>

Security Command Center is the canonical security and risk database for Google Cloud. Security Command Center is an intuitive, intelligent risk dashboard and analytics system for surfacing, understanding, and remediating Google Cloud security and data risks across an organization.

Security Command Center helps security teams gather data, identify threats, and act on them before they result in business damage or loss. It offers deep insight into application and data risk so that you can quickly mitigate threats to your cloud resources across your organization and evaluate overall health. Security Command Center provides a single, centralized dashboard so you can:

- View and monitor an inventory of your cloud assets.
- Scan storage systems for sensitive data.
- Detect common web vulnerabilities and anomalous behavior.
- Review access rights to your critical resources in your organization.
- Apply recommended remediations to resolve vulnerabilities.

Security Command Center gives enterprises consolidated visibility into their Google Cloud assets across their organization. You can quickly understand:

- The number of projects you have
- What resources are deployed

- Where sensitive data is located
- How firewalls rules are configured

With ongoing discovery scans, enterprises can view asset history to understand exactly what changed in their environment and act on unauthorized modifications.

Security Command Center provides powerful security insights about your Google Cloud resources. With this tool, security teams can answer questions like:

- Which Cloud Storage buckets contain personally-identifiable information (PII)?
- Are any of my Cloud Storage buckets open to the internet?
- Which cloud applications are vulnerable to cross-site-scripting (XSS) vulnerabilities?

By applying ongoing security analytics and threat intelligence, enterprises can assess their overall security health in a central dashboard and take immediate action on security risks.

Security Command Center integrates with Google Cloud security tools like Web Security Scanner and Cloud Data Loss Prevention (Cloud DLP), and third-party security solutions like:

- Acalvio
- Capsule8
- Cavirin
- Chef
- Check Point CloudGuard Dome9
- Cloudflare
- CloudQuest
- McAfee
- Qualys

- Reblaze
- Redlock by Palo Alto Networks
- StackRox
- Tenable.io
- Twistlock

Google Cloud security insights from partner products are aggregated in Security Command Center, and you can feed them into existing systems and workflows.

Feature Name	Feature Description
Asset discovery and inventory	Discover your assets, data, and Google Cloud services across your organization and view them in one place. Review historical discovery scans to identify new, modified, or deleted assets.
Sensitive data identification	Find out which storage buckets contain sensitive and regulated data using Cloud DLP (/dlp). Help prevent unintended exposure and ensure access is based on need-to-know. Cloud DLP integrates automatically with Security Command Center.
Application vulnerability detection	Uncover common vulnerabilities like cross-site-scripting (XSS) and Flash injection that put your App Engine applications at risk with Web Security Scanner (/security-scanner). Web Security Scanner integrates automatically with Security Command Center.
Access control monitoring	Help ensure the appropriate access control policies are in place across your Google Cloud resources and get alerted when policies are misconfigured or unexpectedly change. Forseti (https://forsetisecurity.org/), the open source security toolkit for Google Cloud, integrates with Security Command Center.
Anomaly detection from Google	Identify threats like botnets, cryptocurrency mining, anomalous reboots, and suspicious network traffic with built-in anomaly detection technology developed by Google.
Third-party security tool inputs	Integrate output from your existing security tools like Cloudflare, CrowdStrike, Palo Alto Networks, Qualys, and RedLock into Security Command Center. Integrating output can help you to detect: • DDoS attacks

	• Compromised endpoints • Compliance policy violations • Network attacks • Instance vulnerabilities and threats
Real-time notifications	Get Security Command Center alerts via email and SMS with Pub/Sub notification (/security-command-center/docs/how-to-cloud-scc-tools#notifier) integration.
REST API and Client SDKs	Use the Security Command Center REST API or client SDKs for easy integration with your existing security systems and workflows.

Security Command Center enables you to generate curated insights that provide a unique view of incoming threats and attacks to your Google Cloud resources, called *assets*. Assets are resources like organization, projects, instances, and applications.

Security Command Center displays possible security risks, called *findings*, that are associated with each asset. Findings come from *security sources* that include Google Cloud native, 3rd party partners, and your own security detectors and finding sources.

Security Command Center asset discovery runs at least once each day. You can manually re-scan on demand from the Security Command Center Assets display. Assets discovery uses your Security Command Center organization hierarchy to curate a list of your existing and new assets.

Security Command Center integrates with native Google Cloud scanners to surface potential security risks in your assets. Native scanners include:

- Cloud DLP (/dlp)

- Anomaly Detection (/security-command-center/docs/how-to-view-vulnerabilities-threats#anomaly_detection)
- Web Security Scanner (/security-scanner)
- Forseti (https://forsetisecurity.org/)

These scanners operate regularly to track asset changes over time. Security Command Center enables you to inspect your current and past asset states, and compare assets between two points in time.

Along with native security findings, you can integrate findings from your own or third-party sources for Google Cloud resources or hybrid or multi-cloud resources. For more information, see adding security sources (/security-command-center/docs/how-to-security-sources).

Security Command Center currently focuses on asset inventory, discovery, search, and management. Use Security Command Center when you want to understand your security and data attack surface and answer questions like:

- How many projects you have, and how many projects are new
- What Google Cloud resources are deployed, like Compute Engine, Cloud Storage, or App Engine
- What services are in use, such as Virtual Machines (VMs) or buckets
- What's your deployment history
- What images are running on your VMs
- What IP addresses are open to the public
- How to organize, annotate, search, select, filter, and sort across the following categories:
    - Assets and asset properties
    - Findings and finding properties like the type of risk

- Security marks, which enable you to annotate assets or findings in Security Command Center
- Time period

- Get started with the Quickstart for Security Command Center (/security-command-center/docs/quickstart-scc-dashboard).
- Learn about native Google Cloud scanners and how to view the vulnerabilities and threats (/security-command-center/docs/how-to-view-vulnerabilities-threats) they surface.
- Learn how to use the assets display (/security-command-center/docs/how-to-assets-display).
- Learn how to read findings (/security-command-center/docs/how-to-findings).