RELIAQUEST

SOLUTION BRIEF

RELIAQUEST FOR MICROSOFT AZURE CLOUD

Microsoft Azure has grown in popularity amongst organizations that are investing in cloud transformation. This is a fundamental shift for security organizations and introduces unknown risks and blind spots. To protect and enable the business, security teams need to gain granular visibility across not just the cloud infrastructure but also applications and security tools. ReliaQuest helps organizations not only safely migrate to Microsoft Azure but also delivers best-in-class protection. ReliaQuest provides singular visibility by eliminating blind spots and comprehensively detecting and responding to threats.

BENEFITS:

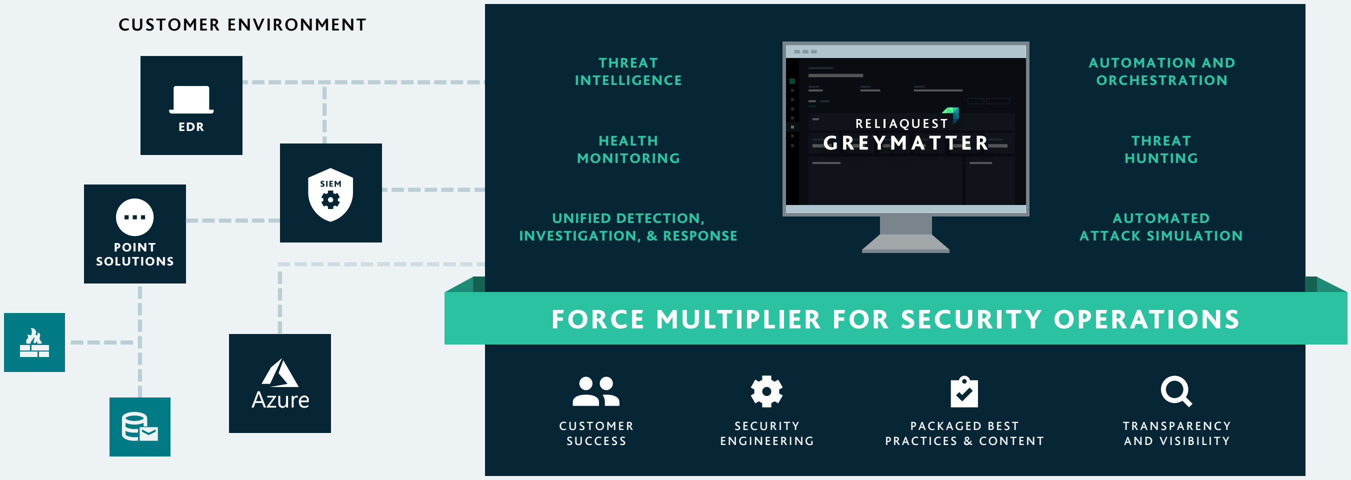
- Gain singular visibility across your MS Azure environment for better situational awareness
- Be proactive with continuously updated threat detection content and IOCs
- Improve security posture with actionable metrics and coverage maps to industry-standard framworks
- Streamline and unify security operations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

Securely Migrate to and Protect Your Microsoft Azure 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 data from across the Azure environment, eliminating any blind spots and providing singular visibility across on-premises and cloud resources. Telemetry sources span authentications, account administration, key/token creations, instance creations/deletions/modifications, admin interactions, and more. Additionally, GreyMatter unifies data from SIEM, EDR, CASB, threat intelligence and any other on-premises technologies or cloud environments to enrich investigations and drive fast response for improved protection.

GreyMatter can process telemetry from any and all Azure resources and activities, including but not limited to:

- Microsoft 365 Defender Suite
- Microsoft 365 Defender for Cloud Apps
- Microsoft Sentinel
- Azure Active Directory
- Azure Key Vault
- Azure Monitor


CUSTOMER ENVIRONMENT
EDR
SIEM
POINT SOLUTIONS
Azure
THREAT INTELLIGENCE
HEALTH MONITORING
UNIFIED DETECTION, INVESTIGATION, & RESPONSE
RELIAQUEST GREYMATTER
AUTOMATION AND ORCHESTRATION
THREAT HUNTING
AUTOMATED ATTACK SIMULATION
FORCE MULTIPLIER FOR SECURITY OPERATIONS
CUSTOMER SUCCESS
SECURITY ENGINEERING
PACKAGED BEST PRACTICES & CONTENT
TRANSPARENCY AND VISIBILITY

Key Capabilities

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

Singular visibility across your Azure environment: Going beyond vendor-exposed data, process data from all relevant sources—including activity logs, audit logs, events, and alerts—to eliminate blind spots.

Comprehensive threat protection and response: Combine 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 of 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.	• Service disabled • New log exclusions created • Email forwarding rule to externaldomain created
Publicly accessible APIs: Configured incorrectly, APIs can be lucrative targets for attackers and can result in account takeovers, carding attacks, fake logins, and more.	• Azure blob made publicly accessible • SharePoint file shared outside organization • Cloud ACL configured to allow all
Exfiltration of data: A primary concern of organizations where sensitive PII, PHI, and PCI data are stolen.	• Consent granted to suspicious application • Data exfiltration to unsanctioned apps
Infiltration: Methods used to penetrate an organization's cloud services via account hijacking, network, or systems.	• Cloud brute force password spraying • Anonymous user SharePoint access
Disruption: Using either DDoS, ransomware or other techniques to disrupt a critical service or application.	• DNS record modified or added • Startup script added to instance • Abnormal multiple VMs created
Exploitation: Methods such as metadata service abuse, resource hijacking, backdoors, and others.	• INGRESS firewall rule created from non rfc1918 address • API call from threat host • Anomalous API user agent

RELIAQUEST

Make Security Possible™

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