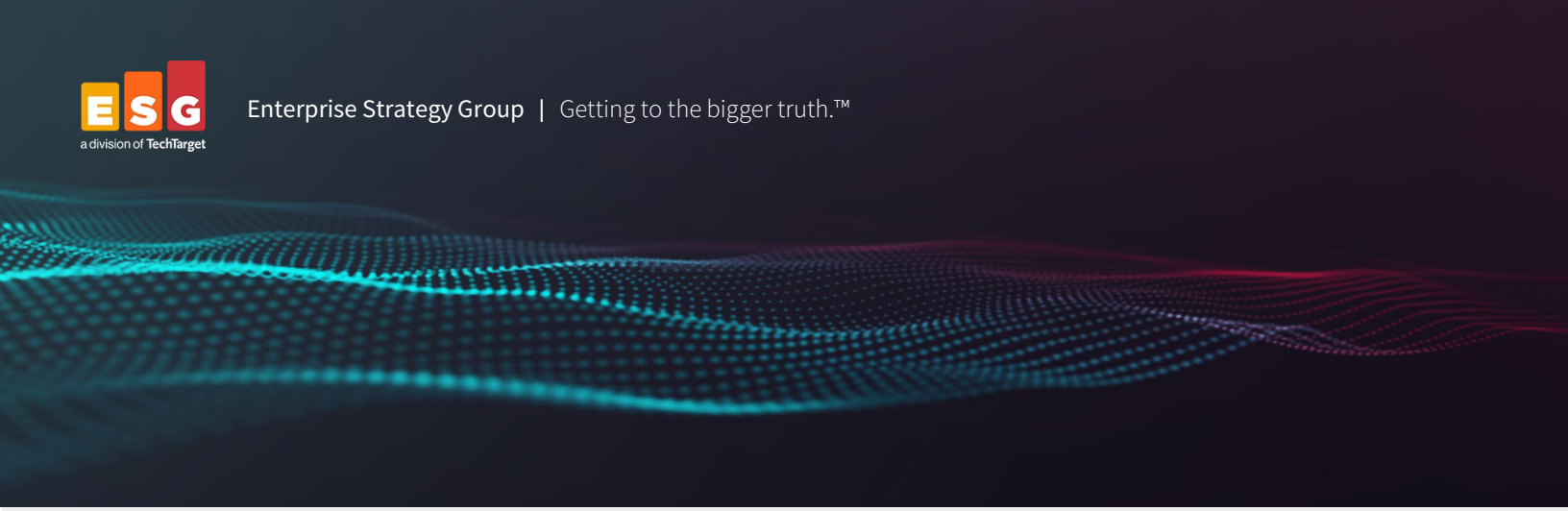


ESG WHITE PAPER

Managed Detection and Response: A Path to Rapid Security Program Growth

By Dave Gruber, Principal Analyst

August 2022

This ESG White Paper was commissioned by Dell Technologies and is distributed under license from TechTarget, Inc.

Contents

Abstract

Accelerating digital transformation, the rapid adoption of cloud, a more complex threat landscape, and a continuing shortage of security skills are pushing security teams to their limits. Current security solutions are unable to keep up, forcing many to prioritize SOC modernization initiatives to revamp technologies and processes. Industry megatrends around zero trust and extended detection and response (XDR) offer a new vision; however, many are struggling to implement and operationalize effective implementations of these strategies. Managed detection and response (MDR) services are providing relief, offering many organizations the people, process, and technology needed to shore up their security programs in this turbulent environment.

Introduction

As the escalating risk of damaging cyber-attacks steal mindshare and budget from core business objectives, organizations must respond by strengthening cybersecurity programs. For some, building out their entire security program with internal resources is plausible, but for most, third-party resources are needed to enable rapid program growth and scale.

Central to all cybersecurity programs is security operations (SecOps), responsible for monitoring and protecting all facets of the digital attack surface. Encompassing network, endpoint, cloud, identity, applications, and data, escalating amounts of security telemetry and alerts involved in SecOps are pushing organizations to their limits, causing many to turn to MDR service providers for relief.

