451 Research

S&P Global
Market Intelligence **Pathfinder**

Practical Requirements for Responding to Cyberthreats with MDR

COMMISSIONED BY

ALERT LOGIC™

APRIL 2021

About this paper

A Pathfinder paper navigates decision-makers through the issues surrounding a specific technology or business case, explores the business value of adoption, and recommends the range of considerations and concrete next steps in the decision-making process.

ABOUT THE AUTHOR

AARON SHERRILL

SENIOR RESEARCH ANALYST, INFORMATION SECURITY

Aaron Sherrill is a Senior Research Analyst for 451 Research, a part of S&P Global Market Intelligence, covering emerging trends, innovation and disruption in the Information Security channel with an emphasis on service providers.

Aaron joined 451 Research after serving as Vice President of Information Security and Chief Technology Officer for two large, pure-play managed service providers. He was instrumental in developing and growing the service provider business, driving the strategy and vision for the companies, developing and leading information security programs, and bringing new managed cloud and security services to the marketplace.

Aaron has 20+ years of experience across a variety industries including serving in IT management for the Federal Bureau of Investigation. He holds degrees in business and computer science, and has an MBA along with multiple certifications, including the Certified Information Systems Security Professional (CISSP) credential.

Executive Summary

Speed is of the essence when it comes to incident response. However, many organizations are surprised to discover that the response capabilities and approaches offered by threat detection and response providers can fall well short of expectations. Response is crucial and requires threat detection and response providers to be flexible and agile to meet the unique needs and requirements of each organization. Learning on the job is not fun or efficient.

Responding effectively to security events means that responses are tailored to each threat, system and execution environment, as well as to compliance and regulatory requirements, customer obligations, and the organization's overall risk appetite. While a threat detection and response provider can help organize, identify and orchestrate most of the key elements of response, organizations must recognize that preparation is an ongoing process that requires continuous refinement via updates and revisions.

Regardless of the type of threat detection and response provider an organization engages, preparing to respond requires security and IT teams to build a foundation that can enable rapid and effective response to all threats. This foundation is built through five core essentials: understanding the organization's tolerance for risk; establishing a priority and risk profile for each asset; applying statutory, regulatory and contractual requirements to response plans; recognizing the impact that expertise and resource limitations have on response capabilities; and developing a robust response playbook library.

This paper examines the value of preparing for security incidents and the factors that organizations should consider when preparing their approach to response. It also reviews how threat detection and response providers vary in their response capabilities, how organizations can leverage automated response, and how partnering with a managed detection and response provider can enhance the organization's ability to detect and respond rapidly to threats at scale.

Key Findings

- Half of midsize and large enterprises believe they are likely to experience a data security breach over the coming year.
- Slightly over half (52%) of organizations reported experiencing an increase in the number of information security incidents following the COVID-19 outbreak.
- Many organizations are transforming their approach to cybersecurity, shifting from an exclusive focus on prevention to a balanced strategy that incorporates prevention, detection and response.
- Over 57% of midsize and large enterprises believe their security staffing level is inadequate to handle the cybersecurity challenges they are facing today, yet only 22% plan to add to their security team in the coming year.
- Over a third of enterprises reported that improving incident response is one of their top strategic security objectives for the coming year.

- Only 46% of enterprises reported that they have a security operations center (SOC) in place, and many of those only operate their SOC during business hours.
- Being prepared for security incidents is one of the most cost-effective security measures an organization can take.
- While all threat detection and response providers aim to detect and ascertain the source of an attack, how they respond to an attack varies tremendously.
- Responding quickly to a successful cyberattack is essential. However, the response must be flexible and agile, able to adapt to an organization's unique requirements.
- Automated response is not an all-or-nothing endeavor. Organizations are employing a combination of manual, automated and human-guided automated response approaches based on their capabilities, resources, risk appetite, asset value, regulatory and customer obligations, and comfort levels. Even for a single security incident, practical strategic response may include a blend of all three approaches.

