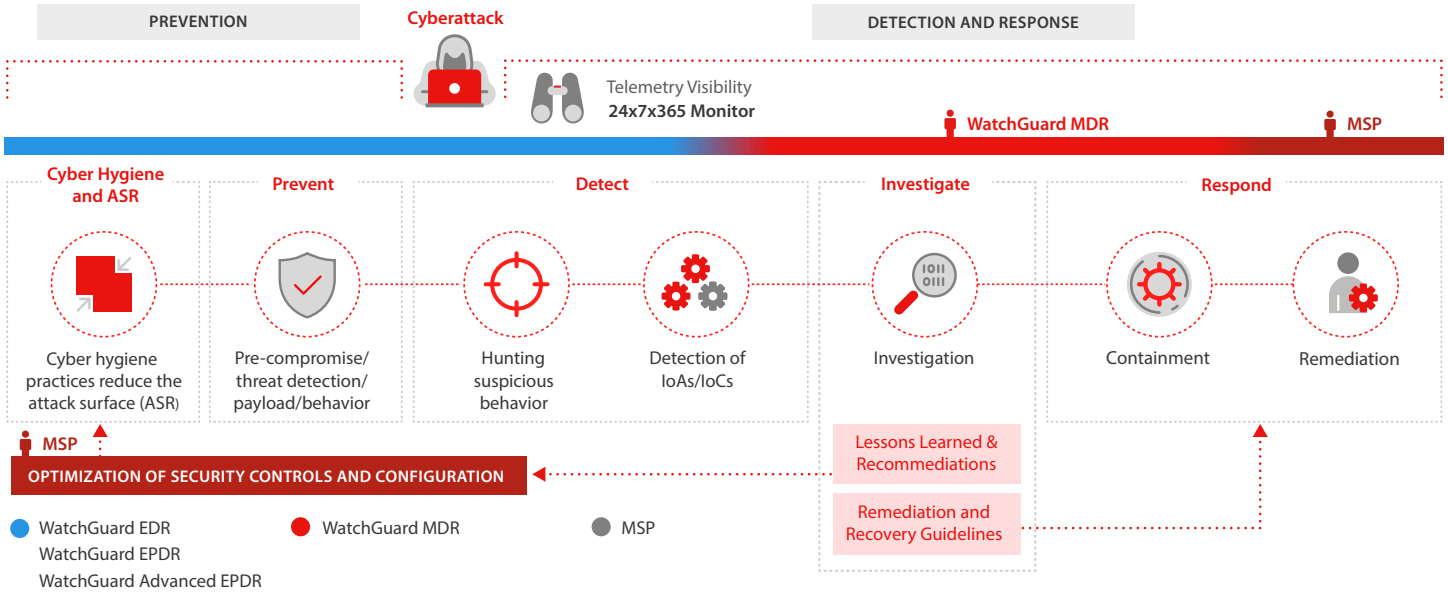
WatchGuard MDR for MSPs

24/7 Detection and Response Without the Overhead.

As the cyber threat landscape continues to expand and grow in sophistication, companies struggle with serious security risks, inefficient cybersecurity posture management, and a scarcity of skilled personnel. So, companies are looking to outsource their protection to managed service providers (MSPs) with the technology, staff, and expertise to address these challenges.

However, managing complex security challenges and the expanding threat surface most companies face today requires skilled people and a lot of investment, making it difficult for MSPs to offer managed detection and response (MDR) services in an effective, economical manner. That's why WatchGuard introduced WatchGuard MDR, a managed service that helps security service providers overcome these problems. By leveraging our thorough detection and response service in their offering, MSPs can meet customers' needs without the overhead of building and maintaining their own 24/7, in-house security operations center (SOC).

WatchGuard MDR provides 24/7/365 cybersecurity services to our partners and their customers, offering endpoint security monitoring, threat hunting, and attack detection, investigation, and containment, with guided recommendations for remediation. The offering is managed by an elite team of cybersecurity experts and powered by AI. It requires no investment in a traditional SOC infrastructure, advanced technologies, or scarce security experts, which addresses the global pressures of scarce cybersecurity professionals and funding.



How It works

WatchGuard MDR provides 24/7 monitoring of the threat activity registered at endpoints, enabling correlation of suspicious activities to detect, investigate, and respond to cyber threats promptly and effectively. Here's how the service works:

Service Onboarding:

The onboarding process initiates immediately upon MDR service activation in the subscriber's account. WatchGuard SOC analysts collaborate to define response types & ensure optimal service. We'll confirm WatchGuard EDR, EPDR, and Advanced EPDR setup and work together to validate the functionality of your security controls, ensuring containment and response readiness.

24/7 Endpoint Activity Monitoring and Data Collection:

WatchGuard MDR leverages endpoint data collected from WatchGuard host sensors and then stored for 365 days in our Cloud SOC. Processed in real time and retrospectively via machine learning and advanced analytics, our threat hunters explore new patterns to enhance cybersecurity.

24/7 Proactive Hunting and Detection:

We use machine learning to analyze this data and detect suspicious activities and anomalies that could indicate the presence of a threat. We map all indicators of attack(IoAs) to the MITRE ATT&CK framework to quickly understand the threat actors. Our MDR personnel proactively seek endpoint threats, reducing detection time and enhancing security efficacy.

