Checkmarx

2025 Survey

# A CISO's Guide

## to Steering AppSec in the Era of DevSecOps

# Table of Contents


**Introduction** ..... 3

**Industry Insights** ..... 4

- Application Security Continues to Be a Business Differentiator ..... 4
- Developers and Product Teams Are Taking Center Stage in Security Decisions ..... 4
- DevSecOps Maturity Challenges Expose Critical Security Gaps ..... 5
- Tool and Process Fragmentation Creates Security Blind Spots ..... 5

**Key Findings: The New Realities Facing CISOs in 2025** ..... 6

- Application Security Continues to Be a Business Differentiator for Companies and Buyers Alike ..... 6
- CISOs Continue the Steady Shift from Security Enforcers to Business Enablers ..... 8
- Application Security Hands-on Management is Shifting to Product Teams and Developers ..... 9
- Budgets are Growing to Accommodate Product Teams and Regulatory Needs ..... 12
- Organizations Are Struggling with DevSecOps Maturity ..... 13
- Current AppSec Programs Underperform and Underdeliver ..... 15
- Fragmented Tools and Partial Coverage Are Leaving Security Blind Spots ..... 16

**Effective Governance in the New Era: What CISOs Must Prioritize in 2025 and Beyond** ..... 18

**Demographics** ..... 19

**Conclusion** ..... 20

**Methodology** ..... 21

# Introduction

2025 marks a pivotal moment for CISOs as the landscape of Application Security undergoes a fundamental transformation. Rather than maintaining direct control over the Software Development Lifecycle (SDLC), many CISOs are evolving into a more dynamic policy/compliance role and must learn to operate in distributed security ecosystems, orchestrating security through development teams, AppSec managers, product security practitioners, and DevSec architects.

As organizations face tighter budgets, faster development cycles, and heightened security risks, CISOs must adapt their approach from direct control to a modular and flexible model. Depending on the organization, their role now mixes strategic oversight with hands-on actions, making security a shared priority between development, security, and product teams.

**CISOs must adapt to a modular and flexible model,**

combining strategic oversight with hands-on actions, and **making security a shared priority** between development, security, and product teams.

The complexity of this transition is amplified by unprecedented business stakes. Companies in every sector are becoming more dependent on software-driven products and services, making security failures not just technical incidents, but business-critical issues. To address this, security teams are working more closely with developers, embedding security at every stage—from code to cloud. Shared KPIs between development and security teams are becoming the norm, fostering alignment and collaborative workflows that balance security needs with development speed.

**While CISOs retain final say in security strategy, development teams are becoming key players in security implementation.** The emergence of roles like Product Security Managers reflects this shift in responsibilities, with new collaborative processes aimed at aligning development and security goals.

However, this redistribution of responsibility comes with significant challenges, revealing concerning gaps in security coverage. Many organizations remain in the early stages of DevSecOps maturity, with uneven protection across applications and fragmented tooling creating dangerous blind spots.

For CISOs and security decision-makers navigating this transformation in how security is handled and distributed across the organization, this report provides a practical roadmap based on a survey of 200 leading CISOs across diverse industries and regions.

Performed in collaboration with Global Surveyz, the research focused on organizations with annual revenues exceeding $750 million and development teams of at least 180 developers. Participants represented key sectors including banking & finance, insurance, software, technology, engineering, media, manufacturing, industrials, and the public sector, spanning the United States, Canada, Western Europe, and the APAC region.

The report outlines key trends and offers actionable insights for fostering stronger partnerships with development teams, aligning security and development goals, and embedding security throughout the development lifecycle. By embracing this new paradigm and addressing its inherent challenges, CISOs can be better equipped to navigate their organizations to better manage risk, achieve greater security coverage, and position security as a true business enabler in an increasingly software-driven world.

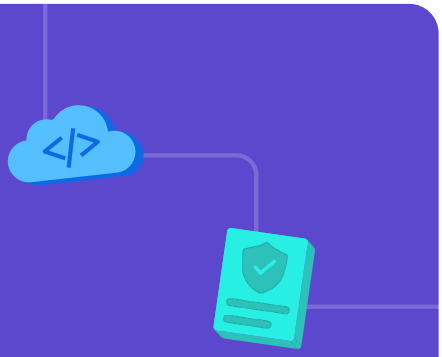
# Industry Insights

01

## Application Security Continues to Be a Business Differentiator

We continue to see that security is no longer just a technical requirement. 49% of respondents report that buyers regularly consider application security in purchasing decisions, with 24% indicating it's "always" a factor. This is in line with the emergence and resources given to Product Security teams as organizations realize that high security is not only table stakes but directly impacts market trust and purchasing decisions.

However, this perspective varies significantly by region, with European buyers showing the highest sensitivity to security concerns, in contrast to more varied approaches in APAC and North American markets.



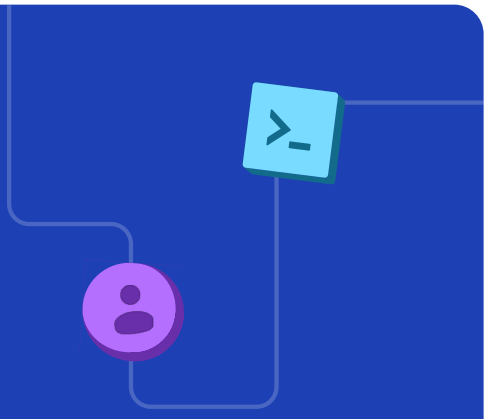
**The emergence of product security roles poses a new opportunity for CISOs.**

02

## Developers and Product Teams Are Taking Center Stage in Security Decisions

Decision-making is shifting away from centralized security teams, with development teams increasingly driving security practices. A strong indicator of this shift can be seen in software-based products, where 50% of organizations still assign security responsibility to CISOs, while 43% move security oversight to product teams.

