RELIAQUEST

SOLUTION BRIEF

RELIAQUEST FOR GOOGLE CLOUD PLATFORM (GCP)

In the past few years, Google Cloud Platform has gained in popularity across organizations of all sizes. GCP's aim to help rapidly build and support a distributed and scalable architecture introduces additional complexities and risk. Access to security-relevant telemetry can be challenging, especially when trying to combine them with on-premises security data for a singular view. To protect and enable the business, security teams need granular visibility across not just the GCP infrastructure but each of the distributed layers, applications, and security components. ReliaQuest not only helps organizations safely migrate to GCP, but also delivers best-in-class protection. ReliaQuest provides singular visibility across GCP resources by eliminating blind spots and comprehensively detecting and responding to threats.

BENEFITS:

- Gain singular visibility across your GCP environment for better situational awareness
- Get proactive with continuously updated threat detection content and IOCs
- Improve security posture with actionable metrics and coverage maps to industry-standard frameworks
- Streamline and unify security operations across your cloud and on-premises IT infrastructure
- Ensure confidence in detections with managed integrations

Securely Migrate to and Protect Your GCP environment

The biggest challenge security teams face with cloud migration and protection is lack of visibility. With a cloud-native Open XDR platform, GreyMatter, ReliaQuest unifies any and all telemetry from across the GCP environment eliminating any blind spots, providing singular situational awareness, including unifying data from across on-premises and GCP cloud. Additionally, GreyMatter unifies data from SIEM, EDR, CASBs, threat intelligence, and any other on-premises technologies to enrich investigations and drive fast response for proactive protection.

GreyMatter processes telemetry from any and all GCP resources and activities, including but not limited to:

- GCP Storage
- Google Workspace
- Cloud IAM
- Workspace
- API Gateway
- Resource Manager
- Compute Engine instance (VM)
- VPC service controls
- Security Command Center
- Ops agent
- WAF
- And more

Key Capabilities

24/7/365 monitoring: Leveraging its cloud-native GreyMatter platform, ReliaQuest offers continuous monitoring of all GCP resources, applications, workloads like VMs and containers, and security tools for real-time situational awareness.

Comprehensive threat protection and response: Leverage ReliaQuest MDR services and Open XDR technology to centralize alerts, reduce false positives, drive fast response, and stay ahead of evolving threats.

Contextual intelligence to drive fast insights: Bring holistic understanding of security issues based on contextual threat intelligence and impact of issues.

Drive efficiencies across each stage of the security lifecycle: Leverage automated data collection, investigation, and response playbooks to take fast action and drive efficiencies.

Field-tested detection content packages: Stay ahead of threats and reduce the impact of events with over 200 detection rules curated for cloud environments, plus continuous updates based on non-stop research and learning from across a growing customer environment.

Managed integrations: We continuously optimize your security tools so you can leverage their latest capabilities and extend returns on your security investments.

MITRE ATT&CK framework mapping: Mappings to MITRE ATT&CK framework and Kill Chain stages help plot coverage and uncover areas for focus to improve security posture.

Industry peer benchmarking: Know how you are doing against your peers when it comes to visibility, team performance, and tool fidelity.

Customer success focus: Gain a dedicated customer success manager who gives you personalized attention, ensuring our services are curated to your needs and exceed your expectations.

Threat Types and Sample Use Cases

THREAT TYPES	EXAMPLE USE CASES
Misconfigurations: Expand the attack surface and can leave cloud resources vulnerable to attack.	• Anomalous grant of IAM permissions • Sensitive role granted to group with external member
Publicly accessible APIs: can be lucrative targets for attackers, and can result in account takeovers, carding attacks, fake logins, and more.	• GCP Service Account used for key and/or instance reconnaissance • Workspace admin role assignments • Domains added to workspace trusted domain
Exfiltration of data: A primary concern of organizations where sensitive PII, PHI, and PCI data is stolen.	• GCP DLP job trigger Deletions/Modifications • Abnormal pub/sub subscription added
Infiltration: Methods used to penetrate an organization's cloud services via account hijacking, network or systems.	• GCP Service Account added User to IAM outside of organization • Service account key reconnaissance
Disruption: Using either DDoS, ransomware, or other techniques to disrupt a critical service or application.	• GCP firewall modification • GCP logging sink modification • Pub/Sub topic/subscriber deletion/modification • Cloud storage deletion activity
Exploitation: Methods such as metadata service abuse, resource hijacking, identify spoofing risks, backdoors, and more.	• GCP Service Account impersonation • Instance SSH keys modified • Gcloud interaction with compute instance