Businesses Need the Added Protection of Managed Detection and Response (MDR) Services

MDR provides ready-to-use detection and immediate, client-side, intervention and containment services

Contents

About the authors

Maxine Holt

Maxine leads Ovum's security proposition, developing a comprehensive research program in this area to support vendor, service provider, and enterprise clients. Having worked with enterprises across multiple industries in the world of information security, Maxine has a strong understanding of the challenges faced and how organizations can look to overcome these challenges.

Andrew Kellet

Andrew Kellett is a former Principal Analyst with Ovum, now working with the company as an Associate. Andrew continues to cover various aspects of cybersecurity.

Summary

In brief

Security threats continue to rise, and a rapidly evolving range of cyberattacks is putting the data of businesses and their customers at increasingly unacceptable levels of risk.

Ovum research shows that many cybersecurity incidents and breaches happen because processes are broken, technology is outdated, and individuals are untrained. Less than 15% of organizations have a proactive approach to cybersecurity and digital risk; they simply do not have the tools in place to keep business systems safe.

Managed detection and response (MDR) services are available to identify, analyze, and respond to the types of cyberthreat that traditional security defenses miss. Efficiencies and cost savings are provided through the use of automated artificial intelligence (AI) and machine learning (ML) techniques. The proficient use of these tools can help improve the accuracy of threat detection and assist security analysts in disrupting attacks before problems occur.

Ovum view

Security for business systems and users starts with data protection. Organizations used to rely on signature-based approaches to keep their business systems safe. However, as the effectiveness of traditional protection products continues to decline – a trend Ovum sees as permanent and irreversible – modern, more responsive approaches are needed.

The security industry has moved on from promising threat prevention. It now offers layered protection through detection and response, which includes a backstop for the identification of previously undetected breaches, with the promise of early identification and remediation.

Early threat identification and the use of automated intelligence-gathering analysis techniques are now vital requirements, but in isolation are not enough. The protection package has to include actionable response and remediation capabilities that combine the use of technology and process with the people skills needed to ensure that business and user protection remains the priority.

The premise of MDR is to help organizations deal with the increasing complexity of security and IT systems and the millions of digital interactions that take place each day across business systems and networks. It is a services-led approach, where leading providers offer a combination of technology and analyst expertise via a security operations center (SOC). The technology is needed to identify threats and breaches as they occur. Human expertise and ownership of the problem is required to ensure that the correct fixes are applied as quickly as possible.

To achieve its set objectives, MDR must offer a nothing-left-out approach to business and data protection. It must have the capacity to analyze all available data, to highlight, prioritize, and disrupt threats that are relevant to the business, and, where necessary, to address response and remediation requirements.

Key messages

- Businesses must think about risk and regulatory issues when shaping protection requirements.
- Consider the benefits of MDR as a core component of organizational security strategy.
- There are strong reasons for choosing an integrated and inclusive MDR platform.

Businesses must think about risk and regulatory issues when shaping protection requirements

All IT systems are potential targets for cyberattack. Regulatory demands put extra pressure on security teams to improve protection, as well as directing enterprises toward the levels of business and data protection they must achieve in order to remain compliant. The financial and reputational damage that a cybersecurity breach can do to a business and the crippling regulatory fines that are likely to follow have forced cybersecurity onto the boardroom agenda and are driving the demand for better levels of protection.

The EU General Data Protection Regulation (GDPR), which came into force in May 2018, affects all EU and UK businesses as well as external businesses that have trading relationships with EU-based organizations. There are already plenty of examples of organizations failing in their GDPR obligations, and fines are being imposed. Noncompliance can be penalized at the highest levels by fines of 4% of global revenues or €20m, which represent a serious impact to any enterprise.

The Networks and Information Systems (NIS) Directive has been developed to improve EU countries' preparedness for a cyberattack. Again, the fines for noncompliance are potentially stringently high, as the relevant Competent Authority has the authority to level substantial financial penalties if necessary. These, along with global regulations such as the Payment Card Industry Data Security Standard (PCI DSS), provide multiple reasons why boards and senior executives can no longer avoid taking responsibility for the business impact of cybersecurity breaches.