24/7 Investigation and Validation:

Investigation and validation are key elements within our MDR service. Aided by machine-learning algorithms trained on real cyber incidents, our experts correlate IoAs into incidents, investigating and validating them to swiftly address potential threats and minimize impact.

Immediate Incident Notification to Partner Teams:

Upon confirmation of a security incident, WatchGuard MDR promptly notifies our MSP partners with post-incident validation, sparing them the task of reviewing unconfirmed cases. Notifications detail investigative insights and impacted machines, empowering fast, informed response actions by partner teams, thus mitigating threats and minimizing potential damages or data loss efficiently.

Mitigation and Remediation Guidelines:

When security incidents arise, the WatchGuard MDR team collaborates closely with MSPs to provide clear, actionable guidance for incident response and damage mitigation. This includes detailed recommendations for containment actions, remediation, and future security posture enhancement. Our guidelines aid partners in quickly and effectively responding to threats, minimizing incident impact, and enhancing clients' overall security posture to prevent similar incidents from happening again.

24/7 Response and Mitigation Executed by WatchGuard or the Partner's Team:

Our MDR experts create custom automated playbooks to mitigate and contain validated threats, including those that involve potential endpoint isolation. If partners opt for their own teams to lead containment efforts, the WatchGuard MDR team provides guided support.

Response and Remediation Executed by the Partner's Team:

Led by partners with WatchGuard guidance, the post-incident containment or remediation phase addresses attacker traces, data restoration, and vulnerability patches. It may also involve enhancing existing security setups or implementing new security controls to forestall similar incidents going forward.

Weekly and Monthly Reporting:

WatchGuard MDR experts deliver weekly and monthly security reports to partners, covering detected IoAs, investigations, identified incidents, and a security health analysis to anticipate potential threats. Partners can customize reports to enhance customer engagement with their MDR service.

Benefits for our partners	
Features	**MSP Benefits**
24/7 monitoring. data collection at WatchGuard SOC in the Cloud	Capitalize on the MDR opportunity without investing in a modern SOC.
24/7 detection, hunting, and investigation by WatchGuard's experts	Augment your team with cybersecurity-skilled staff to provide 24/7 MDR.
24/7 unattended threat containment	Entrust us with round-the-clock containment of uncovered threats.
Immediate notification to the MSP team	Take the lead in your customer relationships while we ensure you're always informed.
Mitigation and remediation guidelines	Access security knowledge and best practices that provide a competitive edge.
Service onboarding and periodic health checks	Prevent attacks from improper security or unmanaged endpoints.
Weekly wellness status and monthly activity reporting	Enhance customer security by staying ahead of threats exploiting vulnerabilities.

MDR Model and Use Cases

1. MDR from an In-House Security Operations Center (SOC):

An in-house SOC is a dedicated facility and team within an MSP responsible for managing and responding to cybersecurity issues in their customers' environment.

- **Control:** Full control over all processes, tools, and data.
- **Cost:** High – involves investing in technology and skilled staff.
- **Scalability:** Scaling requires additional investments in staff and technology.
- **Management:** Entire management and operations are handled internally.

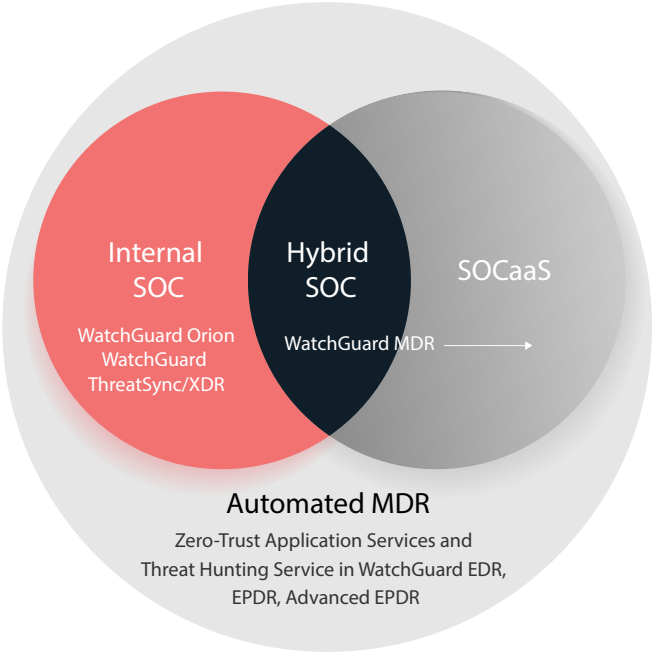
★ **Use Case:** Best for large organizations with substantial cyber-security budgets and high-security requirements.

2. MDR from a SOC as a Service (SOCaaS):

SOCaaS is a service that provides outsourced cybersecurity monitoring, detection, investigation, and response from a third-party MDR.

- **Control:** Limited control as processes are handled by the MDR provider.
- **Cost:** Lower – operational expense rather than a capital investment.
- **Scalability:** Can be scalable, depending on the chosen service.
- **Management**: Managed by third-party cybersecurity professionals.

