

Your Partner Guide to Quickly Bringing MDR to Market

MDR FAST TRACK



Leverage WatchGuard MDR to Meet Rising Demand for Advanced Threat Detection and Response

This guide provides essential steps for partners to quickly bring a branded MDR offering to market, addressing client security needs and unlocking new revenue streams.

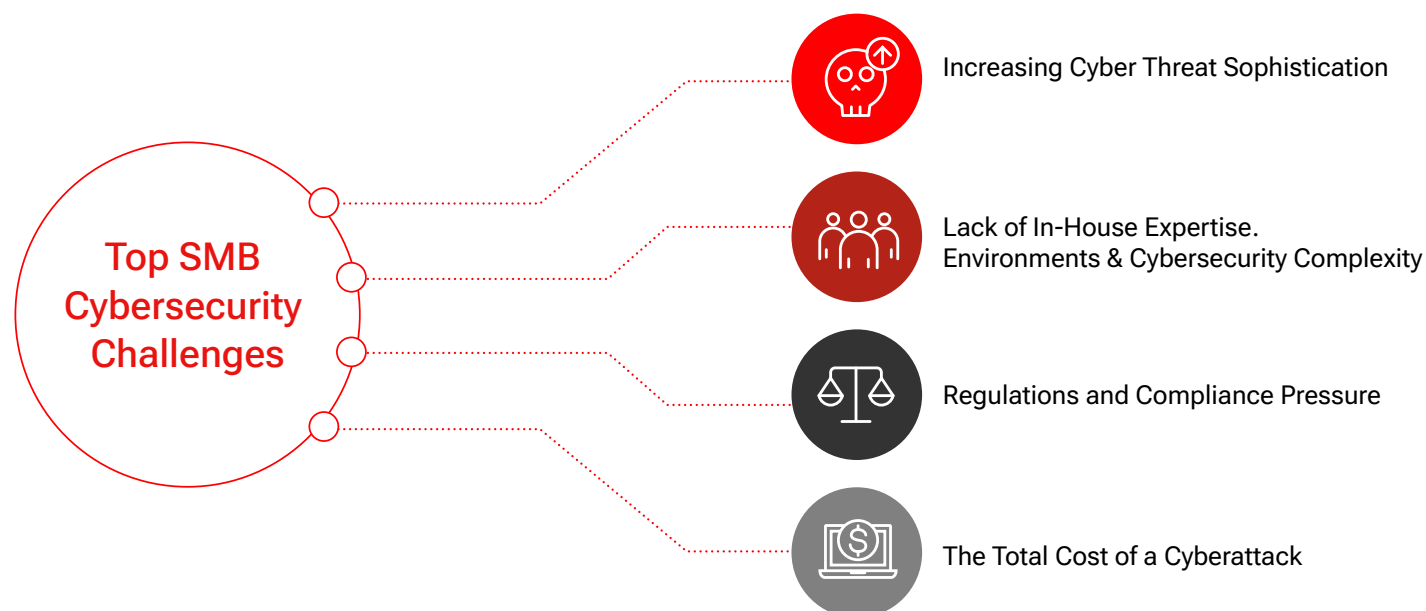
Table of Contents

Introduction	2
Key Cybersecurity Challenges Facing SMBs	2
Increasing Cyber Threat Sophistication	2
Lack of In-House Expertise and Cybersecurity Complexity.....	3
Regulatory and Compliance Pressures	3
The Financial Impact of Cyberattacks.....	3
MDR as the Solution to Address SMB Cybersecurity Challenges.....	4
Six Key Advantages of MDR.....	4
How Partners Can Sell MDR Services	4
Packaging MDR for Profitability	5
Handling Customer Objections to MDR	7
Introducing WatchGuard MDR.....	8
Conclusion	9

Introduction

In today's digital landscape, small and midsize businesses (SMBs) face increasing cybersecurity challenges. As cyber threats grow in sophistication, SMBs, which often lack the necessary security infrastructure, become prime targets. This white paper explores how partners can effectively position and sell Managed Detection and Response (MDR) services to customers. We will review key challenges SMBs face, how MDR can address these issues, and provide strategies for partners to present and package MDR services for profitability.

Key Cybersecurity Challenges Facing SMBs



Increasing Cyber Threat Sophistication

Cyber threats are becoming more advanced and harder to detect. Attacks like “Living off the Land” and ransomware are especially dangerous to SMBs, who often lack the sophisticated defenses of larger organizations.

Example: In late 2022, Russian cybercriminals launched an attack on Ukraine's power grid, demonstrating how cyber warfare can cause widespread disruption. This highlights how cyberattacks can target even critical infrastructure, emphasizing the need for robust security measures.

“For the past four years, the LockBit ransomware group has been on an unrelenting rampage, hacking into thousands of businesses, schools, medical facilities, and governments around the world — and making millions in the process. A children's hospital, Boeing, the UK's Royal Mail, and sandwich chain Subway have all been recent victims”.



“Microsoft and OpenAI say hackers are using ChatGPT to improve cyberattacks. A number of nation-backed groups are starting to use large language models to help with research, scripting, and phishing emails”.



