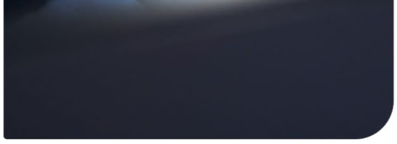
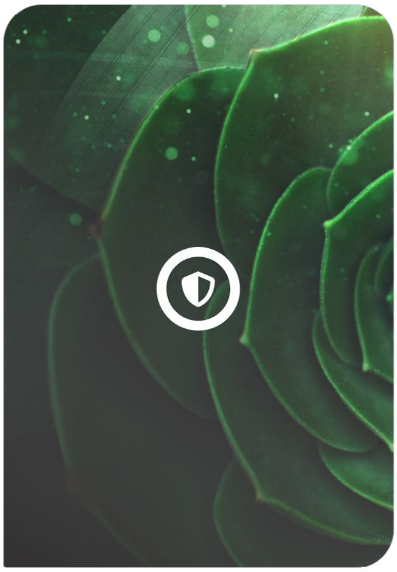
A new world of AI cyber security?

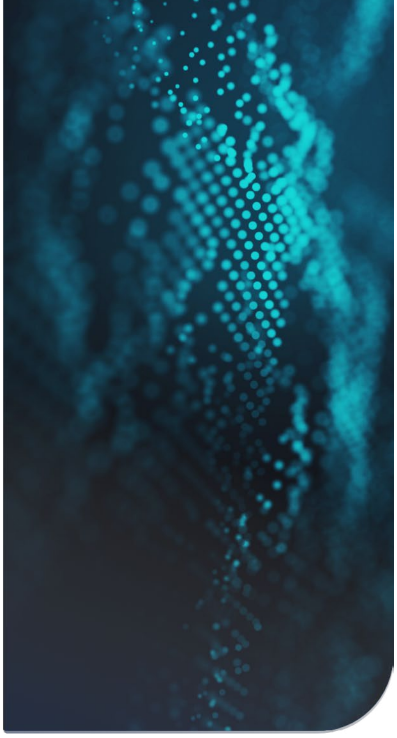
How **AI-driven managed security services** have become the strategic lever for modern enterprise

RelianceCyber

THOUGHT LEADERSHIP E-BOOK SERIES







AI & managed services: economy's cost-benefit

How **AI-Driven Managed Security Services** have become the strategic lever for modern enterprise

DIGITAL TRANSFORMATION

The realm of digital transformation holds incredible opportunities for businesses, but it isn't devoid of risks.

In 2021 the IDC predicted more than half of global GDP would be digitally driven by 2023, a testament to the increasing reliance on digital technology. Conversely, Cyber security Ventures projects that cybercrime could incur costs of £8.4 trillion annually by 2025. Amid these conflicting trajectories, Managed Security Services (MSS) play a pivotal role, serving as both a shield and a strategic compass for businesses in the digital landscape.

Projected cybercrime costs

£8.4 trillion annually by 2025*

THE COST AND EFFICIENCY ADVANTAGE

While most businesses recognise the direct costs of cyber security - hardware, software, and professional fees - they often underestimate the indirect costs. These include potential reputational damage, operational disruption, and regulatory fines following a security breach. The latest IBM Security Report estimated the average cost of a data breach in 2022 was £3.4 million. An eye watering figure.

SO HOW CAN MSS ANSWER THIS CONUNDRUM?

Research conducted by 'MarketsandMarkets' suggests global spending for managed security services will grow to $43.7 billion by 2026, up from $22.8 billion in 2021. The research firm attributed the growing use of MSSPs to the following factors:

- Stringent government regulations
- Increase in security breaches
- Growing sophistication of cyber attacks
- Surge in BYOD and remote work policies
- Cost effectiveness

More importantly, it helps businesses transition from a capital-intensive model to an operationally lean approach to security. The cost savings, along with the ability to focus more resources on core business functions, makes MSS an economically attractive proposition.

* Predicted by the IDC

A paradigm shift of MSS in the new world

As organisations continue to get to grips with the evolving digital and security landscape and many employ some form of **managed security service** (MSS)

PARADIGM SHIFT

Whether it be managed by in-house teams or leveraging external resources - there has been a further paradigm shift.