★ Use Case: Suitable for small and midsize businesses or organizations with limited cybersecurity budgets and staff.



3. MDR from a Hybrid SOC:

A hybrid SOC model combines in-house and outsourced SOC functionalities to balance internal and external cybersecurity capabilities.

- **Control:** Moderate control – internally managed but leverages external resources.
- **Cost:** Can be optimized according to the balance of in-house and outsourced functions.
- **Scalability:** Higher – internal efforts can be augmented with external capabilities.
- **Management:** Involves both internal management and third-party management.

★ Use Case: Ideal for organizations seeking to augment their existing SOC capabilities without substantial investments.

4. Automated MDR (Services)

In an automated MDR context, technology plays a pivotal role in bolstering cybersecurity defense by streamlining and often automatically handling various functions to enhance efficacy and responsiveness.

- **Control:** Detection and response activities are automated. Enables IT teams to focus on strategic, complex, or escalated concerns.
- **Cost:** No additional expenses are necessary, as all technologies, including AI in the Cloud, skilled personnel, tools, and threat intelligence, are included in the product cost.
- **Scalability:** Facilitates easy adaptation to the evolving scale and complexity of organizational environments.
- **Management:** Offers a systematic approach to threat detection and response, minimizing the management effort.

★ Use Case: Automated MDR services are key for businesses with limited cybersecurity staff/budget, providing robust, affordable defense.

Making the cases for WatchGuard MDR

WatchGuard helps MSPs build their own in-house SOCs while maintaining high efficiency in their cybersecurity teams with solutions like Advanced EPDR, WatchGuard Orion, and WatchGuard ThreatSync for XDR. We enable automated MDR with the Zero-Trust Application Service and the Threat Hunting Service in WatchGuard EDR, EPDR, and Advanced EPDR.

With the introduction of WatchGuard MDR, our MSP partners can now deliver managed detection and response services to address ongoing business challenges related to cybersecurity skills and funding gaps.

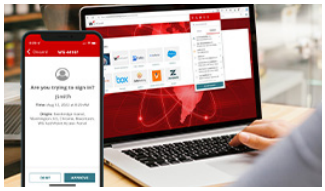
More than Detection and Response: MDR Providers Are Long-Term, Strategic Operating Partners

MDR Is Becoming a Mainstream Security Strategy

The WatchGuard Portfolio

Network Security

WatchGuard offers a wide range of network security solutions, including everything from tabletop and 1U rack-mounted appliances to Cloud and virtual firewalls. Our Firebox® appliances deliver critical security services, from standard IPS, URL filtering, gateway AV, application control, and antispam, to advanced protections such as file sandboxing, DNS filtering, and more. High-performance deep packet inspection (DPI) means you can leverage all our security services against attacks attempting to hide in encrypted channels like HTTPS. Additionally, every Firebox offers SD-WAN right out of the box for improved network resiliency and performance.



Identity Security

WatchGuard AuthPoint® is the right solution to address the password-driven security gap with multi-factor authentication on an easy-to-use Cloud platform. WatchGuard's unique approach adds the "mobile phone DNA" as an identifying factor to ensure that only the correct individual is granted access to sensitive networks and Cloud applications. AuthPoint also delivers an optimized user experience with online and offline authentication methods, along with a web application portal for easy single sign-on access.

Secure Cloud Wi-Fi

WatchGuard's secure, Cloud-managed Wi-Fi solutions provide safe, protected airspace for Wi-Fi environments while eliminating administrative headaches and greatly reducing costs. From home offices to expansive corporate campuses, WatchGuard offers Wi-Fi 6 technology with secure WPA3 encryption. With WatchGuard Cloud, Wi-Fi network configuration and policy administration, zero-touch deployment, customized captive portals, VPN configuration, expansive engagement tools, visibility into business analytics, and upgrades are only a click away.

Endpoint Security

WatchGuard Endpoint Security solutions help you safeguard devices against cyber threats. WatchGuard EPDR and Advanced EPDR, our AI-powered flagship endpoint solutions, enhance your security posture by seamlessly integrating endpoint protection (EPP) with detection and response (EDR) capabilities alongside our Zero-Trust Application and Threat Hunting Services. All are tightly integrated within WatchGuard Cloud and ThreatSync, delivering valuable visibility and intelligence while fortifying cross-product detection and response (XDR).

About WatchGuard

WatchGuard® Technologies, Inc. is a global leader in unified cybersecurity. Our Unified Security Platform® approach is uniquely designed for managed service providers to deliver world-class security that increases their business scale and velocity while also improving operational efficiency. Trusted by more than 17,000 security resellers and service providers to protect more than 250,000 customers, the company's award-winning products and services span network security and intelligence, advanced endpoint protection, multi-factor authentication, and secure Wi-Fi. Together, they offer five critical elements of a security platform: comprehensive security, shared knowledge, clarity & control, operational alignment, and automation. The company is headquartered in Seattle, Washington, with offices throughout North America, Europe, Asia Pacific, and Latin America. To learn more, visit **WatchGuard.com**.