONITORING", with "ASSET MONITORING" currently selected. A section titled "Enable asset discovery for gcp-sec-demo-org.joonix.net" contains instructions about asset discovery and three configuration options:

- All current and future projects
- Include projects
 - Existing projects to be scanned for asset discovery
- Exclude projects
 - Existing projects that will not be scanned for asset discovery

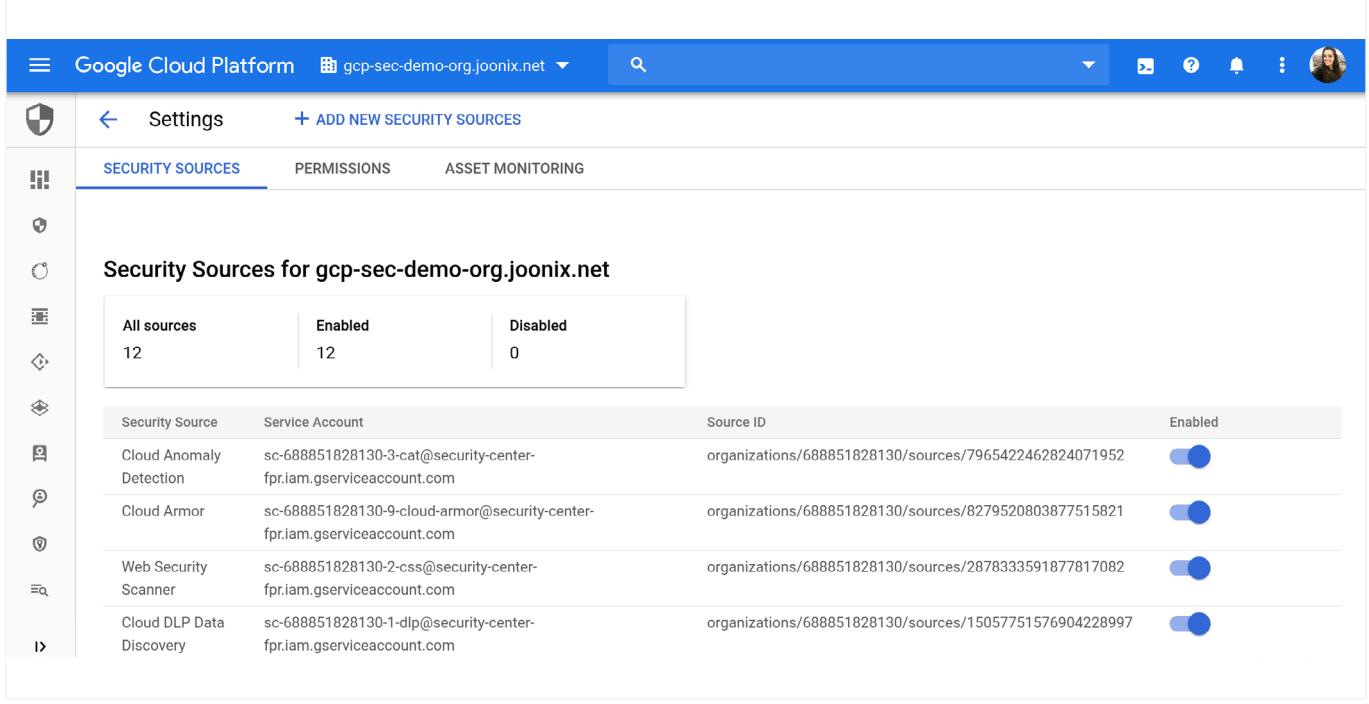
Below these options, a note states: "Resources within VPC service zones will not be included until the Cloud SCC service account is given Read access to the VPC service zone." At the bottom right of the main content area is a "SAVE" button.

Turn on Asset Monitoring

Step 3 / Turn on Security Sources

Once you've enabled Cloud SCC, you can toggle on our built-in features and products to see the security state of your GCP assets. These features and products can surface information such as misconfigured identity and access management policies, leaked credentials, or what storage buckets contain sensitive and regulated data.

We recommend that you turn on all our built-in capabilities and products to increase your visibility into misconfigurations, vulnerabilities, and threats in your environment.



Security Sources for gcp-sec-demo-org.joonix.net

All sources	Enabled	Disabled
12	12	0

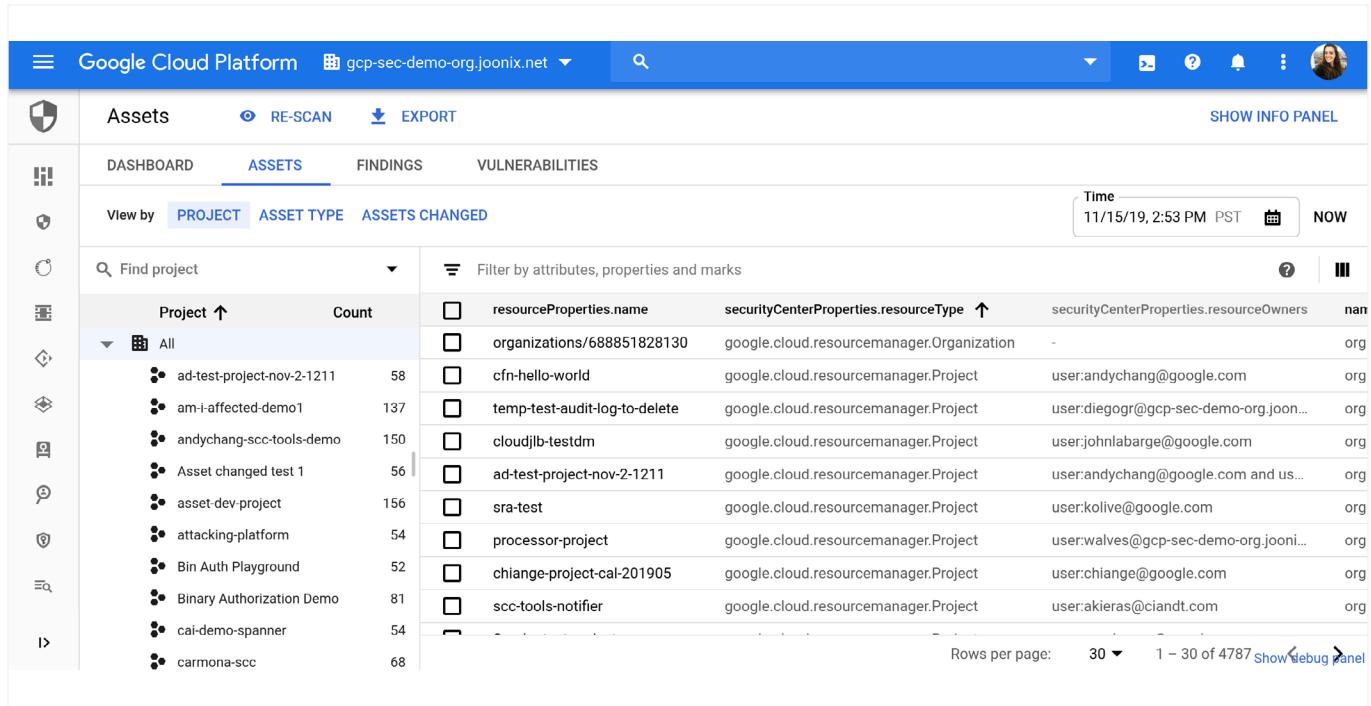
Security Source	Service Account	Source ID	Enabled
Cloud Anomaly Detection	sc-688851828130-3-cat@security-center-fpr.iam.gserviceaccount.com	organizations/688851828130/sources/7965422462824071952	<input checked="" type="checkbox"/>
Cloud Armor	sc-688851828130-9-cloud-armor@security-center-fpr.iam.gserviceaccount.com	organizations/688851828130/sources/8279520803877515821	<input checked="" type="checkbox"/>
Web Security Scanner	sc-688851828130-2-css@security-center-fpr.iam.gserviceaccount.com	organizations/688851828130/sources/2878333591877817082	<input checked="" type="checkbox"/>
Cloud DLP Data Discovery	sc-688851828130-1-dlp@security-center-fpr.iam.gserviceaccount.com	organizations/688851828130/sources/15057751576904228997	<input checked="" type="checkbox"/>

Enable Cloud SCC

Step 4 / View your security state by Assets

Now that you've turned on Cloud Security Command Center, Asset Monitoring, and Security Sources, you can see the security state of your GCP assets. Looking at your security state by project within Assets lets you see issues related to a specific project.

