Secureworks® | Taegis™ ManagedXDR

MDR BUYER'S GUIDE FOR MANUFACTURERS

Why More Manufacturers Are Turning to MDR

BUYER'S GUIDE INTRODUCTION

The Current State of Affairs

"Manufacturing is the most targeted industry for cyberattacks, making up 23.2% of all attacks."

Gartner Product Leaders Insight, March 2022

Managed detection and response (MDR) solutions remain very popular, and with good reason, considering the ongoing activity by cyber threat actors. The attack surface is growing as the manufacturing perimeter expands to include devices within the four walls of a facility along with interconnections to third parties in the supply chain. The global shortage of cybersecurity personnel is estimated at 3.5 million[1], a huge challenge for manufacturers looking to hire resources with cybersecurity skills and experience. More manufacturers are looking for ways to reduce their risk profile and stay protected from threats and vulnerabilities, while protecting their existing IT and OT technology investments.

[1] Boardroom Cybersecurity 2022 Report, Cybersecurity Ventures

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.

Why Old Approaches to MDR Do Not Solve Manufacturers' Risk Challenges

Threat actors remain aggressive, and organizations need a solution that goes beyond alerting to include response and remediation. Cyberattacks against industrial control systems (ICS) have increased in frequency and intensity as threat actors use evasive and persistent tactics to avoid detection in gaining access to systems. Companies invest in MDR solutions to get security expertise from an outside partner, but the old ways of MDR do not solve several major problems. Traditional MDR solutions often focus on endpoint telemetry and do not provide the holistic visibility many organizations need, especially considering customers continue adding security tools to their technology stack, resulting in a landscape of disparate tools that don't work together and result in a disjointed security approach. Security operations teams find themselves struggling with alert fatigue, figuring out which alerts represent a valid security threat, and lacking the time for innovation and strategic initiatives due to daily tactical firefighting. Plus, many existing MDR solutions focus pricing on usage that often leads to surprising upcharges.

A New, Holistic Approach to MDR

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 an MDR solution needs in order to meet the demands of today's manufacturing buyers. It starts with a platform that offers 24/7 monitoring while ingesting data across both IT and OT environments through 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.

5 "Must Haves" for Your MDR Solution

Security analytics Application of threat research-informed data science for threat prevention, detection and response

Proactive threat hunting Proactively isolate any threats that manage to evade existing controls

Incident response Diversity of attacker data gained from IR engagement findings

Access to security expertise and threat intelligence 24x7 Around-the-clock access to expertise and threat intelligence findings

Flexibility in integration with third-party technology Vendor-agnostic approach avoids locking into specific technology vendors

Questions to Ask a Vendor When Evaluating an MDR Solution

- What visibility would your solution provide across my IT and OT environments?
- How would your solution integrate my different endpoint, network, cloud, identity and other technologies into your solution?
- What integration capabilities does your solution have so I can continue leveraging my current security investments?
- Do you correlate and aggregate data into a central console for a unified view?
- How does your solution prioritize alerts and help my staff focus on the most critical?
- How does your solution uncover manual cybercriminal activity that tries to avoid detection?
- How would your solution help me fill my skills and talent gaps?
- What threat intelligence is included as part of your solution?
- How does your solution identify advanced adversary behavior?
- How does your solution provide proactive threat hunting across my environment?
- What incident response capabilities are included as part of your solution?
- How would my staff engage you for incident response support?
- How quickly can you engage your incident response provider in the event of a breach?
- Does your solution offer native prevention capabilities, such as anti-virus?
- How much do you charge to provide access to security experts through your platform?

