Endpoint Security Challenges

Organizations of all types and sizes have upgraded from next-generation antivirus (NGAV) to Endpoint Detection & Response (EDR), driven by cyber-insurance requirements or simply a desire to be more agile in responding to potential threats.

Compared to NGAV - which will block anything that has a high likelihood of being malicious - EDR will report on even relatively minor suspicious activity and support deep investigation, rapid containment, and remediation of that potential threat. Unfortunately, this increased power and flexibility comes at a cost: humans need to research potential 'grey area' threats and manually invoke containment and remediation actions. When added to the burden of IT teams already stretched thin by management of other security tools—each generating their own alerts that have to be dealt with—EDR can create more problems than it solves.

VIPRE EDR

Managed Detection and Response

To help solve this problem, since most organizations can't simply go hire more IT security experts even if they were available, there is a general shift towards outsourcing key aspects of IT security and management. Whether this is just hiring a friend who 'knows computers', contracting with an MSP to handle all your IT, or signing up an MSSP or SOC-as-a-Service to cover your IT security-specific concerns, the need is the same. A more modern and specialized service, Managed Detection and Response (MDR), focuses specifically on helping organizations with response to detected threats: the investigation, containment, and remediation actions of incident response. VIPRE Endpoint MDR focuses specifically on security incidents generated by VIPRE EDR, and solves many of the challenges related to deploying any EDR solution:

Benefits of VIPRE Endpoint MDR

- **Never miss a threat incident raised by VIPRE EDR.**
- **Reduce attack spread through rapid containment of potentially-compromised endpoints.**
- **Reduce dwell time of a threat in your environment to reduce potential damage and information theft.**
- **Clean up quickly and correctly due to expert security guidance.**
- **Reduce drain on employee time allowing them to focus on other projects.**
- **Raise overall security posture based on IT security expert guidance on environment hardening.**

VIPRE Endpoint MDR

VIPRE Endpoint MDR is an overlay for VIPRE Endpoint Detection & Response that provides 24x7x365 monitoring and incident coverage. Our team of security experts will monitor your console to react to any new incidents, and then will quickly triage, investigate, and support the containment and remediation of any valid threats with rapid turnaround times.

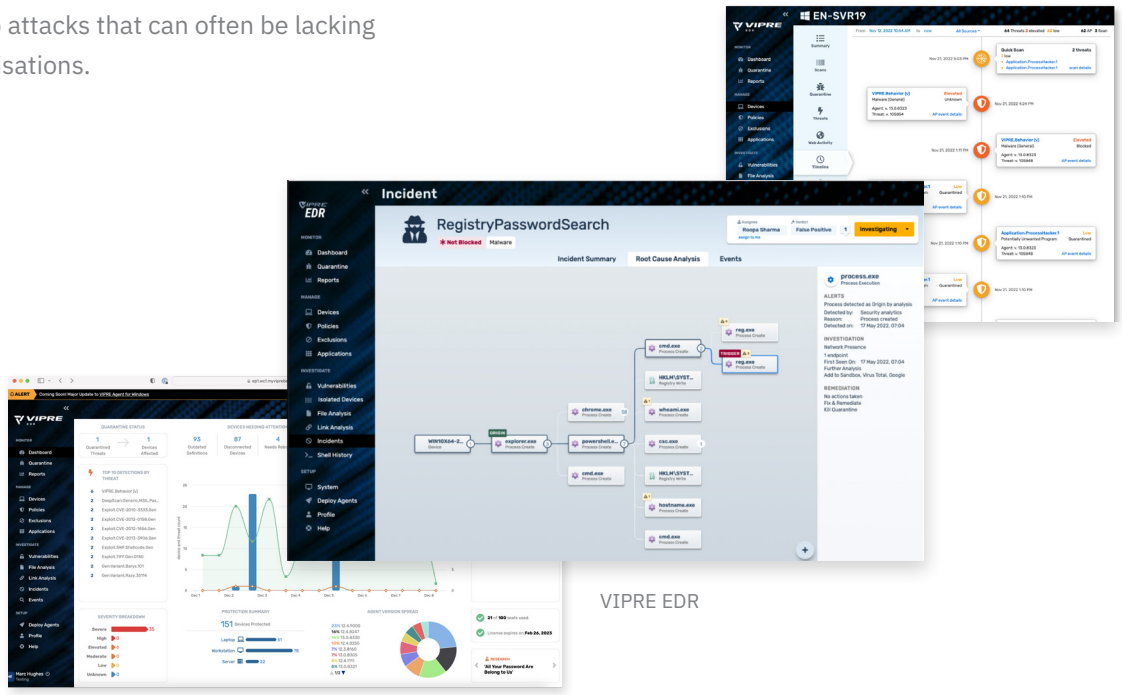
In addition, quarterly security reviews will keep you in the loop about longer-term trends regarding the security of your organization to ensure that your environment - and your security solution - is kept in tip-top shape and operating effectively. We provide the expertise and skills needed to investigate and respond to attacks that can often be lacking in all but the largest organisations.

