WHITE PAPER
SPONSORED CONTENT
CSO

MDR or MSSP for Cybersecurity?

How to Choose What's Best for Your Organization

While MDR and MSSPs each fulfill various security needs, the definition of "managed" is inconsistent between the two. Take the time to examine specific use cases before determining which service is best.

ActZero

SECURITY LEADERS constantly seek ways to get out in front of cybercriminals. And that's tough given today's changing threat landscape, filled with increasingly sophisticated attacks. To solve this, businesses need an always-on security strategy that leverages the latest in threat intelligence, watches for threats around the clock, and responds quickly and intelligently to attacks.

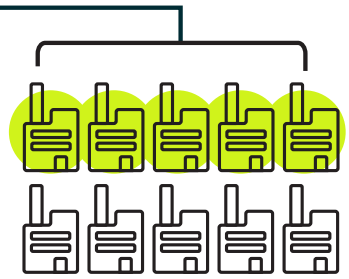
A variety of factors, such as the increasing adoption of cloud, combined with a more sophisticated threat landscape, make isolating meaningful threat signals through the noise more challenging than ever. Research from Microsoft finds cybercriminals have grown ever-more sophisticated, using techniques that make them harder to spot and that threaten even the most mature organizations.

Add to this scenario the growing volume of data and it can be near impossible to parry with meaningful responses. Amid these challenges is an ongoing talent shortage that makes cybersecurity an unfair fight all around. Research from analyst firm ESG finds no significant progress toward a solution to this problem: the skills crisis has impacted 57% of organizations, leading to an increased workload among 62% of respondents and a high burnout rate. The survey also revealed that 95% of respondents think the cybersecurity skills shortage has not improved over the past few years and 44% say it has only gotten worse.

Today's companies are spinning their wheels, spending too much time and money on ineffective, siloed solutions to identifying and remediating threats. For years, many organizations lacking the necessary internal security resources have relied on outsourced managed security services providers (MSSPs). But when it comes to modern managed offerings, managed detection and response (MDR) service providers are increasingly popular with small- and medium-sized businesses and mid-sized enterprises. This is because while MSSPs are effective at managing certain foundational security elements, they cannot deliver high-quality detection and response.

This white paper examines the key differences between MDR and MSSP services and offers guidance on which is best for addressing common global security scenarios and technologies.

50%
of organizations
will use MDR services for threat monitoring, detection, and response functions with containment and mitigation capabilities by 2025



EVALUATING MDR vs. MSSPs

MDR is a service that combines threat hunting, monitoring, and response using both machine and human expertise. MDR assists organizations with quick identification of threats and limits their impact. Much like MSSPs, MDR does not require additional internal staff for implementation.

Gartner estimates that by 2025, 50% of all organizations will use MDR services for threat monitoring, detection and response functions that offer containment and mitigation capabilities.[1]

Gartner defines MDR services as:

- A remotely delivered 24/7 security operation center (SOC) solution that can detect, investigate, and respond to threats.
- Staff that have skills and expertise in threat monitoring, detection, hunting, and incident response.
- Processes that include standardized workflows and procedures.

[1]Gartner, *Market Guide for Managed Detection and Response*, Pete Shoard, Craig Lawson, Mitchell Schneider, John Collins, Mark Wah, Andrew Davies, 25 October 2021

Gartner offers several key findings about MSS providers, including:

- MSS providers offer an array of security services that vary from one provider to another. This breadth of services provides ample options but increasingly overlaps with capabilities offered by other market segments.
- Differentiation and comparison between MSS providers can be difficult for buyers to quantify, as service capabilities and delivery models vary greatly from provider to provider.
- Software as a service (SaaS) security capabilities have taken precedence for many buyers, significantly reducing the need to utilize a third-party provider to maintain security technology.
- Non-security-specific vendors in the IT outsourcing and network service provider markets commonly offer implementation and management services for security technologies, reducing costs by co-contracting network, desktop, and security outsourcing.

MANAGED TOOLS vs. MANAGED THREAT ELIMINATION

When comparing MDR to MSSPs, it is important to note the difference in meaning of the word "managed" as it pertains to each. The "managed" in MSSP means these providers manage the tools you use and keep systems running up-to-date, patched, and compliant.

The word "managed" in MDR refers to a service that manages outcomes. MDR services "manage" threats and work to eliminate them. In other words, an MSSP does the work of ensuring that your tech investments are working, but an MDR provider does the work of safeguarding your technology from attack. It does so by deterring attacks, detecting them when they happen, and responding on your behalf.

Just how does this distinction come into play? It's helpful to understand what an MDR offers versus what an MSSP offers an organization. Let's look at some of the key features of each service.