Compromise Is Inevitable

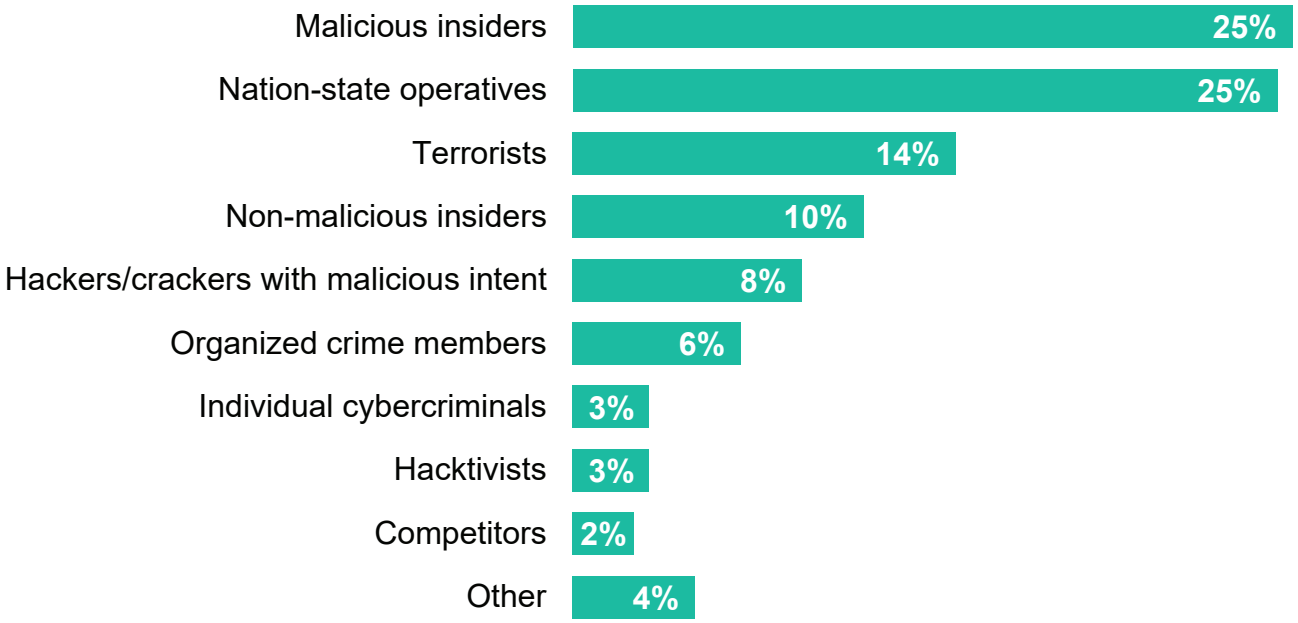
Organizations are discovering that the best and broadest of preventative controls are unable to stop all unauthorized access or malicious activity. The good news is that unless gross negligence is involved, organizations are rarely punished for being attacked or compromised. However, if they fail to respond to security incidents rapidly and effectively, the admonishments and penalties can be severe. As Muhammad Ali said, "You don't lose if you get knocked down; you lose if you stay down."

The impact and outcome of a compromise can be negligible for one business but could permanently cripple another. As the barrage of recent and well-publicized breaches has confirmed, the longer it takes an organization to detect and respond to a compromise, the more severe the consequences. The impact of these consequences can extend well beyond the immediate costs of operational disruption and lost revenue to include regulatory fines, reputational damage, customer churn and lawsuits.

According to 451 Research's Voice of the Enterprise: Information Security, Organizational Dynamics survey, 50% of midsize and large enterprises believe they are likely to experience a data security breach over the coming year. At the same time, 52% of organizations reported experiencing an increase in the number of information security incidents following the COVID-19 outbreak. Compounding matters, organizations stated that they are unprepared to deal with a variety of security threats (see Figure 1).

Figure 1: Organizations are unprepared to deal with a variety of security threat sources

Source: 451 Research's Voice of the Enterprise: Information Security, Organizational Dynamics 2020
Q: Which one of the following sources is your organization least prepared to deal with as a data security threat? (n=185)



Because of this, many organizations are transforming their approach to cybersecurity, shifting from an exclusive focus on prevention to a balanced approach that incorporates prevention, detection and response. The goal of this shift is to minimize the impact and scope of compromise through rapid identification, validation and remediation of active threats.

Unfortunately, many organizations are ill-equipped or unprepared to detect threats in real time and respond to those threats quickly and effectively 24/7. Organizations are finding that developing threat detection and response capabilities demands considerable resources and requires specialized expertise and systems to be effective.

Comprehensive Threat Detection Underpins Response Strategies

Many organizations are seeking to close these security gaps by partnering with a provider that can deliver threat detection and response services. But like most of the security market, the options available to organizations are numerous, with services and options varying substantially from provider to provider. Endpoint detection and response (EDR), network detection and response, cloud detection and response, security operations center as a service, managed detection and response (MDR), extended detection and response (XDR) – many of these terms are used in divergent ways, so it can be difficult for organizations to understand what each provider delivers and the outcomes that the organization should expect to achieve. As the saying goes, the devil is in the details.

