BINARY DEFENSE

WHITEPAPER

Don't Get Boxed In

Own Your Data With The Right MDR Partner

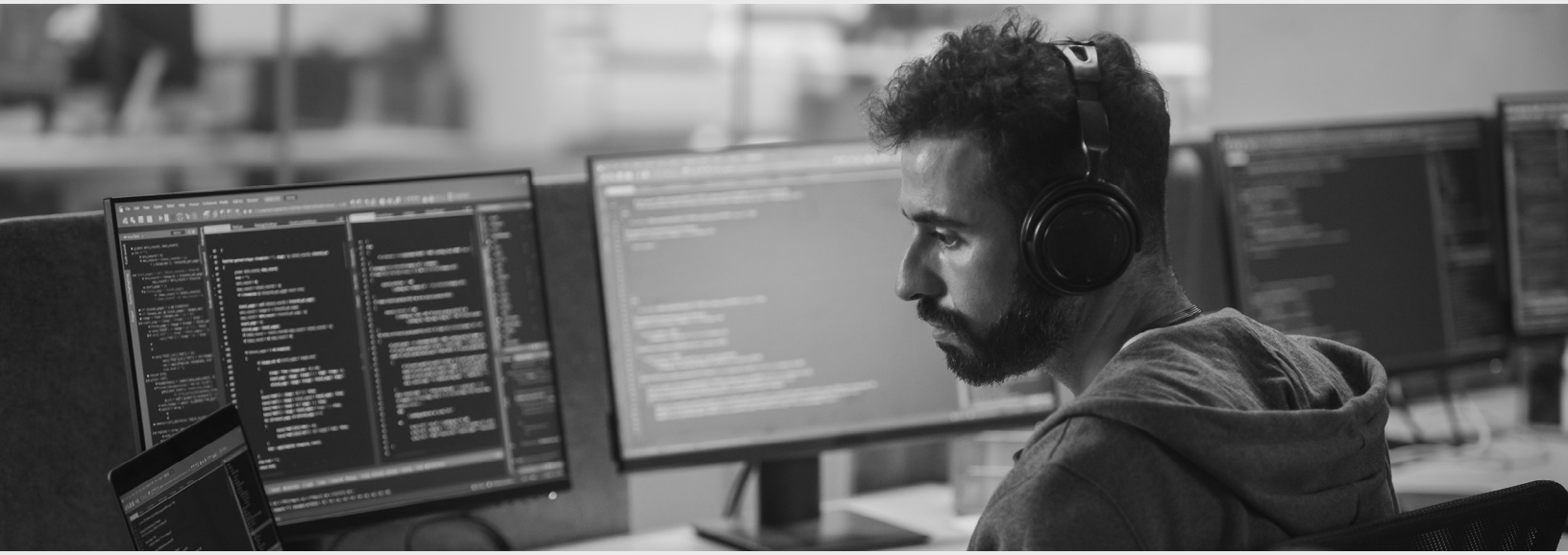
Authors:
Gracie Belle Smith,
Product Marketing Manager at Binary Defense
Israel Peedin,
Team Lead, Solutions Engineering at Binary Defense

Table Contents

Navigating The MDR Provider Landscape

Organizations that turn to Managed Detection and Response (MDR) providers face many challenges and often start from ground zero when searching for the right solution. Security professionals find themselves navigating the search for the right partner without a playbook, unaware of the pitfalls that may arise after selecting a vendor. In the MDR landscape, some solutions have taken the path of heavily relying on their platforms and making promises, only to leave clients feeling abandoned due to poor service delivery. The core issue? Most MDR providers adopt a one-size-fits-all strategy supported by a SaaS platform, which fails to deliver a truly personalized solution.

The voice of the customer frequently underscores issues such as losing detections upon contract termination, the hassle of ripping and replacing their technology stack, unfulfilled vendor promises, poor service delivery, the lack of access to a comprehensive security solution, and the shortage of expertise from MDR providers in their environment.



Vendor-Locked Contracts

When you partner with an MDR provider, you might assume any custom detections, automations, and playbooks remain yours. However, that's frequently not the case. MDR providers often require you to funnel all your data into their proprietary platforms built on the back of an undisclosed SIEM. This approach means if you decide to part ways, you lose access to certain data like custom detections, automations, playbooks, and even valuable context built over time within each investigation. Essentially, you're back to square one if you part ways with this vendor.

By contrast, a true Open XDR approach emphasizes working within your environment and letting you keep everything that is customized over the course of your partnership. MDR providers that take this approach believe that your data should remain exactly that—yours. An Open XDR model is designed to integrate seamlessly with your existing tech stack, ensuring your team retains full control over your data, custom detections, playbooks, automations, and investigations, even if our partnership ends. This approach not only empowers you but also ensures compliance with evolving regulations without the stress of managing third-party systems outside your environment.