MDR service providers have become a critical mechanism for these organizations, providing an array of security service offerings, such as incident response, around-the-clock monitoring, program management, and risk management. Enterprise Strategy Group (ESG) research indicates that MDR services have become a mainstream component of modern cybersecurity strategies for organizations of all sizes and security maturity.

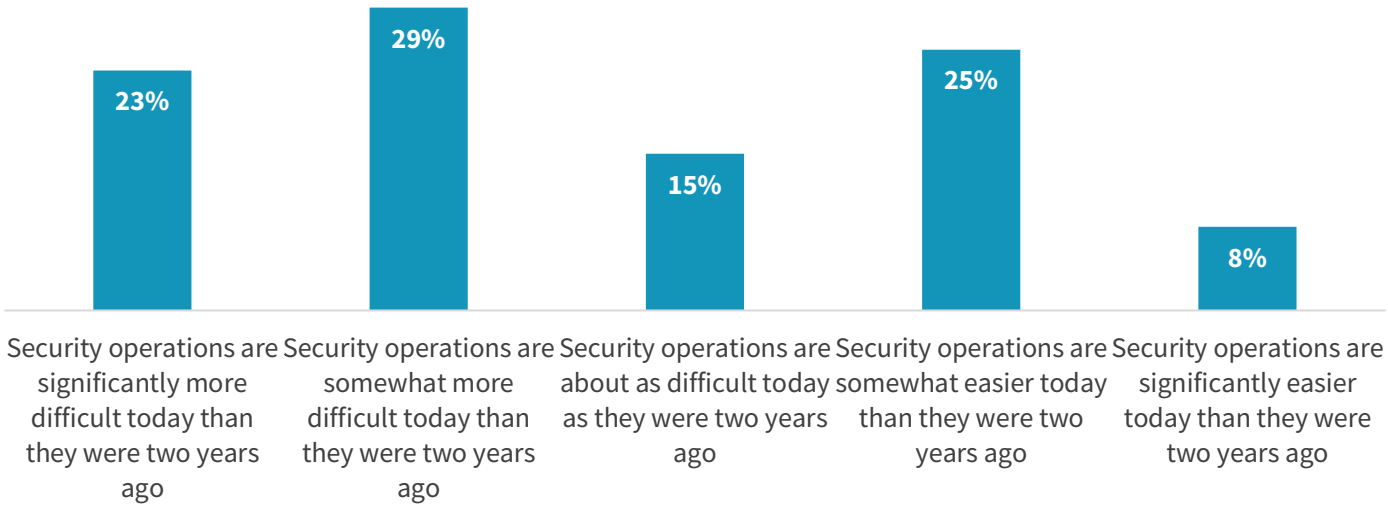
Growing Security Operations Challenges

According to ESG research (see Figure 1), most organizations acknowledge that the entire SecOps scenario is more difficult now than two years ago.[1]

[1] Source: ESG Complete Survey Results, *SOC Modernization and the Role of XDR*, August 2022. All ESG references and charts in this white paper have been taken from this survey results set unless otherwise noted.

Figure 1. More Than Half Think SecOps Is More Difficult

Which of the following responses best reflects your opinion about security operations at your organization? (Percent of respondents, N=376)