You can also view your security state by asset type. This lets you see the state of your organization at a specific time, or check out which assets have changed, so you can look for unauthorized modifications.



The screenshot shows the Google Cloud Platform Security Center Assets page. The top navigation bar includes the Google Cloud logo, the project name "gcp-sec-demo-org.joonix.net", a search bar, and various navigation icons. The main header has tabs for "DASHBOARD", "ASSETS" (which is selected), "FINDINGS", and "VULNERABILITIES". Below the header, there are filters for "View by" (PROJECT, ASSET TYPE, ASSETS CHANGED) and a timestamp "Time 11/15/19, 2:53 PM PST NOW". The main content area displays a table of assets. The columns include "Project ↑", "Count", "resourceProperties.name", "securityCenterProperties.resourceType ↑", and "securityCenterProperties.resourceOwners". The table lists numerous projects, such as "ad-test-project-nov-2-1211" (Count: 58), "am-i-affected-demo1" (Count: 137), and "carmonna-scc" (Count: 68). The table also includes a "Rows per page" dropdown set to 30 and a link to "Show 4787 more".

View your security state by asset type

Step 5 / View your security state by Findings

Findings are what Cloud SCC has discovered about your assets or resources.

You can filter your findings by type, the issue Cloud SCC discovered with your resource, or by source (the feature or product that found the issue). You can also filter findings based on time, so you can quickly gain insight into all the security issues surfaced at a particular time.

Google Cloud Platform gcp-sec-demo-org.joonix.net

Findings EXPORT SHOW INFO PANEL

DASHBOARD ASSETS FINDINGS VULNERABILITIES

View by CATEGORY SOURCE TYPE FINDINGS CHANGED Show Only Active Findings Time 11/15/19, 2:55 PM PST NOW

Find source type Filter by attributes, properties and marks

Source type ↑	Count	category	resourceName	eventTime ↓	createTime
All		<input type="checkbox"/> GCE VM Instance author:service-723325...	//compute.googleapis.com/projects/next1...	2019-11-15T22...	2019-11-15
Access Transparency	12	<input type="checkbox"/> GCE VM Instance author:service-723325...	//compute.googleapis.com/projects/next1...	2019-11-15T22...	2019-11-15
Audit Logs	186879	<input type="checkbox"/> BinAuthz blocked deployment attempt	//container.googleapis.com/projects/binar...	2019-11-15T22...	2019-11-15
Binary Authorization	13	<input type="checkbox"/> GCE VM Instance author:service-723325...	//compute.googleapis.com/projects/next1...	2019-11-15T22...	2019-11-15
Cloud Anomaly Detection	12	<input type="checkbox"/> BinAuthz blocked deployment attempt	//container.googleapis.com/projects/binar...	2019-11-15T22...	2019-02-27
Cloud DLP Data Discovery	70	<input type="checkbox"/> GCE VM Instance author:service-723325...	//compute.googleapis.com/projects/next1...	2019-11-15T22...	2019-11-15
CloudGuard Dome9 integration for Clou...	1	<input type="checkbox"/> GCE VM Instance author:service-723325...	//compute.googleapis.com/projects/next1...	2019-11-15T22...	2019-11-15
Event Threat Detection	49	<input type="checkbox"/> GCE VM Instance author:service-723325...	//compute.googleapis.com/projects/next1...	2019-11-15T22...	2019-11-15
Phishing Protection	3276	<input type="checkbox"/> GCE VM Instance author:service-723325...	//compute.googleapis.com/projects/next1...	2019-11-15T22...	2019-11-15
Qualys Cloud Security for SCC	27	<input type="checkbox"/> GCE VM Instance author:service-723325...	//compute.googleapis.com/projects/next1...	2019-11-15T22...	2019-11-15
Reblaze	80447	<input type="checkbox"/> GCE VM Instance author:service-723325...	//compute.googleapis.com/projects/next1...	2019-11-15T22...	2019-11-15

Rows per page: 30 ▾ 1 – 30 of 276093 Show debug panel

View your security state by findings

How to use Cloud SCC

Watch the video now.



Find and fix misconfigurations in your Google Cloud resources with Security Health Analytics

When you deploy new Google Cloud services, you need visibility into what's running and how you can improve their security. If you don't have that visibility, your organization might not be aware of risky misconfigurations that leave you susceptible to attacks.

To help you find misconfigurations, and respond quickly to them, we developed [Security Health Analytics](#), and built it into Cloud SCC. Security Health Analytics gives you visibility into misconfigurations in your GCP resources and provides actionable recommendations for how to fix them. In this chapter, and the accompanying video, we'll take a closer look at Security Health Analytics.

Step 1 / Enable Security Health Analytics

Since Security Health Analytics is built in to Cloud SCC, to use it you just need to have one of two roles: the Organization Administrator Cloud Identity and Access Management (Cloud IAM) role or the Security Center IAM role.

Step 2 / View different types of misconfigurations

The Security Health Analytics card lists its findings and the types of misconfigurations present in your environment, and can be accessed directly from the Vulnerabilities dashboard in Cloud SCC. And there is a long list of vulnerabilities Security Health Analytics can identify, including:

- Firewall rules that are configured to be open to public access
- Cloud Storage buckets that are publicly accessible
- Instances configured with public IP addresses
- Instances with SSL not being enforced
- Resources where the Web UI isn't enabled

You can find the full list of potential findings in the [documentation](#).

Security Health Analytics

3,885 current findings

Finding	Count
!! OPEN_FIREWALL	9
!! PUBLIC_BUCKET_ACL	8
!! PUBLIC_IP_ADDRESS	56
!! SSL_NOT_ENFORCED	4
!! WEB_UI_ENABLED	6