Limited Expertise

There are several approaches to delivering Managed Detection and Response services, ranging from black-boxed to Open XDR models. A critical need for expertise often drives organizations and their security teams to outsource their SOC needs. Providers using the black box approach, often referred to as the Native XDR approach, work well within their own ecosystem of tools and often require clients to rip and replace their current security investments. Vendors that offer integrations with your security tools yet insist on building detections and use cases within their environment instead of your SIEM lack the in-depth knowledge needed to address complex issues outside their proprietary platform. This can lead to subpar service delivery and force you to allocate limited resources to resolve problems across multiple security tool vendors.

Conversely, MDR providers who work within your existing environment and utilize your preferred tools can save resources, keep data within your infrastructure, and enable SOC analysts to develop a comprehensive understanding of your business and environment nuances. This approach promotes more effective knowledge transfer and improves your ability to detect and respond to threats quickly.

Absence of Security Tool Co-Management

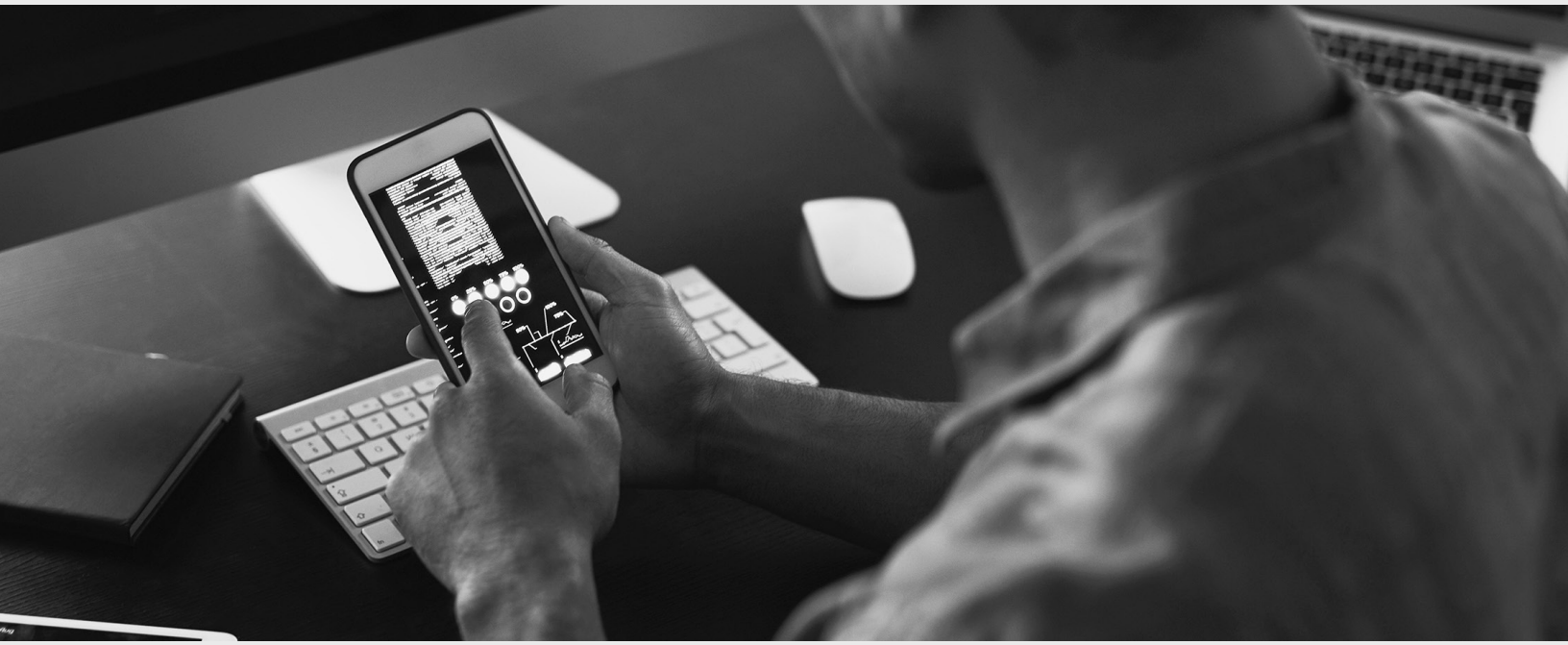
When you partner with an MDR provider, you might assume any custom detections, automations, and playbooks remain yours. However, that's frequently not the case. MDR providers often require you to funnel all your data into their proprietary platforms built on the back of an undisclosed SIEM. This approach means if you decide to part ways, you lose access to certain data like custom detections, automations, playbooks, and even valuable context built over time within each investigation. Essentially, you're back to square one if you part ways with this vendor.