Recent high-profile cybersecurity breaches that have been reported by UK organizations include:

- British Airways (BA), where, during a two-week window, hackers were able to get hold of the personal and financial details of customers who used the company website ba.com. Names, email addresses and credit card information from around 380,000 transactions were put at risk – including card numbers, expiration dates, and the three-digit CVC codes required to authorize payments.
- Dixons Carphone, the owner of Currys PC World and Carphone Warehouse, found that a number of its systems had been breached. The firm initially thought that 1.2 million personal data records were involved, including customer names, emails, and addresses. Subsequent cyberbreach investigations found that 5.9 million customer bank card details and 10 million personal data records were put at risk.
- The Marriott hotel group suffered the potentially largest breach in the UK, as systems containing up to 500 million guest details were found to be at risk. The attack affected systems managing its Starwood portfolio, which included Trump Turnberry in Ayrshire as well as Sheraton Grand London Park Lane, The Westbury Mayfair, and Le Meridien Piccadilly in London. Information including passport numbers, dates of birth, names, addresses, and phone numbers were contained in the database, which was originally attacked back in 2014, with the failure only coming to light in 2018.

Attacks on business systems come in many different forms, from the sophisticated, relatively short-lived, two-week attack suffered by BA to the four-year, under-the-radar data theft at Marriott. Business impact can also be longstanding and problematic, as was the case with the 2014 insider breach at the UK's fourth-largest supermarket group Morrisons, where thousands of staff records were stolen and published online by a coworker. Four years later, the legal ramifications in the high court continue.

Security threats will not disappear anytime soon

To improve business and data protection, organizations and their security teams need more threat visibility, better security management, and greater levels of accountability and control from the products and services they deploy.

The frequency of cybersecurity breaches is forcing organizations to change their protection strategies. Old-style perimeter and siloed approaches miss too much and rarely address other areas of weakness such as insider threats, accidental misuse, configuration errors, and software flaws that sit beyond their remit. The situation is further aggravated by the complexity and connectivity requirements of everyday systems, which make it impossible to simply lock everything down.

The reality is that cybersecurity incidents and breaches are not being prevented. The UK government–sponsored Cyber Security Breaches Survey 2019 identifies that cyberattacks are a persistent threat to private and public sector businesses and charities. It found that about a third (32%) of businesses and just over a fifth (22%) of charities have reported cybersecurity breaches or attacks in the last 12 months. As in previous years, these figures are much higher among larger businesses (around 60%) and high-income charities (52%).

For the 32% of businesses recording breaches or attacks, there was a negative outcome, such as a loss of data or assets, in 30% of cases. For the affected organizations, the average initial incident cost, which covered damage to equipment and lost revenue and data, was said to be £4,180, a significant increase on last year, at £3,160, and 2017, at £2,450. This indicates a trend of rising costs in cases where cyberattacks are able to penetrate an organization's defenses, and includes higher incident costs for medium-sized to large firms of between £9,270 and £22,700.

However, these are just the basic security breach costs. They do not take into account much more expensive issues, such as breach investigation costs, security update requirements, training overheads, PR and brand damage, insurance and legal costs, responsibility for losses incurred by customers and business partners, and fines from regulators. Taking all of these factors into consideration, the 2018 Cost of a Data Breach Study from the Ponemon Institute put the global average security breach cost at £3m. The UK figure was said to be slightly lower, at £2.7m, but US companies reported the highest breach costs, at £6m.

The report also identified that the average time taken to identify a breach had only dropped by five days in the last year (it currently stands at 163 days), and the time taken to contain a breach had only dropped by three days (to 64 days). These are important numbers, because the longer a breach is active, the more damage it can cause and the more expensive it will be to fix. To put this into context, industry figures from IBM claim that businesses that were able to identify and contain a breach in under 30 days saved on average around £755,000 compared to those who took longer.

