Enterprise Strategy Group by TechTarget

SHOWCASE

FEBRUARY 2023

Scaling Security Operations Requires More Than Experts

Dave Gruber, Principal Analyst

Abstract: Research by TechTarget's Enterprise Strategy Group reports that organizations are trapped in the firefight and are finding little time to invest in modernizing security programs. Organizations need help to overcome this challenge. Eighty-five percent of organizations use managed services for a portion or a majority of their security operations today. And of those utilizing managed security services, 88% will increase the use of managed services for security operations moving forward.[1]Combining extended detection and response (XDR) with security experts, best practices, and proven program strategies, MXDR providers are helping security leaders strengthen and modernize security programs capable of scaling over time. And for some, MXDR providers are extracting more value from existing security investments, strengthening security programs and posture in the context of existing security tools investments.

Overview – The Problem

As organizations make massive changes in their IT strategies to support the acceleration of their digital transformation initiatives, many security teams are being pushed to their limits. Traditional cybersecurity program strategies are struggling to scale to meet this growth, leaving many security leaders unable to protect their organizations from the onslaught of modern threats.

More than half of organizations reported that security operations are more difficult today than two years ago. A rapidly growing attack surface, combined with a more complex threat landscape, more cloud usage, and a growing number of security tools are challenging security leaders from modernizing security operations. More concerning is that these influences are leaving many stuck in the firefight, with no time to improve their program.

SOC Modernization Is Needed

Security and IT leaders must transform strategies, rethinking and rearchitecting core operating models capable of supporting a more diverse, distributed, multi-cloud infrastructure together with a highly distributed workforce.

Meanwhile, security leaders are being asked to improve their organization's security posture in the face of a growing threat landscape and uncertain economic times. In the context of regulatory and risk-driven prioritization, scalability and operational efficiency are key priorities.

In response, security and IT leaders must transform their strategies, rethinking and rearchitecting often unmanaged core operating models that are capable of supporting a more diverse, distributed, multi-cloud infrastructure together with a highly distributed workforce utilizing multiple devices daily. Effectiveness, efficiency, and scale are core to this modernization agenda.

[1] Source: Enterprise Strategy Group Research Report, *SOC Modernization and the Role of XDR*, September 2022. All Enterprise Strategy Group references and charts in this showcase have been taken from this research report, unless otherwise noted.

As security leaders explore how they can transform their programs to keep up, many are seeking help from managed detection and response service providers to accelerate program development and modernize security operations.

The Right Approach

Modernizing security operations to be able to scale with current and future growth means rethinking every aspect of each IT function across people, process, and technology, including how they operate together. New strategies are needed that will:

- Enable rapid and broad collaboration between IT and security personnel and machines.
- Leverage automation to achieve speed across all security functions, from the largest to the smallest.
- Balance comprehensiveness and complexity, optimizing the use of the security tool stack and its operations.
- Transform siloed prevention, detection, and response functions into a virtuous security lifecycle, working collaboratively to strengthen security posture over time.
- Continuously strengthen prevention, systematically adjusting controls leveraging intelligence gained in the security operations process.
- Tailor systems and processes in support of security program architecture and specific risk characteristics associated with the many different parts of the operation.

Enabling a More Collaborative Operations Model

Security is truly a team sport. IT and security teams, line-of-business leaders, business outsourcers, cloud service providers, and managed service providers all must work effectively together to secure modern organizations. The use of collaboration tools has exploded in support of a more distributed workforce, yet integrated, automated collaboration support within IT and security tools is severely lagging.

Harnessing the power of modern collaboration mechanisms, such as Microsoft Teams, opens the door for a new level of familiar, proven collaboration mechanisms to be threaded into IT and security operations. These widely adopted collaboration mechanisms can further enable security and IT teams to interact with other business functions in an integrated fashion, as modern security and response activities involve many people outside of the technical staff. Technical teams, line-of-business leaders, end-users, and managed service providers must operate seamlessly to achieve the speed required for modern security programs.

A New Focus on Collaboration

Harnessing the power of modern collaboration mechanisms opens the door for a new level of familiar, proven collaboration mechanisms to be threaded into IT and security operations.

Rethinking Automation Strategies

Scalable security strategies require organizations to rethink their current automation strategies. The topic of automation has long been associated with the security conversation but typically has been aimed at automating wholesale functions, often defined in automated playbooks. These strategies assume well understood actions and workflows, but can limit automation opportunities to known workflows.