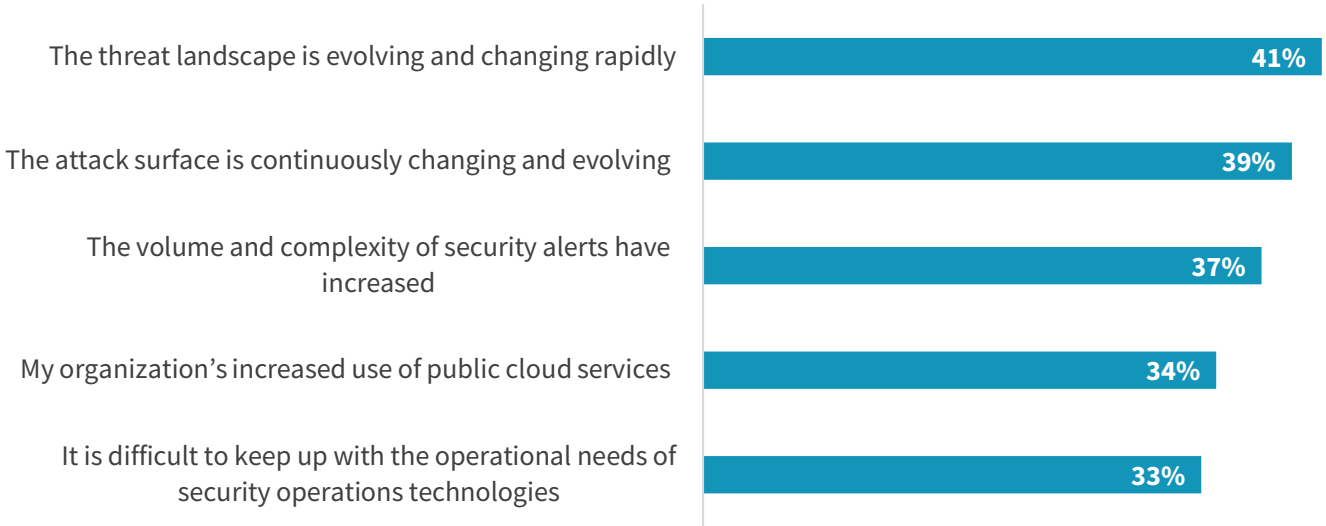


Source: ESG, a division of TechTarget, Inc.

As shown in Figure 2, ESG research also points out other challenges that are making detection and response more difficult than ever, such as the expanding attack surface, the growth and diversity of the threat landscape, and the ballooning use of cloud services for a wider range of applications and use cases.

Figure 2. Top Five Reasons SecOps Is More Difficult

You indicated that security operations are more difficult at your organization than they were two years ago. What are the primary reasons you believe this to be true? (Percent of respondents, N=194, multiple responses accepted)



Source: ESG, a division of TechTarget, Inc.

Modernizing Detection and Response Programs

Attack surfaces and the threat landscape have grown in both size and complexity, and so has the utilization of more security controls, generating thousands of alerts and massive amounts of security data. In support of alert and incident triage and investigation, security teams must aggregate, correlate, and analyze this data, often requiring immense manual processing. But more is required beyond the capture and analysis of alerts and security data.

Security teams are rethinking overall program operations to further incorporate asset and risk data from IT and line-of-business teams to focus on those threats that pose the most significant risk to organizational objectives. For example, stolen domain administration credentials can have a wide range of potential adverse impacts on the organization's operations, finances, and brand reputation in both the short and long terms.

As security leaders rethink strategies, more and more organizations are offloading daily operational activities to third parties as they refocus internal resources on more strategic security activities. As internal security resources focus on rearchitecting security operations processes, MDR service providers handle incident detection, triage, and response, taking swift steps to prevent damage and limit potential operational business disruption.

Others are looking to MDR providers for guidance in overall program development, pulling in experts and proven security operations processes to optimize results.

And as the XDR movement further creates a vision and roadmap for what is needed to modernize detection and response programs, others are looking to leverage MDR providers to assist in the implementation of XDR-grade solutions.

