AMPCUS CYBER
Zero Trust Compliance Service Provider

2024

The ROI of MDR: Balancing Costs with Cybersecurity Outcomes

www.ampcuscyber.com

Introduction

In today's digital landscape, organizations are more vulnerable than ever to sophisticated cyberattacks. From ransomware to data breaches, the financial and reputational impact of such incidents can be devastating. While traditional security measures are vital, they often fall short of providing the comprehensive protection required. This is where MDR comes in—a proactive, round-the-clock security service designed to detect, analyze, and respond to threats in real-time.

The primary question for decision-makers, however, is not whether MDR is effective but whether it delivers sufficient ROI to justify its costs. This white paper delves into the financial and operational benefits of MDR, helping organizations make informed decisions about their cybersecurity investments.

As cyber threats grow in complexity and frequency, organizations face increasing pressure to strengthen their defences while managing costs. Managed Detection and Response (MDR) has emerged as a solution that bridges the gap between robust security and cost efficiency. This white paper explores the return on investment (ROI) of MDR by examining its ability to reduce risks, enhance operational efficiency, and deliver measurable financial outcomes. It also addresses how MDR balances costs with long-term cybersecurity gains, making it a strategic choice for organizations of all sizes.

The Problem: Rising Costs of Cybersecurity and Incidents

Escalating Threat Landscape

- Cybercrime costs are projected to reach $10.5 trillion annually by 2025 (source: Cybersecurity Ventures).
- Advanced persistent threats (APTs), phishing, and zero-day attacks are bypassing traditional defences.

Resource Constraints

- Shortage of Skilled Professionals: Small and mid-sized organizations struggle to hire and retain cybersecurity talent in a market with millions of unfilled positions globally.
- Budget Challenges: Many businesses lack the financial resources to build and maintain an in-house SOC with advanced threat detection capabilities.
- Inefficient Use of Time: IT teams are bogged down by managing alerts and investigating false positives, diverting attention from strategic projects.

Inefficiencies of In-House Security

- Talent shortage: Over **3.4 million unfilled cybersecurity positions** worldwide.
- High operational costs for 24/7 monitoring, detection, and response capabilities.

The Solution: MDR as a Cost-Effective Cybersecurity Model

Managed Detection and Response is a subscription-based service that provides:

- **24/7 Monitoring:** Delivers round-the-clock security monitoring to identify and mitigate threats in real-time.
- **Simplified Security Operations:** Simplifies incident response processes to enhance efficiency and reduce resolution times.
- **Enhanced Visibility and Control:** Ampcus Cyber MDR offers a unified view of your security posture to monitor and manage threats effectively and improve decision-making with actionable insights
- **Access to Expertise:** Leverage a team of experienced cybersecurity professionals to handle threat detection and response.
- **Cost-Efficiency:** Subscription-based pricing significantly reduces infrastructure and staffing costs.

> *Ampcus Cyber MDR offers a unified view of your security posture to monitor and manage threats effectively and improve decision-making with actionable insights*

