



HERJAVEC
GROUP

Detect, Block and Disrupt Threats with
Managed Detection and Response Services

The Dynamic Threat Landscape

IT environments have shifted dramatically in the past year. While the changes have been profound for many organizations, they were an extension of a trend that's been developing for some time: a continuous evolution of the dynamic threat landscape.

Threat actors are resourceful and creative. Whether they take full advantage of a world plunged into chaos due to COVID-19 or launch a targeted attack on a major supply chain vendor, they're constantly innovating and finding new opportunities to infiltrate corporate environments.

Disrupting Sophisticated, Targeted Threats

Today, targeted attacks on all industries are the norm. Business is increasingly more digitized and the supply chain is more interconnected. The COVID-19 pandemic transformed the workplace nearly overnight. With many enterprises permanently embracing hybrid work, the quickly implemented, patchwork security approach will not hold up when corporate and employee devices return to the office from unsecure environments.

Disrupting today's sophisticated, targeted threats requires a threat-centric approach that encompasses three foundational components: technology, people and processes across the entire security lifecycle. But the reality is that many enterprises don't have strong capabilities in all three of these areas.

This ebook examines how you can meet your new security objectives by implementing Managed Detection and Response (MDR). Going beyond reactive security, MDR accelerates your response and provides a more efficient, robust protection against targeted threats.



A hand with a red overlay is pointing to a globe. The globe shows a map of the world with various countries labeled, including Europe, Africa, and Asia. The text is overlaid on the right side of the image.

**Does your security
strategy align with
this changed world?**

MDR Adoption Drivers: Closing Security Gaps

In a 2020 survey of IT and cybersecurity professionals, we found that 63% believed their organization will become compromised by a successful cybersecurity attack in the next 12 months. While the shortage of in-house cybersecurity skills was the biggest challenge, we found that many enterprises also struggled with:

- ▶ Cost and complexity of building in-house security operations
- ▶ Lack of true 24/7 security coverage
- ▶ Lags in time to detect, notify and respond to security incidents
- ▶ Weak expertise across technology types
- ▶ Poor visibility into overall security posture
- ▶ Inability to proactively identify emerging threats across the environment
- ▶ Speed and support for incident response
- ▶ Recognizing these gaps, proactive enterprises are adopting MDR solutions

Drivers behind MDR adoption include the need for:

- ✔ Faster detection, response and automation to disrupt and block attacks
- ✔ A threat-centric approach that spans technology, people and processes
- ✔ Threat detection and response that extends beyond in-house capabilities to accelerate or enhance security
- ✔ Protection against adversaries at a granular, device level
- ✔ Practiced, knowledgeable teams who have the capability to not only continuously monitor but also respond to security incidents 24/7/365

Negative Impacts from Security Incidents Experienced by Companies in the Past 12 Months

(Source: "Managed Security Services Trends 2020," Herjavec Group)



37%

Disrupted business activities



32%

Reduced employee productivity



32%

Deployment of IT resources for triage and remediation

The Growing Risk and Cost of Cybercrime

Even before the COVID-19 pandemic, risk professionals ranked cyber incidents as the biggest business risk globally. This risk moved to the top spot in 2020, up from No. 15 just seven years earlier.¹



The risk comes at a high cost. The estimated global cost from cybercrime — including the investment in security technologies and the losses from cybersecurity incidents — climbed to nearly \$1 trillion in 2020.²

The Evolution of the Security Market

As the dynamic threat landscape has evolved, so too has the threat detection and response security market — starting out with endpoint detection and response (EDR), moving toward MDR and, more recently, expanding to a new iteration, extended detection and response (XDR).

This evolution reflects the changing needs of the modern enterprise. The crossover of some capabilities, however, causes confusion. Which solution should your enterprise adopt? The answer depends on your program's maturity, tools — and your objectives.

“

By 2025, 50% of organizations will use MDR services, up from less than 5% in 2019, according to Gartner.

