Separating Fact from Fiction About MDR

Get the truth about the popular approach to cybersecurity

The encouraging truth about managed detection and response.

Today's attackers are increasingly outpacing the defenses of many organizations. That imbalance, coupled with the fact that many organizations lack the resources to monitor their environment 24/7/365, has created a situation where security needs are going unmet.

For organizations looking to boost their defenses, managed detection and response (MDR) has become an established way to accelerate detection, investigation, and response to threats. In fact, according to Gartner:

"By 2025, 60% of organizations will be actively using remote threat disruption and containment capabilities delivered directly by MDR providers, up from 30% today."[1]

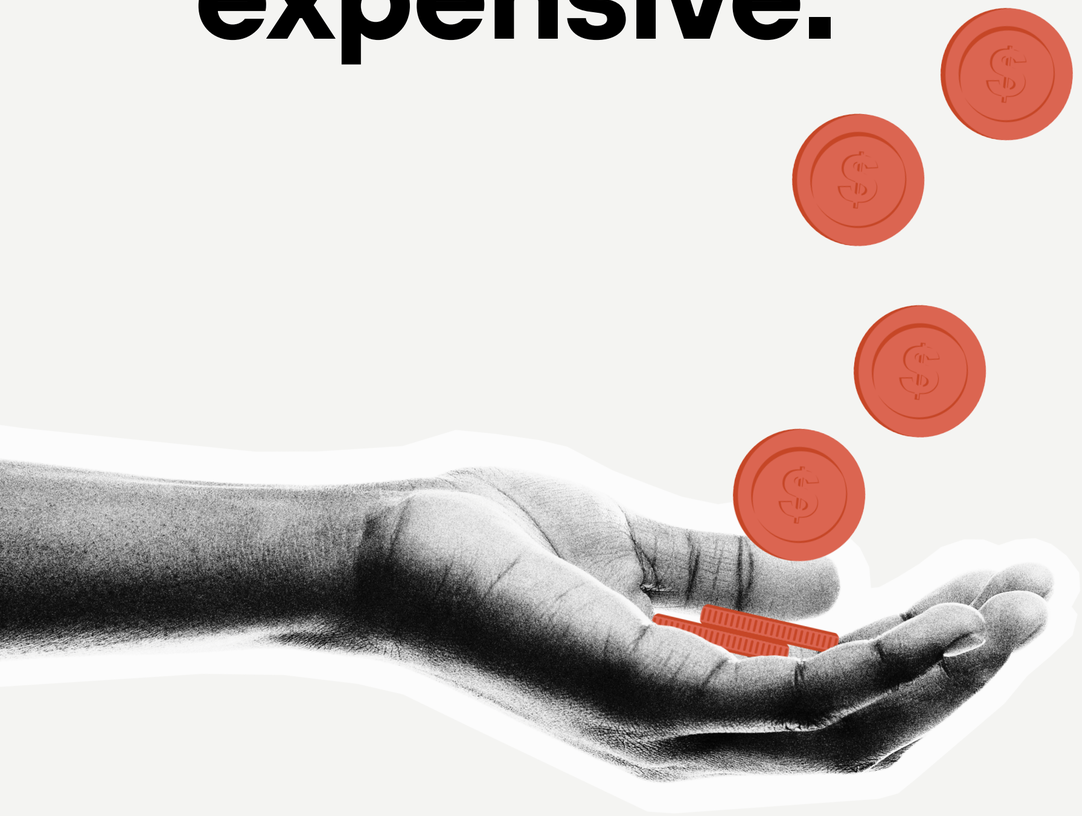
But despite the surge in interest, misconceptions about MDR persist. What are the misconceptions, and what's actually true?

Let's separate the facts from the fiction.

1. Pete Shoard, et al., *Market Guide for Managed Detection and Response*, Gartner, June 24, 2024.

FICTION

MDR is expensive.



FACT

Partnering with an MDR service can be more cost-effective than building and maintaining a modern 24/7 security operations center (SOC).