In fact, 56% of organizations now report that most development teams are fully integrated with AppSec programs, signaling a fundamental transformation in how application security is approached and implemented. This shift in decision-making authority is usually not incidental, but rather part of an intentional strategy, based on the understanding that security must do more to fit developer workflows, as part of a development-centric view.



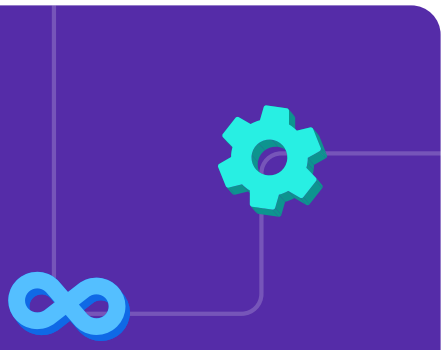
**A new role – product security – is increasingly being seen in enterprise companies.**

03

## DevSecOps Maturity Challenges Expose Critical Security Gaps

As security responsibilities increasingly shift from dedicated security teams to an evolving partnership with development teams, organizations face complex challenges in securing diverse development methodologies. With development processes ranging from agile to legacy approaches, security tools and strategies struggle to provide consistent, comprehensive protection across different workflows.

This underscores the need to move beyond traditional AppSec thinking and develop more flexible, adaptable DevSecOps approaches that can support the entire spectrum of development methodologies.



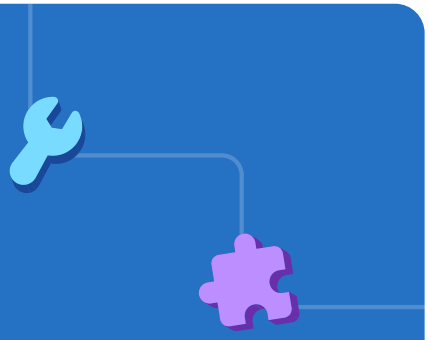
**Organizations are still struggling with DevSecOps maturity.**

04

## Tool and Process Fragmentation Creates Security Blind Spots

Existing security tools remain fragmented, creating significant blind spots in security coverage. As security decisions increasingly move to development teams (as noted in Insight 2 above), this fragmentation may be further exacerbated by disparate decision making without sufficient governance. On average, only 39% of business operations run on secured applications, and 70% of organizations report that half or more of their applications lack robust security measures.

This underscores the urgent need for CISOs to guide standardization while pushing to expand security coverage, particularly in later lifecycle stages like deployment and runtime, where protection is most critical.



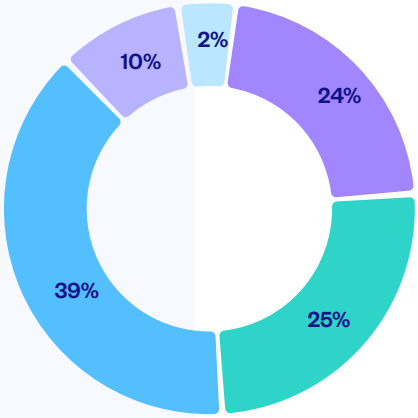
**CISOs need to push to expand security coverage in deployment and runtime.**

# Key Findings: The New Realities Facing CISOs in 2025

## Application Security Continues to Be a Business Differentiator for Companies and Buyers Alike

Application security has long moved from being a strictly technical issue into a growing business concern. For software companies, application security has become a critical buying criterion, shaping prospects' purchasing decisions and influencing customer trust. This continuing evolution elevates AppSec into a board-level and business-level conversation, requiring CISOs to articulate its impact on revenue, brand reputation, and competitive advantage. AppSec managers can also gain greater executive support by framing security needs in business terms, bridging the gap between technical challenges and strategic priorities.

Nearly half (49%) of respondents confirm that application security is a regular factor in purchasing decisions, with 24% saying it's "always" a consideration and 25% noting they're considering it "very often." Regionally, this trend is most pronounced in Europe, where 58% of respondents report that security is "always" a factor, compared to 33% in APAC and only 8% in North America. In Europe, regulatory frameworks like the EU's DORA directive are driving increased scrutiny of security standards, making robust application security essential for software vendors to remain competitive.




| | |
|---|---|
| Always | 24% |
| Very often | 25% |
| Sometimes, but growing | 39% |
| Sometimes, not growing | 10% |
| Not very often | 2% |

FIGURE 1
Prospects' Consideration of Application Security in Purchasing Decisions

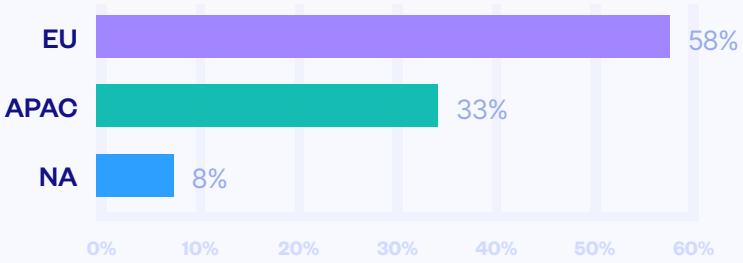
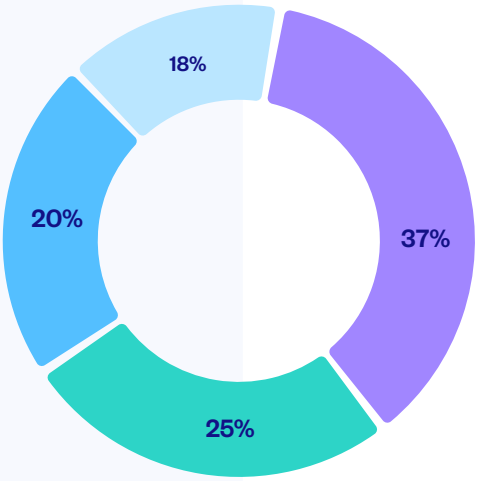



FIGURE 2
"Always", by region

The importance of application security risks at a business level is also mirrored in the CISOs approach to board-level communications. However, discussions often lack the business context needed to drive engagement and action.