Threat detection capabilities vary substantially among providers; many focus their services on a set of threat detection capabilities targeted for specific threat vectors. For example, a number of threat detection and response providers focus solely on detecting threats targeting the endpoint (EDR); this can be effective if an attack comes across an endpoint but provides limited, if any, benefits if the attack comes from another vector, such as the network or the cloud.

As attacks continue to grow in sophistication, enterprises are increasingly looking for providers that can deliver threat detection across multiple vectors, including endpoints, networks, applications, users, cloud services, email and IoT devices, as well as provide broad visibility and perspective to the threats targeting their organizations.

XDR DEFINED

XDR is a relatively new term that tends to describe a platform approach to threat detection aimed at empowering IT and security teams with the technology and tools to detect threats across multiple vectors. However, most XDR providers tend to focus on two or three threat vectors and are often limited to detecting threats in certain environments (e.g., on-premises) and primarily from their own proprietary technologies (e.g., endpoint agents). Providing limited to no expertise, XDR offerings require organizations to make significant investments in advanced security talent to cover 24/7 threat detection, investigation and response.

While acquiring the broadest range of detection capabilities possible is a plausible goal, this breadth of detection is only truly valuable when paired with deep, prioritized and contextualized insights that can help organizations react quickly and decisively to threats before damage occurs. In contrast to XDR, MDR providers tend to deliver coverage across a broad range of threat vectors, providing deep analysis and insights as well as the advanced expertise and guidance that many organizations lack.

