Why Managed Detection and Response (MDR) Is Essential for Modern Cyber Security

What are the biggest cyber security problems that organizations face?

What are the biggest cyber security problems that organizations face?

First, most organizations have limited budgets. The majority of their spending is dominated by firewalls, endpoint security, and network security. As a result, security teams are left with fewer resources and are overwhelmed by daily alerts, leaving little time to create strategic initiatives or hunt for new threats.

Second, even if an organization has the budget needed for security operations, they are still facing the challenge of being understaffed during a severe labor and skills shortage. Worldwide, the cyber workforce shortfall is approximately 3.5 million people.[1]

Third, the attack surface is constantly expanding while threats are becoming more sophisticated. This ever-growing complexity can delay your response to threats and result in missed attacks.

What's the solution?

To fill the threat detection and response gap, organizations are investing in Managed Detection and Response (MDR) solutions.

[1] Karen Scarfone, "Cybersecurity skills gap: Why it exists and how to address it," The Tech Target, 2022.

What is Managed Detection and Response (MDR)?

Does your company struggle with personnel limitations or a lack of expertise? Is your current security program slow to detect threats or remove advanced advanced persistent threats (APTs) that have infiltrated your network?

Managed Detection and Response (MDR) has emerged in response to the problems stated above. MDR is a service that helps organizations detect, respond, and monitor threats across their entire perimeter without having to expend on additional staffing.

Large enterprises may be able to fully staff and resource a dedicated security team, but many other companies struggle to achieve this. MDR providers aim to alleviate this problem by providing highly trained security experts as a service while monitoring your entire IT infrastructure 24/7.

An MDR service typically provides several core features:

- **Incident Investigation.** MDR providers will investigate alerts and determine what actions to take. This is achieved through a combination of artificial intelligence and machine learning.
- **Alert Triage:** Security incidents have different priorities, and a variety of factors can impact the priority of an incident. An MDR provider will prioritize the list of security incidents, handling the most critical one first.
- **Remeditation:** An MDR provider will remove the threat and return the affected site to a known good state.
- **Proactive Threat Hunting:** Detecting hidden, advanced attacks requires a more proactive approach. MDRs will proactively search a company's network for signs of an infection and remediate it if detected.

Why do organizations need MDR?

Organizations need to minimize the time to respond to incidents, without expending additional resources on staffing. In addition, all threat surfaces need to be covered 24x7, including the network, endpoint, email, and more – while leveraging powerful threat intelligence and AI technologies. This is exactly what the modern MDR solution achieves, and it's even more relevant to budget-constrained SMBs.

There are several other reasons why an organization should consider Managed Detection and Response (MDR):

- Security teams are overhwlmed with daily alerts and incidents.
- They struggle with configuring their security technologies, which is made more difficult because companies resort to using an endless number of point solutions instead of a consolidated security architecture.
- Companies lack the expertise and resources needed to remediate security incidents.
- It takes time to build out a mature security program – from hiring the right security team and defining policies, to implementing security technologies and creating standard operating procedures, this entire process can take years to unfold.
- Finding and hiring security talent, especially during the current shortage, is difficult.

By 2025, Gartner predicts that 50% of organizations will use MDR solutions for threat monitoring, detection and response functions. MDR adoption is increasing among businesses who want experienced security teams that can provide 24x7 threat detection and response.

If your organization hasn't adopted an MDR solution or is considering it, then now is the time to get started.

What should you look for in an MDR provider?

The ideal MDR solution should focus on prevention first, not detection. When a cyber attack breaches your network, it's too late. Second, it should be easy to onboard and simple to integrate into your existing security stack and ecosystem. Finally, it should lower your SOC investment and overhead: eliminating the purchasing of tools, integration, recruiting, training, and staffing.

In addition, your MDR solution should possess the following capabilities:

- An easy-to-use, intuitive web portal for complete transparency to service activities
- AI technologies that continuously update your threat intelligence
- Recommendations such as changing passwords and updating configuration
- 24x7x365 monitoring across your entire IT infrastructure
- Remediation across all attack vectors while providing customers with recommended prevention measures and best practices
- Complete security orchestration to ensure full analysis, response, and remediation across your environment

Fortunately, there is a tool that possesses all these capabilities.

Check Point Horizon MDR is the first prevention-focused MDR solution – complete and powerful SOC operations delivered as a service

Check Point Horizon MDR's key value is that it helps you achieve 24x7 threat monitoring and prevention without requiring you to expend more on analysts or tools.

Check Point's Managed Detection and Response (MDR) service is powered by the industry's top experts and leading AI technology to proactively prevent, monitor, detect, and remediate attacks across customers' environments. It covers the entire infrastructure using the most advanced ThreatCloud threat intelligence. Furthermore, you gain the highest level of protection wth security operation services led by the industry's top analysts.

If you want operational peace of mind, then you've got it. Avoid SOC overhead with simple, response, and transparent security operations as-a-service. Avoid the overhead of recruiting and training in-house analysts and staffing 24x7 shifts by relying on Check Point's highly-experiecned security operations team.

This is one of the most exciting and revolutionary solutions that the cyber security industry has seen in the last decade.

To learn more about Check Point's MDR service, visit our website, or talk to sales.

Worldwide Headquarters
5 Ha'Solelim Street, Tel Aviv 67897, Israel | Tel: 972-3-753-4555 | Fax: 972-3-624-1100 | Email: info@checkpoint.com

U.S. Headquarters
959 Skyway Road, Suite 300, San Carlos, CA 94070 | Tel: 800-429-4391; 650-628-2000 | Fax: 650-654-4233

www.checkpoint.com