+47 More

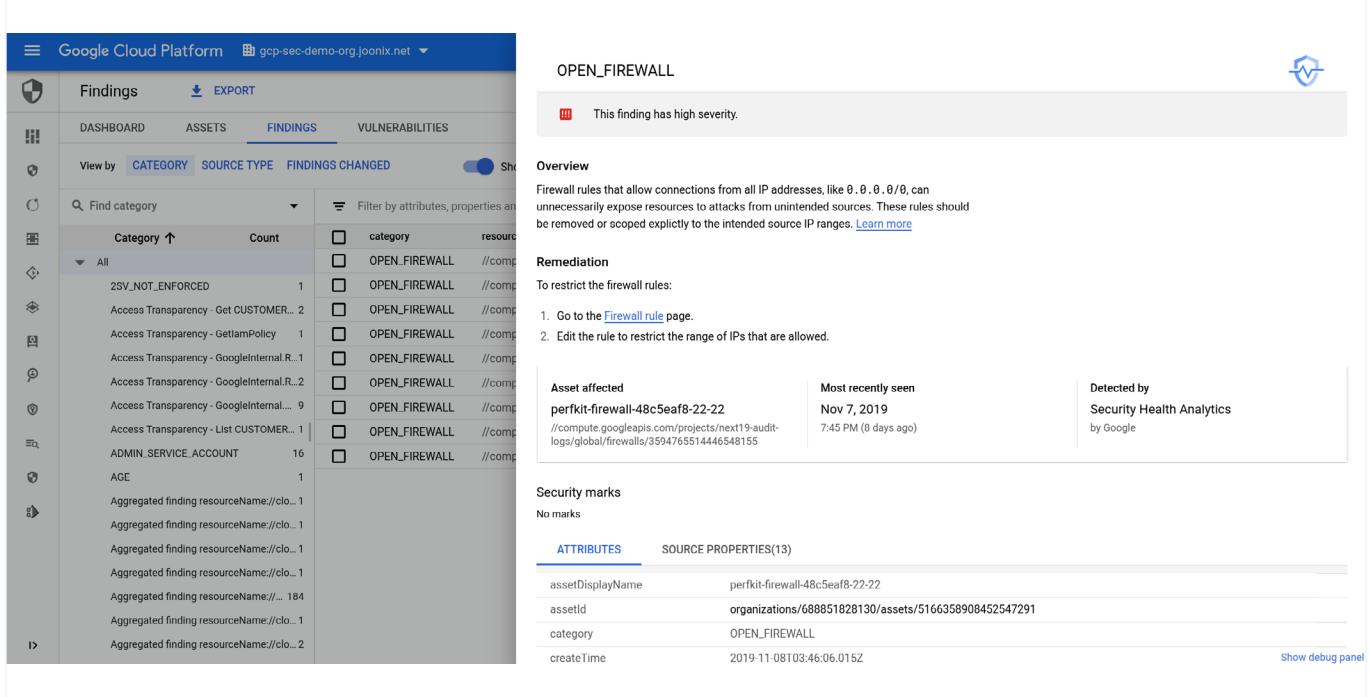


View different types of misconfigurations

Step 3 / Take action on a misconfiguration

When you click on a finding, you get a short description of the issue, as shown in the diagram below. This description includes the GCP asset or resource impacted, how it was detected, an overview of the issue, and even a step-by-step recommendation on how to fix it.

The recommendation, under the “Remediation” heading, provides a link to the impacted resource. Once there, all you need to do is follow the recommendations and click save.



The screenshot shows the Google Cloud Platform Security Health Analytics interface. On the left, there's a sidebar with various icons and a main dashboard area. The main area has tabs for 'Findings' (selected), 'Assets', 'Findings' (selected), and 'Vulnerabilities'. Below these tabs, there are filters for 'View by' (Category, Source Type, Findings Changed) and a search bar ('Find category'). A table lists findings categorized by 'Category' and 'Count'. One entry is expanded to show details for an 'OPEN_FIREWALL' rule.

OPEN_FIREWALL

This finding has high severity.

Overview

Firewall rules that allow connections from all IP addresses, like 0.0.0.0/0, can unnecessarily expose resources to attacks from unintended sources. These rules should be removed or scoped explicitly to the intended source IP ranges. [Learn more](#)

Remediation

To restrict the firewall rules:

1. Go to the [Firewall rule page](#).
2. Edit the rule to restrict the range of IPs that are allowed.

Asset affected	Most recently seen	Detected by
perfkit-firewall-48c5eaf8-22-22 //compute.googleapis.com/projects/next19-audit-logs/global/firewalls/3594765514446548155	Nov 7, 2019 7:45 PM (8 days ago)	Security Health Analytics by Google

Security marks
No marks

ATTRIBUTES **SOURCE PROPERTIES(13)**

assetDisplayName	perfkit-firewall-48c5eaf8-22-22
assetId	organizations/688851028130/assets/5166358908452547291
category	OPEN_FIREWALL
createTime	2019-11-08T03:46:06.015Z

Show debug panel

Take action on a misconfiguration

How to use Security Health Analytics

Watch the video now.

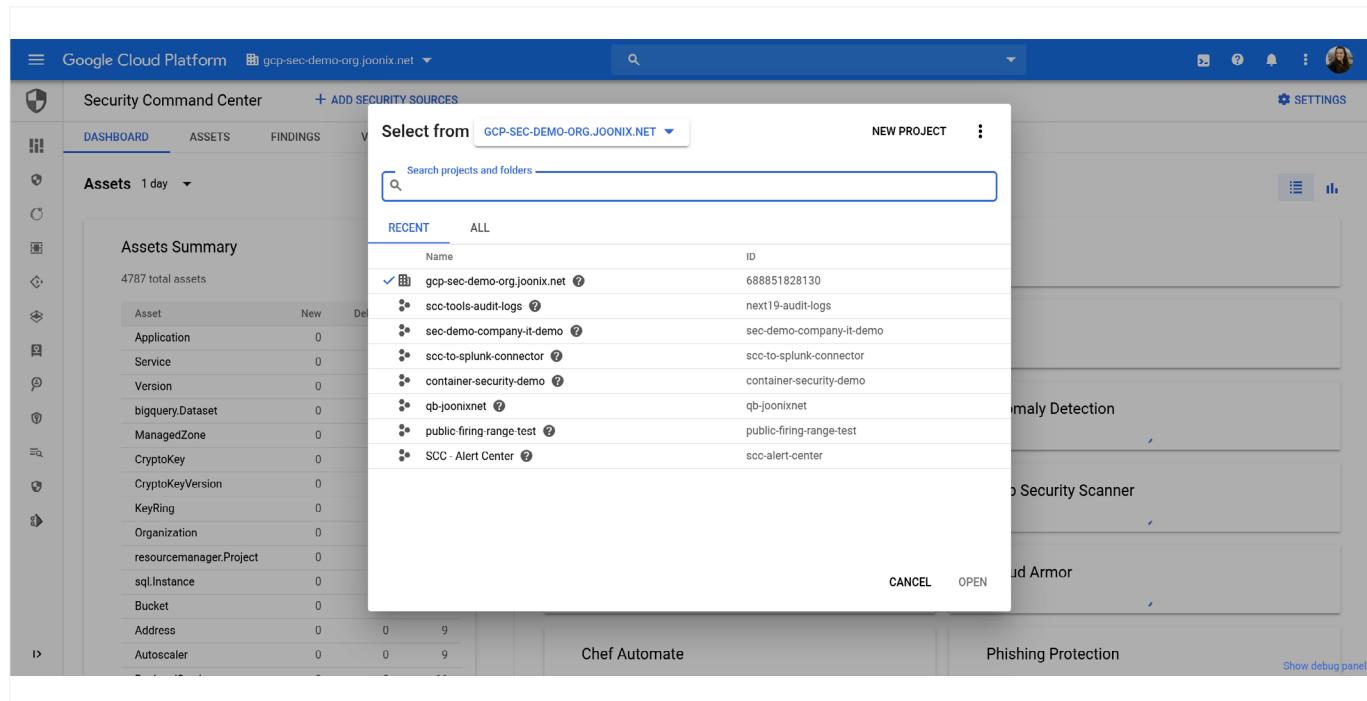


Catch web app vulnerabilities before they hit production with Cloud Web Security Scanner

Today's web applications are developed at a rapid pace, and that pace is only getting faster. This makes it difficult to know if your web apps have vulnerabilities and how to fix them before they hit production. We recognize this problem, and it's why we developed Cloud Web Security Scanner, a built-in feature in Cloud SCC that allows you to detect vulnerabilities—including cross-site scripting or outdated libraries—in GKE, Compute Engine, and App Engine. In this chapter, we'll walk through how to get started with Cloud Web Security Scanner so you can start reducing your web app vulnerabilities.

Step 1 / Enable Cloud Web Security Scanner

Cloud Web Security Scanner isn't turned on by default, so the first step is to enable it. In the Google Cloud Platform Console, visit the Cloud Security Command Center page, choose an organization for Cloud Web Security Scanner, and select the project within that organization that you want to use it on. If you haven't already enabled the Cloud Web Security Scanner API, you'll be prompted to do it here.



