CYBER SECURITY HUB

CISO strategies for proactive threat prevention

As CISOs face increasingly regular and sophisticated threats, many are looking to move from a reactive to a prevention-first strategy via EPP, EDR, MDR and Managed XDR solutions

Inside:

- How to shift from a reactive to a prevention-first strategy
- Being a cost effective CISO by leveraging managed services
- Why Artificial Intelligence (AI) is a key element of a preventative approach

Why CISOs need to adopt prevention-first strategies

CISOs are under immense pressure to protect their organization and keep them out of the breach headlines. The largest obstacle to this goal is an evolving threat landscape that is increasing in sophistication. Payments from successful ransomware attacks fuel this evolution in the form of ransomware-as-a-service models. To break the trend, this report will explore why CISOs and their teams can no longer simply react to these threats and must prevent them from occurring in the first place.

When an organization's cybersecurity tools are reactive solutions, they can leave the organization vulnerable to attack recovering data and systems is not enough. Threat actors became wise to this recovery tactic and started to exfil sensitive data before launching ransomware within the victim environment. As a result, threatening to release sensitive data is often enough to force the organization to pay the ransom even if they have the ability to recover systems and data.

"Threat actors are always changing and evolving their tactics, and we need to account for that change," says Tony Lee, Vice-President – Global Services Technical Operations at BlackBerry.

Being quick to react and recover is important, but it is only half of the picture, according to Lee, because of the name-and-shame tactics and the data released by the threat actors.

Ransomware-as-a-service, where threat actors can use already-developed ransomware tools and services to carry out attacks, continues to thrive and enable threat actors to scale like never before. Organizations that may have believed threat actors did not target before are now targets. Organizations (regardless of size) cannot afford to remain reactive and perform monitoring on a nine-to-five basis. Threat actors are working around the clock globally and a company's defenses must do the same.

In fact, the threat of "new ransomware models" was the top concern facing executives in the third quarter of 2021, according to Gartner's latest ***Emerging Risks Monitor Report***. Those surveyed by Gartner said that ransomware was a bigger concern than pandemic related disruptions, including supply-chain issues.

Finally, organizations must be prepared to face an ever-growing cyber space, as well as a huge volume of data and endpoints. While previously it may have been easy to manage a small set of systems it is now imperative that companies are prepared to deal with an explosion in the number and types of endpoints. The rapid growth and prevalence of IoT is not just a risk to home users, but also organizations. Everything from coffee pots to smart car chargers to **fish tank thermometers** pose a risk to the organization. A preventative approach to solving these issues lies in the technology and strategies CISOs are deploying.

Contents

> "Moving from a reactive to a preventative security posture is not an easy undertaking."
>
> **Tony Lee**
>
> Vice President, Global Services Technical Operations BlackBerry

By focusing on Endpoint Protection Platform (EPP), Endpoint Detection and Response (EDR), Managed Detection and Response (MDR) and Managed Extended Detection and Response (XDR) solutions, this report will reveal how CISOs can use the latest cyber security mitigation strategies to deal with this complex and fast-moving threat landscape.

Using managed services to bridge the skills gap

In the face of today's threats, a preventative strategy should employ 24x7x365 monitoring, threat intel overlay, and continuous threat hunting, all based on AI-powered technology. AI is the force multiplier to help bridge the skills and resources gap making humans more efficient in their jobs. The predictive nature of AI-based EDR and EPP is needed to combat zero-day threats enabling the prevention-first strategy. (See page 6 for details about AI solutions).

It is often a challenge for CISOs to deliver these types of capabilities in-house. Typically, only the largest enterprises with budgets and resources to match have a chance at solving this with in-house only resources. For the rest of the industry, there are managed solutions that are designed to scale using fixed resources.

"Even if budget is not an issue, staffing and time to build are still challenging. In many cases for organizations of all sizes, enlisting the help of an existing MDR or XDR provider is often more cost and time effective than building it yourself," Lee explains.

Using managed services is by no means a new solution. As Lee explains, the demand for environment visibility via an EDR product is driving customers to see the value, but also realize the challenge in implementing and optimizing such a powerful product.

Next-gen AI-based EDR and EPP solutions are being used increasingly to replace legacy antivirus solutions that do not pass as meeting minimal security standards anymore.