By contrast, a true Open XDR approach emphasizes working within your environment and letting you keep everything that is customized over the course of your partnership. MDR providers that take this approach believe that your data should remain exactly that—yours. An Open XDR model is designed to integrate seamlessly with your existing tech stack, ensuring your team retains full control over your data, custom detections, playbooks, automations, and investigations, even if our partnership ends. This approach not only empowers you but also ensures compliance with evolving regulations without the stress of managing third-party systems outside your environment.

Quantity Over Quality

There are several approaches to delivering Managed Detection and Response services, ranging from black-boxed to Open XDR models. A critical need for expertise often drives organizations and their security teams to outsource their SOC needs. Providers using the black box approach, often referred to as the Native XDR approach, work well within their own ecosystem of tools and often require clients to rip and replace their current security investments. Vendors that offer integrations with your security tools yet insist on building detections and use cases within their environment instead of your SIEM lack the in-depth knowledge needed to address complex issues outside their proprietary platform. This can lead to subpar service delivery and force you to allocate limited resources to resolve problems across multiple security tool vendors.

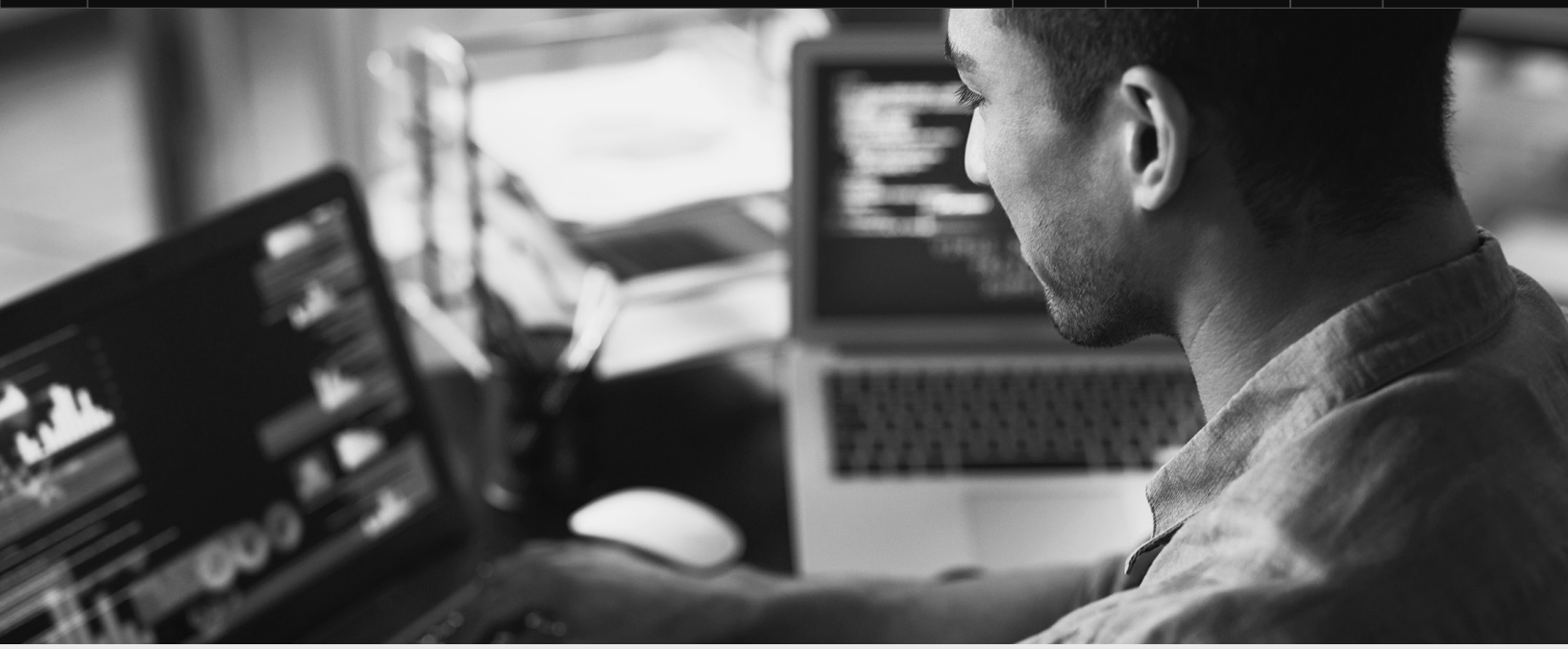
The ideal approach for customers is to work alongside the MDR detection engineers to develop a custom detection strategy tailored to the specific needs of their business and environment. By understanding the intricacies of your operational environment, the SOC analysts can provide a more personalized path to long-term security maturity. This tailored approach ensures that security measures evolve alongside your business, adapting to new threats and changes in your industry, ultimately offering more robust and effective protection.