MDR Use Cases

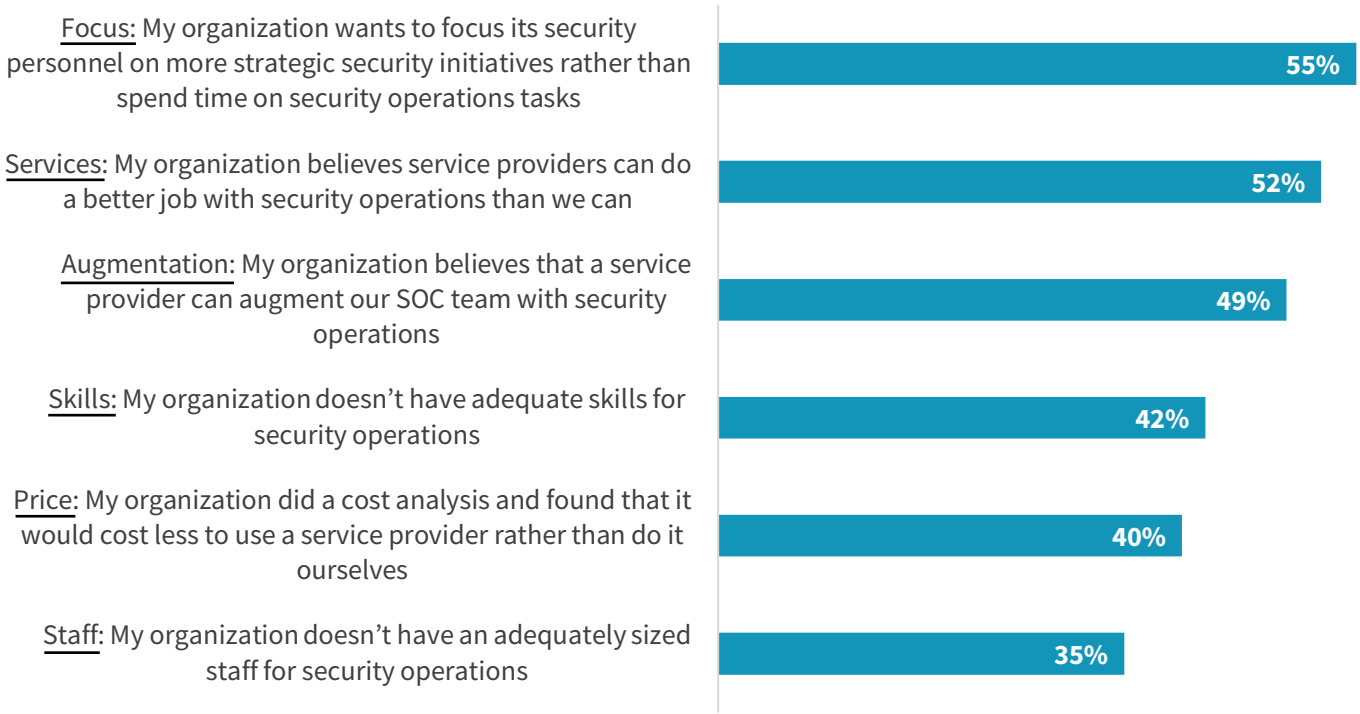
While many MDR providers offer a broad range of security services, core detection and response services that monitor, triage, and investigate alerts are often where early engagements begin. Operational models vary among MDR providers, so security leaders must carefully align their individual organizational requirements with an MDR provider that can deliver on their specific objectives. For example, some security leaders choose to fully outsource their security operations, engaging with an MDR provider to offer complete attack surface coverage, threat monitoring, and remediation. In this model, MDR providers often deliver the technology stack, processes, and security experts needed to render the service. For others, MDR services are an extension of an in-house security operations function, adding off-hours coverage or additional security experts to an in-house team primarily responsible for the technology stack and operations process. These are only two examples of the many use cases where MDR services are utilized.

MDR is, therefore, not a "one-size-fits-all" solution. Instead, it often represents a customizable set of capabilities that can be applied to an individual organization's needs.

Different organizations will choose an MDR partner for different aspects of detection and response, depending on their in-house resources and skills. ESG research explores the primary reasons why in Figure 3.

Figure 3. Why Organizations Are Choosing MDR Partners

What are the primary reasons behind your organization's usage of or plans for managed services? (Percent of respondents, N=368, multiple responses accepted)



Source: ESG, a division of TechTarget, Inc.

Key Value Drivers for MDR Engagement

Security program development requires a focus on both efficiency and efficacy, and MDR services can have a positive impact on each.

- Operational improvement and efficiency. MDR can help organizations reduce the total cost of security operations in several ways, such as infrastructure, personnel, and management. It can also address the "alert fatigue" issue, as well as improve the likelihood that false positives will be reduced significantly.
- Improved cybersecurity efficacy and reduced risk. MDR can help organizations stop threats already in progress, improve detection of potential threats and advanced persistent attacks, activate proactive threat hunting, and institutionalize stronger controls to identify and prevent future attacks.

