FORTINET | RELIAQUEST

SOLUTION BRIEF

Fortinet and ReliaQuest

Force multiply your security operations with the GreyMatter® cloud-native security operations platform integrated with the Fortinet Security Fabric

Executive Summary

ReliaQuest delivers successful security outcomes by force-multiplying an organization's security operations teams, uniquely combining the power of technology and security expertise. ReliaQuest GreyMatter integration with Fortinet enables organizations to increase visibility, reduce complexity, and effectively manage risk.

Challenges

Businesses all around the world are seeing ever-increasing threats against their IT environment, which in itself is dynamic. And as they bring in more enabling technologies to power the business, the attack surface expands—which they try to contain by bringing in new security tools. This only contributes to the tool sprawl. These security tools do not integrate with each other, leaving a landscape that is disparate and contributes to an unmanageable volume of alerts. In many cases, teams lack the talent to optimize these sophisticated security tools, leading to a short shelf life. Lack of integration hurts visibility, leading to blind spots, ineffective detections, and a swivel-chair approach that hinders investigations and results in more noise. And without a unified approach to detection, investigation, and response, security operations teams are further entrenched in fire drills and ill-equipped to efficiently confront threats and protect the business.

To drive better visibility, reduce complexity of security operations, and manage risk better, Fortinet FortiGate Next-Generation Firewall (NGFW) integrates with ReliaQuest GreyMatter, a security operations platform that is built on an open extended detection and response (XDR) architecture. It offers bi-directional integration with Fortinet solutions to ingest data and automate actions. It brings together telemetry from other security solutions, and combining them with data from the Fortinet products, delivers singular visibility across the enterprise ecosystem and unifies detection, investigation, and response to drive security effectiveness and cyber resilience.

Backed by world-class security operations proficiency, ReliaQuest helps security leaders make informed decisions on maturing their programs. It drives consistency, speed, and efficacies by enabling automation across the security operations lifecycle. It enables proactive risk mitigation by delivering continuously curated threat detection and hunting content packages, and preparation through attack simulation and remediation capabilities.

Joint Solution Components

- Fortinet FortiGate Next-Generation Firewall
- ReliaQuest GreyMatter cloud-native security operations platform

Joint Solution Benefits

- Gain full visibility and transparency as a customer, including ablity to participate and collaborate with SOC analysts when and where you want to.
- Leverage codified best practices so that each incident response workflow follows consistent path, reducing errors and false positives and improving mean time to remediation (MTTR) from hours to minutes.
- Utilize alert-level automation to screen out false positives and collect all relevant data for enrichment, eliminating tool-hopping and speeding investigations.
- Leverage the award-winning Fortinet FortiGate NGFW and the Fortinet Security Fabric for unparalleled security protection.

FORTINET FABRIC-READY

Joint Solution

ReliaQuest delivers a unified security operations workspace through which analysts can conduct detection, investigation, response, and resilience activities, eliminating wasteful tool-hopping. Automated data collection across relevant tools accelerates investigation processes. Built-in detection capabilities help map coverage across kill chain and MITRE ATT&CK frameworks, providing real-time snapshots of your risk posture and coverage gaps, regardless of environment: on-premises, hybrid, or cloud. Pre-built playbooks automate responses at machine speeds across commonly detected events to quickly contain threats.

Fortinet FortiGate NGFWs deliver industry-leading enterprise security for any edge at any scale with full visibility and threat protection. Organizations can weave security deep into the hybrid IT architecture, and build security-driven networks to deliver ultra-fast security end-to-end, enable consistent real-time defense with AI/ML powered FortiGuard Services, achieve seamless user experience with security processing units (SPUs), and improve operational efficiency and automate workflows.

