Checkmarx

REPORT

The Future of

APPLICATION SECURITY 2024

The State of Application Security

Application development has changed.

It has moved from waterfall development with infrequent releases, to agile development and continuous delivery. Software is deployed multiple times per day, development is complex, and it is increasingly cloud-native. This has dramatically changed how organizations need to secure their applications.

There is more software deployed in more environments, and less time available to secure it.

The responsibility has shifted away from dedicated security teams and is now shared between AppSec managers and developers. Trust between CISOs, development and security teams - called #DevSecTrust - is critical if the enterprise going to successfully reduce the business risk of vulnerable applications.

Building #DevSecTrust requires a holistic approach. CISOs must understand the issues facing their AppSec and development teams while trying to gain greater visibility over their enterprise's AppSec. AppSec tools must meet the needs of multiple stakeholders, and the rising influence of developers must be recognized if organizations are going to successfully continue to improve their application security posture.

The third annual Future of Application Security survey reveals how key stakeholders are responding to this challenge. We surveyed 1504 developers, CISOs, and AppSec managers from a broad range of industries across the US, Europe, and Asia-Pacific regions.

Discover the current state of application security and areas of future investment that will support #DevSecTrust. Learn how you compare to your peers on AppSec program measurement, the AppSec tools they are using right now, and where they plan to invest in future. Explore developer experience and influence, and the challenges and concerns around cloud deployments.

92%

of companies had a breach due to an application they developed

91%

of companies have knowingly released vulnerable applications

67%

of applications are currently hosted in the cloud

Key Findings

1 Organizations are knowingly releasing vulnerable applications

92% of the organizations surveyed have suffered a breach due to a vulnerability in an application they developed. Yet, 91% have knowingly deployed vulnerable applications. Business deadlines are cited as a main reason for deploying vulnerable code.

Main breach causes

1. Stolen credentials, secrets, or weak authentication
2. Cloud resource, IaC, or container misconfiguration
3. Known and/or unknown vulnerability in code released to production

2 #DevSecTrust is critical

Team alignment and trust are crucial for a successful AppSec program. Alignment and trust between CISOs, AppSec professionals, and developers is necessary to identify and address vulnerabilities that could impact the business. Yet, there are some differences between CISOs, AppSec managers, and developers. Developers and AppSec managers focus on the things that are in their immediate control, while CISOs seem to take a more holistic approach to AppSec.

3 Developer influence is rising, making developer experience more important

Developers are increasingly powerful decision-makers in the buying process. Developer experience is a crucial when considering in any AppSec solution, with vulnerability prioritization, secure code training, and seamless AppSec integration all key focus areas.

Developers' top three security concerns

1. Security impeding development process
2. Difficulty knowing what to fix and how to prioritize risk
3. Lack of context to remediate vulnerabilities

4 Investment plans focus on consolidation, simplification,and improving the developer experience

Consolidation helps build #DevSecTrust and improve developer experience. By consolidating multiple AST solutions onto a single AppSec platform, it's easier to correlate findings, triage results, integrate with developer tooling, onboard faster reducing the learning curve, and see all your risks and vulnerabilities in a single place.

5 Cloud presents a complex, high-priority risk

67% of applications are currently deployed in the cloud and CISOs say managing cloud risk is their top priority in the coming year. AppSec managers and CISOs are concerned about data governance, identity and access management, and software supply chain risks.

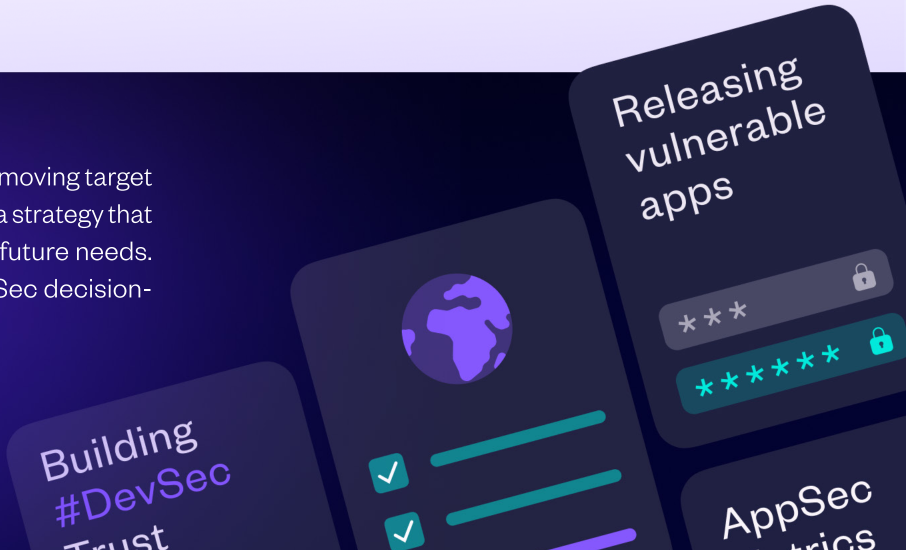
CISO priorities for 2024

1. Managing cloud risk
2. Managing AI risk
3. Increasing cyber transparency

67% of applications are currently deployed in the cloud

As the nature of applications changes, they are a moving target for AppSec programs. Organizations must devise a strategy that allows AppSec to evolve in parallel and predict future needs. To discover the full findings to inform your AppSec decision-making keep reading.

Keep reading to learn more!



Contents

The State of Application Security

Known Vulnerabilities and Increasing Complexities are Driving More Breaches

Application risk is business risk. With digital transformation moving organizations' physical processes and in-person engagement online, it means that enterprises are now relying on applications more than ever. That dependency can become dangerous for businesses of all sizes when vulnerabilities enter the application landscape.

Our survey shows that business risk is rising: 92% of companies surveyed have experienced at least one security breach as the direct result of a vulnerable application they developed in the past 12 months. This is a slight increase from 88% who reported breaches last year. Concerningly, most companies have experienced more than one breach: 2.44 per organization.

92% of companies have experienced at least one security breach in the past 12 months

A Code to Cloud Approach is a Must for Enterprises Today

The growing complexity of applications, paired with the increase in cloud-native development, has rapidly expanded the current attack surface for many enterprises. Because of this, we are seeing a shift to organizations looking to protect their entire software development lifecycle (SDLC), from the first line of code all the way to deployment and runtime in the cloud.

The increased attack surface is reflected in the range of factors that respondents said contributed to their breaches, including but not limited to: misconfigurations in cloud resources, Infrastructure as Code (IaC), containers, stolen credentials, weak authentication, and risks in software supply chains, including vulnerable APIs and open source components.

So, what does this mean? It highlights that breaches can happen anywhere across the SDLC. Modern application development requires a code to cloud approach in order to rise to the challenge of truly reducing business risk - especially when they are being developed with both custom and open source code.