We offer VIPRE Endpoint MDR at two levels designed to meet your business' needs:

Benefits of VIPRE Endpoint MDR

- **VIPRE Endpoint MDR** provides complete coverage for incident monitoring and investigation, and then provides detailed analytics and recommendations to your internal teams to perform the actual remediation. Containment is available, but is limited to network isolation of affected endpoints to prevent spread.

- **VIPRE Endpoint MDR Premium** goes a step further and provides everything within VIPRE Endpoint MDR, plus proactive incident response including forensic analysis, containment, and remediation by the VIPRE team leveraging our Remote Shell and other technologies. Detected artifacts will be fully analyzed in sandbox environments to extract additional IoCs for further investigation and to support additional hardening.



VIPRE EDR

MDR Service Details

Feature	Description	The VIPRE Difference
Onboarding	Deploy VIPRE EDR to your environment and ensure that everything is configured and operating correctly.	• Deploy and verify agents at customer site. • Test that incidents are detected and created correctly. • Gather customer contact/escalation info. • Gather information on baseline security posture.
24x7x365 Monitoring	Security analysts will monitor VIPRE EDR on a 24x7x365 basis for any new Incidents.	• Monitoring and assignment of new Incidents to response teams.
Incident triage	Expert IT security personnel will review all Incidents and ensure that they are properly handled, closing false positives and escalating any unhandled threats to the response team.	• Handle and analyze new inbound Incidents. • Perform a quick analysis to identify obvious FPs and potential threat impact. • Internal assignment and escalation.
FP/TP analysis	Deeper analysis to identify false positives and potential threat impact.	• More intensive analysis by tier 2 team to weed out false positives or clarify potential threat impact. • Adjustments to incident status and severity, plus early identification of potential targets and threat artifacts.
Incident Enrichment	Review incidents to identify known threats.	• Pull IoCs from the Incident and research within known threat databases to identify attack type, source, etc. • Annotate the Incident with any significant findings.
Analyst notes and remediation recommendations	Human analyst insight added to each Incident.	• Human review of Incident to identify significant malicious activity within processes, network connections, files, etc. • Recommendations on how to contain and clean up any threats on the endpoint. • Annotation of Incident with these insights.
Incident escalation	Escalation of all incidents to the customer team for resolution.	• Includes all the notes and recommendations as above. • Flexible escalation based on threat type and severity, i.e. email and SMS.
24x7x365 tech support	Provide dedicated support on product-related issues.	• Reactive response to customer-reported product issues. • Internal escalation for resolution as required.
Executive Reporting - quarterly	Provide a monthly executive summary of activity within the MDR service.	• Analyst reviews customer history and prepares report. • Incident metrics and retrospectives. • Overall threat trends and observations. • Environmental recommendations.
Service Level Agreements	Agreed time within which services will be performed.	• Three different SLA categories: initial incident acknowledgement, full response completion, and round-trip on clarification questions. • SLAs are set based on Incident status and severity. • SLAs fully defined in Statement of Work associated with this service.