EDR is a good first line of defense, yet MDR and XDR can provide faster, more effective response. However, XDR is a vendor-specific tool, designed primarily to unify one vendor's multiple solutions into one system.

For enterprises that want to move beyond monitoring to disrupt and contain threats across complex, multi-vendor environments, MDR is a recommended solution.



MARKET EVOLUTION*

ENDPOINT DETECTION AND RESPONSE:

Solutions for near-real time detection, investigation and remediation of endpoint security events, based on rules and security analytics.

MANAGED DETECTION AND RESPONSE:

Managed solutions that combine technology across host and network layers with advanced analytics, threat intelligence and human experts for 24/7 threat monitoring, detection and response.

EXTENDED DETECTION AND RESPONSE:

Solutions that extend visibility beyond the endpoint and network, collecting and correlating sources of data from multiple control points for a more holistic and robust response.

*Based on definitions by Gartner, 2021

The Benefits of MDR

MDR offers the following top benefits:

- ✔ **Improved visibility**
- ✔ **High-fidelity alerting**
- ✔ **Faster time to detection and time to response**
- ✔ **Active, hands-on expertise**
- ✔ **More robust, holistic security**

Improved Visibility

The perimeter is no longer well-defined, with threats coming in through any number of entry points — and, once inside, escalating privileges and interacting with other endpoints or systems. To block and disrupt threats effectively, you need enhanced, real-time visibility into security events not only for your endpoints but across the entire IT infrastructure — including devices, network, users and cloud platforms. This is where the strength of MDR lies.

MDR improves visibility by monitoring data from all your log sources, collecting and analyzing events from your entire security ecosystem, 24/7. This deep visibility helps ensure that threats don't go undetected and provides you a unified view of your risks.

High-Fidelity Alerting

One of the biggest challenges for enterprises is the sheer number of alerts generated by their security tools, including the security information and event management (SIEM) system. Many of these alerts also create a high number of false positives. As a result, sifting through the logs and correlating events to identify the actual threats is time-consuming, leads to alert fatigue and slows response time.

By combining deep visibility with threat intelligence, behavior analysis and automation, MDR results in high-fidelity alerting. Eliminating the noise enables the security team to focus on unique or high-priority alerts and proactive activities such as hunting for threats that otherwise evade their security toolset.

Faster Time to Detection and Time to Response

For 42% of organizations, it takes at least two to seven days to detect a threat — and often it can take months³. MDR ensures that threats don't fly under the radar. By using security orchestration, automation and response (SOAR) technology to correlate events and orchestrate workflows, your MDR provider can reduce your mean time to detect (MTTD), to be notified (MTTN) and to respond (MTTR).



The Benefits of MDR

Active, Hands-On Expertise

Technology by itself doesn't disrupt threats. You need hands-on human experts who can prioritize and escalate investigations, identify indicators of compromise and hunt for threats. Yet recruiting and retaining talent is a well-known challenge in cybersecurity.

MDR solves this challenge, providing you with continuous support by highly trained analysts. Based on your needs, you can completely outsource your threat detection and response or turn MDR into an extension of your team. This means you can focus on your core capabilities without having to worry about recruiting, retaining and training cyber talent.

Top 3 Security Challenges for Enterprises:

(Source: "Managed Security Services Trends 2020," Herjavec Group)



