CISO Considerations for Managed XDR Investment

Learn how CISOs use managed services and XDR to keep pace with today's evolving threat landscape

Inside:

- Why CISOs choose to add XDR to their detection and response strategy
- How SMBs can use managed XDR to fill knowledge gaps in their own teams
- What the ROI looks like after an investment in managed XDR

Brought to you in association with:

BlackBerry Cybersecurity

Introduction

Hackers are getting smarter and cyber-attacks are continuing to grow in frequency, forcing organizations to confront huge costs when attacks are successful.

The COVID-19 pandemic has driven mass adoption of hybrid and remote work combined with a rise in bring your own device (BYOD) policies. These factors mean the risk of a cyber-attack has increased exponentially while at the same time threat actors continue to become more sophisticated.

The BlackBerry® 2022 Threat Report revealed that small and mid-sized businesses (SMBs) receive 11 to 13 threats per day, per device.

Companies of all sizes are challenged to install policies and secure data on a growing number of devices, which leads to an increased volume of alerts to be managed. All this, while balancing the skills and resources gap in IT and cyber security.

CISOs and security owners, especially those operating SMBs, face several challenges, including stretched budgets, lack of in-house resources, misconfigured security solutions and existing traditional solutions that are unable to keep pace with today's threat landscape. They must be able to optimize their existing security investments to battle the ever-evolving security threats and alert fatigue.

Protection beyond the endpoint

Extended detection and response (XDR) is the latest addition to the detection and response solution family, outlined in CS Hub's recent report, ***CISO Strategies for Proactive Threat Prevention***. The wider detection and response family includes endpoint protection platforms (EPPs), endpoint detection and response (EDR) as well as additional telemetry.

XDR is a unified security incident detection and response platform that automatically collects and correlates data across networks, clouds, endpoints and applications. This technology incorporates and evolves EPP and EDR security capabilities providing visibility across first- and third-party enterprises with protection at and beyond the endpoint.

XDR is growing in popularity and sets out a path to increase cyber security efficiency. According to Gartner's *Market Guide for Extended Detection and Response*, published in November 2021, "By year-end 2027, XDR will be used by up to 40% of end-user organizations".

Managed XDR provides a solution with specialist analysts and threat prevention experts that bolster an organization's own security and IT team's capabilities. In addition, the human element provided through managed services allows companies to access experts who can triage cyber security alerts and remediate attacks.

SMBs need to ensure they have the right software and expertise to manage the vast number of vulnerabilities that exist today. If done correctly, cyber security investments can ultimately save time, money, and reputation.

In this exclusive report, CS Hub explores the reasons many organizations are turning to XDR, CISO's top considerations before investing in XDR, and the value of managed-XDR-as-a-service.

Contents

3 How XDR extends your detection and response capabilities

4 The value in managed services

5 Embedding XDR into your digital estate

6 Conclusion

How XDR extends your detection and response capabilities

XDR expands on EDR by searching for and addressing cyberthreats across an organization's entire digital environment. XDR also looks beyond the endpoint to encompass an organization's entire network, including cloud storage, applications and its endpoints.

An XDR solution is able to unify the detection and analysis of cyberthreats that an organization is facing. It is not limited to endpoints, and therefore, is a more comprehensive solution.

XDR can more effectively ward off cyber-attacks than EDR alone by unifying visibility and management across endpoints, the network and cloud-based assets. Artificial intelligence (AI) can also be an important feature in an XDR solution in order to assist in identifying and stopping evolving cyberthreats.

The added telemetry of XDR is important for painting a more wholistic picture of threat actor activity. Parsing, normalizing and correlating data from multiple sensors provides end-to-end visibility. While moving from EDR to XDR is the correct progression in defensive capabilities, additional telemetry can increase the workload of the network defenders, notes Tony Lee, Vice President, Global Services Technical Operations at BlackBerry.

XDR is also associated with current security information and event management (SIEM) practices, which provide security operations centers (SOCs) with incident data for threat monitoring and response.

Making the switch

Some CISOs have decided to invest in XDR in order to enhance their SIEM platforms. CS Hub spoke to Ash Hunt, Group Head of Information Security at Sanne Group, an asset management services enterprise, about the company's recent adoption of XDR.

Hunt says he has very direct experience with XDR as his organization recently changed its SIEM platform by upgrading to an XDR solution.

