

# WatchGuard CORE 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 Core 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.

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

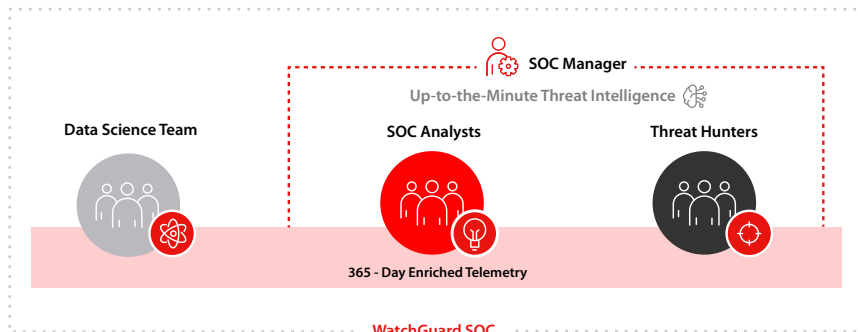
A skilled team of WatchGuard cybersecurity experts keeps your customers' endpoints and Microsoft 365 instances safe with 24/7 activity monitoring, threat hunting, detection, investigation, and optional, selective, and tailored containment for each customer.

In the event of a cyberattack, the team guides you through the response process to stop and remediate threats. For added convenience and to minimize response time, you can also delegate containment to the SOC by default – either 24/7 or during your after-business hours.

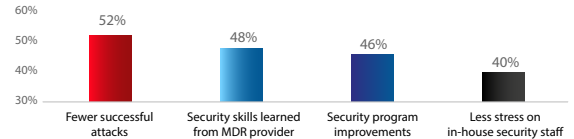
Additionally, as part of onboarding the service, our team assesses the attack surface at the endpoints to strengthen their security posture, improving their overall resiliency to cyber threats immediately.

WatchGuard Core 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.



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



### At-a-glance

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

- 100% MDR for partners – 100% of the time
- Service onboarding to minimize endpoint attack surface
- Continuous endpoint and Office 365 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
- Customized playbooks designed to fit operational needs, whether 24/7 or 8/5
- Client-defined automated containment rules, specific to each endpoint
- Mitigation and remediation guidelines
- Continuous attack surface assessment
- Weekly endpoint health status reports
- Recurring Office 365 defense goal reports

<sup>2</sup> What security teams want from MDR providers ESG, May 2023

## MSP Benefits

- Expand your managed security service portfolio with your branded MDR offering
- Access a modern SOC without building your own – no significant investment needed
- Extend your team with skilled cybersecurity experts
- Gain peace of mind with 24/7 monitoring, detection, and response for your customers
- Flexible always-on MDR service for both 24/7 or 8/5 operations - scale at your own pace
- Customize playbooks to fit each customer's needs
- Quick and easy deployment, especially with WatchGuard Advanced Endpoint Security

## Your Customer Benefits

- Proactively stop sophisticated threats with 24/7 monitoring
- Rely on skilled cybersecurity experts for detection, investigation, and swift response
- Scale your defenses as threats evolve and your business grows
- Gain full visibility into attack surfaces to strengthen security posture
- Reinforce compliance with proactive protection
- Enjoy cost-effective security without an internal SOC
- Trust your long-time provider to maintain your consolidation strategy without changing partners

## 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 Core 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 Core MDR empower MSPs with a robust cybersecurity framework.

