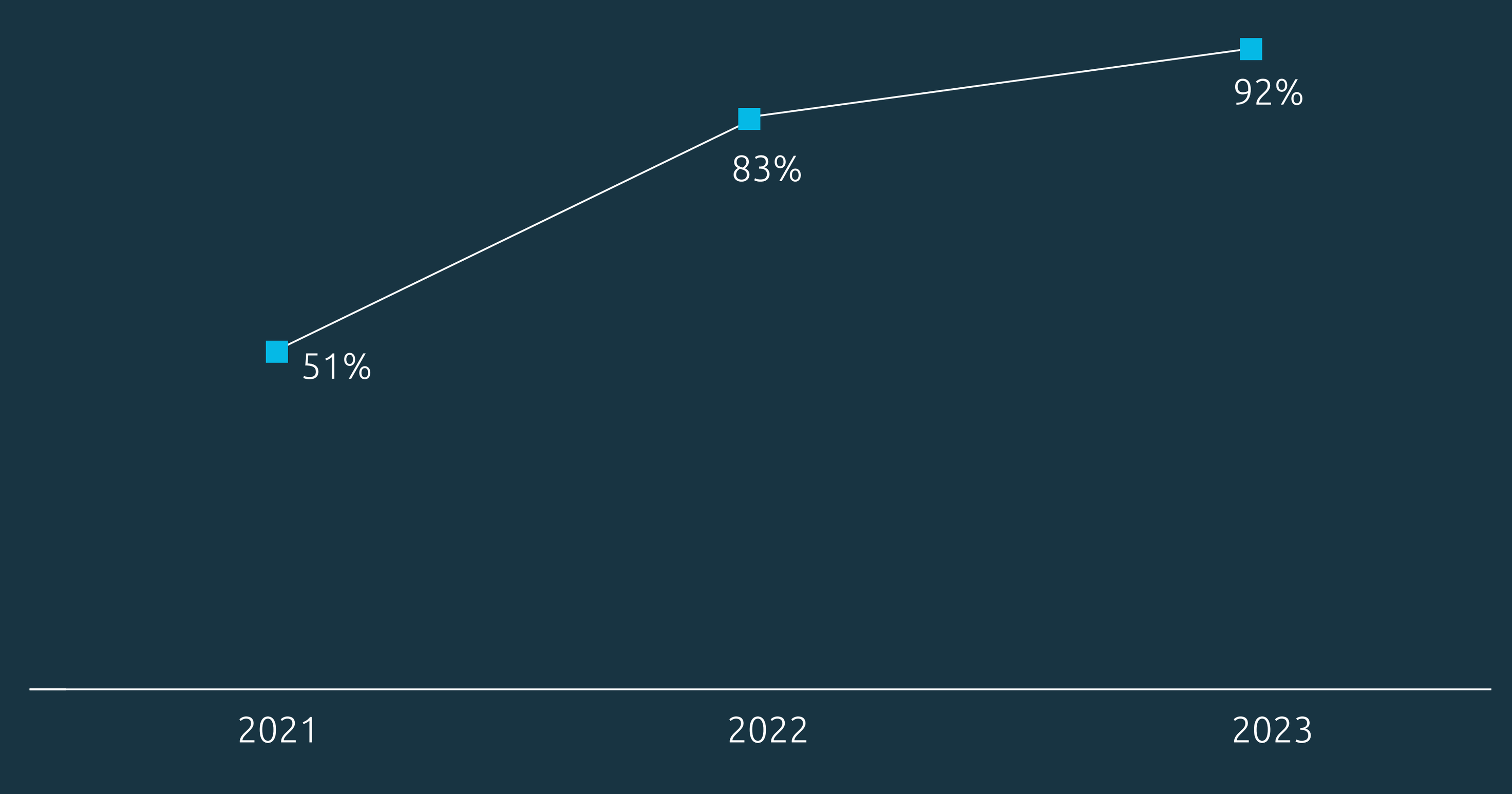
New defenses, new threats

What AI and Gen AI bring to cybersecurity

There has been a substantial increase in cybersecurity breaches from 2021 to 2023

In the past three years, the proportion of organizations experiencing one or more breaches has grown from 51% in 2021 to 92% in 2023

% of organizations that experienced a cybersecurity breach, 2021–23



Source: Capgemini Research Institute, AI and Gen AI in cybersecurity survey, May 2024, N=1,000 organizations.

The breaches have resulted in average financial damages of $50 million for half of the organizations surveyed over the past three years

The AI and Gen AI risk landscape is evolving rapidly

Three ways in which AI and Gen AI can pose risks

More sophisticated attacks and more adversaries

Gen AI lowers barriers for threat actors, heightening cyber risks and enabling more sophisticated attacks. Cybercriminals leverage Gen AI for phishing, social engineering, deepfakes, malware creation, automated hacking, vulnerability exploitation, and bypassing security by mimicking real user behavior or creating malicious GPTs.

