

2025 State of Application Security

62% Ship Insecure Code —
False Positives, Fatigue, and
the Case for Expert Support

Survey Findings from
IT and Security Leaders
Across North America



CYPRESS
DATA DEFENSE

Executive Summary

Application security has become a strategic priority for modern organizations, not just a technical responsibility. It is foundational for business, key to innovation, crucial to getting products to market quickly and securely. It continues to be one of the weakest links for bad actors to exploit for ransomware, IP Theft, and other malicious goals while average cost of a breach in the United States has ballooned to \$9.48 million.¹

New research from TechStudio and Cypress Data Defense, based on responses from 250 IT and security leaders across North America, reveals a mounting crisis in application security.² As release cycles accelerate and architectures grow more complex, the pressure on DevSecOps teams is intensifying.

Findings from the *2025 State of Application Security Survey* uncover widespread challenges, from frequent false positives and insecure code releases to understaffed teams and overwhelmed tools. Even as more teams aim to involve security earlier in development, most still wait until the final stages. This leaves critical risks unaddressed until it's often too late. And with AI apps on the rise, open source-generated code and malicious use of AI tools by hackers will make organizations more vulnerable to exploitation. Teams are constrained, struggling with visibility, and worried about fallout from preventable breaches often without the resources to expand headcount or deliver securely at speed. False alerts create a lot of noise and distractions but surprisingly offer opportunity to bolster security.

The stakes are high. 60 percent say security issues are more likely to delay releases than bugs. Nearly 80 percent are worried about job loss after a breach. And 83 percent are open to outsourcing application security to get the help they need.

This report outlines the true state of AppSec and how expert partners like Cypress Data Defense can deliver critical support and close key security gaps.

The stakes are high—60 percent say security issues are more likely to delay releases than bugs. Nearly 80 percent are worried about job loss after a breach. And 83 percent are open to outsourcing application security to get the help they need.

¹Source: IBM 2024 Cost of a Data Breach Report
²Source: 2025 State of Application Security Survey, conducted by TechStudio, an Energize Marketing company, in partnership with Cypress Data Defense.


Contents

Executive Summary	02
Key Findings	04
AppSec Delays Product Velocity	05
OWASP Gaps Leave Teams Exposed	06
Detection Still Takes Too Long	07
Job Security Tied to AppSec Risk	08
AppSec Budgets Don't Match the Risk	09
Perimeter Still Wins Out	11
Security Shortcuts Still Happen	12
Security Left Behind in the SDLC	13
Critical AppSec Work Goes Undone	14
Noise in the System	15
Why Outsourcing AppSec Is on the Rise	16
What's Fueling the Shift to Expert Help	17
What Keeps Teams Up at Night	18
Conclusion	22
Survey Methodology	23
About Cypress Data Defense	24



Key Findings: Gaps, Pressures, and Opportunities in Modern AppSec

This data highlights the scale of challenges facing AppSec teams, from insecure code to team burnout, and where organizations see opportunities for external support.

**62%** of companies admit to shipping insecure code


**False positives** are eroding trust in security tools

**Security is still bolt-on**, not built-in

**Teams crave more time** for high-value AppSec tasks

**83%** of companies are open to AppSec outsourcing

**60%** say security issues are more likely to delay product launches than feature bugs

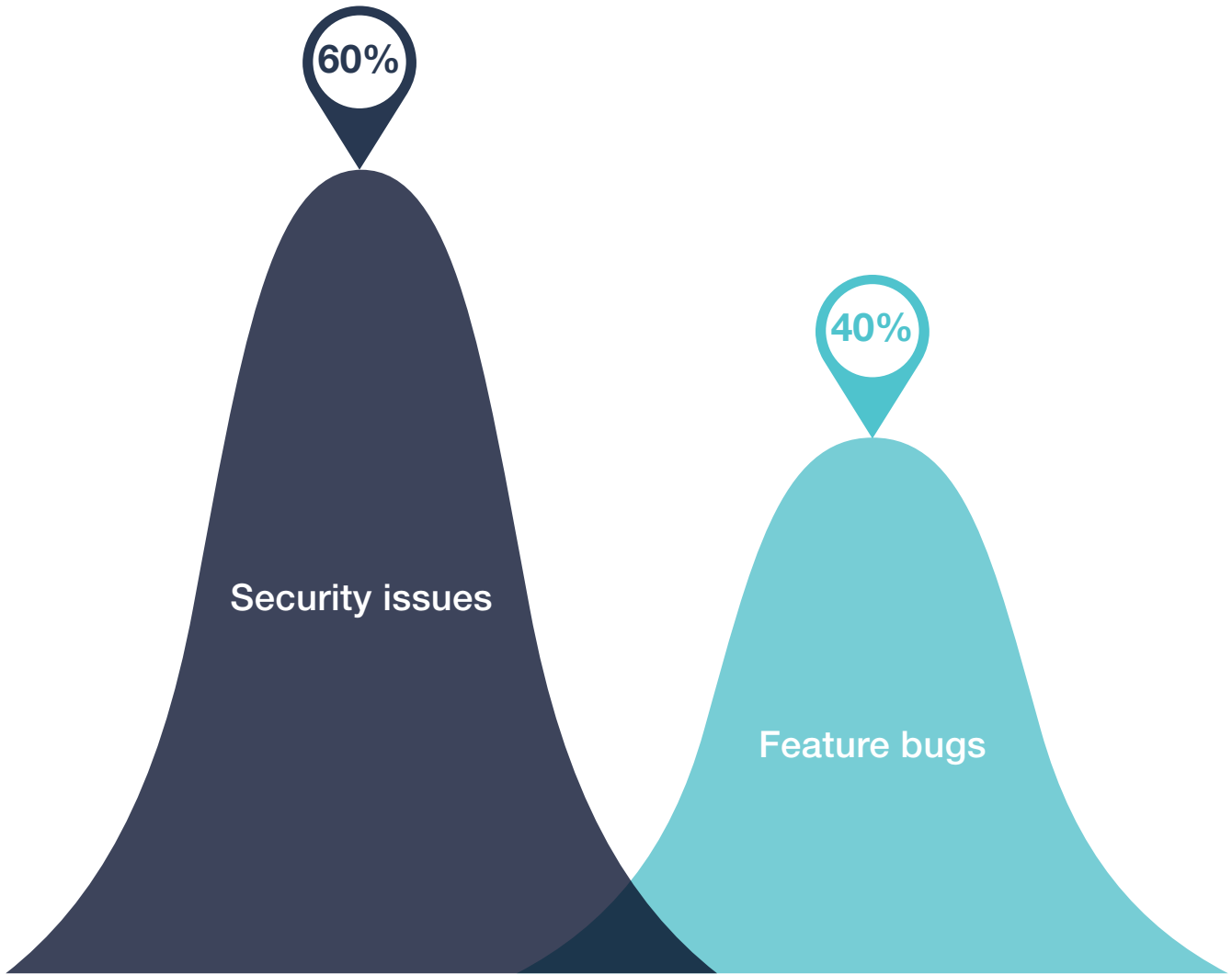
**Nearly 80%** of respondents are worried about job loss due to an AppSec incident