More action is needed from senior management

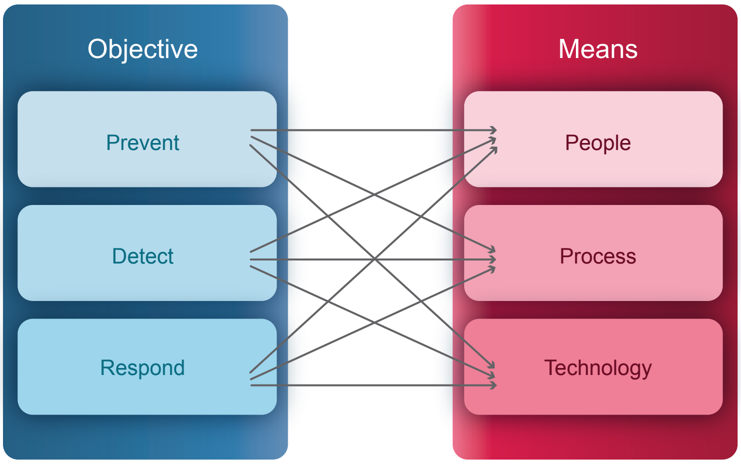
Despite over three quarters (78%) of organizations stating that cybersecurity is a high priority for their senior management, only about a third of businesses (35%) have a board member or trustee with specific responsibility for cybersecurity. This is slightly higher than the figure for last year, which was 30%, but the overall proportion remains far too low.

The future protection mindset has to include a backstop position of detect, identify impact, then respond and remediate. Therefore, as the efficacy of traditional security products continues to decline, better, intelligence-led alternatives are needed.

Accepting that guaranteed protection is unrealistic forces organizations to consider the best breach detection options available and, at the same time, highlights the need for early identification and rapid remediation. Becoming more aware of the threats involved and understanding their realities helps determine the security controls that each organization must have.

However, it continues to be the case that businesses cannot expect to defend themselves through the use of technology alone. Security controls must extend beyond technology to include people skills and insight into business processes and likely vulnerabilities (see Figure 1).

Figure 1: Security controls objectives and means of delivery



Source: Ovum

The objective of enterprise security control is to minimize the risk of a cyberthreat causing damage to an organization. From a protection perspective, this includes data, information, applications, systems, and devices.

A commonly heard complaint when working with legacy protect-and-block approaches is "alert fatigue." Information overkill ensures that all identified issues are reported, but without enough focus being placed on the threat relevance or the protection priorities of the business itself. This is helping drive the "shift right" from protection in isolation to a strong combination of intelligence-led threat detection, identification, and response approaches. The focus has to be on filtering out unhelpful noise and prioritizing threats that, if left unresolved, are likely to cause the most damage.

The lack of skills and availability in the security workforce needs to be addressed

The shortfall of available security resources and skills, associated recruitment and retention issues, and rapidly increasing costs are problems that businesses of all sizes struggle with. Organizations across all sectors are challenged by the problem of recruiting and retaining skilled cybersecurity staff. Reliable industry reports from ISC2 show the number of vacant security positions globally to be just short of 3 million.

The Europe, Middle East, and Africa (EMEA) shortfall is close to 150,000, and this figure is forecast to more than double to 350,000 by 2022. Tech UK, the trade association for UK digital industries, reports that the UK in particular already has an extreme problem with the lack of available security resources. 54% of organizations are understaffed, and the demand for cybersecurity staff is already outstripping supply by a ratio of three to one. This position is likely to deteriorate further, as the number of students looking to attain cybersecurity qualifications continued to decline in the last year. Tech UK estimates that the cybersecurity skills shortfall and unfilled roles are currently costing UK business an additional £2bn a year in cybersecurity losses.

There are managed service opportunities available to make more efficient use of technology, automation, and security intelligence to help overcome some of the human capital shortfall. Nonetheless, increasing security automation will not remove the need for skilled people and human interventions.