For CISOs, the challenge lies in framing technical risks in terms that resonate with business stakeholders, aligning security metrics with organizational objectives such as regulatory compliance, customer acquisition, and retention. While 62% of CISOs report on application security risks to management or the board, 37% of them only report the number of identified vulnerabilities, without further business context or metrics - an approach that may fall short of conveying the broader business implications of security issues. Only 25% of respondents tie vulnerabilities to application or business risk metrics, which could offer a more compelling narrative. Alarmingly, 20% of respondents stated that their board or management does not request information on application security risks, and 18% do not report this information at all.




| | |
|---|---|
| Report on the number of identified vulnerabilities | 37% |
| Report on identified vulnerabilities and other/related application and business risk metrics | 25% |
| Management/board doesn't ask/care about application security risk | 20% |
| Don't report to management on AppSec program metrics | 18% |

FIGURE 3
Communication of Application Security Risk to Management or Board

**62%** **of respondents report on AppSec risks to the board**

but don't translate it into business implications.

# CISOs Continue the Steady Shift from Security Enforcers to Business Enablers

While CISOs have historically been viewed primarily as security enforcers focused on threat detection, access control, and identity management, their shift towards business enablement continues. Supporting business initiatives ranks highest at 34%, while traditional security cornerstones like threat detection and identity management rank near the bottom at 24% and 15% respectively.

This reprioritization reflects CISOs' evolution from technical security guardians to strategic business partners, with increasing emphasis on architecture (31%) and application development security (30%) and emerging concerns like AI governance (29%) outranking conventional security functions.

FIGURE 4
Top Priorities in 2024 for AppSec

As further demonstrated in Figure 4, application security has evolved from a mere technical consideration to a core business driver, evidenced by the tight clustering of the top three priorities, coming in in third with (30%). The high ranking of securing application development, coupled with its proximity to business initiatives, suggests CISOs increasingly view AppSec as a strategic enabler rather than just a technical requirement.

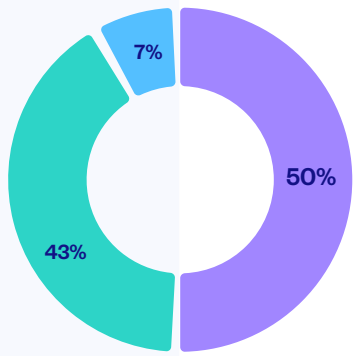
**CISOs' top priority**

is supporting business initiatives.

# Application Security Hands-on Management is Shifting to Product Teams and Developers

While it may seem paradoxical, given the importance CISOs place on ensuring application security, the responsibility for hands-on AppSec is increasingly divided between CISOs and different functions within product teams: 50% of respondents report that the CISO organization retains responsibility for securing software-based products, while 43% assign it to product teams. This shift has led to the emergence of dedicated product security roles within product teams, reflecting a broader trend of embedding security responsibilities closer to development functions. This evolving structure is reshaping the role of CISOs and challenging how the role is viewed traditionally.

As software drives new product categories, such as smart appliances or cloud-native applications, product security teams – who often have a stronger background in application security - now take on a larger share of the responsibility, especially in larger organizations. While this change helps align security efforts with development goals, it also creates challenges with oversight, risk, and governance. CISOs may face "shadow security" issues, where product teams operate without full visibility or oversight, potentially leading to inconsistent security practices.




| | |
|---|---|
| CISO organization | 50% |
| Product organization | 43% |
| Don't sell software-based products | 7% |

FIGURE 5
Responsibility for Securing Software-Based Products

The split in responsibility in securing software-based products between the CISO and product organization **poses new challenges for CISOs to manage risk without direct authority.**

As part of the ongoing shift, developers in many, if not most, organizations hold significant influence over security tools, processes, and priorities. Their ability to veto tooling and shape security strategies – whether through formal or informal influence - requires an adjustment in collaboration for effective risk management. To address this shift, CISOs must establish governance frameworks that set clear security standards, KPIs, and protocols across all teams, while actively considering where implementation can be managed best - by AppSec teams, dedicated product security teams or directly by development. By fostering collaboration and aligning strategies, CISOs can maintain oversight while empowering product teams to mitigate risks directly within the development lifecycle, ensuring comprehensive security outcomes across the organization.

This trend also highlights the need for shared KPIs and governance frameworks to bridge security goals and development workflows. By integrating security objectives into development processes, CISOs can ensure security is maintained at its highest level throughout the software lifecycle—even as more responsibilities shift to development teams. KPI-driven governance enables CISOs to maintain oversight and foster cooperation across teams, ensuring security remains a priority without disrupting development velocity.

Survey data underscores this shift. In 56% of organizations, most—but not all—development teams are fully integrated with AppSec programs, reflecting growing alignment. Additionally, 37% of organizations report a "security-first" development culture, a particularly strong trend in Europe (54%) compared to APAC (47%) and North America (28%). As developers increasingly shape security outcomes, decision-makers must prioritize collaborative frameworks that align development and security teams, building stronger security cultures across the organization.