Why VIPRE?

VIPRE Security Group puts more than twenty years of advanced security intelligence, cutting-edge machine learning, real-time behavioral analysis, and a comprehensive threat intelligence network to work defending against known and unknown attacks. Our supportive approach to MDR is suitable for all small to medium sized businesses.

- **The Best Protection at the Best Price** - VIPRE EDR is consistently ranked in the top tier alongside other market leaders in comprehensive independent tests.
- **Easy to Use** - VIPRE's intuitive solutions make it easier to secure your endpoints from ransomware and other threats.
- **Rapid Deployment** - We can quickly deploy VIPRE EDR with minimal disruption to day-to-day activities.
- **Reduced Downtime** - VIPRE enables both speed and security protecting you from malware without slowing down any processes.
- **Threat Actor Tracking** - 200+ Threat actors tracked continuously.
- **Experienced Incident Response Team** - 2,000+ Hours of incident response every year.
- **Award-winning Support** - included with all of our solutions is access to our award-winning, highly-qualified global tech support team with a consistent 90%+ CSAT rating.

Summary

VIPRE Endpoint Detection & Response is an important solution to ensure that your endpoints are protected against malware, remote compromise, and insider threats. But EDR solutions like ours require some care & feeding to achieve the best value and provide complete protection. VIPRE Endpoint MDR (or MDR Premium) provides an outsourced management layer to ensure that you get the best protection from your EDR solution.

To detect and respond instantly to endpoint threats with next-generation EDR and antivirus technology built for SMEs and the partners that serve them without our MDR offering you can find more detailed information here.

VIPRE SECURITY GROUP

ABSI Technology

VIPRE SECURITY GROUP

Blog Series
VIPRE MDR

Endpoint Cloud Security vs. EDR vs. MDR: Which One Do You Need?

EDR, MDR, and endpoint security are increasingly hot topics, along with the promotion of Zero Trust Architecture for cyber defense.

The US government, for instance, issued an executive order in May 2021 mandating endpoint detection and response (EDR) systems across all federal entities. In addition, the White House Office of Management and Budget (OMB) released a document outlining how agencies should install EDR technologies. This memo's usefulness extends beyond the federal government. It also aids businesses in gauging the efficacy of their existing endpoints.

What is endpoint security?

Endpoint security aims to prevent unauthorized access to the many computers, mobile devices, and other connected assets that make up your business's infrastructure. These access points are the weak spots in your organization's IT security. Endpoint security provides a suite of tools to keep an eye on all your endpoints, identify malicious software and other threats before they impact your systems, and stop data from leaking out accidentally.

When it comes to protecting endpoints, you can choose one of two routes:

- Prevent threats before they reach an endpoint by taking a proactive stance.
- Recognize the presence of a threat once it has been executed, and take steps to fix the problem.

EPP, EDR, and MDR are the three most common varieties of endpoint protection systems. These solutions equip your staff and security teams to effectively reduce risk, shorten response times, and address nearly all alerts. However, the effectiveness and efficiency of even the best-of-breed solutions today depend heavily on the context of these cybersecurity implementations.

This article will examine the differences and similarities between EPP, EDR, and MDR.

Endpoint Protection Platform (EPP)

An Endpoint Protection Platform (EPP) refers to next-generation antivirus (AV) – solutions that build upon traditional antivirus but leverage modern advanced techniques. An EPP protects endpoints from malicious code by operating locally on the device. Detection and automated blocking operations are provided, which are vital to real-time security procedures.

Cloud-based management is a crucial feature of modern EPP solutions, says Gartner, as it enables constant monitoring and data gathering on endpoint activities and the execution of remote remediation measures, regardless of whether the endpoint is located within the corporate network or remotely.