Comprehensive Cybersecurity Solutions

Cost-Efficiency

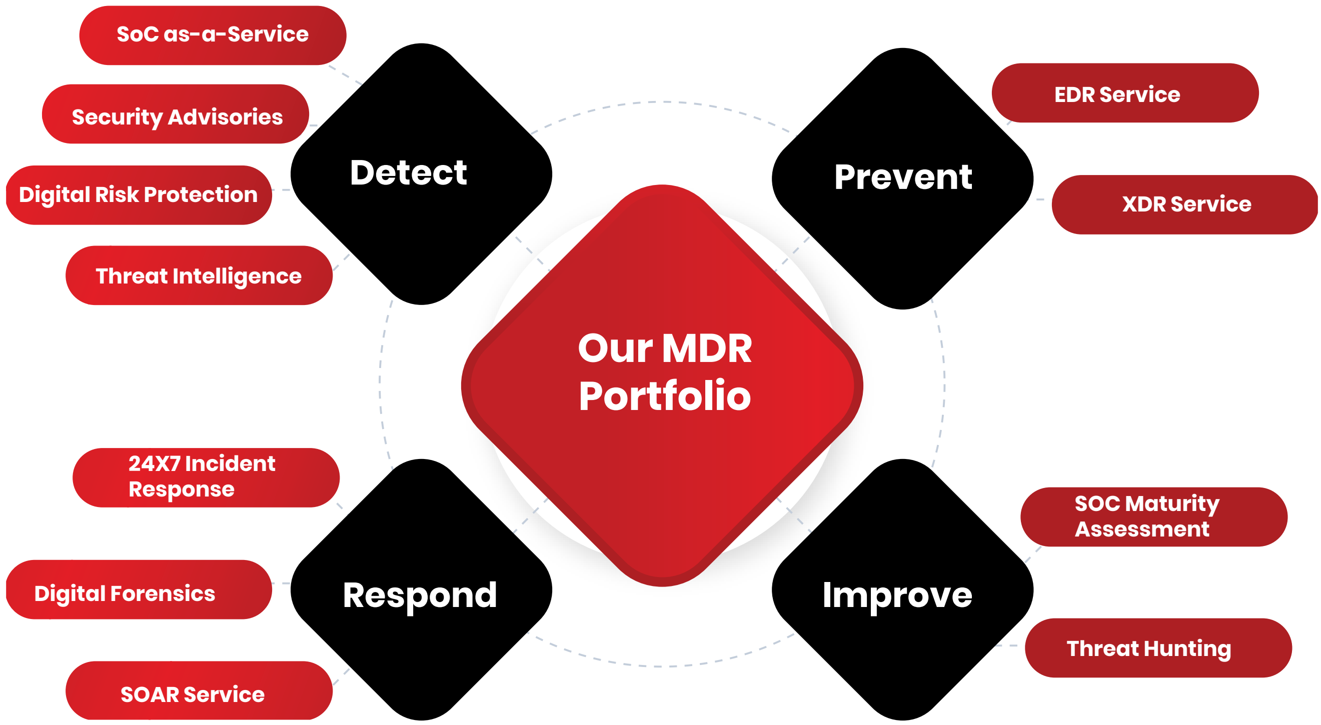
Access to Expertise

24/7 Monitoring

Enhanced Visibility and Control

Simplified Security Operations

Our CyberDefend MDR Service Portfolio: Built for Modern Threats



ANALYSING THE ROI OF MDR

1. **Faster Threat Containment**: MDR isolates and neutralizes threats quickly, preventing the spread of damage and minimizing operational disruptions.
2. **Continuous Security Updates:** With MDR, customers stay ahead of threats without having to invest in or manage the latest cybersecurity technologies themselves.
3. **Optimized Security Spend**: MDR consolidates tools, expertise, and processes into a single service, reducing the need for multiple, costly standalone solutions.
4. **Stronger Risk Management:** MDR strengthens your defenses by reducing breach risks, lowering cybersecurity insurance premiums, and building resilience to ensure smooth business operations even during escalating threats.
5. **Enhanced Compliance:** Ensure compliance with industry regulations like GDPR, PCI DSS, and HIPAA through automated support, reducing effort, costs, and regulatory stress while building trust with customers.
6. **Scalability and Predictability:** MDR adapts to growing business needs, providing more coverage or protection without requiring capital investments in new tools or teams.

