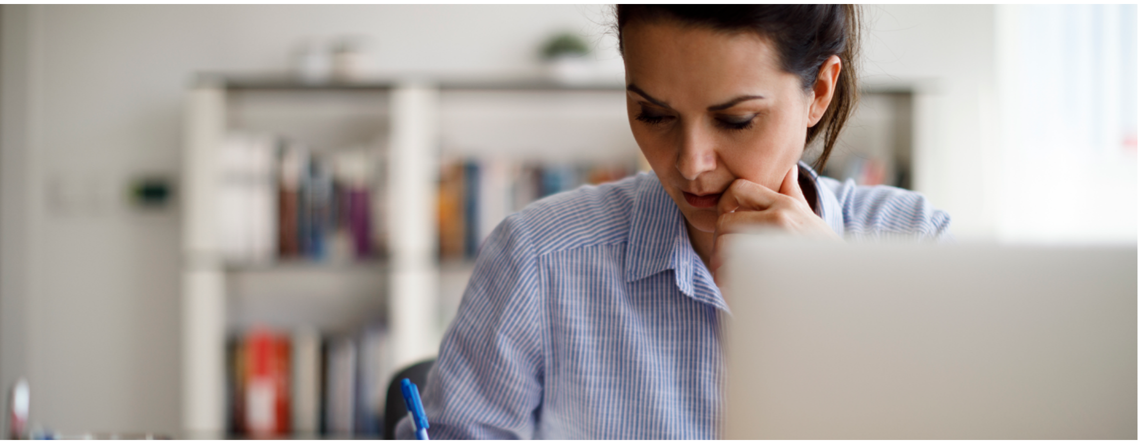
SOLUTION BRIEF

Secureworks®
a SOPHOS company

Evaluating a Managed Detection and Response Provider



Security teams of all sizes and maturity levels are struggling with larger attack surfaces, disparate tools, and insufficient staff and skills. Secureworks® Taegis™ MDR solves these challenges but not all MDR providers are equal in today's market. Read this Brief to learn what requirements to look for in a managed detection and response (MDR solution and how Secureworks stands out in a crowded, changing market landscape.

What's Inside?

This Brief details the key requirements you should consider when evaluating managed detection and response services. It then shows how MDR uses a combination of security analytics software, deep threat intelligence, and leading security expertise to significantly improve threat detection and response times. Links to useful resources like reports, papers, and webinars are included throughout to give you quick access in case you have additional questions or want to see third-party data.

MDR Solutions are Making a Difference

77%

of organizations consider their MDR provider a strategic operating partner that has helped to improve their security program.[1]

70%

of organizations depend on their MDR provider for advanced threat detection.[1]

[1]Source: Source: ESG, What Security Teams Want from MDR Providers, October 2022

Buyer Requirements Table

The following table outlines how any MDR solution you're evaluating must meet certain minimum requirements to solve the challenges above.

Component	Description	Vendor Vetting Questions
Software-Driven Detection Speed	Analytical speed is a powerful weapon in security operations. Any proposed solution needs to be architected around the latest analytics technology, even if you're not directly using it. Be on the lookout for true cloud-native architectures that incorporate data science methods such as machine and deep learning.	1. Describe how quickly you detect <insert threat here> and can you show us how you will respond to it on our behalf? 2. Explain how your cloud-native analytics technology works. Was it built in-house or are you just partnered with another vendor? 3. Discuss how you incorporated data science into your software development process.
Software-Driven Detection Precision	Quickly detecting a false alarm is not very effective. Precise detections fuel precise responses. AI-based Detectors should be purpose-built and used in provider's daily operations. These Detectors are used to find behavioral anomalies such as command and control, brute force attempts, and stolen credentials.	1. Describe how accurately you can detect <insert threat here> and can you show us how you will respond to it on our behalf? 2. Tell us about the experience you have in responding to and evicting threats from organizations? 3. Can you show me a demo of how your solution will apply that experience to keep us safe? 4. Is your software proprietary or via a third party? Does our team get access to your software as part of the solution?
Diversity of Threat Data and Research	With so many sophisticated threats developing, MDR providers must be more committed than ever to providing the most up-to-date threat intelligence to its customers and to organizations looking to build long-term security maturity.	1. How many professionals do you have keeping up to speed on the threat landscape? 2. Show us how your software infuses a diversity of data on historical, current, and potential threats. 3. Does the solution adapt to new attack patterns or is it a static set of rules that are easy to figure out and bypass? 4. Describe the process for how you find threats on other customer environments and feed that data into our defense posture.
Proactive Threat Hunting	Collaboration and transparency between the provider and your team is a key success factor. There needs to be collaborative investigation capabilities and open channels of communication. Threats don't sleep, and neither should your provider's ability to keep you up to speed on a risk to your business.	1. Please show us a demo of the user interface you provide to support co-hunting and collaborative investigations. 2. Describe what happens when we have questions – can we call or live chat with you at any time. 3. Describe how you know what to search for in our environment and what would trigger a hunt with us? Can we initiate a request for help in this area?
Incident Response Support	Your team needs to be able to rely on experienced security professionals to help during critical events. Any provider should provide evidence on how incident response is part of their MDR solution without any hidden fees or costs.	1. Is incident response included in the managed solution? 2. How quickly will you respond in the event of a validated incident? 3. Tell us more about the experience your incident response team has – are they recognized by industry analysts?

