Infosys®
Navigate your next

VIEW POINT

# EFFECTIVE CYBERDEFENSE THROUGH MDR SERVICES

Security is changing. Managed security services are no longer adequate to fight the battle against cyberthreats. Managed detection and response services are better suited for outsourced staffing and expertise, detection, response and 24/7 monitoring.

Infosys® | Knowledge Institute

## Effective cyberdefense through MDR services

Cyberattacks continue to grow in scale and sophistication every day. On average it takes around 200 days to detect a breach. [1] All things considered, a breach can become a multimillion-dollar problem for the affected business. In 2019, the World Economic Forum reported that cyberrisks are consolidating their position alongside environmental risks in the high-impact, high-likelihood quadrant of the global risks landscape. [2] The global loss from cyberattacks in 2018 totaled $1.5 trillion; in 2019 this amount could rise to $2.5 trillion. [3]

Cybercriminals are powerful, difficult to identify and capable of constantly developing new ways to penetrate secured systems. To effectively repel attacks, security teams must undergo continuous training and be able to access the latest solutions and tools. But keeping pace with offenders is difficult and expensive. Adopting new technology and ensuring timely implementation is a major challenge. Often tools become obsolete by the time they are implemented. Moreover, a company may lack sufficient funds to acquire new tools, and even if it has funds, it might lack the skilled personnel needed to operate these tools.

## Lack of skilled talent

The deficit in cybersecurity talent is a major concern. Finding the right IT and computer science professionals is challenging because the global cybersecurity workforce will have 1.8 million unfilled positions by 2022. [4] In particular, there is a significant lack of skills in the areas of analytics, intelligence, rapid response to incidents and investigation. There is also a lack of technical skills for work with security operation centers. We are no longer in the era where a business can be protected by a firewall alone. The skills discussed here are relevant for the new types of threats, and MDR services can fill in the gaps of personnel.

## Stringent regulations

Constantly changing regulations are also making cybersecurity more complex. The best known such regulation is the General Data Protection Regulation (GDPR). Businesses that operate in the European Union (EU) or offer goods or services to individuals located in the EU must comply with the GDPR, which went into effect May 25, 2018. Every such business is legally required to be compliant with GDPR as it protects online spaces and systems against criminal activities that threaten the loss of data and money. Under the GDPR, personal data breach notifications became obligatory. Once data processors identify a breach, companies must notify those whose data was breached "without undue delay," and in no case not more than 72 hours after the company becomes aware of the breach. [5] Stringent regulations are difficult to comply with, especially if an entity does not have the capabilities to detect, address and mitigate the threats.

## Security awareness

Apart from the lack of skilled talent and stringent regulations, poor security awareness is also a problem. In March 2019, Infosys surveyed 867 senior executives and leaders involved in cybersecurity initiatives and found that their top security concerns included low awareness in organizations, corporate espionage and insider threats.

Cyberattacks pose serious risk to organizations. One problem is that many business people may not believe that hackers will target their organization. They may believe that their organization is too small to be on the radar of the criminals or that it has nothing worth attacking. It is important to understand that losses incurred by companies from data breaches are not limited to money. Reputational losses, customer outflows and network restoration work can lead to much larger consequences. The truth is that malicious actors tend to be indiscriminate in their attacks and can almost always find something of value to target. In many cases, enterprises don't even know they have been breached.

For example, the following three hacks involved delayed breach detection and show how this can be an issue even for the largest brands.

## The Yahoo Hack of 2013-2016

The Yahoo hack is considered to be the biggest known data breach of a company's computer network in history. Hackers broke into Yahoo in 2013, but the company only uncovered the breach in 2016. The breach affected all 3 billion accounts that existed in 2013. Digital thieves were able to access personal data such as first and last names, dates of birth, email addresses, phone numbers and passwords.

## The Marriott International Hack of 2014-2018

In 2018, the international hotel chain Marriott announced a massive data breach affecting half a billion people. In mid-September 2018, Marriott staff discovered an attempt to gain unauthorized access to the Starwood reservation system base. The investigation that followed revealed that penetration into the system occurred back in 2014, that is, two years before Marriott acquired Starwood. The data of 327 million Starwood guests was stolen, including

their names, postal addresses, birthdates, phone numbers, passport details and account information, as well as data on preferred methods of communication. For other users, only names, emails and email addresses were considered compromised.

