MDR

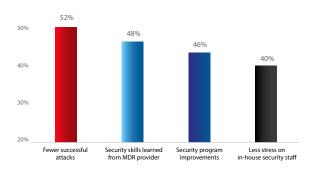Empower Your Defense with Round-the-Clock Protection Against Evolving Threats

Harnessing the MDR potential

SMBs face mounting cybersecurity challenges, from increasingly sophisticated attacks to a shortage of skilled personnel and rising regulatory and cyber insurance demands. Without adequate protection, they risk costly cyberattacks and potential fines for non-compliance. Small and midsize organizations experience substantial improvements in addressing these challenges with MDR.

Our MDR service, in partnership with WatchGuard MDR, offers customers a comprehensive, managed cybersecurity solution that combines 24/7 monitoring, detection, and incident response capabilities. With support from WatchGuard's SOC experts and our experience, this service protects organizations against sophisticated threats, helping to maintain business continuity and improve resilience against cyberattacks.

Midmarket organizations report benefits from MDR[1]

52%	48%	46%	40%
Fewer successful attacks	Security skills learned from MDR provider	Security program improvements	Less stress on in-house security staff

Key Service Features

24/7 Continuous Monitoring and Threat Detection
Our MDR service provides real-time monitoring of endpoints and Office 365 around the clock to detect advanced threats such as ransomware and living-off-the-land attacks. This constant vigilance allows for the swift identification of suspicious activities and proactive actions to protect customers.

Incident Investigation and Proactive Response
In the event of an incident, WatchGuard's MDR team conducts a thorough investigation to understand the nature of the threat and, if necessary, implements containment through isolation. Thanks to the guidelines provided by WatchGuard, our team can actively respond to incidents, knowing which assets were impacted, implementing remediation as quickly as possible, and ensuring a swift return to business as usual.

Security Posture Improvement and Cyber Hygiene Practices
Our MDR service goes beyond threat detection and remediations, incorporating proactive steps to improve customers' overall security posture. This includes implementing cyber hygiene practices, such as reducing endpoint exposure to risk through regular critical vulnerability assessments. By addressing high-risk vulnerabilities, customers build a more resilient defense against potential threats.
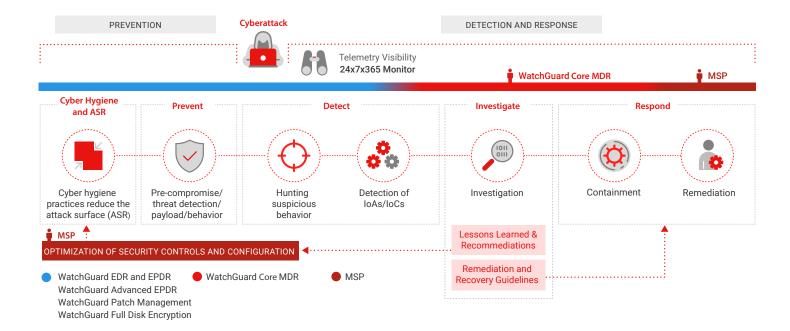
Compliance Support and Continuous Improvement
Adopting a proactive MDR helps customers stay compliant with security regulations (such as NIST, NIS 2, DORA and PCI DSS), implementing a fully end-to-end threat life cycle management and thorough reporting and guidance on cybersecurity best practices. This support includes regular assessments of security posture and recommendations to reduce vulnerabilities, ensuring customers keep pace with regulatory requirements.

Reporting and Security Plans
As part of the service, we provide detailed incident and security status reports for the customers' infrastructure. In addition, weekly and monthly security activity reports are provided, including an analysis of the current state and an action plan for ongoing security improvement.

A Managed Service Offering Security and Confidence
Thanks to the combination of WatchGuard's expertise and our personalized support, the managed detection and response service that we provide enables our customers not only to mitigate advanced threats but also to continually improve their security posture. With the reassurance of cybersecurity experts and advanced solutions, businesses can focus on growth, knowing they are protected against cyberattacks.

PREVENTION | Cyberattack | DETECTION AND RESPONSE

Telemetry Visibility
24x7x365 Monitor

WatchGuard Core MDR — **MSP**

Cyber Hygiene and ASR	Prevent	Detect		Investigate	Respond	
Cyber hygiene practices reduce the attack surface (ASR)	Pre-compromise/ threat detection/ payload/behavior	Hunting suspicious behavior	Detection of IoAs/IoCs	Investigation	Containment	Remediation

MSP

OPTIMIZATION OF SECURITY CONTROLS AND CONFIGURATION

Lessons Learned & Recommediations

Remediation and Recovery Guidelines

- WatchGuard EDR and EPDR
  WatchGuard Advanced EPDR
  WatchGuard Patch Management
  WatchGuard Full Disk Encryption
- WatchGuard Core MDR
- MSP

Your Benefits

Protection Against Sophisticated Threats

Our MDR service provides continuous monitoring and expert response to advanced attacks, such as ransomware, enabling rapid detection and mitigation to minimize business disruption.

Access to Cybersecurity Expertise

With the scarcity of cybersecurity professionals and increasingly complex threats, many businesses lack essential internal resources. Our MDR service grants access to a team of specialists, eliminating the need to build a SOC and ensuring reliable, expert support.

Regulatory Compliance Assistance

Cybersecurity regulations like NIST, NIS 2, and DORA are becoming stricter, with significant fines for non-compliance. This MDR service helps clients stay compliant, reducing the risk of penalties and enhancing trust with partners and customers.

Reduced Operational Costs

Cyberattacks can be financially devastating, especially for SMBs, with the average data breach costing $2.98 million. By outsourcing cybersecurity with MDR, clients gain cost-effective protection, avoiding large investments in personnel and technology.

Rapid Incident Response

A swift response is crucial to minimize the impact of cyberattacks. Our MDR offers immediate response times with automatic containment, ensuring incidents are managed quickly and customers are shielded from major consequences.

Access to Cyber Insurance

Cyber insurance providers increasingly require businesses to contract MDR services to enhance cyber resilience, offering significant premium discounts and added financial protection.

Peace of Mind and Security Confidence

With a team of experts monitoring threats and managing responses, your organization can focus on operations without worrying about cyber risks, benefiting from continuous support from your trusted security partner and WatchGuard's SOC – all without the need to manage multiple security providers.