Furthermore, these solutions do not need to keep a local database of all known indicators of compromise (IOCs). Instead, they check a cloud resource to find the most up-to-date data on issues it cannot categorize.

Simplifying the company's security operations, EPP can pinpoint the source of the assault and aid in the enhancement of information sharing. EPP solutions hosted in the cloud have the potential to reduce administrative expenses, speed up time to value, and encourage agile product development. When malicious software tries to blend in, these tools can provide real-time analytics and identify unusual behavior.

Still, no endpoint protection platform (EPP) is perfect for preventing malicious activity. Even with a 99+% block rate, businesses must recognize the importance of endpoint detection and response for handling "grey area" threats on the endpoint. Thus, we arrive at our next topic: EDR.

Endpoint Detection and Response (EDR)

By employing models to identify whether something dangerous has already been done on an endpoint, Endpoint Detection and Response increases EPP's value. Once EDR recognizes a harmful act, it enables notifications, visibility, investigation and remedy.

As stated in the OMB memorandum, EDR platforms merge "real-time continuous monitoring and collection of endpoint data (for example, networked computing devices such as workstations, mobile phones, servers) with rules-based automated response and analysis capabilities."

An EDR platform primarily serves to:

- Continuously monitor and gather activity data from endpoints that may signal a threat
- Analyze data to detect threat trends
- Automate response to recognized threats to eliminate or contain them
- Alert the security team or SOC when a threat is detected
- Conduct forensics and analysis to learn more about the potential danger and look for any unusual behavior

Managed Detection and Response (MDR)

The security team can keep a close eye on what's happening within the network thanks to the EDR platform's detailed reports and comprehensive visibility. While alert monitoring and validation are critical, security teams typically spend too much time on these tasks – in fact, all but the largest organizations generally lack appropriate in-house expertise with the skills needed to investigate and respond to attacks

When attacks occur that go beyond garden variety malware easily stopped by EPP, it's critical that experienced security resources with knowledge of how computing systems and threat actors work get involved with response. . Therefore, the quality of the response improves when EDR is combined with a managed aspect. With MDR, the business employs a group of security professionals to provide the human element to EDR systems.

With a managed endpoint security solution in place, your company's security team can devote more time to the tasks that provide the greatest return. The best available shared resources are utilized to avoid alert fatigue and better coordinate reactions to detect harmful activities.

Which one to choose? EPP, EDR, or MDR?