AppSec Delays Product Velocity

Anyone who doubts the critical role that application security now plays in bringing products to market should consider this: security issues are more likely to delay launches than feature bugs. In fact, 60% of respondents cited security as the top cause of delay, reinforcing the need to involve AppSec earlier and more consistently across the SDLC.

Delays often stem from late-stage discovery of vulnerabilities during static or dynamic scans, which require rework and retesting. Embedding security at the design and coding phases, through practices like secure code reviews, threat modeling, and integrated scanning, can reduce bottlenecks and improve release velocity. If in-house security efforts are impeding delivery, as this data suggests, organizations may need to augment capacity with external AppSec expertise.

What's more likely to delay your next product launch—security issues or feature bugs?



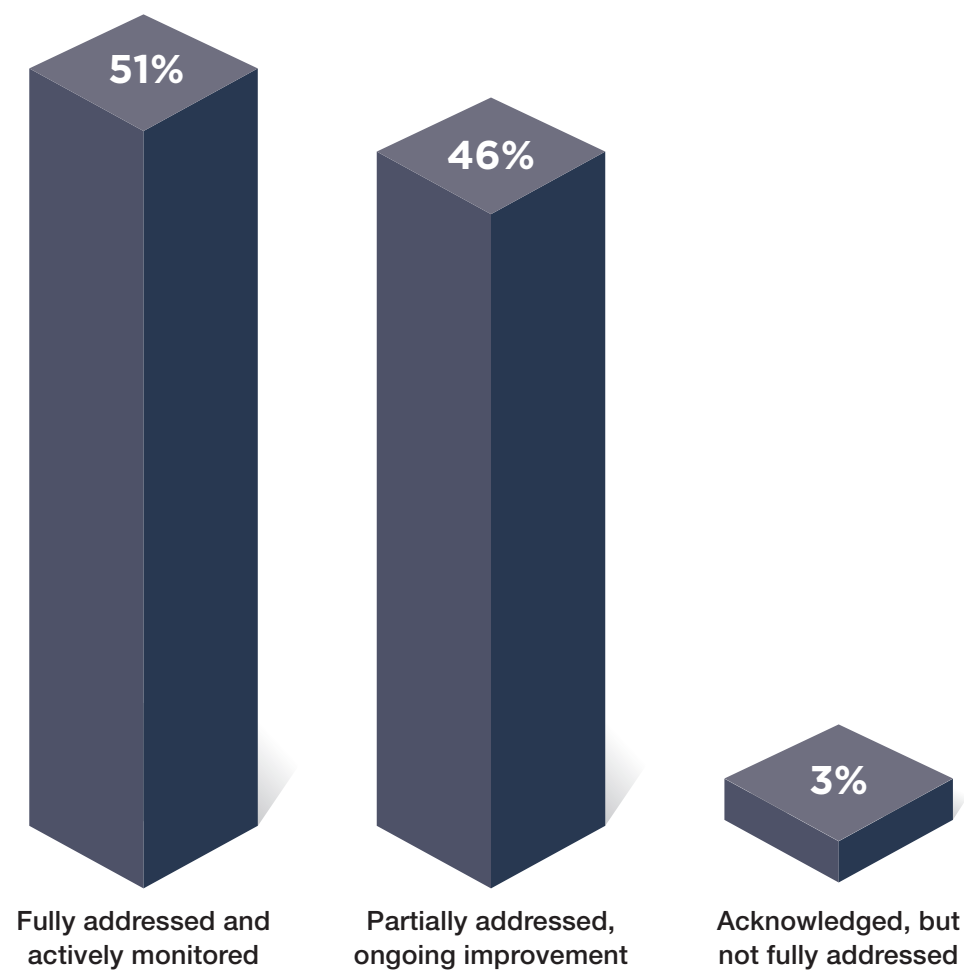
60% of respondents say security issues are more likely to delay product launches than feature bugs, highlighting how security has become a major factor in delivery timelines, and why proactive AppSec must be built into the development process.

OWASP Gaps Leave Teams Exposed

Security teams are aware of the rising threat landscape, but their ability to respond remains uneven. Just over half of respondents (51%) say they fully address and actively monitor **OWASP Top 10 threats**. Nearly as many (46%) admit they are still in the improvement phase. These figures highlight a widespread maturity gap, one that leaves many organizations vulnerable to well-known attack vectors. With OWASP (Open Worldwide Application Security Project) serving as a foundational benchmark

for secure development, incomplete coverage underscores the need for more consistent practices, deeper training, and better AppSec support. Failing to fully address OWASP risks isn't just a technical issue, it translates directly into business liability. According to IBM's 2024 Cost of a Data Breach report, organizations with mature DevSecOps practices saved an average of \$1.76 million per breach, reinforcing the value of proactive AppSec investment.³

How would you describe your organization's preparedness against OWASP Top 10 threats?



Only 51% of organizations report that **OWASP Top 10 threats** are fully addressed and actively monitored, while 46% are still in the improvement phase. This underscores a maturity gap that creates real exposure. Cypress's hybrid approach to AppSec can help teams close that gap.