Expansion of the cyber-attack surface

Organizations face an expanded attack surface with AI adoption, including prompt injection attacks on Gen AI models, vulnerabilities in AI-integrated apps, and 'shadow AI' used outside IT control. Internal misuse of AI tools further increases risk.

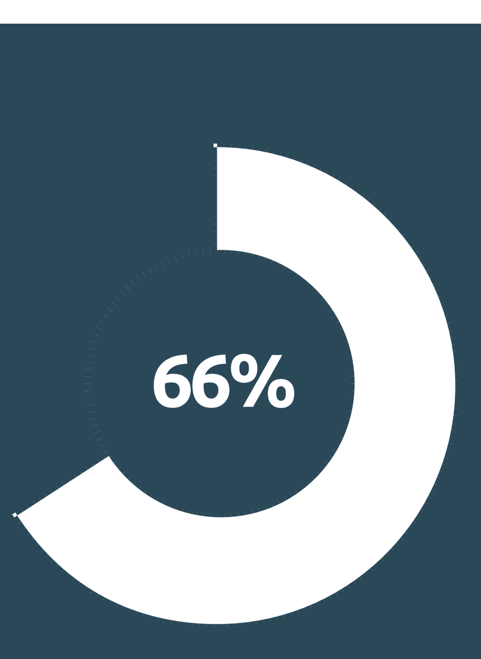
Lifecycle management of custom Gen AI solutions

Securing the entire lifecycle of Gen AI solutions—from data collection to maintenance—is essential to protect sensitive information and maintain integrity. Gen AI also introduces risks, such as hallucinations and vulnerabilities, particularly in code generation, which can lead to potential security issues.

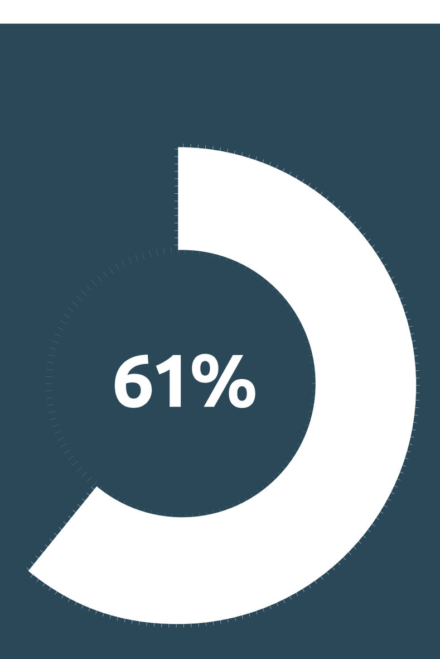
More than two in five organizations have suffered financial losses arising from the use of deepfakes

Nearly six in ten organizations believe they need to increase their security budget to bolster their cyber defenses

Organizations' reliance on AI to reinforce their security infrastructure is intensifying



Use of AI in cybersecurity is a high priority for our organization



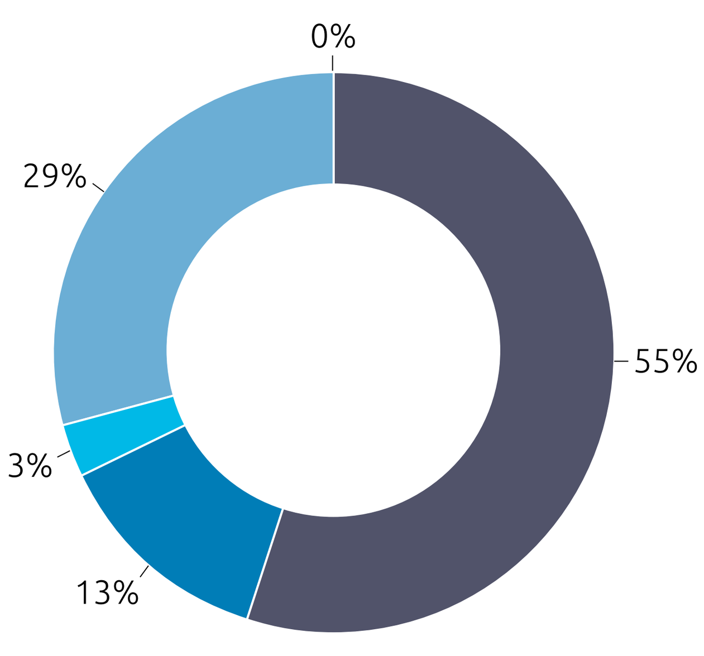
Without AI, we would not be able to identify critical threats

Source: Capgemini Research Institute, AI and Gen AI in cybersecurity survey, May 2024, N=1,000 organizations.

