Secureworks
a SOPHOS company

Why Managed Detection and Response (MDR) is Critical for Institutional Safety

The Current State of Affairs

> **By 2025, 60% of organizations will be actively using remote threat disruption and containment capabilities delivered directly by MDR providers, up from 30% today.**
>
> *Gartner Market Guide for Managed Detection and Response Services, February 2023*

> **The National Student Clearinghouse said nearly 900 colleges suffered a data breach during the mass hack of the file-sharing tool MOVEit.**
>
> *Higher Ed Dive, Sept 2023*

> **The education sector recorded a higher share of ransomware victims than any other in 2022.**
>
> *The State of Ransomware in Education 2023*

Higher education is a prime target for cybercriminals. Colleges and universities contain a treasure trove of valuable data that's readily marketable on the Dark Web including personally identifiable information (PII) of students, faculty and staff; financial records that include five-figure transactions; grant-funded research of interest to nation state actors.

Further, colleges and universities have large, fluid attack surfaces that are inherently difficult to defend. Students, faculty and campus guests are constantly bringing new devices onto the network—and those devices often lack sufficient endpoint protections. A high volume of remote access can also make institutions vulnerable as attackers can readily hide among distance learners since students are logging into systems from anywhere in the world.

Higher education institutions are fertile grounds for ransomware, malware and social engineering attacks.

Shrinking budgets and a cybersecurity skills shortage have made matters worse. The global shortage of cybersecurity personnel is estimated at 3.5 million[1], a huge challenge for higher education institutions looking to hire resources with cybersecurity skills and experience. More higher education institutions are looking for ways to reduce their risk profile and stay protected from threats and vulnerabilities, while protecting their existing technology investments.

The global shortage of cybersecurity personnel is estimated at

3.5 million[1]

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.

Early detection is the key to safeguarding an institution's data assets, as well as its students and staff—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.

1 Boardroom Cybersecurity 2023 Report, Cybersecurity Ventures

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

Threat actors remain aggressive, and organizations need a solution that goes beyond alerting. Solutions should also include response and remediation. Companies invest in MDR solutions to get security expertise from an outside partner, but the old ways of MDR do not solve today's major problems. Traditional MDR solutions often focus on endpoint telemetry and do not provide the holistic visibility many organizations need, especially considering that customers continue adding security tools to their technology stack, which results 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 higher education institution 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 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.

Additionally, MDR also gives institutions more flexibility to scale up and down as necessary as they grow, downsize and/or merge with other institutions. 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.

5 "MUST HAVES" FOR YOUR MDR SOLUTION

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

Security analytics

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

Proactive threat hunting

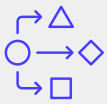
Proactively isolate any threats that manage to evade existing controls

Incident response

Diversity of attacker data gained from IR engagement findings

Access to security expertise and threat intelligence 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

Questions to Ask a Vendor When Evaluating an MDR Solution

- What visibility would your solution provide across my entire higher education ecosystem?
- 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?
- Can your agent be extended to BYO devices?
- 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?
- How much do you charge to provide access to security experts through your platform?
- How does your solution use AI?

Why Secureworks?

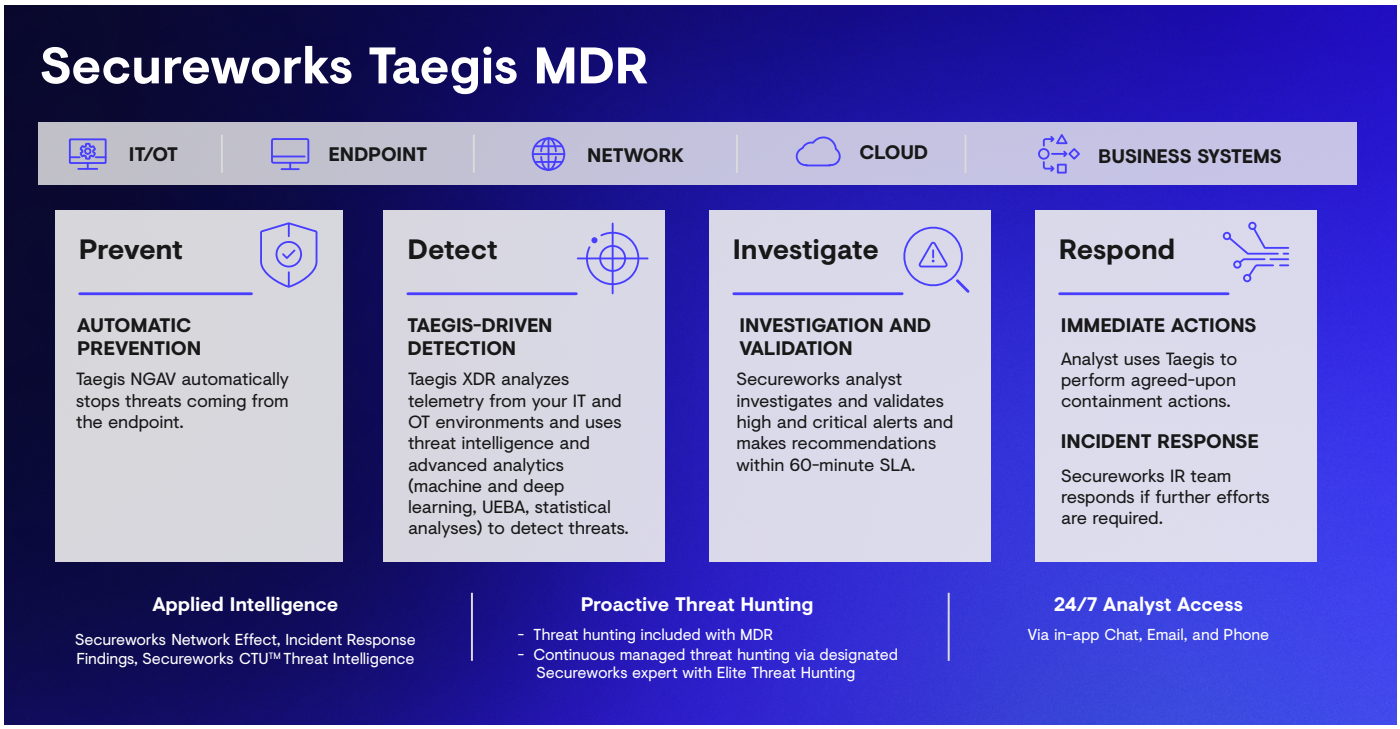
Introduction to Secureworks Taegis™ MDR

The Secureworks MDR solution, Taegis MDR, is our managed detection and response service. Taegis MDR is built on our SaaS-based, open XDR platform, that continuously gathers and interprets telemetry from proprietary and 3rd 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.

Next Steps

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

Secreworks name a Major Player in the 2024 IDC MDR MarketScape. Read the full Report.

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

TRY US TODAY

Secureworks
a SOPHOS company

Secureworks, a Sophos company, is a global cybersecurity leader that protects customer progress with TaegisTM, 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