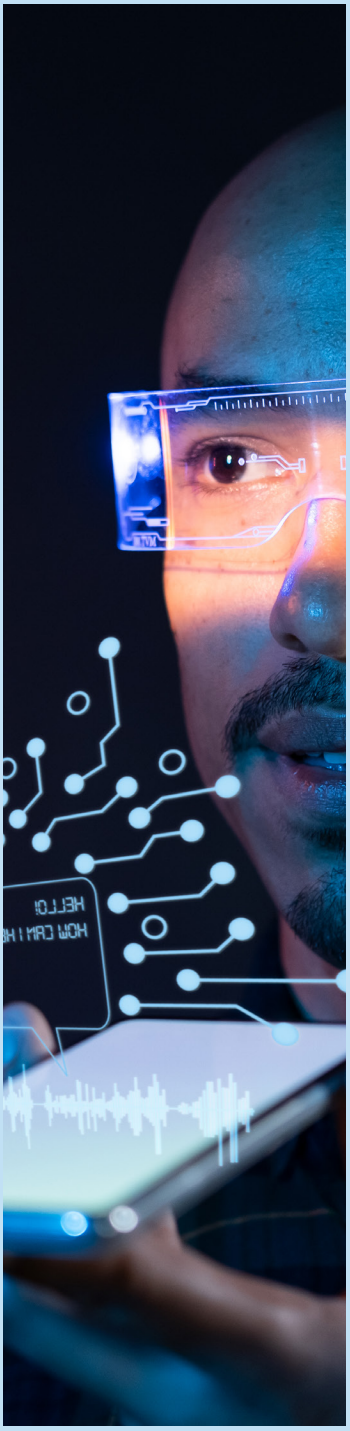
VIEW POINT



THE RISE OF GENERATIVE AI: A GAME-CHANGER IN DEFENSE

Infosys®
Navigate your next

Introduction and Background

Cyber threats are evolving rapidly. Whilst we see investment in cybersecurity, we continue to struggle to stay ahead of the technological curve. Adversaries are quickly evolving, finding ways to circumvent certain people, processes and technology to breach our defences.

The advent of generative AI (GenAI) marks a new era in cybersecurity. Security Operations Centres (SOC) are already overwhelmed by the sheer volume of data flowing in from various sources, including security stacks, information feeds, application data, Vendor and supply chain inputs. Attackers are exploiting these challenges by leveraging malware payloads through new threat vectors.

As organizations increasingly expand their operations beyond traditional firewalls, their attack surface grows exponentially. GenAI can serve as both a powerful ally and a potential adversary. To achieve growth and reach their customer base, organizations must integrate GenAI into their cybersecurity architecture. It is no longer optional; it is a necessity to balance processing power with effective decision-making.

The global cost of cybercrime reached an estimated US$8 trillion during the 2023/24 fiscal year, and this figure is projected to surpass an alarming US$12 trillion by 2026. The financial risk for businesses continues to climb, with the average cost of a significant cyber breach in 2024 now ranging between US$5-8 million—a 20% increase, according to data from insurers like AIG. Additionally, ransomware claims alone have surged by more than 300%, highlighting the mounting threat landscape.

It is imperative for organizations to leverage Generative AI (GenAI), both as a proactive defense mechanism and as a strategic tool for internal operations, to counteract these escalating risks and ensure resilience.

Artificial intelligence is transforming cybersecurity by taking a proactive role in defense strategies, especially in processing and managing up to 300 vulnerabilities daily from multi-tenanted vendor data. With its capacity for automated learning, AI has the potential to revolutionize how organizations safeguard critical assets. However, its implementation must be accompanied by vigilant monitoring to facilitate informed decision-making and ensure focused attention on segregating and securing vital systems.

At the same time, the misuse of AI by cybercriminals poses significant challenges, as it enables the creation of increasingly sophisticated and targeted attack strategies. This dual nature of AI underscores the need for a fundamental shift in traditional security paradigms, balancing innovation in defense mechanisms while mitigating the risks posed by malicious usage.

The rise of hybrid working, the merger and acquisitions of organisations seeking future growth and market expansion means that GenAI, along with other attributes like quantum computing and digital transformation plays a crucial role. At the same time, traditional security perimeter are being reshaped.

Employees now access sensitive data from diverse locations and devices, necessitating organizations to adopt a robust Zero-Trust security model. The rapid pace of mergers and acquisitions, driven by the imperative for business growth and market expansion, increasingly relies on AI as a pivotal enabler. Additionally, advancements in quantum computing have introduced scalability opportunities while simultaneously demanding a reexamination of existing encryption frameworks to ensure future-proof cybersecurity. Within this shifting landscape, AI emerges as a critical tool, enabling near real-time threat identification and mitigation. This capability not only bolsters cybersecurity operations but also aligns seamlessly with broader organizational objectives.