³Source: IBM 2024 Cost of a Data Breach Report

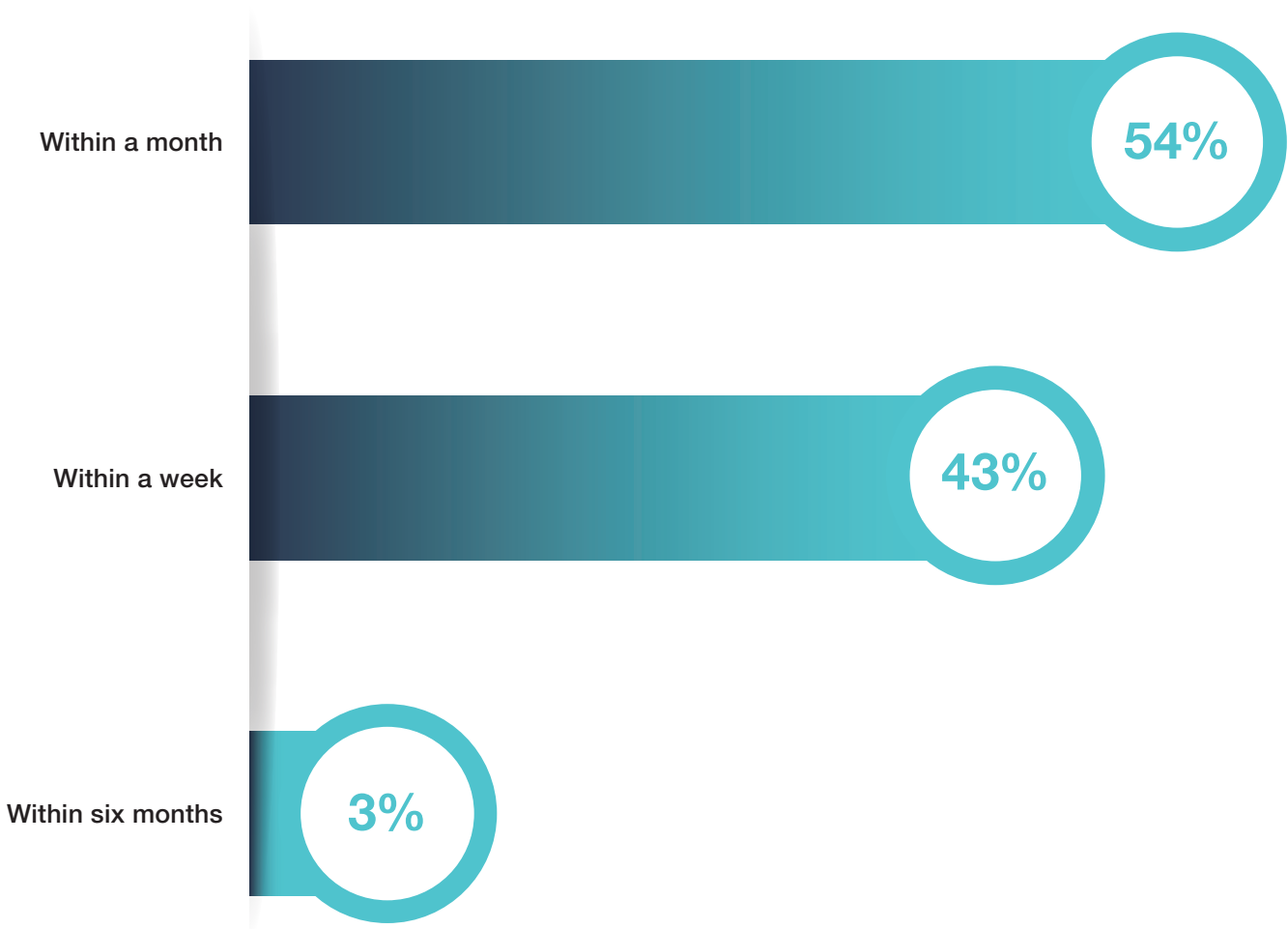
Detection Still Takes Too Long

While breach detection times have improved slightly in recent years, they remain unacceptably long. Just 43% of security teams believe they would detect a breach within a week. The majority say it could take a month or more, ample time for threat actors to escalate privileges, exfiltrate data, or tamper with operations. This detection lag puts customers, employees, and partners at heightened risk and reinforces the need for continuous monitoring and real-time alerting across environments.

“Security logging for cloud instances isn’t implemented, delaying detection.”

— Director of Technology, Financial Services, U.S.

If your app was breached today, how long would it take before someone noticed?