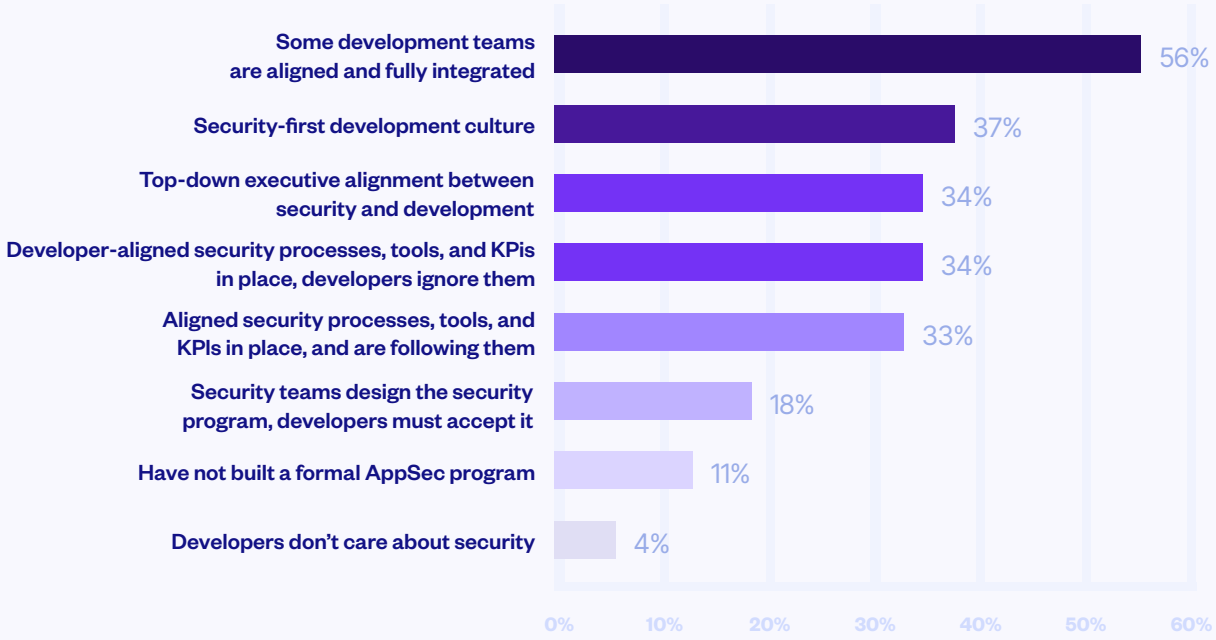



FIGURE 6

Alignment of Developers with Application Security Program

*Question allowed more than one answer and as a result, percentages will add up to more than 100%

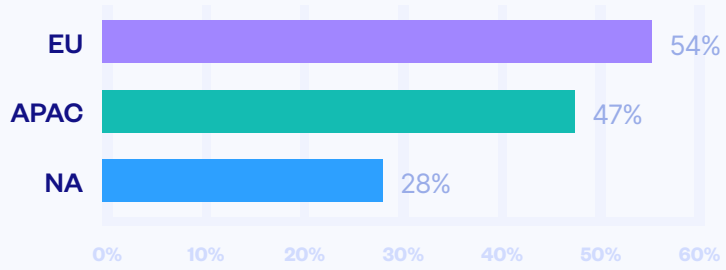



FIGURE 7

"Security-First Development Culture", by region

The survey also finds that the shift in decision-making power is not incidental, but rather part of an intentional strategy, based on the understanding that security must do more to fit developer workflows, as part of a development-centric view. As part of this effort, survey findings reveal key strategies organizations are employing to enhance developer engagement in application security.

The top approach is soliciting feedback from developers to improve security processes (41%), followed by appointing security champions within development teams (37%) and aligning priorities with R&D leadership from the top down (34%).

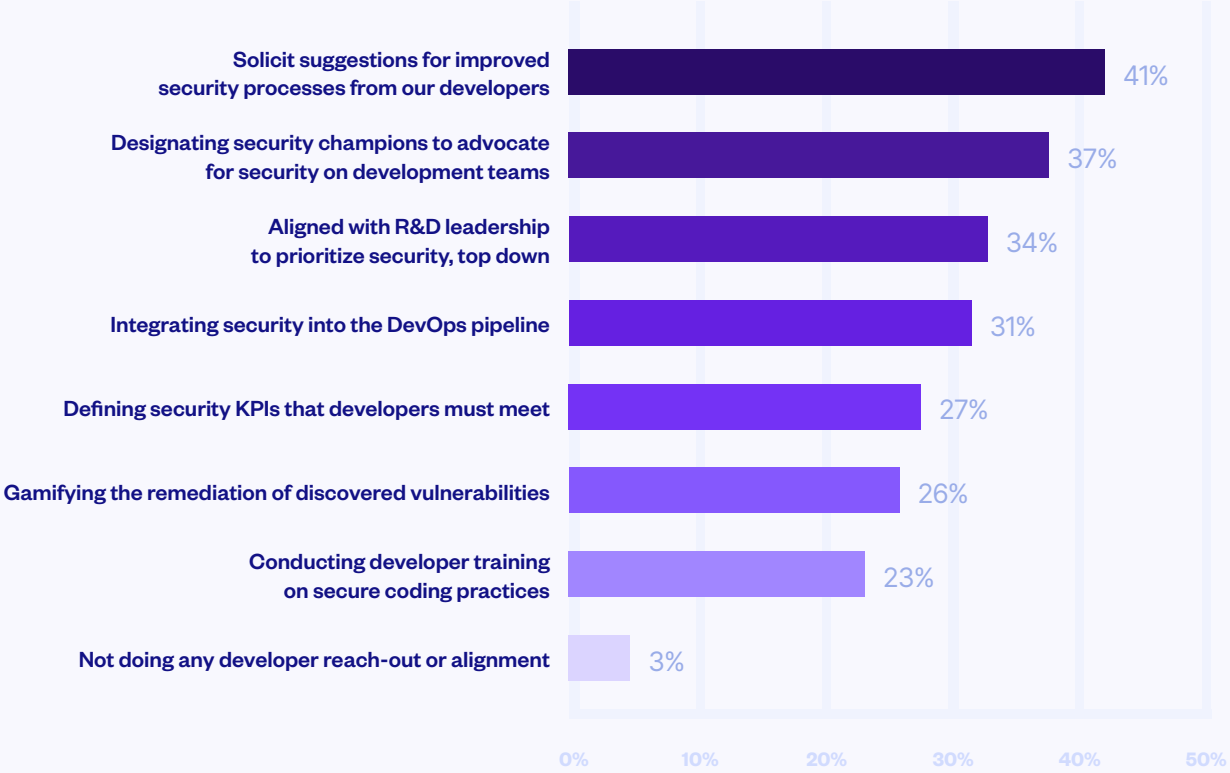



FIGURE 8

Efforts to Increase Developer Engagement in AppSec Program

*Question allowed more than one answer and as a result, percentages will add up to more than 100%