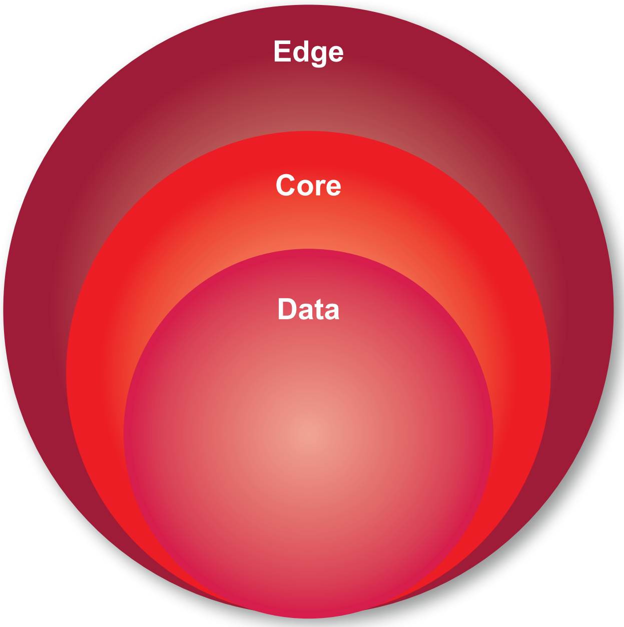
The best possible approaches depend on achieving the right balance of technology and human capital. Again, this cannot simply be a predefined set of one-size-fits-all measures; it must be a good fit for each organization, its available resources, and its security budget. Therefore, any suggested use of managed security services has to offer the benefits of a skilled technology provider and the human expertise it can make available.

Consider the benefits of MDR as a core component of organizational security strategy

Despite the known problems for security managers of legacy security systems, very few are willing to dispense with the comfort blanket of protection that these systems still provide, often because of the considerable financial investments made. Most are now looking for the added protection of a security detection approach that can be relied upon to identify attacks and threats that have bypassed existing security controls and that can also offer response and remediation services that keep business systems and their users safe.

Managed detection and response combines endpoint and network (including cloud) detection and response, log data analysis, and a comprehensive people, process, and technology approach (see Figure 2).

Figure 2: MDR components



Endpoint/mobile device

Endpoint detection and response **(EDR)**

Network (including cloud)

Network detection and response **(NDR)** – also known as network traffic analysis **(NTA)**

People, process, technology

Combining people, process, and technology enables comprehensive **response** capabilities within MDR

Log data

Analysis of **log data** adds layers of understanding to MDR

Source: Ovum

MDR is a managed security service that offers 24x7 intelligence-led cyberthreat monitoring, detection, and response services. It is offered by specialist MDR providers as well as some managed security service providers (MSSPs), which position the technology as a component of their overall service delivery stack.

The difficulties with the componentized approach to MDR that MSSPs bring to the table are twofold. Their management and service delivery approach, which in all probability would be an extension of their overall security management model, is likely to pass triage, analysis, and associated recovery responsibilities back to the client's own security team. Also, where threat recovery, correction, and response facilities are available, they are often delivered as additional and chargeable services.

In comparison, fully supported and maintained MDR looks to offer holistic threat monitoring and breach detection and identification services, as well as assisted response and remediation facilities. It uses a combination of automated, intelligence-based security tools – AI-based advanced analytics. These are enhanced by the human expertise of the MDR provider's security analysts, who offer assistance during time-critical incident response investigations. MDR support services can help with incident and breach investigations, provide thought leadership validation, and take ownership of threat remediation and containment activities.

The combination of AI-based automation and specialist support services in MDR is used to help combat the security skills shortfall that most organizations already struggle to address. It can offer the type of focused threat intelligence that security teams need to make the best use possible of available resources.

