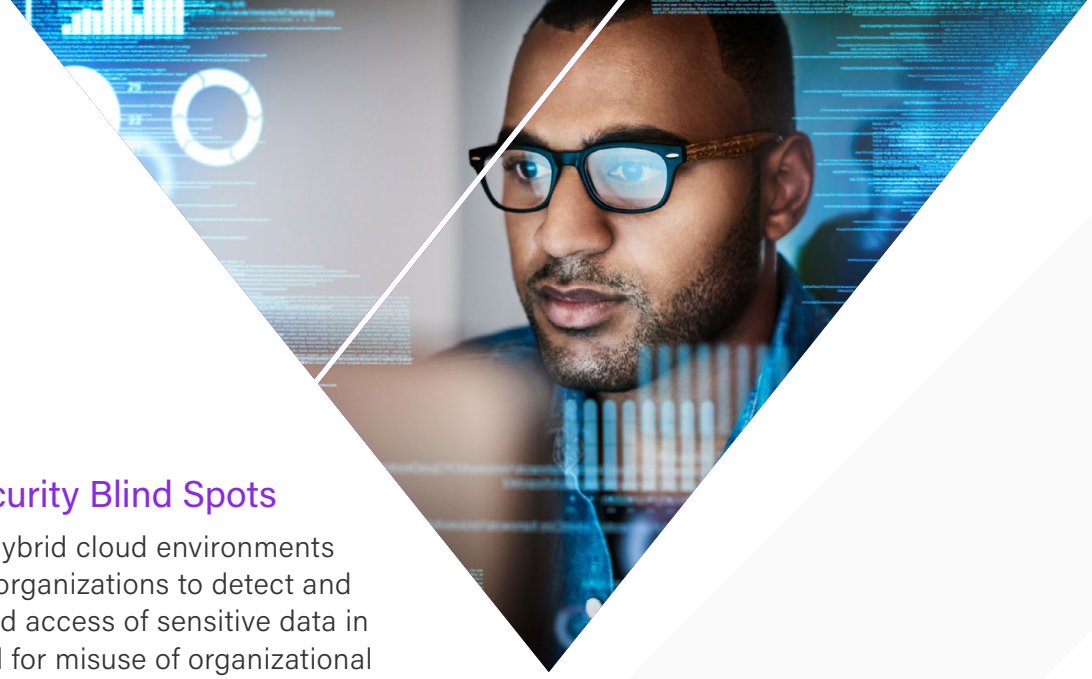
securonix

Google Cloud

SOLUTION BRIEF

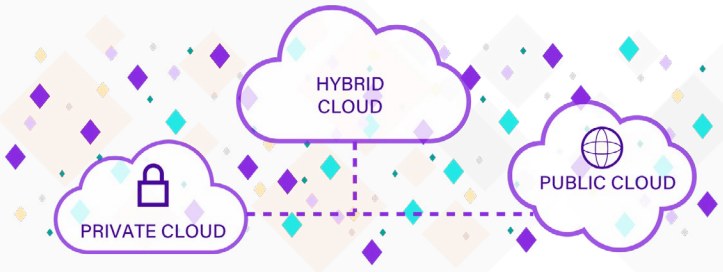
Google Cloud Platform (GCP) Security Monitoring

Identify patterns and pinpoint potential threats in your GCP environment



Remove Cloud Security Blind Spots

The rapid adoption of hybrid cloud environments has made it harder for organizations to detect and respond to unauthorized access of sensitive data in the cloud. The potential for misuse of organizational cloud resources can lead to higher risks of data exfiltration. Securing your GCP infrastructure from cyberattacks is critical to strengthening your overall security posture.



Our Approach

Securonix analyzes possible security events to look for malicious activity. Through integrations with the GCP, Google Kubernetes Engine, and the Google Cloud Operations Suite, Securonix leverages Google's security infrastructure to collect all threat information into a single source of truth for detection and response.

Solution Benefits

Gain 360 Visibility

Gain full visibility across virtual private cloud (VPC), storage, Google Kubernetes Engine (GKE), compute, and identity and access management (IAM) events for end-to-end visibility across your Google Cloud.

