ReliaQuest GreyMatter for Operational Technology

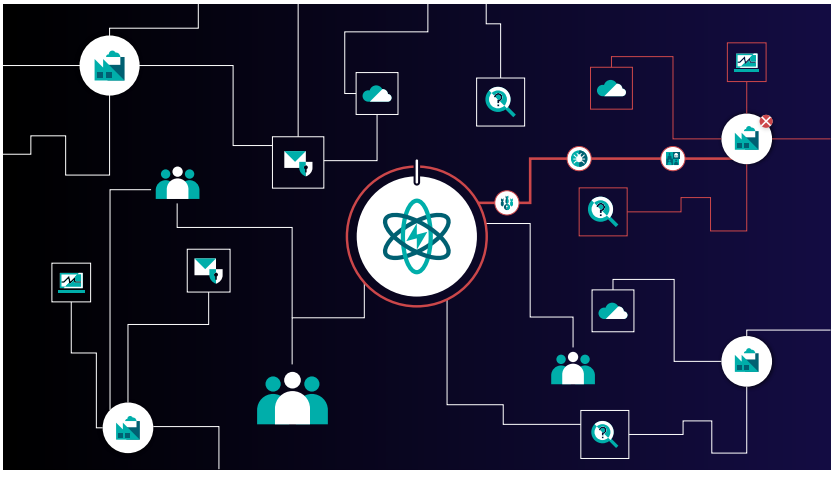
Improving Visibility and Managing Risk for Operational Technology Security

Operational technology (OT) is the hardware and software that controls and monitors physical processes, devices, and infrastructure. Securing OT environments is critical—a compromise in operational technology security can lead to serious business repercussions, including lost revenues, reputational damage, environmental damage, and even loss of human life.

Threat actors know how important OT infrastructure is, which makes it a high-value target.
The consequences of adversary activities can be devastating:

- Production and shipment stoppages that halt revenue
- Reputational damage Increased costs and reduced profits from interrupted production
- Patient lives in danger from compromised medical equipment

Digital innovation requires OT systems to interact with information-technology (IT) systems. While this connection improves efficiency, it also expands the potential attack surface and provide adversaries with a path to OT systems.



> "OT systems are usually very important for organizations. They are core systems for value and revenue creation. If they go down, they stall operations. The more connected they become, the more they expand the attack surface. This increasingly makes them attractive targets for ransomware and the development of targeted malware."

Gartner®, Market Guide to Operational Technology Security, Katell Thielemann, Wam Voster, et al, 4 August, 2022.

Operational Technology Security with the ReliaQuest GreyMatter® Security Operations Platform

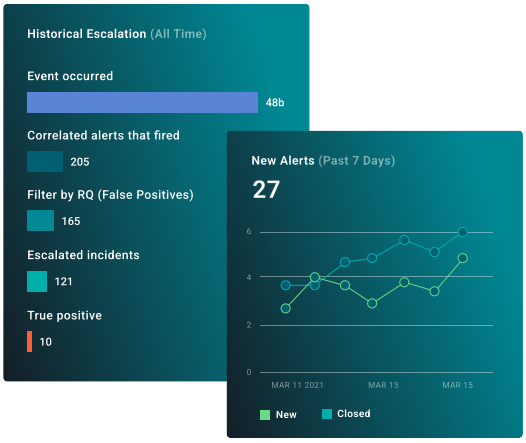
The ReliaQuest GreyMatter® security operations platform can help businesses secure both their IT and OT environments. GreyMatter allows organizations to leverage their existing security technology stacks to increase visibility, reduce complexity, and manage risk.

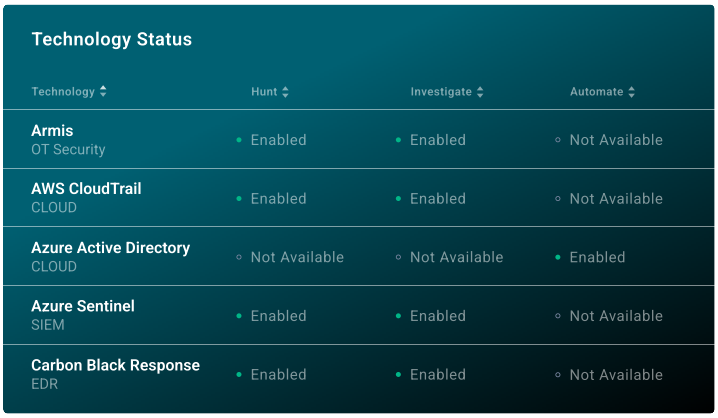
Alert On and Enrich OT Security Incidents

GreyMatter accelerates investigations and reduces mean-time-to-resolve for threats affecting OT environments. GreyMatter integrates with the OT security ecosystem on a bi-directional basis, enriching investigations to accelerate MTTR and prevent pivoting between consoles. This allows analysts to quickly understand incident significance and context as well as the impact on operations, facilitating remediation.

Visibility into OT

GreyMatter improves visibility to cyber threats in OT environments so security teams can understand and improve their organization's OT security posture. GreyMatter expands visibility by logging and alerting on OT environments specifically. This level of granularity, combined with continuous monitoring, prevents potential disruption of critical OT systems. Whether you or not an organization has an OT security solution in place, GreyMatter can integrate with your existing SIEM and leverage telemetry from network access control (NAC) technology, engineering/OT hosts, and EDR solutions. The resulting detections and continuous monitoring help to prevent potential disruption of critical OT systems.





Unify IT and OT Security Operations

Correlate IT and OT security incidents to deliver a consolidated view across both IT and OT environments. GreyMatter facilitates escalations for OT and IT threats with OT-specific processes and counters threats propagating between OT and IT environments.

RELIAQUEST®

reliaquest.com

800.925.2159

info@reliaquest.com