51%

Cybersecurity skills shortage in-house



38%

Cost and complexity of building in-house



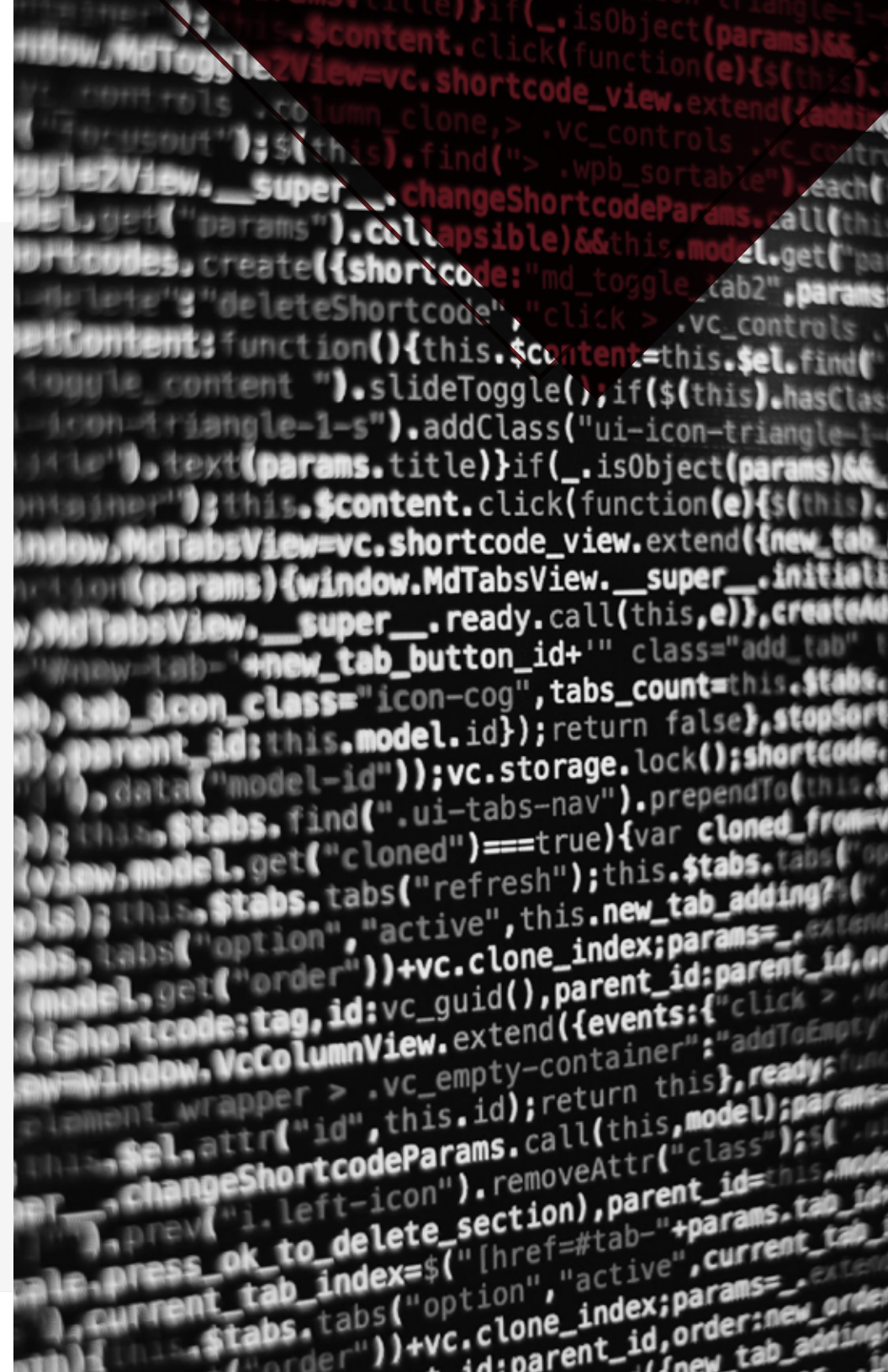
38%


Lack of 24x7 security coverage

More Robust, Holistic Security

MDR augments your in-house capabilities, integrating automated response from playbooks, threat intelligence and threat hunting to go beyond alerting and perform comprehensive investigations.

A key outcome of working with an MDR partner is a more holistic strategy that continues to provide robust security as the threat landscape evolves. By bringing together people, technology and processes into a unified platform, MDR takes a threat-centric approach that disrupts attacks.



A hand holding a Rubik's cube, symbolizing complexity and problem-solving. The image is dark with a reddish tint, and the text is white and bold.