The integration of artificial intelligence (AI) and machine learning (ML) is changing and refining how the "best in the business" approach cyber security. Whilst traditional MSS has always been crucial, the rise of AI, the adoption of Security Orchestration, Automation, and Response (SOAR) tools, and the introduction of Extended Detection and Response (XDR) introduce an unparalleled layer of sophistication to the field.

Machine learning is changing and refining how the "best in the business" approach cyber security.

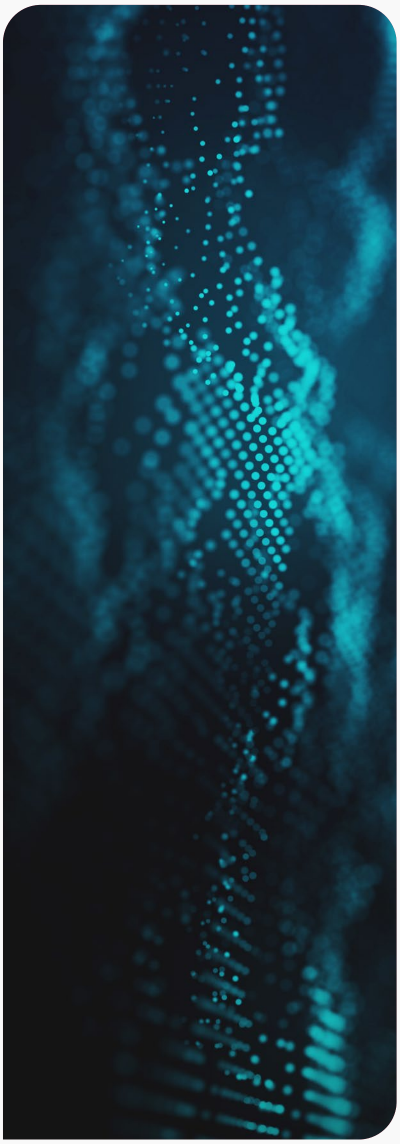
This evolution is welcome news given the speed and proliferation of threats and attacks. There is however a catch, with the rise in AI, Automation and ML, businesses may be lulled into a false sense of security, believing that buying more tools incorporating cutting edge technology will solve their security worries or woes. The magical and much coveted silver bullet.

THE HOLY TRINITY OF TECHNOLOGY: AI, ML AND AUTOMATION

In the past years and more recently months, the market has seen an explosion of AI-powered cyber security tools. Promising to swiftly and painlessly answer organisations' complex and unrelenting security needs by automating, and thus removing the need for swathes of resources dedicated to or spending significant amounts of time on managing the security estate. Additionally, there is the allure of the potential for a smaller and less skilled workforce. Why invest in expensive security professionals that need constant training and are hard to keep hold of, when the machines and technology can do it for you?

AI

In recent months the market has seen an explosion of AI powered cyber security tools



Innovation through automation: Overcoming in-house limits

Evolving and complex cyber threats require more than just new tools; they demand genuine security measures

THE RIGHT TOOLS?

However despite this notion, many organisations faced with the prospect of cyber threats see tools as the solution, investing heavily in an array of advanced security technologies that incorporate AI, ML and Automation.

They assign their management to existing teams, assuming this will suffice. However, this approach often leads to under-utilisation of these tools due to a lack of adequate skills or time among the internal teams. Ultimately counteracting the original purpose of employing such tools and technologies.

Suggested reading
Security is not a tool: The case against security tooling.

What leads these decisions is the constant challenge that organisations face with regard to skill and resource, something that is underscored by Gartner's prediction that nearly half of cyber security leaders will change jobs by 2025. This lack of resource and expertise often creates a knowledge gap within organisations, rendering their well-intentioned security investments less effective. The journey to cyber security has evolved and as such demands more, more than mere human vigilance and more than total delegation to tools and tech. It requires real-time responsiveness, predictive analytics, and a proactive approach.

AI and ML support MSS by automating routine tasks, with a view to allowing professionals to focus on strategic decisions. Google's and Microsoft's advancements in Security Information and Event Management (SIEM) systems, underpinned by AI, underscore the growing emphasis on automation in the cyber security arena and its importance. But wielding these powerful tools and understanding the vast amounts of data they produce often exceeds the knowledge of in-house teams.