A new data-driven, more intelligent model is needed to support the limited security professionals available—a model in which every aspect of day-to-day security operations is continuously measured and analyzed to identify new processes and tasks to automate, resulting in increases in the speed, accuracy, and consistency of security

experts. This intelligent automation model can accelerate multiple security objectives, speeding investigations, increasing analyst throughput, and reducing dwell times. Applying automation wherever possible in the security operations process, from data ingest, correlation, analysis, and enrichment to assistive functions that help individual analysts perform core investigative and response tasks, optimizes where and how individuals spend their time.

Balancing Comprehensiveness and Complexity

Is comprehensiveness king? Or is it the enemy of operationalization? In a world of "more is better," consuming as much as is needed, but not everything possible, helps optimize infrastructure and reduce complexity.

As IT strategies drive investment in new or enhanced security tools, many organizations face unprecedented levels of complexity and integration challenges. As a result, two-thirds of security leaders reported that their organizations are actively consolidating the number of security operations tools in their IT environments.

In the quest for simplification, a new focus on what existing investments and capabilities are underutilized, overlapping, or simply misconfigured is helping IT and security leaders rationalize future strategies. Many are looking to security service partners for help, as they modernize programs and decide on fewer, more capable platforms that can grow with their needs.

While most see value in the quest to gather more insight through more security data, nearly one-third of organizations actually cited the increased amount of security data they collect and process as a reason security operations have become more difficult over the past two years. Careful consideration is needed to gather and analyze the signals required to optimize threat detection without crushing operations with unneeded data and operational complexity.

The Role of Systematic Prevention

While most organizations have heavily invested in individual, preventative security controls aligned to each major IT function, configuring and optimizing those controls to support the continuously growing and changing attack surface continues to pose challenges. As security teams face and learn about new tactics, techniques, and procedures used in attacks, strengthening preventative controls is required to keep up.

Proactive activities like continuous assessment and the optimization of preventative controls inform and can reduce detection and response activities, while intelligence gained through detection and response can inform and strengthen preventative controls. Operationalizing this virtuous process will strengthen security posture over time. While prevention continues to be a critical security strategy, it can no longer work independently, but instead must work collaboratively with other preventative controls and detection and response mechanisms.

Tailored Operations

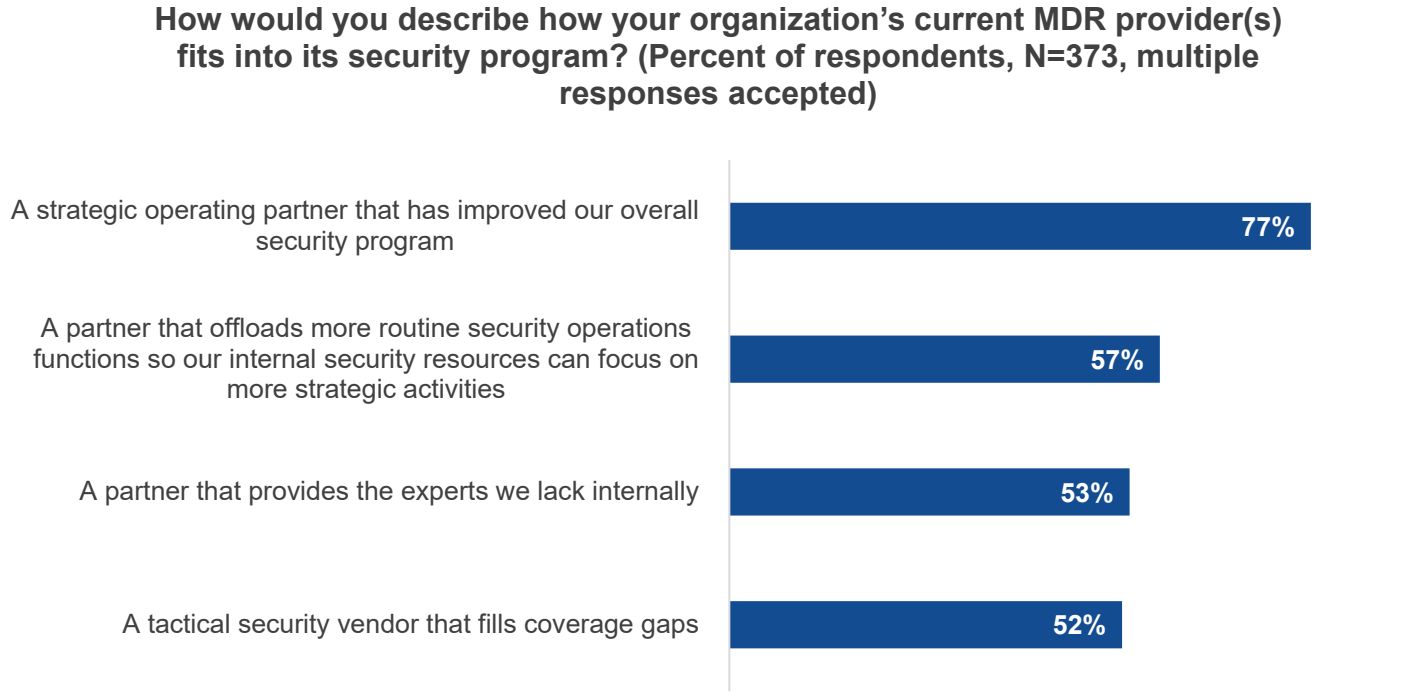
There is power in leveraging what is common across the industry, but every organization has its own infrastructure and operational design and constraints. The specific applications, systems, and infrastructure used to support each part of the business, together with the risk profile associated with each, must inform security strategy and operations. While attackers have a general understanding of IT and security practices, only defenders have a complete understanding of their individual environment.