The screenshot shows the Google Cloud Platform Security Command Center (SCC) interface. The left sidebar contains various security icons. The main navigation bar includes 'Google Cloud Platform', the project name 'gcp-sec-demo-org.joonix.net', a search bar, and user profile information. The 'ASSETS' tab is selected under the 'DASHBOARD' section. A modal window titled 'Select from' is open, showing a dropdown menu for 'GCP-SEC-DEMO-ORG.JOONIX.NET' and a search bar. Below the dropdown, there are two tabs: 'RECENT' and 'ALL'. A list of assets is displayed with columns for 'Name' and 'ID'. One asset, 'gcp-sec-demo-org.joonix.net', has a checked checkbox next to it. Other assets listed include 'scc-tools-audit-logs', 'sec-demo-company-it-demo', 'scc-to-splunk-connector', 'container-security-demo', 'qb-joonixnet', 'public-firing-range-test', and 'SCC - Alert Center'. At the bottom of the modal are 'CANCEL' and 'OPEN' buttons. The background of the main interface shows sections for 'Vulnerability Detection', 'Cloud Web Security Scanner', and 'Cloud Armor'.

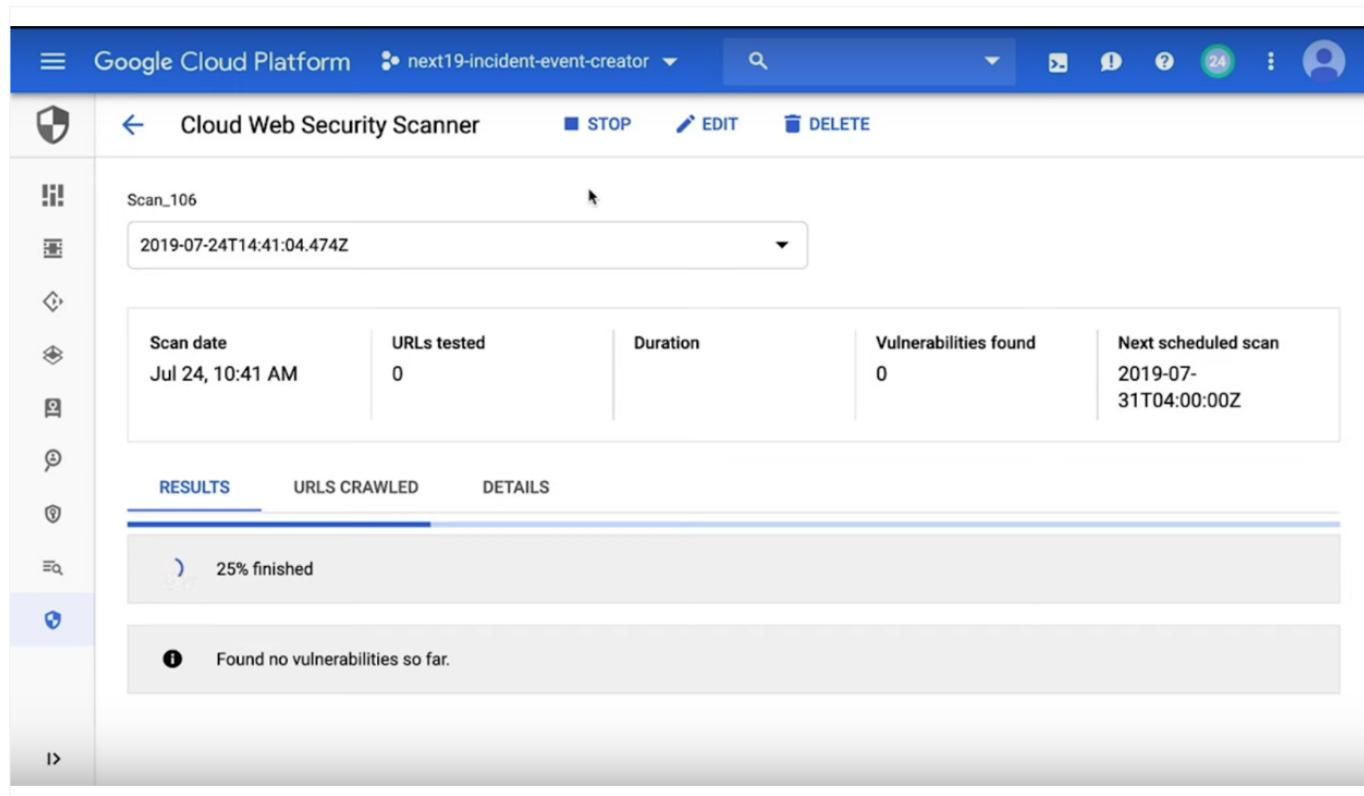
Enable Cloud Web Security Scanner

Step 2 / Create, save, and run scans

Cloud Web Security Scanner allows you to create, save, and run scans to detect key vulnerabilities in development before they're pushed to production.

To create a scan, add the url of the application you'd like to test, then save it by visiting the scan's configuration page—where you can also find out more information about the scan, its history, and the controls for editing it. When you want to run a scan, just schedule the time you want it to run from the Cloud Web Security Scanner page.

Once you've completed these steps, Cloud Web Security Scanner will automatically crawl your application—following all the links within the scope of your starting URLs—and attempt to exercise as many user inputs and event handlers as possible. When the scan is done, it will show any vulnerabilities it detected.



Scan_106

2019-07-24T14:41:04.474Z

Scan date	URLs tested	Duration	Vulnerabilities found	Next scheduled scan
Jul 24, 10:41 AM	0	0	0	2019-07-31T04:00:00Z

RESULTS URLs CRAWLED DETAILS

25% finished

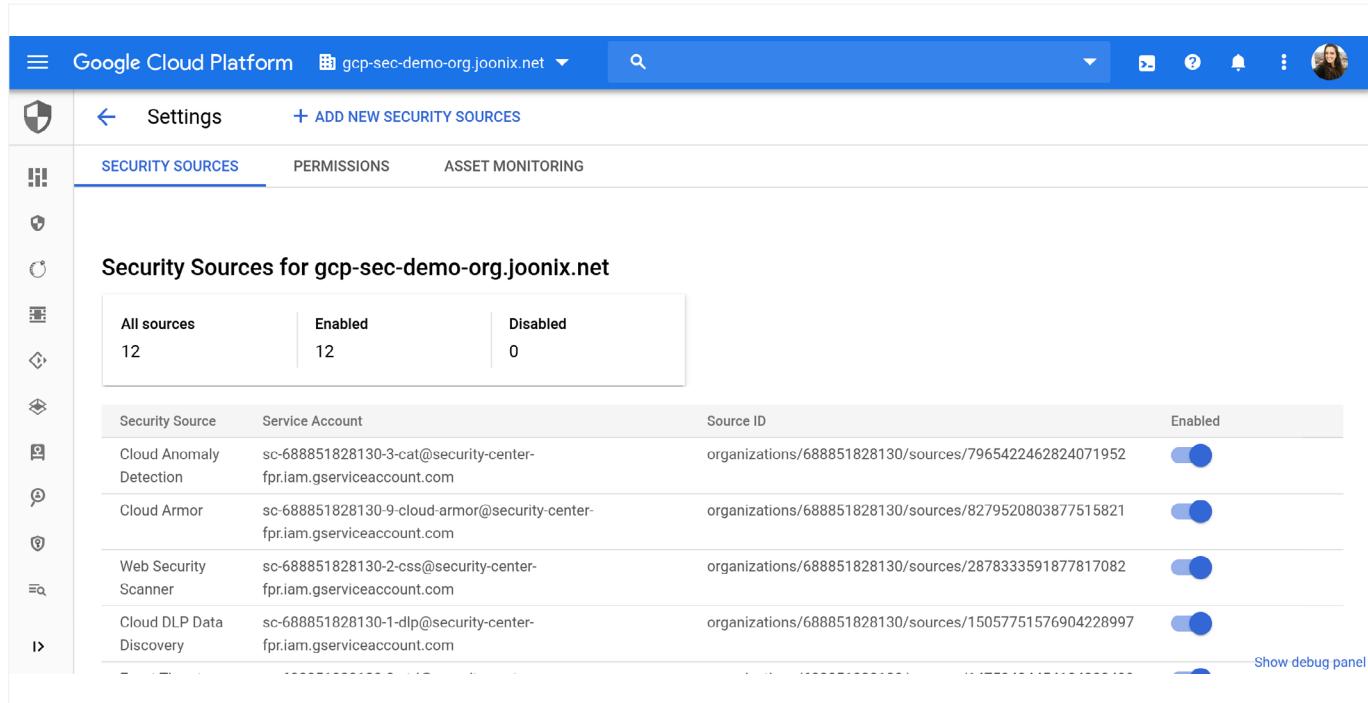
Found no vulnerabilities so far.

