RELIAQUEST

DATA SHEET

OPEN XDR-AS-A-SERVICE: AN INTEGRATIVE PLATFORM FOR YOUR CURRENT SECURITY STACK

Achieve XDR Outcomes Today with ReliaQuest GreyMatter

The Continued Reality for Security Teams

Every year it seems there is a new tool in security that will finally address the challenges security teams have been struggling with for years. The reality is, these tools aren't making security teams more efficient—but rather create more work and result in increased risk to the business. With too many tools and a lack of integration across them, teams look to add expertise, but still fail in their quest for greater visibility, and confidence that they are reducing risk. Security talent gets tired of being stuck in a reactive state and their skills do not get used to their full potential, often causing churn, setting security programs back even further.

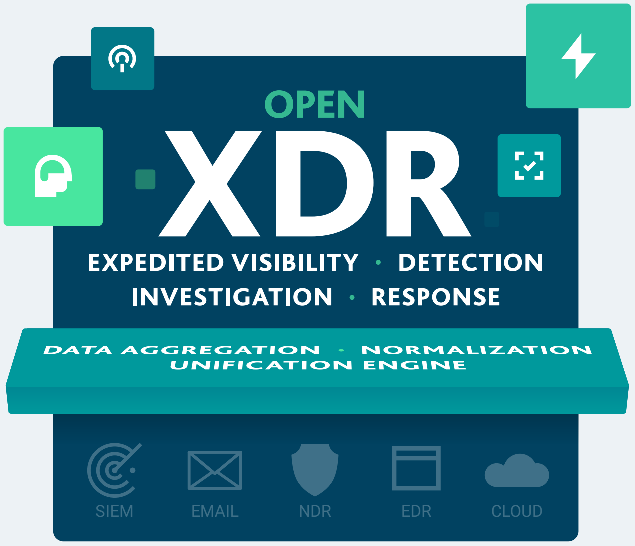
Common Challenges:

- ✕ Limited visibility requires pivoting across tools
- ✕ Complex integrations and configurations
- ✕ Ineffective use or ROI on existing investments
- ✕ Time wasted on repetitive, manual tasks

Will Open XDR Finally Make Security Possible?

While the terms XDR (extended detection and response) and Open XDR (cross-platform detection and response) may be new, the problems it solves and outcomes it delivers are not new to security teams. Jon Oltsik, principal analyst at Enterprise Strategy Group defined XDR as:

"XDR is an integrated suite of security products spanning hybrid IT architectures, designed to interoperate and coordinate on threat prevention, detection, and response. In other words, XDR unifies control points, security telemetry, analytics, and operations into one enterprise system."



While there are many benefits to XDR, there are some limitations that introduce new problems to security teams like continuous implementation of tools, stitched together integrations and taking years to realize XDR outcomes.

Open XDR allows your team to achieve unified visibility across your existing security investments. The platform facilitates ongoing, curated integration across technologies, enabling orchestration and automation across tools to investigate and resolve issues more quickly. With a foundation of Open XDR, you're able to achieve all the benefits your tools have to offer and deliver on your security program goals while still enabling the business.

The Path to Achieve Your Security Outcomes

Open XDR-as-a-service does not require your team to rip and replace anything that you've invested time or money into. It's an integrative approach that delivers the foundation security teams need to be more efficient and get to decision points faster in their day-to-day operations. A key component to Open XDR platforms is an integration layer that provides cross-technology visibility, detection, investigation and response capabilities without the pain of continually integrating, parsing, searching and normalizing that data when you need it. Or even worse, sifting through excel spreadsheets or multiple alerts from different tools to combine the data you need to get an accurate picture of what actually happened in your environment. The ultimate outcome of XDR is that your team can get out of reactive mode. Instead of filtering through alerts and making sense of the data, they can focus on the fun things in security, like threat hunting and attack simulations. Your team will be happier and able to better protect the business against your highest priority use cases, whether it's ransomware, insider threat, phishing, compliance regulations, or whatever is most important to you.

ReliaQuest GreyMatter delivers an Open XDR-as-a-service approach that enables organizations to force-multiply security operations through the unified detection and remediation of threats across their otherwise siloed IT architecture without replacing work that's already been done. GreyMatter is agnostic and provides the same high-fidelity investigation and response capability regardless of the integrated tool set. Within GreyMatter you can investigate and threat hunt across disparate data from your SIEM, EDR, firewall or anything else that is important to your workflow and drill into the returned results via a centralized dashboard. GreyMatter also unlocks your ability to execute a response across multiple vendor platforms, updating firewalls ACL's, disabling a user in AD and killing a process on an endpoint without ever leaving the GreyMatter interface. On average, our customers are saving 30 minutes per investigation. Imagine what that would be like for your team.

Features:

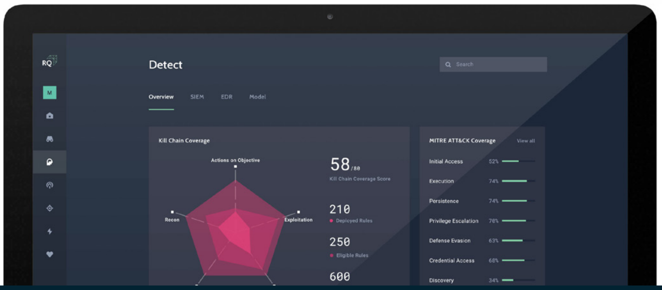
- ✓ Managed integrations across your existing investments
- ✓ Unified and normalized data for investigation, threat hunting, and response
- ✓ Continuous optimization of tools, detection content and controls
- ✓ Security expertise dedicated to your security program goals

Benefits:

- ✓ Respond to threats in 40% less time
- ✓ Operationalize and capitalize on existing security investments
- ✓ Increase efficiency with automated response, threat hunting and attack simulation

> **GreyMatter is part of our fabric—our strategic vision. It optimized operations and minimized risk.**
>
> -CISO, Leading Financial Services Organization

Learn how to increase visibility, decrease complexity, and reduce risk with ReliaQuest GreyMatter
www.reliaquest.com



RELIAQUEST
Make Security Possible™

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