Organizations invest significant resources to **increase developer involvement** in DevSecOps efforts.

The migration of application security responsibilities varies significantly across different organizational contexts, reflecting a more complex and nuanced reality than simple delegation. In companies selling software-based products, where security directly impacts business goals like time to market, brand reputation, and customer acquisition, the transformation is accelerating faster (see figure 5 above) - evidenced by the emergence of dedicated product security teams.

This progression reflects a fundamental truth: organizations have already made the decision to view application security as an inseparable part of their business operations and many are shifting day-to-day decision making to the teams that are most directly involved with and capable to integrate AppSec with business objectives. But similarly to the delay between the decision to change course on an ocean freighter – there's a lag between steering the helm and when the bow actually stabilizes on the new course.

An example of that is what we see in Figure 3 above, where a significant number of CISOs are still caught in the old course - with only 25% tying vulnerabilities to business metrics and 37% reporting security without business context.

For CISOs, success in this transitional period means leading rather than merely reacting to the transformation – actively treating AppSec as the business differentiator it is when reporting to the board and establishing governance frameworks (through platform engineering teams, organizational structures, and process standardization) that enable developer and product teams to integrate security into their workflows, while maintaining oversight.

# Budgets are Growing to Accommodate Product Teams and Regulatory Needs

AppSec budgets are growing as organizations prioritize secure development practices and adapt to evolving ownership dynamics in security. With the shift in decision-making from CISOs to product teams, targeted investments are required to safeguard application lifecycles and maintain compliance with regulatory frameworks like Europe's DORA directive. Supporting this trend, 78% of respondents reported an increase in their AppSec budgets for 2024, with 40% noting significant growth. While 71% anticipate further budget increases in 2025, only 25% expect substantial growth, signaling a potential moderation in investment rates. This may indicate a shift toward more focused spending as ownership and priorities evolve within organizations.

Regional variations highlight the impact of regulatory environments on budget allocation. In Europe, 56% of respondents reported significant budget growth, compared to 34% in North America and 33% in APAC. Europe's stringent compliance landscape, exemplified by the DORA directive, underscores the importance of sustained investment to ensure application resilience and security.

For CISOs and development teams, this data underscores the need to align budgets with strategic security objectives, ensuring that resources are deployed effectively to protect critical business applications and customer trust.