The Increasing Complexity of Cyber Threats

Cyber criminals are exploiting AI to carry out increasingly complex attacks. These advanced threats can evade traditional security measures and cause severe damage long before they are detected. A recent study by Darktrace found a 135% increase in social engineering attacks[4] as a result of the widespread use of ChatGPT. Tools like WormGPT can generate convincing phishing emails in multiple languages, making it easier for cybercriminals to trick their targets.

In this context, organisations should be proactive and must leverage AI not only as protective counter measure but also to support business proactively. Leveraging AI in cybersecurity architecture and monitoring frameworks enables organizations to proactively anticipate and counter threats. By integrating AI to support routine decision-making processes, businesses can focus on critical operations while benefitting from comprehensive oversight. This strategic approach enhances data and network protection and provides a significant competitive advantage, particularly for enterprises with multi-channel, global client reach.

Traditional security models, which rely heavily on process, people and technology whilst trying to identify boundaries, have become obsolete in certain industries. Defining a perimeter is no longer sufficient through customer demand and supply chain requirements. Consequently the "zero trust" model - which assumes that threats can exist inside the network - offers a more robust approach.

AI can improve this model exponentially by continuously monitoring network activity, identifying anomalies, and responding to potential threats in real-time at Network, end-user device, platform, system, solution and service levels. By using AI, this model ensures that only authorized users can access sensitive data, while also adhering to both person and process. Additionally, it supports technology in the decision-making process through live chatbots, and or predetermined controls. This not only mitigates risks, but also ensures a higher level of safety for all employees, the organization's business operations, and wider supply chains and critical assets.

AI-driven security systems can quickly identify false positives and rule them, escalating only genuine threats to the security team. This streamlined process reduces the burden on IT teams, allowing them to focus on more strategic initiatives. For instance, the previously mentioned figure of 300 vulnerabilities per day every day is broken down through the use of AI to 20-30 vulnerabilities of criticality which meet the thresholds of business impact and risk tolerance. This focus along with built in playbook remediation options powered by AI, hastens the decision making process, enabling employees to focus on significant issues rather than distractions, thus responding quicker and more effectively.

The Role of AI in Threat Detection and Incident Response

One of the foremost advantages of integrating AI into cybersecurity lies in its unparalleled ability to process vast amounts of data both rapidly and accurately. With the foundational infrastructure of 5G—capable of supporting over one million connected devices per square kilometer compared to 100,000 for 4G—nearly complete, we now have the means to handle highly scalable and densely connected data flows across varied device ecosystems. Empowered by such infrastructure, AI can ingest and analyze terabytes of data in mere seconds, a task that otherwise would take minutes or even hours. This exceptional data-processing capability is critical in identifying patterns and anomalies that signal potential security breaches, allowing enterprises to proactively safeguard against threats.

Detection and remediation

As discussed, threat detection was one of the earliest applications of cyber AI. It can augment existing attack surface management techniques to reduce noise and allow scarce security professionals to zero in on the strongest signals and indicators of compromise. Additionally, It can also make decisions and act more rapidly and focus on more strategic activities.

AI algorithms can analyse data from multiple sources (network traffic, user behaviour, system logs and monitoring, supply chain activity etc.) to detect potential threats. Unusual patterns can be a sign of a cyberattack. For example, AI can detect a sudden spike in data transfer rates, which could indicate an attempt at data exfiltration. By identifying these anomalies in real-time, AI allows organisations to pinpoint this to an End User Device (EuD) and take immediate action and prevent potential breaches.

Moreover AI and machine learning to automate areas such as security policy configuration, compliance monitoring, and threat and vulnerability detection and response. For instance, machine learning–driven privileged access management platforms can automatically develop and maintain security policies that help enforce zero-trust security models. By analyzing network traffic patterns, these models can distinguish between legitimate and malicious connections and make recommendations on how to segment the network to protect applications and workloads.

Leveraging next-generation AI involves AI-driven network and asset mapping into Configuration Management Database (CMDB). Visualisation platforms can provide a real-time understanding of an expanding enterprise attack surface within a network across global footprint. The AI engine can identify and categorize active assets, including containerized assets, which can provide visibility into rogue asset behaviours. Supply chain risk management software incorporating AI and machine learning can automate the processes of monitoring physical and digital supply chain environments, tracking how the way assets are composed and linked inside the organisation seamless and in real time. This protects against bad behaviours and flags potential areas for investigation offering options for warranted remediation.