MDR is a strategic approach that can actually result in long-term security operations savings. MDR providers leverage economies of scale, expertise, and mature processes to accelerate your mean time to response (MTTR) and strengthen your security posture. (In other words, you benefit from their efficiencies.) And MDR experts—sometimes at a world-class level—monitor your environment and respond to threats 24/7/365, providing a level of coverage and a caliber of insight that are difficult to achieve in-house.

When you partner with an MDR provider, you gain cutting-edge technology and deep expertise at a predictable operating expense, instead of a hefty upfront investment. Ultimately, the long-term benefits to your business from robust security—strengthened posture, threat containment, reduced risk, staff retention, and improved morale—save you money.

The cost of maintaining an on-site SOC has dramatically increased.

In fact, SOCs are becoming so expensive that many organizations are simply getting priced out. According to Gartner:

"Midsize enterprise organizations do not have the budget to fully staff a 24/7 security operations center."[2]

2. Paul Furtado, *Security Staffing Options for Midsize Enterprises*, Gartner, January 2022.

FICTION

MDR focuses only on endpoint security.

FACT

Modern MDR services can provide comprehensive visibility across endpoint, cloud, network, identity, and third-party data.

True, some MDR services respond only to threats on your endpoints. But just as XDR platforms extend beyond simple endpoint protection to secure your network, the cloud, and beyond, the best modern MDR services provide a broader view of your environment.

MDR analysts can use XDR to aggregate security telemetry from endpoints, network, cloud, and identity sources and apply high-fidelity threat intelligence to prevent, detect, and respond to even the most sophisticated threats. The result is comprehensive protection against threats that might otherwise be missed.

PRO TIP

Don't settle for part of the package.

When you are evaluating MDR services, look for a provider that seamlessly integrates with an XDR and SIEM platform, has expertise on your technologies, and—once they're on board—will work quickly to get an intimate understanding of your unique environment.

FICTION

MDR will overload your team with alerts.

FACT

Unlike typical managed security service providers (MSSPs), MDR services provide monitoring, investigation, response, *and* remediation, taking a huge load off your team's shoulders.

MDR not only helps you manage the endless backlog of alerts; the right provider will actually reduce the number of alerts you receive, rather than increasing email alert fatigue. MDR also provides around-the-clock monitoring, analysis, and resolution of security incidents and containment of threats. MDR can be natively integrated with XDR, too, so your team can interact with a single UI for both services, with the MDR provider resolving incidents directly in your XDR platform.

Your partnership with your MDR provider should be collaborative, with their team working closely with yours to tackle the day-to-day operational and reactive tasks to allow you to focus on proactively advancing your security program. In other words, MDR will extend your capabilities, rather than burdening your staff with more work.

PRO TIP

MDR does not manage everything.

MDR is a partnership that will reduce risk, help you improve your security posture, and extend and elevate your team. It is not a replacement for your team. You will still need SecOps staff to resolve issues unique to your organization, including patching or updating/upgrading software and making business and risk decisions. The MDR will typically provide detailed recommendations and step-by-step guidance on these.

FICTION

You'll lose control with an MDR provider.

FACT

MDR providers work with you to determine their level of involvement, so decision-making is always in your hands.

When you work with a leading MDR provider, you'll have the ability to choose the level of remediation they'll provide and the types of actions they'll take. You can align on which response actions the MDR may perform in real time and which require your approval first, before they take action. You'll receive customized actionable reports on a regular cadence, specific to your environment.

The choice is always yours and can change over time. Your MDR provider will give you the tools, knowledge, and support to make informed decisions. They should also be available 24/7/365 for you to contact them directly and ask a question.

PRO TIP

Communication is key.

When you're evaluating MDR services, look for a provider that has a process in place for defining their level of involvement and decision-making; it should be clear and comprehensive. And when it comes to communication, ask about the channels offered. Does the provider integrate with your collaboration software? Will you be talking directly to analysts?

FICTION

You don't need MDR if you have all the tools.

FACT

MDR and XDR are complementary offerings in a comprehensive cybersecurity strategy.

XDR solutions are technologies that aggregate and correlate security data from multiple sources—including endpoints, networks, and cloud—to provide broader visibility and context for robust and accelerated threat detection, prevention, and response.

