Secureworks
a SOPHOS company

Why Managed Detection and Response (MDR) is Critical for Keeping Government Agencies Secure

The Current State of Affairs

> **Malware attacks increased by 148%, while ransomware incidents were 51% more prominent during the first eight months of 2023 than they were during the same period a year earlier for cyber attacks affecting U.S. State, Local, Tribal, and Territorial government organizations.**
>
> *The Center for Internet Security, Inc. (CIS) and Multi-State Information Sharing & Analysis Center (MS-ISAC), Nationwide Cybersecurity Review (January 2024)*

Government agencies are a prime target for cyber criminals. The attack surface is growing as the attack perimeter expands to include devices within the four walls of a facility along with the interconnections with approved third-party vendors. Government agencies hold the keys to critical infrastructure, election security, personal data of citizens, sensitive information, and many essential services.

Cyber attackers may be looking for financial gain, personal data theft, or intellectual property theft from sensitive research projects funded by government organizations or private enterprise to conduct espionage. Government agencies are fertile grounds for ransomware, malware, and social engineering attacks.

Many state and local government agencies operate legacy systems that may not be adequately protected against modern cyber threats. Shrinking budgets and the ongoing cybersecurity skills shortage have made matters worse. The global shortage of cybersecurity personnel is estimated at 3.5 million[1], a huge challenge for government agencies as well as the private sector looking to hire resources with cybersecurity skills and experience.

The global shortage of cybersecurity personnel is estimated at

3.5 million[1]

More government agencies are looking for ways to reduce their risk profile and stay protected from threats and vulnerabilities, while protecting their existing technology investments as well as their constituents.

Throwing technology at the increasing number and sophistication of threats doesn't scale and isn't adequate to meet the security needs of organizations especially government agencies that may have set budgets. As a result, security teams — regardless of size and maturity — are struggling with larger attack surfaces, disjointed point products and security tools.

Early detection is the key to safeguarding an institution's data assets — because the sooner a threat is discovered and eliminated, the lower the likelihood that a small breach of the perimeter will result in a more significant security incident.

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 to meet the demands of today's government agency buyers. It starts with software. This new approach is built on software featuring analytics technology and AI that drives not just speedy detection, but precise detection — which fuels precise response actions. Diversity

1 Boardroom Cybersecurity 2023 Report, Cybersecurity Ventures

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 security analyst 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.

Additionally, MDR gives government agencies more flexibility to scale up and down as necessary as they grow, downsize and/or merge with other departments. The key decision facing leaders charged with maintaining the digital safety and reputation of their institutions isn't whether to adopt MDR; it is which MDR provider makes the most sense for their immediate and long-term requirements.

Questions to Ask a Vendor When Evaluating an MDR Solution

- What experience do you have working across other government agencies?
- 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?
- How does your solution use AI?
- 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?

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

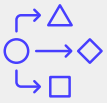
Proactively isolate any threats that manage to evade existing controls

Incident response

Diversity of attacker data gained from IR government engagement findings

Access to security expertise and threat intelligence 24/7

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

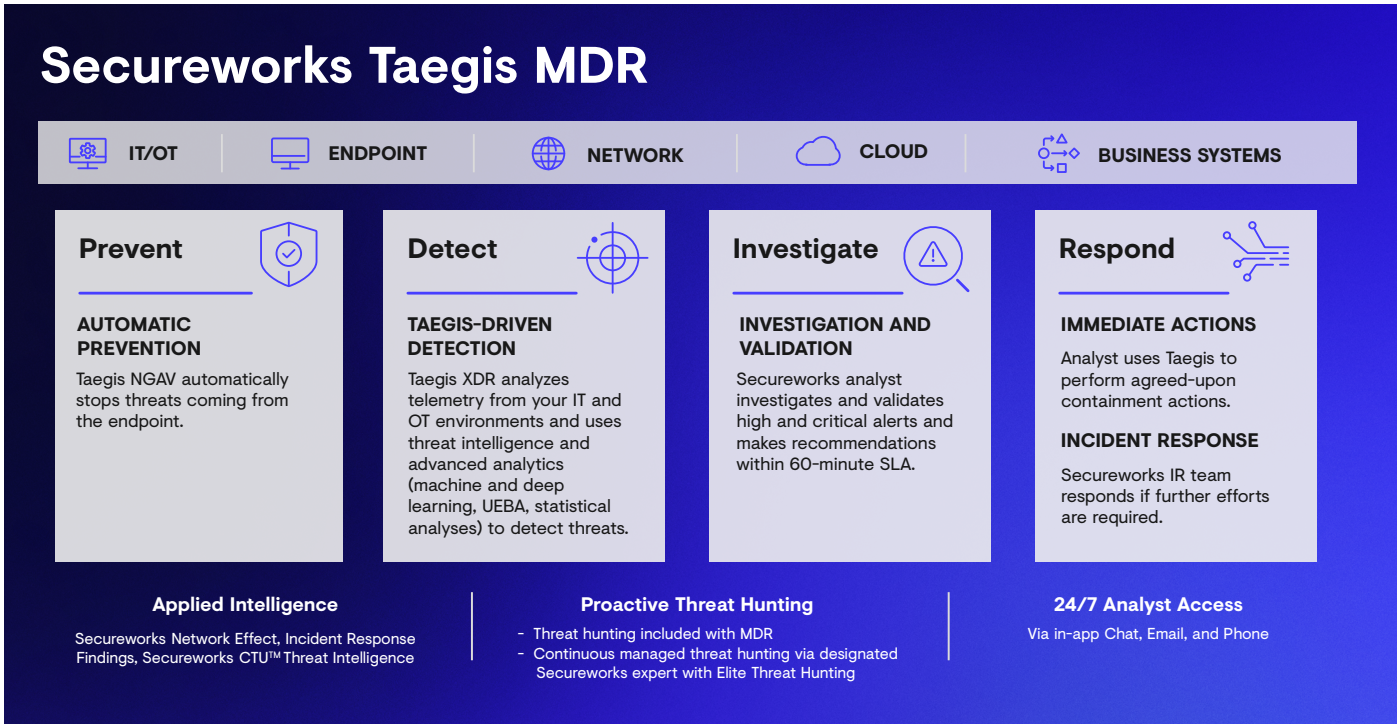
Why Secureworks?