What to Look for in a Modern MDR Solution Provider

Keep in mind that MDR solutions, in general, are not new. In fact, they have been around for a while and have established a nice track record for success. But many "Generation 1.0" MDR solutions were designed and implemented for a different era: less data, fewer threats, simpler detection. The next generation of MDR solutions—and the third parties deploying and managing them—must take into account a broader, deeper, and more complex set of challenges that make detection and response more important and more difficult than ever.

When evaluating MDR solutions, organizations should look for such capabilities as:

- 24/7 monitoring of events and logs, yielding fast and high-visibility information on suspicious activity and alerts by volume, location, and type.
- Continuous and scalable network monitoring and threat analysis.
- AI-driven recommendations for contextual response options.
- Regulatory compliance reporting.
- "Human" security advisors in direct contact with in-house teams.
- Detailed, real-time analysis based on threat detection, triage, investigation, and forensics.
- Vulnerability assessments, prioritization, and mitigation guidance.

When considering the large number of potential service providers that can deliver some, most, or even all outsourced MDR capabilities, organizations should look for partners that can deliver:

- Contextual threat intelligence.
- Rich telemetry.
- Proven track record in the organization's geographic coverage area, vertical market, and regulatory profile.
- Demonstrated threat-hunting capabilities.
- A long-term commitment to cloud-based MDR, with extensive capabilities in multi-cloud and hybrid cloud environments, zero trust, and the shared responsibility model of cloud security.
- A proven ability to scale their service over time, based on innovative technology, proven processes, and demonstrated expertise by its people.

The Dell Technologies Approach To MDR

The Dell Technologies approach to managed detection and response combines flexible, intelligent, and scalable technology with experienced cybersecurity professionals. Its subscription-based service is designed to give organizations both cost predictability and a seamless shift to a higher level of service, if and when necessary.

The technology platform for Dell Managed Detection and Response is Taegis XDR, a fully managed, cloud-native service developed by Secureworks, a Dell Technologies company. Taegis XDR detects, analyzes, and acts on fully vetted threats across a distributed and diversified attack surface to help protect organizations ranging from huge global enterprises to relatively small businesses.

The power of Taegis XDR is maximized through the expertise and skill of Dell's large group of security analysts and engineers, whose collective knowledge spans decades of expertise in helping to protect organizations against both known and heretofore unknown threats. This combination delivers an efficient way to unify detection and response across the

entire IT architecture, in large part by its continuously updated threat intelligence database. Dell Managed Detection and Response also monitors, analyzes, and identifies adversarial behavior to shorten mean time to detection and response.

Configured and deployed as a subscription-based managed service, Dell Managed Detection and Response dramatically reduces organizations' need to seek out and recruit security professionals to handle more threats, more attacks, and more alerts. Dell Managed Detection and Response complements and extends an organization's internal capabilities both efficiently and effectively. As a result, in-house SecOps personnel can focus more time and energy on other security-related tasks.

Success Stories: How MDR Works in the Real World

ESG spoke with IT and security leaders from Dell MDR customers to gain insights into specific use cases, operational models, and outcomes.

Example #1: Midsized Municipal Government

Municipal governments' IT and cybersecurity resources rarely match up to those of their private sector counterparts, but that doesn't mean that they don't face the same kinds of problems. In this example, a midsized county in a southwestern U.S. state was struggling to confront and overcome a growing number of security threats, but also to keep spending within tight constraints.

When a new IT director was hired, he immediately recognized the growing threat landscape facing his small team and spotted potential vulnerabilities in their detection-and-response capabilities. "Our security posture was just not up to snuff, but we had to be able to expand our capabilities without expanding payroll—a subject that is highly sensitive to executive decision-makers," he said. "But I know I could appeal to their concerns to be fiscally frugal while also pointing out the need to address our vulnerabilities."

