Secureworks®

WHITE PAPER

Managed Detection and Response: The Right Answer for Today's Security Challenges

By 2025, 60% of organizations[1] will be actively using remote threat disruption and containment capabilities of Managed Detection and Response (MDR) solutions — a steep climb from 30% of organizations using MDR today. And these organizations are motivated by what they see happening around them. They don't want to become an example — like the 79% of organizations[2] that reported experiencing a ransomware attack within the last year.

What's driving this transition? Pain. From chief executives down to the security teams that investigate and respond to incidents, organizations are feeling the crunch of some very common pain points.

They're facing challenges like:

- **Staffing Shortage:** An ongoing, sustained shortage of cybersecurity talent, measured in the millions of empty positions globally, is making it hard to adequately protect data and systems.
- **More Risk:** Attack surfaces are expanding beyond the traditional fronts of network and endpoint to include the cloud, identity systems, email, and other business applications. The volume of new terrain to exploit is growing fast.
- **Lagging or Insufficient Budget:** Many organizations see budgets rising slower than the rate of attack surface expansion. While some organizations struggle with an insufficient budget to fund cybersecurity, many more organizations have a budget but are finding it cannot keep pace with the threat actors they face.
- **Flying Blind:** Knowing your attack surface is daunting enough, but maintaining enough visibility to stay ahead of threats is another. Too often, threats aren't spotted until they've blossomed into full-fledged attacks.
- **Lack of Efficiency:** Time really is money, and cybersecurity isn't immune from the demand for getting more done with less money.

60%

of organizations will be actively using MDR solutions by 2025[1]

79%

experienced a ransomware attack within the last year[2]

- **Evolving and Rising Threats:** Organizations are seeing heavier losses from attacks like phishing and ransomware, while the average dwell time of threats within systems is dropping. This is compounded by higher cyberattack rates on weekends and holidays when security staff are more likely to be out of the office.
- **Regulatory, Performance, and Insurance Pressures:** Businesses are facing more pressure to prove security posture and performance, meet regulatory requirements, and address concerns from cyber insurance providers.

The stakes have never been higher. Fortunately, MDR is positioned to solve these problems.

But quality MDR must integrate the right technology infrastructure with human intelligence and machine learning to power a higher level of security. It has to be human-led and technology-supported. Furthermore, it must deliver turnkey Security Operations Center (SOC) functionality that instills customer confidence from day one, while also fostering the collaboration necessary to transform an organization's security from the inside out.

MDR must integrate the right technology infrastructure with human intelligence and machine learning to power a higher level of security.

MDR: Evolution of a Solution

In recent years, many organizations faced the difficult task of choosing between a variety of different provider types that all looked very different.

Some organizations started outsourcing their cybersecurity to Managed Security Service Providers (MSSP) in an effort to secure the 24/7 coverage they wanted. But that meant those organizations didn't always have true visibility into the value they were receiving from an MSSP's delivery of what was often a black box solution.

Some organizations relied on management of a single platform like SIEM. Whatever way you slice it, these approaches all had one thing in common: they were filled with holes, lacked the appropriate platform, and didn't include native response capabilities or human-driven intelligence to fulfill on their hype.

Other organizations entrusted their cybersecurity to EDR vendors who had recently rebranded their solution as MDR, even if that constituted more of a "managed" version of EDR that didn't really cover the holistic expanse of the customer's IT and OT infrastructure.

This variety of options was anything but ideal, overwhelming organizations with choices and expenses, while still failing to fully address the threats they faced.

And so, companies began evaluating MDR solutions, with some iterations having inherent pitfalls like an over-reliance on endpoint telemetry and an overall lack of transparency.

An endpoint-focused security approach as seen in recent years monitored endpoints, collating telemetry, and assessing it for threat level. This led to a focus on more real threats versus noise, and most certainly helped teams and MSSPs respond appropriately to real threats.

Some MDR solutions have inherent pitfalls like an over-reliance on endpoint telemetry and an overall lack of transparency.