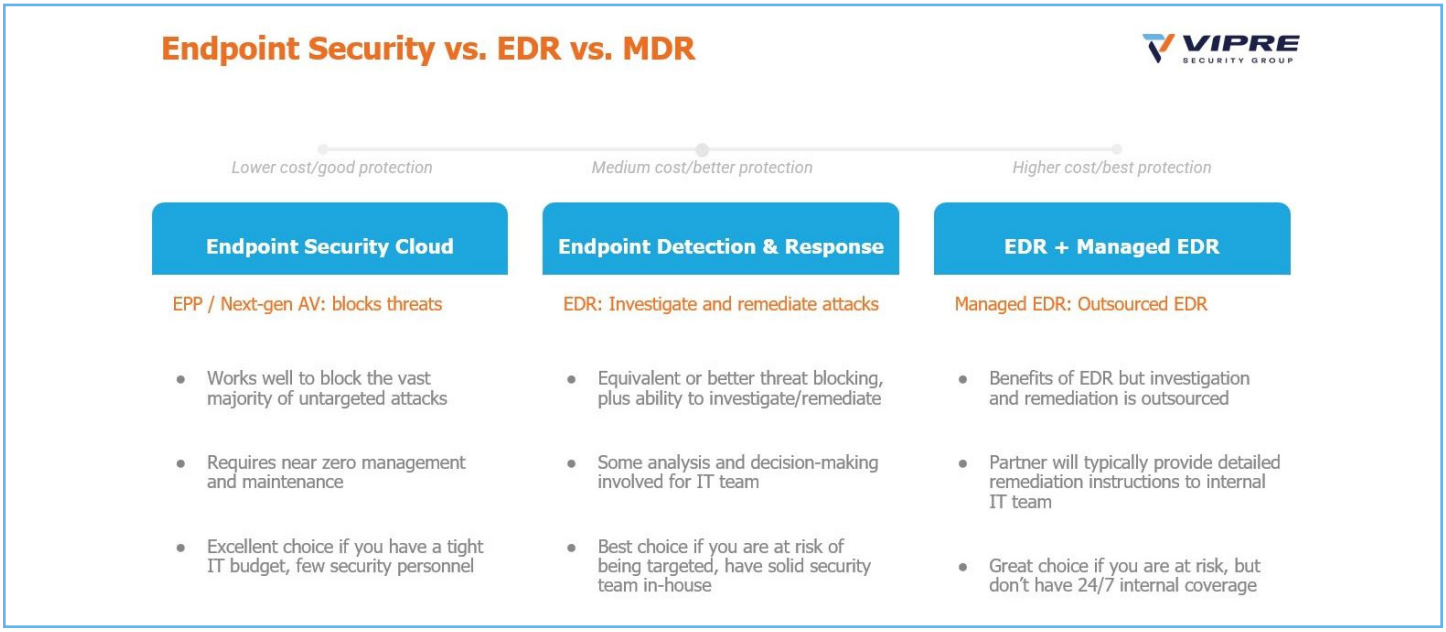
Depending on your situation, you can choose one or more of these options.

- With EPP, you can proactively safeguard your system's endpoints from the vast majority of threats without needing ongoing monitoring, and it only requires minimal management. EPP consumes fewer system and personnel resources while still providing solid protection if implemented well.

- EDR provides coverage for additional advanced threats and can detect early stage attacks that have not risen to the level of malicious action. EDR also allows organizations to investigate and respond to advanced attacks with minimal overhead, but requires some in-house expertise to manage properly.

- If you don't want to maintain an in-house cybersecurity team 24/7 but still need to keep an eye on your systems, MDR is the way to go because it can leverage shared IT security expertise and make that expertise available at all hours.. Frequently, MDR is less expensive than retaining an in-house security team (if you can even find resources to hire) since MDR providers can capitalize on shared resources and apply lessons from one customer to all other customers.

The image below provides a high-level comparison of the three options.



The need for endpoint security will persist so long as computers are in use. However, the definition would shift from enhanced perimeter protection and disaster recovery to a more hybrid and all-encompassing set of capabilities to counter the ever-evolving cyber threats. Which one you choose is up to you and is determined by factors such as the organization's risk profile, propensity for taking risks, and financial wherewithal.

Contact us today to learn more about our endpoint security tools and how they go beyond standard antivirus solutions to provide the threat protection your business needs.

6 Essential questions you need to ask your MDR provider

A fully staffed 24/7 Security Operations Center (SOC) can cost over $1 million, not including the expenses for tools such as SIEM, SOAR, and EDR that analysts use to detect threats. Therefore, to enjoy the advantages of a SOC, many small and medium-sized businesses (SMBs) opt for Managed Detection and Response (MDR) services.

MDR provides small and medium-sized businesses with a team of experts available 24/7 to monitor and prioritize alerts, keep up with the latest adversary tools, techniques, and procedures (TTPs), and promptly address any threats that may arise, among other services.

Although there are three defining characteristics, not all MDR providers are created equal. Choosing the right provider is essential to unlocking the valuable benefits of MDR. The right MDR provider identifies and—crucially—contains breaches as they happen. The wrong provider overwhelms your security team with alerts and forces them to interpret the data themselves and attempt to prevent threats independently.

