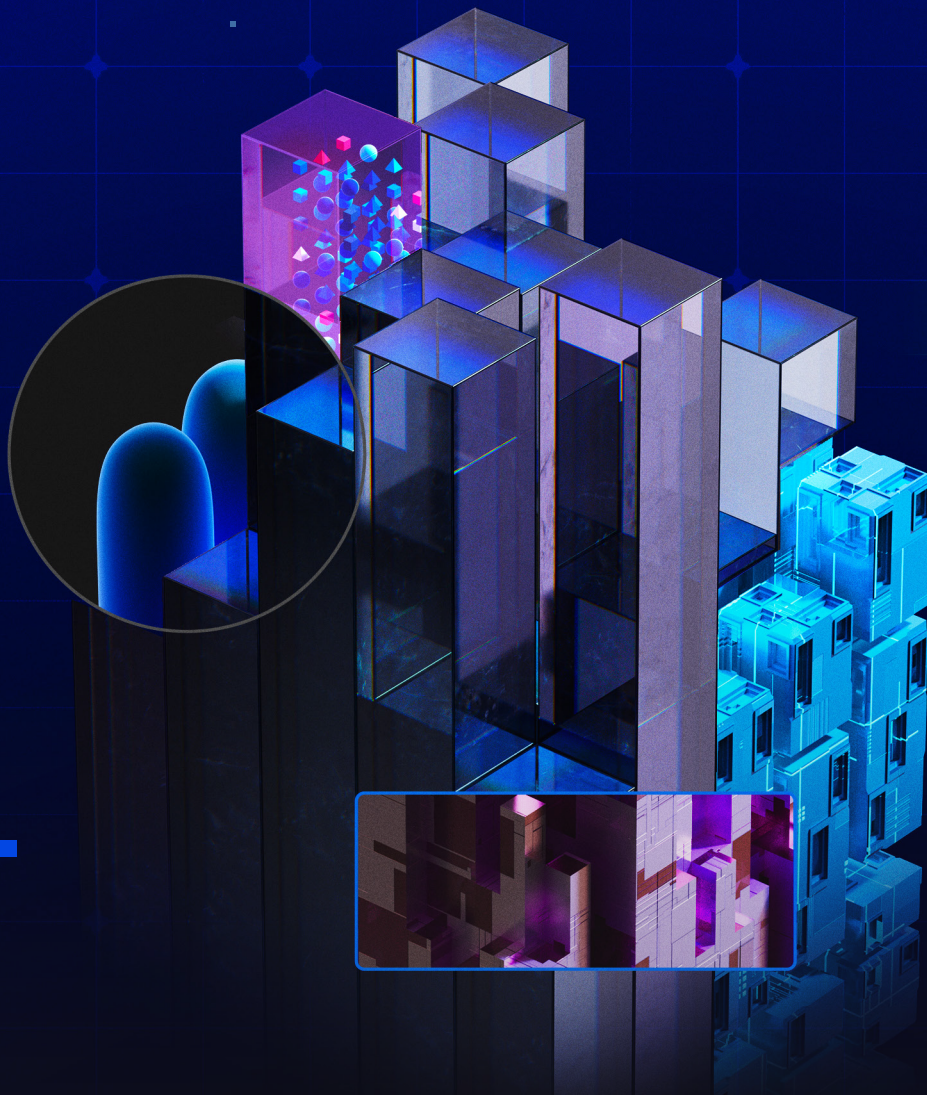




SURVEY ANALYSIS REPORT

Gaining Ground on Mobile DevSecOps

Maturity trends emerge from year-over-year
mobile application security report analysis

