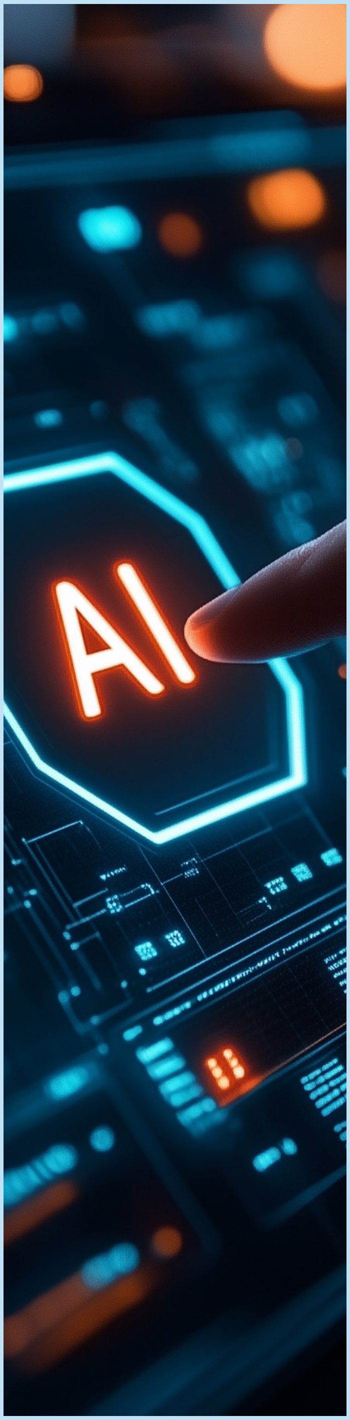
VIEW POINT



UNDERSTANDING GENERATIVE AI: BALANCING OPPORTUNITIES AND CYBER THREAT RISKS

Abstract

From accelerating product development to redefining customer experiences, generative AI (GenAI) is reshaping enterprise operations. But as its capabilities grow, so do the risks. While unlocking unprecedented opportunities, GenAI also exposes businesses to escalating AI-driven cyber threats, from data leakage to AI-powered attacks. Business leaders can no longer afford to overlook the darker side of generative AI in cybersecurity.

This PoV looks at how organisations can balance the power of generative AI with the need to stay cyber-safe. By understanding the risks and acting early, leaders can adopt AI in ways that drive innovation while keeping their business secure.

Infosys®
Navigate your next

Rapid expansion of generative AI

Generative AI is quickly becoming a core part of cybersecurity, powering key functions like threat detection, vulnerability checks, and incident response. As cyber threats grow in number and complexity, more organisations are using GenAI to boost speed, accuracy, and resilience in their security.

The market for generative AI in cybersecurity is experiencing astounding growth. According to a 2025 market analysis, the global GenAI cybersecurity market reached $2.45 billion in 2024 and is projected to surpass $7.75 billion by 2029, eventually hitting $23.9 billion by 2034. North America leads global adoption with over 40% of the market share, followed by APAC and Western Europe. Companies are now building GenAI into their cybersecurity plans and investing heavily in smart tools. Security teams rank GenAI's ability to integrate with existing platforms as one of their highest needs.

From securing patient data to protecting financial transactions and critical infrastructure, generative AI in cybersecurity is playing a growing role in industry-wide cyber defence:

Healthcare: As hospitals digitise more patient records and adopt connected medical devices, GenAI is being used to detect unusual access patterns, flag data breaches, and protect sensitive health data.

Transportation: As autonomous vehicles and smart traffic systems generate massive streams of real-time data, GenAI helps protect these systems from tampering and cyber intrusions. It's also used to secure vehicle-to-infrastructure communication and maintain the safety of intelligent transport networks.

Finance: In a sector heavily targeted by fraud and cyberattacks, financial institutions are using GenAI to strengthen fraud detection systems, monitor real-time transactions, and identify suspicious behaviour. It also supports secure data analysis, credit scoring, and trading decisions by reducing the risk of manipulated or corrupted data.

Manufacturing: With connected devices and robotics on the rise, manufacturers are using GenAI to detect anomalies in network traffic, secure factory control systems, and protect IP. It helps prevent cyber sabotage, ensure operational uptime, and safeguard digital twins and production lines.

Entertainment: GenAI is being used to protect user data on streaming and gaming platforms, detect deepfake content, and secure digital assets in virtual environments. As content creation becomes more AI-driven, media companies rely on GenAI to monitor for copyright misuse, content manipulation, and platform abuse.

GenAI is doing great things across industries, but there's a catch. Its role in cybersecurity is like that of a double-edged sword that demands caution.

