RELIAQUEST

SOLUTION BRIEF

RELIAQUEST FOR SAAS APPLICATIONS

The benefits of Software-as-a-Service (SaaS) applications are hard to ignore, and organizations are adopting them at an accelerated pace. But lack of transparency into vendor security policies and lack of visibility into cloud resources and activities make it challenging for security teams to protect data and users in these environments. While cloud-specific security tools better address the security needs of this new environment, they do not integrate well with the enterprise ecosystem. ReliaQuest delivers best-in-class protection and comprehensive security services by eliminating any blind spots and bringing singular visibility across SaaS applications and helps proactively identify and respond to various threats.

BENEFITS:

- Eliminate blind spots and gain singular visibility into SaaS resources and activities.
- Improve security posture with actionable metrics and coverage maps to industry-standard frameworks.
- Streamline security operations across your entire IT infrastructure – on-premises, cloud, and hybrid.
- Ensure confidence in detections with managed integrations

Gain Visibility into and Secure Your Saas Applications

Literally every enterprise application has a SaaS version – Office 365, Workday, Salesforce, Coupa, G Suite, Adobe – and the list goes on. But each has its own security policies and no standard way to share telemetry on resources or activities. This lack of transparency is a cause for concern among security operations members because they cannot gain holistic situational awareness and won't have insights into enterprise threats that use prominent cloud attack paths.

With a cloud-native Open XDR platform, GreyMatter, ReliaQuest unifies any and all telemetry from across the SaaS application environment, eliminating any blind spots and providing singular visibility that unifies data from across on-premises and cloud resources. Coverage spans but is not limited to activities such as authentication and authorization, administration, API access, file and folder access, and more. Additionally, GreyMatter unifies data from SIEM, EDR, CASB, 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 SaaS resources and activities, including but not limited to:

- Identify and access control
- Audit and security logs
- API access and activity
- Mobile access
- Location-based access
- Changes to admin controls
- Privileged and non-privileged access

Key Capabilities

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

Comprehensive and unified threat protection and response: Leverage ReliaQuest MDR services and Open XDR technology across on-premises and cloud applications to centralize alerts, reduce false positives, drive fast response, prevent threats and stay ahead.

Provide coverage for anytime, anywhere access: Close blind spots and cover attack surface expansions caused by mobile devices on open and public networks.

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.

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
Abnormal authentication scenarios: Compromise of OAuth applications or user accounts can lead to data compromise.	• Activity from an infrequent country • Impossible travel scenarios • Activity from terminated/disabled user
Misconfigurations: Expands the attack surface and can leave cloud resources vulnerable to attack.	• Data containing sensitive information (e.g., PII) observed • Addition of credential to an OAuth application • Office application – email forwarding rule added • Office application – shared file/folder publication
Exfiltration of data: A primary concern of organizations where sensitive PII, PHI, and PCI data is stolen or manipulated including dissemination, alteration, and deletion.	• Suspicious impersonated activity • Mass download of data • Office application – data accessed from personal account
Infiltration: Methods used to penetrate an organization's cloud services via account hijacking, network, or systems.	• Malicious OAuth application consent • Suspicious OAuth application observed downloading files

RELIAQUEST
Make Security Possible™

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