Secureworks®
a SOPHOS company

Click here to request a demo of the Taegis XDR platform.

OR

Click here for more information on Taegis MDR solutions.

Choosing the Right MDR Provider: What You Should Know

Gain more insights into finding the right MDR solution.

Watch the Webinar

To download a Data Sheet on Taegis MDR, **click here.**

The answers to these questions will reveal if the proposed MDR solution can improve your defense posture, or if it will waste your limited time and resources. Of course, each environment has unique variables to consider, such as staff size, existing technology investments, and industry or geographic nuances. But this basic list of considerations will help you avoid making a regrettable decision.

Taegis MDR

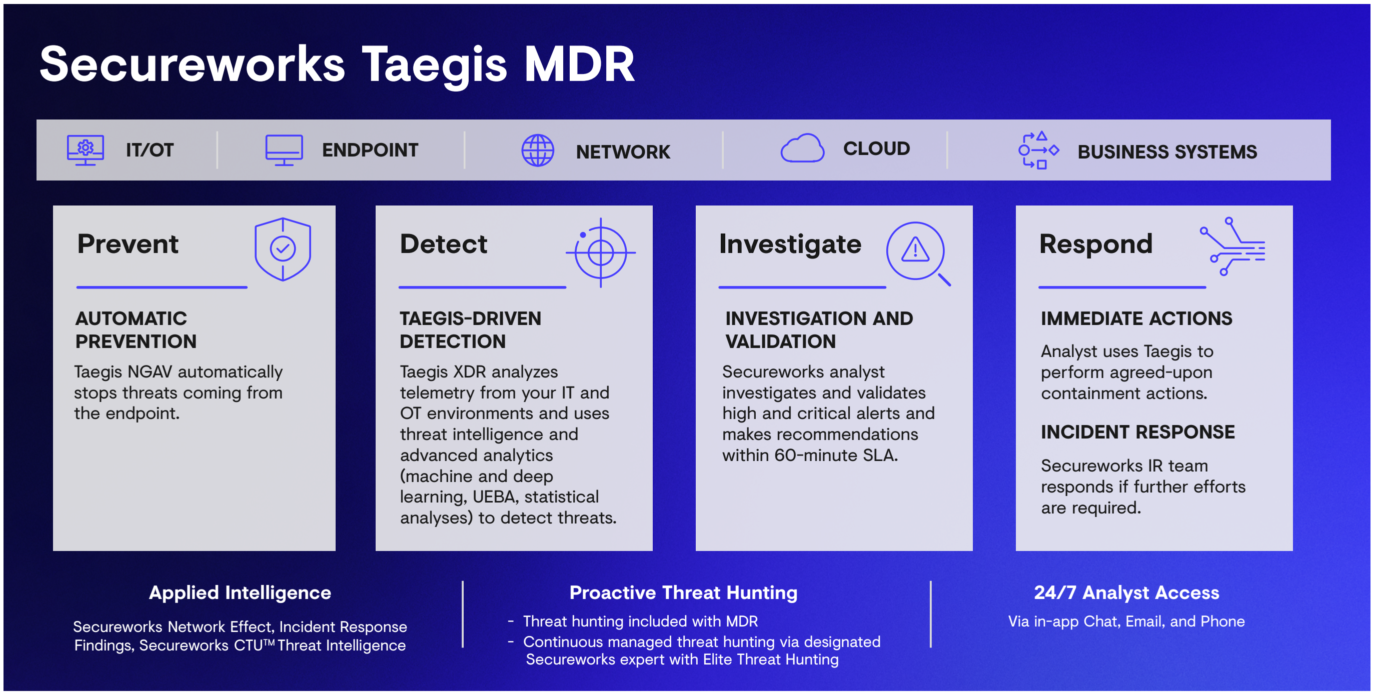
Detection speed and precision requires a software-driven formula. Our Taegis MDR solution is built on a highly powerful security analytics platform called the Taegis platform. It was built using advanced data science techniques to reliably expose adversaries that would otherwise go undetected.

