RELIAQUEST | zscaler

Make Security Possible.

HOW WE DO IT

ReliaQuest GreyMatter, a Security Operations Platform Built by Security Operations Experts

Firewall solutions like Zscaler are a critical component of a comprehensive cybersecurity strategy. Originally conceived to ease the analysts' burden of monitoring and filtering network traffic, Zscaler ingests data from both web and non-web sources from across the enterprise and provides alerts for review. While this solution is very effective in monitoring and alerting events, it can be challenging to keep optimized and derive continuous value. Analysts may find it difficult to constantly curate and update detection rule logic, and correlate events across hybrid environments.

ReliaQuest GreyMatter®

By integrating ReliaQuest GreyMatter with Zscaler, GreyMatter ingests, analyzes, and alerts on events generated by Zscaler. GreyMatter correlates these Zscaler events with events from other telemetry sources including endpoints, networks, and users for full visibility into a customer's security landscape. Armed with a unified visibility, customers can perform investigations and deploy remediation steps faster than ever before.

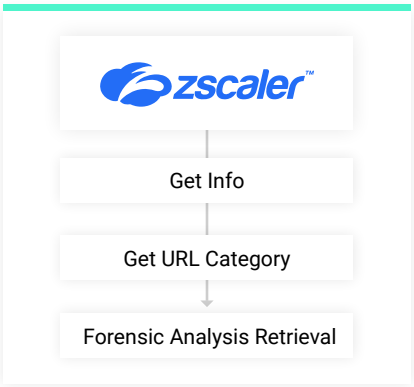
GreyMatter saves analysts additional time by providing users with the ability to update detection rules directly from the GreyMatter UI, based on the automated analysis of the compiled data gathered from their security ecosystem. It's never been easier to keep Zscaler continuously optimized against an ever-changing threat landscape.

Benefits:

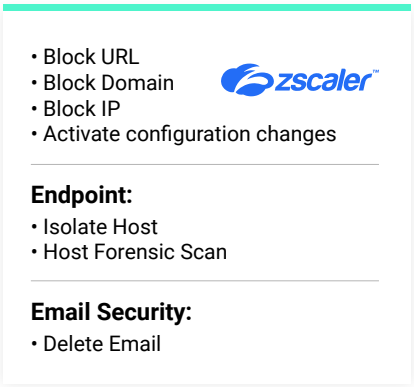
- Get unparalleled visibility across your security tools whether on-premises or in one or more clouds.
- Streamline, unify, and automate security operations processes to reduce MTTR from hours to minutes.
- Model the business impact of adding new security tools to your environment to help pick solutions that best meet the IT security needs of your organization.
- Improve security posture with actionable metrics and coverage that maps to industry-standard frameworks.

Leverage Your Existing Security Stack:

Detection: GreyMatter uses Zscaler to detect a malicious alert



Investigation: Actions for the Investigation section



Response: Actions for the Response section

Step 1: The GreyMatter platform uses Zscaler's detection capability and its advanced threat intelligence to detect when an executable file has been downloaded from a website that Zscaler classified as phishing.

Step 2: The detection alert is ingested into GreyMatter which initiates automatic queries to Zscaler for more information on the detected threat, such as indicators of compromise (IoCs) like the URL, domain, and impacted IP address. GreyMatter also obtains the executable's forensics analysis from Zscaler Sandbox. GreyMatter then correlates the Zscaler data with other security events such as endpoint logs, email security detections, and threat intelligence feeds to gain additional insight and a comprehensive view of the threat.

Step 3: GreyMatter records the case details by automatically writing up the investigation results analysis within its platform, notating that the event began with a phishing email to a user who clicked a link that directed them to a highly malicious webpage that auto-downloaded an executable.

Step 4: After that, GreyMatter uses its bi-directional API to send commands back to Zscaler for remediation to block the malicious URL and domain and the sender IP to prevent further communication with the business. GreyMatter also engages with the email security and endpoint tools to purge the phishing email from all recipients and isolate the affected host from the network to initiate a forensic investigation on the compromised system.

Step 5: The final step is for GreyMatter to notify the necessary team members of the actions made as well as any additional information, such as rule modifications to Zscaler.

Key Capabilities:

Singular visibility across your security tools: ReliaQuest GreyMatter, built on an Open XDR architecture, provides bi-directional integration across all security tools, whether on-premises or in one or more clouds, to ingest data and automate actions.

Round-the-clock monitoring: Leveraging its cloud native GreyMatter platform, ReliaQuest offers continuous monitoring of all resources, applications, and security tools for real-time situational awareness.

Field-tested detection content packages: Stay ahead of threats and reduce the impact of events with over 600 detection rules curated for mixed-vendor 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 reduce MTTR from hours to minutes.

MITRE ATT&CK framework mapping: Mapping 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.

The Results:

400%
Improvement in threat detection in the first 90 days.

12x
Increase in visibility accelerating threat detection and response.

35%
Reduction in TCO due to operating more efficiently.

RELIAQUEST®

reliaquest.com 800.925.2159 info@reliaquest.com