Enterprise Strategy Group™

Mobile Application Security Can't Be an Afterthought

Tyler Shields | Principal Analyst
Melinda Marks | Practice Director

ENTERPRISE STRATEGY GROUP

JULY 2025

This Enterprise Strategy Group eBook was commissioned by Guardsquare and is distributed under license from TechTarget, Inc.

Research Objectives

As mobile application usage continues to surge, so, too, does the frequency and sophistication of cyberthreats targeting these platforms. With the number of mobile application security incidents increasing, the associated risks to the businesses that publish the apps are also rising. Building a secure mobile application requires a multilayered approach to mobile app security that is properly integrated across the software development lifecycle (SDLC). While exploring the specific risk exposures and the evolving threat landscape, this research analyzes the demands on mobile application developers as they are under pressure to ship their mobile applications quickly without sacrificing security. Understanding how the market views mobile app threats and vulnerabilities, as well as the balance between user experience, time to market, and protection, enables organizations to design and implement stronger, more effective mobile application security strategies.

To gain further insight into these trends, Guardsquare commissioned Enterprise Strategy Group to execute a survey of 315 application development, cybersecurity, and IT decision-makers at organizations in the United States, the United Kingdom, Brazil, and Singapore involved with or responsible for purchasing technologies aimed at securing their mobile applications.

This study sought to:

- **Examine** how mobile security priorities are evolving in response to emerging threats, new technologies, and regulatory changes.
- **Evaluate** key security concerns and their effect on business operations, compliance, and customer trust.
- **Review** challenges organizations face, including development speed tradeoffs, skills shortages, budget constraints, and difficulties in integrating security into DevOps workflows.
- **Explore** the impacts of automation and AI-based development tools, as well as the overall effectiveness of current mobile app security strategies in place.

Key Findings

A Misalignment Exists Between the Perception and Reality of Mobile Application Security Risk

PAGE 4

Current Mobile Application Defenses Are Insufficient in Isolation

PAGE 11

Organizations Struggle to Embrace Mobile App Security Without Sacrificing Development Speed

PAGE 15

Making Day-to-day Development Processes Easier Also Improves the Effectiveness of Mobile App Security

PAGE 19

Multilayered Mobile Application Security Provides Preventative Defense in Depth

PAGE 23

A Misalignment Exists Between the Perception and Reality of Mobile Application Security Risk

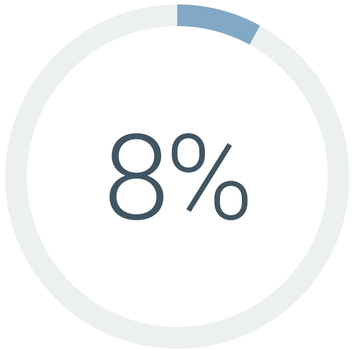
On average, organizations release

13 unique mobile applications per year.

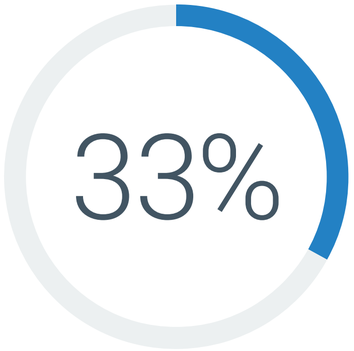
More Mobile Applications Means More Opportunities for Security Threats

On average, organizations release 13 unique mobile applications per year. Due to the significant number of application releases and updates, the volume of threats targeting mobile applications has risen. Additionally, as the number of applications released per year climbs, the amount of mobile application code that is written increases as well. More code creation increases new opportunities for coding errors and software vulnerabilities while expanding the attractive attack surface for threat actors to potentially exploit.

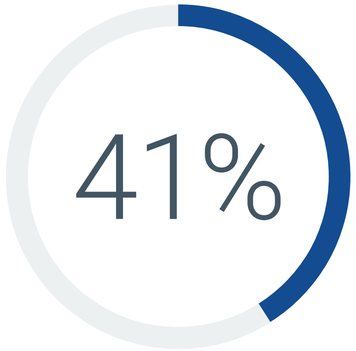
Average Number of Unique Mobile Applications Released per Year (Android and iOS Version Counted as Separate Apps)



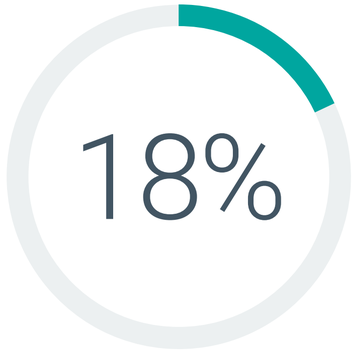
1 to 5 apps



6 to 10 apps



11 to 20 apps



More than 20 apps

BACK TO CONTENTS

The Threat Landscape: Organizations Suffer from Cybersecurity Incidents

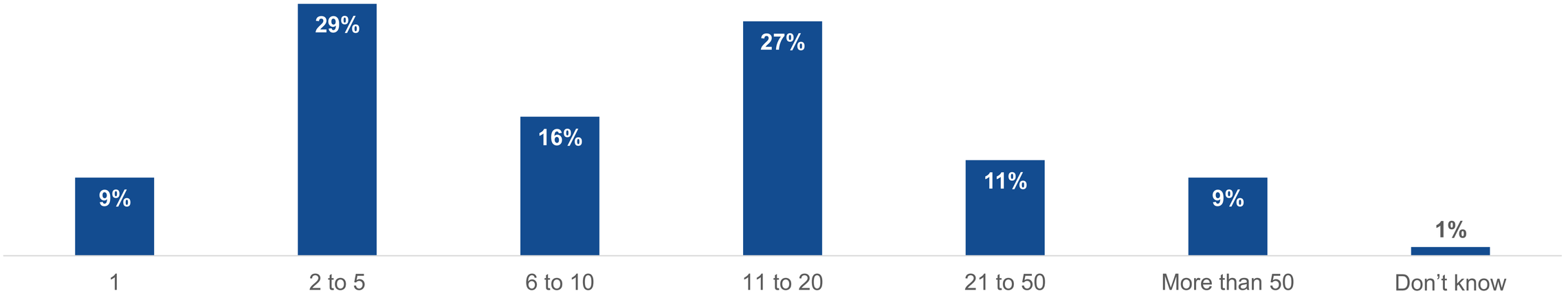
The study showed that 62% of organizations have faced at least one mobile application security incident over the last 12 months. Of those facing incidents, the vast majority (92%) faced multiple incidents. Security team members reported experiencing a significantly higher percentage of mobile application security incidents than developers over the last twelve months. This discrepancy is likely due to a lack of developer awareness of mobile app security issues, as they often do not have full visibility into vulnerability analysis, attack telemetry, and/or security reporting for the code that they write throughout its lifecycle. Often, developers are only informed of issues that exist in their specific code sections and not every mobile application built by the organization. This results in a risk perception mismatch between mobile app developers and the security team around the actual number of issues and incidents that have occurred.

On average, organizations have experienced

9.1 mobile application security incidents

over the last 12 months.

The Number of Mobile Incidents for Those Who Faced Mobile Cybersecurity Incidents



BACK TO CONTENTS

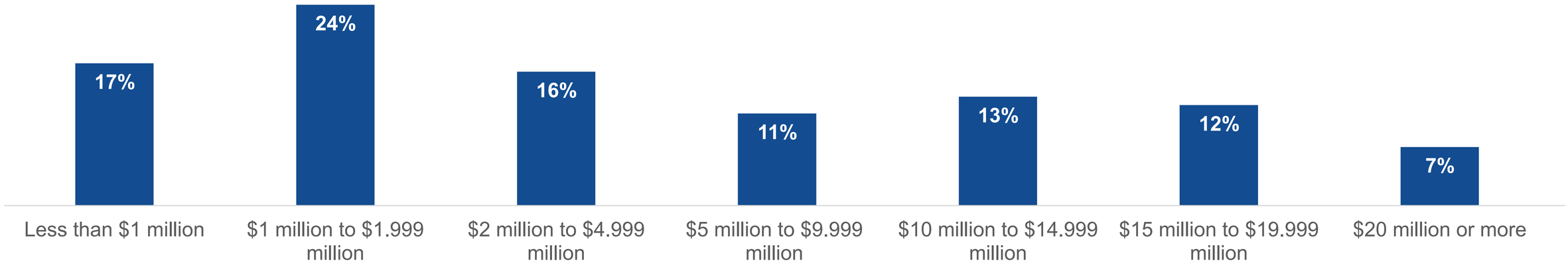
The cost of a mobile application security incident ranges from less than

$1 million to more than $20 million.

