Enterprise Strategy Group | Getting to the bigger truth.™

ESG SHOWCASE

Why MDR Has Become Integral to Modern Cybersecurity Strategies

Date: August 2022 **Author:** Dave Gruber, ESG Principal Analyst

ABSTRACT: No one debates the importance of detection and response capabilities in a cybersecurity program. The big issue is how best to ensure timely, accurate, reliable, and consistent detection and response when threats are multiplying in number and morphing in complexity faster than most organizations can adapt. Managed detection and response (MDR) as a third-party managed service is an approach that allows organizations to keep pace.

Introduction: The Rise of MDR

All organizations are faced with a stark reality: Cybersecurity threats are rapidly increasing, attack surfaces are expanding, and traditional processes and tools for detecting and responding to threats no longer are sufficient. Both the threats themselves and the bad actors who perpetrate them are more adept, agile, and persistent, creating a digital moving target for security and IT professionals tasked with protecting corporate assets.

A plethora of security controls add cost and complexity to detection and response efforts by requiring security teams to manually triage a constant flood of alerts to tease out valid threats from false positives. Building a bigger security operations center (SOC) and populating it with more tools and more security engineers is expensive—and that's assuming organizations can identify and hire enough security professionals in the face of the huge and growing cybersecurity skills gap.

As cybersecurity programs are rearchitected, organizations are turning more frequently to managed detection and response providers for help.

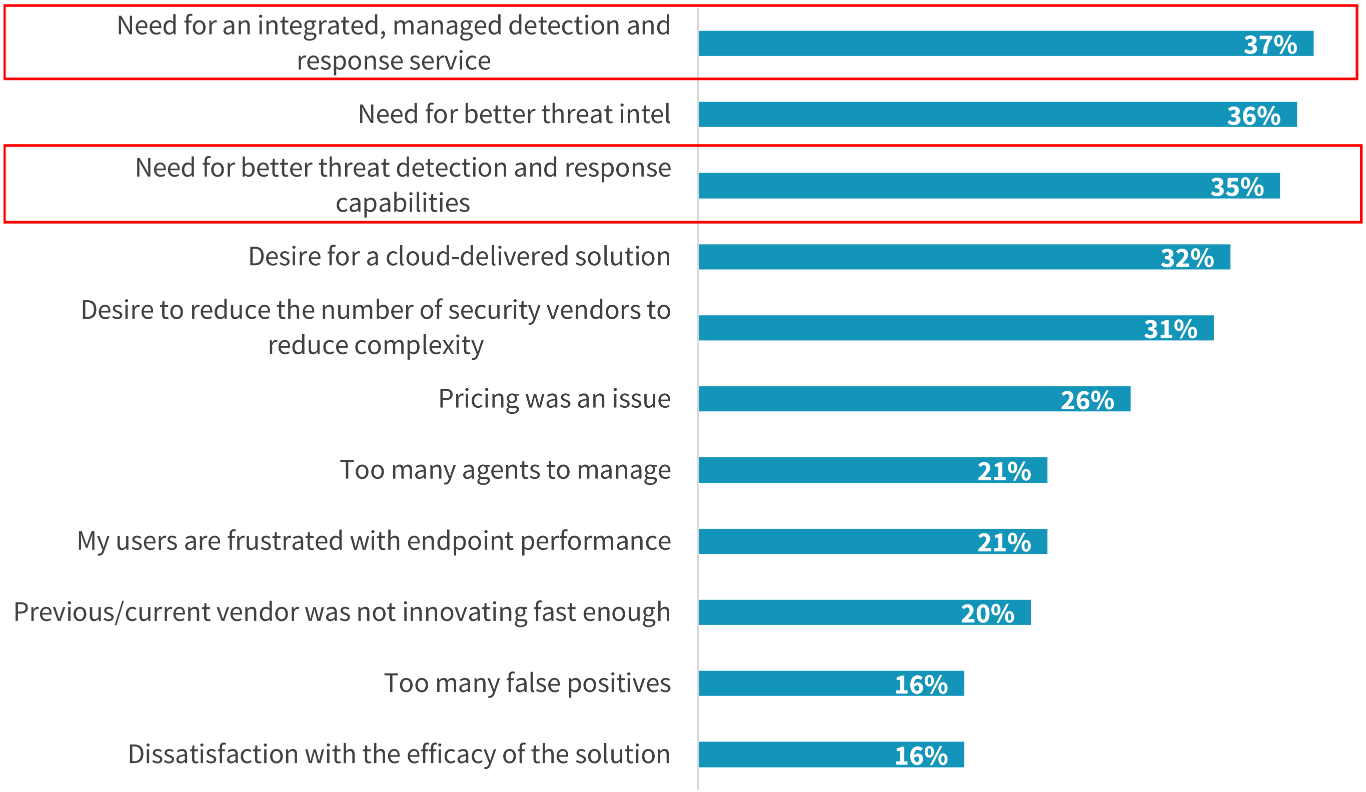
As cybersecurity programs are rearchitected, organizations are turning more frequently to managed detection and response providers to refine processes, fill resource and skills gaps, and modernize security operations tools. Many associate MDR with endpoint security, as ESG research reveals that the need for an integrated MDR service is a prominent factor driving organizations to change their endpoint security solution vendors (see Figure 1).[1]

[1] Source: ESG Complete Survey Results, *Endpoint Security Trends*, December 2021. All ESG research references and charts in this showcase have been taken from this survey results set.

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

Figure 1. Drivers for Changing Endpoint Security Vendors

If your organization recently switched, has an active project to switch, or is planning to switch endpoint security solution vendors, what drove/is driving this change? (Percent of respondents, N=300, multiple responses accepted)



Source: ESG, a division of TechTarget, Inc.