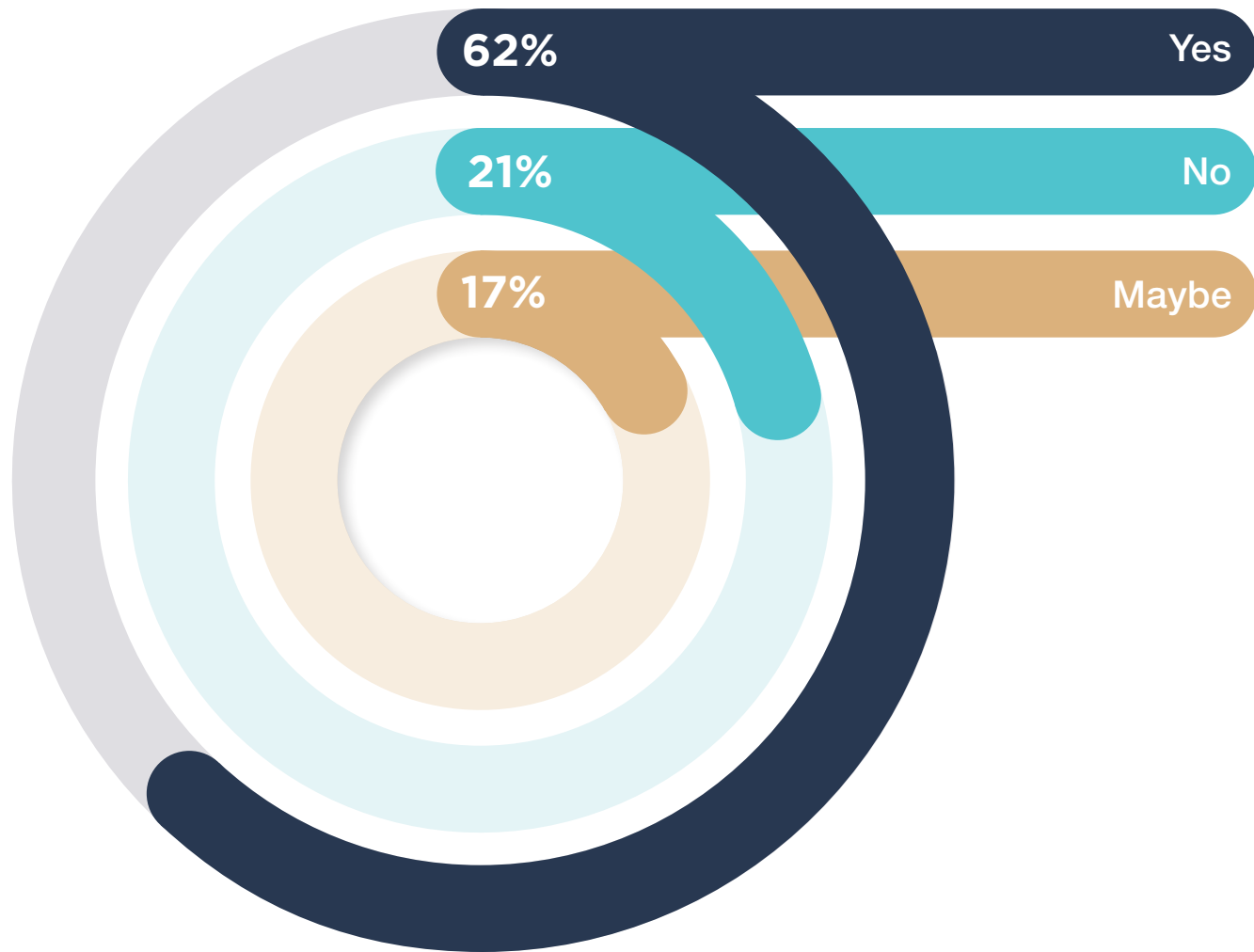


Nearly 43% believe their team would detect a breach within a week, while 54% estimate it would take up to a month. This lag in detection reinforces the need for continuous AppSec monitoring and alerting.

Job Security Tied to AppSec Risk

The inevitability of an application-level cyberattack and ongoing gaps in AppSec maturity are fueling concern among IT and security leaders, many of whom worry they'll be held accountable if something goes wrong. Nearly 80% of respondents expressed concern that a security incident could cost them their job: 62% admitted they are worried about being let go, while another 17% said it was a possible outcome. This level of anxiety highlights the personal risks tied to AppSec and reinforces the need for trusted, expert support.

Are you worried about getting fired because of an application level cyberattack?

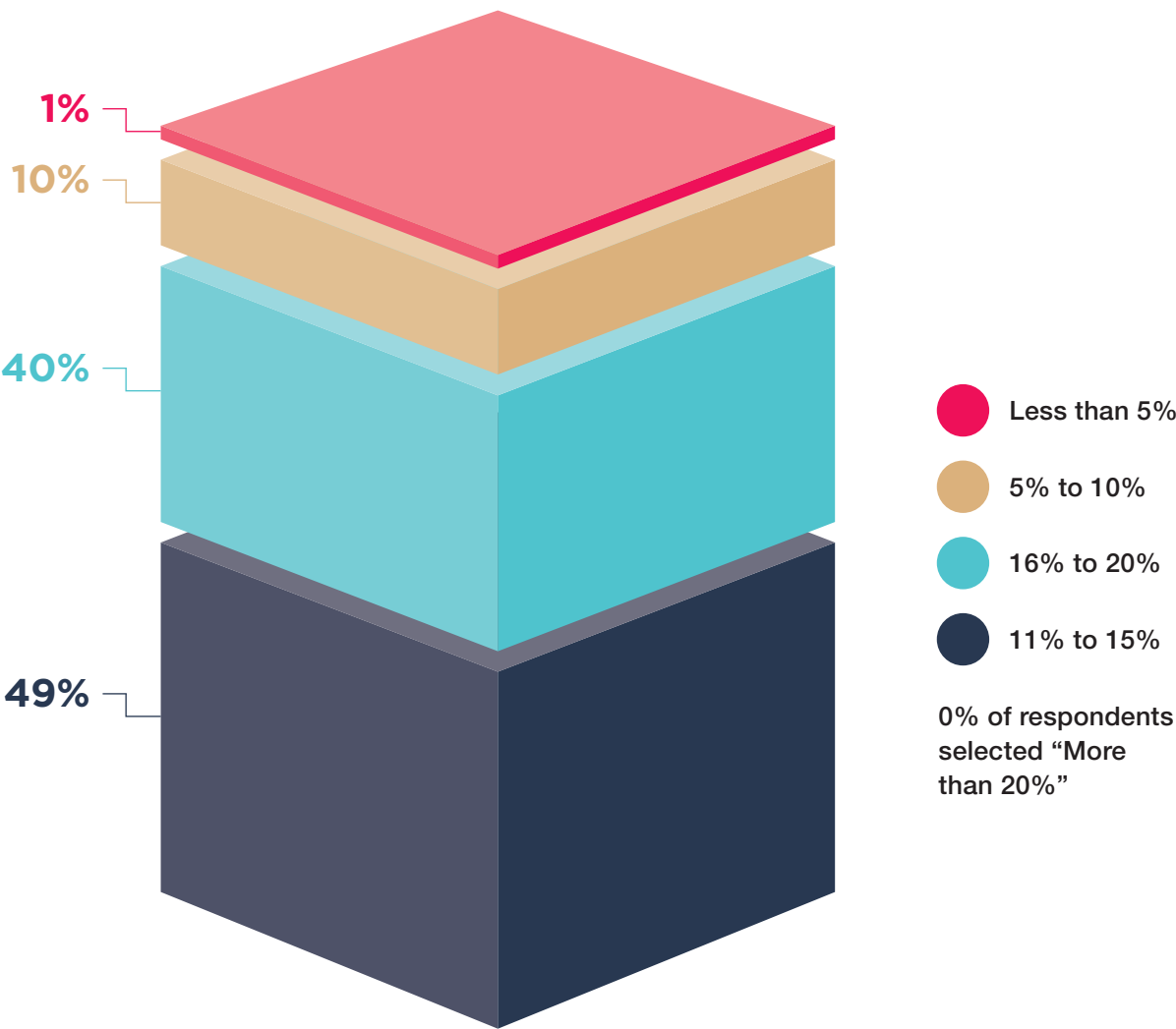


62% of respondents admit they're worried about losing their job due to an AppSec incident, illustrating the high-stakes pressure security leaders and engineers face, and the importance of trusted third-party support.

AppSec Budgets Don't Match the Risk

Despite the growing risk of cyberattacks, many organizations are still underinvesting in application security. Nearly 90% of respondents say their teams allocate just 11% to 20% of their overall security budgets to AppSec, with none reporting investments above 20%. While this might appear sufficient at first glance, it falls short when considering that a significant share of breaches originate from application-layer vulnerabilities. As application threats escalate, budget alignment remains a critical gap.