Average Cost of a Mobile Application Security Incident: $6,997,435

The cost of a mobile application security incident ranges from less than $1 million to more than $20 million. Taking the weighted average of the responses, a typical mobile app security incident will cost an organization about $7 million. This surveyed cost of a mobile app security incident demonstrates that there is significant business risk in releasing unprotected mobile applications. From concrete discovery and remediation costs, to regulatory fines, to more abstract losses like reputational damage to the business, a single mobile app security incident can have a substantial financial impact.

Cost of a Mobile Application Security Incident



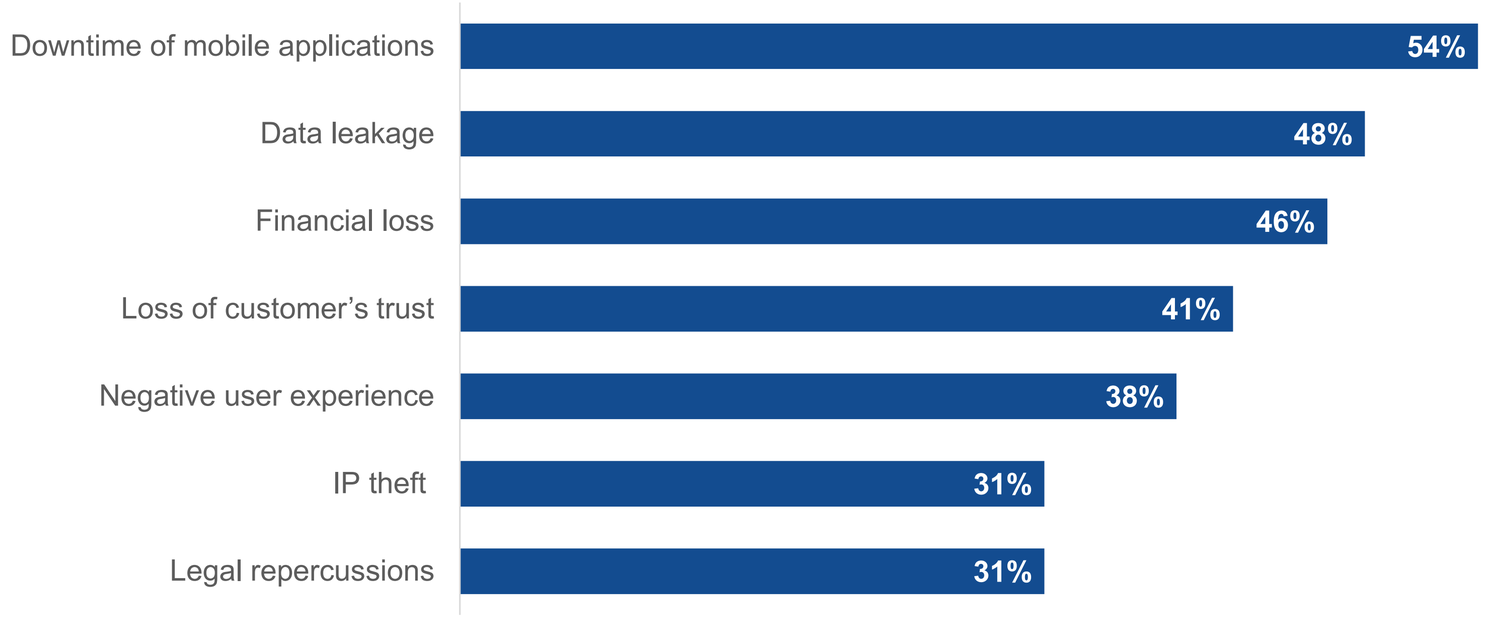
BACK TO CONTENTS

"With business-critical mobile apps, downtime can carry **significant financial losses** if users are unable to safely use or access services."

Business Impacts From Cybersecurity Incidents on Mobile Applications

The ripple effects of a mobile app security incident can be felt far and wide. The challenges go well beyond developer time and effort to repair a vulnerability or remediate an attack. With business-critical mobile apps, downtime can carry significant financial losses if users are unable to safely use or access services. Data leakage can expose private customer information or user credentials, while exposing development organizations to regulatory compliance consequences, litigation, and a loss of customer trust. In addition to any direct business impacts, the recovery process from some types of incidents can be extremely costly and time-consuming before normal operations may resume.

Impact of Mobile Application Security Incidents

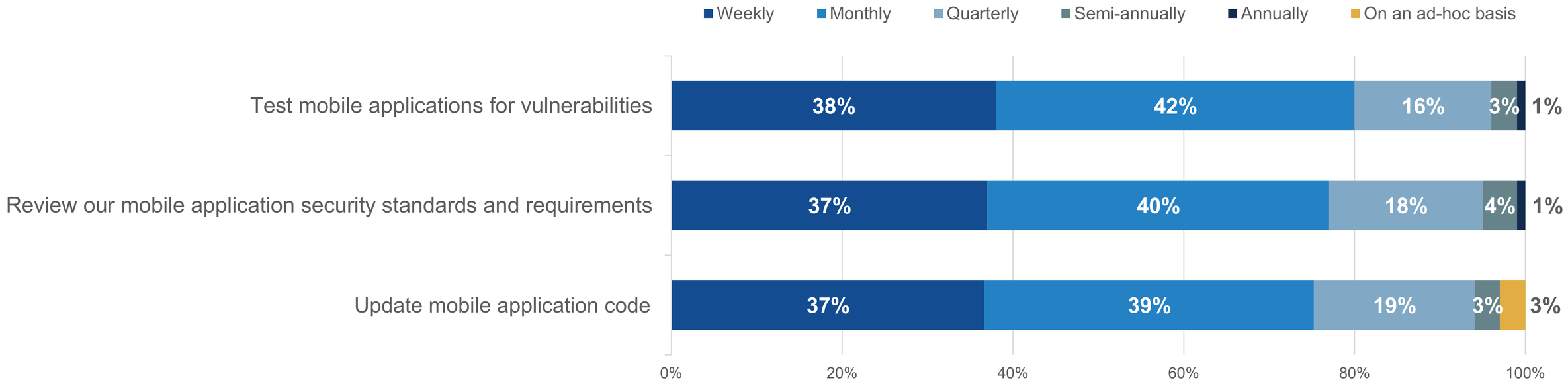


BACK TO CONTENTS

Frequent Mobile Code Security Assessments Are Critical for Managing Risk in the Evolving Mobile Threat Landscape

Along with the increasing number of mobile application releases each year, updates to the mobile application code base are increasing in frequency as well. Only 38% percent of those surveyed are analyzing their mobile apps for vulnerabilities on a weekly basis, while nearly 20% have a gap of a quarter or more between vulnerability tests. Assessment of mobile application code for security issues should be completed as frequently as possible, ideally aligned with developer workflows, such as code commits and application rebuilds, rather than on arbitrary time-based schedules. Mobile app code security assessments are critical to drive efficient remediation of security issues and decrease the risk of vulnerabilities remaining in published applications.

Frequency of Mobile Application Assessments and Updates



BACK TO CONTENTS

The Evolving Threat Landscape Requires a Proactive Security Mindset

Mobile application developers and security teams continue to be siloed. Limited data sharing around mobile app risks from security to developers leads to overconfidence in the level of protection built into the mobile application development process. This overconfidence results in a decreased level of vigilance from developers, thus increasing risk. Security teams must focus on breaking down the barriers that exist between the two departments as well as communicating security risk data and concepts earlier so that all team members have similar risk knowledge. The earlier this communication occurs, the more that developers and security teams can collaborate on education, proactive protection, code improvement, and, ultimately, risk reduction.