View your findings and fix them

Step 3 / View your findings and fix them

After you've turned on Cloud Web Security Scanner and run your scans, you can also use it to explore the findings (results). It can identify many common web vulnerabilities on these pages, including Flash injection and mixed content.

In addition to using the Cloud Web Security Scanner page, you can enable Cloud Web Security Scanner under Security Sources and view your findings directly on the Cloud Security Command Center dashboard. This lets you see findings from Cloud Web Security Scanner, and other built-in security features, in one place to get a holistic look into your security posture in GCP. Just click on a finding to bring up more information about the issue and how to fix it.



The screenshot shows the Google Cloud Platform Security Sources interface. At the top, there's a navigation bar with the Google Cloud Platform logo, the project name "gcp-sec-demo-org.joonix.net", a search bar, and various icons for settings and notifications. Below the navigation bar, the left sidebar has icons for shield, network, identity, logs, monitoring, and security. The "SECURITY SOURCES" tab is selected, while "PERMISSIONS" and "ASSET MONITORING" are also listed. The main content area is titled "Security Sources for gcp-sec-demo-org.joonix.net". It shows a summary table with three rows: "All sources" (12), "Enabled" (12), and "Disabled" (0). Below this, a detailed table lists five security sources, each with its name, service account, source ID, and an "Enabled" toggle switch. The sources listed are Cloud Anomaly Detection, Cloud Armor, Web Security Scanner, and Cloud DLP Data Discovery. At the bottom right of the table, there's a link "Show debug panel".

View your findings and fix them

How to use Cloud Web Security Scanner



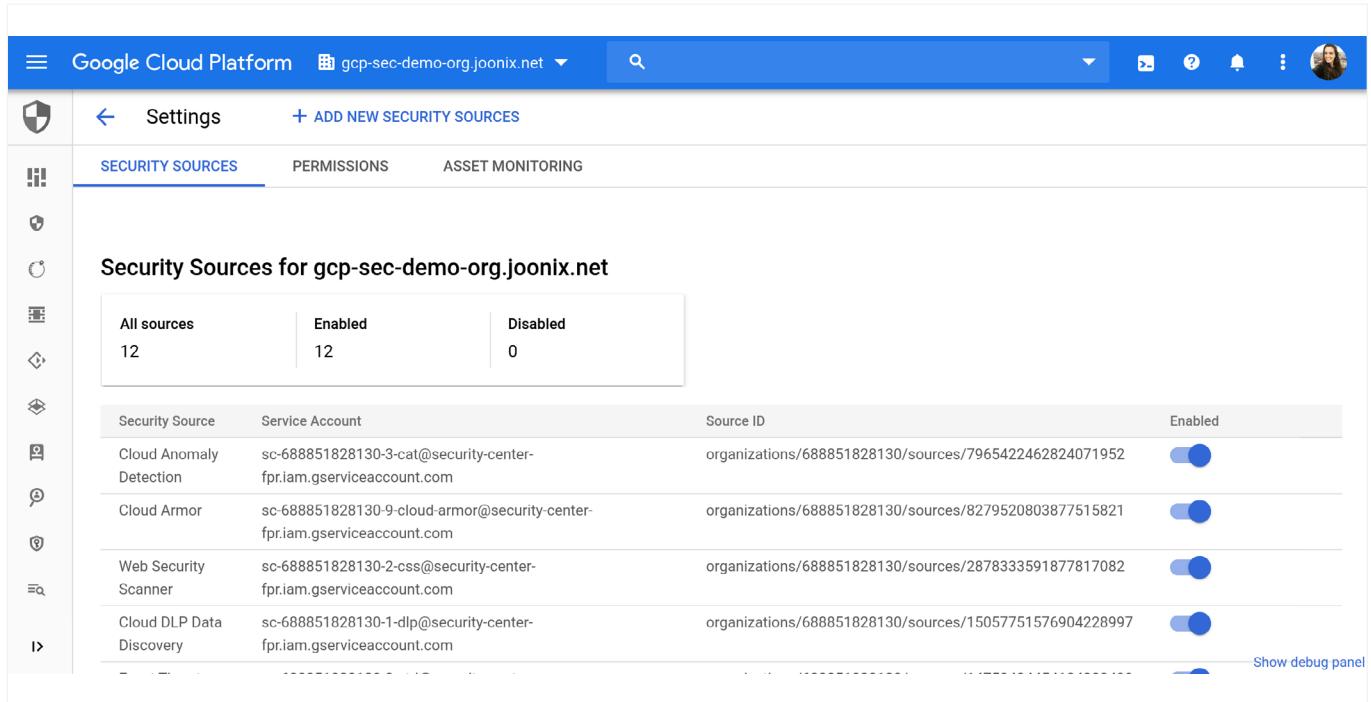
[Watch video now.](#)

Detect and remediate security anomalies with Cloud Anomaly Detection

When a threat is detected, every second counts. But, sometimes it can be difficult to know if a threat is present or how to respond. Cloud Anomaly Detection is another built-in Cloud SCC feature that uses behavioral signals to detect security abnormalities, such as leaked credentials or unusual activity, in your GCP projects and virtual machines. In this chapter, we'll look at how to enable Cloud Anomaly Detection and quickly respond to threats.

Step 1 / Enable Cloud Anomaly Detection from Cloud Security Command Center

Cloud Anomaly Detection is not turned on by default. You need to go to Security Sources from the Cloud SCC dashboard and activate it. Keep in mind, to enable a security source, you need to have the Organization Administrator Cloud IAM role. Once its turned on, findings will automatically be surfaced and displayed in the Cloud Anomaly Detection card on the Cloud Security Command Center dashboard.



The screenshot shows the Google Cloud Platform Cloud Security Command Center (Cloud SCC) interface. The top navigation bar includes the Google Cloud Platform logo, the project name "gcp-sec-demo-org.joonix.net", a search bar, and various navigation icons. The main menu on the left has "Settings" selected, and there are tabs for "SECURITY SOURCES", "PERMISSIONS", and "ASSET MONITORING".