What % of your overall security budget is allocated to application security?



89% of respondents allocate between 11% and 20% of their security budget to application security. This reflects growing recognition of AppSec as a critical investment area. However, very few exceed that threshold. This shows most teams remain resource-constrained.



.....
“Encrypted or hidden data can look suspicious to scanners.”

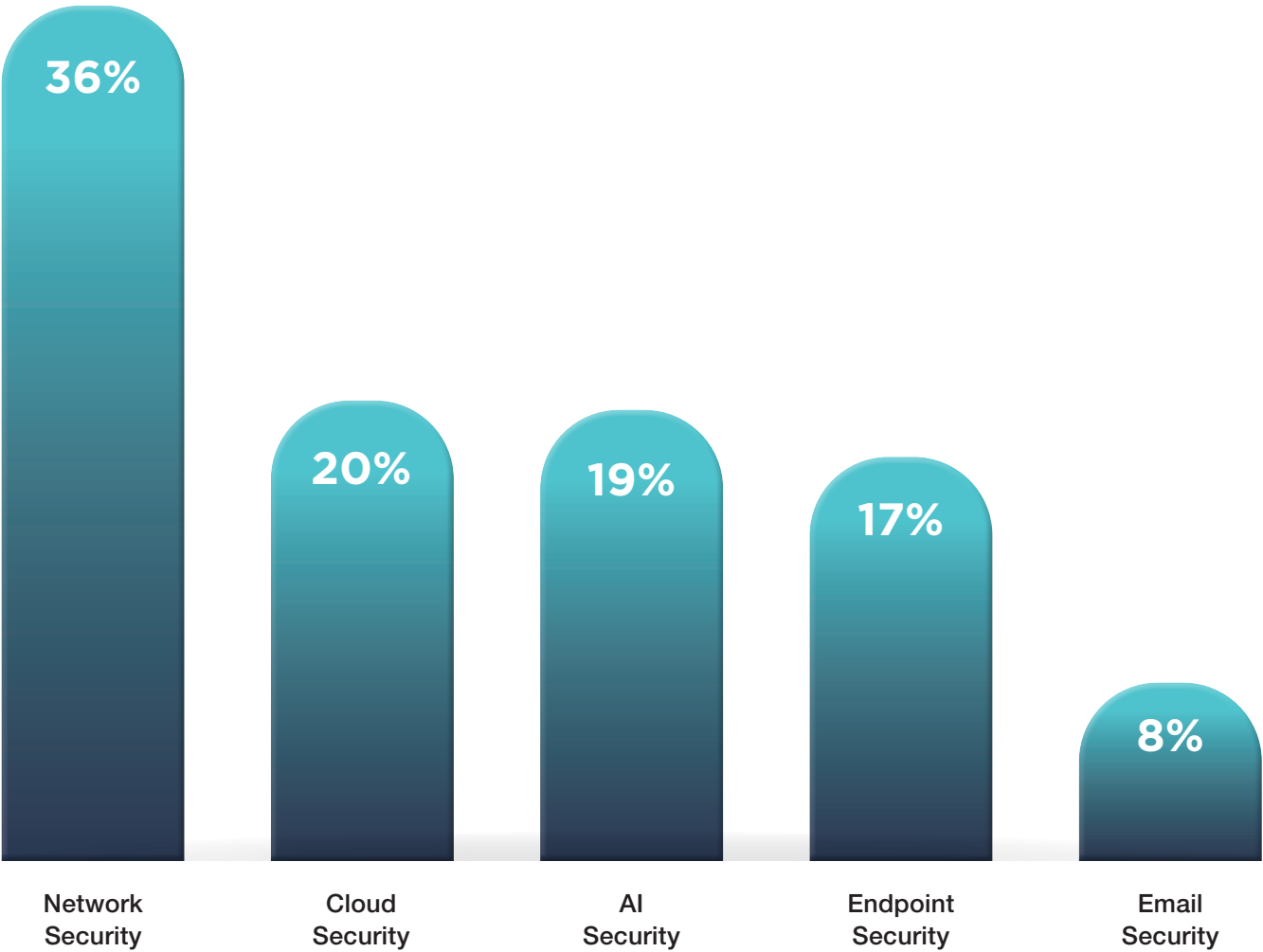
— Chief Information Security Officer,
Financial Services, U.S.

.....

Perimeter Still Wins Out

Organizations continue to prioritize perimeter defenses over application-layer protections. More than one-third of respondents say network security receives more budget than AppSec, and nearly 20% point to cloud security as a higher priority. It’s a concerning trend, given that application flaws account for 43% of breaches, leaving critical gaps where attackers are most likely to strike.

Which of the following areas currently receive more budget than Application Security in your organization?