Finding an MDR provider who enhances your security portfolio and delivers to expectations often comes down to knowing what questions to ask.

1. What is the breadth of threat surface coverage?

Detecting a known or new threat—and being able to respond effectively—requires coverage of the entire threat surface. With endpoints increasing in number and significance for every business, your MDR solution must protect your endpoints against malware and fileless attacks. A threat actor uses fileless malware to persist and exfiltrate data on endpoints in business environments. This malware sometimes serves as a primary attacking tool, and in others, it acts as a backup. It is, therefore, essential to recognize any suspicious or abnormal activity to prevent the lateral movement of malicious actors.

2. How do you ingest and process data?

To minimize risk, it is crucial to have extra security measures and quick reaction times. The ideal solution is a cloud-based, machine learning-powered platform supported by security experts who filter through countless daily alerts to pinpoint genuine threats and stop them before they cause harm to your business.

When considering MDR providers, inquire about their data ingestion and processing methods, as well as their technology and processes. Ask about their constant improvements and performance metrics to monitor effectiveness. Modern cybersecurity that can combat evolving threats requires efficient data processing rather than solely operating security technology.

3. How do you respond to threats?

A key differentiator among MDR providers is defining the term “response.” Unfortunately, many providers only transfer the burden of threat hunting to SMBs, who need to diagnose potential malware and understand how to remediate it.

Minimizing threat actor dwell time is paramount because skilled attackers can cause damage and exfiltrate sensitive data within a few hours. For example, LockBit ransomware can encrypt 100,000 files across various Windows operating systems and hardware specifications in just 5 minutes and 50 seconds.

To effectively respond to threats, it is vital to accurately identify events that require a response and avoid false alarms. Although no MDR solution is fully automated, it is beneficial for businesses to seek for MDR providers that automate ‘parts’ of their workflow to assist and expedite response to identified threats.

4. How do you overcome the cybersecurity talent gap?

Essentially, MDR combines advanced threat detection technologies, extensive processes to monitor and react to the signals generated and recognized by those technologies, and—most importantly—expert analysts who decide if and when a response is needed for actual attacks against customers.

Many companies who try to build an in-house SOC capability find out the hard way that operating and scaling an effective SOC requires overcoming the hurdle of cybersecurity skills shortage. With such an expanding threat surface and myriads of generated alerts, the question to seek answers to is, “How do you process all of that data?”

What programs are in place to ensure professional development and talent retention? Which tools and technologies do you invest in to improve operational effectiveness, efficiency, and human-machine collaboration in the face of ever-increasing threat signals? How do you prevent mental burnout; the number one problem cited in surveys of cybersecurity professionals?

5. How do you communicate with your customers?

When working with an MDR vendor, it’s crucial to have open and consistent communication. This includes receiving regular summary reports through a central dashboard or email so that you can stay informed about their threat detection and response activities.

Clear communication not only helps you understand your environment better but also allows you to improve your security posture. Additionally, these reports enable you to assess the quality of service you’re receiving and observe how the MDR provider responds to detected threats.

To ensure effective communication, it’s essential to ask the MDR team about their preferred method of communication, frequency of updates, and availability for support outside of business hours.

6. What about pricing plans?

Utilizing an MDR service can result in a significant ROI. However, it’s important to note that different MDR vendors charge varying rates. Some vendors offer better security and features, hence charging more, while others offer fewer features at a lower cost. It’s crucial to consider whether the lower cost option still provides sufficient features for your business needs and to be cautious of vendors that try to upsell unnecessary features. By choosing a more cost-effective option, you can save a substantial amount of money in the long term while still receiving ample protection for your business.

By teaming up with an MDR provider offering tailor-made services for small and medium-sized businesses, advanced EDR features, experienced security experts, and reasonable licensing fees, you can secure a reliable service partner to help you achieve your business objectives both in the present and in the long run. VIPRE is the vendor you are looking for. With a combined experience of 260 years, VIPRE can analyze, and respond to IT security threats that may arise in your organization.