However, as security teams expand detection and response programs, upgrading to more comprehensive extended detection and response (XDR) solutions, MDR offerings are providing organizations a path to update both technology and operating models capable of providing more comprehensive attack surface coverage and advanced threat detection. New approaches are needed, combining around-the-clock monitoring, real-time global threat intelligence, automation, and advanced machine learning analytics—all capable of working with massive amounts of security telemetry in support of rapid detection and threat hunting. While XDR continues to evolve and mature, MDR services can enable organizations of all sizes and levels of security maturity to operationalize detection and response, leading to the mitigation of advanced threats. This is especially important as organizations redefine the scope and scale of cybersecurity boundaries from the data center to the edge to the cloud. MDR brings together the people, processes, and technologies needed to extend threat detection and response use cases across the distributed enterprise.

Key Drivers for MDR Adoption

The use of MDR services is on the rise, offering security teams a path to extend coverage, close gaps in staffing, and strengthen overall program objectives. Use cases vary, but underlying drivers include:

- Threat Landscape: The number of cyber-attacks, and the increasing sophistication of those attacks, has put a tremendous strain on organizations to detect and respond faster and more definitively.

- Adversarial Intent: Adversaries have become smarter, more persistent, and even more strategic in how they plan and carry out their attacks. A powerful "criminal ecosystem" has emerged where bad actors share tactics and even collaborate on attacks.

- Economics: The CapEx commitment to building and expanding a SOC is substantial—typically a seven-figure expenditure, and sometimes even more.

- Cybersecurity Technology Refresh: The cybersecurity stack of controls must be refreshed more frequently for organizations doing all or the bulk of their security operations activities in-house. These include moving from first-generation endpoint detection and response to a more comprehensive XDR/MDR framework.

- Skills Shortage: The much-discussed cybersecurity skills gap is a perennial issue. The inability to properly staff in-house cybersecurity positions often results in challenges in detection and response objectives, putting assets at risk.

Cyber-attacks are indiscriminate. Small and mid-size organizations, with their limited staff, budget, and prior exposure to all types of attacks are at risk. Even very large organizations need supplemental staffing, scalable controls, and executive-level consulting on strategies to detect and respond to the evolving threat landscape.

What to Look for in an MDR Service and an MDR Service Provider

There are some important and intractable requirements for any organization evaluating an MDR service, including:

- Contextual Threat Intelligence: Enable real-time threat intelligence and detection, including correlation of multiple indicators to identify threats or dismiss false positives.

- Proactive Use Cases: Support active hunting of known threats.

- Rich Telemetry: Undertake deep forensic investigations and sophisticated analytics, which are particularly important to identify new, emerging threats.

- Remediation: Offer context-specific, AI-driven remediation guidance.

- Risk Mitigation: Vulnerability assessment and management.

When it comes to selecting an MDR service provider, organizations should look for partners that can deliver specific, demonstrated capabilities, including:

- 24/7 coverage: Provide around-the-clock continuous monitoring on a 24/7 basis.

- What-if scenario planning and consultation.

- Human expertise and experience by the service provider.

- Guidance to C-suite executives and board members.

- Ability to ensure governance, compliance, and business continuity.

Additionally, organizations should ask potential MDR partners about service-level objectives. These functions include mean time to react from alert to initiation of investigation, mean time to respond from investigation initiation to the time when an incident analysis is provided to the organization, and mean time to resolve from the investigation initiation to the time when full resolution has taken place.

The Dell Technologies Approach to MDR

Identifying, evaluating, and partnering with an MDR service provider requires organizations to focus not only on their current needs in detecting and responding to threats, but also on how those needs are likely to evolve and expand in the future. While no organization has a crystal ball when it comes to predicting the future of cybersecurity threats, organizations should look for an MDR partner with 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 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 business unit. 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.

Taegis XDR is further strengthened by the skills of Dell's large group of security analysts and engineers whose collective knowledge spans decades of expertise, 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 through 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.

> **Dell Managed Detection and Response also monitors, analyzes, and identifies adversarial behavior to shorten mean time to detection and response.**

Finally, since this is a managed service, Dell Managed Detection and Response dramatically reduces organizations' need to seek out and recruit security professionals for already-overtaxed, in-house IT and security operations teams. Dell Managed Detection and Response is designed to complement and extend organizations' own capabilities in a cost-efficient, yet strategic manner.

The Bigger Truth

The rapidly expanding attack surface, repeated ransomware attacks, and a generally more complex threat landscape is driving investment and momentum in XDR and MDR as organizations modernize threat detection and response programs. While individual security strategies vary, the need for a broader view of the attack surface and the ability to aggregate, correlate, and analyze massive amounts of security data from the individual security controls that protect it are an important step in gaining control.

Managed detection and response services are both effective and readily available, as security teams leverage MDR providers to strengthen skills, processes, and security technologies. ESG research shows that organizations investing in XDR want companion MDR services to help implement and operate these solutions. This means engaging with solution providers that have a proven track record in delivering both security solutions and services. When applied over time, that can help IT and security teams develop and scale their security programs.

ESG recommends exploring MDR solutions from companies like Dell Technologies that come with the people, processes, and technologies to help organizations achieve these objectives.

All product names, logos, brands, and trademarks are the property of their respective owners. Information contained in this publication has been obtained by sources TechTarget, Inc. considers to be reliable but is not warranted by TechTarget, Inc. This publication may contain opinions of TechTarget, Inc., which are subject to change. This publication may include forecasts, projections, and other predictive statements that represent TechTarget, Inc.'s assumptions and expectations in light of currently available information. These forecasts are based on industry trends and involve variables and uncertainties. Consequently, TechTarget, Inc. makes no warranty as to the accuracy of specific forecasts, projections or predictive statements contained herein.

a division of TechTarget

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