Perception of Mobile Application Security

While there is a strong awareness of risk, silos between teams can lead to ineffective security implementation.

My organization is aware of the risks associated with unprotected mobile applications

94% Agree

Collaboration between cybersecurity and mobile development teams could improve mobile application security

93% Agree

Overconfidence in their abilities is indicative of a potential gap in perception vs. actual preparedness.

Our current application security approach includes tools and processes to address mobile application security

97% Agree

Our development teams have enough knowledge to handle mobile application security

94% Agree

Our current mobile application security protections are sufficient to prevent cybersecurity threats

93% Agree

Purchasing security tools after a security incident is indicative of a more reactive, rather than proactive, approach.

A security incident is often the catalyst for a security purchase

85% Agree

BACK TO CONTENTS

Current Mobile Application Defenses Are Insufficient in Isolation

Security Incidents Highlight a Gap Between Policy and Execution

Although an overwhelming majority of organizations—97%—report keeping up-to-date policies for mobile application security requirements, 62% of those surveyed have experienced one or more mobile application security incidents in the past 12 months. While policies appear to be widely implemented, the effectiveness of the policies is limited, as evidenced by the number of security incidents that occur. When policy and practice are not supportive of one another, business risk is elevated.

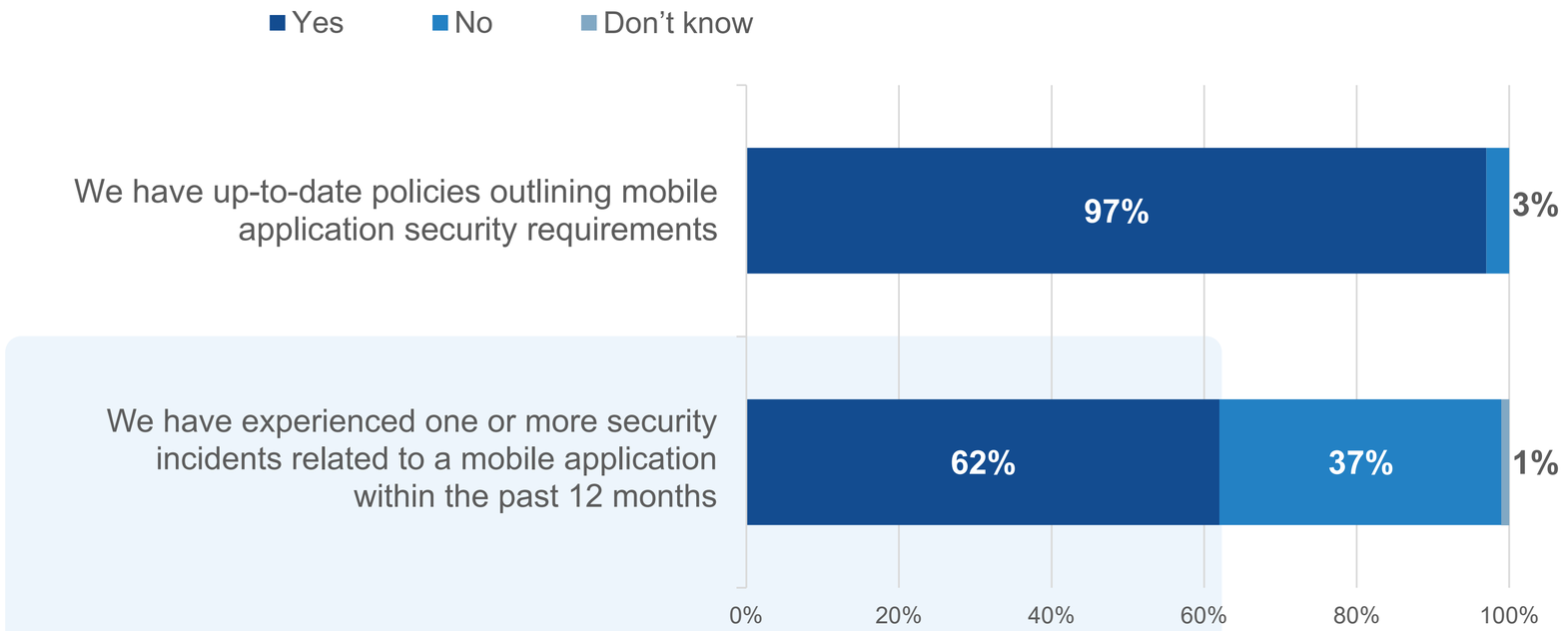
Security respondents

71%

App dev/software engineers

54%

Mobile Application Security Incidents and Policy Implementation



Security respondents are

1.3x more likely

to indicate they have experienced a security incident related to a mobile application over the last 12 months than developers.

BACK TO CONTENTS

The Need for Comprehensive Security That Doesn't Impede Productivity

Security teams today give priority to data protection, privacy, threat monitoring and detection, and security automation. However, successful mobile application security cannot come at the cost of successful adoption or usage of the application. Cost, performance, and user experience must be important considerations in the security equation and not ignored at the demand of security controls.

Mobile app security teams should look for ways to improve (or at least maintain) the user experience while implementing protections and controls. An emphasis on brand reputation, compliance, and intellectual property protection indicates mobile app security must be a business-critical priority rather than a technical consideration, and security teams can align and support development to reach common goals.

Areas Prioritized for Mobile Application Security

Organizations must balance security with cost, performance, and usability. With growing regulatory requirements (e.g., GDPR), it is also more important than ever for organizations to protect their sensitive data.

Security strategies must align with business and regulatory needs for protecting IP, data, and customer PII.

BACK TO CONTENTS

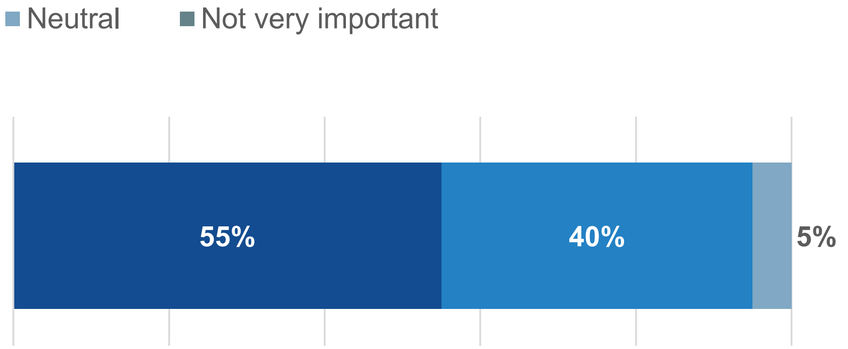
Organizations Seek Robust Security That Is Easy to Deploy

Mobile application security must be comprehensive and easy to deploy and maintain while supporting in-depth security capabilities. The ability to embed security directly into the mobile app code drastically increases protection, while a deployment model for those same robust security controls must be easy to use and support rapid implementation. Developers and security teams need strong security that's easy to use or they will move away from the approach.

High Priority for Mobile Application Security

This priority is indicative of the importance of deep code integration for stronger protection.