But an endpoint-focused approach has real shortcomings, including:

- **A lack of decisive response capability.** Chaotic alerts and general alert fatigue has made developing a decisive response more difficult for overtaxed security teams.
- **The potential for tool sprawl.** More tools might sound better, but this phenomenon can create coverage gaps and can send security teams into a tilt-a-whirl, swiveling between point solutions that don't work well together.
- **The need for more hours or staff (or both).** It's counter-productive that more solutions could mean the need for more staff or hours, but that's exactly what many organizations are finding amidst a global cybersecurity skills shortage.
- **Limited visibility to your full infrastructure.** Blind spots left by endpoint-focused or disparate solutions can allow threat actors to gain access to valuable data and systems.

There's one other major issue with some iterations of MDR: **An overall lack of access and transparency.**

For many internal teams engaging with an MDR provider, there may be a gap between the dashboards and interfaces you see versus what your provider sees. Your team may not see the same data your provider does. Worse yet, in an emergency breach situation, there could be a lack of response capability that leaves your team hanging. Finally — as if you needed more to worry about — switching vendors could be a nightmare, losing services as well as any infrastructure that has been developed by your previous provider.

The Capabilities That Comprise Best-in-Class MDR

Quality MDR is purpose-built to address and resolve the most common pain points that organizations report, while offering better value and visibility. And to do that, the best MDR has a technological foundation of extended detection and response (XDR).[3]

XDR is a single platform that ingests telemetry across IT and OT. As an XDR platform ingests this telemetry, it adds layers of threat detection, integrated threat intelligence, streamlined investigation support, and even playbooks that help drive response actions. MDR that is built on an XDR platform ultimately supplies unparalleled automation, collaboration, and visibility across a unified picture of your systems.

That's why Secureworks® Taegis™ ManagedXDR is an MDR solution built on the Taegis XDR platform. With this unique foundational technology, Taegis ManagedXDR provides superior detection, unmatched response, and an open-without-compromise platform designed to meet today's organizations wherever they are in their security journey.

And what do industry experts have to say about how MDR should function for organizations looking to get the most out of their solution that will truly address their pain points?

In its "2023 Market Guide to Managed Detection and Response," Gartner recommends that security leaders seek out a SOC-supported MDR solution capable of supplying some key benefits:

1. Remotely delivered human-led SOC capabilities even when the customer lacks any existing internal security team — or, as is often the case, when an organization needs to quickly ramp up or scale their existing security team.
2. A fast approach to containment and reporting of incidents. How quickly can your MDR provider respond on your behalf? How soon will they let you know of a major incident? Finally, how well can they integrate with and support unique legal or compliance requirements your organization may have?
3. Ability to equip your organization with pre-defined playbooks, workflows, and enough integrations to maximize any existing security investments you have in place. This is important for building the true value of MDR — and helping your organization see faster realization of measurable ROI on that investment.
4. Alignment to business requirements and the capability to provide insights that can support reporting, from interdepartmental information sharing all the way to rolling reports up to your board.

What Gartner is outlining here are components of best-in-class MDR, not simply a "band-aid" that works just for short-term cybersecurity purposes. Your MDR solution should be part of an overall strategic move towards better security, better efficiency, and better value.

Your MDR solution should be part of an overall strategic move towards better security, better efficiency, and better value.

Quality MDR delivers tangible improvements to your organization's security posture, reducing risk and giving broad visibility while delivering better efficiency at a budget conscious price point.

So how do you make sure your chosen MDR solution is different than the rest of the pack?

Key Differentiators of Best-in-Class MDR

As more organizations turn to MDR to help them solve their most pressing problems, it's helpful to have a checklist of "must-have" elements. This can be a valuable way to compare solutions, leading you to the best possible decision about your future MDR solution.

THE BEST MDR...

Offers Complete Visibility Across the IT and OT Landscape

A strong MDR solution examines your entire infrastructure, offering visibility across network, business applications, cloud, email, endpoints, identity, and OT infrastructure. That means eliminating gaps in your attack surface that could allow threats to find a way in. Furthermore, this level of coverage must include managed investigation and response — to help identify real threats and respond accordingly.