Contact us today to learn more about our MDR services and how they provide the threat protection your business needs.

MDR vs. EDR: Choosing the Right Cybersecurity Solution

When searching for security solutions to protect your organization against cyberattacks, it can be difficult to sift through the variety of options and determine which would be the most helpful for your needs.

A solution can be top-of-the-line and exceedingly effective at what it aims to do, and still not be the right choice for you. It is important to do the research, read up on the pros and cons of each option, and understand what a given solution does and does not do, before deciding to implement it as part of your cybersecurity strategy.

Defining EDR and MDR

Endpoint detection and response (EDR) solutions are commonly used by businesses and growing even more popular and for good reason. With an increase in affordable EDR solutions and a push towards more complex tools than traditional antivirus software, more and more organizations are able to implement EDR to protect their assets and data against cyberattacks. Many EDR solutions come with a wide range of standard and optional features, but the basic function of an EDR tool is to detect potential threats and security incidents at the endpoint and aid in the investigation and remediation of events that are deemed risky.

Managed detection and response (MDR) services are designed to take the protection of EDR software and add the use of external security experts for incident investigation and response. Cybersecurity expertise is in short supply these days, and even if it can be found, it is often too costly for a business, especially a smaller one, to employ in-house cybersecurity experts to respond to potential threats flagged by EDR software. MDR solutions allow the same experts to use their combined skills to help many companies, their shared experience, and insights from helping other companies compounding so that an outsourced security team can address and remediate risks to your organization.

Key Differences and Pros of MDR

The primary difference between EDR and MDR is in the investigation and remediation of potential security incidents. EDR will catch events that look risky at the enterprise endpoint and block actions, alert users, or otherwise respond to stop a potential attack. It can also help to ensure compliance with regulations and may return fewer false positives than more rudimentary solutions.

However, it is down to the organization to employ the experts necessary to thoroughly respond to and adequately remediate any security incidents. Many organizations lack the funds and other resources to employ these experts in-house, and still more companies may have a hard time even finding cybersecurity experts to employ. MDR solutions, on the other hand, provide many of the same benefits as other security tools, including EDR, plus the benefit of a security-as-a-service solution that takes the responsibility for cybersecurity expertise and remediation off the shoulders of the organization. These solutions often use the same technology that is included in EDR software, the AI power that enables fairly accurate threat detection, as well as third-party human security experts to detect, find, identify, investigate, remediate, and analyze security incidents. Different solutions also offer different features that may appeal to certain organizations, such as the option to have the vendor's security team help the in-house IT team through remediation.

Understanding the MDR Vendor Landscape

In order to be sure that you are getting the best solution for your organization, it is vital to understand the range of solutions, tools, and services on the market. Many security-oriented companies are attempting to establish themselves as MDR providers in addition to their other products and services, but not all security firms are adequately equipped to handle every responsibility that goes into MDR. Managed security service providers (MSSPs) may be good at managing firewalls and VPNs, but lack the capacity for threat hunting, incident response, and remediation.

In comparison, many vendors of EDR and security information and event management (SIEM) solutions offer optional features in their products that enable customized detection and response, but the product-focused approach necessarily limits their ability to provide the required response and remediation. Organizations seeking an effective MDR service should be clear on what MDR can, and should do, as well as what they specifically want out of it. If you favor the proactive approach of a third-party service provider combining technology and human expertise for incident response and remediation, MDR may be the right choice.

It is crucial for businesses to be aware of the security solutions they need, which products and services are available to meet these needs, and how effective are these solutions at solving the needs. 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, and the variety of features offered by different security providers. Certain MDR providers may be more or less equipped to handle different parts of the process of incident response and remediation. With a combined experience of 260 years, VIPRE can analyze and respond to IT security threats that may arise in your organization.

VIPRE SECURITY GROUP

ABSI Technology