“Russian cyber spies were behind a hack which disrupted part of Ukraine's power grid in late 2022 in a rare and advanced form of cyberwarfare, U.S. cybersecurity firm Mandiant, part of Google, said in a report on Thursday.”



Lack of In-House Expertise and Cybersecurity Complexity

According to the 2024 (ISC)² Cybersecurity Workforce Study, the global shortage of cybersecurity professionals has reached nearly 5 million. SMBs are disproportionately affected by this skills gap, which leaves them more vulnerable to cyberattacks due to their lack of internal expertise.

Regulatory and Compliance Pressures

Compliance with regulations such as NIST, NIS 2, DORA, HIPAA, and PCI DSS is becoming increasingly mandatory. Fines for non-compliance can reach up to \$10 million or 2% of global turnover. Many SMBs struggle to allocate the necessary resources to meet these requirements, increasing their risk.



The Financial Impact of Cyberattacks

Cyberattacks are financially devastating for SMBs. The Ponemon Institute reports that a single data breach can cost a small business approximately \$2.98 million. These costs include direct expenses, such as ransom payments and legal fees, and indirect costs, such as reputational damage and downtime.

2024 Cybersecurity
Workforce Study found:

5M

of global shortage
of cybersecurity
professionals



Cybercrime is a real
threat to SMBs

2.98M

is the average lost
from a single data
breach in a small
business



MDR as the Solution to Address SMB Cybersecurity Challenges

Managed Detection and Response (MDR) services provide continuous threat monitoring, detection, and expert-led response. Outsourcing cybersecurity to MDR providers allows SMBs to access 24/7 protection without needing an internal SOC.

How Partners Can Sell MDR Services

To effectively sell MDR services, partners must identify their target customer segments, tailor their offerings, and develop a clear value proposition. Key steps include:

- **Understanding the Ideal Customer Profile:** Different industries have varying cybersecurity needs and compliance pressures.
- **Defining MDR Packages and Bundles:** Offering tiered services such as monitoring, patch management, and compliance can meet diverse customer needs.
- **Developing a Marketing Strategy for MDR:** Inform and educate their audience through targeted campaigns, highlighting MDR's unique benefits.

Six Key Advantages of MDR

1. 24/7 Monitoring and Proactive Threat Management
2. Expert Analysis and Customized Responses
3. Rapid Incident Response
4. Compliance Assistance
5. Cost-Effective Solutions
6. Peace of Mind



Packaging MDR for Profitability

MSPs deeply understand their clients' environments, needs, and risks. This positions them perfectly to offer service packages that combine advanced technologies like MDR with their expertise. By doing so, they create security solutions that address their most pressing challenges. Here are some strategies to help integrate MDR effectively into their portfolio and drive success:

1. Avoid Making MDR Just an Add-On:

MDR is no longer optional. It's essential for protecting businesses from advanced threats. It should be bundled with other solutions, such as solid endpoint security and attack surface reduction practices to create a comprehensive package.

2. Consider Their Customers' Needs:

They know their clients' security needs and budgets. Offer packages that address their problems and provide real value at the right price.

3. Provide an Upgrade Path:

Not every customer will start with the highest-tier package. Demonstrate the benefits they are missing and encourage gradual upgrades over time.

4. Clarify MDR's Value:

Don't assume clients fully understand what MDR offers. Highlight the benefits – such as reduced threat response time, lower incident costs, and enhanced compliance – within their bundle.

5. Offer Additional Support and Reporting:

Some customers may require more detailed reporting or extra support, especially for regulatory compliance. This is an opportunity to upsell premium services.

By packaging MDR with complementary services, products, or specific features, they provide a robust, end-to-end security solution.



To address the growing challenges customers face – such as advanced threats, lack of in-house expertise, complex environments, compliance pressures, and the high costs of cyberattacks, it's essential to offer a service ladder that includes MDR as a core element. These services enhance customers' security posture and provide peace of mind. The following can be a ladder of managed security services designed to tackle these issues by integrating MDR.

Your Customers' Pain Points



Increasing
Cyber Threat Sophistication



Lack of In-House Expertise.
Environments & Cybersecurity Complexity



Regulations and Compliance
Pressure



The Total Cost of a
Cyberattack



Cyber Insurance

Packaging MDR

Level 1: Managed Endpoint Prevention, Detection, and Containment:

This entry-level service provides advanced threat prevention and detection, with 24/7 monitoring. It includes automated breach notifications, ransomware detection, and containment, with minimal disruption to the customer's environment.

Level 2: Fully Managed Endpoint Security

This tier builds on the previous level by enhancing cybersecurity hygiene through vulnerability identification and patch management. It also ensures rapid recovery in the event of an incident, allowing for minimal downtime.

Level 3: Fully Managed Endpoint Security + Supply Chain Defense

This package focuses on defending against supply chain attacks in addition to endpoint security. It shares threat intelligence with key partners (e.g., indicators of compromise, Yara rules), ensuring business operations are protected from external vulnerabilities.