Detect Threats Faster

Decrease your mean-time-to-detect with context-enriched data insights and advanced threat chain analytics.

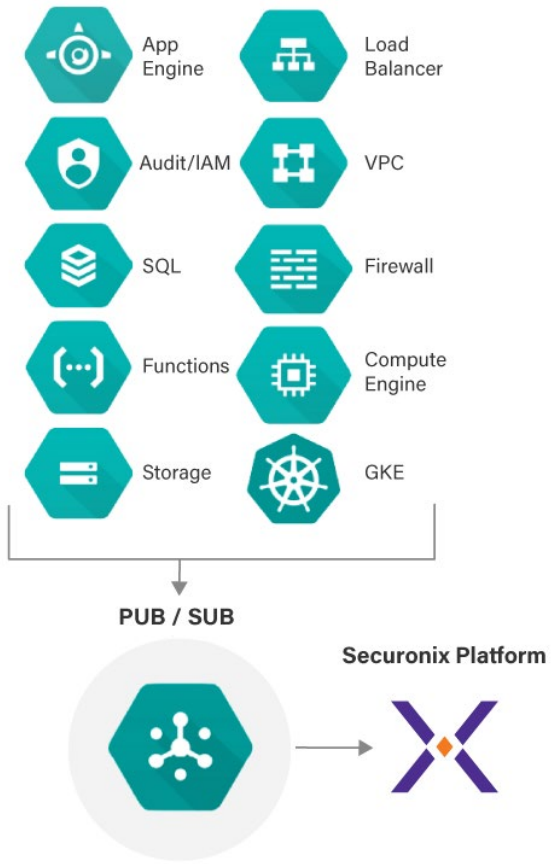
Unlock Data Insights

Visualize security events and changes in your GCP environment with out-of-the-box and custom dashboards and reports.

How it Works

The Securonix Next-Gen SIEM integrates with multiple GCP services and products, correlating data and adding the context needed for you to view the security status of your environment at a single glance. This data is processed to identify tangible threats, including data compromise, unauthorized access attempts, suspicious traffic, and many others.

A bi-directional integration enables security operations center (SOC) analysts to act on threats immediately, instead of needing to pivot to other applications for action. Securonix integrates with GCP components to enable end-to-end security monitoring, advanced threat detection, data retention, and automated incident response capabilities.



Detect Faster with GCP-specific Threat Models

A direct API integration with the GCP stack allows you to correlate events in the cloud with contextual information from other on-premises data feeds. Our advanced analytics models then automatically stitch together related anomalies to detect and prioritize high-risk threats across your entire environment.

Key Use Cases

Securonix provides pre-built cloud security monitoring content to detect anomalous security events including:

- Unauthorized access such as a login from a rare IP or geolocation, a spike in failed logins, a land speed anomaly, or a malicious IP.
- GCP configuration anomalies such as a spike in instance creation or deletion, suspicious admin activities, or unusual App Engine requests.
- Suspicious GCP IAM activity such as suspicious user creation, admin privilege changes, password policy changes, or rare privileged activity.
- Anomalous API connections including from a rare IP or geolocation, or a malicious IP address.
- Suspicious Google Cloud VPC traffic including port scans or connections on anomalous ports.

For more information about Securonix, schedule a demo at: www.securonix.com/request-a-demo

About Securonix

Securonix is redefining SIEM for today's hybrid cloud, data-driven enterprise. Built on big data architecture, Securonix delivers SIEM, UEBA, XDR, SOAR, Security Data Lake, NDR and vertical-specific applications as a pure SaaS solution with unlimited scalability and no infrastructure cost. Securonix reduces noise and prioritizes high fidelity alerts with behavioral analytics technology that pioneered the UEBA category. For more information visit securonix.com

About Google Cloud Platform

Google Cloud Platform, offered by Google, is a suite of cloud computing services that runs on the same infrastructure that Google uses internally for its end-user products, such as Google Search, Gmail, Google Drive, and YouTube. For more information visit cloud.google.com