**Look past the basic features
to understand how the MDR
solution meets your business
and security needs.**

Key MDR Capabilities

The MDR market is vast. While some services are standard among vendors, capabilities vary. When evaluating your options, look past the basic features to understand how the MDR solution meets your business and security needs.

Important capabilities and features to consider include:



24/7, active, expert support: Although 24/7 coverage is typical for MDR solutions, not all vendors offer around-the-clock hands-on support by human experts. Without real-time security event monitoring, triage, escalation, response and threat hunting, you're creating a wider window for threat actors to meet their objectives inside your environment. Look for an MDR partner with world-class talent who brings breadth and depth of expertise to the table. This should include a variety of skill sets, from analysts and engineers to threat hunters.



SOAR integration with automated workflows and playbooks: A SOAR platform improves your time to value with automated, predefined playbooks. For enterprises, benefits of integration include improved detection, notification and response times, standardized processes, enhanced content development across verticals and geographies, and better overall return-on-investment. Your MDR provider should be leveraging a SOAR platform in-house to enhance speed of investigation by deduplicating alerts, enriching context and automating blocks and changes, where possible. This ensures that cyber analysts are prioritizing proactive hunting, further security investigation and response.



Integrated threat intelligence: Threat intelligence is one of the areas of differentiation for MDR services. Threat intelligence that combines industry-leading commercial, government and open sources on a global scale should automatically feed into your environment, as well as underpin proactive threat-hunting activities.



Proactive threat hunting: Unlike reactive practices, threat hunting focuses on emerging threats rather than known attacks. This requires having a team who's not encumbered by alert investigation. For many enterprises, dedicating in-house staff to proactive threat hunting is not feasible, and a high-quality vendor who offers holistic services should provide those resources and expertise.



Ability for digital forensics and incident response: When you have a high-impact security incident, you don't want to waste valuable time assembling an incident response team and bringing them up to speed. Some MDR vendors offer incident response services, typically on a retainer model. Having fast access to a team of experts who can support digital forensic analysis, contain the threat and facilitate remediation helps you reduce dwell time — and, consequently, the cost and impact to your business.



Why You Need Proactive Threat Hunting

Traditionally, security operations have relied on a variety of tools to detect a suspicious event and send out an alert. You waited for the signs that a threat actor may be prowling in your environment — and then you jumped into action to remediate. While this remains a necessary part of security operations, it invariably puts you at least one step behind the cybercriminals.

Threat hunting turns that approach on its head. Instead of waiting for adversaries to break through your defenses and make themselves known by triggering an alarm, you're trying to catch them in the act and, ideally, much sooner than would otherwise be possible.

This proactive strategy is critical in today's cybercrime landscape, serving as an additional tool for disrupting threats and malicious actors effectively. It enables you to consistently look for IOCs and to better understand and strengthen your security posture.



Technology Stack: BYO or Vender-Provided?

MDR services offer different types of service delivery for the security technology stack. These models vary in their degree of flexibility.

Full stack provided by vendor: In the least flexible scenario, vendors require you to implement their own, proprietary technologies. While the vendor platform for managing and delivering the service may be state-of-the-art, not having any choice in the technologies puts you at a disadvantage. And since you can't leverage your existing investments, this model may also incur higher costs in the long run.

BYO stack: In a BYO model, the vendor uses your existing technologies to deliver security operations. This option provides you complete control over the tools in your ecosystem, but also requires you to update and upgrade your stack as your needs change. And in some cases, the MDR provider only supports specific security vendors.

Vendor-agnostic model: MDR providers who use a vendor-agnostic approach offer you the choice of bringing your own stack and supplementing it with additional solutions from best-of-breed providers. This model goes beyond a simple black-box solution, offering you flexibility as well as ensuring you have the best products to protect your entire infrastructure.