While leveraging industry knowledge is key to strengthening and accelerating security programs, the ability to individualize strategies and tactics around each organization's IT and security architecture and implementation is critical to the success of the program. A one-size-fits-all model simply doesn't work in security. Scalable security strategies and operations must, therefore, leverage industry learnings yet be flexible and customizable in support of the unique architecture and risk profile of each function within the organization.

Managed Detection and Response: A Mainstream Security Strategy

According to Enterprise Strategy Group survey data, 85% of organizations report investing in some type of managed detection and response (MDR) services for a portion or majority of their security operations. And these investments are paying off, improving organizations' overall security program, enabling internal resources to focus on more strategic activities, and filling staffing and coverage gaps (see Figure 1).[2]

Figure 1. The Role of MDR Providers



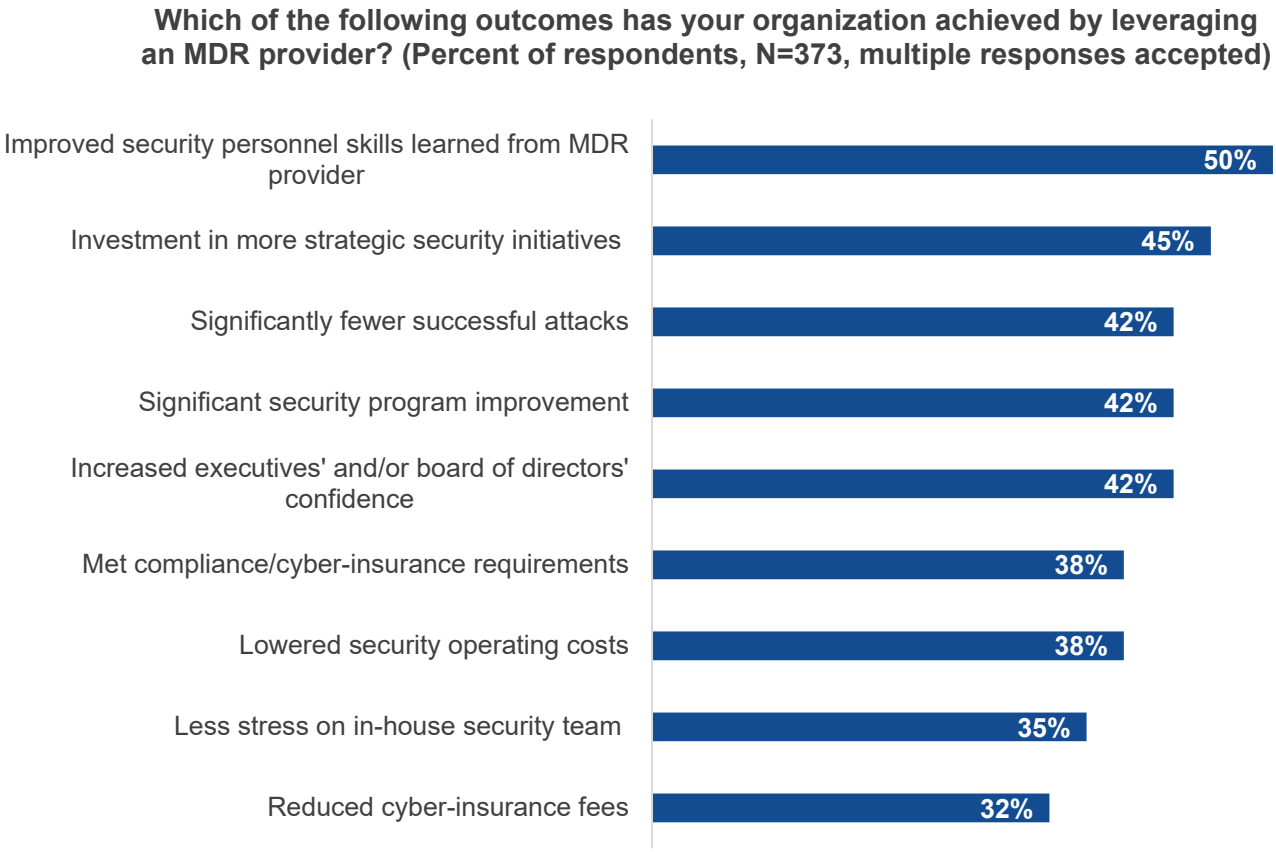
Source: Enterprise Strategy Group, a division of TechTarget, Inc.

