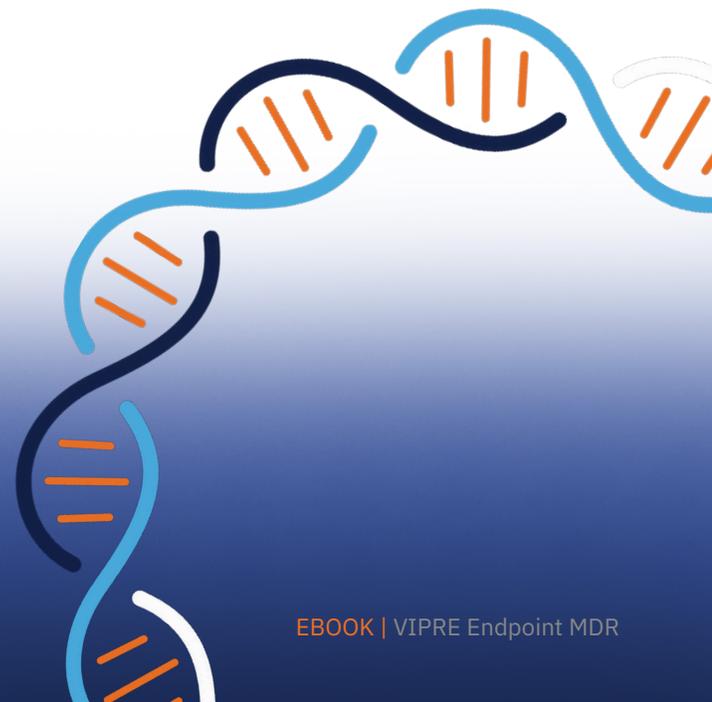
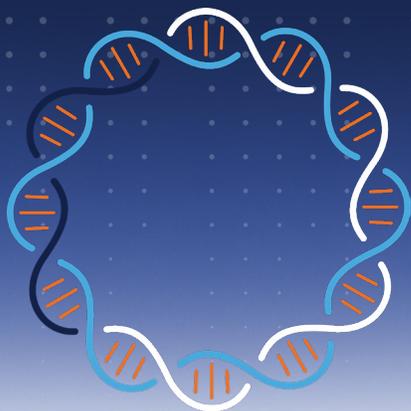


VIPRE Endpoint MDR - eBook

Why Your Business Needs **Managed Detection and Response (MDR)** Services





Contents

Introduction	03
Understanding Managed Detection and Response (MDR)	04
The Importance of Managed Detection and Response (MDR) Services	04
- Early Detection and Response	04
- Proactive Threat Hunting	05
- Expert Analysis and Incident Response	05
- Continuous Monitoring and Compliance	05
Signs Your Business Needs Managed Detection and Response (MDR) Services	06
- Limited Resources and Expertise	06
- Increasing Cybersecurity Threats	07
- Lack of 24/7 Coverage	07
- Regulatory Compliance Requirements	07
- High Value of Data and Intellectual Property	07
Why VIPRE Endpoint MDR?	08



Introduction

Why Your Business Needs Managed Detection and Response (MDR) Services

In today's rapidly evolving digital landscape, businesses face an ever-growing number of cyber threats.

These threats are becoming increasingly sophisticated, capable of bypassing traditional security measures and causing significant damage to organizations of all sizes. As a result, businesses must prioritize the implementation of robust cybersecurity solutions to protect their sensitive data, critical systems, and reputation. One such solution that has gained prominence in recent years is Managed Detection and Response (MDR) services. In this comprehensive guide, we will explore what MDR is, why businesses need it, and how it can help organizations proactively detect, analyze, and respond to cyber threats.

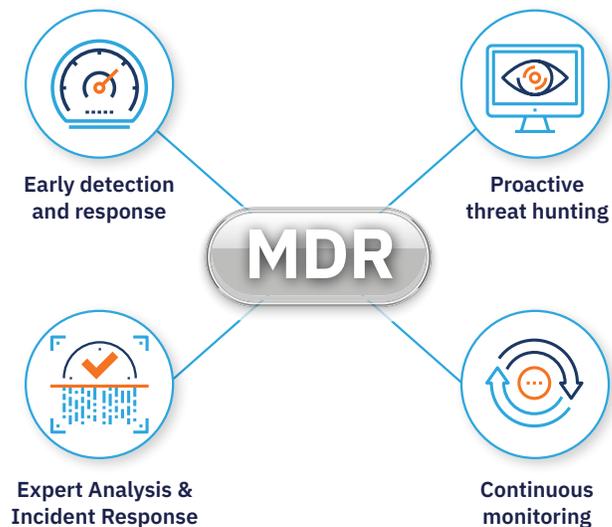


Understanding Managed Detection and Response (MDR)

Managed Detection and Response (MDR) is an outsourced cybersecurity service that provides advanced threat detection, analysis, and response capabilities.