The "SECURITY SOURCES" section displays a summary table:

All sources	Enabled	Disabled
12	12	0

Below this, a list of security sources is shown:

Security Source	Service Account	Source ID	Enabled
Cloud Anomaly Detection	sc-688851828130-3-cat@security-center-fpr.iam.gserviceaccount.com	organizations/688851828130/sources/7965422462824071952	<input checked="" type="checkbox"/>
Cloud Armor	sc-688851828130-9-cloud-armor@security-center-fpr.iam.gserviceaccount.com	organizations/688851828130/sources/8279520803877515821	<input checked="" type="checkbox"/>
Web Security Scanner	sc-688851828130-2-css@security-center-fpr.iam.gserviceaccount.com	organizations/688851828130/sources/2878333591877817082	<input checked="" type="checkbox"/>
Cloud DLP Data Discovery	sc-688851828130-1-dlp@security-center-fpr.iam.gserviceaccount.com	organizations/688851828130/sources/15057751576904228997	<input checked="" type="checkbox"/>

A "Show debug panel" link is located at the bottom right of the table.

Enable Cloud Anomaly Detection from Cloud Security Command Center

Step 2 / View findings in Cloud Security Command Center

Cloud Anomaly Detection can surface a variety of anomalous findings, including:

- **Leaked service account credentials:** GCP service account credentials that are accidentally leaked online or compromised.
- **Resource used for outbound intrusion:** One of the resources or GCP services in your organization is being used for intrusion activities, like an attempt to break in to or compromise a target system. These include SSH brute force attacks, Port scans, and FTP brute force attacks.
- **Potential compromised machine:** A potential compromise of a resource in your organization.
- **Resource used for crypto mining:** Behavioral signals around a VM in your organization indicate that it might have been compromised and could be getting used for crypto mining.
- **Unusual Activity/Connection:** Unusual activity from a resource in your organization.
- **Resource used for phishing:** One of the resources or GCP services in your organization is being used for phishing.

Step 3 / Remediate findings from Cloud Security Command Center

After Cloud Anomaly Detection generates a finding, you can click on the finding for more information about what happened and use that information to fix the security issue.

Google Cloud Platform gcp-sec-demo-org.joonix.net

Settings + ADD NEW SECURITY SOURCES

SECURITY SOURCES PERMISSIONS ASSET MONITORING

Security Sources for gcp-sec-demo-org.joonix.net

All sources	Enabled	Disabled
12	12	0

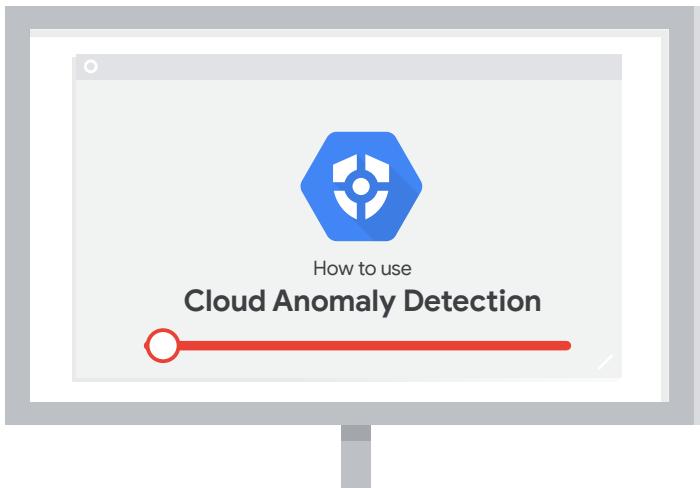
Security Source	Service Account	Source ID	Enabled
Cloud Anomaly Detection	sc-688851828130-3-cat@security-center-fpr.iam.gserviceaccount.com	organizations/688851828130/sources/7965422462824071952	<input checked="" type="checkbox"/>
Cloud Armor	sc-688851828130-9-cloud-armor@security-center-fpr.iam.gserviceaccount.com	organizations/688851828130/sources/8279520803877515821	<input checked="" type="checkbox"/>
Web Security Scanner	sc-688851828130-2-css@security-center-fpr.iam.gserviceaccount.com	organizations/688851828130/sources/2878333591877817082	<input checked="" type="checkbox"/>
Cloud DLP Data Discovery	sc-688851828130-1-dlp@security-center-fpr.iam.gserviceaccount.com	organizations/688851828130/sources/15057751576904228997	<input checked="" type="checkbox"/>

Show debug panel

View your findings and fix them

How to use Cloud Anomaly Detection

Watch the video now.



Detect and respond to high-risk threats in your logs with Event Threat Detection

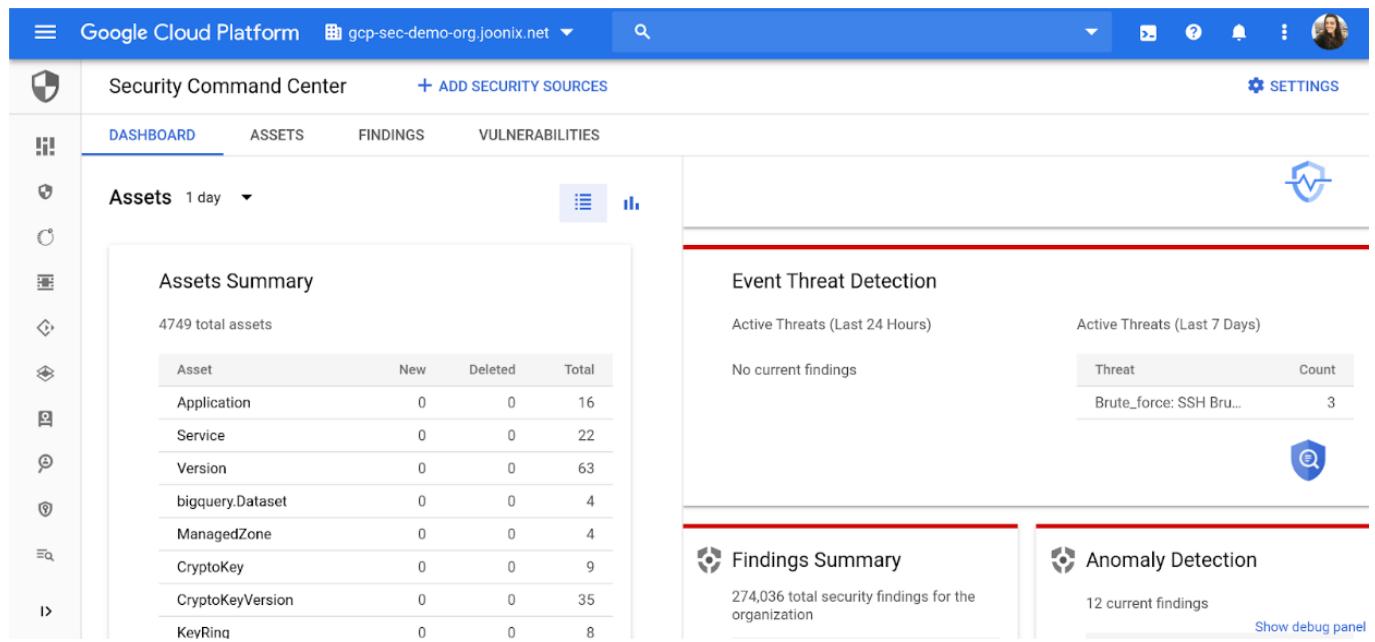
Data breaches aren't only getting more frequent, they're getting more expensive. With regulatory and compliance fines, and business resources being allocated to remediation, the costs from a data breach can quickly add up. In fact, the average total cost of a [data breach in the U.S.](#) has risen to \$3.92 million, 1.5% more expensive than in 2018, and 12% more expensive than five years ago, according to IBM.

[Event Threat Detection](#), another built-in feature of Cloud SCC, can notify you of high-risk and costly threats in your logs and help you respond. Let's learn more about it.

Step 1 / Enable Event Threat Detection

Once you're onboard, Event Threat Detection will appear as a card on the Cloud SCC dashboard.