A combination of machine and deep learning trained using our proprietary threat intelligence and customer data powers behavioral threat analytics. The software includes built-in detection use cases, simple investigation workflows, and automated containment actions across your endpoint, network, and cloud environments (see Figure 1).

Secureworks fuses human and machine intelligence to improve security for organizations of all sizes, with capabilities including:

- MITRE ATT&CK mapping
- Incident response and threat hunting expertise
- Threat intelligence and research
- 20+year history of service excellence

Taegis MDR enables your team, however advanced, to deal with an increasing workload and threat volume. We bring our expertise into your daily operations. Your team can collaborate with us on hunts, chat with our analysts, and periodically assess your security posture.



Secureworks Taegis MDR

IT/OT | ENDPOINT | NETWORK | CLOUD | BUSINESS SYSTEMS

Prevent

AUTOMATIC PREVENTION

Taegis NGAV automatically stops threats coming from the endpoint.

Detect

TAEGIS-DRIVEN DETECTION

Taegis XDR analyzes telemetry from your IT and OT environments and uses threat intelligence and advanced analytics (machine and deep learning, UEBA, statistical analyses) to detect threats.

Investigate

INVESTIGATION AND VALIDATION

Secureworks analyst investigates and validates high and critical alerts and makes recommendations within 60-minute SLA.

Respond

IMMEDIATE ACTIONS

Analyst uses Taegis to perform agreed-upon containment actions.

INCIDENT RESPONSE

Secureworks IR team responds if further efforts are required.

Applied Intelligence

Secureworks Network Effect, Incident Response Findings, Secureworks CTU™ Threat Intelligence

Proactive Threat Hunting

- Threat hunting included with MDR
- Continuous managed threat hunting via designated Secureworks expert with Elite Threat Hunting

24/7 Analyst Access

Via in-app Chat, Email, and Phone

Figure 1. Taegis MDR

10 Reasons to Consider Secureworks for your MDR Needs

1 **Benefit from over 20 years of expertise**

Partner with a security organization that uses 20 years of security operations expertise to expose, contain, and resolve advanced threats.

2 **Partner on investigations**

Raise the skill level of your team by partnering on investigations with our experts.

3 **Live Chat with our security analysts**

Instantly pull up a chat window to get expert help whenever you need it.

4 **Enhance your security posture with frequent reviews**

Continuous improvements to your security posture with periodic reviews and reporting, as well as add-on for easy and flexible access to Secureworks Services.

5 **See more threats with unique data diversity**

Act on threat knowledge from thousands of incident response and adversarial testing engagements, a team of elite threat researchers, and our experience protecting over thousands of customers globally.

6 **Act with confidence – backed by human and machine intelligence**

Save time and increase effectiveness through automation of basic tasks and collaborative investigations.

7 **Detect and respond to unknown threats**

Find evasive threats like fileless malware and know exactly how to respond.

8 **Hunt threats proactively to check anomalies**

Our experts help you hunt for persistence mechanisms, threat actor tactics, anomalous networks communications, and anomalous application usage.

9 **Incident response expertise**

Available incident response for added peace of mind.

10 **Protect your cloud deployments**

Use our cloud-native architecture to detect and respond to events from your AWS, Office 365, and Azure envronments.

Experiencing an Incident?

If your organization needs immediate assistance for a potential incident or security breach, please contact us directly on our Incident Response Hotline.

Global Hotline:
770-870-6343

United States & Canada:
1-877-884-1110

United Kingdom:
0808-234-1203

Click here for more information.

For more information, call **1-877-838-7947** to speak to a Secureworks security specialist
secureworks.com

About Secureworks

Secureworks, a Sophos company, is a global cybersecurity leader that protects customer progress with Taegis™, an AI-native security analytics platform built on more than 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.