HUGHES
An EchoStar Company

WHY MDR MIGHT BE THE PERFECT FIT FOR YOUR SMB

INTRODUCTION

For small and medium-sized businesses facing aggressive and persistent cyber threats with limited resources and budget, Managed Detection and Response (MDR) offers a path to protection.

According to Verizon's 2021 Data Breach Investigations Report, 46% of all cyber breaches impact businesses with fewer than 1,000 employees. Sixty-one percent of small and medium-sized businesses (SMBs) were the target of a cyberattack in 2021. As the U.S. Small Business Administration reported, there were over 700,000 attacks against small businesses, totaling $2.8 billion in damages that same year.

Why are SMBs being singled out? Because they often lack the resources, budget, expertise, and staff to adequately protect their networks—and attackers know it. They know that if they are aggressive and persistent enough in their attacks, they will likely prevail.

Fortunately, SMBs do not have to go it alone. Managed Security Service Providers (MSSP) have developed solutions, such as Managed Detection and Response (MDR) capabilities, that are specifically tailored to meet the unique needs of the SMB. MDR provides a comprehensive security solution that combines cutting-edge technology, experienced security analysts, and real-time threat intelligence to detect and respond to cyber threats.

In this e-book, we explore MDR's offerings in detail, including what it is, how it differs from traditional security solutions, what benefits it delivers, how it can be implemented, and what the future holds in terms of MDR trends and capabilities. With a better understanding of how MDR offers a cost-effective path to protection, an SMB can determine whether it might be a good fit for their business needs.

What is MDR?

So, what exactly is MDR and how does it differ from traditional security solutions?

MDR is a security service that combines advanced threat detection and response capabilities along with managed services, delivering a more complete and comprehensive security solution. Traditional security solutions, such as firewalls, anti-virus software, and intrusion detection systems, typically address only a single aspect of security. Businesses must therefore cobble together protection from disparate piece-parts and ensure they are kept up to date on the latest threats, through patches and upgrades.

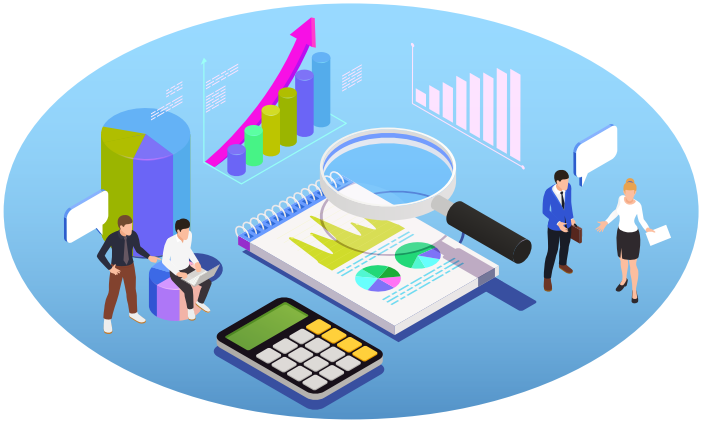
On the other hand, MDR provides a proactive, integrated approach to security that is far more effective. MDR relies on innovative technologies, including artificial intelligence (AI), machine learning (ML), and threat intelligence, to continuously monitor and analyze traffic and events for signs of malicious activity. If a threat is detected, the MDR provider's security analysts immediately investigate and respond to the threat, minimizing the risk of a breach and the impact of an attack. Having the latest threat detection technologies coupled with 24/7 monitoring and managed services is what paves the way for protecting the network and the business.

The Foundation of MDR

- **Managed Security Information and Event Management (SIEM):** Collects event log data from a range of sources to identify activity that deviates from the norm with real-time analysis to drive action.
- **Endpoint Detection and Response (EDR):** Continually monitors end user devices to identify threats like ransomware and malware.
- **24/7 Security Operations Center (SOC):** Delivers a full-time operational team armed with tools and technologies for real-time threat detection and mitigation.
- **Incident Response:** Outlines the formal procedures for identifying, investigating, and responding to potential threats to minimize impact.
- **Network Monitoring:** Provides real-time, end-to-end visibility needed to identify early indicators of compromise associated with an active cybersecurity event.