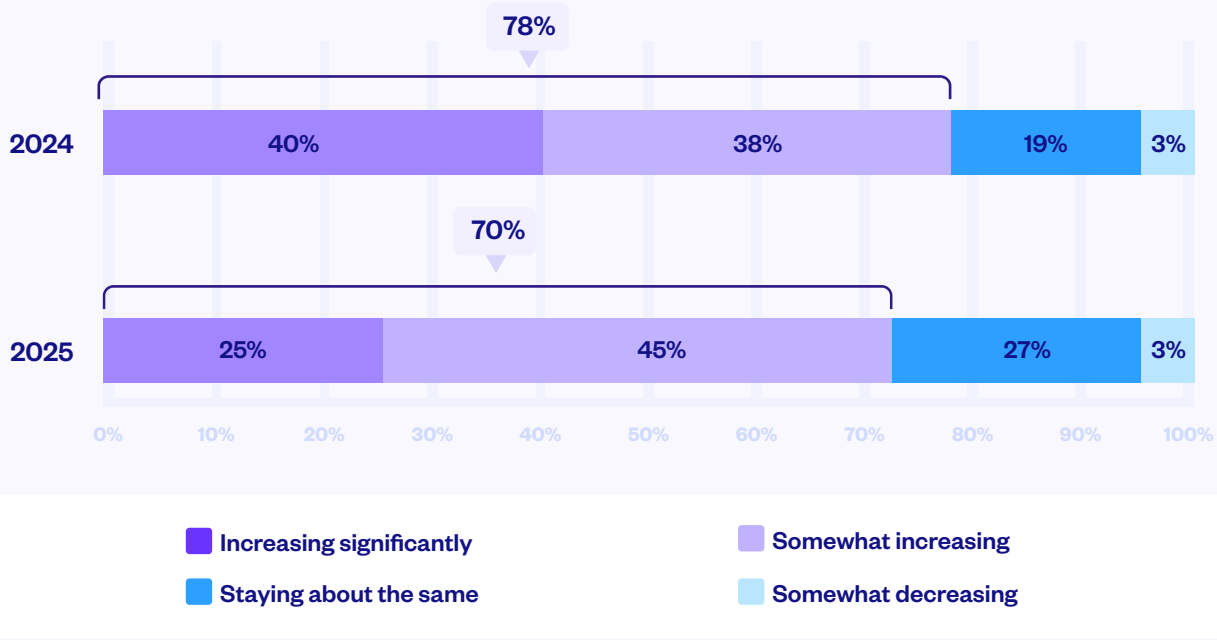



FIGURE 9
2024/2025 AppSec Budgets compared to 2023

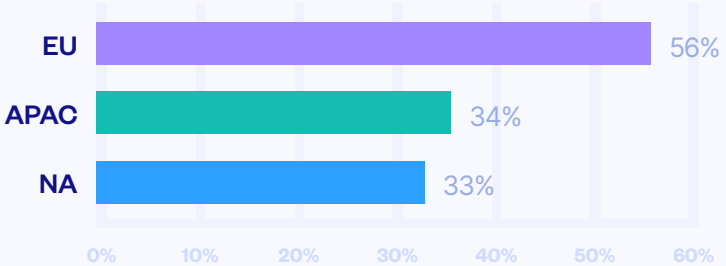



FIGURE 10
"Increasing significantly", in 2024, by Region

# Organizations Are Struggling with DevSecOps Maturity

Establishing a solid DevSecOps culture is essential for CISOs aiming to manage risk effectively and expand security coverage across more applications. While AppSec budgets – which were limited to begin with - and purchasing authority are shifting to product teams, CISOs' core mission is evolving into a broader, more complex role of strategic oversight and roadmap implementation, reducing organizational risk through setting security goals and ensuring that policies and initiatives are properly executed across the organization.

This shift can only succeed with a mature DevSecOps approach that integrates security into every stage of the development lifecycle, with CISOs taking on a governance role similar to internal regulators, setting security policies and requirements that teams must follow. This approach must leverage continuous integration and automated controls, where developers receive security feedback directly within their environments, and critical non-compliant builds are automatically halted until security standards are met. Achieving this level of integration requires alignment between security and development teams, alongside executive commitment to fostering a security-first culture.

The DevSecOps journey is intrinsically linked to agile practices, underscoring the importance of automation and adaptability. CISOs must collaborate closely with development leaders and platform engineers to embed security seamlessly within agile workflows, transforming DevSecOps from a buzzword into a foundational component of the organization's security framework. This collaboration ensures that security is not just a bolt-on but a core part of the development process.

Despite continuous efforts, most organizations remain in the early stages of their DevSecOps journey. Only 20% report a "high" or "very high" level of DevSecOps maturity, while 43% are just "getting started" or at a "low" level. Alarmingly, 8% have yet to start at all. This immaturity is reflected in application security coverage: 70% of organizations report that half or more of their applications lack significant security measures. These findings highlight a significant gap between awareness and execution, emphasizing the need for organizations to prioritize accelerating their DevSecOps adoption to secure the growing application landscape.

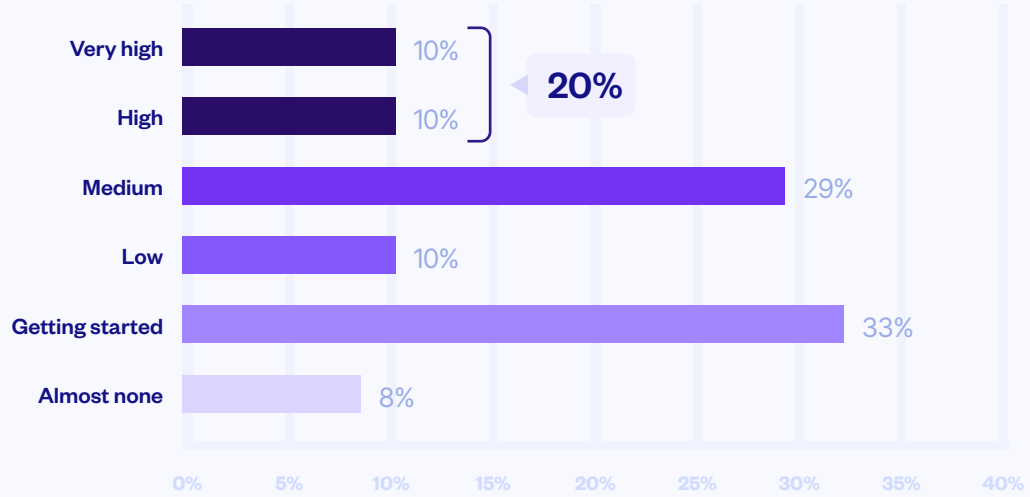



FIGURE 11
DevSecOps Maturity

DevOps remains aspirational with **51% of organizations** having no to low DevOps maturity.

Security integration is particularly challenging in large enterprises where development teams are split between modern agile practices and traditional waterfall methods, with different dev teams often managing thousands – or even tens of thousands – of development pipelines simultaneously in a single organization. This inconsistency creates challenges for application security, as agile teams typically rely on tools designed for fast, iterative development, while legacy teams may need traditional, more static tooling. The resulting fragmentation complicates security coverage, as many modern tools struggle to accommodate both agile and legacy workflows effectively.

Survey data underscores the extent of this challenge: Only 34% of applications, on average, are developed using modern or agile methodologies, and 82% of respondents report that half or fewer of their applications follow these approaches. This significant reliance on traditional development processes highlights the need for scalable solutions that support organizations as they navigate the shift toward agile and DevOps methodologies.

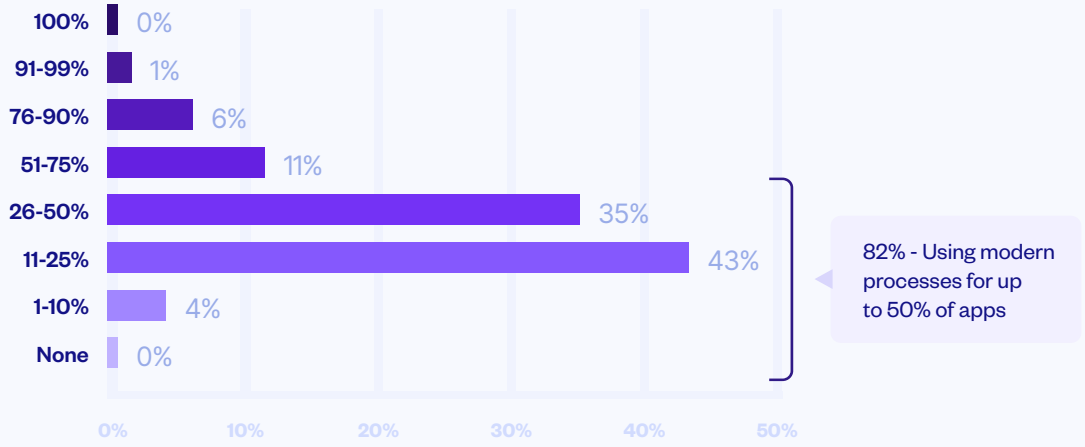



FIGURE 12
Percentage of Applications Developed Using Modern or Agile Processes

**82%** **of respondents report that half or fewer of their applications are developed using modern development processes.**

