Secureworks® | Taegis™ ManagedXDR

BUYER'S GUIDE

Managed Detection and Response Buyer's Guide

Buyer's Guide Introduction

The Current State of Affairs

Managed detection and response (MDR) solutions are the hottest thing in cybersecurity, and the marketplace has been flooded in recent years with a variety of vendors offering solutions such as managed EDR, managed SIEM, or a combination of the two. Many of those solutions rely on a combination of technologies that must be customized and integrated by a service provider to provide proactive threat detection and rapid response.

Consider the findings from an Enterprise Management Associates study[1] that found:

48%	Small/midsized enterprises that say in-house security staff are overwhelmed by number of security tools/layers to manage
33%	Large enterprises that say in-house security staff are overwhelmed by number of security tools/layers to manage

[1] Enterprise Management Associates study, Selecting a Managed Detection and Response Service: What Clients Think and Prospects Want, June 2020.

This doesn't meet customer desires for a holistic solution from one vendor. Throwing technology at the increasing number and sophistication of threats doesn't scale and isn't adequate to meet the security needs of organizations. As a result, security teams – regardless of size and maturity – are struggling with larger attack surfaces, disjointed point products, and security tools. There is also a lack of cybersecurity personnel that possess the skills, experience, and time to adequately investigate and respond to threats. The number of open cybersecurity positions far exceeds the available talent pool.

Why the Old Way of Doing MDR Does Not Solve the Problem

Threat actors remain aggressive, leaving many security operations teams overwhelmed with alerts and unable to pivot away from daily tactical firefighting to more strategic, proactive threat hunting. Organizations continue to respond by adding security tools to their technology stack, further enabling an uncoordinated approach to securing data and devices. Security staffs are overloaded, and there isn't help on the way as the industry continues to face a severe shortage of qualified cybersecurity professionals. Customers today seek a solution that will keep staff from being overwhelmed by the number of security tools to manage, while also allowing those resources to focus on proactive and strategic activities.

A New Approach to MDR

Merely providing security alerts is no longer adequate to meet today's security needs. Organizations are overwhelmed with the amount of noise their tools are generating, and are struggling with trying to figure out which alerts represent a valid security threat. There is no shortage of managed detection and response solutions, but determining the ones that can deliver the elements you need to stay ahead of adversaries is a challenge.

There are certain requirements a solution needs to meet the demands of today's MDR buyers. It starts with software. This new approach is built on software featuring analytics technology that drives not just speedy detection, but precise detection – which fuels precise response actions. Diversity of threat data and research are must haves, as detecting and evicting threats requires a vast amount of threat data and a deep understanding of how threats behave.

A critical element is proactive threat hunting. Collaboration and transparency between an MDR provider and a customer allow for not just sharing information, but building trust and a way to openly communicate. So too is the ability for an MDR provider to respond during critical events, with clear understanding of incident response capabilities and responsibilities included as part of the solution.

Required Capabilities Needed to Solve the Problem

5 Things Your MDR Solution Must Do

What comprises the right managed detection and response solution?
Here are 5 must haves:

Security analytics

Proactive threat hunting

Incident response

Access to security expertise and threat intelligence 24x7

Flexibility in integration with third-party technology

Questions to Ask a Vendor When Evaluating an MDR Solution

- What visibility do you have throughout your entire ecosystem?
- How many different security technologies do you have?
- How well do your security technologies work together?
- Can you correlate and aggregate information and have the confidence of getting a unified response?
- Does your staff have the time and expertise to consume and investigate the alerts you get today?
- Do you wonder if there are threats that you are missing?
- What is the impact if a member of your security staff leaves?
- How do you keep your threat intelligence current?
- Can you identify if there is an advanced adversary present?
- Can you perform proactive or continuous threat hunting?
- How do you engage incident response resources?
- How does the handoff from your security staff to incident response resources unfold?
- How quickly can your incident response provider begin work?
- Does your solution include NGAV capabilities?