BENEFITS OF MDR IN NUMBERS

Metric	Traditional Security	MDR
Initial Investment	High (Infrastructure, Staff)	Low (Subscription-based)
Average Time to Detect Threat	207 days	Hours to minutes
Average Cost of Breach	$4.45M	Reduced by 50-70%
24/7 Monitoring Cost	Very High	Included
Staffing Requirements	Large, Specialized Teams	Minimal

CALCULATING ROI: KEY METRICS

To evaluate the ROI of MDR, consider the following key metrics:

Metric	Pre-MDR	Post-MDR	Impact
Mean Time to Detect (MTTD)	High	Low	Reduced dwell time for threats
Mean Time to Respond (MTTR)	High	Low	Faster containment and mitigation
Number of Security Incidents	High	Reduced	Fewer incidents reaching impact stage
Downtime (in hours)	High	Reduced	Lower operational disruption
Compliance Penalties/ Fines	Potentially High	Minimal	Improved regulatory compliance

CASE STUDY: HOW AN E-COMMERCE COMPANY TRANSFORMED SECURITY WITH MDR

Client Overview

A mid-sized e-commerce company handling thousands of transactions daily, with sensitive customer data at the core of its operations. Operational uptime and data security were critical to maintaining customer trust and business growth.

THE CHALLENGE

Without an existing SIEM or dedicated security tools, the company struggled to manage:

1. **Frequent Suspicious Activity:** Increasing brute-force login attempts and unauthorized access attempts were going undetected.
2. **Delayed Incident Detection**: Threats often went unnoticed until significant damage was done.
3. **Resource Constraints:** The IT team lacked the expertise and time to monitor and respond to security events effectively.
4. **Customer Confidence Erosion:** Security concerns were starting to affect customer trust and retention.

THE SOLUTION

The company adopted a Managed Detection and Response (MDR) service to establish a proactive, comprehensive security approach from scratch. The MDR solution provided:

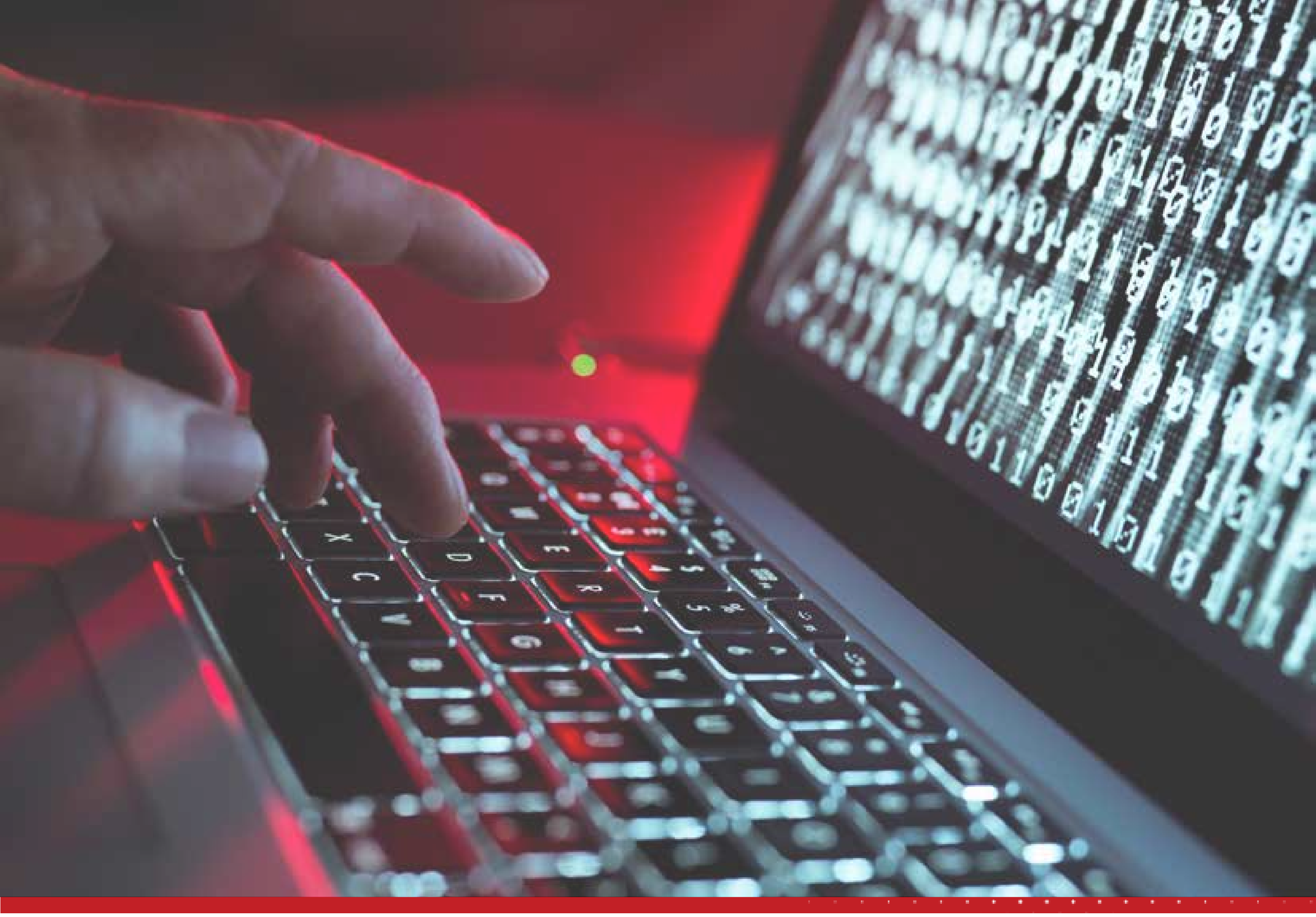
1. **24/7 Monitoring and Threat Detection:** Constant vigilance over their network, endpoints, and customer-facing platforms.
2. **AI-Driven Threat Analysis:** Intelligent detection tools identified suspicious patterns and prioritized actionable threats.
3. **Rapid Response Team:** Dedicated experts responded immediately to neutralize threats and minimize impact.
4. **Security Expertise:** Guidance on hardening their infrastructure and closing vulnerabilities.