MDR services combine cutting-edge technologies, expert analysts, and round-the-clock monitoring to swiftly identify, investigate, and mitigate cyber threats.

These services go beyond traditional security measures by offering continuous monitoring, proactive threat hunting, and incident response services. MDR providers leverage advanced analytics, threat intelligence, and human expertise to detect and respond to threats in real-time, minimizing the potential damage caused by cyber incidents.



The Importance of Managed Detection and Response (MDR) Services



Early Detection and Response

One of the primary reasons why businesses need MDR services is the ability to achieve early detection and response to cyber threats.

Traditional security measures often rely on preventative controls like firewalls, antivirus software, and network safety tools. While these measures are important, they may not be sufficient in detecting sophisticated and evolving threats.

MDR services utilize Endpoint detection and Response (EDR) solutions to employ advanced technologies, such as artificial intelligence (AI) and machine learning (ML), to analyze vast amounts of data and identify anomalies that may indicate a potential security breach. By detecting threats early on, businesses can respond swiftly and effectively, minimizing the impact of cyber incidents.



Proactive Threat Hunting

EDR solutions used in conjunction with MDR services take a proactive approach to cybersecurity by actively hunting for threats that may have evaded traditional security measures, and they do so across the entire network environment.

For example, if a threat is detected on one endpoint, the EDR can extract the indicators of compromise (IoC) and continue hunting to see if they may be elsewhere within the environment.

By utilizing EDR to continuously monitor network traffic, logs, and endpoints to identify suspicious activities and indicators of compromise, MDR services can leverage advanced analytics and threat intelligence to uncover hidden threats and vulnerabilities within the organization's network. By actively searching for threats, MDR services can prevent potential breaches before they occur, reducing the risk of data loss, financial damage, and reputational harm.



Expert Analysis and Incident Response

MDR services provide businesses with access to a team of skilled cybersecurity analysts who possess the knowledge and expertise to analyze and respond to cyber threats effectively.

These experts investigate detected threats, understand their nature and impact, and develop tailored response strategies. By partnering with MDR service providers, businesses can leverage the experience and insights of these professionals without the need to maintain an in-house cybersecurity team. This ensures that incidents are addressed promptly and effectively, minimizing downtime and financial losses.



Continuous Monitoring and Compliance

Achieving continuous monitoring and maintaining compliance with industry regulations is a significant challenge for businesses of all sizes.

MDR services provide continuous monitoring and auditing capabilities, ensuring that threats are detected and addressed in real-time. By monitoring network activities, analyzing logs, and generating reports, MDR services assist businesses in maintaining a robust security posture and demonstrating adherence to regulatory frameworks. This not only helps businesses meet compliance requirements but also protects the organization's reputation and instills trust among employees, customers, and partners.



Signs Your Business Needs Managed Detection and Response (MDR) Services

While every business can benefit from MDR services, certain signs indicate that it may be time for your organization to consider implementing this proactive cybersecurity solution. Here are some indicators that suggest your business could benefit from MDR services:



Limited Resources and Expertise

The costs to build an in-house security operations center (SOC) can be prohibitive for most organizations, especially small and medium-sized businesses (SMBs) and small and medium-sized enterprises (SMEs).

Allocating sufficient resources and maintaining a qualified in-house cybersecurity team to run a SOC can be challenging and costly.

The estimated cost for building and running an internal SOC is nearly \$2.9M per year and those costs could scale up to \$5M or more for an advanced SOC depending upon the needs of an organization.

- Average IT security analyst ~\$92,000/yr¹
- Need roughly 10-12 analysts for full 24/7 coverage²
- Plus hardware, software, training, etc.
- Average cost to build a SOC is \$2.86M³

By partnering with an MDR service provider, businesses can outsource part of the SOC to an expert, sharing costs with many other organizations and access a dedicated team of experts who possess the knowledge and expertise to detect, analyze, and respond to threats effectively. This allows organizations to leverage the skills of experienced professionals without the burden of recruitment and training costs.

Building and running an in-house security operations center (SOC)

Estimated cost
PER YEAR \$2.9M

...And up to \$5M or more for an advanced SOC

1 - <https://www.indeed.com/career/security-analyst/salaries>

2 - <https://www.infosecurity-magazine.com/opinions/calculating-true-cost-soc/>

3 - <https://www.securitymagazine.com/articles/98722-building-a-security-operations-center-soc-on-a-budget>



Increasing Cybersecurity Threats

The cybersecurity landscape is constantly evolving, with cyber threats becoming more sophisticated and frequent.

Businesses face a wide range of threats, including malware, ransomware, phishing attacks, and insider threats. As these threats continue to grow in complexity, traditional security measures may struggle to keep up. MDR services offer advanced threat detection capabilities and the ability to respond swiftly to mitigate risks.