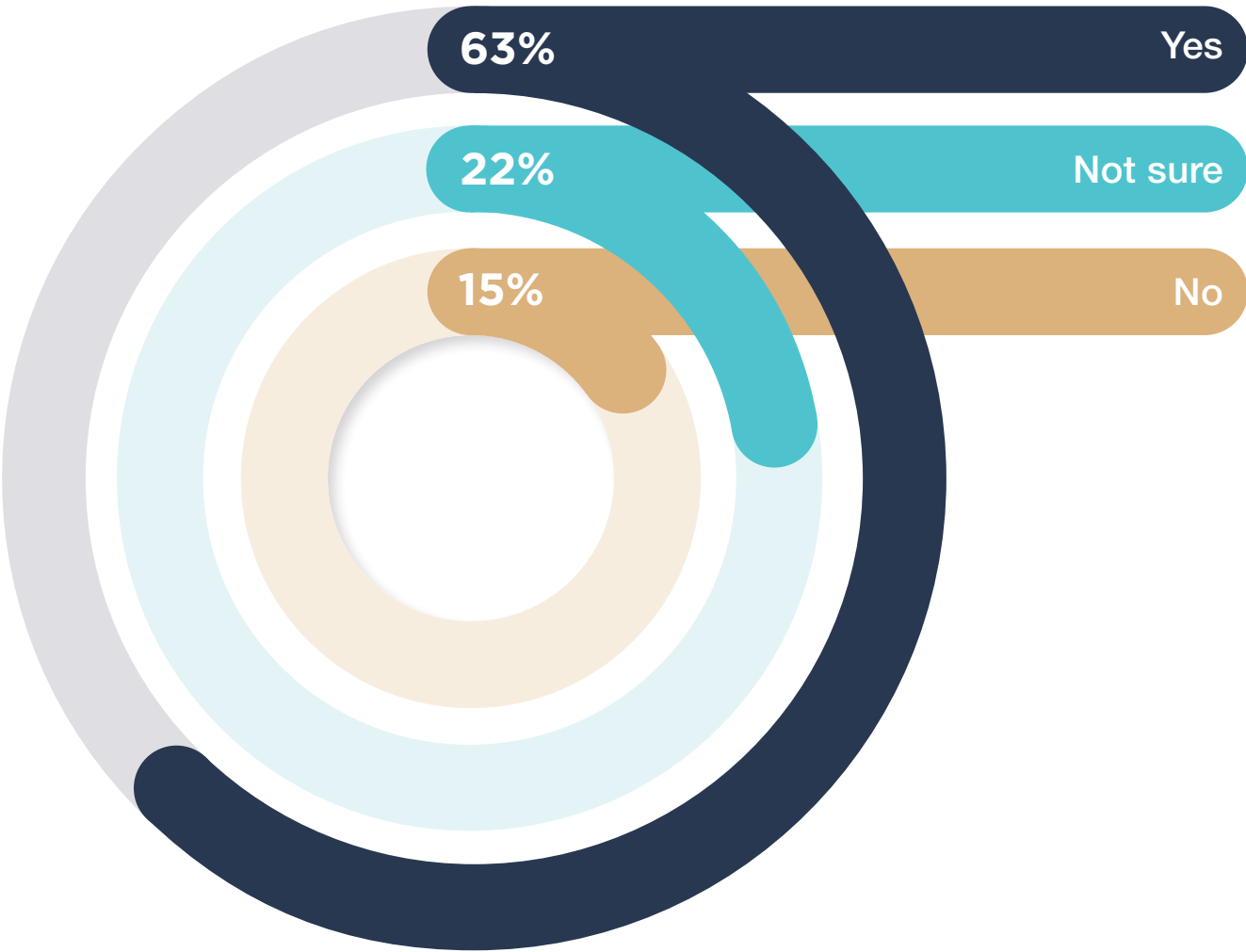


36% of respondents say network security receives more funding than application security, while 20% say cloud security does. This suggests that many organizations still prioritize traditional perimeter defenses over application-layer protection. That’s a concerning trend, given that application flaws account for 43% of breaches.

Security Shortcuts Still Happen

The pressure to bring apps to bear quickly in highly competitive markets has pushed an alarming number of security practitioners to do what should be the unthinkable, knowingly ship insecure code. A striking 63% of respondents admit their organization has knowingly released insecure code to meet a deadline. Another 22% aren't even sure, highlighting a breakdown in oversight and a culture where speed is still prioritized over security.

Has your company ever knowingly pushed insecure code to meet a deadline?



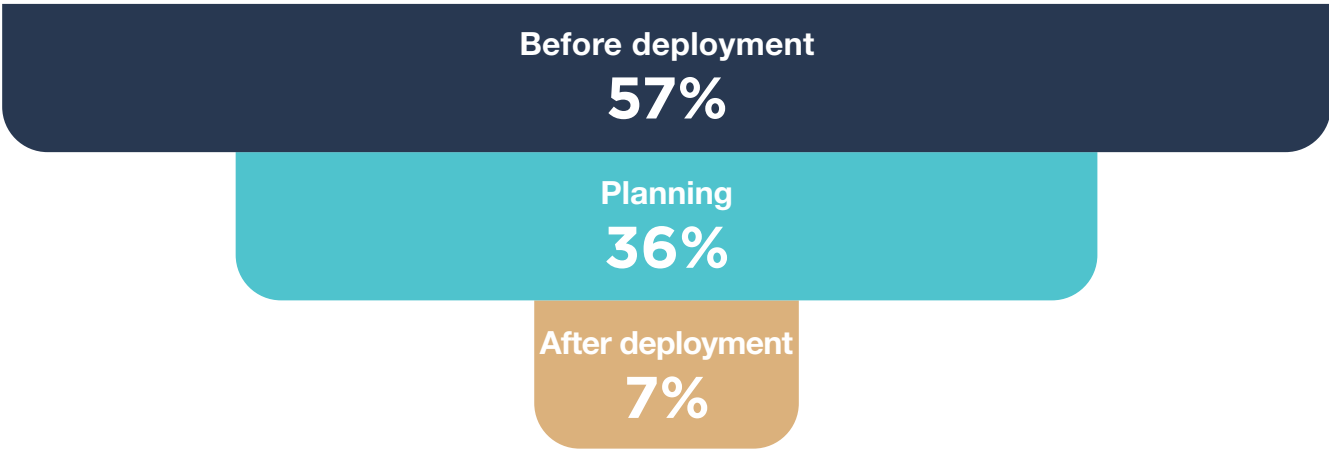
63% of respondents say their organization has knowingly released insecure code to meet a deadline, and 22% say they aren't sure. The data is clear that delivery pressures are still winning out over risk mitigation in many teams.

Security Left Behind in the SDLC

While many organizations recognize that strong security practices can accelerate innovation and support business goals, too many still treat security as a bolt-on rather than a built-in component. Only 36% of teams involve security at the planning stage, while 57% wait until late testing or deployment. This late entry limits risk reduction opportunities and prevents teams from fully benefiting from a true partnership with security.

Integrating security from the outset of the Software Development Life Cycle (SDLC) can improve release velocity, reduce risk exposure, and lower remediation costs, especially as systems grow more complex.

When do you typically involve security in your SDLC?



“Unsecured APIs in mobile backend services are a big worry.”

— Director of Technology, Education, U.S.

“The pressure to ship quickly means perfect code is useless if the server is misconfigured.”

— Director, Information Technology Operations, Retail, U.S.

Only 36% of respondents involve security during the planning stage of the SDLC, while 57% wait until just before deployment. This delay misses key opportunities to shift security left and reduce costly rework. Earlier integration could dramatically improve both risk posture and release velocity.

Critical AppSec Work Goes Undone

Even organizations with strong security teams and sizable budgets struggle to keep up with essential AppSec tasks. Half of respondents say their teams lack the time or resources for secure code reviews, one of the most fundamental safeguards against releasing vulnerable applications. Other critical activities such as security unit testing (42%) and threat modeling (36%) are also deprioritized due to internal bandwidth constraints. These gaps highlight the need for expanded AppSec support across all stages of the development cycle.