Event Threat Detection works by consuming Cloud Audit, VPC flow, Cloud DNS, and Syslog via fluentd logs and analyzing them with our threat detection logic and Google's threat intelligence. When it detects a threat, Event Threat Detection writes findings (results) to Cloud SCC and to a logging project. For this blog and video, we'll focus on the ETD findings available in Cloud SCC.



The screenshot shows the Google Cloud Platform Security Command Center (SCC) interface. On the left, there's a sidebar with various icons for security features like Cloud Audit, VPC Flow, Cloud DNS, and Cloud Logging. The main dashboard has tabs for DASHBOARD, ASSETS, FINDINGS, and VULNERABILITIES. The DASHBOARD tab is selected. On the left under ASSETS, there's a summary for 4749 total assets, including a table for Application, Service, Version, bigquery.Dataset, ManagedZone, CryptoKey, CryptoKeyVersion, and KeyRing. To the right, there are several cards: one for Event Threat Detection showing 'No current findings' and threat counts (e.g., Brute_force: SSH Bru... 3), one for Findings Summary (274,036 total security findings), and one for Anomaly Detection (12 current findings). A red bar highlights the Event Threat Detection card.

Asset	New	Deleted	Total
Application	0	0	16
Service	0	0	22
Version	0	0	63
bigquery.Dataset	0	0	4
ManagedZone	0	0	4
CryptoKey	0	0	9
CryptoKeyVersion	0	0	35
KeyRing	0	0	8

Enable Cloud Anomaly Detection from Cloud Security Command Center

Step 2 / Detecting threats

Here are the threats ETD can detect in your logs, and how they work:

- **Brute force SSH:** ETD detects the brute force of SSH by examining Linux Auth logs for repeated failures followed by success.
- **Cryptomining:** ETD detects coin mining malware by examining VPC logs for connections to known bad domains for mining pools and other log data.
- **Cloud IAM abuse Malicious grants:** ETD detects the addition of accounts from outside of your organization's domain that are given Owner or Editor permission at the organization or project level.
- **Malware:** ETD detects Malware in a similar fashion to crypto mining, as it examines VPC logs for connections to known bad domains and other log data.
- **Phishing:** ETD detects Phishing by examining VPC logs for connections and other log data.
- **Outgoing DDoS, port-scanning:** ETD detects DDoS attacks originating inside your organization by looking at the sizes, types, and numbers of VPC flow logs. Outgoing DDoS is a common use of compromised instances and projects by attackers. Port scanning is a common indication of an attacker getting ready for lateral movement in a project.

Step 3 / Respond to threats

When a threat is detected, you can see when it happened—either in the last 24 hours or last 7 days—and how many times it was detected, via the count.

Event Threat Detection

374 total security findings

Active threats (last 24 hours)			Active threats (last 7 days)		
Threat	Severity	Count	Type	Severity	Count
Malware: domain		8	Malware: domain		52
Cryptomining: IP		4	Malware: IP		37
Malware: hash		4	Malware: hash		32
Brute force: SSH		2	IAM: anomalous grant		11
+4 more			+4 more		

Respond to threats

When you click on a finding, you can see what the event was, when it occurred, and what source the data came from. This information saves time and lets you focus on remediation.

Finding Details

Summary

Finding type Persistence: iam Anomalous Grant	First discovered Apr 3, 2019 2:59 PM (Apr 3, 2019)	Most recently seen Aug 22, 2019 11:25 AM (Aug 22, 2019)	Source
---	---	--	---------------

Security marks

etd_status : inactive score : 70

ATTRIBUTES
SOURCE PROPERTIES(10)

Attribute	Value
evidence_0_sourceLogId_timestamp	2019-04-03T21:58:51.603Z
detectionPriority	HIGH
detectionCategory_technique	persistence
sourceld_customerOrganizationNumber	688851828130
detectionCategory_ruleName	iam_anomalous_grant
evidence_0_sourceLogId_insertId	-4fqgx1ceva
properties_project_id	next19-target-232915
detectionCategory_indicator	audit_log
eventTime	2019-04-03T21:59:17.697Z
sourceld_projectNumber	291523997950

Event Threat Detection

To further investigate a threat detected by Event Threat Detection, you can send your logs to a SIEM. Because Event Threat Detection has already processed your logs, you can send only high value incidents to your SIEM, saving time and money.

You can use a Splunk connector to export these logs. Splunk automatically sorts your key issues—you can see events and categories—so you can investigate further and follow the prescribed steps.

How to use Event Threat Detection



[Watch the video now.](#)

Stop data exfiltration with Cloud Data Loss Prevention

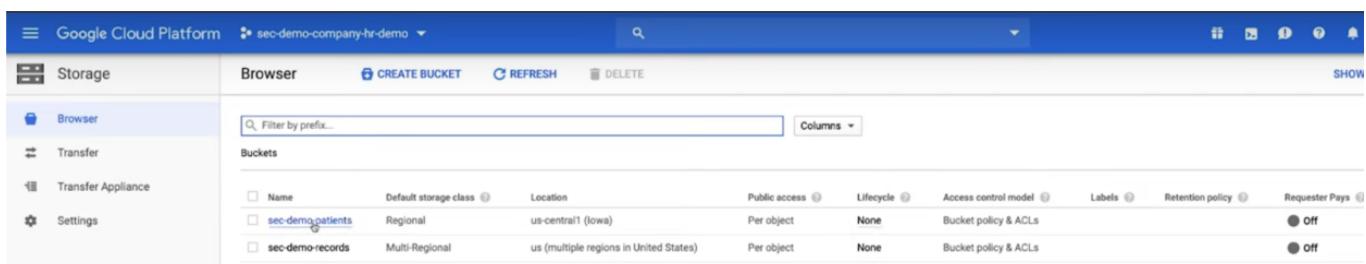
Compliance is a complex, ever changing issue that can put a real strain on your IT department—and your bottom line. As the [cost of data breaches and compliance violations continues to rise](#), it's never been more important to prevent sensitive data from being exposed.

[Cloud Data Loss Prevention](#) (Cloud DLP) helps you better understand and manage sensitive data and personally identifiable information (PII) to meet your specific compliance requirements. It does this by providing fast, scalable classification and redaction of information like credit card numbers, names, social security numbers, US and selected international identifier numbers, phone numbers, and GCP credentials. With just a few clicks directly from the Cloud Storage interface, Cloud DLP scans Cloud Storage buckets, folders, and objects for sensitive data, helping you stay in compliance with regulations and keep your data safe.

For the final chapter, we'll look at how you can get started protecting sensitive data with Cloud DLP, and then send the results directly to Cloud SCC.

Step 1 / Select your storage repositories

The first step is to choose the storage repository you want Cloud DLP to scan. If you want to scan your own existing Cloud Storage bucket, BigQuery table, or Cloud Datastore kind, simply open the project that the repository is in.