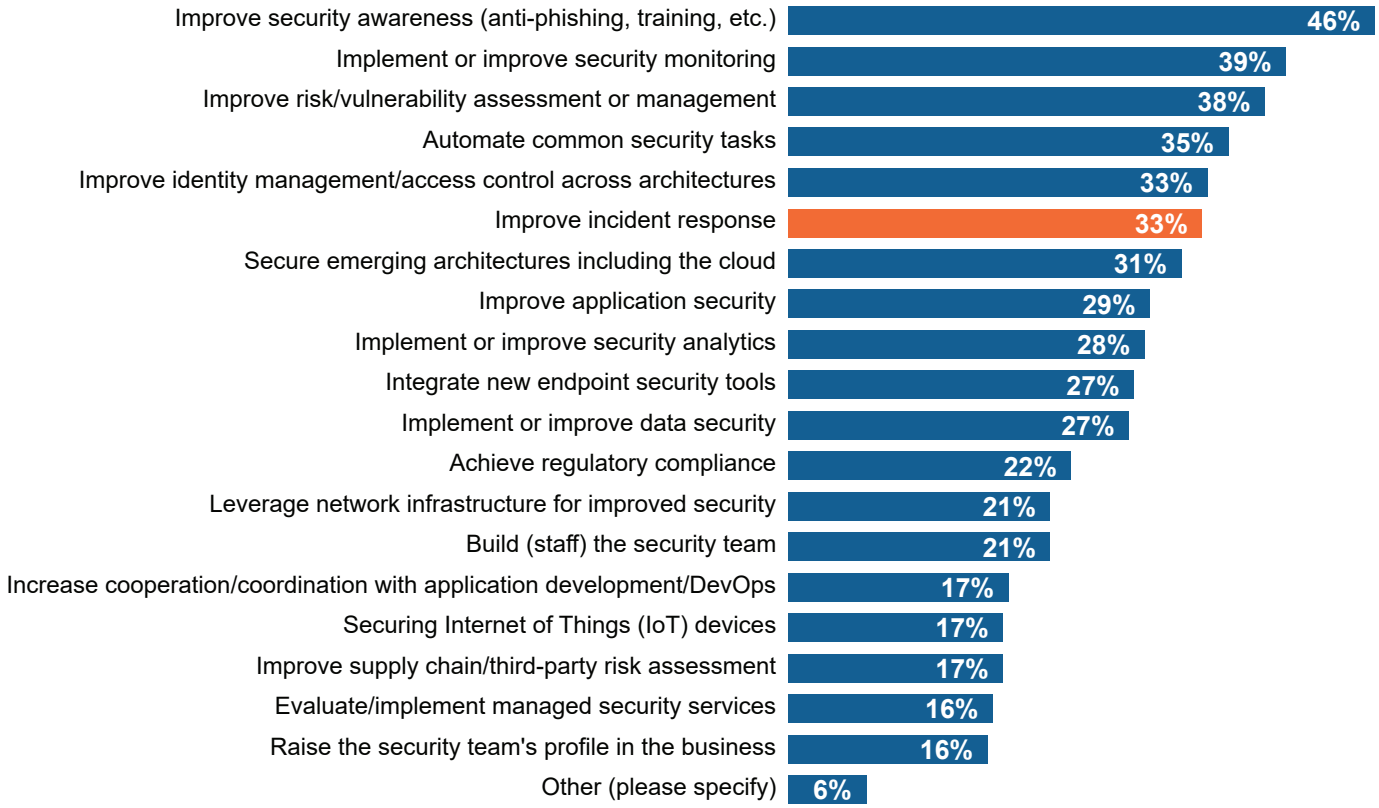
Preparing to Respond

Security and IT teams have many considerations when it comes to response. While all of them are valuable to some extent, if they lack depth and are built on a narrow scope of threat detection, organizations will likely fail to achieve the outcomes they desire. In short, preparation pays off. Being prepared for security incidents is one of the most cost-effective security measures an organization can take. Being prepared is the key difference between an organization responding to a security incident versus reacting to it. The difference between the two is anything but trivial. A response to an active threat is planned and engineered to produce a desired outcome, whereas reacting to a security event is done in the moment, based on the moment, hoping for the best. Reacting tends to be a matter of surviving and often results in a situation that is worse than the original event.

In a recent 451 Research study, over a third of enterprises reported that improving incident response is one of their top strategic security objectives for the coming year (see Figure 2). However, improving incident response requires more than purchasing and implementing new technologies.

Figure 2: Top strategic security objectives

Source: 451 Research's Voice of the Enterprise: Information Security, Budgets & Outlook 2020
Q: What are your top strategic security objectives for 2020? Please select all that apply.
Base: All respondents (n=242)



Effectively responding to security events means that responses are tailored to each threat, to each system, to each execution environment, to compliance and regulatory requirements, to customer obligations, and the organization's overall risk appetite. While a threat detection and response provider can help organize, identify and orchestrate most of the key elements of response, organizations must recognize that preparation is an ongoing process that requires continuous refinement via updates and revisions.

Regardless of the type of threat detection and response provider an organization engages, preparing to respond requires that security and IT teams build a foundation that can enable rapid and effective response to both known and unknown threats. This foundation is built through five core essentials: understanding the organization's tolerance for risk; establishing a priority and risk profile for each asset; applying statutory, regulatory and contractual requirements to response plans; recognizing the impact that expertise and resource limitations have on response capabilities; and developing a robust response playbook library.

Understand the Organization's Risk Tolerance

Understanding the organization's risk appetite is a key first step to preparing to respond to security incidents. Not only does a clearly defined and articulated risk appetite enable the organization to prioritize resources and spending on areas where it has the lowest tolerance for residual risk, but it also provides an anchor point for how responses to security incidents should be escalated and executed. This alignment ensures that response efforts achieve the outcomes that support the business's goals and needs.

For example, organizations with a low risk tolerance may find it acceptable to immediately isolate customer-facing systems and applications to mitigate a potential threat, while others are willing to accept more residual risk in order to maintain availability, favoring less-invasive measures to address threats. While risk appetites will vary from organization to organization and evolve over time, the appetite for risk will also vary by asset, application, data type, execution venue, regulatory requirements and customer agreements.

Establish Asset Estate, Priority and Risk Profiles

In order to protect data and assets (applications, users, networks, databases, APIs, etc.), organizations must first know that they exist. Maintaining asset visibility across the organization's digital footprint is becoming increasingly difficult as applications and services are progressively procured and implemented outside of traditional IT processes. New asset types, emerging technologies, the shift to remote work, mergers and acquisitions, and cloud-based services are only adding to these challenges.

MDR providers are increasingly adding technologies and capabilities to help organizations identify and understand their overall attack surface. Asset and attack surface discovery provides continuous visibility of the organization's entire digital real estate, delivering insights about the relevance of assets, enabling the prioritization of response and remediation efforts, and helping teams demonstrate the value and effectiveness of the security services they are delivering to the enterprise.

Understand and Apply Statutory, Regulatory and Contractual Compliance Requirements

Responses to threats and attacks not only need to consider the target assets and the organization's tolerance for risk, but responses must also be crafted with regard to obligations to customers via service-level agreements (SLAs), third-party agreements and regulatory requirements. While most IT and security teams are focused on identifying and responding to security incidents, they often fail to recognize that their obligation does not end after taking corrective action or restoring operations. Security provisions in contracts, state and federal laws and SLAs all have deadlines for reporting or responding to potential breaches. These requirements can have a significant impact on how the response to a security event is executed.

