RELIAQUEST

SOLUTION BRIEF

RELIAQUEST FOR AMAZON WEB SERVICES (AWS)

Amazon Web Services is one of the top cloud services that organizations build and migrate their applications to as part of their digital transformation. 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 to gain granular visibility across not just the AWS infrastructure but also into the OS, application, and security layers. ReliaQuest helps organizations not only safely migrate to AWS but also delivers best-in-class protection. ReliaQuest provides singular visibility by eliminating blind spots and comprehensively detecting and responding to threats.

BENEFITS:

- Gain singular visibility across your AWS 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 AWS Environment

The biggest challenge security teams face with cloud migration and protection is lack of visibility. With our cloud-native Open XDR platform, GreyMatter, we unify telemetry from across the AWS environment, eliminating any blind spots and providing singular visibility that unifies data from across on-premises and AWS cloud resources. Coverage spans telemetry from various sources including CloudTrail, GuardDuty, CloudWatch, S3, EC2 instances, and more. 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 AWS resources and activities, including but not limited to:

- CloudTrail
- GuardDuty
- CloudWatch
- S3
- EC2
- Athena
- Shield
- Route 53
- VPC flow data
- AWS Elastic Load
- AWS Security Hub
- Inspector
- CloudFront
- Elastic Kubernetes
- Amazon Workspaces
- Amazon API Gateway

Key Capabilities

24/7/365 monitoring: Leveraging its cloud-native GreyMatter platform, ReliaQuest offers continuous monitoring of all AWS resources, applications, 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.

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.

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

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: Expands the attack surface and can leave cloud resources vulnerable to attack.	• AWS user added outside organization • AWS flow logs removed • AWS user added to a privileged group
Publicly accessible APIs: can be lucrative targets for attackers, and can result in account takeovers, carding attacks, fake logins, and more.	• S3 bucket made publicly accessible • API unauthorized action attempts • Sensitive cloud bucket permissions modified
Exfiltration of data: A primary concern of organizations where sensitive PII, PHI, and PCI data are stolen.	• EC2 instance assigned public IP • Compute VPN tunnel created
Infiltration: Methods used to penetrate an organization's cloud services via account hijacking, network or systems.	• AWS API IAM key created for other account • AWS user enumeration • AWS API activity for inactive user • API service account impersonation
Disruption: Using either DDoS, ransomware, or other techniques to disrupt a critical service or application.	• Cryptominer behavior on container • AWS config logging disruption
Exploitation: Methods such as metadata service abuse, resource hijacking, backdoors, and others.	• Cloud instance access keys modified • IAM policy modification • AWS root account usage

RELIAQUEST
Make Security Possible™

(800) 925-2159 www.reliaquest.com info@reliaquest.com