Which AppSec activities do you wish your team had time or resources for? (Select all that apply)



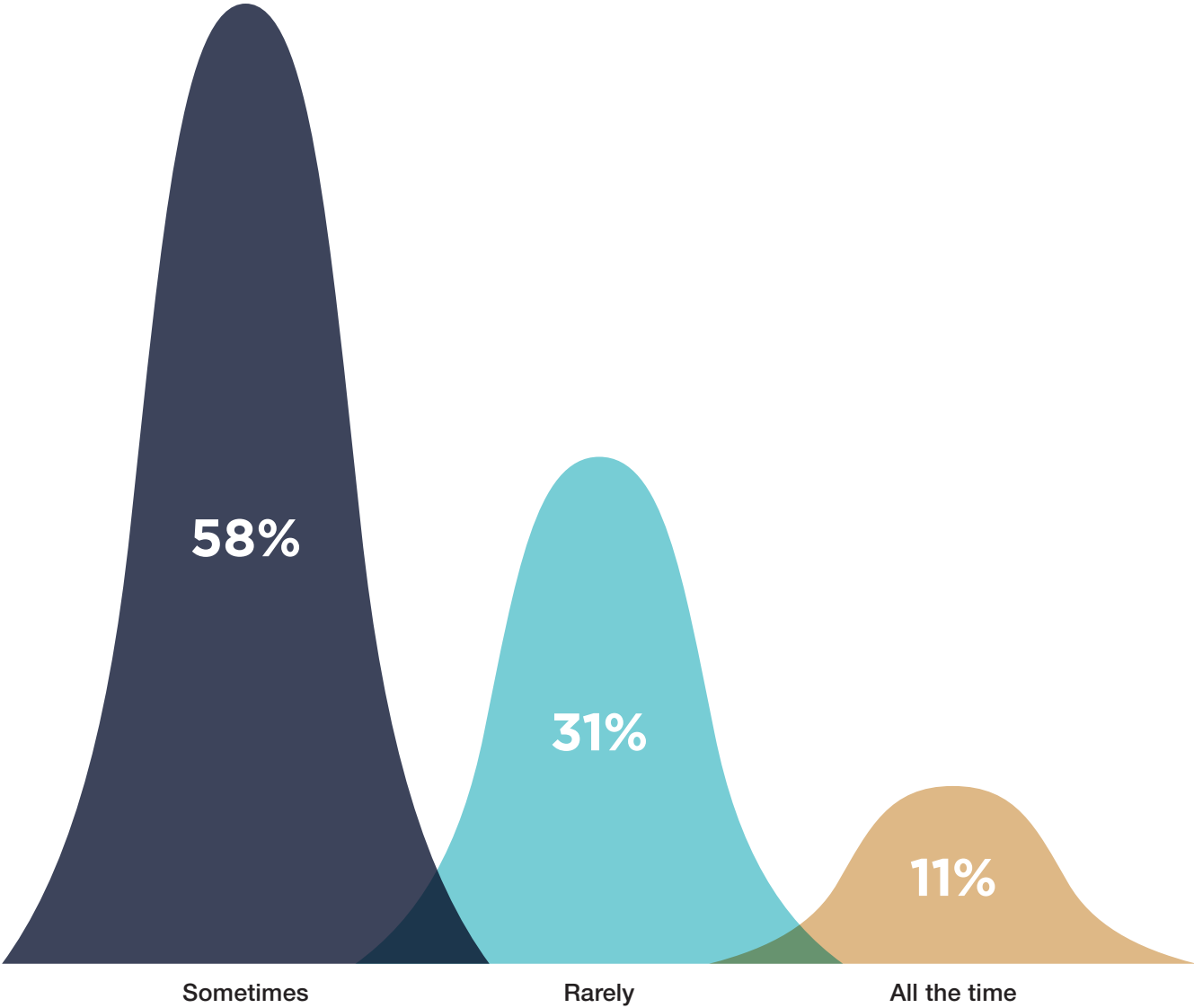
50% of respondents say they lack time for secure code reviews, 42% cite unit testing, and 36% mention threat modeling. These gaps point to a widespread need for AppSec support across all stages of the development lifecycle. Cypress’s service model helps teams execute these high-impact activities without straining internal bandwidth.

Noise in the System

False positives remain one of the most persistent frustrations in application security. 58% of respondents report encountering them frequently, with 11% saying they happen constantly. These alerts can overwhelm teams, dilute attention from real threats, and undermine trust in security tools—ultimately delaying triage and resolution.

Yet there’s a silver lining: many teams are learning from these noisy signals. Repeated false positives have prompted stronger collaboration, improved tuning processes, and a sharper focus on what matters most. Outsourcing to partners who offer depth without disrupting agility becomes a strategic advantage.

How often do you get false positives from security scanners?



58% of respondents report frequent false positives from security scanners, and 11% say it happens all the time. The noise created by poorly tuned tools continues to drain time and attention. Cypress’s human-led validation approach helps teams focus on what truly matters.....actual risk.

Why Outsourcing AppSec Is on the Rise

Data-Driven Insights

Have you considered outsourcing any part of your Application Security program?



83% of respondents have considered outsourcing at least part of their application security program. This shows strong market readiness for managed AppSec solutions. Cypress is well positioned to meet this demand with scalable, expert-driven services.

Security burnout is real

Most security professionals—**over 8 in 10**—say they are open to outsourcing parts of their AppSec program. The reason? Internal teams are maxed

out, and false positives are a key source of friction, distracting teams from real threats.

Common Business Drivers for Outsourcing Application Security

The cost of a breach is too high to risk internal shortfalls

Finding and retaining specialized AppSec talent is difficult and expensive

A loss of customer trust or service disruption could damage the brand

Compliance requirements are becoming more complex and demanding

Security teams are already overextended across other IT functions

Accelerated development cycles leave little time for thorough in-house reviews

Organizations can't afford to monitor application security 24/7

Breach detection and response must keep pace with modern threats

What's Fueling the Shift Toward Expert Help

More Signal, Less Noise

Security teams aren't giving up, they're getting smarter. But the tools they rely on often generate more confusion than clarity. Many respondents shared frustrations about scanner misfires and system blind spots:

“Scanners act as tools, but humans decide what matters.”

— Director, Strategic Technology, Financial Services, U.S.

“Heuristic-based detection is too aggressive in our environment—this affects scan accuracy.”

— Director of Information Technology, Healthcare, U.S.

“Manual checks are encouraged when alerts look suspicious.”