As traditional managed security service providers (MSSPs) struggle to deliver Tier 2/Tier 3 analyst value in triage, investigation, and response, security leaders are turning to MDR/MXDR providers for help. While MSSPs largely depend on SIEMs and data ingested from whatever legacy tools are in place, MDR/MXDR providers typically center detection and response around the use of endpoint detection and response (EDR) and, increasingly, extended detection and response (XDR) solutions, enabling MDR/MXDR providers to deliver far greater value than their MSSP counterparts. This value extends beyond basic security operations, helping 42% of organizations increase the overall security maturity of their program.[3]

More than a simple service provider, 77% of organizations described their MDR provider as a strategic operating partner that has improved their overall security program, and half reported that MDR service providers are further helping improve their organization's security personnel skills as they work together.[4]

[2] Source: Enterprise Strategy Group Complete Survey Results, *What Security Teams Want from MDR Providers* Study, to be published..
[3] Source: ibid.
[4] Source: ibid.

Figure 2. MDR Outcomes



Source: Enterprise Strategy Group, a division of TechTarget, Inc.

Introducing Ontinue

Ontinue, the MDR division of Open Systems, is helping organizations leverage their existing Microsoft platform and security investments to implement scalable, highly efficient, and effective security programs through Ontinue ION. Ontinue's deep focus on the use of AI-driven automation and real-time collaboration through Microsoft Teams in support of all security activities, processes, and actions saves security analysts two days of effort per week on average, while accelerating overall security program growth. Ontinue's specialized knowledge of the Microsoft ecosystem—particularly the Microsoft Defender suite, Microsoft Sentinel, and Microsoft Teams—makes the Ontinue ION platform the MXDR platform of choice for Microsoft customers.

Alerts and incidents generated from across clouds and devices by the Microsoft Defender suite and other controls are aggregated in the customer's Microsoft Sentinel, allowing customers to maintain control of their data. Ontinue ION plugs into the customer's Sentinel and automatically resolves 70% of high severity incidents. Any incidents that require additional investigation are passed to the ION Cyber Defense Center—a globally distributed 24/7 security operations center—for resolution by Cyber Defenders, the equivalent of Tier 2/3 security engineers. Every Ontinue customer is also assigned a Cyber Advisor, who is responsible for learning the customer's unique environment, operational realities, and teams to tailor protection to the customer. Cyber Advisors are ultimately responsible for the proactive security activities that advance the customer's overall security program maturity.

Conclusion

Security teams are facing a turning point in their ability to scale to meet the critical needs of their organizations. Modernization is needed, requiring rethinking and rearchitecting core strategies, including how people, process, and technology work together. Effectiveness, efficiency, and scale are core to this modernization agenda.

As security leaders explore how they can transform their programs to keep up, many are seeking help from MXDR service providers to accelerate program development and modernize security operations. Providers innovating through advanced automation and collaboration are helping organizations implement highly efficient and effective security programs. Enterprise Strategy Group recommends security leaders looking to leverage an MXDR provider consider Ontinue ION from Open Systems to accelerate this transformation.

Visit www.ontinue.com to learn more.

About Enterprise Strategy Group
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. © TechTarget 2023.

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