THE RESULTS

1. Incident Frequency Reduced by 65%: MDR eliminated unauthorized access attempts and mitigated suspicious activity quickly.
2. Saved $900,000 in Potential Breach Costs: Prevented financial losses from downtime, data breaches, and operational disruptions.
3. Improved Customer Trust and Retention: Strengthened security reassured customers, leading to a 25% growth in repeat transactions.
4. Seamless Security Setup: The MDR provider implemented a full security solution without the need for the company to invest in or manage complex tools like SIEM.

THE STRATEGIC CHOICE FOR MODERN SECURITY

Investing in MDR is not just about enhancing cybersecurity—it's about achieving a strategic balance between cost and value. By minimizing the financial and operational impact of cyber incidents, MDR delivers measurable ROI while strengthening organizational resilience. Whether your business is a small startup or a large enterprise, MDR offers the comprehensive protection and cost-efficiency required to navigate today's evolving threat landscape.



THE AUTHOR'S NOTE

Sujay, Chief Cyber Defense Officer at Ampcus Cyber, brings over 15 years of expertise in MDR, SOC operations, assessments, and VAPT. He has successfully led multidisciplinary SOC teams of over 200 professionals, specializing in threat hunting, incident response, and digital forensics. With a focus on innovation, Sujay ensures Ampcus Cyber remains at the forefront of cybersecurity, empowering clients to build resilience in today's rapidly evolving digital landscape.

-Sujay Mendon

Kavita, MDR Presales Lead at Ampcus Cyber, brings expertise in designing advanced MDR solutions by identifying customer challenges and aligning security strategies with business objectives. With a consultative approach, she ensures organizations achieve robust security capabilities that address the unique needs of organizations.

-Kavita Konar

USA
Ampcus Cyber Inc., 14900
Conference Centre, Drive Suite
# 500, Chantilly, VA 20151.

India
3rd Floor, Beta Block, Sigma
Tech Park, Varthur, Bengaluru,
Karnataka – 560 066.

Philippines
3rd Floor, Unit #8, Blk 9 Lot
8 Downhill St. Towerhills
Subdibision, Dolores Taytay,
Rizal, Philippines

Dubai
906-67, 9th floor, Concord
Tower, Dubai Media City, Dubai,
UAE