The ability to embed security directly within the mobile application code, making it harder to bypass or reverse-engineer (95% important)



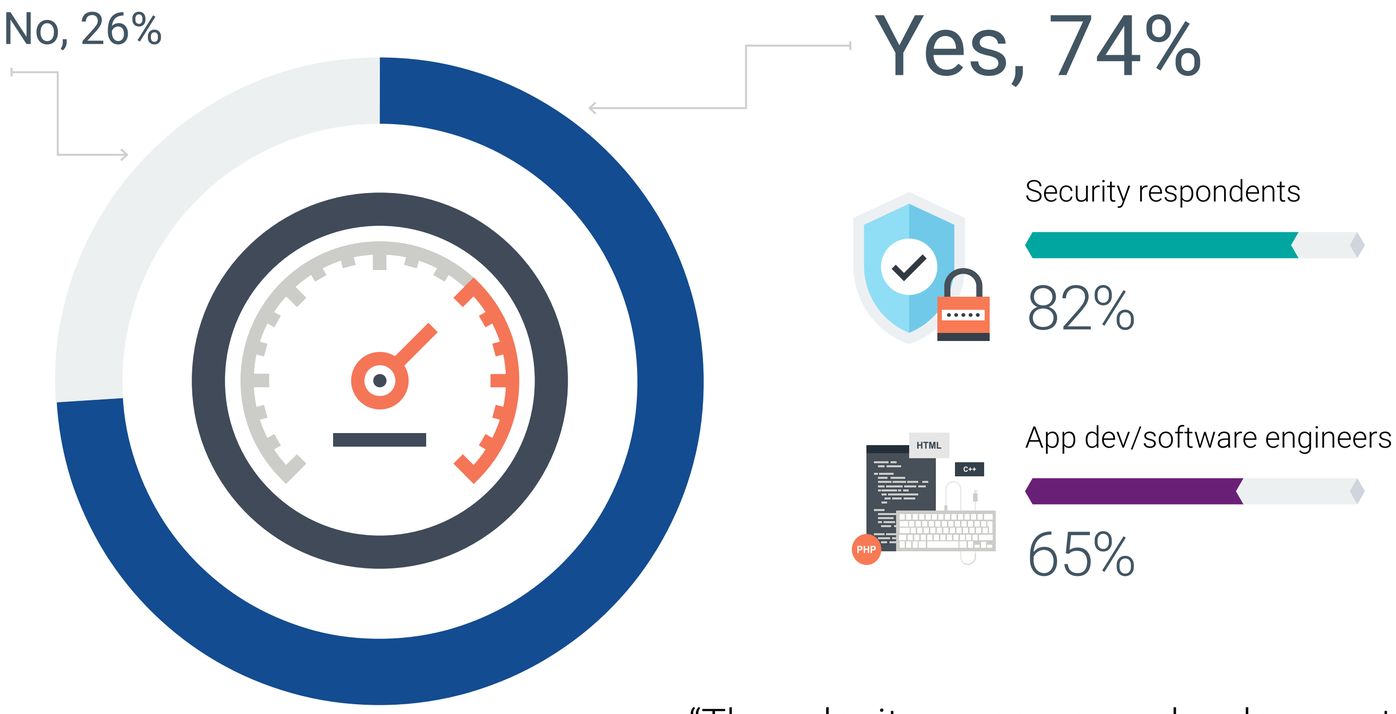
BACK TO CONTENTS

Organizations Struggle to Embrace Mobile App Security Without Sacrificing Development Speed

Development Velocity Pressures on Mobile Application Teams

The business constantly puts pressure on mobile app developers and security teams to release code at an increased pace. When asked whether the development team is under pressure for increased development velocity, 74% of respondents said, "Yes." However, this is perceived most acutely by security teams (82%), as opposed to the developers themselves (65%). Security teams, by their very nature, enable a process that decreases the pace of development to ensure that secure code is created. It's a difficult balance, but one that application security teams have danced for decades. Security teams are increasingly focused on making sure that they can improve development velocity, resulting in this added pressure.

Development Velocity Pressures on Mobile Application Teams



"The velocity pressure on development teams **is perceived most acutely by security teams,** as opposed to developers themselves."

BACK TO CONTENTS

Developer Velocity Decreases With Security Focus

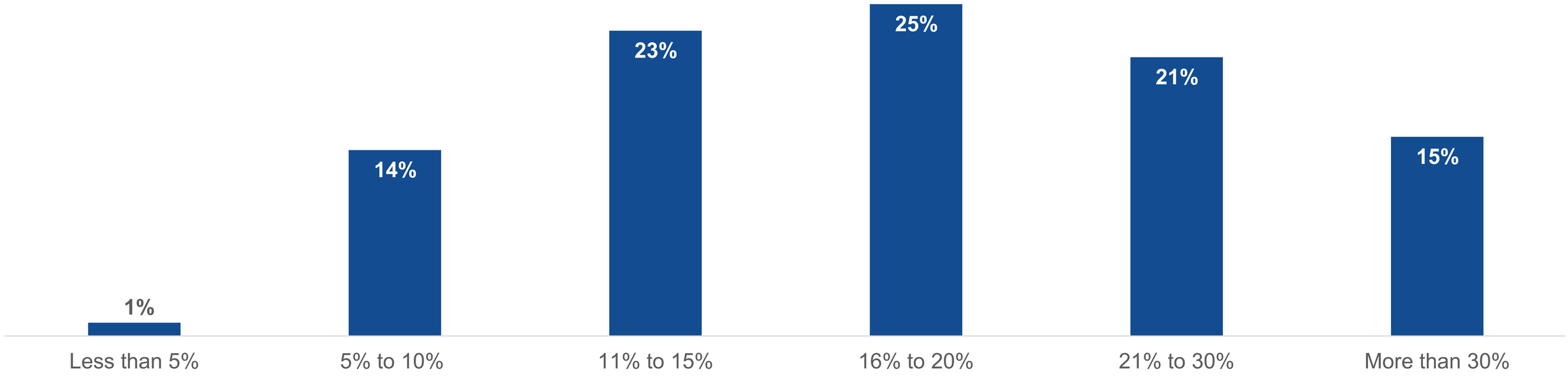
Developers are spending nearly a fifth (18.8%, on average) of their time on mobile application security-related tasks. That results in a nearly 20% tax to the cost of human resources developing mobile apps. In a development organization of meaningful size, that tax adds up to a significant cost to the business. Security teams must look for ways to decrease the impact on developers whenever possible and specifically focus on increasing the bottom line of the business.

Developers are spending

nearly a fifth

of their time on mobile application security-related tasks.

Time Developers Spend on Mobile Application Security-related Tasks

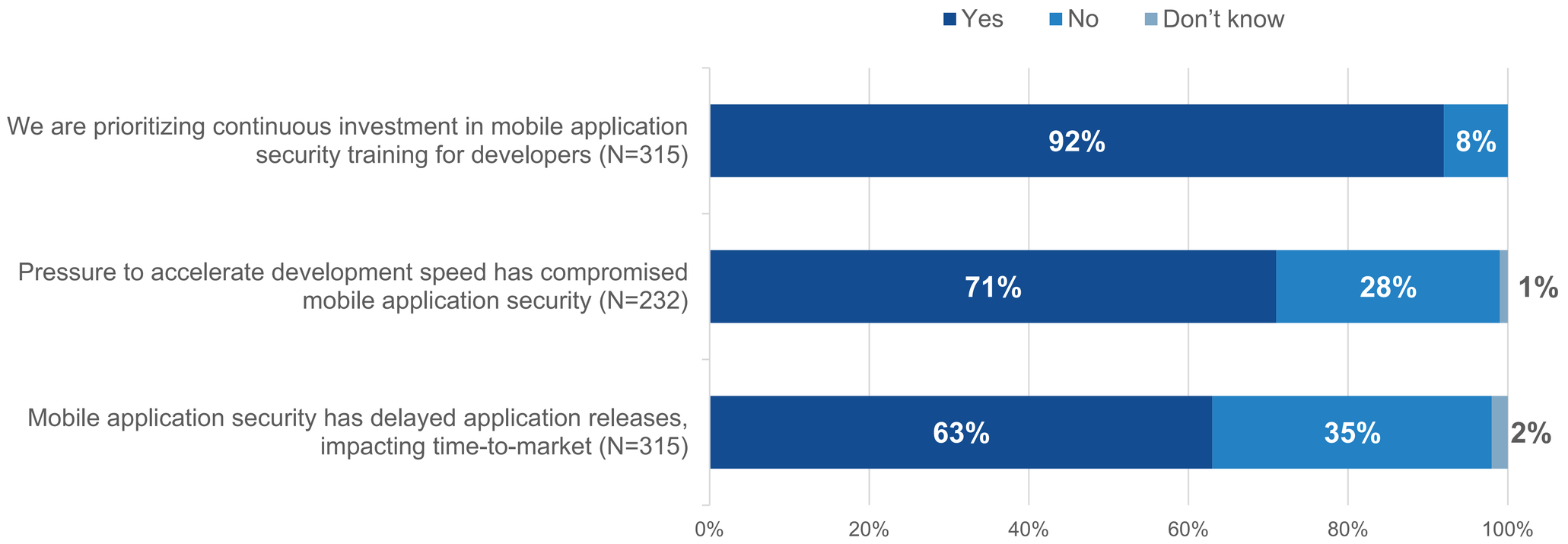


BACK TO CONTENTS

Organizations Need Help Striking the Right Balance Between Development and Security

