COMCAST BUSINESS | MASERGY

WHAT YOU'LL LEARN

- How the scope of services differ
- Use cases: when to use each service
- Checklist for evaluating providers

E-GUIDE

MSS, MDR, SOCaaS: The differences in security services and how to choose

There's always been a long list of acronyms for all the tools and technologies used in the security industry, but the catalog just keeps getting longer with the latest point of confusion being the sprawling abbreviations used to describe security services. Take for example:

- Managed Security Services (MSS)
- Managed Detection & Response (MDR) services
- Security Operations Centers as a Service (SOCaaS)

When most companies today need the help of at least one managed security services provider, IT leaders must understand the difference between these services and more importantly, how to choose what's best for them. Here are some quick definitions and tips to help compare and contrast security services.

MSS vs. MDR services

MSS Explained: MSS is likely the most familiar abbreviation; it's been around for a while. As a general term, it describes a managed service provider that specializes in a broad set of security services. Traditional services that fall under an MSS include technology management and security threat monitoring. These services are perfect for those with internal security operations teams that need help managing tasks across multiple security technologies.

287

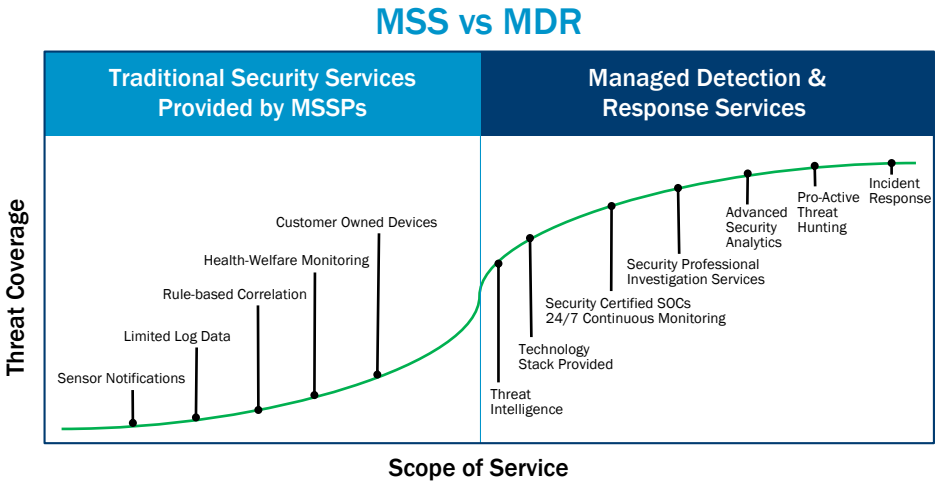
The average number of days it takes an organization to identify and contain a breach

$4.2M

The average cost of a data breach

Source: IBM 2020-2021 Data Breach Report

But as security has evolved, so too have the services. As such, providers needed a way to evolve their offerings with updated acronyms.



While an MSS provider hands the client a list of priority alerts to respond to, an MDR service will both produce that list and act on it too.

MDR Explained: MDR takes the MSS concept one step further, focusing on the critical actions of security operations: detect and respond. MDR services include advanced threat detection services, threat intelligence capabilities, and most importantly incident response — certified security analysts taking action against any identified malicious activity.

The Key Difference: While you may find that some MSS providers perform a limited number of templatized response actions, they generally escalate actions to the client rather than take matters into their own hands. Meanwhile, MDR providers take pride in client collaboration, customizing threat response actions around their client's own systems, processes, and compliance requirements. MDR services are also known for putting endpoint security at the center of their service. MDR includes a team fighting cyber crime on your behalf. The value of that action cannot be understated, as this is where most mid-size companies and their security operations are failing today.

MDR benefits:

- Accelerated threat discovery
- Faster response time
- Reduced dwell time—the amount of time an attacker has inside your IT environment before being detected and contained (average dwell time is 287 days for a given breach, according to **IBM**)
- Additional security personnel: certified analysts and expertise

SOCaaS or SOC Services

Now we're going to start splitting hairs.

SOCaaS is the new flavor du jour, and according to Forrester, it sits somewhere between MSS and MDR. Think of it this way, SOCaaS executes detection and response workflows akin to MDR, but instead of putting endpoint protection platforms at the epicenter, it typically puts SIEM at the epicenter.

Most SOCaaS providers don't include critical response services. They simply focus on technology platforms, escalating security incidents to the client to handle. SOCaaS is recognized for log ingest, tuning, and SOC augmentation — not threat detection and response services.

Keep in mind, these are generalizations and not hard and fast definitions. You might find solutions that break the mold, as each provider has their own approach and their own way of compiling security technologies and services into one offering.

Use cases: When to use what

- When you need to support your internal security operations, turn to an MSS provider
- When you need to find and respond to threats as fast as possible, use an MDR service
- When SIEM problems are your biggest concerns, start with SOCaaS and then expand

People and process are 90% of security success

For decades, IT leaders have been solving security problems simply by slapping on another technology, but that approach is no longer effective. In fact, services (people and expertise) are more important than technology today. Gartner's "Market Guide for Managed Security Services" sums this up well by advising that an effective security program is "60% process, 30% expertise, and 10% technology."

Most SOCaaS solutions don't include critical threat response services.

An effective security program is

60%
process

30%
expertise

10%
technology

What to look for in any security service provider

Whether you need MSS, MDR, or SOCaaS, you will want a trusted partner who brings industry expertise and a capable team. But you'll also want to ensure the right strategy, services, and technologies are in place. Here are some buyer criteria from Nemertes Research to help guide in any search:

Strategy

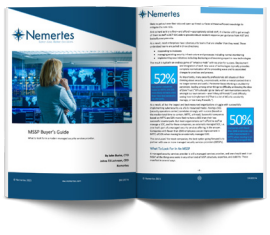
- **Improvement approach:** Industry-leading framework for proactive improvement
- **Risk-based approach:** System for assessing, prioritizing and communicating risks
- **Incident approach:** Process for addressing and resolving threat incidents

Services

- **Environment coverage:** Protection for endpoint, network, cloud, and on-premise
- **Intelligence feeds:** Threat intelligence subscriptions are integrated with solutions
- **Active threat-hunting:** Proactive searches to find undetected threats

Technology

- **Toolset options:** The provider works with the client's existing tools
- **AI and automation:** Analytics and technologies to accelerate security processes
- **Metrics and dashboarding:** Metrics are tracked and accessible in a unified portal



Get the complete Security Services Buyer Guide from Nemertes

So where does Masergy fit in? We're both an MSS provider and an MDR provider. Learn more about our Managed Security services.

20%

of breaches were initially caused by compromised credentials

38%

amount of breach costs represented by lost business and lost revenue

Source: IBM 2020-2021 Data Breach Report

About Masergy

Masergy is the software-defined network and cloud platform for the digital enterprise. Recognized as the pioneer in software-defined networking, Masergy enables unrivaled, secure application performance across the network and the cloud with Managed SDWAN, UCaaS, CCaaS and Managed Security solutions. Industry leading SLAs coupled with an unparalleled customer experience enable global enterprises to achieve business outcomes with certainty.

Let's get started

Call for Sales

+1 (866) 627-3749

Schedule a Consultation

REQUEST MEETING