MSSPs KEEP YOUR SYSTEMS UP-TO-DATE AND RUNNING

MSSPs focus on managing technology. MSSP solutions often include next-generation firewalls (replacing intrusion prevention systems and URL filters—including those in cloud-based firewalls), and a host of other prevention-focused tools that keep threats out of your environment. Contracts and service level agreements are generally task-based and typically include clauses around the maximum number of changes, response times to questions or alerts, the ability to add or remove devices, and hardware replacement/ ownership. MSSPs are the partner you turn to for setup and configuration of key services, and to ensure your technologies are up-to-date and continue running.

While MSSPs play a role in supporting businesses, they also have limitations, including:

- Lack of personalized support
- Lack of intricate understanding of a customer's individual needs and culture
- Limited monitoring capabilities
- Limited visibility of the threat landscape.

MDR FINDS, CONTAINS, AND ELIMINATES THREATS

An MDR is a managed outcome service that helps eliminate threats to your organization. IT and security leaders turn to MDR to detect, contain, and respond to attacks. MDR services proactively pair threat intelligence with threat hunting to monitor a client's environments for signs of attacks. When threats are detected, MDR services respond with an appropriate level of action to contain and mitigate the threat. It's also important to note that not all MDR services are created equal, so spend some time determining which one offers the best detection and response capabilities and will not bog your organization down with needless alerts.

Where they shine: Use cases for MDR and MSSP

NETWORK DEFENSE

Almost every organization with a security strategy is (and some without, are) using a firewall. Most security leaders purchase them with the understanding that they will prevent unauthorized access in or out of the company's network. A firewall is table stakes to security and one of the oldest technologies used for protection.

Organizations often turn to their MSSP to set up and configure their firewall and ensure it then continues to work, routing traffic appropriately—and MSSPs do this very well. Unfortunately, that is often the extent of the MSSP's services when it comes to firewall management.

MDR offers a different type of prevention management. Rather than configuration and overall maintenance, MDR uses advanced threat research, analytics, and forensics to make determinations on security threats coming into an organization's environment.

Rather than configuration and overall maintenance required of MSSPs, MDR uses advanced threat research, analytics, and forensics to make determinations on security threats.

This is also the case for managed antivirus (AV). Most organizations have deployed signature-based AV technology. MSSPs are often used to manage the time-consuming setup and configuration of this technology, and they help to keep it up to date.

MDR more often offers next-generation antivirus to protect against both unknown and known threats. By adding advanced threat intelligence, behavioral detection, and threat modeling, they eliminate reliance on signatures to detect malicious activity. This exposes threats faster and more accurately, and those threats can be blocked in near real-time by automation afforded by the MDR service.

MANAGED SIEM

Security information and event management (SIEM) is another foundational security technology utilized by most organizations. A SIEM system works with many other IT tools to compile data and event analysis, which is typically delivered to system and organization controls (SOC) analysts through a console.

SIEMs can be complex to configure and manage, which is why an MSSP is often necessary. In the case of a SIEM, MSSPs are very effective for addressing issues such as maintenance of the system, licensing concerns, and lifecycle management.

While SIEM works well for many non-complex search and alerting situations and environments, there can be challenges in more disparate IT environments. Typically, SIEM's primary source of logs are servers and security tools which already generate alerts. Raw data, like that generated in the cloud and complex breaches, are not setting off alarms like other sources do. This fractured approach jeopardizes the overall productivity of SIEM, especially for management and operations. Additionally, SIEMs require the configuration of use cases, or rules, during initial setup. The SIEM uses these criteria to flag logs and generate alerts that the MSSP will then address, typically by forwarding and escalating.

The core problem in security operations is a simple matter of mathematics. SIEM tools receive hundreds of thousands of alerts per day representing important events identified by a range of tools across the enterprise. Hidden in these alerts are telltale signs of active attacks in various stages. SIEM and MDR solutions alike must identify the attacks as quickly as possible and eradicate them before they become serious breaches. That's where MSSPs and managed SIEM fall short; without advanced filtering, MSSPs would need dozens of analysts working non-stop in order to keep up with average daily loads—an unscalable solution. By leaving SOC analysts with the responsibility of determining what to do with alerts, organizations risk missing attacks.

MDR is distinctly different because it helps manage outcomes and prevent incidents. MDR services proactively couple threat intelligence with threat hunting to detect, investigate, block, and respond to threats en masse, essentially replacing the intermediary function of the analysts. MDR technology aims to respond to alerts fast and accurately, reducing daily alerts.

Where they shine: Use cases for MDR and MSSP

MANAGED INFRASTRUCTURE

An organization's IT infrastructure, including endpoints, routers, switches, and cloud technology, all need day-to-day maintenance and management. This is where MSSPs reveal an advantage over MDR, because MDR providers simply do not provide this kind of service.

Organizations must maintain and update their tools while also adding and scaling, meaning a partnership with an MSSP is critical. MSSP services allow for customization of a customer's technology portfolio and environment. MSSPs also provide guidance and information on various threats and trends such as nation-state attacks, for example.