— Chief Technology Officer, Financial Services, U.S.

“Apps with lots of logs raise too many alerts.”

— Chief Technology Officer, Financial Services, Canada

“Static analysis tools mislabel safe variables as dangerous.”

— Chief Information Security Officer, Financial Services, U.S.

What Keeps Teams Up at Night

From unencrypted data and exposed APIs to insecure mobile practices and internal process failures, security teams shared what really keeps them up at night. These aren't just theoretical risks — they reflect real-world exposures happening today across development environments.

The findings are clear: security teams want better visibility, faster feedback, and greater confidence in the tools and processes meant to protect them.

What keeps you up at night when it comes to application security?

Top AppSec Concerns by Category

Cloud and Configuration Gaps

“Public or shared keys for cloud access are a big worry.”
— Chief Technology Officer, Financial Services, U.S.

“Cloud misconfigurations caused by automation tools cause sleepless nights.”
— Chief Technology Officer, Financial Services, U.S.

“Uncontrolled cloud console access risks unauthorized changes.”
— Chief Technology Officer, Retail, U.S.

“Legacy cloud accounts with weak credentials keep me up.”
— Director Of Technology, Retail, Canada

API and Token Exposure

“Authentication details exposed in URLs are a big concern.”
— Director Technology, Financial Services, U.S.

“Broken API permissions allow unauthorized data access.”
— Associate Director of Information Literacy and Instructional Technology, Education, U.S.

“API tokens stored insecurely in mobile apps pose a huge risk.”
— Chief Information Security Officer, Financial Services, U.S.

“Internal API endpoints lack proper authentication checks.”
— Cloud Security Engineer, Financial Services, U.S.

Mobile App Vulnerabilities

“Sensitive info like passwords is stored in insecure logs.”
— Director Of Technology, Financial Services, U.S.

“Authentication tokens exposed in mobile apps can be hijacked.”
— Chief Information Security Officer, Education, U.S.

“No integrity checks for mobile app installation or updates is troubling.”
— Security Operations Engineer, Financial Services, U.S.

“Insecure third-party SDKs in mobile apps can be exploited.”
— Chief Technology Officer, Financial Services, U.S.

Data Security and Visibility

“Sensitive data isn’t encrypted during transit between devices and servers.”

— Director, Information Technology, Healthcare, Canada

“We don’t use cloud provider audits to find weaknesses.”

— Chief Technology Officer, Financial Services, U.S.

“Non-encrypted S3 buckets for sensitive data are a big issue.”

— Chief Technology Officer, Financial Services, U.S.

“Error messages showing too much detail could help attackers.”

— Chief Technology Officer, Financial Services, U.S.

Process Gaps and Human Error

“Developers at times skip security steps when in a hurry to work faster.”

— Director of Information Technology, Healthcare, U.S.

“Perfect code is useless if the server is set up wrong and can open doors for hackers.”

— Director Information Technology Operations, Retail, U.S.

“AI-generated code might have hidden bugs that are easy to miss.”

— Director of Information Technology and Security, Healthcare, U.S.

“Putting off fixing problems can pile up and make the app unsafe.”

— Director of Technology and Innovation, Education, U.S.

Authentication and Access Control

“Weak password reset mechanisms allow attackers to bypass security checks.”

— Senior Director of Information Technology, Healthcare, U.S.

“No proper logout functionality leaves mobile sessions open.”

— Chief Information Security Officer, Financial Services, U.S.

“Serverless functions often run with overly broad permissions, accessing more than they should.”

— Chief Technology Officer, Financial Services, U.S.

“Poor session handling makes it easy for hackers to take over accounts.”

— Director of Information Technology, Retail, U.S.

Conclusion: A New Mandate for Modern AppSec

The research is clear: AppSec teams are under pressure, under-resourced, and in need of better solutions. While automation and shift-left strategies remain important, the data shows there's no substitute for context-aware security and expert support. In today's dynamic development environment, organizations need more than tools, they need partners.

Cypress's hybrid approach with its EASy managed service, combining tooling expertise, developer alignment, and flexible outsourcing, offers a scalable path forward, delivering security leadership without the overhead of building it in-house. As threats become more sophisticated, proactive and precise application security isn't just a priority. It's a prerequisite for innovation and resilience.

Contact Cypress Data Defense to learn how your team compares—and how to strengthen your security posture without slowing down innovation.

Let's talk about how Cypress can strengthen your Appsec posture—without slowing your roadmap.

Protect What Matters

Survey Methodology

The 2025 State of Application Security survey was conducted in May 2025 by TechStudio, an Energize Marketing company, in partnership with Cypress Data Defense. It gathered insights from 250 IT and security leaders across North America, 92% based in the United States and 8% in Canada.

Respondents came from companies with 250 to 1,000 employees, evenly split between smaller mid-market firms (54%) and larger mid-market firms (46%). All organizations reported annual revenue between \$50 million and \$1 billion, ensuring a consistent business profile across the sample. The survey focused on security-conscious sectors, with Financial Services (67%) leading the response pool, followed by Education (20%), Healthcare (7%), and Retail (6%).

Participants primarily held senior roles: C-level executives made up 56% of the sample, followed by Directors (33%), staff-level security engineers (10%), and VPs (2%). Titles included Chief Information Security Officer (CISO), Chief Technology Officer (CTO), Director of IT, Application Security Lead, and DevSecOps Manager.

All respondents had direct involvement in application security strategy, tooling, or operations. The survey explored practices, challenges, budgets, staffing, tooling limitations, and perspectives on outsourcing and AppSec readiness.

The survey has a margin of error of ±5.7% at a 95% confidence level.



Cypress Data Defense

Cypress Data Defense is a leading provider of application security and network security solutions. Founded by a team of cybersecurity experts, our mission is to empower organizations to deliver secure, high-quality software without compromising speed or innovation.

Why Choose Us?

At Cypress Data Defense, we're committed to making security a seamless part of your development process.



Expertise: Decades of experience in application security and compliance.



Innovation: Cutting-edge solutions tailored for Agile and DevOps teams.



Results: Proven track record of reducing vulnerabilities and streamlining compliance.

Cypress Data Defense
14143 Denver West Pkwy
Suite 100
Golden, CO 80401

PH: **720.588.8133**

Email: **info@cypressdatadefense.com**

www.cypressdatadefense.com



@cddsecurity



Cypress Data Defense



CYPRESS
DATA DEFENSE