Introduction to Taegis™ MDR

The Secureworks MDR solution, Taegis MDR, is a fully managed cybersecurity solution that combines an open, powerful platform with extensive security expertise for 24/7 protection. Taegis MDR is built on our SaaS-based, open XDR platform, that continuously gathers and interprets telemetry from proprietary and third-party sources, including endpoints, networks, cloud, identity 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, Taegis MDR customers have full access to collaborate.

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



How Secureworks Solves the Problem

For organizations seeking to protect data and devices with improved investigation capabilities and accelerated ability to respond, Taegis MDR provides threat detection and investigations, threat response actions, and 24/7/365 access to Secureworks security analysts. Taegis MDR proactively protects customer environments with around-the-clock monitoring across the entire ecosystem. Unlike traditional solutions that focus only on notifications, Taegis MDR combines advanced analytics to detect and respond quickly to threats. For organizations looking for a more tailored solution, Taegis MDR Plus provides hands-on assistance with creating automated customer use cases for alerts, security posture, and compliance needs, along with expanded threat hunting, premium Taegis platform support, and credits to use for Taegis Professional Services to evolve your security program. Taegis MDR Enhanced is our premium tier of MDR that includes higher-touch threat investigation and response, premium governance and advisory sessions, and a designated SOC. While levels of Taegis MDR include proactive threat hunting, Elite Threat Hunting is an option for customers who desire continuous threat hunting and bi-weekly meetings with a designated threat hunter. Taegis MDR for OT provides customers with access to OT security experts, integration with customer OT toolsets, and collaborative build out of IT and OT escalation processes, plus playbooks and reporting. Taegis MDR is backed by our 20+ years of experience in protecting customers from security threats, access to security experts within 90 seconds, findings from thousands of incident response and adversarial testing engagements performed annually, and our Counter Threat Unit™ research team actively monitoring hundreds of threat groups and actively managing more than 2 million unique threat indicators daily.

Secureworks is Level 1 and Level 2 accredited by the National Cyber Security Centre (NCSC) for delivering Incident Response services, is CREST accredited, and a member of the Offensive Security customer advisory board. Additionally, Secureworks is compliant with Service Organization Control 2 standards (SOC 2 Type II) and ISO 27001 certified.

CUSTOMER REFERENCES

> *I wanted to have assistance as we went through the incident. Speed was important, and it also was a great chance for a young team to watch an experienced team of security experts go through incident response. We could not get this wrong. This had to be done right.*
>
> **City of Amarillo**

> *Working with Secureworks leveraging their XDR platform and expertise through their managed XDR offering has been a phenomenal experience. The value we receive from Secureworks Taegis is high.*
>
> **The Town of Gilbert**

> *The expertise of the folks doing the work, the ones up at night, doing the analysis and detecting and preventing is reassuring to us. We didn't want a team of network engineers. We wanted to partner with a team of experienced, dedicated cybersecurity experts.*
>
> **U.S. County**

Next Steps

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

In the Forrester Wave: MDR Services in Europe, Q4 2023, Secureworks dominates as a leader Forrester says. Read the full report.

Secureworks earns Frost & Sullivan XDR Best Practices Award. Read the full report.

TRY US TODAY

Secureworks®
a SOPHOS company

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.

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