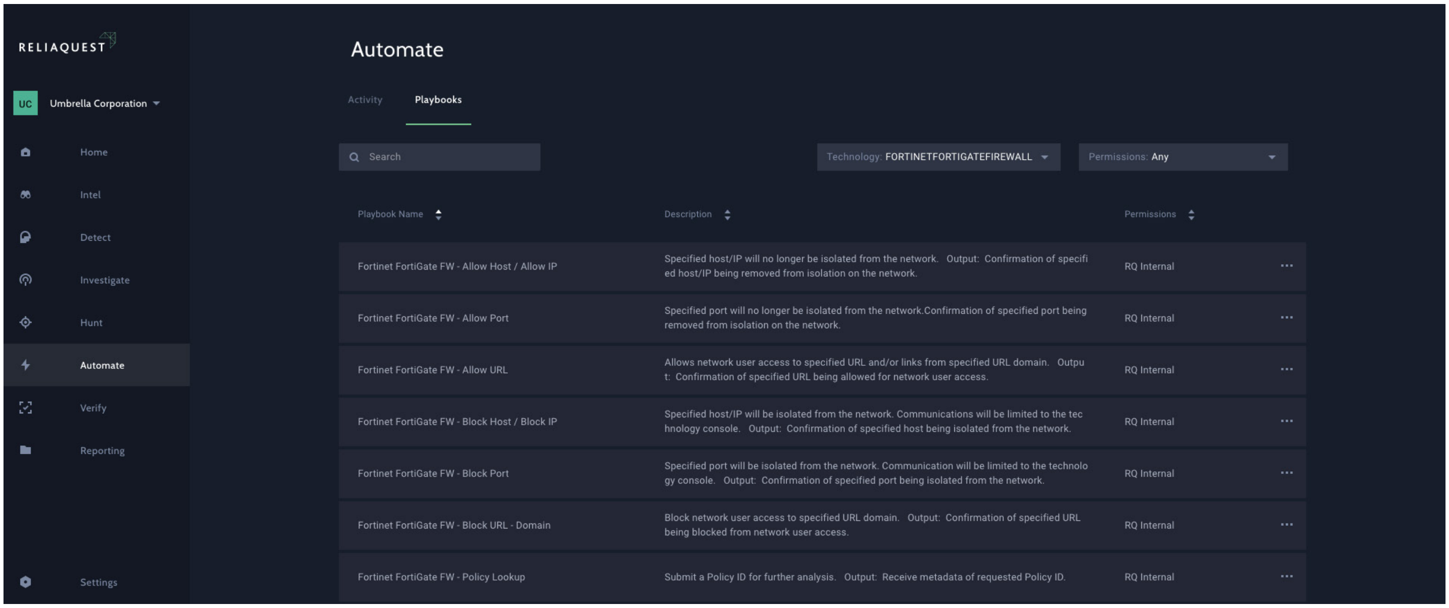
The FortiGate is a key part of the Fortinet Security Fabric, which is the industry's highest-performing cybersecurity platform, powered by FortiOS, with a rich open ecosystem. It spans the extended digital attack surface and cycle, enabling self-healing security and networking to protect devices, data, and applications. The Fabric can be extended across organizations via seamless integration with diverse Fabric-Ready technology alliance partner solutions. Enabling a broad ecosystem minimizes gaps in enterprise security architectures while maximizing security return on investment (ROI).

The process flow is as follows: Alert details from the FortiGate are sent to GreyMatter; investigation is performed, with Block Host actions being done in GreyMatter; commands are then sent to the FortiGate in real time to address the issue.

Joint Solution Integration

GreyMatter utilizes a bi-directional API connection to the customer's FortiGate devices. Within GreyMatter, an analyst can receive alerts of all severity and take actions in real time against those threats. The analyst can block specific sites, IPs, and even specific hosts, all of this without pivoting away from the GreyMatter console.

Available Automated Response Playbooks in GreyMatter for a FortiGate NGFW include the following: Allow Host/Allow IP, Allow Port, Allow URL, Block Host/Block IP, Block Port, Block URL – Domain, Policy Lookup.



