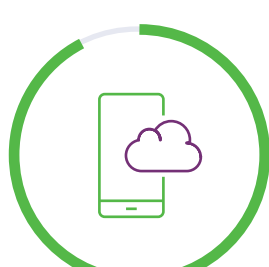


[illegible]

Software security must be a top priority going forward. Here are five reasons why.

Software is taking on new forms, incorporating internal and third-party components, APIs, new architectures, containers, and more. This software complexity creates software vulnerability.



90%

Apps that will be cloud-native
in 5 years²

Software drives modern business, but it can be a double-edged sword, presenting a massive attack surface ripe for targeting. Organizations that release vulnerable software are jeopardizing their reputation, customer relationships, and bottom line.



13.319

Vulnerabilities detected in 2019
across 1.607 apps⁴

Developers are delivering software faster while also becoming the “gatekeepers” of security, a balance that’s difficult to strike. New developer-centric solutions like automated AST tools that fit right into their existing workflows and game-like AppSec training make it exponentially easier for them to embed security into code.



96%

DevOps leaders that are prioritizing "software development life cycle" (SDLC) automation in 2021⁶

Organizations that desire
developers to be properly
trained in producing secure
code⁷

As developers move faster, they're relying more on open source code versus building software from scratch. But, without SCA, the benefits of open source can easily be overshadowed by the risks, including security vulnerabilities, license compliance, and loss of IP control.



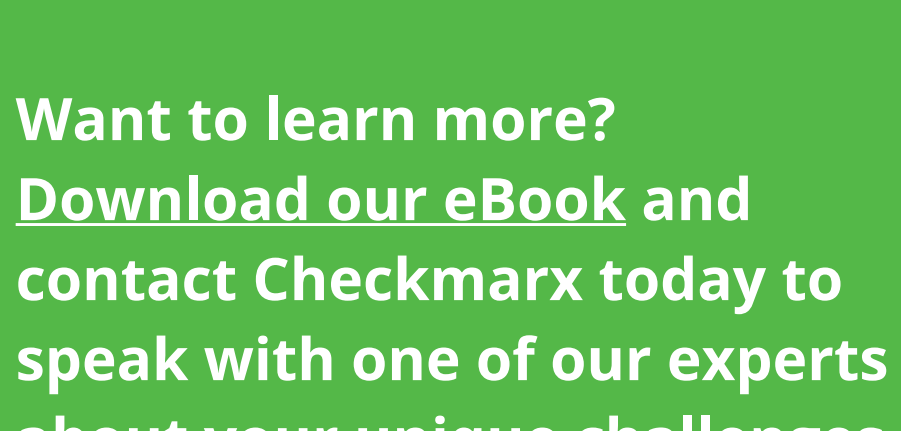
130%

Uptick in CVEs discovered within open source software from 2018 to 2019⁹

Digital transformation has shifted into hyperdrive, with software serving as the catalyst for innovation. It's imperative to conduct security testing earlier in development and leverage solutions that streamline workflows and expedite vulnerability remediation.



35%
IT decision makers that cite
cybersecurity as the top investment
priority when it comes to digital



9: <https://info.risksense.com/open-source-spotlight-report-pr>