By striking the right balance between development velocity and comprehensive security, organizations can optimize for the creation of secure mobile application code at the fastest possible pace. Building in security processes starting as early in the development process as possible to help developers protect their mobile applications is an effective way to balance the scales. Implementing mobile app security technologies that focus on the balance between developer ease of use and comprehensive, multilayered protection will also go a long way to optimize efficiency across teams. Using upgraded processes and technologies breaks the security bottleneck that can hinder secure development.

Statements Applicable to the Application Development Process and Teams



BACK TO CONTENTS

Making Day-to-day Development Processes Easier Also Improves the Effectiveness of Mobile App Security

Strengthening DevSecOps Practices

Organizations struggle across three main areas as they work to secure their mobile applications.

First, they face challenges balancing performance and compliance against security. Traditional mobile app security offerings have had to compromise performance and compliance features in favor of security controls; however, modern technologies are growing past this blockade by offering high performance and feature-rich security offerings.

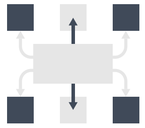
Organizations are also looking for ways to balance security with the pressure to deliver mobile application features as quickly as possible. Security processes need to be well incorporated into developer workflows so that their pace of development is not hindered.

Finally, organizations struggle with resource and budget constraints. Mobile application security technologies should be deployed in such a manner that they decrease the quantity of human resources and the budget required to create secure mobile applications over time. Realistically, security teams shouldn't have to compromise and neither should developers.

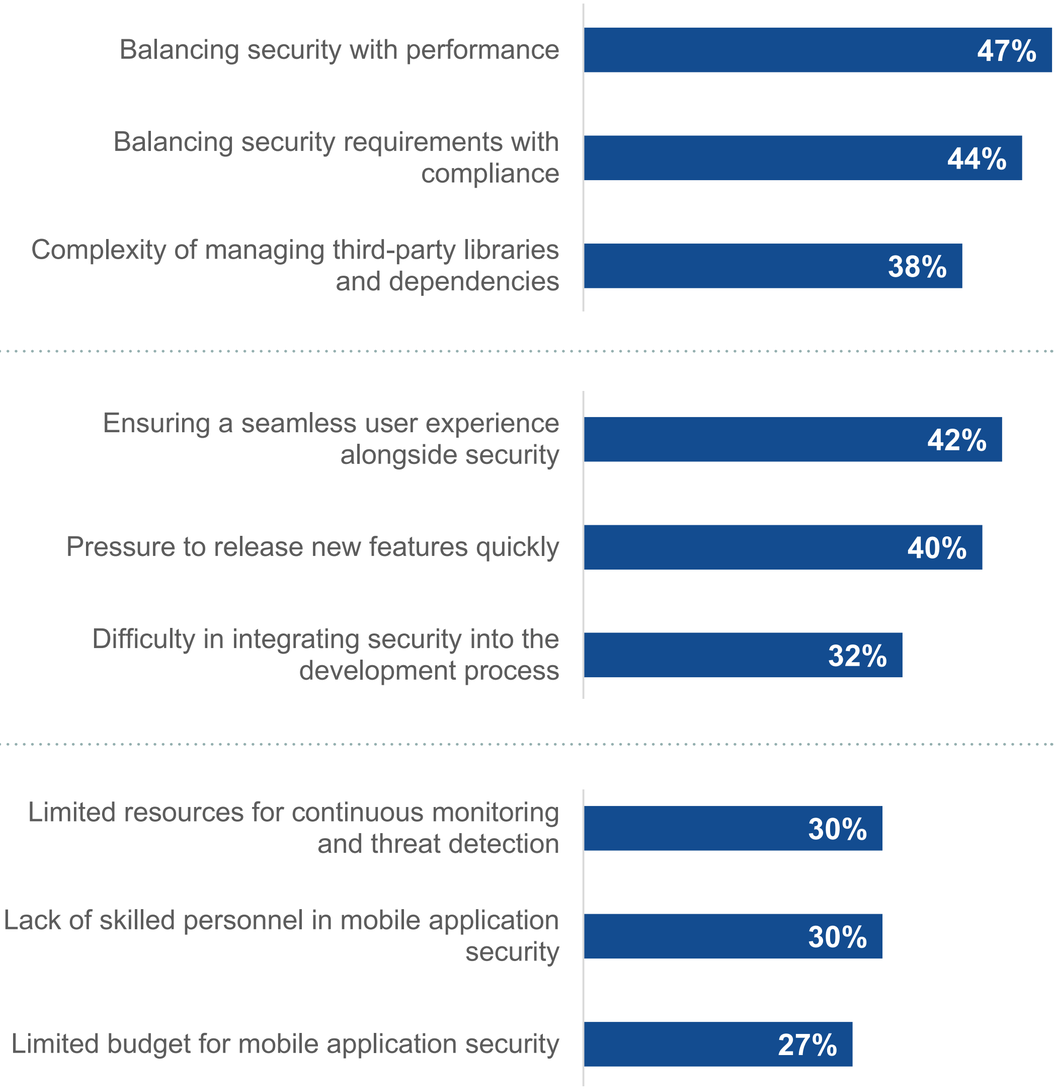
Challenges Experienced in Securing Mobile Applications