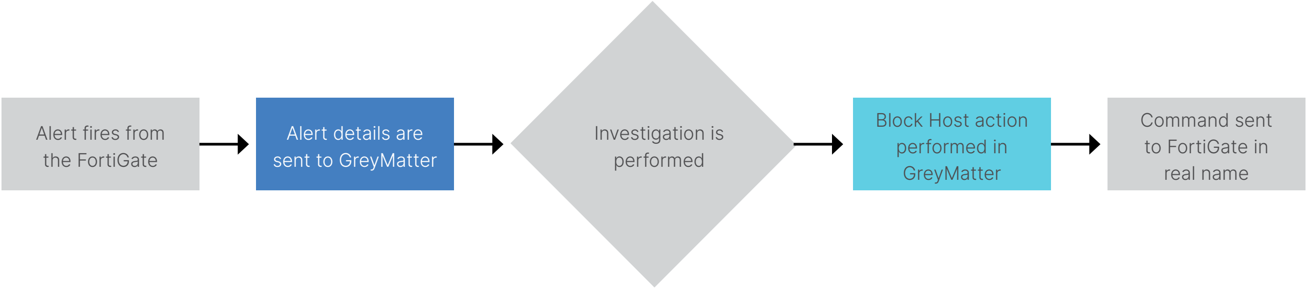
Technology: FORTINETFORTIGATEFIREWALL

Permissions: Any

Playbook Name	Description	Permissions
Fortinet FortiGate FW - Allow Host / Allow IP	Specified host/IP will no longer be isolated from the network. Output: Confirmation of specified host/IP being removed from isolation on the network.	RQ Internal
Fortinet FortiGate FW - Allow Port	Specified port will no longer be isolated from the network.Confirmation of specified port being removed from isolation on the network.	RQ Internal
Fortinet FortiGate FW - Allow URL	Allows network user access to specified URL and/or links from specified URL domain. Output: Confirmation of specified URL being allowed for network user access.	RQ Internal
Fortinet FortiGate FW - Block Host / Block IP	Specified host/IP will be isolated from the network. Communications will be limited to the technology console. Output: Confirmation of specified host being isolated from the network.	RQ Internal
Fortinet FortiGate FW - Block Port	Specified port will be isolated from the network. Communication will be limited to the technology console. Output: Confirmation of specified port being isolated from the network.	RQ Internal
Fortinet FortiGate FW - Block URL - Domain	Block network user access to specified URL domain. Output: Confirmation of specified URL being blocked from network user access.	RQ Internal
Fortinet FortiGate FW - Policy Lookup	Submit a Policy ID for further analysis. Output: Receive metadata of requested Policy ID.	RQ Internal

Figure 1: ReliaQuest GreyMatter automate screen where playbooks are executed with the FortiGate NGFW.

The process flow is as follows: Alert details from the FortiGate are sent to GreyMatter; investigation is performed, with Block Host actions being done in GreyMatter; commands are then sent to the FortiGate in realtime to address the issue.


Alert fires from the FortiGate
Alert details are sent to GreyMatter
Investigation is performed
Block Host action performed in GreyMatter
Command sent to FortiGate in real name

Joint Use Cases

Using GreyMatter to understand prioritized alerts from FortiGate NGFWs

Instead of dealing with a large number of alerts from the FortiGate NGFW, the analyst isprovided with an aggregated view of the prioritized alerts. This leads to greater efficiency by reducing the time required for analysts to chase false positives.

Performing action(s) in FortiGate through a GreyMatter playbook

By having the appropriate response actions and playbooks available in GreyMatter, an analyst can quickly act on potential threats without leaving the GreyMatter console, thereby improving efficiency and reducing MTTR.

About ReliaQuest

ReliaQuest delivers successful security outcomes by force multiplying an organization's security operations teams. It uniquely combines the power of technology and security expertise to make security possible for organizations by increasing visibility, reducing complexity, and managing risk. ReliaQuestGreyMatter is a cloud-native security operations platform that is delivered as a service any time of the day, any place in the world. Built on an open XDR architecture it offers bi-directional integration across any vendor solution, whether on-premises or in one or multiple clouds, to ingest data and automate actions. It brings together telemetry from any security and business solution to deliver singular visibility across the enterprise ecosystem and unifies detection, investigation, and response to drive security effectiveness and cyber resilience.

Hundreds of Fortune 1000 organizations trust ReliaQuest to operationalize their security investments, meeting them where they are regardless of maturity and helping them grow and improve their programs at their own pace. ReliaQuest is a private company headquartered in Tampa, Florida, with multiple global locations. For more information, visit www.reliaquest.com.

May 21, 2022 4:06 AM

1594201-0-0-EN