The bright side of genAI: Transforming cybersecurity operations

GenAI's ability to generate insights, simulate scenarios, and adapt in real time allows security teams to respond faster and smarter to evolving threats. Here's how organisations are putting GenAI to work:

Smarter threat detection

GenAI quickly processes massive volumes of data, like network traffic and user behaviour, to detect anomalies and identify active threats. It adapts to new tactics, uncovering attacks that traditional tools often miss.

Automation at scale

From vulnerability scanning to policy enforcement, GenAI handles repetitive security tasks with speed and accuracy, freeing analysts to focus on complex investigations and threat strategy.

Adaptive playbooks

GenAI builds and updates response playbooks based on live threat intelligence. These playbooks evolve every few weeks to reflect new risks, automatically suggesting patches, isolating systems, or blocking suspicious activity.

Faster incident response

By automating alert triage, log analysis, and prioritisation, GenAI cuts response time significantly. Some SOCs report over 50% faster detection rates and shorter downtimes thanks to GenAI-powered remediation.

Context-aware risk insights

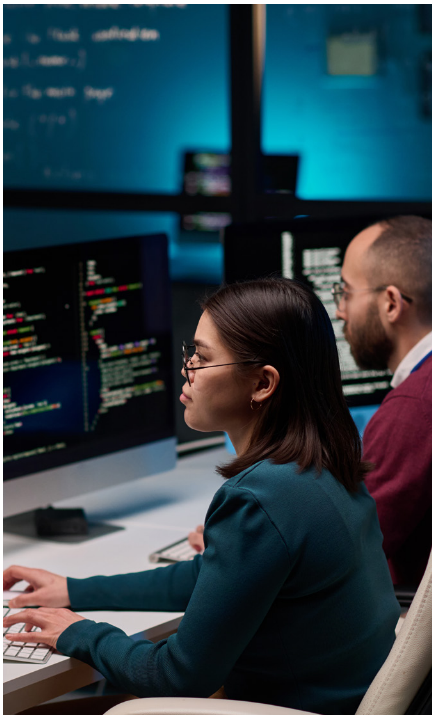
GenAI combines real-time signals from users, devices, and systems to generate dynamic risk scores. This helps teams make smarter, faster decisions about where to focus their defences.

AI-driven threat hunting

With the ability to model attacker behaviour and simulate breach scenarios, GenAI helps analysts uncover hidden threats. It finds subtle anomalies across millions of logs that manual review would overlook.

Proactive defence

GenAI learns from past breaches and simulates future attack paths, helping teams identify weak spots before they're exploited. This shifts cybersecurity from reactive to preventive.



GenAI in the wrong hands: a growing threat

While GenAI strengthens defences, it also opens the door to new, more dangerous forms of cyberattacks. Criminals and nation-state actors now use generative tools to launch faster, more scalable, and increasingly personalised attacks.

Scalable AI-powered attacks

Cybercriminals use GenAI to write malware, craft convincing phishing emails, and automate vulnerability scans. These tools make sophisticated attacks accessible to less-skilled attackers, amplifying risk across the board.

Deepfakes and misinformation

GenAI makes it easy to create believable fake videos, audio, and text. These assets can be weaponised in social engineering schemes or used to manipulate public opinion and harm reputations.

Privacy and bias concerns

Without strong governance, GenAI systems may misuse sensitive data or unintentionally introduce bias in decision-making. Ethical use and regulatory compliance must be core to any AI deployment.

Escalating the cyber arms race

Nations and organised threat groups are investing heavily in GenAI-powered cyber capabilities. This rapid development is accelerating global digital conflict and increasing the risk of AI-driven cyber warfare.

AI-driven cyber threats by the numbers

The scale and sophistication of AI-driven attacks are staggering:

36,000

AI-driven vulnerability scanners execute at speed, reaching 36,000 scans per second.

79%

of threats are malware-free, relying on behavioural and access exploits.

51 seconds

The fastest recorded e-crime breakout time, from compromise to lateral movement, is just 51 seconds.

$4.88

The average cost of a data breach in 2024 reached $4.88 million, and AI-related attacks contributed to faster breakout times and deeper infiltration.