Delivers Real Security Expert Advice with Speed

Real, fast connection to a live SOC team analyst is a critical part of quality MDR. That means responding with lightning speed to questions or issues — with qualified human beings and not just some automated response queue. A good MDR provider will work alongside you and give you direct access to experienced analysts to help resolve challenges and advance serious issues, with unlimited support that persists until the job is done.

Practices Collaboration Through Transparency

You can't feel truly "in step" with your MDR provider if you can't see the interface they use. That's like taking directions in the dark from someone who is wearing night vision goggles. Instead, quality MDR will be transparent, with the same interface and platform for both your internal team and your provider. Bonus points if the platform was built with UX as a focus and has a history of successful investigations across a breadth of customers and industries.

Maximizes Your Budget and Future-Proofs Existing EDR Investments

It's not uncommon for organizations to have more than one endpoint detection and response (EDR) agent. That's why best-in-class MDR should ingest data across a mixed-EDR agent environment, without needing you to rip-and-replace existing investments. Furthermore, your MDR should protect you from dreaded vendor lock-in and provide you with flexibility and adaptability. No matter where you're starting from, your MDR solution should meet you there — not demand that you change to suit the solution.

Provides Quality Incident Response Expertise

In case of a real security incident, your MDR provider must move seamlessly, decisively, and quickly into full Incident Response (IR) mode. They should have an experienced team at the ready, plus on-site or virtual support available to you anywhere in the world and the ability to work with insurers and lawyers (an unfortunate but necessary part of the process). Look for solutions that offer unlimited response to security incidents to ensure that the problem is completely resolved and remediated.

THE BEST MDR... (CONTINUED)

Liberates Organizations Through Options

Your MDR provider should allow you the freedom to remove the managed service and take over managing your own security with the same platform intact as the foundation — all to avoid the added cost of any extra technology changes.

Helps Organizations Replace Other Solutions and Get Longer Data Retention

Some MDR solutions have limited log management storage. Because of this, they'll rely on solutions like Security Information and Event Management (SIEM) to extend storage capability. But that can quickly become cost prohibitive. In fact, some customers will find themselves paying double for the same storage they could get with a holistic, XDR-based MDR solution. Choose an MDR provider that stores more of your raw telemetry for less cost, with options to scale log management and data to longer periods based upon your own needs. A good MDR solution will maximize budget, bundle in longer data retention, and will replace part — if not all — of your SIEM spend.

Filters Through Noise to Detect the Real Threats

A good MDR provider cuts through the noise to get to the most critical alerts: real threats. That means having the breadth of experience and knowledge to sort through the noise, while having the integrations necessary to cover all your applications — and that means going way beyond the endpoint-focused approach of some MDR solutions.[4] A quality MDR solution will be designed to dynamically know how to escalate only the most critical threats, governed by a provider that knows when to get your team involved. It's once again that unique combination of the right technology and deep human knowledge and expertise.

Uses the Latest, Most Updated Threat Intelligence

Detection algorithms in your chosen MDR solution should factor in active, evolving threat intelligence that is constantly updated — applying it for immediate protection of your infrastructure through constantly updated or newly created detectors. That's why Secureworks tracks threat groups, dark web activity, and emerging threats — thus making leading threat intelligence a part of the Taegis XDR platform.

Reports Regularly on Performance and Progress

Going back to transparency, your MDR provider should be reporting back to you regularly — at least quarterly — on performance and security maturity. This includes how you stack up against your peers and where you're exceeding or lacking, with recommendations on how you can improve security posture.

With Taegis ManagedXDR, our customers are equipped to develop improved security maturity and build better security posture.

Secureworks: Committed to Helping Organizations Catch the Threats

A quality MDR solution equips your organization for the future, providing you with the insight, transparency, and support you need to build long-term security posture and resistance to the most aggressive cyber threats. They arm you with insights, data, and the right platform and perspective to help mold your long-term cybersecurity.

Designed with this long-term vision in mind, Taegis ManagedXDR is a fully managed threat prevention, detection, and response solution that combines our powerful, open Taegis XDR platform with extensive security expertise. Taegis XDR is a security SaaS platform delivered on top of Amazon Web Services (AWS).