He first set out to evaluate the county's incumbent endpoint security vendor that was then touting a 90-day "free trial" of software upgrades to address improved detection and response. But, finding that software lacking in functionality for their needs and the vendor's communications not up to expectations, he decided on a more comprehensive MDR solution.

"Fortunately, we had in place an arrangement for Dell to provide a virtual CSO (chief security officer), so the county leaders were aware of the benefits of using a managed services approach, in this case for detection and response." He added that the Dell team acted as a complement to—rather than a replacement for—the small in-house team of security and IT professionals the county had in place. "They were an extension of our team, and they worked alongside our folks very seamlessly."

The real benefit of the arrangement soon became clear when a global hacking campaign targeted Microsoft Exchange web mail, a popular platform used by a wide range of organizations—including the county. "Microsoft developed and sent a patch as soon as they discovered the attack, but zero day on the attack was probably a month earlier," the county's IT director said. "We were contacted by our Dell virtual CSO after hours, and the Dell MDR team parachuted in. They sent us scripts to check the server, and we quickly discovered that one of the servers was compromised."

"Dell (and their Secureworks partners) really knew what they were doing. We had two, three calls a day, every day, throughout the duration of the time we were dealing with the breach attempt." He added that the incident response team went through their findings with the county's personnel, showing them code snippets and other indications of the breach attempt and the evidence of the compromise.

Finally, they provided a number of technical and non-technical recommendations that not only addressed the potential impact of the breach attempt, but also bolstered the county's cybersecurity profile over a broader perspective and timeframe.

"Our experience showed us that the way to go when looking for enhanced detection and response is to find a reliable, proven, and trustworthy MDR specialist that has been through this before, rather than trying to find a cheap way to upgrade EDR software," he said. "Not just during the aftermath of the breach attempt, but in working with them on a regular basis, I just remember the warm, fuzzy feeling knowing we have a good team working to help keep us safe."

Example #2: Midsized School District

School districts have historically under-invested in IT in general, and in cybersecurity specifically. But with ransomware and other cyber-attacks against school districts on the rise, local public education officials have been scrambling to come up with better, more reliable, and affordable ways to protect against vulnerabilities.

For instance, one midsized U.S. school district found itself under attack from ransomware, and its entire technology-driven operations were shut down. With 8,500 students and staff spread out over 21 facilities, the district had in place a reasonably sized IT profile with 100 physical servers and another 63 virtual servers, connected to more than 11,000 devices for students and staff. Clearly, this district had many potential entry points for bad actors and needed a partner that could act fast.

After determining the ransomware attack was real and had to be addressed immediately, the school district's IT team contacted Dell Managed Detection and Response. "By day two of the attack, we had 10 people here from Dell," recalled the district's IT director. "We have had a highly trusted relationship with the team at Dell, and they took charge right away."

Fortunately, the net result was a positive one for the district. "Of the more than 6 million files in our systems, we only lost six," the IT director noted. "And we never even paid the threat actor. We are a real-world example of surviving ransomware and continuing to do our work safely and securely.

"Working with Dell has been a positive experience. Our onsite security analyst is always happy after they speak with Dell's people, and we have a 95% better stance today than we did before working with Dell on managed detection and response."

The Bigger Truth

As the escalating risk of damaging cyber-attacks steal mindshare and budget from core business objectives, organizations must strengthen cybersecurity programs. While use cases vary, most are leveraging MDR service providers to grow and scale their programs.

MDR service providers offer a path to overcome many of the recognized challenges in building a successful security program, including security experts, proven processes, and scalable, easy-to-deploy security technologies.

Dell Technologies has assembled a tightly integrated set of technology, experienced security experts, and best practices to help organizations detect and respond to threats in near real time. As seen by the case studies in this white paper, Dell Technologies has helped a wide range of organizations across different industries and resource profiles to thwart the impact of emerging threats throughout the enterprise.

Enterprise Strategy Group is an integrated technology analysis, research, and strategy firm that provides market intelligence, actionable insight, and go-to-market content services to the global IT community.

www.esg-global.com contact@esg-global.com 508.482.0188