MORE THAN TOOLS: A CASE FOR MSS

Having top-tier security tools is important, but it's not a panacea (read: Security tooling security is not a tool, tools don't innovate). The notion of having "all the gear and no idea" rings particularly true in cyber security.

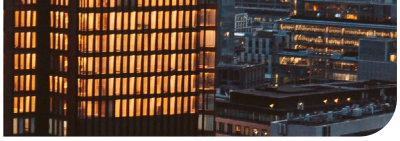
Even the best firewall or advanced network access management tools can amplify risk if misconfigured or poorly managed, as evidenced by high-profile breaches like the 2019 Capital One data breach caused by a misconfigured web application firewall. And while the benefits of AI-powered tools are undeniable, their efficacy hinges on human expertise. Skilled professionals can extract actionable insights, innovate, and ensure tools are used to their utmost potential. MSS providers' extensive exposure across sectors enables them to anticipate the evolving threat landscape based on the breadth and depth of their experience, as well as their unique insight, assuring comprehensive threat mitigation.

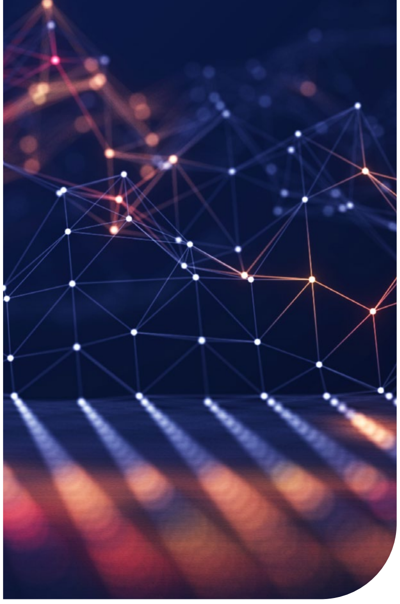
Even the best tools can amplify risk if misconfigured.

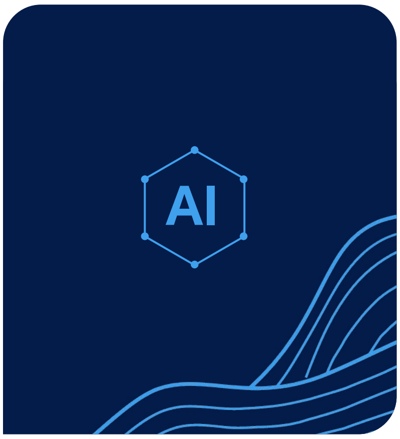
As evidenced by the **2019 Capital One data breach** caused by a misconfigured web aplication firewall.

TAILORED STRATEGIES

Additionally, fostering a security-conscious culture is paramount. MSS providers, adhering to standards such as those from the National Cyber Security Centre (NCSC), create tailored strategies that resonate with a company's culture and goals, promoting a proactive security mindset that often permeates the organisation. Ultimately, MSS providers serve as an extension of your team, ensuring expert management of security tools and mitigating the risks associated with their mismanagement. They offer strategic guidance, operational efficiency, and robust security measures, making them a critical ally in your digital transformation journey.







Understanding and redefining MSS with AI and automation

The incorporation of **Artificial Intelligence (AI)** and **Machine Learning** (ML) is radically changing the field of Managed Security Services (MSS).

Rather than just automating routine tasks, these technologies are leading the way in making predictive analysis standard practice. This shift is fundamentally altering how we understand and respond to cyber security threats.

THE STORY OF XDR AND THE SYNERGY OF CONVERGED MSS AND XDR SOLUTIONS POWERED BY AI (AND EXPERTISE)

Extended Detection and Response (XDR) has become a game-changing component in modern cyber security strategies. XDR offers a holistic view of threat activities across various network assets, providing a level of visibility and control that traditional endpoint solutions can't match. When integrated with AI and ML, Extended Detection and Response becomes a powerhouse for sifting through vast amounts of data, identifying threat patterns, and predicting potential security breaches before they can escalate.