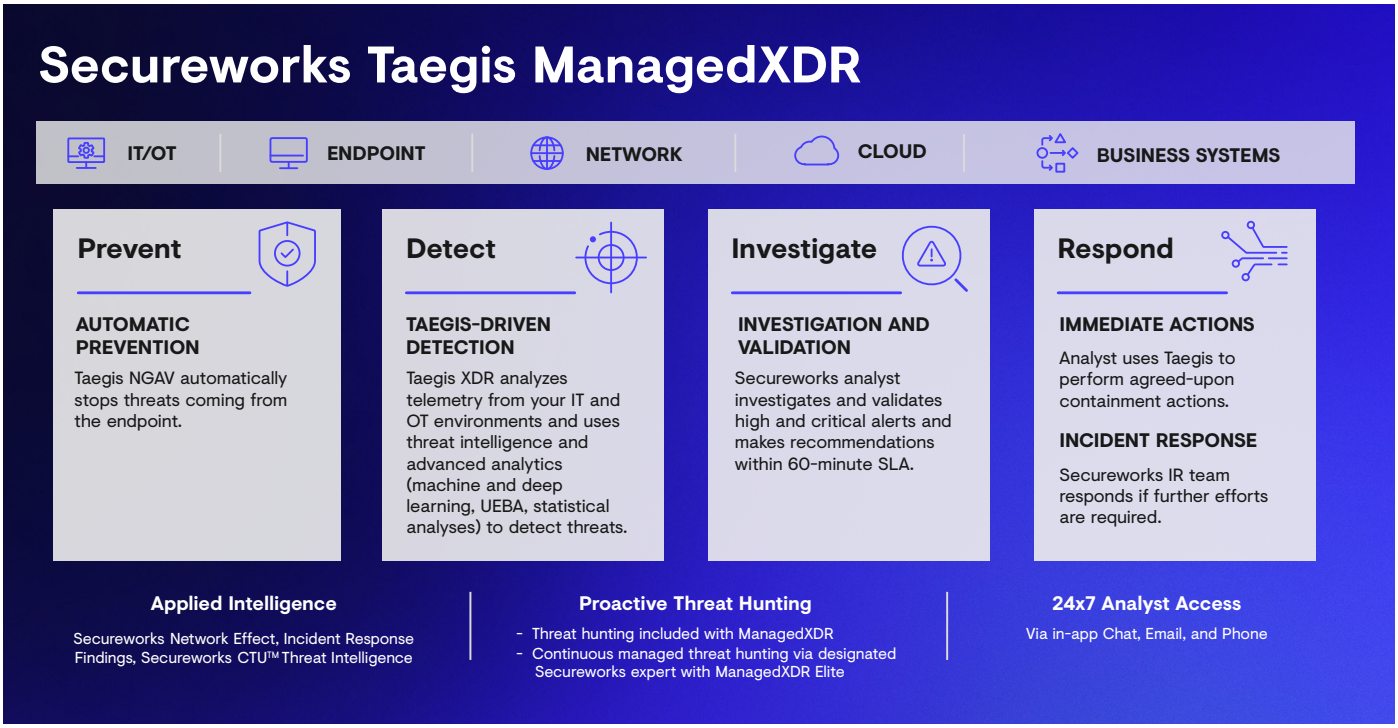
Why MDR from Secureworks?

Introducing Secureworks MDR: Taegis™ ManagedXDR

Secureworks Taegis ManagedXDR is our managed detection and response solution. ManagedXDR is built on the Taegis cloud-native security platform that continuously gathers and interprets telemetry from proprietary and third-party sources, including endpoints, networks, cloud, OT, IT, identity systems, and other business systems. We use this telemetry to detect and prevent threats, automatically prioritizing the most serious ones, enabling faster, more confident responses with time- and cost-saving automation.

Through real world active incidents, adversarial testing, and ongoing threat research, we study, learn, and analyze our adversaries' behaviors. With these insights, our security experts and data scientists proactively create detectors, identify patterns, and share intelligence about new threats and vulnerabilities. These insights, coupled with advanced technologies, form the basis of Taegis. While Secureworks fully manages the technology, ManagedXDR customers have full access to collaborate.

Secureworks protects organizations by providing battle-tested, best-in-class cybersecurity solutions that reduce risk, optimize IT and OT security investments, and fill your talent gaps. ManagedXDR combines our software that applies advanced analytics to detect threats with more than 20 years of experience in security operations, threat research and incident response.



Introducing Secureworks Taegis ManagedXDR for OT

For organizations seeking to protect their systems and data, Secureworks Taegis ManagedXDR for OT provides threat monitoring, detection, investigation, and collaborative response for IT and OT environments. Based on our managed detection and response solution, Taegis Managed XDR for OT provides customers with 24/7 rapid access to security experts within 90 seconds, integration with customer OT toolsets (Dragos, SCADAfence, Claroty), and collaborative build out of IT and OT escalation processes, plus playbooks and reporting. The solution also includes quarterly security reviews, monthly threat hunting, onboarding support, and access to proactive services to raise cyber resiliency. Taegis ManagedXDR for OT is backed by our 20+ years of experience in protecting customers from security threats, findings from more than 3,000 incident response and adversarial testing engagements performed annually, and our Counter Threat Unit™ research team actively monitoring hundreds of threat groups and managing more than 700,000 unique threat indicators.

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, moveero

"Breaches have a far-reaching cost impact. If systems go down, you can see it in the billing. Billing drops off but expenses just keep going. Our leadership team sees the value we are getting by keeping the business going, staying protected against things like ransomware."

IT Risk & Compliance Manager, Global Aviation Manufacturer

"We liked the Taegis value proposition: very extensive visibility and integration throughout our environment, with the fastest return on investment. Secureworks Taegis is a perfect match for our IT environment and business operations."

Hoong Jon Lee, Group IT Security Program Manager, Jotun

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

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

In the Forrester Wave™: Managed Detection and Response, Q2 2023, Secureworks is cited as a Strong Performer for its Taegis 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.

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