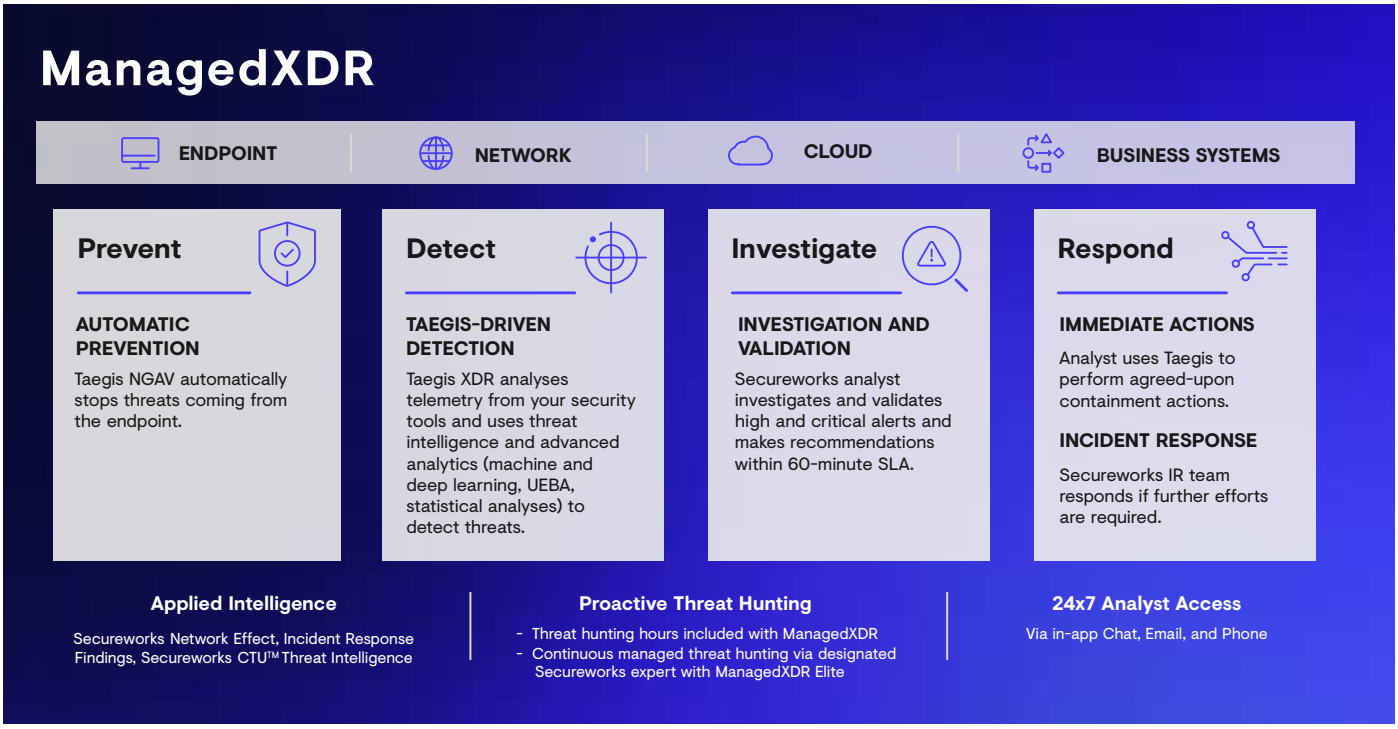
Why Secureworks?

Overview of Secureworks History

Secureworks has spent the past two decades providing industry-leading information security services, with a focus on managed security services, incident response, threat intelligence, and security consulting. Founded in 1999, our sole focus has been on cybersecurity. The Secureworks® Taegis™ platform – formerly known as Red Cloak™ – marks our shift to delivering software services, leveraging the years of threat findings and security expertise to combine human intellect with security analytics.

Introduction to Secureworks Taegis ManagedXDR

Taegis ManagedXDR is a managed detection and response service, with threat hunting and incident response capabilities delivered through our Taegis XDR security analytics application. Our Taegis software platform uses threat intelligence, machine and deep learning, and user behavioral analytics for rapid threat detection across customer endpoint, network, and cloud environments. While Secureworks fully manages the technology, ManagedXDR customers have full access to collaborate.



How Secureworks Solves the Problem

For organizations seeking to protect data and devices with improved investigation capabilities and accelerated ability to respond, ManagedXDR provides threat detection

and investigations, threat response actions, and 24x7x365 access to Secureworks security analysts. ManagedXDR proactively protects customer environments with around-the-clock monitoring across the entire ecosystem. Unlike traditional solutions, ManagedXDR combines our software that applies advanced analytics to detect and also respond quickly to threats. ManagedXDR includes proactive monthly threat hunting, with continuous threat hunting and bi-weekly meetings with a designated threat hunter via our premium ManagedXDR Elite. ManagedXDR is backed by our 20+ years of experience in protecting customers from security threats, the findings from more than 1,400 incident response engagements performed annually, and our Counter Threat Unit™ research team actively monitoring over 135 threat groups and updating 52,000 threat indicators daily.

Customer References

"I was kept awake at night wondering how we would address a security incident if it were to happen. We had a strong approach to security practices and the business's leadership team had confidence in us as a team, but we had no way of dealing with incidents in a timely manner. The partnership with Secureworks and the Taegis™ ManagedXDR service removes this concern."

Dr. Faisal Jaffri,
Global IT Director,
GKN Wheels & Structures

"For the current year, it saved us over half of what we were planning to spend on an in-house solution. It was pretty cut and dried."

Mike Rue,
Director of IT Infrastructure and Operations,
Firma FX

"We could tell that Secureworks was investing significant resources, and it was a priority for Secureworks. That was evident, and once we came on board, we saw that Secureworks continues to invest in its platform and continues to mature, and you're investing a lot of resources into it."

David Mohr,
Manager of Information Security,
PacificSource

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

About 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.

Next Steps

Explore the software that powers our ManagedXDR solution. Register for a free 14-day trial to take our Taegis XDR product for a test drive.

Check out Forrester Consulting's Total Economic Impact™ study of ManagedXDR.

In the Forrester Wave™: Managed Detection and Response, Q1 2021, Secureworks is cited as a Leader for its ManagedXDR solution in the MDR market. Read the full report.

Secureworks has been named a leader in the IDC MarketScape: U.S. Managed Detection and Response Services 2021 Assessment. Learn more.