Using threat hunt and IR engagement insight from more than 4,500 customers and 10,000 IR and testing engagements,[5] Secureworks can help your organization learn the skills it needs to catch the threats that are evading other so-called MDR solutions.

THE SECUREWORKS DIFFERENCE

- We provide <90 second access to real SOC analysts, with unlimited support included.
- Our Secureworks SOC and customers always share the same interface.
- We deliver the best support for a mixed-EDR environment, helping organizations meet their needs today and in the future.
- We keep a full-service IR team at-the-ready, with unlimited IR support included for assets monitored.
- We give you the freedom to remove the managed service* and manage your solution in-house, using the same platform and avoiding any change in technology.
- We help organizations replace and maximize SIEM budget with one year of log retention included, with lower total cost of ownership and better performance — plus easy expansion options.
- We filter the most noise from the most sources. Secureworks finds 99.6% of native system alerts to be false positives — diving deeper to maximize existing tools and wasting no time on false positives.
- Our detection algorithms are powered by 40B+ unique threat and knowledge nodes, updated continuously by our team of 50+ threat researchers using intel from thousands of incident response exercises per year.
- We provide quarterly customized expert maturity and performance updates for all MDR customers.

*Removal of services can occur at end of contract period

Today's organizations are hungry for better insight, better service, and better cybersecurity. Smart security leaders know that the adversary is always just another creative step away — and that there's no sure-fire way to avoid an incident. For organizations finding themselves tempted to settle for a black-box, service-only approach to MDR or an EDR-centric delivery model, settling can ultimately increase operational risk of an attack. Instead, smart security leaders should focus on a solution that helps them build long-term learning, growth, and security maturity.

Organizations searching for the right MDR provider and solution need:

1. A solution that will protect their systems
2. A provider that will communicate and collaborate with their internal teams
3. To achieve a greater level of cybersecurity maturity

When a solution helps you do all three, you'll know you've got the highest quality MDR available — the kind of MDR backed by an open XDR platform, giving you reliable monitoring with on-demand SOC capabilities in one holistic, cohesive solution.

To learn more about how Secureworks Taegis ManagedXDR satisfies the critical MDR needs of today's most secure organizations, visit secureworks.com.

1 Gartner Market Guide for Managed Detection and Response, February 2023
2 ESG eBook, The Long Road Ahead to Ransomware Preparedness, March 2022
3 Secureworks Taegis XDR Buyer's Guide, 2022
4 White Paper: It's Time For your Cybersecurity to Move Beyond the Endpoint, Secureworks, 2023
5 Secureworks 2022 State of the Threat: A Year in Review, 2022

Secureworks®

Secureworks®

Secureworks® (NASDAQ: SCWX) is a global cybersecurity leader that protects customer progress with Secureworks Taegis™, a cloud-native security analytics platform built on 20+ years of real-world threat intelligence and research, improving customers' ability to detect advanced threats, streamline and collaborate on investigations, and automate the right actions.

CORPORATE HEADQUARTERS

United States
1 Concourse Pkwy NE #500
Atlanta, GA 30328
+1 877 838 7947
www.secureworks.com

EUROPE & MIDDLE EAST

France
8 avenue du Stade de France
93218 Saint Denis Cedex
+33 1 80 60 20 00

Germany
Main Airport Center,
Unterschweinstiege 10 60549
Frankfurt am Main Germany
069/9792-0

United Kingdom
One Creechurch Place,
1 Creechurch Ln
London EC3A 5AY
United Kingdom
+44(0)207 892 1000

1 Tanfield
Edinburgh EH3 5DA
United Kingdom
+44(0)131 260 3040

United Arab Emirates
Building 15, Dubai Internet City
Dubai, UAE PO Box 500111 00971
4 420 7000

ASIA PACIFIC

Australia
Building 3, 14 Aquatic Drive
Frenchs Forest, Sydney NSW
Australia 2086
1800 737 817

Japan
Solid Square East Tower 20F
580 Horikawa-cho, Saiwai-ku
Kawasaki, 212-8589
Japan
81-(44)556-4300
www.secureworks.jp