What MDR is and Why You Need It

Managed Detection and Response (MDR) is one of the fastest-growing areas of cybersecurity for a simple reason: companies can not keep up with all the cyber threats they face. Endpoint tools and security information and event management (SIEM) systems help, but organizations still need someone to deal with all the alerts those tools produce.

MDR is increasingly the answer, as Gartner estimates 50 percent of organizations will be using MDR services by 2025 and that the market is growing at a rate nearly five times that of other managed security service (MSS) offerings.[1]

Read on to quickly get a handle on what MDR is all about and why you more than likely need it.

What's driving demand for MDR

Companies are flocking to MDR because they're drowning in security threats and alerts. One recent study showed businesses suffered 50% more cyberattack attempts per week in 2021 vs. 2020.[2]

Ransomware is a particular concern. More than 20% of companies have suffered a ransomware attack and it is present in almost 70% of breaches involving malware, according to the 2022 Verizon Data Breach Investigations Report. [3]

To fight back, companies are implementing tools including endpoint detection and response (EDR), SIEM and security orchestration automation and response (SOAR) platforms. That's a positive step, and those tools do indeed help detect cyber threats by generating alerts when they detect suspicious activity.

The problem is, it requires seasoned security staff to configure, monitor and optimize the tools, and to examine the alerts they produce to determine which are benign vs. worrisome. That means standing up some kind of security operations center (SOC) or practice, with staff monitoring the tools 24×7.

Which leads to the other big MDR driver: the lack of experienced security personnel to staff those SOCs. While the size of the global security workforce is growing, it's not keeping pace with demand, according to the 2022 (ISC)^2 Cybersecurity Workforce Study. The global security workforce now stands at 4.7 million people, but there's room for about 3.4 million more.[4] That means the workforce is around 40% shy of where it needs to be.

That, of course, is driving up salaries for security professionals. So, even if you could find qualified personnel to initially staff your SOC, it will be difficult and expensive to keep them for the long haul.

What MDR is and how it helps

As a result, even large organizations struggle with the day-to-day management of their cybersecurity tools. These tools often produce huge volumes of alert data that companies simply can't filter through fast enough to find – and respond to – alerts that represent critical threats.

An effective MDR service will work with your existing security tools and infrastructure, including EDR, SIEM and SOAR tools. The MDR provider will ingest all the telemetry from these tools from across your entire environment, including cloud and hybrid cloud infrastructure.

That's an important point, because complex, hybrid IT environments have large attack surfaces that are by nature difficult to secure. A good MDR provider will be able to correlate alerts coming from across the entire attack surface and zero in with confidence on those that are indicative of an actual threat. The goal is to eliminate all the false-positives alerts, leaving only confirmed threats that require immediate action.

Once it identifies a confirmed threat, responses vary by MDR provider in terms of what happens next. Most will alert the customer's security team to the threat, but leave it up to the team to respond. That relieves you of the need to stand up a 24×7 monitoring operation, but you'll still need to be prepared to respond to an alert ¬– including those that come in around 3 a.m. on a Saturday.

Separating the best MDR providers

In a 2021 report on the MDR market, Forrester Research said good MDR providers avoid "becoming the alert factories their MSS cousins became." When evaluating MDR providers, Forrester advises companies look for:

A squad model: a dedicated team of analysts, responders, and customer support specialists that work within a given vertical and geography and offer a customized delivery experience.

Superior detection capabilities: The ability to combine strong hunting methodologies with organic threat intelligence, and apply learnings from each client to others at scale. "The happiest MDR customers found vendors that could easily scale detection, customize alerts, and offer response actions intimately tailored to the client environment," Forrester said.

A complement to your team: An MDR provider should sync with your technology stack, specialize in the specific types of detection and response activity that matter to you, and generally act as a complement to your security team.

The Trustwave MDR approach

Trustwave MDR fulfills – and exceeds - those requirements.

Trustwave MDR is based on its cloud-native eXtended Detection and Response (XDR) security operations platform, Trustwave Fusion. We ingest security telemetry into Fusion from your existing security tools and infrastructure, including hybrid and multi-cloud operations.

Once a threat or anomalous behavior is detected, the team investigates to eliminate all false-positives, leaving only confirmed threats that require immediate action. This alone dramatically improves the productivity of a security team by eliminating time wasted chasing alert noise and false positives.

Rather than leave the response up to the client, Trustwave can take incident response actions on their behalf or in conjunction with their team, depending on predefined response protocols. That response may vary depending on the asset or severity of the alert, in accordance with your security policy. Not to worry, these discussions won't be happening at crunch time – they're all part of the Trustwave onboarding process, so we'll know what to do when the time comes.

Get your security team the help you know they need, with Trustwave MDR.

To learn more, visit our Managed Detection and Response page.

[1] Market Guide for Managed Detection and Response Services, Gartner Research, October 25, 2021.

[2] "Alarming Cyber Statistics For Mid-Year 2022 That You Need To Know," Forbes.com, June 3, 2022.

[3] 2022 Data Breach Investigations Report, Verizon Business, 2022.

[4] (ISC)^2 Cybersecurity Workforce Study, 2022

www.trustwave.com