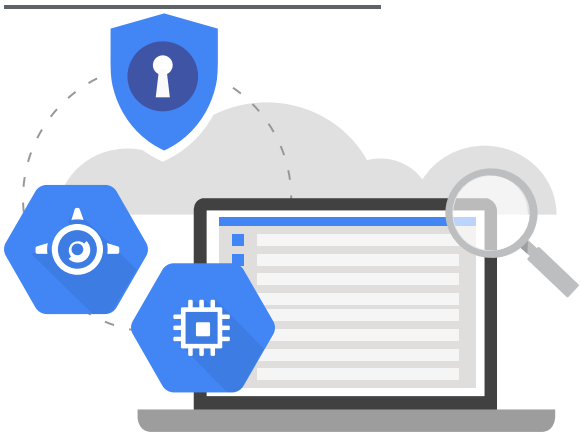
A comprehensive security management and data risk platform for GCP.

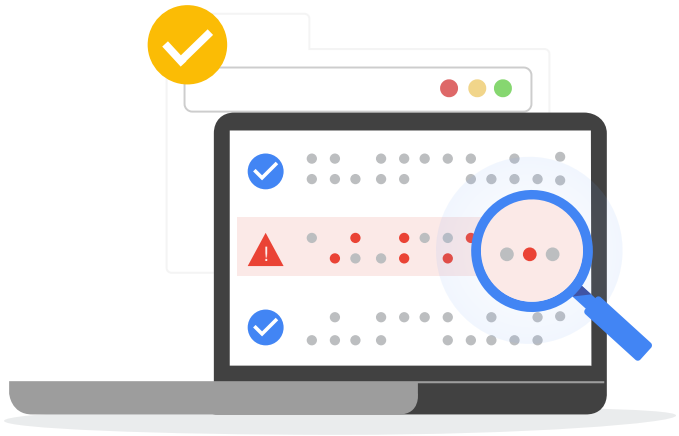
Go to console (https://console.cloud.google.com/marketplace/details/google-cloud-platform/cloud-security-command-center?_ga=2.156576505.-374456964.1526667099)

View documentation (/security-command-center/docs/) for this product.

With visibility into what resources are in Google Cloud Platform and their security state, Cloud Security Command Center makes it easier for you to prevent, detect, and respond to threats. Identify security misconfigurations in virtual machines, networks, applications, and storage buckets from a centralized dashboard. Take action on them before they can potentially result in business damage or loss. Built-in capabilities can quickly surface suspicious activity in your Stackdriver security logs or indicate compromised virtual machines. Respond to threats by following actionable recommendations or exporting logs to your SIEM for further investigation.



Cloud Security Command Center gives enterprises centralized visibility into their GCP resources across Compute Engine, Kubernetes Engine, and more (https://cloud.google.com/docs/). Instantly see what assets in your GCP infrastructure are in violation of the CIS Benchmarks and take action. Built-in security analytics and threat intelligence assesses the overall security state and activity of your virtual machines, network, and storage buckets and surfaces vulnerabilities in your applications. These insights can help you take proactive measures to reduce your exposure to risks.



Cloud Security Command Center reveals virtual machines that have been used for malicious purposes. Event Threat Detection (https://cloud.google.com/event-threat-detection) uses industry-leading threat intelligence, including Google Safe Browsing (https://safebrowsing.google.com/#policies), to detect suspicious activity in your logs. Reduce the amount of time you spend investigating logs and focus on high-risk events and remediation.

Cloud Security Command Center integrates with Google Cloud Platform security tools like Binary Authorization or Google Cloud Phishing Protection. You can also integrate third-party security products from Acalvio, Capsule8, Cavirin, Chef, Check Point CloudGuard Dome9, Cloudflare, CloudQuest, McAfee, Qualys, Redblaze, Redlock by Palo Alto Networks, StackRox, Tenable.io, and Twistlock.