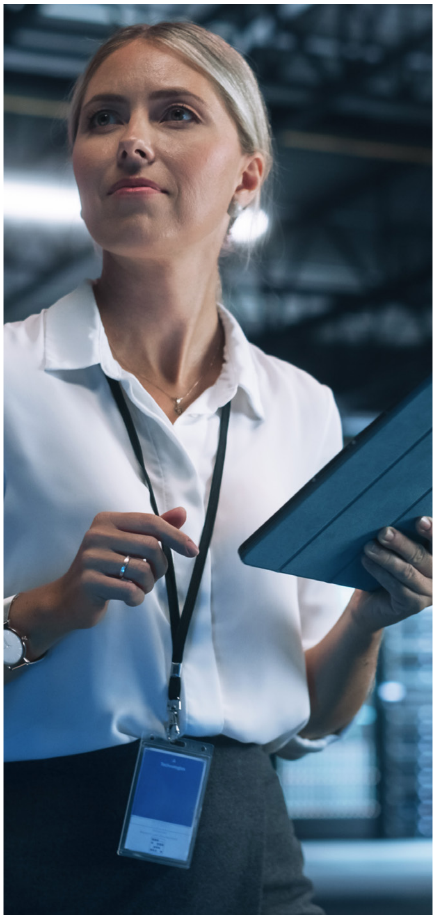
20-30 seconds

Voice cloning can now be achieved with as little as 20 to 30 seconds of recorded speech, and realistic video deepfakes can be produced in under an hour using easily accessible tools.

With such rapidly evolving threats, how can organisations confidently harness the opportunities of generative AI without exposing themselves to risk?

Strategies for secure and responsible GenAI adoption

To truly harness the potential of generative AI while minimising its risks, organisations need a deliberate, risk-informed approach from the outset. The following strategies offer a practical path to secure, ethical, and scalable GenAI adoption:



Establish a cross-functional AI risk governance group

Create a team that includes cybersecurity, legal, compliance, operations, and ethics leads. This group ensures end-to-end visibility, manages blind spots, and aligns AI use with internal policies and external regulations.

Build and maintain an AI inventory

Track all GenAI tools, both approved and shadow applications, across business units. This enables oversight, minimises unauthorised use, and ensures security reviews aren't bypassed.

Apply controls before scaling

Before moving GenAI projects from proof-of-concept to production, implement clear access controls, data protection rules, audit trails, and monitoring. Embed security tools to support core functions from day one.

Secure the full AI lifecycle

Adopt a "shift left, expand right, and repeat" mindset:

Shift left: Integrate security during design and model training stages.

Expand right: Continuously monitor AI behaviour post-deployment, looking for drift, misuse, or vulnerabilities.

Repeat: Periodically reassess risks and controls as models evolve and business use cases scale.

Enforce robust governance and data controls

Define clear policies on how GenAI systems access and use data and establish accountability for AI-generated decisions. Use role-based access controls, implement differential privacy where needed, and regularly audit for policy violations.

Why this matters: Taking these steps helps organisations move beyond tactical GenAI experiments to strategic, secure deployments. With security, transparency, and governance embedded from the start, enterprises build resilience, trust, and long-term value in their AI journey. To highlight the importance of an effective strategy, it helps to look at real-world examples.

What real GenAI threats look like

Many organisations face blind spots as GenAI tools multiply. A survey found enterprises use an average of 66 GenAI apps, often without IT or security oversight. In one Hong Kong case, deepfake impersonation during a video call led to a $25 million fraud, underscoring the need for strong identity verification.

In another instance, a large enterprise deployed an agentic AI SOC analyst to combat alert fatigue and support its overwhelmed security team. False positives were a major issue, with some SOCs reporting rates as high as 99%. After implementation, the organisation saw a 90% drop in false-positive alerts, allowing analysts to focus on real threats. Automating triage and routine investigations freed up time for more strategic work. The result was cleaner alert dashboards, faster incident response, lower burnout, and a more resilient SOC.

As generative AI becomes more embedded in critical functions, regulators are stepping in to enforce responsible use and transparency.

Facing the compliance and trust challenge

In addition to managing risks, organisations face growing pressure to meet regulatory mandates and uphold ethical standards in their GenAI deployments.

Governments and regulators are taking action to govern generative AI in cybersecurity. The EU AI Act and U.S. Executive Orders now require GenAI systems to ensure transparency, implement watermarking, and provide explainability. Organisations that handle sensitive data or offer public-facing AI applications must comply with these rules or face penalties.

For instance, financial services firms need to make sure AI models used in fraud detection are explainable, while healthcare providers must offer clear transparency around AI-generated diagnoses or recommendations.

On the ethical front, leaders must prevent GenAI from perpetuating bias, exposing customer data, or spreading misleading information. Transparency, fairness, and accountability should be integral to every AI deployment.

Generative AI in cybersecurity: a call to responsible innovation

Generative AI can either strengthen cybersecurity or deepen risks. Its impact depends on how it's used. Success depends on how organisations balance innovation with strong governance and vigilance. For CISOs, CIOs, and decision-makers, mastering this balance is essential. Those who navigate these dual forces responsibly will unlock GenAI's full potential and lead in the evolving threat landscape.

Infosys®
Navigate your next

For more information, contact infosysbpm@infosys.com