Table of contents

Introduction 2

TREND 1 3

TREND 2 5

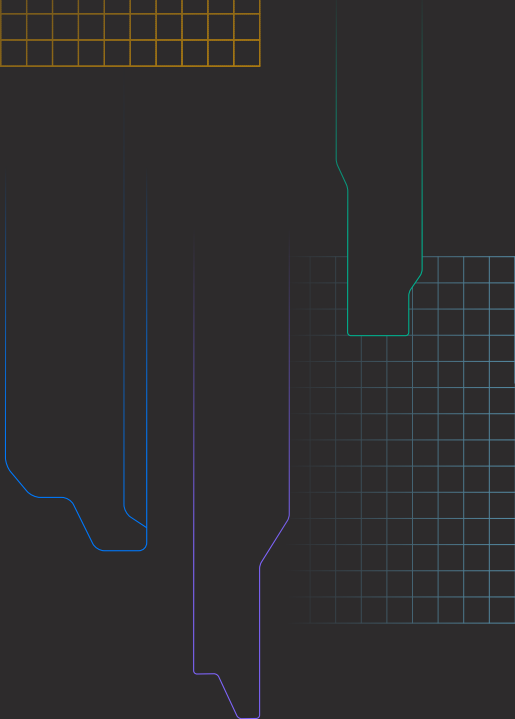
TREND 3 7

TREND 4 8

Summary 9

About Guardsquare 10

Research cited 10

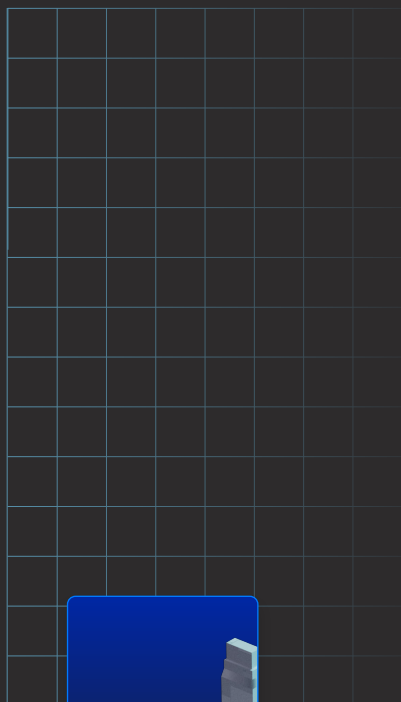


Introduction

A recent [TrendCandy survey](#) of mobile application developers and security leaders from around the world shows that the vast majority of organizations experienced one or more mobile app security incidents in the past year.

The root cause behind these persistent security issues has to do with the nature of mobile apps themselves. Mobile applications operate outside of trusted networks and controls, making any and all transactions inherently untrusted. This trust gap is further widened by increasing pressure to accelerate development cycles for new apps as well as widening adoption of AI-based coding and testing tools.

While the continuous onslaught of mobile app threats hasn't let up, other findings show signs of positive change. When comparing this current report to previous independent research published in [2024](#) and [2025](#), several trends emerge – ones that suggest a progressive shift is happening in how mobile application security is viewed and implemented at many organizations.

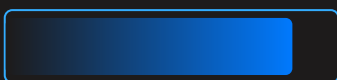


TREND 1

Organizations are maturing – from overconfidence in de facto mobile app protections toward better awareness of specific security needs.

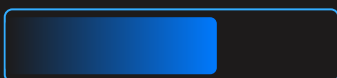


IN 2024



91%

of organizations felt they did not release unprotected mobile apps



67%

believed that OS-level protections (i.e., Android or iOS) alone were sufficient for keeping mobile apps secure



20%

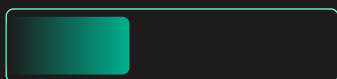
of organizations said they protected their mobile apps using DIY tools built in-house

IN 2025



93%

of respondents thought their current mobile app protections were sufficient



40%

of organizations only relied on OS-level protections or DIY security solutions

IN 2026



91%

prefer security that covers the entire SDLC



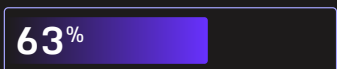
82%

say exposure to backend/API abuse is increasing, yet only 48% monitor API activity



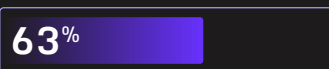
84%

of mobile app developers now acknowledge that OS-level protections aren't sufficient security on their own



63%

of respondents were aware of unauthorized modding or cloning of their mobile app in the past 12 months



63%

say they lack visibility into how attackers target their apps in the wild

2X

Fragmented visibility doubles time-to-remediation

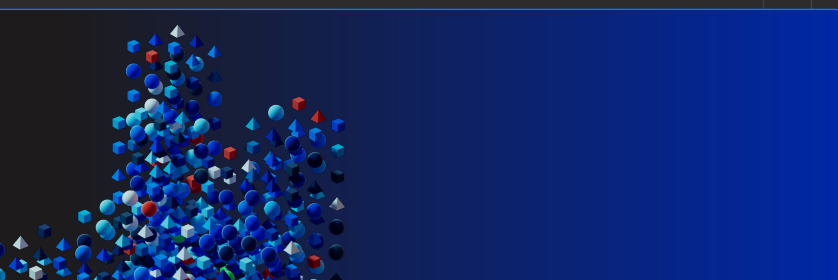
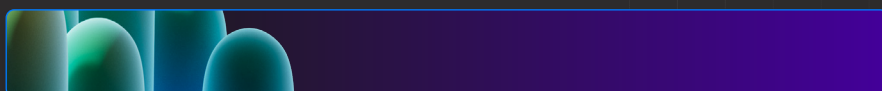
The first step in addressing many problems (not just security) is admitting that an issue actually exists. Overconfidence in existing security practices (OS-level protections and DIY tools) was a common theme among survey responses in both 2024 and 2025. But this year, things seem to be showing signs of positive change in a few key areas.

