opentext™

The peril and promise of generative AI in application security

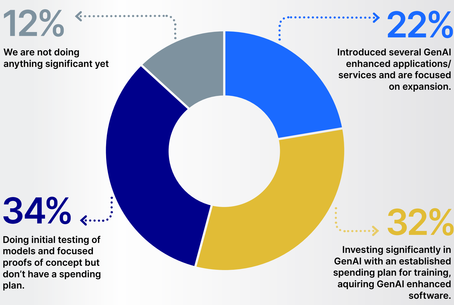
By April 2024,

17% of organizations had introduced generative AI (GenAI) applications into production, with another 38% making significant investments

GenAI brings unprecedented opportunities to strengthen cybersecurity, but also introduces new risks that require cutting-edge solutions.

Let's see how AI is shaping the future of application security and what steps you can take to harness AI safely.

What is your organisation`s current state of evaluating or using Generative AI(GenAI)?



The double-edged sword of GenAI

While AI-driven tools enhance threat detection, they can also be weaponized to create sophisticated attacks.

GenAI's reliance on complex, often untraceable open-source models and data creates vulnerabilities, allowing attackers to insert malware or back doors into widely used repositories.

Attackers are using generative models to develop more complex phishing scams, code injection techniques, data poisoning, and automated data breaches.

IDC predicts

40%

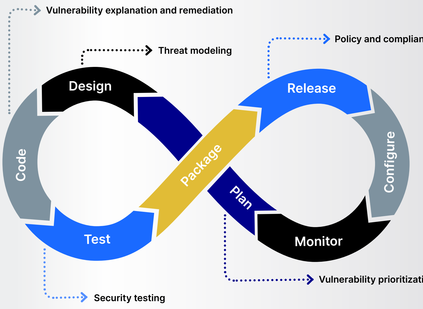
of new apps will integrate AI by 2026

Benefits of AI in application security

AI brings critical advantages, including real-time threat intelligence, automated response, and predictive analysis to prevent attacks before they happen.

Incorporating GenAI into application security can result in more secure, efficient, and resilient applications while freeing developers and security professionals to focus on more complex and challenging problems.

Enhancing application security with GenAI



Managing AI risks in AppSec

Organizations must adopt strong risk management strategies, focusing on ethical AI, transparency, and robust security practices to counter potential misuse of AI technologies.

Despite the risks, the potential of AI to redefine security makes it essential. Balancing innovation with proactive risk management will be key for safe AI adoption in security.

IDC research shows

44%

of organizations customize open-source GenAI models,

rising to

54%

among those with GenAI in production.

For a more detailed analysis of the security challenges related to GenAI and how to unlock its potential in application security, read the IDC white paper.

opentext™