This emphasizes the need for tooling that can handle multiple development processes.

Additionally, Figure 13 highlights regional differences in AppSec maturity in terms of developer training, with European organizations more likely to implement AppSec in the developer training phase (32%), compared to just 13% in North America and 3% in APAC.

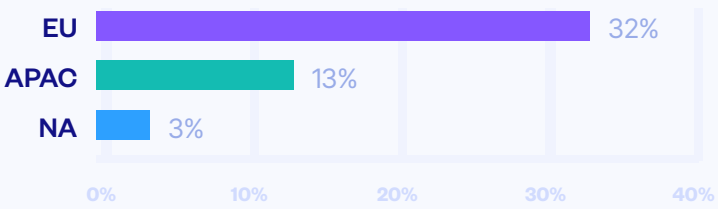



FIGURE 13
"Increasing significantly", in 2024, by Region

# Current AppSec Programs Underperform and Underdeliver

**Only a third of organizations are able to identify and remediate most or all vulnerabilities.** The majority, two-thirds of organizations, are unable to consistently remediate critical vulnerabilities, with the gap between detection and resolution being a significant challenge.

Another 31% have AST tools but struggle to ensure identified vulnerabilities are remediated, and 31% focus on improving the pace of addressing critical issues.

FIGURE 14

Effectiveness of AppSec Program in Identifying and Reducing Risk

*Question allowed more than one answer and as a result, percentages will add up to more than 100%

CISOs are working on **improving their AppSec program.**

# Fragmented Tools and Partial Coverage Are Leaving Security Blind Spots

The growing complexity of application security is underscored by the increasing number of tools organizations rely on to manage their security posture. Survey data highlights the extent of this challenge: 42% of organizations report using between 10 and 14 application security tools, adding to the already substantial workload of CISOs who must oversee tools for both network and application security.

As individual development teams increasingly influence tool selection, organizations fail to get a unified view of risks, further complicating policy management and strategic oversight.