The Role of the SOC in MDR

One key aspect of MDR that is most difficult for SMBs to duplicate on their own is having an around the clock Security Operations Center (SOC) to rely upon. It can take millions of dollars to stand up a SOC, and millions more in recurring costs annually to run it. Even recruiting, hiring, and training an IT security team is often too cost-prohibitive for the SMB. Yet with MDR, SMBs can leverage the capabilities and services of a SOC without the capital expense.



While SOC teams may differ, most include the following:

- **Security analysts** who serve as cybersecurity first responders. They are on the frontlines, identifying and reporting threats, and implementing changes to protect the network and the organization.
- **Security engineers** are the software and hardware specialists who deploy, maintain, and update all the tools, technologies, and systems involved in securing the critical infrastructure, as well as document the security protocols.
- **A SOC manager** directs the team of analysts and engineers and orchestrates any responses to major security threats.

MDR providers that deliver Security Operations Center as a Service (SOCaaS) often have additional resources. For example, they may have professionals to establish security-related strategies and policies, manage incidents as they occur, and communicate requirements and actions in the case of a significant data breach. MDR therefore provides SMBs access to deep expertise and infrastructure that would be out of reach otherwise.

The Benefits of MDR

MDR is designed to complement existing security solutions and integrate with existing firewalls, intrusion detection systems, and other security technologies. In this way, MDR fills in network security gaps and provides a more comprehensive solution. For the SMB, that adds up to a host of benefits, such as:

- Proactive real-time threat detection and quick response capabilities that minimize risks and impacts of a breach.
- Advanced technologies, such as AI and ML, enable MDR to provide a more effective approach to securing the network.
- Dedicated experts to protect the business from threats.
- Affordable protection that eliminates the need for an SMB to invest in their own expensive security equipment, software, and staff.
- The ability to scale to meet the needs of a business as it changes and grows.
- Peace of mind in knowing that systems and data are protected!

5 Steps to Implement MDR

While implementing MDR requires careful planning and coordination, the right provider can enable the transition to be smooth and seamless. For most implementations, the MDR provider will:

1. Assess the business' current security posture, which includes evaluating the existing security technologies, processes, and personnel.
2. Develop a plan to outline specific technologies, processes, and personnel required for the implementation.
3. Install and configure the technology, including the MDR platform, to protect the SMB's network and data.
4. Train the SMB's essential personnel on the use of the MDR platform and processes involved in responding to cyber threats.
5. Monitor and maintain the network security systems to protect the SMB from potential threats and breaches.

What Does the Future Hold?

While MDR offers robust protection for SMBs today, several trends promise to continually improve the future of MDR, including the following:

- **Further integration with other security solutions.** As technologies evolve, MDR is expected to integrate with additional security solutions, such as Network Detection and Response (NDR), Secure Service Edge (SSE), and others.

- **Advanced threat intelligence.** As AI and ML algorithms incorporate more advanced threat intelligence, MDR will continually improve in its ability to identify and respond to threats in real-time.

- **Security Orchestration, Automation, and Response (SOAR).** Over time, advanced tools and algorithms will enable MDR to become more automated, eliminating the manual processes involved in incident analysis and response. This will increase the speed and accuracy of threat response.

- **Greater focus on cloud security.** As more SMBs adopt cloud technologies, MDR providers will need to focus on how to protect cloud infrastructure, systems, and data.

- **Increased adoption that leads to lower costs.** With more and more businesses adopting MDR as their primary security solution, market competition will increase. The good news is that adopting MDR will lead to lower cost solutions.

Given today's rapidly changing and complex cyber threat landscape, SMBs must proactively protect their networks. Anything less puts them at risk. But with MDR, SMBs no longer need to worry about being singled out by cyber-attacks. Instead, they can be confident they have the resources, expertise, and staff necessary to adequately protect their networks. Regardless of how aggressive and persistent threats may be, it will be the SMB that prevails.

For additional information, please call 1-888-440-7126 or visit www.hughes.com.

HUGHES®
An EchoStar Company

www.hughes.com

11717 Exploration Lane
Germantown, MD 20876 USA