> "The XDR piece does mature the capability from a threat perspective in a way that traditional EDR does not."
>
> **Ash Hunt**
>
> Group Head of Information Security, Sanne Group

"I certainly wanted SOAR [security orchestration, automation and response] and UEBA [user and entity behavior analytics] capabilities on my SIEM, so adding them automated orchestration and response," he explains.

"The XDR piece does mature the capability from a threat perspective in a way that traditional EDR does not. And EDR is a fantastic capability, but it is sort of binary; it's going to do what it needs to do," Hunt continues. "But XDR, particularly for my SIEM platform, takes logging and monitoring to the next level. It gives me the ability to manage my threat landscape in a way that traditional EDR quite does not do on its own."

While XDR does not set out to replace EDR, there are clear additions that it can provide to a CISO's toolkit in order for them to keep pace with today's evolving threat landscape.

The next consideration for CISOs is whether to build an XDR solution in-house or whether to invest in a managed service provider that can act to enhance in-house knowledge and provide SMBs in particular with 24x7x365 monitoring.

Those organizations that lack headcount or skills to implement EDR and XDR should look to a managed XDR solution that can augment existing staff for a fraction of the cost of building this capability in-house.

The value in managed services

Many SMBs are dealing with an influx of security threats combined with a lack of security resources and knowledge.

One of the most prominent issues organizations face today is dealing with the volume of data they are presented with, filtering alert noise and focusing on the right signals. Alert fatigue is a big problem.

"As we gather more telemetry and gain greater visibility via XDR, this can overwhelm defenders with new alerts. All while threat actors continue to adapt and improve as part of an ever-evolving ransomware-as-a-service (RaaS) model," notes BlackBerry's Lee.

This is exacerbated by the well-known headcount shortage in the cyber security industry which makes it difficult to both hire and retain good talent.

Lee notes that these primary issues will not be solved by scaling in headcount alone – an efficient, turn-key, scalable managed XDR solution is the fastest and most cost-effective option to tackle these issues.

For many, implementing enterprise-grade detection and response capabilities is a significant undertaking, and building a SOC from scratch is not only time-consuming but represents a significant cost for many.

Even traditional tools such as unified threat management systems (UTMs) and intrusion and detection/prevention systems (IDS/IPS) need to be monitored 24x7x365.

Steeped in the strategy

For Robin Smith, CISO at Aston Martin Lagonda, a luxury car manufacturer, managed services are the future for his team and part of the strategy on which he is working.

With 25 years of experience managing a workforce, Smith highlights how behavior, capacity management, visibility and delivery can all prove problematic when running an in-house cyber security team.

Comparatively, Smith says he would opt for "an agile, elastic service that can be expanded and contracted as resource requires it".

With the need for 24x7x365 threat detection, an outsourced service can also often provide the hours that an in-house team does not have the capacity to work.

"Certainly, for Aston Martin, commissioned security services is the model we are moving toward because agility, resource management and innovation are going to be baked into that service," he says.

Careful consideration

When looking for a partner to supply a managed XDR solution, organizations should consider their overall vision and focus for the vendor.

XDR does not prevent 100% of cyber-attacks, but does instrument action and make evidence forensically available for analysis. Brian Robison, Vice President of Solutions and Strategy at BlackBerry, says it is important to choose a vendor who can do their best to prevent the customer from becoming a victim, while having enough technology in place to gather the forensic evidence if needed.

A multi-layered service capability is also important and should focus on prevention of an attack rather than detection and remediation alone.

To this end, capabilities should include 24x7x365 AI-powered endpoint protection, continuous threat hunting, threat intelligence overlay and rapid response to provide the best chances at preventing an attack.

Embedding XDR into your digital estate

It is evident there are benefits to both XDR and managed services as separate entities. A managed XDR solution can enhance your organization's detection and response capabilities. It is, however, imperative that CISOs consider the best investment for their existing digital estates in the case of any company, but maybe even more so with SMBs.

Investment in XDR technology alone is not enough. An organization must have the resources to be able to deliver the capabilities and manage the technology. An organization may be able to move its detection and response in a positive direction with XDR, but ultimately, to find success in the solution, the onus of responsibility is always with the people behind the tool.

> "We would be hard-pressed to find an organization that would not benefit from XDR."

Tony Lee

Vice President, Global Services Technical Operations at BlackBerry

With this in mind, SMBs may be inclined to lean toward a managed XDR solution that comes with a vendor providing the expertise and knowledge to implement the tool to be used to its full potential.

"We would be hard-pressed to find an organization that would not benefit from XDR. The question most organizations should ask is can they build this capability themselves faster and cheaper than purchasing a turn-key solution? Dedicated managed XDR providers benefit from economies of scale that are typically not afforded to a single organization trying to build their own solution," Lee says.