## The Equifax Hack of 2017

In 2017, Equifax, one of the world's largest credit bureaus, said their database had been hacked, causing personal information of more than 143 million people to be compromised. Hackers gained access to social security numbers, birthdates, consumer names, driver's license numbers and credit card information. The attack was detected at the end of July 2017, but hackers had penetrated the company's servers in May of the same year. [6]

These recent big hacks demonstrate how easily cybercriminals can bypass cybersecurity and remain undetected for months. Times are changing, and having merely preventive measures is no longer enough. An entirely new approach to cybersecurity is necessary.

All the factors combined make for a complex security landscape. Cybersecurity is a vast area that requires various sets of skills to deal with access management, government risk and compliance, data security, security monitoring, incident response and others. Often, in-house security teams lack relevant expertise in constantly evolving tools and spend a lot of time dealing with large volumes of log data. They struggle with managing systems and tools, and have little time to thoroughly investigate and analyze an incident. But there are external services that can provide the necessary support.

## Security solutions

In the last couple of years, MDR has emerged as a new approach to information security. MDR programs are specialized, outsourced security services that are focused on 24/7 service for threat detection, response, and remediation. Compared to managed security services, MDR services can detect known and unknown threats. They can go beyond sending alerts and actually respond to threats as they happen, providing endpoint detection and response solutions. Unlike MSS, which can detect only known incidents, MDR providers can detect and prevent even complex targeted attacks.

## What challenges does MDR solve?

Quality MDR services effectively eliminate false alarms, detect real security threats and develop an incident response in real-time. While the average time for detection of a breach is close to 200 days, MDR services allow faster threat detection and response. One of the components, which allows MDR services to respond faster to potential incidents and to detect attacks that have gone unnoticed, is endpoint detection and response solution (EDR).

A 2019 Infosys survey found that the most common requests from clients are "end-to-end cybersecurity and protection" as well as the ability to "assess, build, and manage cybersecurity capabilities that enable a response to incidents." Often EDR solutions do not reach their maximum potential due to a lack of time, skills and expertise in handling the EDR tools. Advanced EDR tools form the core of MDR services and play a critical role in detection, analysis and response functions.

EDR tools are "the tools primarily focused on detecting and investigating suspicious activities (and traces of such) other problems on hosts/endpoints." [7] Any end-user device such as a laptop or a server is an endpoint.

Thousands of devices and endpoints generate millions of log events and data. Using EDR tools, MDR providers are able to analyse this data and detect threats early. The advanced analytics engine normalizes and co-relates this data and identifies security offenses requiring investigation, filtering them down to a critical few. Once it is done, the analysts prioritise the critical alerts for immediate action.

In addition, MDR services address the challenges arising from the lack of security skills within organizations. While some organizations can afford upskilling and the creation of an SOC to conduct full-time threat hunting, the majority of businesses face resource constraints and look for alternative solutions. This is a problem even for medium-sized and large enterprises, which often suffer from cyberattacks but lack the capabilities and manpower to provide an effective response to the hackers.

MDR services reduce the dependency on the security skills by providing automated incident responses. When the detected incidents engage the incident response platform, the platform determines all the characteristics associated with the incidents. Then it builds the incident specific response plan. Based on the configured plan MDR services can detect advanced threats and initiate response. MDR services consequently minimize the damage that breaches can have on security systems.

## What are the main differences between MDR Services and MSS?

There are two main things to look at. First, traditional MSS provides standard security monitoring such as threat monitoring, compliance, reporting and incident response services. MDR services expand this by also bringing EDR as well as threat containment, research and managed threat hunting. (See Figure 1)

Figure 1. Differences between MDR Services and MSS

| | MDR | MSS |
|---|---|---|
| Detects known (signature-based) threats | Yes | Yes |
| Detects unknown threats | Yes | No |
| Analyzes log threats and provides incident response | Yes | Yes |
| 24/7 monitoring by a staffed security operations center | Yes | Yes |
| Purpose-built technology for signal enrichment and event correlation to reduce false positives | Yes | No |
| Provides threat research | Yes | No |
| Provides tech stack (EDR, deception, etc.) | Yes | No |
| Provides threat containment | Yes | No |

Source: Infosys

MSS is a predecessor of MDR services. The most active MSS providers track security events and send alert messages if anomalies are detected. These services don't investigate the anomalies for elimination of false positives, i.e., something mistakenly called an error, and they don't actively react to security threats. However, some MSS providers do offer other network services like virus protection and firewall management.