Another advantage to utilizing an MDR service is the shared knowledge of threats and responses that may be found among other customers which can then be utilized to the advantage of the entire client base, i.e., if a threat pattern is detected on one system, the MDR service provider knows to be on the lookout for it and can apply any lessons learned to other clients.

By partnering with an MDR service provider, businesses can stay ahead of evolving threats and reduce their vulnerability to cyber attacks.



Lack of 24/7 Coverage

Cyber threats can occur at any time, and businesses need round-the-clock monitoring to detect and respond to incidents promptly.

However, maintaining an in-house security operations center (SOC) with 24/7 coverage can be challenging and costly. MDR services offer continuous monitoring and response capabilities, allowing businesses to benefit from 24/7 threat detection and incident response without the need for significant investments in personnel and infrastructure.



Regulatory Compliance Requirements

Many industries have strict compliance requirements and regulations that govern how organizations handle and protect sensitive data.

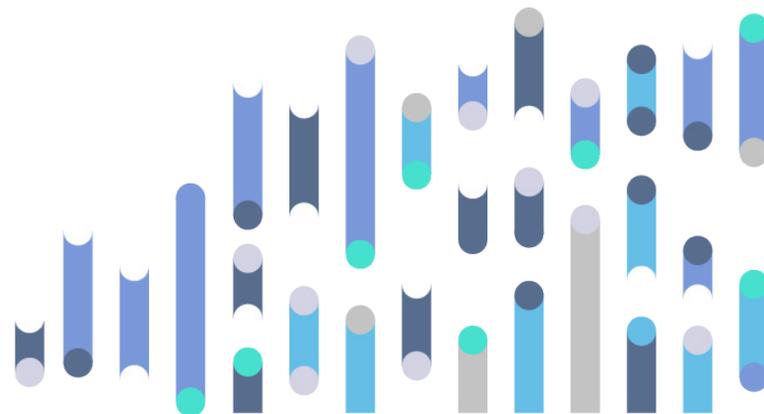
Achieving and maintaining compliance can be a complex and time-consuming process. MDR services can help businesses meet compliance requirements by providing continuous monitoring, incident response capabilities, and audit-ready reports. By partnering with an MDR service provider, businesses can demonstrate their commitment to data security and ensure that they meet the necessary regulatory obligations.



High Value of Data and Intellectual Property

Organizations that handle sensitive data, intellectual property, or trade secrets are prime targets for cybercriminals.

The loss or compromise of such information can have severe consequences, including financial losses, reputational damage, and legal liabilities. MDR services offer advanced threat detection capabilities and round-the-clock monitoring to protect valuable assets. By partnering with an MDR service provider, businesses can proactively detect and respond to threats, minimizing the risk of data breaches and intellectual property theft.



Why VIPRE Endpoint MDR?

In today's digital landscape, where cyber threats are prevalent and ever-evolving, businesses must prioritize the implementation of robust cybersecurity solutions.

VIPRE Endpoint Managed Detection and Response (MDR) service provides businesses with the advanced threat detection, analysis, and response capabilities necessary to mitigate risks and protect sensitive data and critical systems.

By leveraging cutting-edge technologies, expert analysts, and continuous monitoring, VIPRE Endpoint MDR services can proactively detect and respond to cyber threats, reducing the potential impact of security incidents. Whether your organization lacks the resources and expertise to maintain an in-house cybersecurity team or faces increasing cybersecurity threats, VIPRE Endpoint MDR offers a reliable and effective solution to enhance your organization's security posture.

VIPRE Endpoint MDR delivers:

- MDR services at a fraction of the cost of building out an in-house SOC.
- 24/7/365 coverage that would not only be cost-prohibitive with an internal IT security team, it often wouldn't be possible due to weekends, holiday schedules and staff limitations.
- A live team of cybersecurity experts monitoring your systems and responding to incidents. Real people detecting real issues and remedying real situations. No "canned" responses or "one-size fits all" fixes.
- A pre-packaged offering with a fixed price that enables clients to get up and running more quickly - no need to wait for a full scoping of the project that could be required by other vendors.

Partnering with a proven leader in NextGen antivirus endpoint service provider like VIPRE allows businesses to focus on their core operations while having peace of mind knowing that their cybersecurity needs are being addressed by experienced professionals. Consider your own organization's capacity for incident response and remediation, whether the resources exist to hire an in-house security team to accomplish these tasks, then decide whether you can afford to gamble with your business' cybersecurity.



North America
sales@vipre.com
+1 855 885 5566

UK and other regions
uksales@vipre.com
+44 (0)800 093 2580

DACH Sales
dach.sales@vipre.com
+49 30 2295 7786

Nordics Sales
nordic.sales@vipre.com
+45 7025 2223