Nova Quantum

Managing Security in Google Cloud Platform (GCP)

Combine native GCP security features with our Managed Security Services to secure your cloud environment today!

Google Cloud
Partner Advantage

Through 2020, 95% of cloud security failures will be the customer's fault

Gartner

Source: Gartner Revels Top Predictions for IT Organizations and Users for 2016 and Beyond, October 2015

Insecure misconfiguration & lack of controls #1 cause to cloud based data centers breaches

Forbes

"Through 2020, 80% of cloud breaches will be due to customer misconfiguration, mismanaged credentials or insider theft, not cloud provider vulnerabilities"

"A historic 424% jump in breaches related to misconfigured cloud infrastructure, largely due to human error."

Google Cloud Partner Advantage

Source: https://www.forbes.com/sites/forbestechcouncil/2018/08/09/the-one-cloud-security-metric-every-ciso-should-know/#3ff8c87e5375 , Author: Josh Stella, Forbes council

Cloud security is a shared responsibility

Shared responsibility model for cloud security

Google's commitment	Joint responsibility
Secure foundation	**Google provides built-in controls**
Physical assets	Virtual machines and networks
Datacenter operations	Apps and workloads
Cloud infrastructure and fabric	Data

It can feel hard to create a secure cloud environment

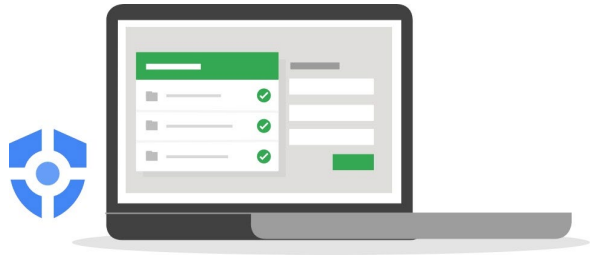
We understand your dilemma

- *Cloud Services are being created and destroyed every minute*
- *Security is always changing; there are new threats every week*
- *It's hard to find experienced Cloud Security Practitioners*
- *How do you keep your environment secure while staying abreast of the latest security solutions?*

Nova Quantum

How does your company understand the quality of their security posture against security controls that are possible to configure within GCP?

GCP Security Command Center



- Prevent, detect, and respond to threats.
- Prevent threats and meet compliance requirements with visibility and control over your Google Cloud services and data.
- Detect and respond to threats targeting your Google Cloud assets.
- Security Command Center integrates with Google Cloud security tools like Binary Authorization or Phishing Protection.

How does your company understand and resolve its most urgent cloud security issues?

This is how NovaQuantum reviews your environment

1

Assess

- Review the core security configurations of your environment
- Analyze data using an automation engine to detect findings
- Identify opportunities to strengthen your existing security controls

2

Recommend

- Identify security remediations to address security gaps and other opportunities that are identified
- Propose improvements to key areas of your organization's security architecture

3

Review

- Deliver a detailed report of findings and recommendations

How does your company understand the quality of their security posture against industry recognized security standards?

Security and Compliance

Many organizations security needs are driven by compliance requirements. Here are the most commonly used security standards:

Standard	Author	Description
GCP CIS 1.1.0	Center for Internet Security	Set of security controls published by the Center for Internet Security
PCI DSS 3.2.1	Payment Card Industry Standards Council	Standards required for organizations that manage payment card data
ISO 27001	International Standards Organization	Set of security controls for information security systems. Standard 27017 is cloud computing specific.
NIST 800-53	National Institute of Standards and Technology	Security and Privacy Controls for Federal Information Systems and Organizations.

By default, most of the environments are NOT compliant with any security standards!

Our Proposal: let us manage your GCP security!

While there are quite a few native GCP tools and services that can perform the auditing of your environment, their configuration and ongoing maintenance is time consuming and requires very specialized skills.

We provide managed GCP Security services:

- Perform an initial assessment of the existing infrastructure and identify the critical components
- Enable auditing of the environment against one(or more) of the following regulatory standards: GCP CIS 1.0.0, NIST 800-53, PCI DSS 3.2, ISO 27001, and SOC TSP.
- Provide continuous monitoring and **enforcement** *(only for zero risk controls)* of your custom security policies
- Provide monthly/weekly reports of the compliance status
- Provide a **Cloud Security Posture Review**:
  - Review and evaluate the current architecture and security configurations of your GCP environment, as compared to GCP security best practices
  - Capture findings and develop a report with recommendations on how to improve the security posture of your GCP environment.

Google Cloud
Partner Advantage

Nova Quantum

Cloud Security Posture Review topics

Deep dive analysis on the following security domains:

1	2	3	4
Resource Management	**Identity, Authentication & Authorization**	**Network Security**	**VM Security**
GCP org hierarchy	User & group management	VPC architecture	VM identities
Environments & resource isolation	Administrative roles	Firewall rules	Remote access
Project creation	Authentication	Network logging	Image management
Resource provisioning	Assigning IAM roles	VPC service controls	
Organization policies	Service accounts	DDoS and WAF	
		Identity Aware Proxy	

Cloud Security Posture Review topics(cont.)

Deep-dive analysis on the following security domains:

5	6	7
Data security	**Security operations**	**GKE security**
Encryption key management	Logging	GKE cluster provisioning
Cloud Storage security	Monitoring	Secure cluster default configurations
BigQuery security	Policy scanning	Cluster IAM/RBAC
Cloud SQL security	Incident Response	Container image building
Data Loss Prevention		Container lifecycle management
		Container runtime security
		Workload hardening and isolation

Pricing for our services

We are taking pride in our transparent pricing policy:

1. Initial deployment and configuration of your custom security policies – This is the effort associated with the initial creation of the security framework that you want to be compliant with: not all the security policies available in GCP by default would make sense for your particular environment as some of them could impede your normal management operations, for example.
2. Creation of the Cloud Security Posture report: We review your current configurations and platform controls, provide detailed recommendations, and present best practices to reduce risk and mitigate common threats to your environment.
3. On-going management – This is the effort required for daily support of the GCP Security Compliance service, monitoring of log sources, policy violations, remediation of security controls and on-going alerts tune-up.

Plans that scale with your environment

Small Environments (under 100 resources)	Medium Environments (100-250 resources)	Large Environments (>250 resources)
Initial fee: contact us!	Initial fee: contact us!	Initial fee: contact us!
Monthly fee: contact us!	Monthly fee: contact us!	Monthly fee: contact us!

Google Cloud Partner Advantage

Nova Quantum