The comprehensive insights gained from XDR add an extra layer of intelligence, making threat detection and response more effective and timely.

The real magic happens when XDR is combined with Managed Security Services to create a converged solution

This melding of services allows organisations to benefit from the best of both worlds — the robustness of MSS and the advanced analytics of XDR. While AI, ML, and automation are critical in making this integration efficient, their true potential can only be harnessed when managed by professionals with the right expertise.

A tool is only as effective as the hands that wield it. MSS providers who bring this level of expertise ensure that AI, ML, and automation are utilised to their full extent, making the converged MSS and XDR solution a formidable asset in modern cyber security strategy.

In this framework, teams skilled in both MSS and XDR can fine-tune AI algorithms, interpret machine learning models, and optimise automated processes to match an organisation's unique needs and vulnerabilities. This expertise is crucial for configuring settings, analysing data outputs, and making real-time decisions to maintain an adaptive, resilient security posture. So, while AI, ML, and automation are indispensable tools for managing cyber security threats, their effectiveness ultimately hinges on the skills and expertise of the teams that manage them.

A closer look: The pivotal role of AI in MSS

Exploring Real-World Benefits of Converged **MSS** and **XDR**

Top 5 Use Cases Demonstrating the Synergy of Converged MSS and XDR Solutions:

Below we explore some of the top use cases that outline the tangible benefits and operational efficiencies brought by integrating these cutting-edge technologies into your security strategy.

Advanced threat hunting

1

A converged MSS and XDR solution, when integrated with AI and machine learning algorithms, enables more effective and proactive threat hunting. By combining data from multiple security layers, experts can easily identify anomalies and proactively address threats before they escalate into security incidents.

Streamlined incident response

2

With the support of a managed security service, incident response becomes a well-oiled machine. Automated workflows driven by AI and machine learning can instantly classify and prioritise threats, enabling experts to focus on complex cases requiring a nuanced approach. Ultimately reducing the time from detection-to-resolution time and significantly minimising damage.

Compliance management

3

Converged solutions simplify regulatory compliance, offering automated reporting and real-time analytics, meaning companies can more easily prove compliance to auditors. Ideal for highly regulated sectors like healthcare and finance.

Insider threat mitigation

4

With a cohesive view from the XDR and expertise from MSS, detecting insider threats becomes more practical and effective. Behaviour analytics driven by machine learning can flag suspicious internal activities, while the managed security service ensures a timely and appropriate response to these threats, thereby safeguarding crucial data and systems.

Optimised cloud security

5

As businesses increasingly migrate to the cloud, securing these environments becomes critical.

A converged MSS and XDR solution offers extended visibility and control over cloud assets.

Automated tools can instantly detect misconfigured settings or unauthorised access, and expert teams can quickly intervene to remedy the vulnerabilities, ensuring a secure and resilient cloud infrastructure.

These use cases underscore the importance of having a balanced approach, where cutting-edge technology and human expertise unite to offer a robust security strategy.

By adopting a converged MSS and XDR solution enriched by AI and machine learning, businesses can bolster their security posture, ensuring that they are well-equipped to face the evolving cyber security landscape.

Conclusion

The path towards digital transformation is replete with opportunities and challenges.

While investing in sophisticated security tools is important, ensuring that they are effectively managed by competent teams is paramount.

MSS providers play a vital role in bridging the skills gap, managing the advanced cyber security tools effectively, and helping businesses navigate their digital transformation journey securely. By shifting the perspective on cyber security from being a burdensome necessity to a strategic enabler, MSS helps businesses adapt to the dynamic threat landscape. This approach ensures that as businesses chart their course in the digital era, they are not just shielded from present threats but also prepared for future ones.

Reliance Cyber specialises in AI, ML and automated MSS solutions, engineered to bring enterprise-level security to mid-market organisations.

We are market leaders in developing and delivering security solutions to companies that do not have the resources, capabilities or capital to build and operate comprehensive security solutions.

If you would like expert advice on how to secure your infrastructure to meet the challenges of an ever-evolving digital landscape, please get in touch.

A new world of AI cyber security?

Explore the leadership series

RelianceCyber

reliancecyber.com