Lee points out that using some legacy solutions may in fact mean an organization is unable to obtain cyber insurance due to a high risk of breach.

"Cyber insurers want to see next-gen products as well as EDR and 24x7 monitoring as a minimum. This combination of AI-based EPP and EDR provides a "prevention-first" strategy followed by visibility in case there is a need for investigation and validation," Lee said.

Skill shortages

While EDR may be growing in popularity, it can prove difficult for organizations to really master as it requires both commitment and possibly even dedicated resources.

"Organizations realize the necessity [for EDR] but they do not in many cases have the in-house expertise to avoid another shelfware product so that's why they look towards managed services," Lee adds.

For example, **in the research carried out by UK's Department for Digital, Culture, Media & Sport**, the UK government said in March 2020: "Approximately 653,000 businesses (48 percent) have a basic skills gap. That is, the people in charge of cyber security in those businesses lack the confidence to carry out the kinds of basic tasks laid out in the government-endorsed Cyber Essentials scheme and are not getting support from external cyber security providers."

Even if organizations were willing to hire additional in-house staff, they are faced with a headcount shortage in the cyber security industry.

Moreover, in an August 2021 speech by President Biden on improving cyber security in the US, he said, "Our skilled cyber security workforce has not grown fast enough to keep pace [with hackers and criminals]."

"We've created our own problem because we're focused on a detect and respond world, not a preventative world."

Brian Robison

Vice-President of Solutions Strategy at BlackBerry

Biden noted that about half a million cyber security jobs remain unfilled.

While organizations may be grappling with this so-called skills shortage, managed services can assist by allowing organizations to have cybersecurity solutions supplied rather than building them in-house.

Brian Robison, Vice-President of Solutions Strategy at BlackBerry, views the skills shortage as a problem that has been created by the cyber security world itself. "We've created our own problem because we're focused in a detect and respond world, not a preventative world. We're spending millions and millions of dollars of our board's money to react to a threat that could have been blocked," he says.

"We need managed services to bridge the gap to efficiently scale to cover thousands of organizations and hundreds of thousands of endpoints. These services are able to protect more devices by efficiently using a smaller set of highly skilled people along with finely tuned processes and technology," Lee adds.

Professional services organization **KPMG said in a 2021 post** that, as the skills gap becomes more acute, the answer is not just to bring in more people but to use technology and automation for repetitive tasks.

The job of technology is not necessarily to replace people but to assist those who are working in cyber security in carrying out the most important tasks.

How investment in prevention-first pays off

Through the use of MDR and Managed XDR, combined with EDR and EPP solutions, businesses can optimize their investment in cyber security.

Ultimately, Lee believes that utilizing managed services is the most cost-effective way to ensure an organization's cyber security.

"We have performed multiple cost model analysis for MDR/Managed XDR versus building in-house and only in the very largest organizations, such as those in the Fortune 100, would it start becoming more cost-effective for them to do it in-house," he explains.

This is especially true for small- and mid-size organizations since employing enough staff to do the job of a managed services provider can be impractical, they are simply not large enough to absorb the investment needed for the additional headcount.

We know that small- and mid-sized businesses must carefully consider effective investment in cyber security because they are at high risk. The **US Small Business Administration** notes that small businesses are particularly attractive targets because they have information that cybercriminals want, and they typically lack the security infrastructure of larger businesses.

Not only do managed services provide businesses with the solutions they need to counter these threats but the shift to a prevention-first strategy also provides an opportunity to be more cost-effective with a security strategy.

"Prevention is far less time-consuming and costly than investigation and containment. The earlier we can prevent the attack in the cyber kill chain – the less resources we will need to consume. Thus, a prevention-first strategy can also help reduce the skills and resources gap along with defensive spend," Lee says.

CISOs shifting their approach

CISOs must consider the benefits investment in a prevention-first strategy will bring to their business and Robison also says that today's CISOs need to turn the corner from being a cost center to becoming a more proactive part of the business.

The conversation needs to change from one that is focused on investment in legacy antivirus solutions, which Robison believes is ultimately a drain on resources, to preventative solutions that stop the threat before it becomes a cost to the organization through ransom payout and remediation efforts.

"What this requires you to do is to partner with vendors that help you grow the business," he says.