Inflexible Tech Stack

Limited tech stack integrations can become a roadblock for customers looking to add security controls to their environment that aren't compatible with the MDR vendor's proprietary platform. While some providers claim to offer an Open XDR (Extended Detection and Response) approach, they often play well only within their ecosystem. This limitation forces businesses to adopt workarounds for custom log ingestion and parsing, leading to inefficiencies.

Not all MDR providers truly embrace the Open XDR philosophy. MDR providers with the expertise to integrate seamlessly with your existing security tools can eliminate inefficiencies caused by workarounds and ensure your data is used effectively and meaningfully. This flexibility allows the MDR provider to become a true enterprise security partner rather than just another vendor.



Multiple Vendors for Comprehensive Coverage

Many businesses find themselves piecing together various security solutions from multiple providers to meet their needs. This patchwork approach can be both costly and inefficient, often leading to gaps in coverage and increased complexity in managing multiple systems. MDR providers that offer a comprehensive enterprise security solution eliminate the need for a la carte purchases, providing a unified, cohesive defense strategy that is easier to manage and more effective in mitigating threats. These providers not only supply robust security measures but also deliver continuous monitoring and rapid response to incidents, which can significantly reduce the risk of breaches. Strong partnerships and a commitment to becoming a true enterprise security ally set these providers apart, ensuring businesses have reliable support and expertise to navigate the evolving threat landscape.

Unkept Promises

The MDR market is saturated with providers making lofty promises, yet many fall short in delivery. Over-reliance on automation can degrade the quality of context and investigation, leading to diminished service over time. This often results in false positives causing alert fatigue or, worse, missing true threats, leaving your organization to handle the fallout. Providers focused on feature-heavy roadmaps for their black-boxed platforms frequently shift priorities. When tech debt and a SaaS emphasis overshadow consultative service delivery, especially under the influence of private equity firms, the quality of service suffers, leading to unmet customer expectations. As MDR providers grow and expand, they often struggle to scale their support for service delivery. This can lead to a gradual decline in the quality of customer experience with analysts and support teams. MDR providers that focus on service delivery and value through outcomes prioritize fulfilling their commitments. Their human-driven, tech-enabled approach ensures that while leveraging automation for efficiency, the quality of service remains uncompromised. In addition to bringing in new talent to support their customer base, a customer-centric MDR provider understands that the customer experience should remain consistent or improve as their operations scale. They craft personalized solutions tailored to your needs, offering consistent and reliable protection against evolving threats.

In Conclusion

In conclusion, the key to successful MDR adoption lies in choosing a provider that offers a consultative and personalized approach. Look for solutions that respect your data ownership, develop a custom detection strategy, integrate seamlessly with your existing tech stack, and offer comprehensive security solutions. Avoid the pitfalls of vendor lock-in and unkept promises by partnering with a provider that values your long-term security posture and growth. If you're ready to take control of your data and enhance your security operations, consider exploring personalized MDR solutions. With the right approach and partner, you can navigate the complex world of cybersecurity with confidence and peace of mind. The landscape is ever-changing, but with a reliable MDR provider by your side, you can stay ahead of emerging threats and protect your organization's critical assets.

Explore Binary Defense's Cybersecurity Buyer's Guide to gain a deeper understanding of today's threat landscape, along with insight into the top cybersecurity solutions offered by Binary Defense including MDR, Threat Hunting, Digital Risk Protection, Phishing Response, Dedicated Resources and more.

Cybersecurity Buyer's Guide

BINARY DEFENSE

Binary Defense is a trusted leader in Managed Detection and Response (MDR), helping organizations across industries stay ahead of modern cyber threats. Our team of SOC analysts, threat hunters, detection engineers, and researchers works around the clock to deliver outcomes that matter: earlier threat detection, faster response, and stronger long-term security.

We take an attacker's mindset to defense, combining deep expertise with proactive tradecraft to protect what matters most.

Learn more at binarydefense.com, explore our blog for the latest insights, or follow us on LinkedIn.

600 Alpha Parkway, Stow OH 44224
sales@binarydefense.com