Comparison Chart

Comparing Managed Security Services: MSSP vs. MDR vs. ReliaQuest

Cyber threats continue to make headlines every day. Pair that with the ever-changing business landscape, e.g., migrating to the cloud or implementing hybrid work, and it's no surprise that businesses are finding it tough to keep up. Due to budget constraints or hiring difficulties, analysts are often left without the resources they need to move from manual, ad-hoc practices to proactive security. Constantly stuck in fire-drill mode, analysts don't have the time to shore up security before threats arise, leaving the business vulnerable.

Where Managed Services Come In

Managed security services vendors can help companies bridge these gaps. The most common approaches are managed security services providers (MSSPs) and managed detection and response (MDR).

Most managed services offerings, including MSSPs, provide 24/7 monitoring solutions—a boon to overworked SOC teams.

One step above that is managed detection and response (MDR), which moves beyond basic monitoring capabilities to include some threat intelligence and incident response at the endpoint.

For coverage and automation beyond the endpoint, the ReliaQuest GreyMatter security operations platform uses its Open XDR architecture to secure and automate the entire security operations lifecycle across any environment.

In this chart, we'll compare these three approaches across the most critical capabilities businesses are looking for when evaluating managed security services.

Capability	MDR	MSSP	ReliaQuest
24/7 monitoring	✓	✓	✓
Detection	Minimal, out-of-the-box	Detection content is a black box, unavailable for review, and often out-of-date	Detection content is available, continuously updated, and environment-specific
Investigation	Provider does not give additional context for alerts	Minimal alert context leaves your team to takes on the legwork	You get full context into all investigations across your environment
Response	Provides no containment or response actions	Response actions limited to endpoint	Provides automated response capabilities across customer ecosystem
Noise reduction	None—any and all alerts that come through the SIEM or other log sources reach your team	Minimal—often unclear how or why it triages alerts	Automation ensures only the most relevant alerts hit your desk
Tool support and optimization	May include some device management, such as firewall	Provides no support beyond its own tooling	Supports maturity growth of your SIEM and EDR platforms
Metrics	Reporting on a by-request basis that requires analysis on your end to decipher anything actionable	Generally, reporting on a quarterly basis meant to make the provider look good	Real-time measurement, always available in the platform Map and measure risk, understand coverage gaps, measure tool effectiveness, benchmarking and business unit comparison
Breach and attack simulations	✗	✗	GreyMatter Verify capability includes fully packaged, automated field-tested scenarios
Threat hunting	✗	Sometimes available as an add-on, but limited to endpoint	Fully automated across multiple tools and environments, including, optionally, cloud
Threat intelligence	✗	Obfuscated and unclear, unavailable to the end user	Our Intel function provides actionable threat intelligence that's fully viewable, searchable within the platform, and integrated with your technologies
Integrations	Usually limited to its own SIEM	Brings its own toolset, does not connect with outside tools	Vendor-agnostic, bi-directional integrations provide robust analysis and response across your environment
Customer success	Static, not invested in customer growth	Static, not invested in customer growth	Grows with you over time; a dedicated success manager works with you to create a security roadmap

Where ReliaQuest Wins

MSSP and MDR don't always fit the bill. Certainly, the monitoring coverage is nice, but what about detection and response? What about improving your maturity?

For companies looking to outsource cybersecurity because of a lack of talent or resources, ReliaQuest delivers successful security outcomes by force-multiplying an organization's security operations teams.

- ✓ We lead with technology. Instead of over-reliance on people or services, GreyMatter enables your team with automation.
- ✓ We're adaptable. Not only is "Adaptable" one of our company values, but it shows in our tech and support, too. We want to keep you secure across change events, new tools—whatever.
- ✓ We're invested in growing your business, both at the bottom line and in terms of maturity. Together, we'll build a roadmap to improving your security operations.
- ✓ We're worth it. A Forrester TEI study showed a 350% return on investment within 3 years.1
- ✓ We focus on transparency, consistency, and speed.
  - We're not a black box. We're here to enable your team, so you have full visibility into our processes.
  - We use insights from across our customer base to ensure all our customers are protected.
  - Automation makes things super-fast. With our help, you can cut your MTTR in half.[1]

1. *The Total Economic Impact™ of ReliaQuest*, Forrester, 2021.

> **Without a partner like ReliaQuest and the ReliaQuest GreyMatter platform, it would be hard for us to deliver the proactive security services of a best-in-class SOC.**

Dave Summitt, CISO
Moffitt Cancer Center