

# How to achieve DevSecOps in the era of AI coding assistants



## Increasing software release frequencies

As the reliance on software applications intensifies, IDC forecasts that more than

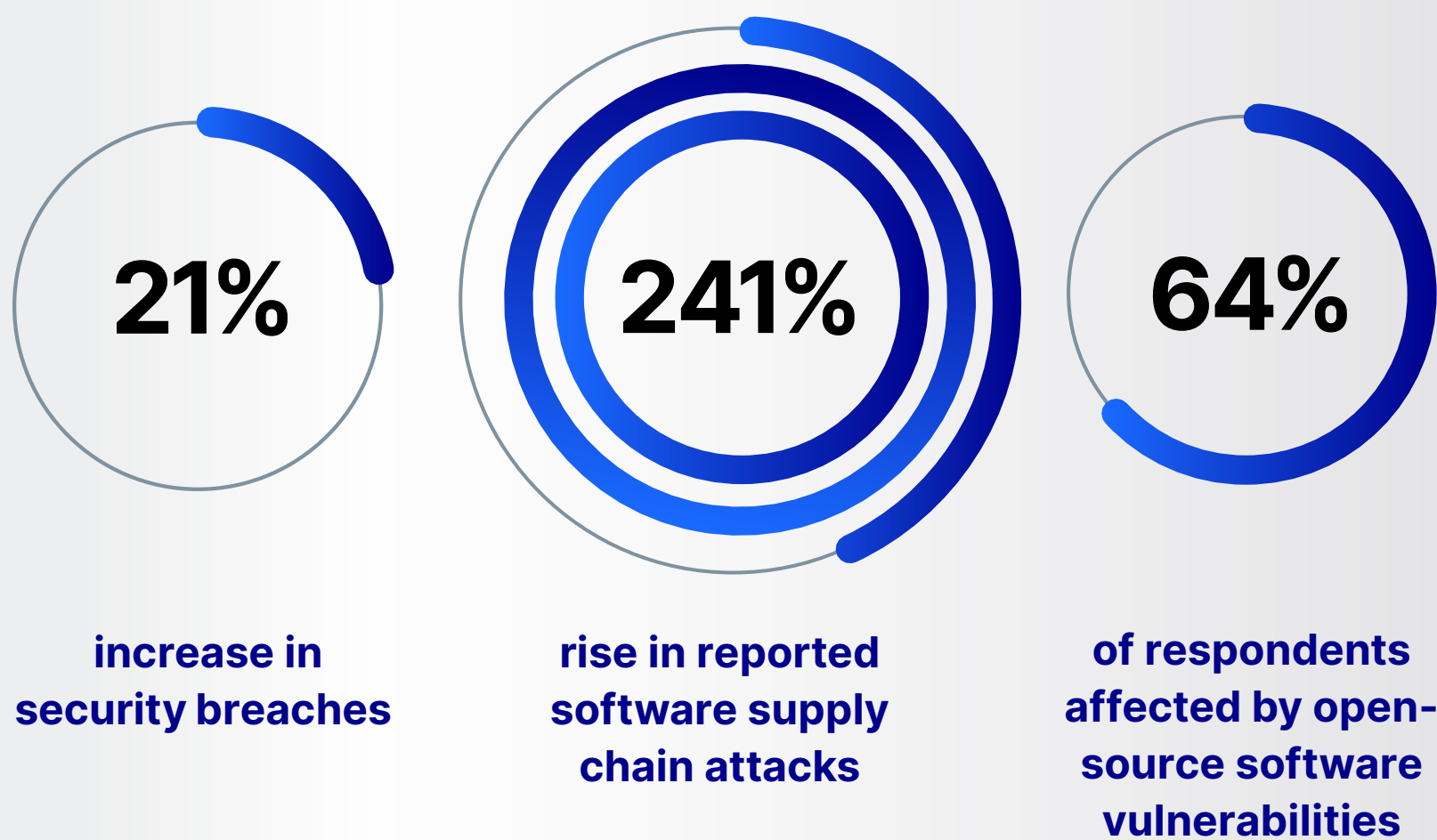


net-new applications will be developed by 2028.

With more applications comes a larger attack surface, providing more opportunities for cyberthreats, vulnerabilities, and breaches.

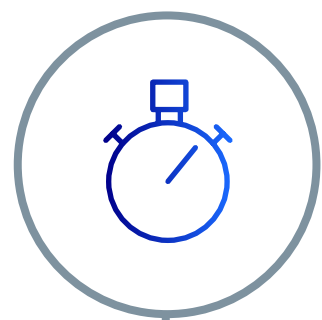
## Prevailing lack of DevSecOps maturity

From 2022 to 2023, IDC survey data revealed a



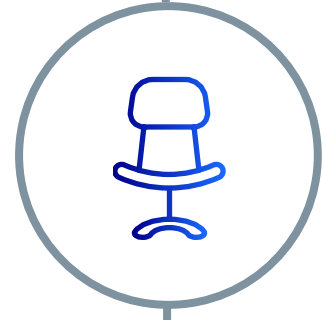
## Security at the speed of DevOps

DevSecOps automation allows organizations to develop and release higher-quality applications more swiftly by integrating security seamlessly into the development process. This automates security checks, code analysis, and vulnerability assessments throughout the DevOps pipeline.




**Reduce manual work**

Automating repetitive security checks throughout the DevOps pipeline frees developers and security professionals to focus on more strategic tasks, leading to faster development cycles and quicker time to market.




**Lessen the swivel chair effect**

Automation lessens the “swivel chair effect,” which happens when DevOps teams are manually switching between security and development tools. By putting the “Sec” in “DevSecOps” you can improve developer flow, minimize delays, and avoid bottlenecks in the development process.



**Minimize human error**

Automation minimizes the chance of human error.



**Improve collaboration**

Developers and security teams get a shared view of security risks, promoting a culture of “security by design,” where security is an integrated part of the development process, not an afterthought.

Read the full report, [Achieving High-Velocity DevOps with Security Automation](#) ›