MDR is a managed service delivered by experts who use EDR/XDR technology to provide continuous, reliable coverage and response, working with you to improve your security posture. An MDR will have deep knowledge of XDR and will help you operationalize XDR to get the most out of it.

The best MDR providers also offer proactive threat hunting—an area where human expertise is vital—for detecting the most sophisticated threats. Highly skilled threat hunters actively search your environment for suspicious signals and emerging threats, identifying and containing issues before they escalate. It's one critical way that MDR strengthens your overall security posture.

In an IDC survey,

64%

of organizations stated that MDR will help them gain faster detection of intrusion.[3]

3. *The Emergence of Managed Detection & Response (MDR),* IDC, June 24, 2020.

FICTION

You've got a SOC, so you're completely covered.

FACT

Many SOCs partner with MDRs to help them address the growing complexity of today's threat landscape.

Even the largest SOCs often find themselves in firefighting mode with little time for strategic initiatives. Having a backlog of alerts, sometimes in the thousands, is not unusual. And arranging shift work for 24/7 monitoring is a major challenge—not to mention expensive.

MDR enables you to scale your capabilities and add coverage without staffing your SOC internally around the clock. It complements and extends your internal SOC team to deliver 24/7/365 monitoring, plus additional expertise, reporting, threat intelligence, and threat hunting capabilities to enhance your security posture. As a result, your team can avoid burnout—and focus on proactive and strategic projects.

Keeping a SOC staffed is an ongoing challenge.

Even if you can afford to staff a SOC 24/7/365, turnover is a given. A recent survey from the SANS Institute uncovered the following:

"SOCs aren't designed, built, or operated to address the human capital cycles that actually occur... Three years or fewer is the most common [duration of employment]."[4]

4. Chris Crowley, et al., *SANS 2023 SOC Survey*, SANS Institute, June 2023.

FICTION

MDR is only for very large enterprises.

FACT

MDR services are for companies of all sizes and can level the playing field, giving mid-sized businesses the same protection and expertise as large enterprise SOCs.

If you're a mid-sized company, you might assume that you're less vulnerable than big enterprises. You're not. Cybercrime is often a crime of opportunity. Smaller organizations can actually be more exposed—with more security gaps, fewer cyber resources, and older infrastructure than their larger peers. Unfortunately, bad actors know that smaller businesses can be "softer" targets.

MDR is for organizations of all sizes. And by partnering with an MDR provider, you can almost immediately gain access to experts who will work for you to ensure that you can confidently respond to even the most sophisticated threats 24/7/365. It's a way to level the playing field, getting access to enterprise-grade protection and response without the need for a huge investment in infrastructure and staff.

41%

of small businesses fell victim to a cyber-attack in 2023,
a rise from 38% in 2022... and close to double from 22% in 2021.[5]

5. *Hiscox Cyber Readiness Report 2023*, Hiscox, 2023.

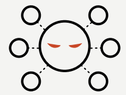
Unit 42 MDR:

Our world-class security experts become an extension of your team

When choosing an MDR service, why not opt for the one modeled after the SOC protecting the largest security company in the world?

Unit 42® MDR from Palo Alto Networks® includes a team of expert threat hunters and cybersecurity analysts who not only protect our own network but also advise CISOs around the world. As your MDR provider, they work for you around the clock to detect and respond to cyberattacks, allowing your team to scale fast and focus on what matters most.

Unit 42 MDR leverages Cortex XDR® and Cortex XSIAM,® our own products, so our analysts have unmatched expertise in the product technology as well as visibility into all data—endpoint, network, cloud, and identity—stitched together to provide the context needed for faster investigation and response.



The Unit 42 MDR service includes high-fidelity threat intelligence and proactive threat hunting, with seasoned experts manually seeking out emerging adversaries and hidden threats using threat intelligence and the powerful data searching capabilities of Cortex XDR and Cortex XSIAM.

Ready for true peace of mind with an MDR partner equipped to quickly identify and stop the malicious activity most likely to impact your organization?

Talk to an expert about the strategy that's right for you.

3000 Tannery Way
Santa Clara, CA 95054

Main: +1.408.753.4000
Sales: +1.866.320.4788
Support: +1.866.898.9087

www.paloaltonetworks.com/unit42/respond/managed-detection-response