Taking the MSSP route is not the only available option

When considering a business's security protection requirements and the opportunities available to work with an external security partner, the first port of call has often been an MSSP. Without doubt, there is value to be gained from an MSSP partnership approach, especially for larger organizations with the security resources and structures in place to manage the relationship and deal with the security event monitoring and reporting services on offer. However, the question that needs to be asked is about management and support expectations and the levels of service that the MSSP is prepared to provide as part of its standard package, without generating additional charges.

Organizations that do not have previous experience of the intricacies of threat detection and response or the processes and people available to manage the relationship are more likely to struggle to gain value from the full MSSP experience. As an alternative, a balanced MDR threat detection and containment/remediation strategy can provide practical, targeted protection that can be aligned with the specific requirements of the organization and the threats it has to address.

MDR should not be seen as an unchallengeable panacea for threat detection. It currently occupies a position in the security market that traditional security products and MSSPs are not addressing well enough. So, when selecting an MDR provider, it is important to ensure that the right mix of technology and supporting expertise is available.

The ability to prioritize and respond to threats is an important MDR differentiator

Most MDR providers offer threat monitoring, detection, and alerting services. Ovum research reveals that client organizations are looking for more. The greater challenge for MDR providers is to deliver equally well on both the detection and response sides of the equation, taking responsibility for delivering threat detection and remediation services that add value and context. Furthermore, these services must be supportable by a combination of the service provider's expertise and the client's available security resources.

For small to medium-sized enterprises (SMEs), the MDR value proposition is liable to be driven by the automated threat identification and detection facilities, plus a reliance on the skills that the service provider can make available when threat and breach responses are urgently required.

It is often argued that the main difference between the MDR requirements of SMEs and larger enterprises revolves around their respective threat detection and response situations. For certain, the demand for automation and external support is going to be greater in SME environments with fewer internal resources. However, the provision of an SOC and analyst expertise by an MDR provider to remediate, respond to, and shut down unknown threats gives organizations of all sizes additional support in addressing the complex cyberthreat landscape.

There are strong reasons for choosing an integrated and inclusive MDR platform

Businesses need next-generation security solutions that genuinely improve on the way that systems and data are protected. Any additional approach must offer better levels of protection than existing legacy systems and deal with security breaches that are not currently being detected.

MDR has the tools and support services to achieve these objectives, but service providers must also have the capability to go further than the threat monitoring and identification phases and provide the comprehensive threat disruption, recovery, and remediation services that future client organizations are crying out for.

Businesses should be looking for an MDR provider that can combine threat monitoring and automated intelligence gathering with a managed detection and response strategy. The approach should include automated threat monitoring and gathering techniques, big data and behavioral analytics strategies, and SOC-based threat identification, disruption, and recovery techniques using analyst expertise.

Businesses should expect their MDR provider to offer 24x7x365 monitoring alongside full threat visibility across all operational systems and resources, including on-premises, cloud, and hybrid IT environments. It should include facilities that combine human threat-hunting skills with automated analytical detection facilities to identify known threats and discover previously unknown ones.

ABOUT OVUM

Ovum is a leading global technology research and advisory firm. Through its 180 analysts worldwide it offers expert analysis and strategic insight across the IT, telecoms, and media industries. Founded in 1985, Ovum has one of the most experienced analyst teams in the industry and is a respected source of guidance for technology business leaders, CIOs, vendors, service providers, and regulators looking for comprehensive, accurate, and insightful market data, research, and consulting. With 23 offices across six continents, Ovum offers a truly global perspective on technology and media markets and provides thousands of clients with insight including workflow tools, forecasts, surveys, market assessments, technology audits, and opinion. In 2012, Ovum was jointly named Global Analyst Firm of the Year by the IIAR.

For more details on Ovum and how we can help your company identify future trends and opportunities, please contact us at marketingdepartment@ovum.com or visit www.ovum.informa.com. To hear more from our analyst team join our Analyst Community group on LinkedIn www.linkedin.com/company/ovum and follow us on Twitter www.twitter.com/Ovum.