Looking at another area of concern, AI can automate many aspects of incident response, from identifying the source of the breach to isolating affected systems to initiating remediation. This reduces the time it takes to contain and mitigate the impact of the breach and thus minimizes damage and Recovery Time Objectives (RTO).

Reduction of false positives

False positives are as we know a time consuming and widespread problem in cybersecurity. They occur when legitimate activities are flagged as potential threats, resulting in unnecessary alerts. AI can significantly reduce false positives by learning from historical data and improving its accuracy over time allowing security teams to focus on real threats. Additionally having a proactive security posture, supported by professionally trained AI can enhance security posture and promote cyber resilience. This allows organizations to stay operational even when under attack and reducing the amount of time an adversary can remain in the environment.

Shortage of cybersecurity professionals

On the other hand, the shortage of skilled professionals is a central concern for organizations. Existing IT teams are often overwhelmed by the volume of threats they need to manage. AI can ease this burden by automating routine tasks and providing actionable insights. By enforcing AI-predetermined policy controls, the necessity for Level 1 (L1) and Level 2 (L2) analysts in a Security Operations Center (SOC) or Security Information and Event Management (SIEM) system, allows those resources to focus on test and development analytics of critical assets. whilst.

Task automation

In the field of cybersecurity, repetitive tasks are legion. Monitoring network activity, analyzing activity reports, and managing security patches are just a few examples. AI can automate these tasks, freeing up valuable time for professionals to focus on more complex problems.

Actionable data

AI can analyse data and generate relevant insights, allowing cybersecurity teams to make informed decisions and even take a proactive approach. This includes identifying network vulnerabilities, predicting potential attacks, and recommending specific strategies. Not only does this improves the overall security posture of the organization, but it also increases the effectiveness of security measures.

Conclusion & Summary Next-Gen AI – The Way Forward

Integrating GenAI into cybersecurity is now crucial for businesses and organisations that want to protect their assets in an ever-changing security landscape. AI improves threat detection, reduces false positives, and eases the burden on operations teams. The AI-powered zero-trust model provides a robust framework for data protection, especially in hybrid work environments. However, to stay ahead of cybercriminals, organizations must innovate and adapt their security strategies to become more efficient and competitive.

Many organizations are still in the preliminary stages of using cyber-AI, but as attack surfaces and exposure outside of traditional enterprise networks continue to grow, AI offers more. Many organizations are still in the preliminary stages of using cyber-AI, but as attack surfaces and exposure outside of traditional enterprise networks continue to grow, AI offers significant advantages.

Approaches such as machine learning, natural language processing, and neutral networks can help security analysts distinguish bad signals from the noise. By using pattern recognition, supervised and unsupervised machine learning algorithms, and predictive and behavioural analytics, AI can help identify and repel attacks and automatically detect abnormal user behaviour, allocation of network resources, and or other anomalies. AI can be used to secure both on-premises architecture and enterprise cloud services, although securing workloads and resources in the cloud is typically less challenging than in legacy on-premises environments.

On its own, AI (alongside any other technology, for that matter) is not going to solve today's or tomorrow's complex security challenges. AI's ability to identify patterns and adaptively learn in real time as events warrant can accelerate detection, containment, and response; help reduce the heavy loads for example on SOC analysts; and enable them to be more proactive. These workers will remain in high demand, but AI will change their roles. Organizations will need to reskill and retrain analysts to help change their focus from triaging alerts and other lower-level skills to more strategic, proactive activities. Finally, as the elements of AI- and machine learning–driven security threats begin to emerge, AI can help security teams prepare for the eventual development of AI-driven cybercrimes.

References

1. A few figures to back this up is that in 2023/24 FinYr cybercriminal cost across industries reached US$8trillion (Cyber Ventures article dated Jan 2024)
2. Unfortunately, this figure is projected to exceed US$12 trillion by 2026 (IBM Cost of Data Breaches report, March 2024)
3. The average cost of a significant cyber breach in 2024 has surged to US$5-8 million, a 20% increase from the previous year, according to insurers like AIG (CNBC article, February 2024)
4. A recent study by Darktrace found a 135% increase in social engineering attacks (https://ir.darktrace.com/press-releases/2023/4/3/8b2d6ba25d9d54a1895956a985fe4a7d08d9f42607a112fb17964e4b57fad7d6)

About the Author

Luke Smith

AVP – Senior Industry Principle

Luke is a seasoned security professional with expertise in architecture, information assurance, regulatory compliance, and audit. He has a proven ability to design and implement robust security frameworks, safeguarding sensitive data and ensuring adherence to industry regulations. He is Proficient in various cybersecurity frameworks, cloud platforms, and infrastructure security. He drives organizational success through technical proficiency and strategic thinking.

For more information, contact askus@infosys.com

Infosys®
Navigate your next