Need to ensure security and compliance do not slow things down

Need to support rapid secure development



Need to optimize resource use

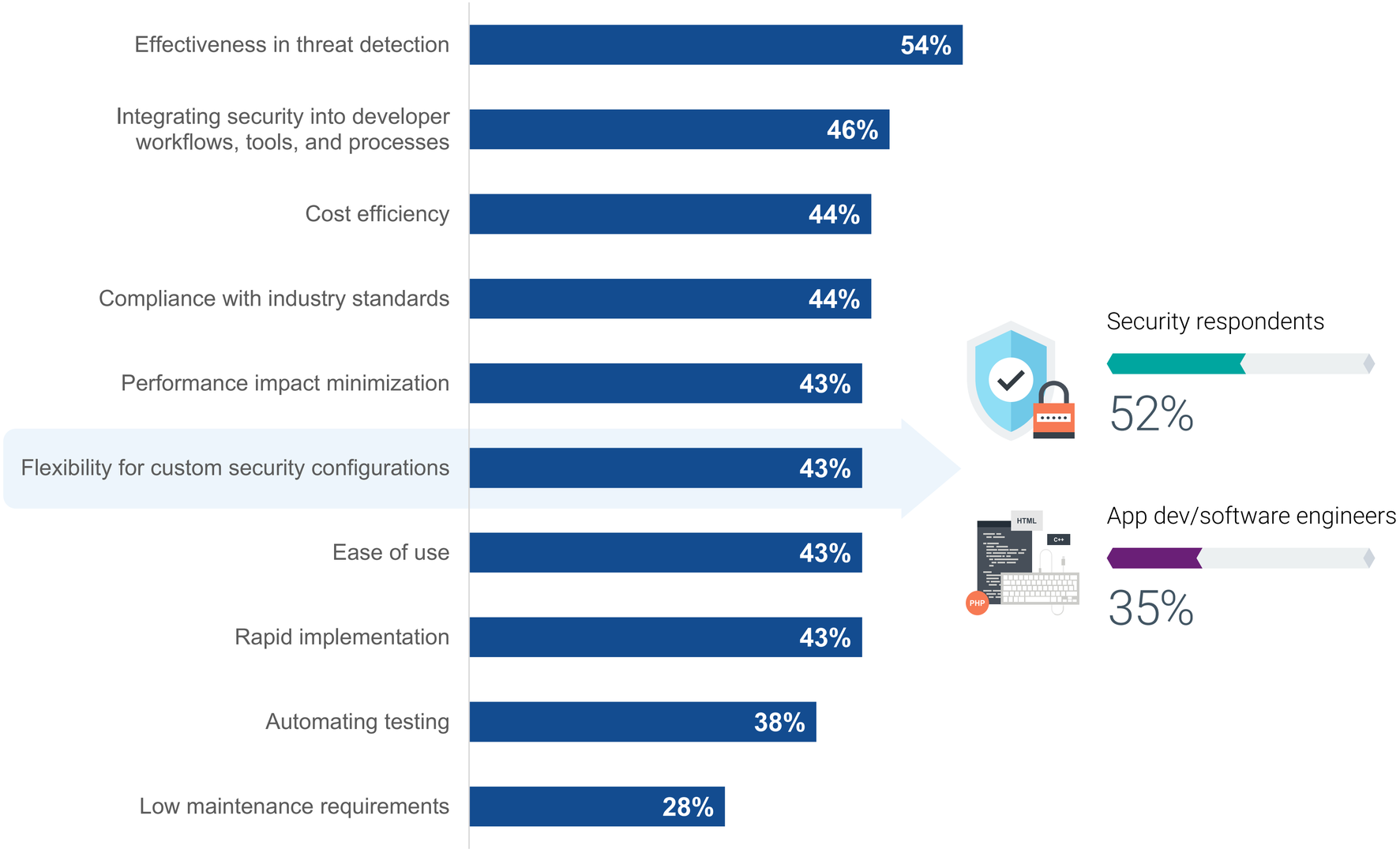


BACK TO CONTENTS

Development Team Security Priorities

The priorities for mobile app development teams are focused on a balance between security, compliance, and developer velocity, as is expected, based on the challenges organizations are facing around mobile application security. While many of the priorities were close between security and app development respondents, security teams have one extra demand that isn't as relevant to developers. The security team needs flexibility for custom security configurations to achieve both security and developer efficiency goals. This means that security teams are not looking for a singular security model to be deployed but instead to have the flexibility in the specific controls they put in place to make sure they help the business with performance and user experience as much as possible.

Top Priorities for Development Teams Regarding Mobile Application Security

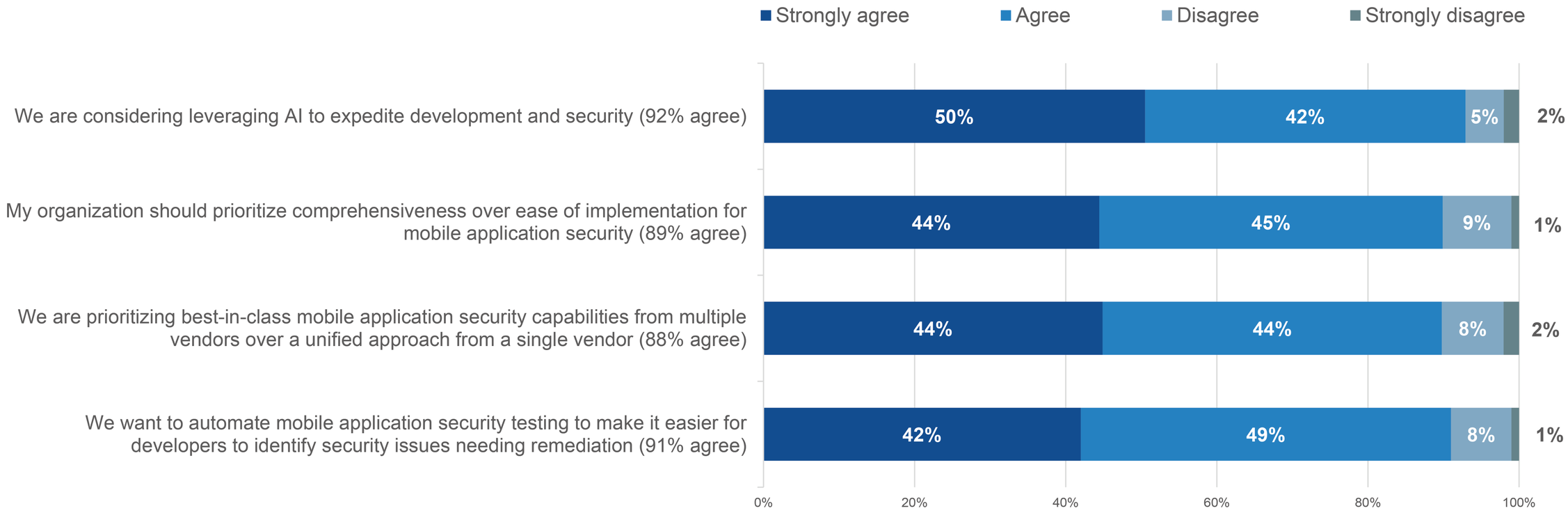


BACK TO CONTENTS

Organizations Are Prioritizing Efficiency, Automation, and Best-in-class Security Solutions

Organizations are looking for security tools to support rapid development, growth, and scale so they don't have to sacrifice security as they increase productivity. With effective security in place, they can better support AI tools and enable efficient secure development.

The Need for Security Tools Supporting Rapid Development



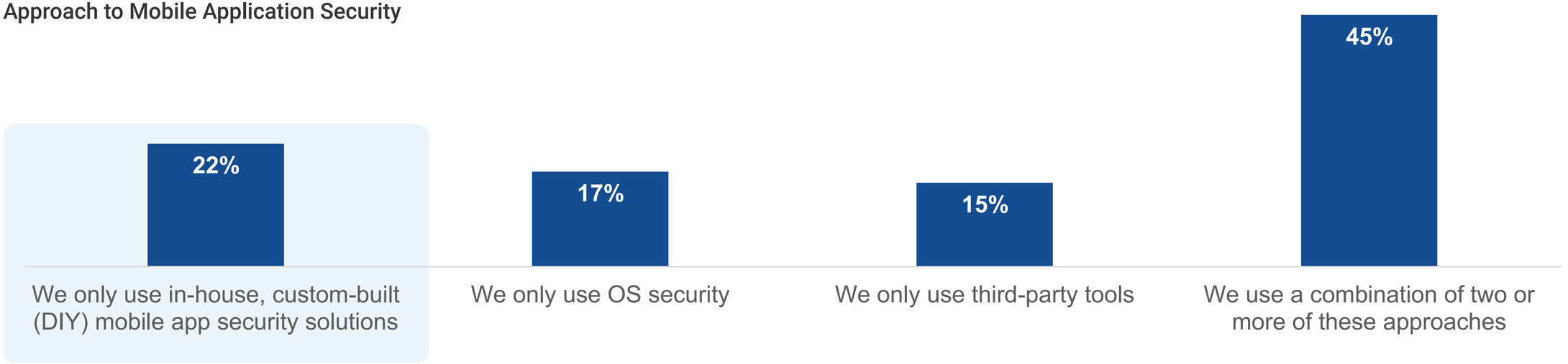
BACK TO CONTENTS

Multilayered Mobile Application Security Provides Preventative Defense in Depth

Security Teams Lean Toward Custom Solutions, While Most Organizations Favor a Blended Security Approach

A combination of multiple security approaches provides a defense-in-depth model for the security of mobile applications. 45% of organizations use a combination of in-house, OS, and third-party security tools for their mobile applications. Security teams are 1.9x more likely to use in-house, custom-built mobile app security solutions than development teams. This is likely because security is looking to find the most effective security controls possible, while developers are more focused on what's going to enable them to create code faster. In an ideal world, technologies would solve for both problems, and both parties would align to achieve their goals.