Top 3 Factors That Impact the Selection of Managed Detection Services

(Source: "Managed Security Services Trends 2020," Herjavec Group)



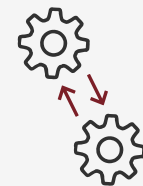
63%

24/7 coverage of security operations



54%

Solution cost



50%

Ability to integrate/leverage our security technology stack

Buying Considerations

Working with a full-service managed security services provider (MSSP) comes with advantages that traditional MDR vendors don't have. Additional benefits from working with an MSSP include:

- ✓ A holistic view of your security and environment
- ✓ Complete security lifecycle view, from gap analysis to remediation
- ✓ Comprehensive investigations and battle-tested incident response resources with state-of-the-art discovery and forensic tools
- ✓ A combination of threat intelligence and learnings from incident response, security assessments and testing engagements
- ✓ Automated, predefined playbooks and resolver group expertise that are enhanced by a global client base for cross-industry and cross-geographic learnings and correlations

5 Important Questions to Ask a Potential MDR Partner

- 1. What attack surface areas do you cover?** – The provider should monitor and respond to threats across your entire ecosystem and have the ability to support not only your endpoints and network but also cloud and segmented environments.
- 2. What are your detection capabilities?** – To protect you against known and unknown threats, your MDR provider needs far more than signature-based detection. High-fidelity threat intelligence and behavioral analytics are some of the advanced capabilities to examine.
- 3. How do you disrupt and block threats?** – MDR providers view “response” differently. Understand whether the MDR solution goes beyond alerting to provide comprehensive investigations and whether they include active threat hunting.
- 4. How do you escalate incidents?** – When you experience a high-impact incident, time is of essence. Ask your potential vendor how the security team handles these scenarios.
- 5. How do you measure your security effectiveness?** – To help you understand your risks and changes in your security posture over time, the vendor should provide a measurable service and actionable reports.



**Engage a partner who
can elevate your security
operations as well as
consistently innovates to
add more value to your
security investments.**



Herjavec Group's Managed Security Services Practice defends global, enterprise-level organizations from increasingly sophisticated, targeted cybercrime threats. Our industry-recognized HG SOC Operations take on the day-to-day defense of your infrastructure by monitoring your network, systems and data, 24/7/365. With HG MDR and our supporting HG Managed Security Services, we deliver an integrated, measurable, threat-centric, holistic service.

Robert Herjavec founded Herjavec Group in 2003 to provide cybersecurity products and services to enterprise organizations. HG has been recognized as one of the world's most innovative cybersecurity operations leaders, and excels in complex, multi-technology environments. In addition to Managed Security Services, Herjavec Group's service expertise includes Advisory Services, Technology Architecture & Implementation, Identity Services, Management, and Incident Response. Herjavec Group has offices and Security Operations Centers across the United States, United Kingdom, Canada and India. For more information, visit HerjavecGroup.com or contact a security specialist at: info@herjavecgroup.com.

Recognized Industry-Wide

LEADER IN MANAGED SECURITY SERVICES



SECURITY COMPANY OF THE YEAR



SECURITY SERVICES LEADER



BEST IAM SERVICE



#4 ON THE



TOP HEALTHCARE CYBERSECURITY PROVIDER



MANAGED SECURITY SERVICES

- ▶ SOC Operations
- ▶ Managed Detection & Response
- ▶ Security Technology Engineering
- ▶ Threat Management
- ▶ Managed Phishing
- ▶ Vulnerability Management
- ▶ Incident Response

PROFESSIONAL SERVICES

- ▶ Security Workshops
- ▶ Advisory Services
- ▶ Privacy & Compliance Services
- ▶ Identity & Access Management
- ▶ Technology Architecture & Implementation
- ▶ Security Assessments & Testing

Sources:

1 "Allianz Risk Barometer: Identifying the Major Business Risks for 2020", 2 "The Hidden Cost of Cybercrime," Center for Strategic and International Studies, 2020, 3"2019 Incident Response Survey," SANS