More than three in five organizations find AI provides higher efficiency in cybersecurity

Gen AI will reinforce cybersecurity

Leadership at more than half of the organizations believe in Gen AI for security

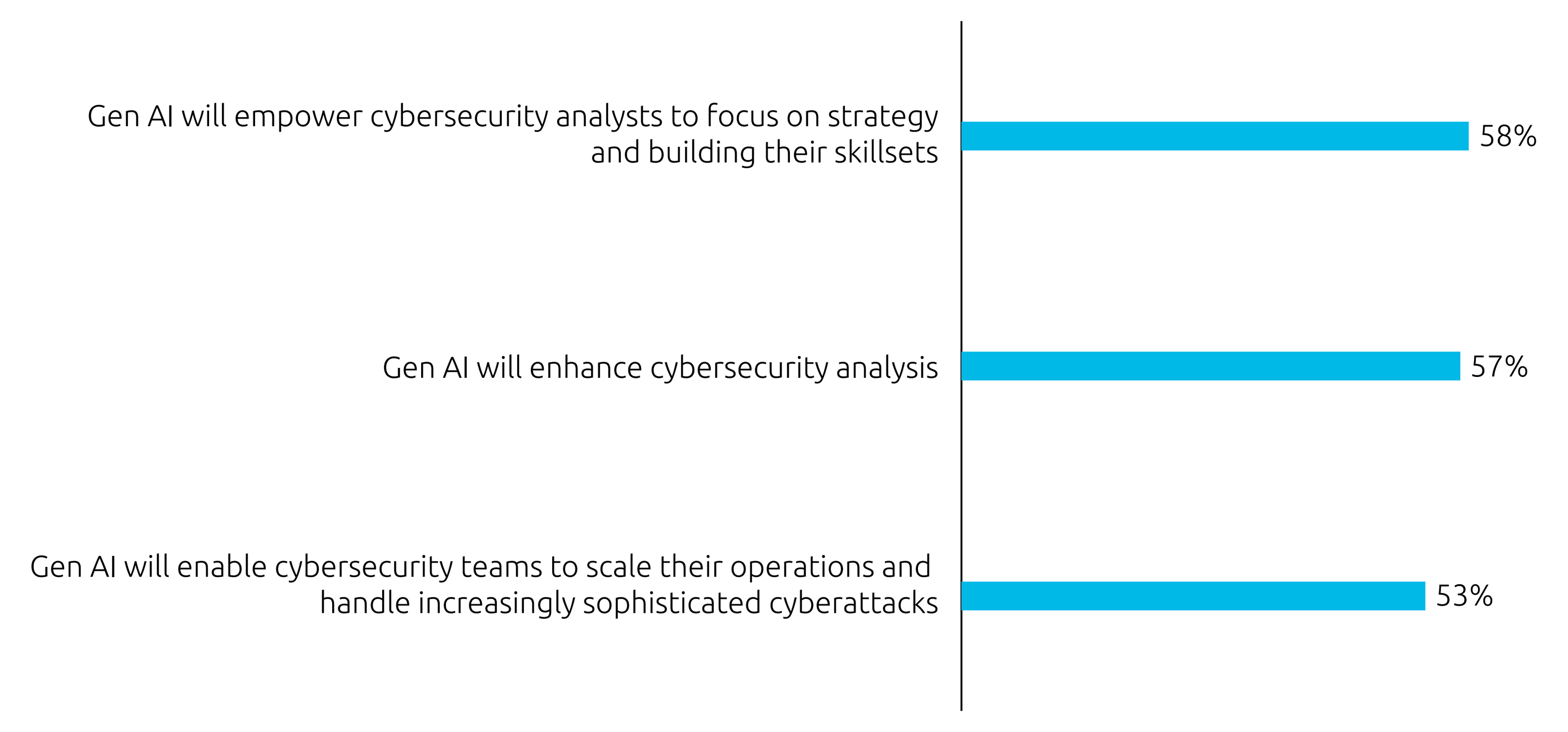


- Our leadership is a strong advocate of Gen AI to advance cybersecurity
- Our leadership is taking a 'wait-and-watch' approach to Gen AI's use in cybersecurity
- Our leadership is not convinced of the potential of Gen AI to advance cybersecurity
- Our leadership is divided on the potential of Gen AI to advance cybersecurity
- Our leadership is not sufficiently aware of the potential of Gen AI to advance cybersecurity

Source: Capgemini Research Institute, AI and Gen AI in cybersecurity survey, May 2024, N=1,000 organizations.

Gen AI will empower cybersecurity analysts to concentrate on strategy for combating complex threats

How will Gen AI change the roles of cybersecurity professionals?



Source: Capgemini Research Institute, AI and Gen AI in cybersecurity survey, May 2024, N=1,000 organizations.

Recommendations: Using AI and Gen AI to strengthen your cyber defenses

Strengthening the defenses of your organizations using AI and Gen AI

Assess your security landscape and risks continuously

- **Develop** AI/Gen AI security strategy
- **Establish** framework, policies, and guidelines
- **Formulate** plans for integration and monitoring
- **Create** awareness and training programs
- **Safeguard** business processes and cultivate a culture of risk awareness

Acquire necessary infrastructure

Source: Capgemini Research Institute analysis.

Download report

Subscribe to our research