RELIAQUEST OPEN XDR VS MDR:

COMPARING MANAGED DETECTION AND RESPONSE SERVICES

Choose the right partner for your business.

As cybersecurity grows ever more complex, many businesses, especially those with limited resources, are turning to managed security solutions.

However, not all managed solutions are created equal. In this chart, we'll take a closer look at two of the most popular options, managed detection and response (MDR) and open extended detection and response (Open XDR-as-a-Service), and compare them on critical points to help your business decide which approach is the best fit.

What's MDR?

Managed detection and response is an approach whereby a third-party company manages your endpoint-focused threat detection and response capabilities. MDR can look beyond the endpoint, depending on provider.

What's Open XDR-as-a-Service?

XDR is the latest buzzword in the security industry. XDR goes beyond traditional endpoint strategy and holistically leverages your entire security infrastructure. So what's the "open" part? Most XDR approaches are limited to a single portfolio vendor, locking you into that vendor's toolset.

What's the "as-a-Service part"? It's a cloud native platform designed to continuously integrate existing security data and tools and apply threat research, detection, investigation response and security engineering capabilities, all wrapped with 24/7/365 security expertise. You get transparency, collaboration, and best practices—not just a ticketing service.

You get the value and outcomes of MDR and XDR without the management overhead.

Capability	ReliaQuest GreyMatter Platform Open XDR-as-a-Service	MDR
24/7/365 SOC support	Global support that includes threat detection and research, incident response, and security engineering	Often has only in-region, incident response support
SaaS/cloud-native platform	SaaS-native platform that can leverage cloud, hybrid, or on-prem security data sources	SaaS platform with support typically for on-prem or cloud data sources
Environment-specific detection content	Continuously curated signature and behavior-based detection content tuned for your technology stack, industry, and business needs	Broad IOC rule sets
Threat intelligence feeds	A threat intelligence platform (TIP) that curates, scores, augments, and deploys threat feeds across your environment complemented by a threat research team identifying and containing emerging threats	Various open source or proprietary threat feeds, often uncorrelated, creating noise and false positives
Reduced alert noise	Automated aggregation, escalation, and resolution of alerts, driving to 89% reduction in alerts, both false positives and duplicates	Alerts escalated to your team with no context or background; no scrubbing of duplicates, creating noise vs. value
Transparency of process and tools	Full visibility and transparency into the detection, investigation, and response process	✕
Metrics that matter for board-ready reporting	Reporting on MTTR and KPIs, and benchmarking against similar organizations for visibility, team performance, and tool efficacy via the patented Security Model Index	Reporting based on number of alerts
Solutions that can immediately improve the efficacy and efficiency of existing SOC technologies and processes	Customers see ROI in 30 days	Deploy monitoring agents immediately, but tuning and effective alert triage take time
Customer Success Manager	CSM regularly meets with your team to track progress, triage issues, update roadmaps, and recommend next steps. You have direct access to the SOC for on-demand expertise.	✕

Capability	ReliaQuest GreyMatter Platform Open XDR-as-a-Service	MDR
Strong project management, security architecture, and deployment services	World-class deployment and success program (91% customer retention)	Deployment services
Tool stack	Visibility and integration across your tech stack/current investments (includes cloud, SIEM, EDR, email, vulnerability, firewall, SOAR, etc.). Training "from the trenches" should you wish to learn best practices for your tools.	Vendor-provided EDR; not integrated with other tools
Purpose-built health monitoring	Goes across key technologies	✗
Roadmap and accountability to mature security program	Continuously developed and deployed detection content based on your environment and risks	Often gated at 25–50 detection use cases
Cross-client threat intelligence correlation	☑	✗
Behavioral based analytics (network effect; distillation of emerging trends across customer base)	☑	✗
Transparency into detection rule logic to coach new practitioners	Transparency into the origin of the use case itself to have more context when it fires, speeding analysis and improving decision making	✗
Proactive threat hunting for wide-ranging, fast-moving threats	Threat hunting team initiates threat hunting on your team's behalf as major risks unfold (e.g., Solorigate, Kaseya, etc.)	Varies by vendor
Integrated and interoperable toolset to coordinate on threat prevention, detection, and response	Enables reponse across customer-owned tools and platforms vs. MDR-only platform	✗
Automation at your pace	We are automating at the backend to continuously improve response times. When you are ready, we can make plays available to youor team for additional automation.	✗

RELIAQUEST

Make Security Possible™

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