

# WatchGuard MDR

Empowering our partners with WatchGuard SOC Expertise

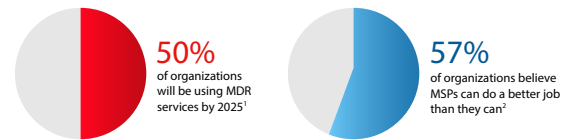


## Harnessing the MDR potential

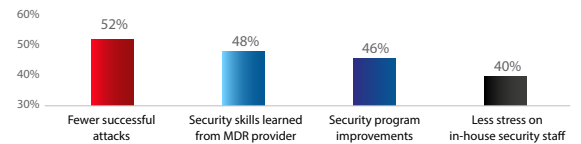
As the threat landscape evolves, businesses struggle with complex security challenges and the scarcity of cybersecurity professionals. Limited resources and time further hinder effective cybersecurity management. Businesses are turning to managed security providers (MSPs) for outsourced cybersecurity operations to address these issues.

However, security operations centers (SOCs) require skilled staff and significant investments, posing challenges for MSPs to offer managed detection and response (MDR). WatchGuard introduces WatchGuard MDR, empowering partners to overcome these obstacles. By including our comprehensive detection and response service in their portfolio, partners can meet customers' demands without building their own SOC, bridging the cybersecurity skills and funding gaps.

### Increased demand for MDR



### Midmarket organizations report benefits from MDR<sup>2</sup>



## Team up with our cyber experts for top-notch MDR

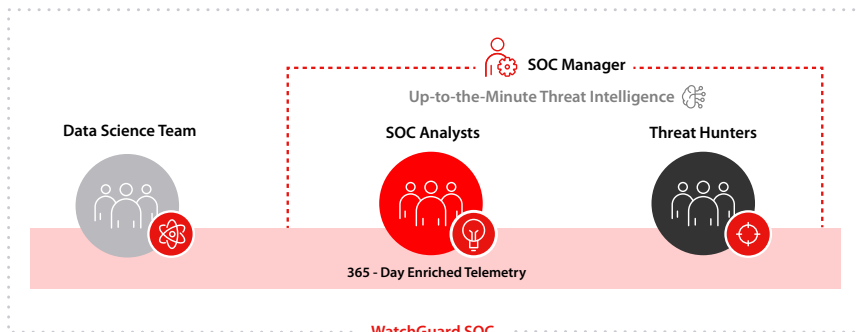
A WatchGuard skilled team of cybersecurity experts keeps your customers' endpoints safe with 24/7 security monitoring, threat hunting, attack prevention, detection, and containment.

In case of a potential cyberattack, the team guides you through the containment and remediation process to stop and remediate threats immediately. For your convenience and to minimize the time to respond in case of an attack, you can also delegate the containment to us. We automatically detect and block the adversaries in their tracks for you to gain time to analyze and remediate the compromised attack.

Additionally, as part of onboarding the service, our team assesses the attack surface at the endpoints to strengthen their security posture, improving their overall resiliency to cyber threats immediately.

WatchGuard MDR supports you with automatically delivered periodic service activity and security health status reports that help you to provide preventive and attack surface reduction services.

Our team of experts from WatchGuard SOC transforms endpoint monitoring and 365-day telemetry into actionable security analytics, augmented by industry-leading, trusted security machine learning/AI, and up-to-the-minute threat intelligence operated around the clock.



## At-a-glance

Experience the power of proactive cybersecurity and gain peace of mind knowing that skilled security experts protect your customers. WatchGuard MDR provides:

- 100% MDR for partners – 100% of the time
- Service onboarding to minimize endpoint attack surface
- Continuous endpoint activity monitoring
- 365-day telemetry retention in the Cloud
- Around-the-clock proactive hunting, behavioral detection, and investigation
- Immediate incident notification to your preferred point of contact by email or phone
- Detailed attack reports leveraging MITRE ATT&CK framework
- Tailored playbooks for automated containment filtered by endpoints
- Mitigation and remediation guidelines
- Continuous attack surface assessment
- Weekly endpoint health status reports
- Monthly risk status, monitored activity, detections, and responses reports

<sup>1</sup>Gartner. Market Guide for Managed Detection and Response Services. 25 October 2021. <sup>2</sup>What security teams want from MDR providers ESG, May 2023

## Benefits

With WatchGuard's MDR, our MSPs can seamlessly deliver top-tier cybersecurity capabilities without the burden of building and managing their modern SOC. We empower their business and leverage our expertise to provide their customers with comprehensive threat hunting, detection, and response, significantly reducing the risk of cyberattacks and safeguarding their valuable assets.

Stay ahead of the curve and capitalize on the MDR revolution with WatchGuard's MDR. Transform your security operations and drive unparalleled customer value, ensuring a resilient defense against today's ever-evolving cyber threats.

### MSP Benefits WatchGuard MDR

- Keep competitive by expanding your managed service portfolio
- No investment is required. Get access to a modern SOC without building yours
- Extend your team with skilled cyber experts
- Rest peacefully night and day. We have you covered around the clock
- Provide 24/7 hunting, threat detection and response to sophisticated threats
- Tailor the response with flexible containment rules
- Consolidate your customers' security stack, including managed services

### Customer Benefits MDR from Their MSP

- Proactive approach to stop threats in real time
- 24/7 monitoring, detection, and response to minimize breach time to respond
- Knowledge and expertise of skilled cybersecurity professionals
- Scalability for changing threat landscapes
- Flexibility in deployment options and business growth
- Threat and attack surface visibility enabling security improvements
- Meeting compliance and regulatory requirements

## The power of efficient prevention, hunting, detection, and response

Prioritizing the combination of prevention and attack surface reduction and proactive detection and response is crucial for enhancing your customers' cybersecurity posture. These security strategies are all interconnected. Prevention efforts aim to minimize incidents and associated costs, while detection and response address threats that slip through preventive measures, minimizing the time to detect and respond to them to reduce the overall security cost.

WatchGuard MDR maximizes automated threat prevention, detection, and response by utilizing WatchGuard EDR, EPDR, or Advanced EPDR and its managed services. The Zero-Trust Application Service autonomously minimizes the malware attack surface, enhancing security posture and

enabling scalable detection and response. Skilled cybersecurity analysts leverage the Threat Hunting Service to investigate IoAs and weak signals, uncovering complex cyberattacks. The continuous Security Health checks in the service evaluate configuration and attack surface exposure. Our cybersecurity analysts provide guidelines to minimize endpoint attack surfaces, fortify security controls, fine-tune settings, and recommend timely patching.

By combining attack surface reduction, prevention, and effective detection and response strategies, WatchGuard EDR, EPDR, or Advanced EPDR and WatchGuard MDR empower MSPs with a robust cybersecurity framework.