General Approach to Mobile Application Security



Security teams are

1.9x more likely

to use in-house, custom-built mobile app security solutions than development teams.

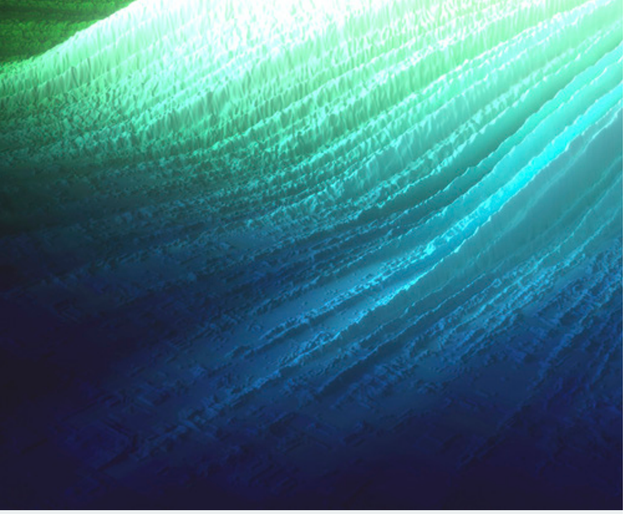
Security respondents

29%

App dev/software engineers

15%

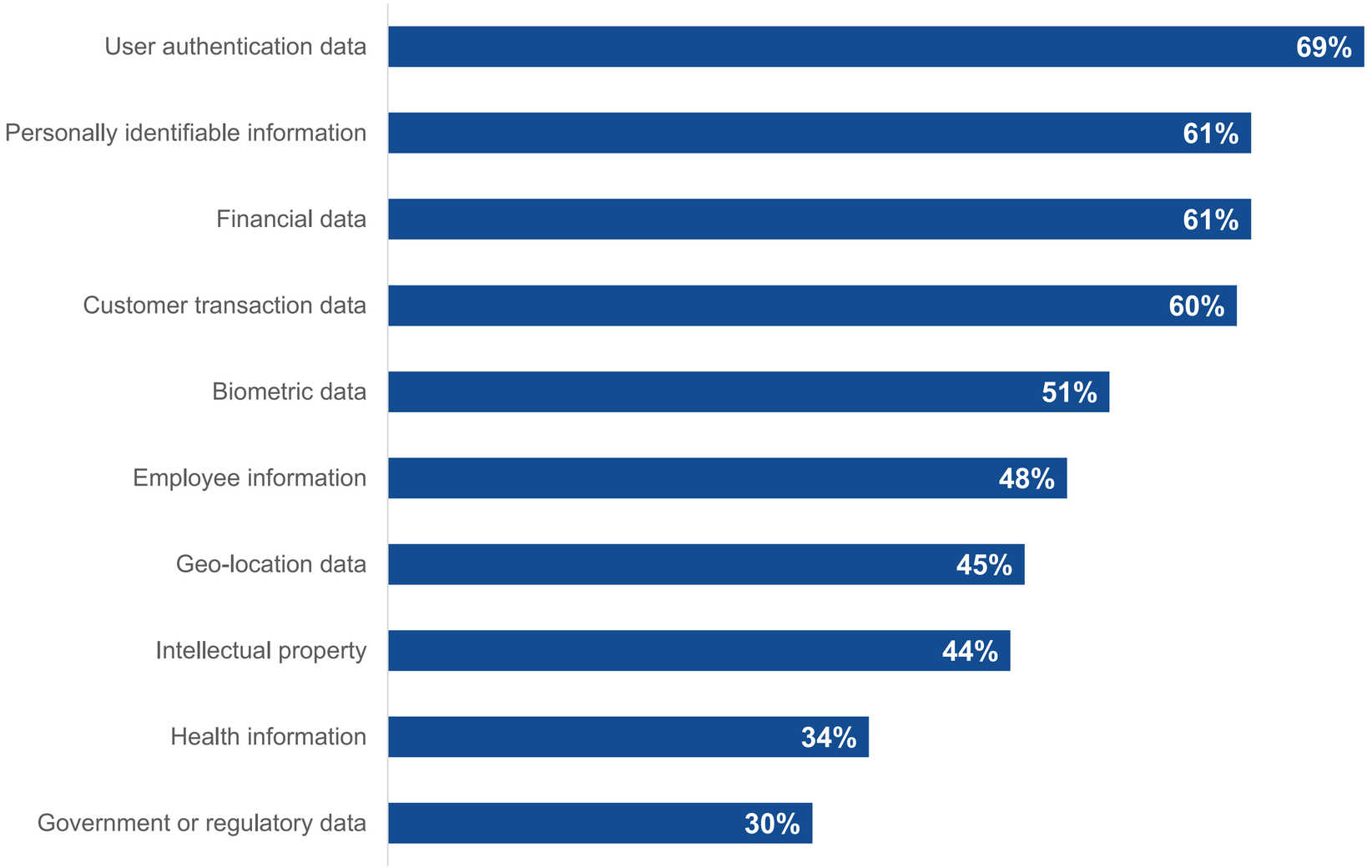
BACK TO CONTENTS



Mobile Apps Need Multiple Layers of Protection to Handle Sensitive Data

Mobile applications operate on and store significant amounts of sensitive data. From direct user data to metadata such as PII, biometrics, and geolocation data, mobile applications require a breadth of protections to ensure that all data classes are properly secured.

Different Types of Sensitive Data Handled by Mobile Applications

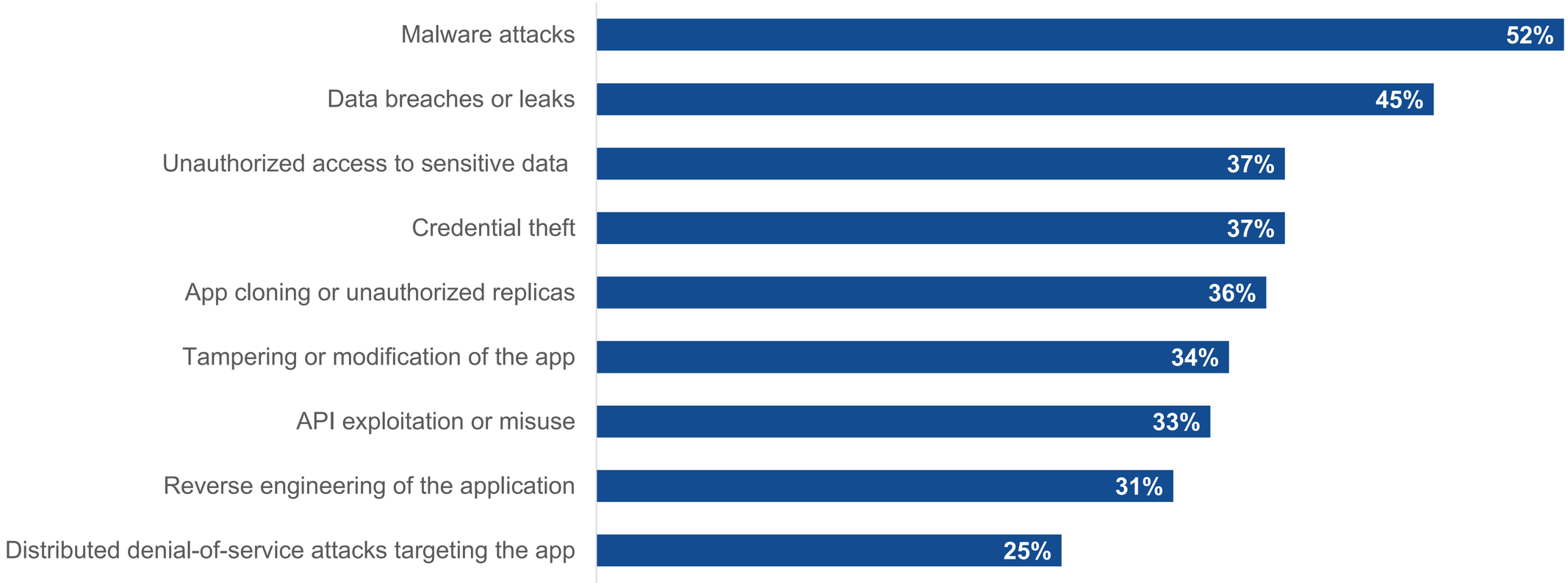


BACK TO CONTENTS

Malware Attacks, Data Leaks, and Unauthorized Access Are the Most Cited Security Incidents

"The high frequency of malware, data leaks, and unauthorized access means there is a need **for real-time threat detection and monitoring for mobile applications**."