Two years ago, two-thirds (67%) of mobile developers thought OS-only protections were sufficient protections for their apps. But now, over 80% of developers are acknowledging that these protections on their own do not provide adequate mobile application security. The vast majority (91%) say they now prefer security that covers the entire software development lifecycle (SDLC) – from planning and design through release and maintenance.

The 2026 data also shows some specific awareness of where and why threat actors are targeting their apps. Over 80% of survey respondents have observed increasing exposure to API abuse and backend (server-side) mobile

application attacks. However, only 48% of organizations are actually monitoring their API activity. This suggests a significant visibility gap – more than half the industry is flying blind while their APIs and mobile app backends are being targeted. Additionally, nearly two-thirds of respondents said they were aware of unauthorized modding or cloning of their mobile apps over the past 12 months (which also has API/server-side implications when it comes to common fraud attacks against high-value apps for retail, banking, mobile wallets, and other financial services transactions).

There's also been significant progress in terms of "knowing what we don't know". Nearly two-thirds of respondents acknowledge a visibility gap, reporting that they can't see how attackers are targeting their mobile apps in the wild. This points to a need for more and/or better threat monitoring tools at many organizations. Security leaders should also note that teams reporting fragmented visibility (meaning a lack of integrated client- and server-side visibility) took twice as long to remediate mobile security issues.



TREND 2

Time-to-market pressure continues to build for developers – and some consequences of compromised mobile app security are coming to the surface.



IN 2024

**30%**

of organizations believed that investing in mobile app security would delay their time to market

IN 2025

**63%**

reported that mobile app security had delayed releases, impacting time to market

**74%**

indicated their app dev teams were under increased pressure to accelerate velocity

**71%**

acknowledged this pressure had compromised their mobile app security

IN 2026

38%

of respondents believe security slows development

79%

now cite time-to-market pressure as the top barrier to stronger protection

57%

of developers admit shipping code they knew was vulnerable due to deadlines

65%

reported customer churn/uninstalls due to security issues

96%

of mobile developers now use AI in building apps and SDKs and 81% say AI-generated code has introduced new vulnerabilities

Some things change, while others stay constant. Developers remain under increasing pressure to accelerate the delivery of new mobile applications, SDKs, and version updates.

In 2024, nearly one-third of surveyed developers felt that any security investment would effectively slow down their ability to deliver mobile apps on schedule. In 2025, nearly two-thirds of respondents felt security had actually delayed a release and impacted time to market. Nearly three-quarters of organizations were under elevated pressure to accelerate release velocity, and over 70% said this pressure had compromised the security of their mobile applications.

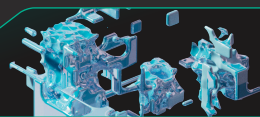
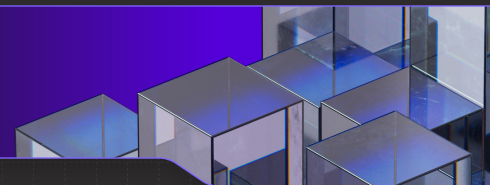
Today, time to market is still a dominant fact of life for mobile app development teams. Even more developers (38%) now say security slows them down and nearly 80% say time-to-market pressure is the top barrier to stronger protection.

Widespread adoption of AI-generated code is a key differentiator for accelerating delivery cycles in 2026. Nearly all respondents now use AI to build their mobile apps and SDKs – and over 80% admit this practice has introduced new vulnerabilities.* Over half of developers admitted to shipping code that they knew was vulnerable due to deadlines.



These findings align with third-party studies and quantitative analysis of AI-generated code samples. [Stanford researchers](#) found that seasoned app developers using AI tools were 80% more likely to produce less secure code than equally experienced devs coding without assistance. [NYU researchers](#) concluded that up to 40% of code generated by AI co-pilots contains exploitable security vulnerabilities. A [December 2025 report](#) comparing AI co-authored code against similar human-only code found that the AI-generated samples had both a higher volume of issues as well as higher severities – 40% more critical issues and 70% more major issues.