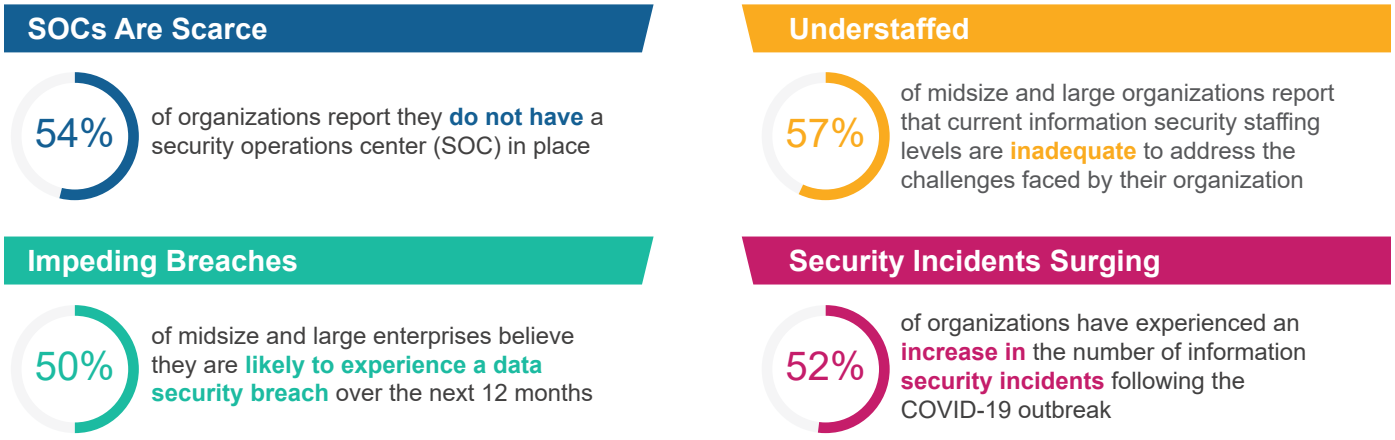
Recognize Expertise and Resource Limitations

Finding the expertise and capacity needed to respond to an ever-increasing volume of security events can be overwhelming for even the most well-funded security programs. The expertise shortage has been well-publicized over the past decade, but the problem may be worse than most organizations realize. Over 57% of midsize and large enterprises believe their security staffing level is inadequate to handle the cybersecurity challenges they are facing today, yet only 22% plan to add to their security team in the coming year (see Figure 3).

The lack of security expertise is significantly impacting organizational efforts to protect the enterprise. According to 451 Research data, only 46% of enterprises have a security operations center in place, and many that do only operate their SOC during business hours. At the same time, the security talent enterprises have on staff tend to be generalists who lack deep expertise in critical areas such as incident response, forensics, application security, network security and cloud security.

Figure 3: Barriers to improving the organization's security posture

Source: 451 Research's Voice of the Enterprise: Information Security, Organizational Dynamics and Digital Pulse: Coronavirus Flash Survey, June 2020



Recognizing and acknowledging the organization's capacity and expertise limitations is a key factor when preparing a response strategy for security events. For most organizations, the gap will not be addressed by simply hiring the needed talent – the pool of talent to hire from is scarce and expensive. And while training is a key initiative for many security and IT teams, training takes time and fails to address capacity constraints. Many organizations are finding that partnering with a managed detection and response provider not only provides needed capacity and expertise but can also be a catalyst to improving their overall security posture.

Develop Playbooks

Security playbooks – prescribed steps to respond to specific incidents and threats – can significantly limit the negative impact of a security event, decrease response time, and increase response effectiveness by minimizing the mistakes that can arise from spur-of-the-moment decisions. Addressing each type of cyberthreat with its own playbook ensures that incidents are handled in a consistent manner and that errors are minimized while enabling security and IT staff to scale and handle complex incidents.

However, codifying response processes into a playbook can be an imposing task for most security teams. Creating playbooks requires careful and thoughtful planning and constant updating – a challenge for understaffed teams who are faced with a long list of competing priorities. Rather than developing playbooks on their own, many organizations are leveraging security playbooks from managed detection and response providers. Armed with a robust library of customizable playbooks based on threat intelligence and frameworks like MITRE ATT&CK, managed detection and response providers can deliver insights and capabilities that most organizations would struggle to match.

It is also worth noting that playbooks are one of the key building blocks for automating response processes to security events. While full-scale automation may not be a near-term goal for many enterprises, automation is quickly becoming a key factor in scaling rapid response to the continuously surging volume of security events that organizations are facing.

