Redefining resilience: Cybersecurity in the gen AI era

When it comes to gen AI and cybersecurity, who has the advantage, attackers or defenders? According to the World Economic Forum's Global Cybersecurity Outlook Report 2024, 56% of executives believe that attackers will have the advantage over defenders in the next two years[1], highlighting the urgent need to reinvent cybersecurity for the gen AI era.

Gen AI's impact on the threat landscape

Like many businesses and government organizations, cybercriminals are eager to harness the potential of gen AI, leading to a rise in gen AI-powered cyberattacks. There has been a notable surge in ransomware attacks, for example, which have risen 76% since the launch of ChatGPT at the end of 2022[2]. These attacks are often initiated through gen AI-powered phishing, and are affecting sectors like local governments, education, manufacturing and healthcare. Malicious large language models (LLMs), such as Fraud GPT and PentestGPT, are creating content to facilitate cyberattacks. These LLMs can be purchased for as little as $200 a month on the dark web.

Phishing attacks have also surged—by a staggering 1,265%—since the launch of ChatGPT[3]. For example, we're seeing a huge increase in voice deepfakes emulating executives to fraudulently authorize financial transfers. Recently, Hong Kong Bank suffered a $25 million loss due to a sophisticated deepfake scam. The scammers digitally recreated the company's chief technology officer, along with other employees, on a conference call instructing colleagues to transfer money[4].

[1] Global Cybersecurity Outlook Report 2024
[2] Accenture Cyber Threat Intelligence Research
[3] SlashNext State of Cyber Phishing Report 2023
[4] Deepfake scammer walks off with $25 million in first-of-its-kind AI heist

Threat actors like hackivist group Ghost Sec have been experimenting with dark LLMs to create python-based ransomware, which is distributed with high levels of obfuscation that increase its potential success[5].

According to Accenture Cyber Intelligence research, certain industries, such as financial services, government and energy, are more targeted when it comes to gen AI attacks. These industries tend to use more sophisticated technology making them more vulnerable to sophisticated attacks. That's why sectors like financial services and government are actively developing and customizing defenses against gen AI attacks.

Gen AI-specific vulnerabilities

Gen AI exposes organizations to a broader threat landscape, more sophisticated attackers and also new points of attack. As organizations move from pilots and discrete use cases to larger-scale, gen AI implementations, the cybersecurity risks will increase. That's because there will be more scale and complexity of adoption, for example, users in systems, more data and more integration. These increased risks span everything from gen AI model disruption and prompt injection to training data exposure, theft and manipulation. Vulnerabilities like these are new, and most organizations are not prepared to handle them. New capabilities such as shadow AI discovery, LLM prompt and response filtering and specialized AI workload integration tests are now required to properly mitigate these new risks.

Whether guarding against AI-powered attacks or protecting their own AI landscapes, organizations must update their security posture—and fast. The key to gaining the upper hand in the era of gen AI will be embedding security by design along your journey.

[5] Accenture Cyber Threat Intelligence Research

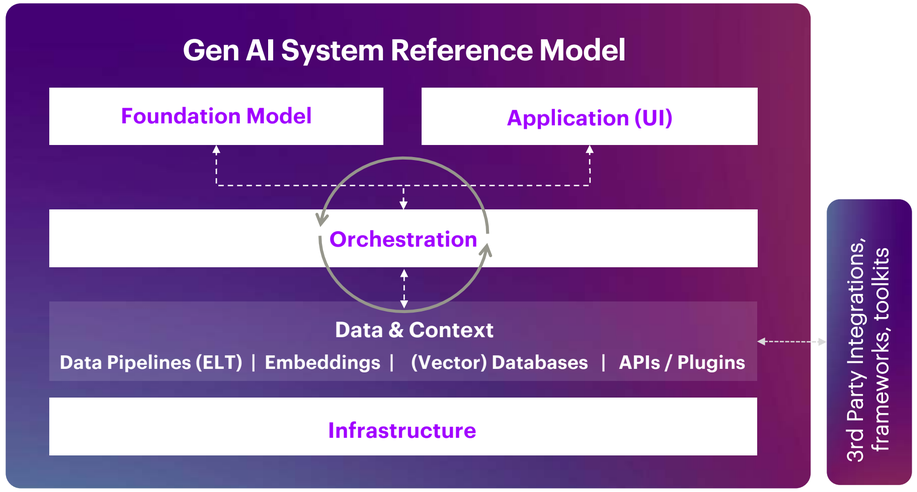
Accelerating the secure gen AI journey

Companies doing well recognize that security isn't slowing them down, but is key to accelerating gen AI success. In order to accelerate the adoption of gen AI at scale and to protect enterprise gen AI environments effectively, companies should leverage the following recommendations:

Incorporate gen AI security in Governance, Risk, and Compliance (GRC): Gen AI security should be an integral part of GRC, establishing a clear governance framework, policies and processes. Organizations must also stay up-to-date with evolving regulations. For example, the European Union AI Act aims to ensure AI systems are developed and deployed with security considerations, and the Biden administration's executive order lays the groundwork for secure development and use of AI. Engaging in private and public partnerships with regulators can help companies influence future regulation.

Assess the gen AI security risk level: Conduct a comprehensive security assessment —informed by the latest cyber intelligence— to understand the current security maturity within your gen AI environment. Evaluate gen AI architectures and ensure alignment with industry best practices. The Accenture Gen AI Security Diagnostic can provide insights into areas that require improvement for a more secure adoption of gen AI.

Secure gen AI environments at every layer: Organizations must focus on securing the entire gen AI stack, including the data layer, the foundational model, gen AI applications, as well as identity access and controls. Traditional security measures can be replicated, but AI-specific solutions should also be explored to address the unique vulnerabilities of gen AI environments.



Reinvent cyber resilience with gen AI

The good news is, gen AI also presents an opportunity for cyber defense and the reinvention of cybersecurity. By fully leveraging gen AI, organizations can turn the tables on potential attackers and enhance their cyber defense capabilities.

Traditional security solutions alone are insufficient to combat AI-powered risks. Organizations should embrace AI-powered defense technologies, and test using the gen AI technologies that threat actors could use against them. Some examples include AI-powered red teaming and penetration testing—which will become mandatory for organizations as gen AI regulations evolve.

Many platform companies and hyperscalers are releasing AI security features in their own environments and for broader consumption. Accenture's Managed Detection and Response (MxDR) service is powered by security-specific gen AI intelligence from Google Cloud, and is designed to integrate with common security environments and other clouds. There are new players in the space that have created gen AI-security-specific solutions from scratch to protect environments.

Consolidating security vendors can also reduce complexity and enhance your overall security posture. Many organizations have 40 to 50 different security tools in place today—which is costly and not secure.

Client stories

Lendlease: Lendlease needed the flexibility to adapt to shifting global risks. Accenture and Google Cloud collaborated to create a next-generation detection and response capability, leveraging gen AI and powered by a specific large language model designed for security use cases. This resulted in improved incident detection, response actions, communication and remediation.

Large Australian Bank: Accenture worked with a large Australian Bank to transform their environment into a gen AI-powered ecosystem with a strong focus on security. Specific data protection and security measures were implemented to safeguard the data lake, gen AI applications and digital identity. Security played a crucial role in enabling the responsible adoption of gen AI and accelerating the bank's business objectives.

Get in touch

Explore the next steps and opportunities for new growth and customer relevance by bringing your team to our Accenture Gen AI Studios.

Contact Daniel Kendzior, Managing Director, Accenture Security
daniel.kendzior@accenture.com

accenture