When Your Organization Needs More Than MDR

WHITE PAPER

With security tool sprawl and wider diversification of threats, traditional managed detection and response tools often lack the functionality needed to adequately protect organizations and their users against data breaches. Consider an alternative: Open XDR-as-a-Service.

Cybersecurity is one of the great challenges of our generation. But what steps should organizations take to detect and respond to fast-emerging cybersecurity threats more quickly, efficiently and reliably?

A huge number of cyberattacks start as phishing attacks, and an alarmingly high proportion of those originate at the endpoint. The rapidly changing nature of the endpoint—from traditional network-connected desktop and notebook computers to smartphones, smart devices and the proliferation of the cloud—has made it challenging for organizations to ensure that their traditional security tools are up to the task. Not only that, but the endpoint alone represents only a subset of the information needed to detect, investigate and respond to a diverse and rapidly growing set of threats.

There's yet another challenge that must be acknowledged and accounted for: Organizations are struggling to get an accurate, up-to-the-minute inventory of what endpoints they have and the number of locations where those endpoints are deployed. This creates an increasing need to identify and track multiple inputs and outputs that extend far beyond the endpoint.

TechTarget® | Custom Media

RELIAQUEST

Cybersecurity tools such as security incident and event management (SIEM) solutions and service offerings like managed detection and response (MDR) have played important roles, but the eye-popping pace at which new threats are emerging has rendered such tools far less effective. In an era of remote work and widespread use of consumer-class devices, services and networks, new threats have surfaced and put intense pressure on enterprise security professionals.

Now add to the mix the impact of cybersecurity skills gaps on overworked and often under-resourced staff, as well as challenges in retaining security professionals already on staff. It's easy to see why new tools, new skills and even entirely new processes are needed.

Organizations need to go beyond ramping up their hiring of in-house security staff or buying more endpoint security products. A new approach is warranted: It's time for extended detection and response—or, more appropriately for today's challenges, Open XDR-as-a-Service.

Going Beyond Managed Services and MDR

For years, managed services and MDR providers have been the answer to supporting emerging and small security teams when the traditional endpoint format was the primary means of entry into applications, databases and other data sources.

But today's threat landscape is far different from that just a few years ago, and it is accelerating and spreading exponentially. The time to act is now, setting your foundation so you have an agile security program ready to meet the changing demands of your organization and the threat landscape. Threats are not only coming faster and at accelerating intervals, but they are targeting other points of entry, such as cloud computing, smart devices and nontraditional digital supply chain sources, such as HVAC, SCADA and ICS systems.

This rapidly evolving threat landscape needs a different approach to cybersecurity. Here's why:

- **Speed of entry for new threats.** The amount of time between a threat entering a system or application and when it is discovered—called dwell time—is long enough that hackers can exfiltrate data and be gone before anyone notices. Multiple cybersecurity consulting organizations say the typical cyberattack has a dwell time of at least a month, and a report from SANS Institute indicates that one in seven enterprises reported discovering **dwell times of up to six months**.[1] Another point to consider: IT security teams often don't even know if a business group is launching a new application or cloud service, or if a new merger brings with it new security threats.

- **Decentralized data and sprawling log sources.** Within network data, packet captures, cloud data, Active Directory data and email logs lies the context organizations need to address security issues and bring those dwell times down. But often this data is dispersed across cloud and on premises and typically has different "owners" in an organization. Tracking all this data down, accessing it and centralizing it to do comprehensive detection, investigation and response is the foundation of a solid security program.

- **Security tool sprawl.** Just as new threats have popped up in recent years, so too have new, purpose-built tools to combat them. While many of these tools have their place in the cybersecurity defense landscape, managing all those different tools has become too complex, costly and time consuming for most security teams.

- **Challenges hiring, training and retaining staff**. Facing a global cumulative shortage of at least 4 million security professionals, organizations simply cannot fill necessary positions fast enough to keep up with the rapid spread of threats—at least not on their own.

Research from Enterprise Strategy Group and the Information Systems Security Association (ISSA) notes that 76% of cybersecurity professionals surveyed said it is extremely or somewhat difficult to recruit and hire security professionals.[2]

While MDR providers, managed security service providers and various point products still play a role for many organizations, their limitations make them untenable in a new era of threat diversification and proliferation. Tools that focus only on analytics or just on the endpoint will not adequately address current and future problems.

[1] "SANS 2019 Incident Response (IR) Survey: It's Time for a Change," SANS Institute, July 31, 2019

[2] "ESG Research Report: The Life and Times of Cybersecurity Professionals 2021 Volume V," Enterprise Strategy Group and ISSA, July 28, 2021

How Open XDR-as-a-Service Extends Your Defensive Strategy

For these reasons, organizations should consider a new option that addresses the need for a comprehensive solution that does not require large incremental CapEx spend, additional software tools or new in-house security professionals. Open XDR-as-a-Service offers a flexible, efficient, intelligent and scalable way to confront the new challenges of cyber-risk now and in the coming years.