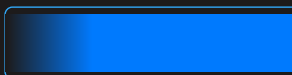
Compromising on mobile app security in deference to delivery cadence pressure is also having a direct impact on line-of-business concerns. About two-thirds of organizations have experienced customer churn and/or app uninstalls due to security issues.



TREND 3

Mobile app risk is becoming structural. Organizations are getting better at absorbing and normalizing incidents, even as threats become more persistent.

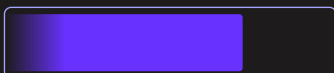
IN 2024



87%

of respondents reported at least one mobile app security incident in the previous twelve months

IN 2026



72%

say they experienced at least one mobile security incident over the last year, while

92%

of organizations report threat levels increasing in the past two years

Over the last two years, organizations reporting one or more security incidents have dropped from 87% (2024) to 72% (2026), while the vast majority (92%) of organizations have observed increasing threat levels over that same period.

This is a particularly interesting and nuanced development. It would be easy to attribute the 15% drop as simply “fewer security incidents reported” and correlate that to improved incident prevention. But the combined context that most organizations are observing a worsening mobile threat landscape

(which aligns with [recent mobile threat data from Verizon](#)) suggests that orgs are more specifically getting better at proactively detecting, managing, and surviving attacks.

Security incidents remain a significant problem, but organizations seem to be getting better at absorbing the impact of endemic mobile threats as they increase in volume and sophistication each year. This looks to be another sign of incremental security maturation for most mobile app publishers.

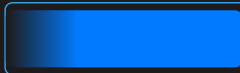


TREND 4

The global shortage of skilled security specialists continues to hamper organizations.



IN 2024



71%

of survey respondents reported a security skills gap within their organization

IN 2026



74%

of developers report that a mobile security skills gap on their team is slowing progress

Some challenges remain largely unchanged over the three-year reporting cycle. Three out of four organizations lack full staff capabilities to effectively manage their mobile app security needs in-house. These findings are consistent with the current general estimate of [4.8 unfilled cybersecurity jobs](#) worldwide. While some financially privileged organizations may be able to address the issue through competitive hiring practices, most mobile app development teams will have to continue managing their security skills shortcomings without assistance from their human resources department.

So, if we can't throw more and/or better security staff at the problem, then we need to unburden the people we already have working within the DevSecOps pipeline. This means purpose-built

(i.e., mobile app specific) security that seamlessly integrates into existing developer workflows without disrupting delivery cycles or user experience; tools that help automate core security tasks (such as continuous code testing); and multiple layers of protection – including code hardening (i.e., different forms of obfuscation), runtime checks, API/ server-side protection, as well as threat monitoring.

TrendCandy's 2026 survey findings overwhelmingly validate this approach to mobile app security:

96%

of teams using multi-layered protection report fewer incidents

Summary

Despite signs of progress, some key challenges persist

While many things are changing for the better in terms of mobile app security awareness and practices, other table stakes for achieving DevSecOps remain a work in progress.

TrendCandy's 2026 survey picked up on a few persistent myths and misperceptions that organizations are clinging to:

- 50% believe iOS is inherently more secure than Android
- 28% believe mobile app tampering is rare
- 28% believe obfuscation slows performance
- 24% think RASP causes crashes

There also appears to be a cultural divide between developers and security leaders:

72% of security leaders struggle with getting developer buy-in. At the same time, nearly all (96%) 2026 survey respondents agree that shared dashboards improve collaboration across teams.

Aligning priorities and fostering better collaboration between development and security teams requires tools (automated testing and multilayered protections) that seamlessly integrate with existing pipeline practices across the entire SDLC.

The days of compromising security for time to market, application performance, and/or user experience are coming to an end – and all are equally essential to a mobile application publisher's ultimate success.

Learn more at guardsquare.com



About Guardsquare

Guardsquare offers the most complete approach to mobile application security on the market, delivering the highest level of protection, with ease. Guardsquare integrates seamlessly across the full development cycle, from mobile app security testing and code hardening to real-time threat detection and API security. Guardsquare provides enhanced mobile application security across the entire development process.

More than 975 customers worldwide across all major industries rely on Guardsquare to help them identify security risks and protect their mobile applications and SDKs against reverse engineering and tampering in the ever-evolving threat landscape.

Research cited

Enterprise Strategy Group, ["Mobile Application Security Can't be an Afterthought"](#)

TrendCandy, ["The Rise of Client-side Risk and the Trust Gap"](#)

Vanson Bourne, ["Assessing Mobile Application Security"](#)

Verizon, ["Mobile Security Index 2025"](#)