Types of Mobile Application Security Incidents Experienced Over the Last 12 Months



BACK TO CONTENTS

Proactive Risk Awareness Is Driving Mobile Application Security Adoption

When looking at factors triggering the need for mobile application security, organizations are increasingly taking a proactive approach driven by both internal sources (risk assessments, emerging threats, and vulnerabilities) and external pressures (security incidents).

Emerging threats and vulnerabilities (58%) and past security incidents (58%) were nearly as common, highlighting that reactive measures are still a significant driver.

Mobile app security is no longer just a checkbox for compliance—it's being prioritized across the board due to growing internal scrutiny, evolving threat landscapes, and rising stakeholder expectations.

Factors That Triggered the Need for Mobile Application Security

BACK TO CONTENTS

Key Takeaways

As organizations increasingly deploy mobile applications, these applications can be an attractive target if not secured properly. The research showed that most organizations have faced multiple cybersecurity incidents over the past year with serious impacts, including application downtime, data loss, financial loss, and loss of IP.

> "Embracing trusted and proven third-party technology can augment security talent shortages and help development teams release robust mobile app protections, **without compromising development, speed, app performance, user experience, or compliance**."

Although organizations want to take measures to secure their applications, it can be difficult to incorporate security without slowing development down. To keep up with the pace and sophistication of threats, organizations need security technologies that fit within developers' existing workflows. Embracing trusted and proven third-party technology can augment security talent shortages and help development teams release robust mobile app protections, without compromising development, speed, app performance, user experience, or compliance.

Organizations should look for a comprehensive approach that works throughout the software development lifecycle. The right approach should start at the code level to proactively mitigate risk by catching issues before an application is released and then continue with ongoing mobile app security testing and real-time threat monitoring. By combining these protections with developer training and secure coding best practices, organizations can ensure security even as they increase software development productivity with mobile applications to meet business goals and gain a competitive advantage.

BACK TO CONTENTS

GUARDSQUARE

Mobile application protection

ABOUT

Guardsquare offers the most complete approach to mobile application security on the market, delivering the highest level of protection with ease. Guardsquare's software integrates seamlessly across the development cycle, from app security testing to code hardening to real-time visibility into the threat landscape. Guardsquare products provide enhanced mobile application security from early in the development process through publication.

More than 900 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.

LEARN MORE

RESEARCH METHODOLOGY AND DEMOGRAPHICS

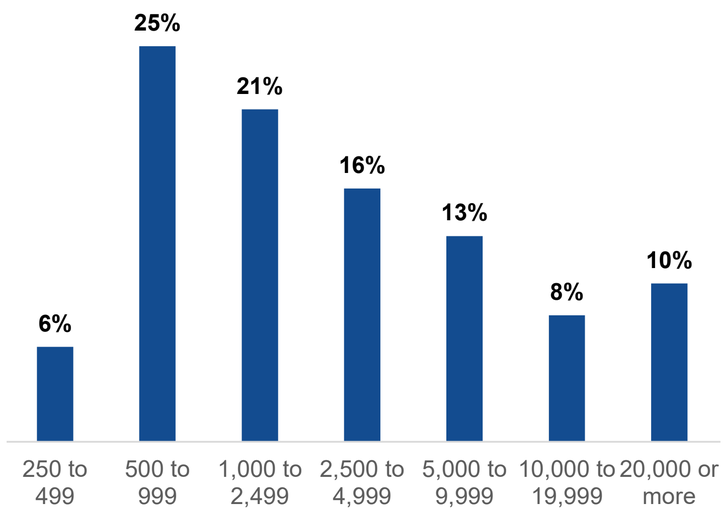
This study—fielded between January 8, 2025 and January 30, 2025—included application development, cybersecurity, and IT decision-makers involved with or responsible for purchasing security technologies aimed at protecting the mobile applications at their organization.

Respondents in the study came from organizations across industries designated as midmarket (250-999 employees, 31%) and enterprise (1,000+ employees, 69%). These organizations were based in the United States, the United Kingdom, Brazil, and Singapore.

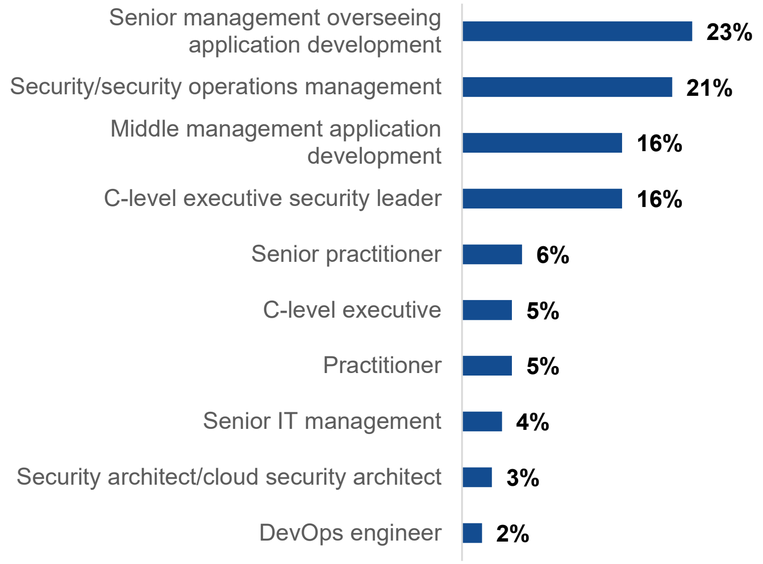
After applying data quality control best practices and screening the remaining completed responses (on several criteria) for data integrity, a final sample of 315 respondents remained. All respondents were provided an incentive to complete the survey in the form of cash awards and/or cash equivalents. The survey confidence level is 95% with a margin of error of + or - 6 percentage points.

Note: Totals in figures and tables throughout this report may not add up to 100% due to rounding.

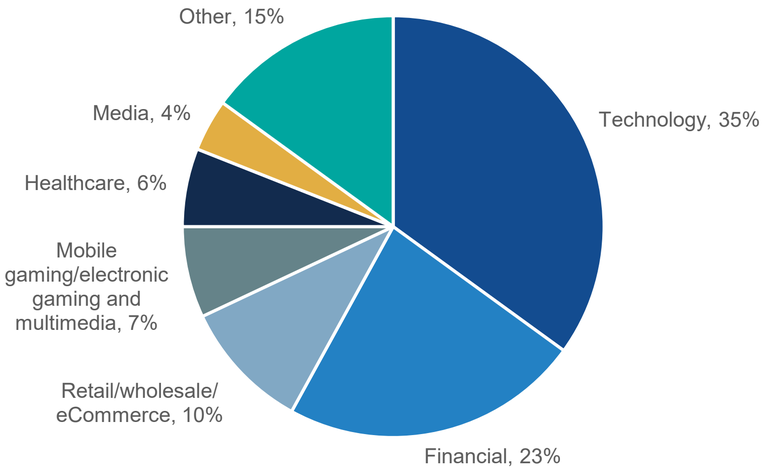
Respondents by Number of Employees



Respondents by Job Title



Respondents by Industry



BACK TO CONTENTS

Enterprise Strategy Group, now part of Omdia, provides focused and actionable market intelligence, demand-side research, analyst advisory services, GTM strategy guidance, solution validations, and custom content supporting enterprise technology buying and selling.