Discover and view your assets across App Engine, BigQuery, Cloud SQL, Cloud Storage, Compute Engine, Cloud IAM, Google Kubernetes Engine, and more (https://cloud.google.com/docs/). Review historical discovery scans to identify new, modified, or deleted assets.

Find out which storage buckets contain sensitive and regulated data using the Cloud DLP API. Help prevent unintended exposure and ensure access is based on need-to-know. The DLP API integrates automatically with Cloud Security Command Center.

Uncover common vulnerabilities such as cross-site-scripting (XSS), outdated libraries, and more (https://cloud.google.com/security-scanner/docs/scan-result-details) that put your App Engine applications at risk with Cloud Security Scanner. Cloud Security Scanner integrates automatically with Cloud Security Command Center.

Leverage the Cloud Security Command Center REST API for easy integration with your existing security systems and workflows. Export Cloud Security Command Center data to Splunk or other SIEMs for further analysis.

Native ability to surface the identity and access management policies for your cloud resources. Help ensure the appropriate access control policies are in place and get alerted when policies are misconfigured or unexpectedly change. Forseti, our open source security toolkit for Google Cloud Platform, integrates with Cloud Security Command Center.

Identify threats such as coin mining, unusual activity, hijacked accounts, compromised machines used for botnets or DDoS attacks, and anomalous data activity with Cloud Anomaly Detection, developed by Google. Cloud Anomaly Detection integrates automatically with Cloud Security Command Center.

Automatically scan Stackdriver security logs for high-profile indicators of compromise with Event Threat Detection (https://cloud.google.com/event-threat-detection) and further explore these findings from Cloud Security Command Center.

Integrate output from your existing security tools into Cloud Security Command Center to detect security and compliance policy violations and instance vulnerabilities and threats.

Receive Cloud Security Command Center alerts via Gmail, SMS, and Jira with Cloud Pub/Sub notification integration. Quickly remediate security alerts by using Cloud Pub/Sub events and Cloud Functions.

Integrate Cloud Audit Logging events for Compute Engine, Google Cloud networking, Cloud Storage, Cloud IAM, and Binary Authorization into Cloud Security Command Center to help meet regulatory requirements or provide an audit trail while investigating an incident.

Understand the security state of your GCP assets and whether they are compliant. Quickly resolve misconfigurations by clicking directly on the impacted resource and following the proscribed steps on how to fix it. Security Health Analytics integrates automatically with Cloud Security Command Center.

> “Cloud Security Command Center gives us unprecedented visibility into the security posture of our VM instances and containerized workloads running within GCP. With this security service, we can quickly review and assess risks across all our GCP assets.”

Alexander Schuchman, Director of Information Security, Colgate-Palmolive

Cloud Security Command Center integrates with Google Cloud Platform security tools like Binary Authorization or Google Cloud Phishing Protection. You can also integrate third-party security solutions from Acalvio, Capsule8, Cavirin, Chef, Check Point CloudGuard Dome9, Cloudflare, CloudQuest, McAfee, Netskope, Perimeter, Qualys, Reblaze, Redlock by Palo Alto Networks, StackRox, Sysdig, Tenable.io, and Twistlock.

Read blog post → (/blog/products/gcp/)

Learn more → (/security-command-center/docs/how-to/)

Learn more ↗ (https://www.youtube.com/watch?time_continue=6&v=PfXZovlblJc

Learn more ↗ (https://services.google.com/fh

There is no separate charge for using Cloud Security Command Center. However, you will be charged if you upload more than 1 GB per day of external findings into Cloud Security Command Center. In addition, some Cloud Security Command Center detectors, such as Cloud DLP API, charge by usage. Learn more on the DLP API pricing page (https://cloud.google.com/dlp/pricing).

New to GCP? Get started with any GCP product for free with a $300 credit

New to GCP? Get started with any GCP product for free with a $300 credit.

Try it free (https://console.cloud.google.com/freetrial/)

Our experts will help you build the right solution or find the right partner for your needs.

Contact sales (/contact/)

Find a partner (https://cloud.withgoogle.com/partners/)