Critical thinking

XDR is indeed the latest addition to the detection and response portfolio. CISOs should, however, carefully consider their investment in XDR, according to Aston Martin's Smith.

"You should always be open-minded about emergent solutions, but you should also think critically about the value, benefit, cost and impact of this new version of endpoint detection and response," Smith asserts. "You should ask yourself, have we applied EDR well enough that we should migrate to XDR?"

BlackBerry's Robison notes that XDR is only valuable if the organization can invest and resource it enough to be successful – this is where managed XDR steps in.

"Ultimately, the technology is only a tool, and if it is not expertly used and resourced properly, it becomes useless shelfware where no benefits are derived," Robison says.

ROI

Simply speaking, return on investment (ROI) calculations typically focus on the number of hours saved when not responding to alerts.

However, BlackBerry's Lee argues that there are more important factors to consider, including the value of the protected data and the value of the widgets produced for those in manufacturing.

"Every organization has value or protects something valuable – even if it is 'only' their reputation," Lee says. "These factors and values might be difficult to calculate unless the organization (or similar organization) has experienced an incident, but they should not be discounted."

As with any investment, consider the ROI in terms of impact and gain for an organization making the resource commitment.

It is critical for CISOs to take stock of their own digital estate, combined with the resources and budget they have available, before investing. Adding the latest technology may be a step in the right direction, but without careful consideration, an organization could invest in a tool and service it does not use to its full potential.

Conclusion

Your investment in Managed XDR

It is clear that there is a business case to be made by many organizations that managed XDR should be part of their cyber security investment plans going forward.

XDR offers more than EDR alone, including a reduction in the number of false positives, more accurate incident response, a comprehensive context for remediation and streamlined operations.

In addition, those looking to include UEBA capabilities in their threat detection and response capabilities should consider how XDR can play a part.

An XDR solution is ultimately the next step many organizations should be making, but, as with all investments, we can see how critical thought should go into this investment to ensure that it is the right technology and the right time to add it to an organization's defensive stack.

Managed services

With the need for 24x7x365 threat detection and response, there is an advantage to having an agile managed service provider for XDR.

For SMBs, consideration should be given to what a managed service can offer, but there also should be clear communications and a working relationship between the organization and the service provider.

A managed XDR solution and the necessary skills to properly operationalize the technology can work together to provide organizations with maximum value.

A managed XDR solution can allow an organization to focus on the core activities critical to their success and growth rather than spending time worrying about the ever-evolving threat landscape.

Please note: All comments made by the contributors of this report are solely the views of the individuals without any relation to their employers, institutions or business partners.

Additional Resources

Find out more about managed XDR and how to adopt a prevent-first security strategy by watching these video interviews

How to successfully move from reactive to preventative security

Watch this exclusive CS Hub conversation on how to successfully move your business from a reactive cyber security posture to a preventative one.

Businesses often rush to react to the last cyberattack yet do nothing to prevent the next one. In today's growing cyber security threats, organizations from enterprise level to small and medium-sized businesses must take steps to prevent attacks rather than simply react.

Two BlackBerry security experts join Beth Maundrill, editor at CS Hub to discuss:

- *The main issues security owners face today*
- *How EPP, EDR, MDR and Managed XDR fit into a prevention-first strategy*
- *What approach security owners should take when moving to a prevent-first security posture*

How to optimize threat detection, investigation, response and threat hunting in real time

Watch this exclusive CS Hub conversation with BlackBerry Cybersecurity leaders on how to optimize threat detection, investigation, response, and threat hunting in real-time.

There has been a drastic change in the way organizations conduct business today with digital transformation, expanding digital independence, and the increase in remote workforce.

There is also the struggle to find key cybersecurity resources to combat the growing cyber-criminal organizations.

As a result of these challenges, opportunities for cyber criminals and the risk of attack have increased exponentially.

During this conversation with Tony Lee, VP of global services technical operations, and Brian Robison, VP of solutions strategy at BlackBerry, we will discuss the best line of preventing an attack through real-time activities by leveraging AI-driven endpoint security products with sophisticated cyber security managed services. Watch the conversation to learn:

- *What SOCs and IT teams need to implement to combat today's threat actors*
- *How small and medium-sized businesses can implement enterprise-grade detection*
- *Where BlackBerry has seen success in implementing AI-driven endpoint security solutions, optimizing detection, investigation, response and real-time threat hunting*