Press contact:
Florence Lievre
Tel.: +33 1 47 54 50 71
Email: florence.lievre@capgemini.com

AI and Gen AI are set to transform cybersecurity for most organizations

While Gen AI heightens vulnerabilities, more than half of organizations also anticipate faster threat detection and increased accuracy through its use

Paris, November 19, 2024 – The Capgemini Research Institute's new report, "New defenses, new threats: What AI and Gen AI bring to cybersecurity", published today, suggests that while new cybersecurity risks are emerging, due to the proliferation of AI and generative AI (Gen AI), these technologies represent a transformative shift in reinforcing cyber-defense strategies for the long term to predict, detect, and respond to threats. Two thirds of organizations are now prioritizing AI within their security operations.

According to the report, while AI is considered by organizations as a strategic technology to strengthen their security strategies, the increased adoption of Gen AI across various industries[1] brings heightened vulnerability. Gen AI introduces three major risk areas for organizations: more sophisticated attacks with more adversaries, the expansion of the cyber-attack surface, and a growth in vulnerabilities in the entire lifecycle of custom Gen AI solutions. These risks are also compounded by the misuse of AI and Gen AI by employees which can significantly increase the risk of data leakage.

Two in three organizations are wary of increased exposure to threats
Almost all organizations surveyed (97%) say they have encountered breaches or security issues related to the use of Gen AI in the past year. Gen AI also brings additional risks, including hallucinations, biased, harmful, or inappropriate content generation, and prompt injection attacks[2]. Two in three organizations (67%) are worried about data poisoning and the possible leakage of sensitive data through the training datasets used to train Gen AI models.

Moreover, Gen AI's ability to generate highly realistic synthetic content is posing additional risks: more than two in five organizations surveyed (43%) said they have suffered financial losses arising from the use of deepfakes.

Nearly 6 in 10 believe they need to increase their cybersecurity budget to bolster their defenses consequently.

AI and Gen AI are paramount for detecting and responding to attacks
Surveying 1,000 organizations[3] that have either considered AI for cybersecurity or are already using it, the report finds that most rely on AI to strengthen their data, application and cloud security due to the technology's ability to rapidly analyze vast amounts of data, identify patterns and predict potential breaches.

---

[1] Nearly one-quarter (24%) of organizations have enabled Gen AI capabilities in some or most of their functions and locations - Capgemini Research Institute, "Harnessing the value of generative AI 2nd edition: Top use cases across sectors," July 2024.

[2] This involves using malicious inputs to manipulate AI and Gen AI models, compromising their integrity.

[3] 1,000 organizations across 12 sectors and 13 countries in Asia Pacific, Europe, and North America, with annual revenues of $1 billion and over.

More than 60% of them reported a reduction of at least 5%, in their time-to-detect, and nearly 40% said their remediation time fell by 5% or more after implementing AI in their security operations centers (SOCs).

Three in five organizations surveyed (61%) believe AI to be essential to effective threat response, enabling them to implement proactive security strategies against increasingly sophisticated threat actors. In addition, the same proportion of respondents foresee Gen AI strengthening proactive defense strategies in the long term, anticipating faster threat detection. Over half of them believe also that the technology will empower cybersecurity analysts to concentrate more on strategy for combating complex threats.

"The use of AI and Gen AI has so far proved to be a double-edged sword. While it introduces unprecedented risks, organizations are increasingly relying on AI for faster and more accurate detection of cyber incidents. AI and Gen AI provide security teams with powerful new tools to mitigate these incidents and transform their defense strategies. To ensure they represent a net advantage in the face of evolving threat sophistication, organizations must maintain and prioritize continuous monitoring of the security landscape, build the necessary data management infrastructure, frameworks and ethical guidelines for AI adoption, and establish robust employee training and awareness programs," said Marco Pereira, Global Head Cybersecurity, Cloud Infrastructure Services, Capgemini.

Methodology

The Capgemini Research Institute surveyed 1,000 organizations that have either considered AI for cybersecurity or are already using it, across 12 sectors and 13 countries in Asia Pacific, Europe, and North America. They have annual revenues of $1 billion and over. The global survey took place in May 2024. Organizations surveyed represent a diverse range of sectors including automotive; consumer products; retail; banking; insurance; telecom; energy and utilities; aerospace and defense; high-tech; industrial equipment manufacturing; pharma and healthcare and public sector.

About Capgemini

Capgemini is a global business and technology transformation partner, helping organizations to accelerate their dual transition to a digital and sustainable world, while creating tangible impact for enterprises and society. It is a responsible and diverse group of 340,000 team members in more than 50 countries. With its strong over 55-year heritage, Capgemini is trusted by its clients to unlock the value of technology to address the entire breadth of their business needs. It delivers end-to-end services and solutions leveraging strengths from strategy and design to engineering, all fuelled by its market leading capabilities in AI, cloud and data, combined with its deep industry expertise and partner ecosystem. The Group reported 2023 global revenues of €22.5 billion.

Get the Future You Want | www.capgemini.com

About the Capgemini Research Institute

The Capgemini Research Institute is Capgemini's in-house think-tank on all things digital. The Institute publishes research on the impact of digital technologies on large traditional businesses. The team draws on the worldwide network of Capgemini experts and works closely with academic and technology partners. The Institute has dedicated research centers in India, Singapore, the United Kingdom and the United States. It was recently ranked #1 in the world for the quality of its research by independent analysts.

Visit us at https://www.capgemini.com/researchinstitute/