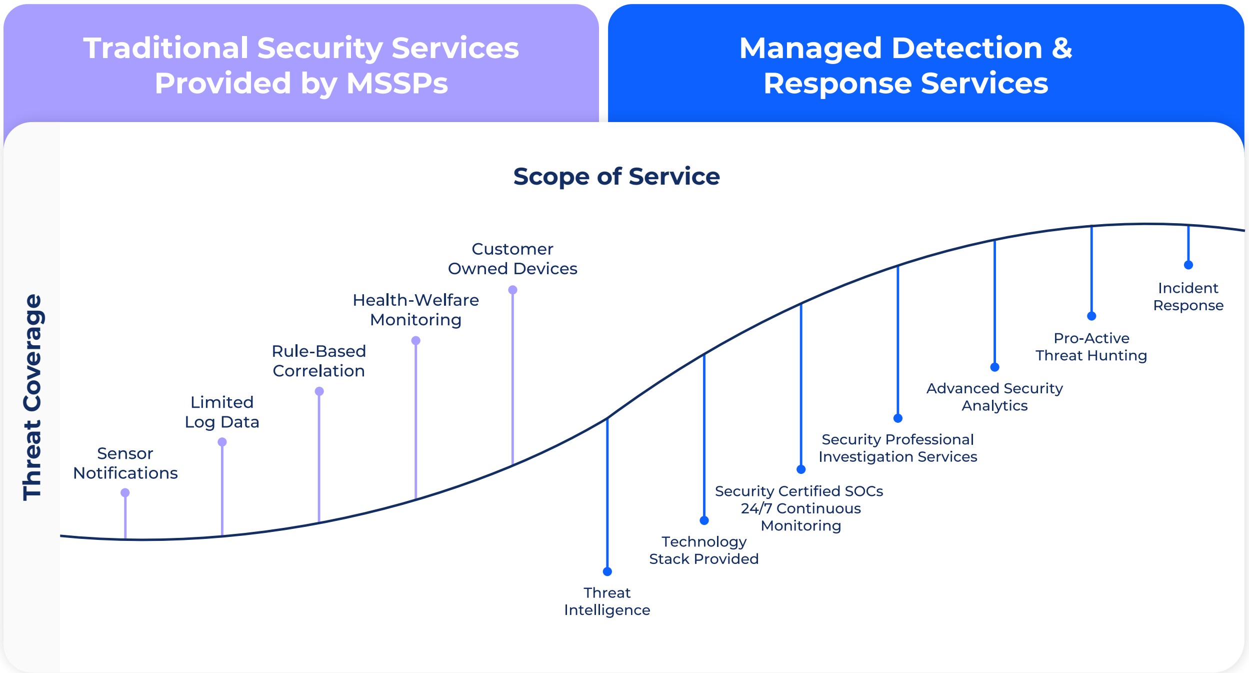
COMCAST
BUSINESS

# Managed Detection and Response vs. Managed Security services

## The difference and how to choose

The world of managed security services is changing rapidly, expanding with Managed Detection and Response (MDR) services. According to Gartner, 50% of organizations will be using MDR services as early as 2025. This turnkey approach is designed to accelerate threat discovery and response time, but what exactly is MDR? How is it different from traditional services provided by managed security service providers (MSSPs), and how do you know if you need it?

## MSS vs MDR


Traditional Security Services Provided by MSSPs
Managed Detection & Response Services
Scope of Service
Threat Coverage
Sensor Notifications
Limited Log Data
Rule-Based Correlation
Health-Welfare Monitoring
Customer Owned Devices
Threat Intelligence
Technology Stack Provided
Security Certified SOCs 24/7 Continuous Monitoring
Security Professional Investigation Services
Advanced Security Analytics
Pro-Active Threat Hunting
Incident Response

## The difference between MDR and traditional security services

Reaching beyond traditional MSSP offerings (including technology management and threat monitoring), MDR integrates advanced technology, processes, and a remotely delivered security operations center (SOC) staffed by experts to detect, analyze, and respond to threats in real time.

Some analysts simplify it as the difference between monitoring services that hand the customer a list of prioritized alerts with suggested action items and an extended, more comprehensive service in which the provider takes an active role inside the customer's environment.

The key element is the response. While existing internal IT resources can lack the resources to monitor and respond to threats in real time, MDR provides round-the-clock monitoring and fast incident response. What's more, MDR leverages advanced threat detection, utilizing AI and machine learning to identify and address known and emerging threats.

**MDR integrates best-in-class:**

✓ Technology

✓ Processes

✓ Remote SOC delivery

## How it works

Using a combination of technology and human resources, MDR services focus on advanced threat detection and mitigation. MDR providers look for actors that have infiltrated the perimeter of the IT environment—in the cloud or on premise. It's a comprehensive solution that includes:

**24/7 Monitoring and Response**
Round-the-clock monitoring and fast response to security incidents.

**Advanced Threat Detection**
AI and machine learning to identify and address known and emerging threats, like Advanced Persistent Threats (APTs) and zero-day exploits.

**Expertise and resources**
A SOC with security professionals with extensive knowledge and industry certifications.

**Data for reporting**
Data and reporting to help businesses with important documentation often requested for compliance audits.

Filtering security noise to identify what's real, what's important, and what's potentially the most crucial, MDR providers leverage best practices in response and work collaboratively with the customer to enable improvement.

## Key benefits of MDR

MDR empowers businesses with managed security focused on advanced threat detection, adherence, and operational efficiency, all without needing to devote resources to create and manage a traditional SOC.

**Benefits also include:**

- Accelerated threat discovery
- Faster response times
- Reduced dwell time*
- Additional security expertise

*The amount of time an attacker has inside your IT environment before being detected

While an improved security posture is typically the priority consideration, another benefit surfaces when considering the cybersecurity skills shortage and cost of employee churn. Building in-house security teams presents serious challenges. According to recent studies, the global cybersecurity labor gap stands just shy of 4 million professionals, with two-thirds of organizations facing labor gaps in their cybersecurity teams.

## Knowing if MDR is right for you

MDR is particularly helpful for IT leaders who:

→ Are struggling with an overwhelmed IT staff without 24/7 security monitoring

→ Have a siloed approach to security with multiple products that are not working together

→ Are considering building an in-house security operations team

→ Need security data including to respond to compliance audits

→ Are using unmonitored cloud services and apps

COMCAST
BUSINESS

Learn more about Comcast Business Cybersecurity Solutions.

Learn more