MSSPs also play a key role in patch management, ensuring that the technologies an organization has in place are regularly updated and do not contain security holes. While MDR providers don't typically offer patch management, their services do include prioritized recommendations about patches for users to remediate vulnerabilities themselves.

MANAGED IDENTITY AND ACCESS MANAGEMENT

Managing identity and access management (IAM) is another great example of how MSSPs play an important role in managing the cyber and IT tech stack. IAMs are logins, or in other words, the tools an organization uses to ensure authorized users can access the applications they need. They also ensure that unauthorized users cannot access these applications. IAMs utilize automation to enhance business productivity, ultimately helping to boost security, improve productivity, and reduce costs. MSSPs provide the valuable service of deploying IAM platforms and ensuring they are updated and working appropriately.

However, an MDR offers threat monitoring when it comes to IAM. For example, if IAM tools fall victim to a takeover attack by a cybercriminal, an MDR can contain the threat, and offer information about other anomalous behavior and strange login patterns that can flag malicious activity. More specifically, an MDR will monitor for suspicious account activity, vulnerabilities, and exploits against the tools protected by IAM and/or the IAM itself to detect threats and revoke access. This kind of threat detection and management is where MSSPs fall short in this scenario.

MANAGED EDR

Endpoint detection and response (EDR) is an agent or application that runs on each endpoint in an organization, curating log data from the endpoint and enabling response actions to be taken. But, as the name implies, it focuses only on the endpoint—which is only one small fraction of where compromises occur.

MSSPs often manage EDR for customers, but like other scenarios outlined here, that means keeping the technology updated and working. Even with EDR management by an MSSP, it still only sees a portion of compromises and misses anything beyond the endpoint. MSSPs take no action against threats they do discover, instead alerting the customer to a potential compromise.

MDR treats the EDR sensor as one of many sources of data. It combines this information with other sources, like cloud, network, or even extended detection and response (XDR), to provide a more holistic picture of threats. EDR on its own, managed by an MSSP is often not very effective. As part of a broader system, EDR enables the detection of and response to threats across multiple vectors.

MANAGED IaaS AND SaaS APPLICATIONS

Most organizations have systems and applications in the cloud. Cloud SaaS and infrastructure as a service (IaaS) are flexible for them, but also appealing to cybercriminals due to unprotected APIs and the ease of achieving unauthorized access. Threat actors can easily exploit over-privileged accounts and misconfigured controls to obtain access to corporate data and important company systems, making cloud-based solutions a blind spot in a business's security posture.

MSSPs often offer a turnkey secure data center for an app or for hosting, which gives customers an infrastructure and a light addition of security services to protect against traditional security threats like workload or virtual machine disruption and data theft. An MDR solution protects businesses by detecting and responding to threats across the environment, including SaaS and IaaS. MDR providers see data centers and clouds as extensions of an environment and deploy the same way, with the same intent: to find and block attackers.

Breaking it down: Choosing MDR or MSSP

There clearly are distinct differences between MSSPs and MDR, yet each managed service has its own benefits, and there are arguments to be made for using each. So how do you decide which one to choose? Consider the specific needs and technology of your organization, and when possible, leverage internal or 3rd-party resources to help.

Here are some additional factors to consider:

AN MSSP IS A GOOD CHOICE WHEN:

- Your IT team lacks the skills or time to effectively manage cyber security systems you own or plan to own internally. This includes changes and uptime monitoring for items such as network and log management tools that your team intends to use for reports/data processing, etc.
- You need to outsource basic security services, such as alert triage.
- You require on-demand skills to help manage existing security tools like firewalls and web content filtering and potentially infrastructure.

MDR IS A GOOD CHOICE WHEN:

- You don't know which technologies to add and manage, and you want a comprehensive service to block attacks on your endpoints, mobile devices, network, and cloud services.
- Your company has considerable cybersecurity regulatory or customer requirements that are difficult to achieve with the people, processes, and technology currently in place.
- You do not know what vulnerabilities or risks to focus on in protecting your systems from cyberattack.
- You are concerned about your ability to effectively respond 24/7 to threats.
- You are concerned that you're not protected against advanced or emerging threats, or the latest headline attacks from dedicated adversaries.
- You receive no alerts at all, too many alerts, or too many false positives from tools or providers; or you are overwhelmed with alerts, many of which turn out to be false positives.

THE BOTTOM LINE

Your choice of MDR or MSSP depends on many factors that are specific to your organization. When in doubt, a trusted partner can help guide the way.

To get started, contact ActZero or schedule a demo.

About ActZero

ActZero can help guide you in your decision to choose MDR or MSSP. Contact us to learn more.

If MDR is the right choice for you, learn how ActZero's MDR can help you drive security engineering, increase internal efficiencies and effectiveness and, ultimately, build a mature cybersecurity posture. Whether shoring up an existing security strategy or serving as the primary line of defense, ActZero enables business growth by empowering customers to cover more ground.

ActZero