MDR services don't simply provide threat notifications — for example, they respond and contain threats by shutting down ports or changing VLANs. MSS services don't include the endpoint. They simply notify their users or, at most, make changes to managed equipment. MSS services manage the tools and alert the users, while MDR services collect data from tools and endpoints. This allows MDR providers to determine whether a company can be or has been breached.

Overall, MSS providers help concentrate investigation efforts, leaving it up to a company to decide whether or not to perform the actual investigation, to prepare responses and to eliminate false positives. MDR providers, on the other hand, offer IT security service with reduced time for threat detection. They combine a technological solution with outsourced human security analysts. The expert team usually includes forensic analysts, experienced security professionals, incident respondents, threat hunters and others. MDR services detect intrusions, malicious activity and malware in a network. They help to react fast to eliminate and mitigate threats.

## Evaluating MDR services is critical

Reliable data protection, IT infrastructure security, stable business processes and compliance with regulations are mandatory conditions for the sustainable development of modern businesses. Businesses grow more dependent on information technologies when they try to automate corporate processes.

*When an organization integrates more IT into its systems, its risk of being hacked increases.*

Companies require an experienced team of specialists to manage threats and provide an appropriate response to guarantee secure operation of the IT systems. Without such expertise and staff, companies' cybersecurity teams often struggle with managing systems and tools, leaving little time to thoroughly investigate and analyze incidents.

It is critical for any organization with sensitive information that might be attractive to cybercriminals, to have an effective response to attempted hacks. Because the nature of their businesses makes their information high-value targets for cybercriminals, health and financial services providers are the most obvious organizations in need of effective detection and response services. These organizations often lack complete, functional SOCs and struggle with recruiting and retaining on-demand cybersecurity professionals.

The skills that are relevant to the new types of cyberthreats are going to be difficult to build in-house. The demand for qualified cybersecurity professionals, threat readiness, GDPR compliance and 24/7 monitoring will drive more outsourced players into offering MDR services. Corporations that understand the value of MDR will be best positioned to evaluate MDR suppliers and their capabilities.

## References


1. "An Insight Into the Dark Side of Cyber World," Infosys, 2019, www.infosys.com/services/cyber-security/insights/Documents/insight-dark-sight-cyber-world.pdf
2. "The Global Risks Report 2019 (14th ed.)" World Economic Forum, January 2019 http://www3.weforum.org/docs/WEF_Global_Risks_Report_2019.pdf
3. "Threat Zone '19: False Sense of Cybersecurity," Bi.Zone, 2019, https://bi.zone/research/threat_zone_2019/
4. "Global Cybersecurity Workforce Shortage to Reach 1.8 Million as Threats Loom Larger and Stakes Rise Higher," (ISC)2, June 2017, https://www.isc2.org/News-and-Events/Press-Room/Posts/2017/06/07/2017-06-07-Workforce-Shortage
5. Council Regulation (EC) 2016/679 General Data Protection Regulation OJ L 119, Art 33(1)
6. "The 18 Biggest Data Breaches of the 21st Century," CSO, 2018 https://www.csoonline.com/article/2130877/the-biggest-data-breaches-of-the-21st-century.html
7. "Named: Endpoint Threat Detection & Response," by Anton Chuvakin, Gartner Blog Network, 2013, https://blogs.gartner.com/anton-chuvakin/2013/07/26/named-endpoint-threat-detection-response/


## Authors


**Yulia De Bari**

*Consultant – Infosys Knowledge Institute*
Yulia.Debari@infosys.com

**Lakshminarayanan RS**

*Senior Delivery Manager – Cyber Security*
Rajaram.Narayanan@infosys.com

**Manish K Sehrawat**

*Principal Consultant – Cyber Security*
ManishKumar02@infosys.com

## About Infosys Knowledge Institute

The Infosys Knowledge Institute helps industry leaders develop a deeper understanding of business and technology trends through compelling thought leadership. Our researchers and subject matter experts provide a fact base that aids decision making on critical business and technology issues.
To view our research, visit Infosys Knowledge Institute at infosys.com/IKI

For more information, contact askus@infosys.com

Infosys®
Navigate your next