Types of Response

While all threat detection and response providers aim to detect and ascertain the source of an attack, how they respond to an attack varies tremendously. At one end of the spectrum are providers that offer a full range of response capabilities that can be tailored for each organization. At the other end are providers that only notify customers of identified threats. While most threat detection and response providers tend to offer a range of response capabilities, it is important to understand how these response capabilities differ from provider to provider.

Simple Notification

For many threat detection and response providers, the scope of response stops with notification. Once notified, security or IT teams must formulate their own response. While this approach may be ideal for a robust and experienced security team that wants to control response from end to end, it can fail to meet the expectations of organizations that are seeking guidance, analysis, recommendations and assistance.

The reliability of threat notifications also varies among providers. While many providers quickly pass notifications to customers in an attempt to lower their mean time to detect, they also pass along many false-positive alerts. Providers that vet and validate events and threats before notification can add significant value.

Another often-overlooked consideration is that many providers notify customers of security events via email. Organizations quickly discover that email is a poor medium to manage events that may require immediate investigation or response. Although many providers integrate with common support and ticketing systems, customers are often responsible for escalation. Modern providers offer customers mobile apps that enable security and IT teams to review security event details, approve response actions or escalate for further investigation. This can be ideal for organizations that are not staffing a SOC 24/7.

Notification with Response Guidance and Recommendations

Although some providers' response process stops with notification, many providers will not only notify customers of a security event, but also provide prescriptive analysis along with guidance and recommendations for response. This analysis enables IT and security teams to contextualize threats and prioritize response efforts. Although organizations are responsible for executing response actions, the additional guidance and actionable advice can be helpful for teams that have limited expertise or incomplete playbooks.

Containment/Blocking

Many threat detection and response providers offer capabilities that go beyond notification and advice to include more robust measures such as containment and blocking. Spanning manual, semi-automated and fully automated response actions, these measures can include disabling accounts, pushing configuration changes to third-party technologies and isolating compromised hosts.

The goal of threat containment is to quickly stop and disrupt an attack and minimize its impact. Organizations can predetermine actions the provider can take on their behalf, with which assets, under what conditions; they can outline which assets or conditions require review and approval, and which circumstances they will handle through other countermeasures. This flexibility enables organizations to evaluate each event with regard to the asset's risk profile, the organization's risk tolerance and compliance requirements.

Remediation/Eradication

Remediation takes various forms: manual or automated remediation actions, consultative services, and boots on the ground for more complex situations. The goal is to fully eradicate the threat and root cause from the organization's IT ecosystem and prevent reoccurrence. For more complex or involved instances, providers may offer professional services or partner with a third party to assist organizations in eradicating threats from their environment.

Recovery/Restoration

Recovery/restoration is a distinct discipline that is outside the scope of services offered by most threat detection and response providers. While response aims to contain and neutralize the impact of threats and events, recovery aims to restore systems to their initial state.

Breach Management

Breach management is another distinct discipline that is typically outside the scope of services offered by threat detection and response providers. A few providers offer professional services that include assessing a customer's preparedness, building breach response capabilities, creating communication and notification plans, data forensics, evidence collection, and malware analysis. However, most providers partner with third-party specialty firms to deliver these services.

Figure 4: Overview – types of response from threat detection and response providers
Source: 451 Research

Simple Notification	Once notified, security or IT teams must formulate their own response. Ideal for a robust and experienced security team that wants to control response from end to end.
Notification with Guidance and Recommendations	Provides prescriptive analysis along with guidance and recommendations for response, enabling IT and security teams to contextualize threats and prioritize response efforts.
Containment/Blocking	Spanning manual, semi-automated and fully automated response actions that include disabling accounts, pushing configuration changes and isolating compromised hosts.
Remediation/Eradication	With the goal of fully eradicating the threat from the customer's IT ecosystem and preventing reoccurrence, remediation takes various forms – manual and automated actions, consultative services and boots on the ground for more complex situations.
Recovery/Restoration	A distinct discipline that is typically outside the scope of services offered by threat detection and response providers. May be offered as a professional service or through partners.
Breach Managment	A distinct discipline that is typically outside the scope of services offered by threat detection and response providers. May be offered as a professional service or through partners.

A Phased and Strategic Approach to Response

Responding quickly to a successful cyberattack is essential. However, the response must be flexible and agile, able to adapt to an organization's unique requirements. While many organizations are prepared to adopt automated response to threats for a portion of their IT ecosystem, many others are still leery of unintended consequences that automation may trigger. Organizations are seeking response capabilities that can adapt to the needs of specific systems, environments, workloads and threats, as well as enable a systematic adoption of automation at strategic points, providing as much or as little human intervention as desired. Such capabilities require a combination of manual response, human-guided automated response and fully automated response.

