SECURONIX™

SOLUTION BRIEF

Security Monitoring for Google Cloud Platform

While your organization is embracing the Google Cloud Platform, it is also inheriting some unique cloud security risks including:

- The potential for misuse of organizational cloud resources, such as for cryptomining or DDoS attack hosting.
- Attacks taking advantage of weak credential security and insecure interfaces, such as privilege escalation and account compromise, that leads to data exfiltration.

Securing your Google Cloud Platform (GCP) infrastructure from cyberattack is a key component to strengthen your overall security posture.

Protecting Your Expanding Threat Surface

In the past enterprises used firewalls and network segregation to protect applications from external cyberattack. Now the network has moved out of the enterprise domain and into the cloud, where it is managed by public cloud providers. As network control moves out of the enterprise, the focus of security operations moves away from prevention-centric tools, such as firewalls and endpoint solutions, toward detection-centric solutions, such as SIEM, UEBA, and other more adaptive solutions.

How Securonix Secures Google Cloud Platform

The Securonix platform 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 information is processed to identify tangible threats, including data compromise, unauthorized access attempts, suspicious traffic, and several others.

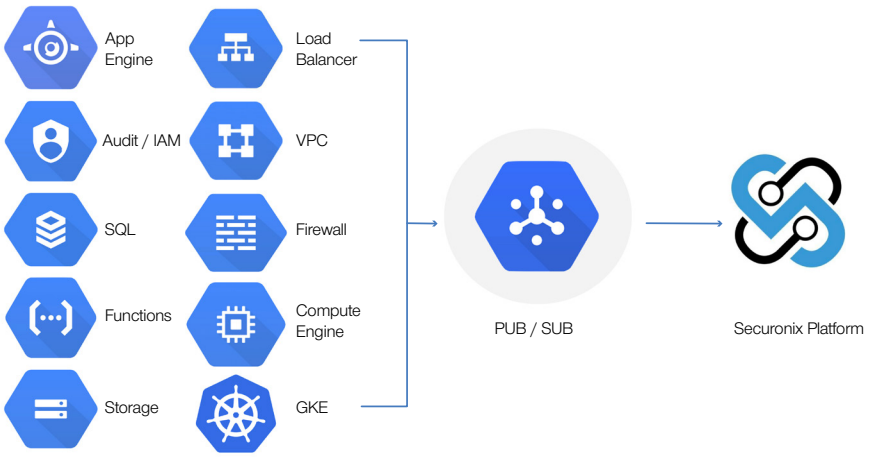

Figure 1: Securonix Integrates With the Google Cloud Platform

Solution Benefits

- 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 Google Cloud.
- Fast detection and response with streamlined, direct API integration.
- Decrease mean-time-to-respond with enriched data and additional context for threat modeling.
- Visualize activities and changes in your GCP infrastructure with out-of-the-box dashboards and reports that are customizable.

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.

GCP Pub/Sub and Google Cloud Operations Integration

Integrating with Google Cloud operations suite (formerly Stackdriver), Securonix monitors actions taken within the complete suite of GCP services. Securonix integrates with GCP Pub/Sub to pull events from Google Cloud for ingestion and analysis. These events are critical for identifying indicators of cloud compromise, such as anomalous service usage or account behavior, unauthorized or unusual cloud resource usage, and cloud access from unusual geographic locations.

Use Case: Threat Modeling by Correlating Alerts Across GCP Components

Advanced attacks are not detectable with a single event. Rather, they consist of a series of telltale events which need to be tied together in order to identify the threat. Securonix threat models do this by stitching together alerts from across data sources.

For example, a cryptojacking attack may consist of:

- A suspicious console login found in the GCP console logs.
- A related permission elevation found in the GCP IAM logs.
- A spike in start instances in GCP or rare start instances found in the configuration logs.
- GCP logging being disabled in the GCP Stackdriver logs.

In Securonix these alerts are stitched together into a threat chain, mapping indicators to the different attack stages that correspond with the MITRE ATT&CK framework.

Conclusion

With hundreds of different services and applications, an effective Google Cloud security solution needs to be able to ingest and correlate data across GCP services in order to ensure broad visibility. Securonix provides a platform that not only identifies advanced threats, but also recommends remediation actions.

A modern cloud deployment needs a cloud native, connected, and mature solution that can provide both visibility and industry-leading analytics. The Securonix platform delivers all of this and more. As an industry leader recognized by Gartner, Securonix is an ideal solution to keep your Google Cloud secure.

Key Use Cases

- 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.

About Securonix

Securonix transforms enterprise security with actionable intelligence. Using a purpose-built security analytics platform Securonix quickly and accurately detects high-risk threats to your organization. For more information visit www.securonix.com.

SECURONIX™

LEARN MORE
www.securonix.com

LET'S TALK
+1 (310) 641-1000