Level 4: Fully Managed Endpoint Security + Regulatory Compliance

Tailored for businesses operating in regulated sectors, this service offers 24/7 MDR with automated compliance policies aligned with frameworks such as NIST, NIS 2, and DORA. Detailed reporting and audit documentation are included to ensure compliance during regulatory audits.

Level 5: Fully Managed Endpoint Security + Cyber Insurance

Some customers may require more detailed reporting or extra support, especially for regulatory compliance. This is an opportunity to upsell premium services.

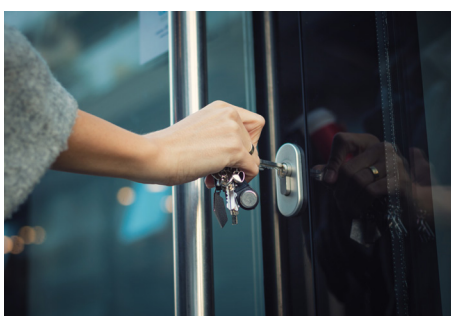
Handling Customer Objections to MDR

A common customer objection they may hear is: “Do I need MDR?” The answer is yes. Stress the rising sophistication of cyber threats and the need for continuous monitoring to improve detection and response. Reference high-profile breaches to highlight the risk for businesses of any size.

If customers think MDR seems excessive, remind them of the cost of a single breach and how MDR can prevent such incidents. For those questioning why existing security isn't enough, explain that security needs a layered approach. MDR complements existing solutions, more effectively addressing today's advanced threats.

Finally, if they worry MDR is just an unnecessary upgrade, emphasize that it's not just technology, it's backed by the expertise of the WatchGuard SOC and advanced AI, combined with your team's knowledge of their environment. MDR is an essential upgrade for now and the future.

The Protection Analogy: Locks, Sensors, and Surveillance Cameras



Locks = AVs



Sensor alarms = EDR



Monitoring = MDR

To simplify MDR's value, consider using this analogy:

Think of your security system as your house. The locks on your doors and windows represent your traditional AV and Endpoint Protection (EPP) products. They block threats from entering, but if a skilled intruder finds a way to pick the lock, they can still gain undetected access.

Now, imagine you've installed motion sensors inside your home. These sensors represent Endpoint Detection and Response (EDR) tools. They detect unusual movements inside and trigger alarms when suspicious behavior is detected.

However, even with motion sensors, you sometimes need a security expert to analyze what's happening. Here's where MDR steps in – MDR is like having a 24/7 surveillance team actively monitoring your security cameras. These experts don't wait for an alarm to go off; they're continuously watching for suspicious activity, ready to respond instantly. If an intruder breaks in, MDR swiftly addresses the threat before it causes significant harm, allowing you to rest easily, knowing your house is secure.

This analogy highlights the importance of having multiple layers of security in place. MDR is that extra layer that ensures a rapid and proactive response, giving businesses peace of mind.

Introducing WatchGuard MDR

Cybersecurity is highly complex and evolves so rapidly that organizations with limited resources struggle to manage it effectively on their own.

WatchGuard MDR is an extension of our MSPs, providing 24/7 monitoring, proactive detection, containment, and expert guidance to help recover and improve their customers' overall security posture.

Managed by cybersecurity professionals around the clock, it offers flexible support tailored to your operational needs, whether 24/7 or 8/5.

What Sets WatchGuard MDR Apart:

1. It enables partners to build their own branded MDR offering to expand their revenue streams.
2. It provides peace of mind for MSPs and their customers, as dedicated security experts monitor their customers' environments 24/7.
3. It accelerates the time to value as it is simple and easy to deploy. It doesn't require additional deployment when the customer is protected with WatchGuard Advanced Endpoint Security solutions.
4. It is highly flexible to the MSP operational model, delivering a 24/7 enterprise-grade MDR service, whether they operate 24/7 or 8/5, allowing them to scale as they grow and for customers, allowing tailor configurations.

Why WatchGuard MDR

- Build your own branded MDR offering. Expand revenue streams.
- Enterprise-grade MSS. Peace of mind.
- Easy to deploy. Rapid time to value.
- Operational Flexibility. Scale as you grow.



"MDR services have become a beacon of hope, offering a compelling managed service tailored to meet the growing threat landscape and customer expectations. Resource-constrained CIOs and CISOs now have an option to elevate their cybersecurity program in an affordable manner that is personalized to meet their unique security and risk needs."

Craig Robinson
Research VP at IDC

MDR

MDR made easy

The cybersecurity threat landscape constantly evolves, and SMBs need a robust solution to protect against sophisticated attacks. Managed Detection and Response (MDR) offers a cost-effective, scalable security solution that enables business continuity and compliance with regulations. Partners who effectively position MDR services will help their customers mitigate risks, improve their position in the market, and drive profitability.

Don't miss the opportunity to enhance your managed security services with MDR as a core offering.

Take advantage of the fast track that WatchGuard, a 100% MSP-focused cybersecurity vendor, provides its partners. Visit [WatchGuard MDR](#) to explore more.



About WatchGuard

WatchGuard® Technologies, Inc. is a global leader in unified cybersecurity. Our Unified Security Platform® 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](#).