Manual Response

Most organizations still prefer manual response because they are comfortable and familiar with that approach, and they see it as a safer option than automated response with its unknowns and potential/perceived risk. However, manual response is becoming increasingly difficult to justify because of the low efficiency, high costs and delayed response times involved with manually addressing an increasing volume of events.

Although automated responses can better address most threats and events, manual response is still a valid approach for certain use cases. For example, an automated response may not adequately address unknown or complex threats and security events that require a more methodical approach. Manual response also may be a preferred approach for highly interconnected systems, for unknown systems, or in cases where operational integrity is a primary concern (e.g., critical infrastructure such as power and water systems). Even so, driving toward automated response often brings benefits that outweigh most potential or perceived risk.

Fully Automated Response

On the opposite end of the spectrum is fully automated response. Most threat detection and response providers incorporate automation into their detection capabilities. Ingesting, normalizing, parsing and correlating security data from disparate security sources and enriching event data with threat intelligence to enable informed, context-aware, intelligent decisions significantly minimizes the mean time to detect while empowering tremendous scale, consistency and efficiency.

Applying this level of automation to response actions can enable organizations to contain and disrupt threats with both speed and scale. The ability to automate multiple types of response beyond a single vector and across multiple types of systems is crucial because more sophisticated threat actors exploit diverse vectors to compromise systems. With preplanned and customized playbooks, threat detection and response providers can ensure that automated response evaluates actions in the context of the asset's risk profile, the organization's risk tolerance and compliance requirements.

Although the benefits of automated response are significant, many organizations are hesitant to fully embrace automated response for every system and every type of threat. Most organizations are adopting fully automated response for less-critical systems and for well-known, commodity threats, steadily and methodically increasing the use of fully automated response across a wider range of use cases as they see positive results and begin to feel more comfortable with automation.

Human-Guided Automated Response

While manual response has strategic value in certain situations, and broader adoption of fully automated response is a long-term objective, organizations are finding that the ideal solution for most use cases is human-guided automation. Human-guided automation brings together the speed and scale of fully automated response with oversight and intuition for an effective and scalable approach and strategy to incident response.

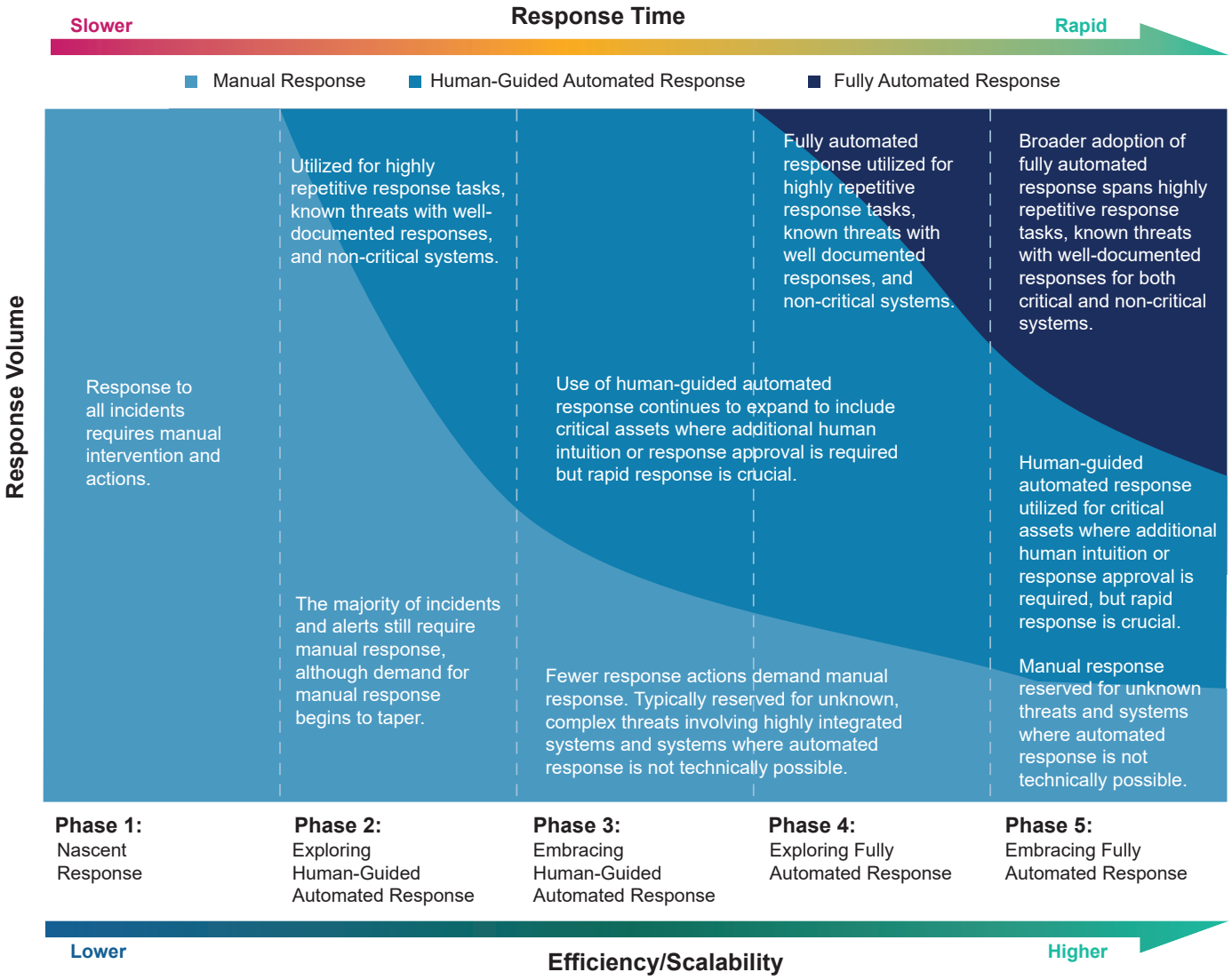
Automated response, infused with human decision points, can dramatically improve incident resolution capabilities and eliminate many of the repetitive tasks that are overwhelming IT and security teams and hindering rapid response. At the same time, human-guided automation helps facilitate the building of trust in playbooks, automated response actions, and the recommendations provided by threat detection and response providers. As organizations experience the benefits of automated response, they are becoming more comfortable with implementing it on a greater scale. This will only continue to expand as artificial intelligence/machine learning (AI/ML) and context-aware threat intelligence enable knowledgeable, discerning and reliable automated response processes.