What is Open XDR-as-a-Service? It's a cloud-native platform that unifies security operations workflow between an outsourced security operations center and an enterprise's in-house security team to accelerate incident response. It enhances visibility, detection, investigation, response and resiliency functions that have been slowed and compromised in recent years by the wave of new, innovative and persistent attacks.

Unlike services alone, which take you only so far as a security operations team, or security tools, which need to be integrated to better detect and orchestrate response, Open XDR-as-a-Service meshes a modern technology platform that delivers automation across every stage of the security workflow with best practices from a team of security experts. This combination helps security leaders better identify, measure, communicate and reduce risk.

It also provides the key benefit of acting as a force multiplier for an organization's overworked and under-resourced in-house cybersecurity team. By collaborating with the skilled professionals of a proven third-party cybersecurity expert, organizations immediately benefit from access to a broad range of cybersecurity knowledge and problem-solving.

Open XDR-as-a-Service offers predictable costs, easy and fast scalability, and dramatically improved visibility into threats in your environment. It also acts as a hub for communication with organizational leaders outside of your security team for threat discovery, analysis and remediation.

Open XDR-as-a-Service offers a flexible, efficient, intelligent and scalable way to confront the new challenges of cyber-risk now and in the coming years.

How to Evaluate and Select a Solution

The first step in selecting the right Open XDR-as-a-Service option is determining your priorities. For instance, your organization may need a solution that is designed and deployed with real-world workflows in mind, so the solution closely maps to how work is done—and how data is utilized—in your organization's day-to-day activities. You might want to make sure that your solution is truly vendor-agnostic, meaning it seamlessly works with tools and data sources already deployed in your organization—each perhaps with different user interfaces, query languages and the like.

Maybe you just need a team of experts to respond to issues on your behalf. Perhaps you want to focus on cutting the amount of time necessary to fully investigate the location of, cause of and damage done by incursions. Or maybe you need access to very smart and highly experienced security professionals who have seen and dealt with the broad range of cybersecurity problems that threaten your organization.

ReliaQuest, a proven, experienced player in the cybersecurity space, offers a purpose-built solution that helps organizations detect and respond to threats, starting with an assessment of your environment, business priorities and risk concerns.

GreyMatter, ReliaQuest's Open XDR-as-a-Service platform, is a cloud-native solution that provides detection content tuned to your environment that can drive a 52% reduction in mean time to resolve. GreyMatter eliminates alert overload and provides transparency, best practices and metrics to show how your security posture is improving. When organizations partner with ReliaQuest, they are increasing threat coverage by 72% in three to six months.

GreyMatter speeds investigations with specific content that aligns to different types of threats. ReliaQuest's security analysts and threat intelligence teams are continuously developing and applying detection content as new threats emerge. Rather than receiving plain-vanilla alerts, organizations receive automatically assembled and highly customized research packages with all the information and tools necessary to investigate the cause, location and impact of threats—as well as recommendations on how to respond. ReliaQuest experts can also respond on your behalf.

According to ReliaQuest's customer research, "noise," which can cause confusion or mistakes in detecting and responding to threats, can be reduced by as much as 89% through automation provided in the platform.

All collected data, regardless of data source or security tool, is normalized to support visualizations, filtering and searches across the comprehensive data set. And, because GreyMatter is a SaaS-based solution, traditional CapEx investments are replaced with a predictable, easily controlled operating expense.

ReliaQuest optimizes efficiency by eliminating the need for hiring armies of security analysts to detect and respond to threats, while providing highly improved visibility into risks and threats that extend far past traditional endpoints and managed detection services.

Conclusion

Organizations need more help than ever to address the growing number of cyber-risks. Understaffed, underskilled and under-resourced teams must rapidly evolve their capabilities to match the proliferation of threats and protect their organization's short- and long-term success. Simply hiring more on-staff security professionals or buying yet another set of point products for individual tasks or threats isn't the answer.

ReliaQuest offers an enhanced security defense framework in a SaaS-based environment, combining the expertise and experience of ReliaQuest's security professionals with a user-friendly platform for shared transparency to help you quickly improve your security posture and program performance and reduce risk for your organization.

For more information, please visit www.reliaquest.com/greymatter/mdr/.

Don't limit your security program with a traditional approach to MDR. Take a strategic approach to up-level cybersecurity operations with ReliaQuest Open XDR-as-a-Service. We will help you evolve your security program to accelerate response times at the endpoint and beyond to cut noise, reduce risk, accelerate business initiatives and deliver meaningful metrics–all backed by a team of security experts.

Find out more at: www.reliaquest.com/greymatter/mdr/.