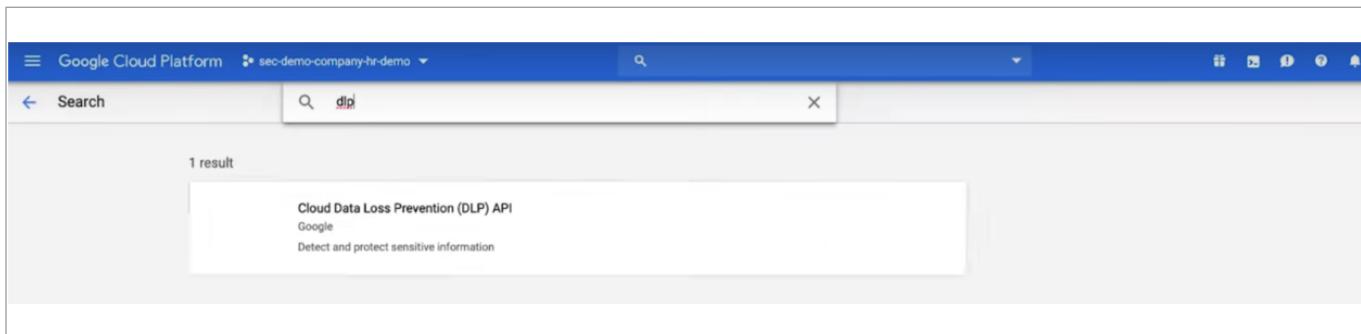
The screenshot shows the Google Cloud Platform Storage Browser. The left sidebar has options for Storage, Transfer, Transfer Appliance, and Settings. The main area shows a table of Buckets:

Name	Default storage class	Location	Public access	Lifecycle	Access control model	Labels	Retention policy	Requester Pays
sec-demo-patients	Regional	us-central1 (Iowa)	Per object	None	Bucket policy & ACLs			Off
sec-demo-records	Multi-Regional	us (multiple regions in United States)	Per object	None	Bucket policy & ACLs			Off

Step 2 / Enable Cloud DLP

For Cloud DLP to scan a project, that project must be in the same organization where you enable Cloud SCC, and must contain the Cloud Storage bucket, BigQuery table, or Cloud Datastore kind you want to scan.

Once you've confirmed this information, go to APIs and Services in the menu on the left, then Library. Then all you have to do is search for the Cloud DLP API and enable it.



Enable Cloud DLP API

Step 3 / Choose the Organization Administrator IAM role

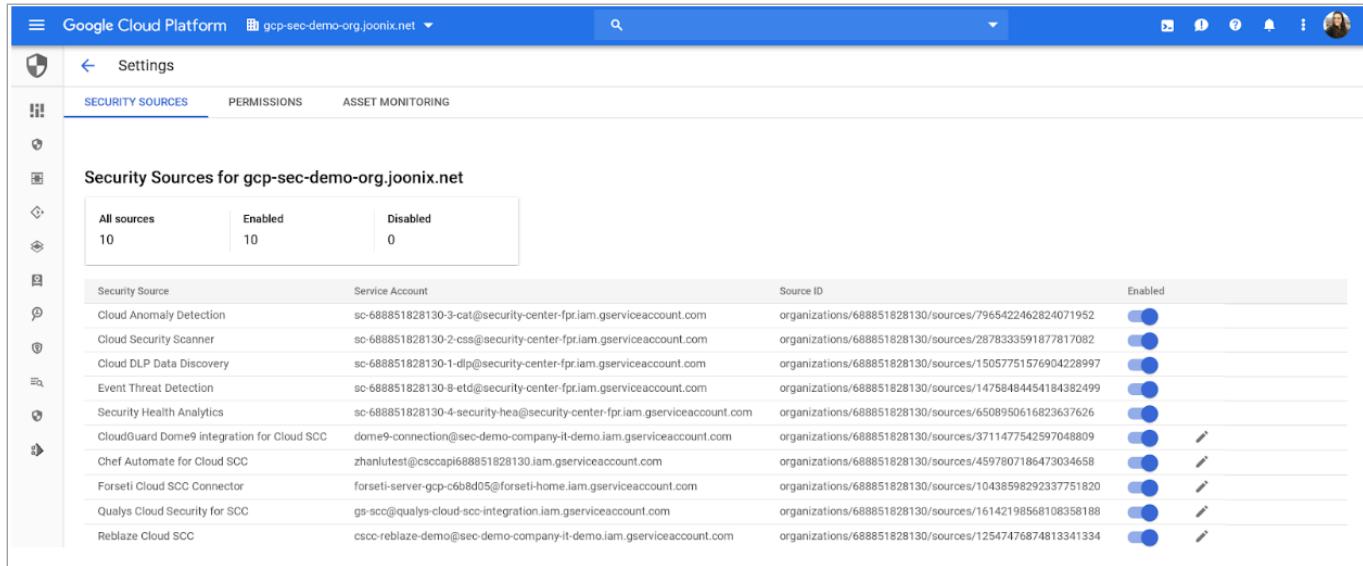
Before you can use Cloud DLP to send the results of your scans to Cloud SCC, you need to first ensure that you have the Organization Administrator IAM role before you can enable additional Cloud IAM roles. To set this up, click on the Organization drop down list and select the organization for which you want to enable Cloud SCC. Find the username in the Member column or add a new user, then add the Security Center Admin and DLP Jobs roles.

The screenshot shows the Google Cloud Platform IAM & admin interface. On the left sidebar, under the 'IAM' section, the 'Members' tab is selected. In the main area, there's a table titled 'Permissions for organization "gcp-sec-demo-org.joonix.net"' showing member details. A modal window is open over the table, titled 'Add members to "gcp-sec-demo-org.joonix.net"'. It shows a list of users and their email addresses. A dropdown menu labeled 'Role' is open, showing 'Security Center Admin' selected. A sub-menu titled 'Select a role' is open, showing 'DLP Jobs Editor' selected. At the bottom of the modal, there's a 'MANAGE ROLES' button.

Choose the Organization Administrator IAM role

Step 4 / Enable Cloud DLP as a Security Source for Cloud SCC

From Cloud Security Command Center, go to Security Sources and toggle on Cloud DLP. Findings for Cloud DLP will display in the Findings cards on the Cloud SCC dashboard—which lets you view security information from Cloud DLP and other security products in one centralized location.



Security Source	Service Account	Source ID	Enabled
Cloud Anomaly Detection	sc-688851828130-3-cat@security-center-fpr.iam.gserviceaccount.com	organizations/688851828130/sources/7965422462824071952	<input checked="" type="checkbox"/>
Cloud Security Scanner	sc-688851828130-2-css@security-center-fpr.iam.gserviceaccount.com	organizations/688851828130/sources/287833591877817082	<input checked="" type="checkbox"/>
Cloud DLP Data Discovery	sc-688851828130-1-dlp@security-center-fpr.iam.gserviceaccount.com	organizations/688851828130/sources/15057751576904228997	<input checked="" type="checkbox"/>
Event Threat Detection	sc-688851828130-8-etd@security-center-fpr.iam.gserviceaccount.com	organizations/688851828130/sources/1475848445184382499	<input checked="" type="checkbox"/>
Security Health Analytics	sc-688851828130-4-security-hea@security-center-fpr.iam.gserviceaccount.com	organizations/688851828130/sources/6508950616823637626	<input checked="" type="checkbox"/>
CloudGuard Dome9 integration for Cloud SCC	dome9-connection@sec-demo-company-it-demo.iam.gserviceaccount.com	organizations/688851828130/sources/3711477542597048809	<input checked="" type="checkbox"/>
Chef Automate for Cloud SCC	zhanlutest@csccap688851828130.iam.gserviceaccount.com	organizations/688851828130/sources/4597807186479034658	<input checked="" type="checkbox"/>
Forseti Cloud SCC Connector	forseti-server-gcp-c6b8d05@forseti-home.iam.gserviceaccount.com	organizations/688851828130/sources/10438598292337751820	<input checked="" type="checkbox"/>
Qualys Cloud Security for SCC	gs-scc@qualys-cloud-sec-integration.iam.gserviceaccount.com	organizations/688851828130/sources/16142198568108358188	<input checked="" type="checkbox"/>
Reblaze Cloud SCC	cscc-reblaze-demo@gcp-sec-demo-company-it-demo.iam.gserviceaccount.com	organizations/688851828130/sources/12547476874813341334	<input checked="" type="checkbox"/>

Select your storage repositories

Cloud DLP uses information types—or infoTypes—to define what it scans for. An infoType is a type of sensitive data, such as a name, email address, telephone number, identification number, credit card number, and so on. You can find out more about infoTypes in the [Cloud DLP documentation](#).

How to use Cloud DLP



Watch the video now.