Strategic Response

Automated response is not an all-or-nothing endeavor. Organizations are employing a combination of manual, automated and human-guided automated response approaches based on their capabilities, resources, risk appetite, asset value, regulatory and customer obligations, and comfort levels. Even for a single security incident, a practical strategic response may include a blend of all three approaches.

Figure 5: A strategic/phased approach to response

Source: 451 Research



A phased approach to response is a common journey for security and IT teams as they aim for broader adoption and usage of automation in their response to security events. However, implementing and managing security automation and orchestration systems along with security tool integrations and workflow systems can be a significant obstacle to broader automation adoption. Modern threat detection and response providers with broad response capabilities enable organizations to methodically and strategically adopt an automation strategy that best fits individual use cases within their IT ecosystem.

Conclusion

It's inevitable that a breach will happen no matter how many preventative controls are in place. While preparation and automation are key components to effective and rapid response, it is the combination of a threat detection platform with broad detection capabilities augmented by threat intelligence and human expertise that underpins successful response. Flexible and agile automated response capabilities infused with insights from AI/ML and human analysis can be a force multiplier for security and IT teams.

The impact and benefits of rapid and efficient incident response cannot be overstated – reduced operational costs, lower risks, improved security posture and retained customer trust, to name a few. While it may be tempting for some organizations to build out their own threat detection and response capabilities and SOCs, most will find that developing these capabilities and staffing a SOC for 24/7 operations is a significant, time-consuming and costly challenge. Organizations may find that partnering with a managed detection and response provider can enable them to quickly realize these outcomes and achieve security at scale across an increasingly diverse IT ecosystem.

To learn more about MDR, download the *MDR Buyer's Guide*.

451 Research

S&P Global
Market Intelligence

About 451 Research

451 Research is a leading information technology research and advisory company focusing on technology innovation and market disruption. More than 100 analysts and consultants provide essential insight to more than 1,000 client organizations globally through a combination of syndicated research and data, advisory and go-to-market services, and live events. Founded in 2000, 451 Research is a part of S&P Global Market Intelligence.

NEW YORK
55 Water Street
New York, NY 10041
+1 212 505 3030

SAN FRANCISCO
One California Street,
31st Floor
San Francisco, CA 94111
+1 212 505 3030

LONDON
20 Canada Square
Canary Wharf
London E14 5LH, UK
+44 (0) 203 929 5700

BOSTON
75-101 Federal Street
Boston, MA 02110
+1 617 598 7200