Robison compares the shift in focus CISOs must make to the actions CIOs' took to move from on-premises solutions for an organization's data to cloud solutions for their data centers.

"CIOs changed their models from being a massive cost center to becoming a more proactive business delivery model," he says. "The CISO has not rounded that corner yet."

"The biggest paradigm shift that I see being capable in the world today is helping the CISO change the conversation and say I need to make this investment [in a managed service].

He explains that this is essentially what the CIO did years ago when they recognized the need to get rid of the on-premises solutions which are costly to the organization and switch to the more efficient cloud-based services.

This is by no means an easy task and it is challenging for CISOs to stand in front of the board and tell the CEO there is a better way of doing things, Robison notes. Ultimately, most businesses will discover that outdated, traditional reactive solutions do not prevent breaches when a breach happens it will be extremely costly.

The cost of a breach to small- and mid-sized businesses are often astronomical and can ultimately be mitigated with commitment and investment in preventative solutions such as MDR/Managed XDR, EDR and EPP.

Using AI is imperative to the solution

AI offers solutions where computers can process large amounts of data to learn patterns, so it knows how to behave without the assistance of humans – this includes predicting what may occur next from analysis of what has already happened.

The value of MDR and Managed XDR solutions can be enhanced through the use of AI to provide the 24x7x365 coverage required in a scalable fashion.

"The reality is the human aspect of legacy EPP and EDR solutions cannot scale, there are too many new versions of new viruses," says Robison.

The AI component of MDR/Managed XDR, EDR, and EPP is essential to have a predictive advantage against today's threats.

In July 2021, the **World Economic Forum noted** that well-deployed AI can be used to counter today's security threats. In addition, the World Economic Forum highlights that AI can help respond to threats almost immediately, especially when there is too much data for humans to process.

The math model

AI is necessary because network defenders already face a huge volume of alerts. Many organizations are unable to analyze all the endpoint threats and vulnerabilities, and when coupled with the labor shortage previously discussed, this is where AI can be that force multiplier.

AI-powered endpoint protection is able to use advanced machine learning to uncover malware, fileless and user-based threats in the environment. Meanwhile, the benefits of AI are already being felt by those who use it. As of 2019, **64 percent of senior IT executives surveyed by Statista** stated that AI helped lower costs to detect and respond to breaches in their organizations.

Statista stated that 83 percent of US-based respondents it surveyed agreed to the statement "we will not be able to respond to cyberattacks without AI". Many vendors claim to employ artificial intelligence in their products as a bit of an "us too" marketing exercise, Lee says. Thus, CISOs are encouraged to look for vendors who have been in this space for a while and have mature AI math models.

> "The AI component is critical to all of this otherwise it just does not scale efficiently."
>
> **Tony Lee**
>
> Vice President, Global Services Technical Operations, BlackBerry

"The beautiful thing about the math model is the predictive nature of it, so even when a brand-new threat comes out, there is a high probability that the math model already has coverage on the new threat without even being told about it," Lee explains.

Essentially AI can do what humans cannot by trawling through vast amounts of information to identify threats and use the learnings from said information to predict what future threats may look like.

Conclusion

To move from a reactive to a preventative strategy, CISOs must recognize that there is a need to shift away from outdated legacy antivirus technology and toward next-gen solutions that prevent attacks before they happen.

MDR, Managed XDR, EPP and EDR solutions, combined, can offer an effective approach that does not drain resources and allows organizations to minimize alert fatigue.

In addition, these solutions must work together.

"A fully integrated EPP, EDR, and managed service is required for any hope of correlating events. Trying to correlate EPP and EDR events in two disparate systems is not scalable," Lee says. "This needs to be delivered as a single package by managed security experts who know how to wield the products the best. Since no EPP is 100 percent, EDR provides the ability to gather evidence, threat hunt and even take extended actions."

"These two technologies combined with managed services enables incident analysts and hunters that work as an extension of your security team. This allows internal security teams to focus on key security initiatives rather than spending time and resources triaging alerts or recovering from an attack," he adds.

AI also has a vital role as the volume of threats and incidents cannot be identified by humans alone. The predictive aspect of AI is crucial to identify threats before they happen.

While faced with a shortage of cyber security professionals, a prevention-first strategy is the only way for organizations to defend against today's 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.