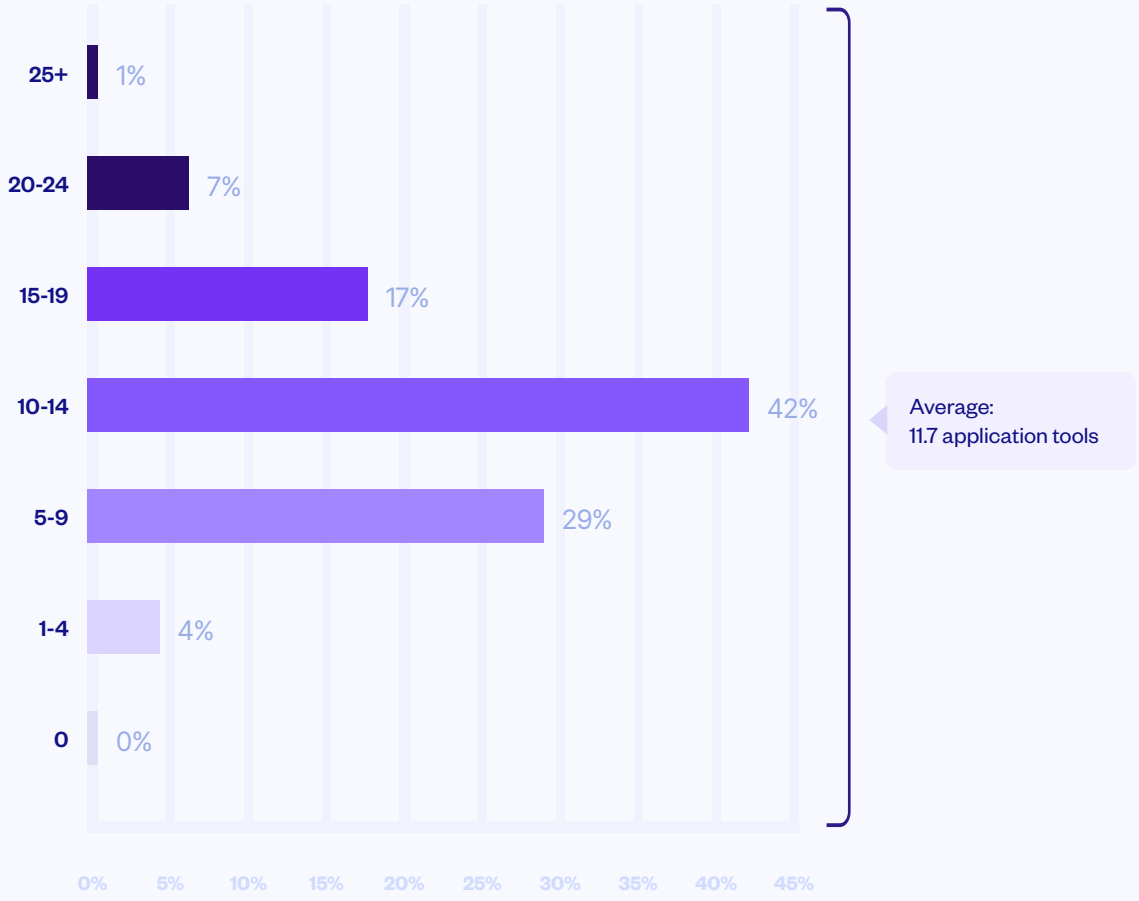



FIGURE 15

Number of Application Security Tools in Use

**CISOs are swamped with a plethora of tools,** placing an increased emphasis on vendor and platform consolidation.

This question of tool fragmentation often reflects where organizations are in their transformation journey - those successfully making the shift typically do so by establishing a centralized process for tool selection and implementation (for example, through platform engineering teams). In contrast, if individual development teams make independent decisions, tool sprawl will get out of hand, with inefficiencies and security risks following right behind. Adding to the visibility challenge, AppSec controls remain heavily focused on the early stages of the software lifecycle.

While the emphasis on early implementation aligns with the "shift-left" movement, focusing solely on stages like coding and testing leaves critical gaps in later phases, such as deployment and runtime. These gaps pose significant risks, as vulnerabilities introduced or discovered post-development often go unaddressed, leaving organizations exposed. The survey data reveals that AppSec controls are most commonly implemented during the Test (46%), Build (45%), and Code (42%) phases, reflecting the continued dominance of early-stage security practices.

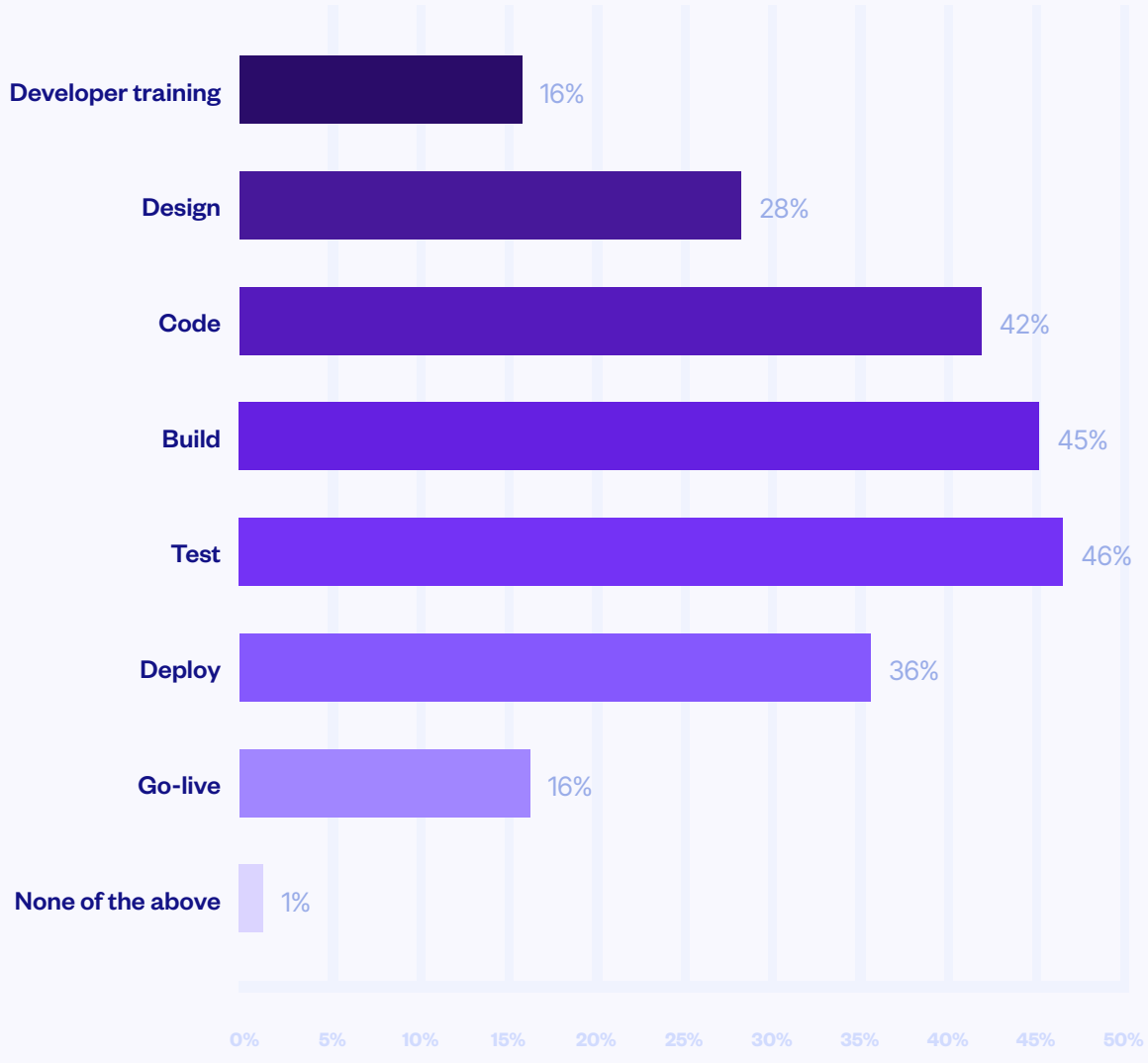



FIGURE 16

AppSec Controls Implementation by Stages of Software Development Lifecycle

*Question allowed more than one answer and as a result, percentages will add up to more than 100%

# Effective Governance in the New Era:

## What CISOs Must Prioritize in 2025 and Beyond

As the security landscape evolves, Information Security leaders must embrace a new paradigm where influence takes precedence over direct control. Based on the survey's findings, this is the roadmap for CISOs to effectively achieve their security objectives in a developer-driven world.

### Visionary Governance

CISOs must shift their focus to strategic policy management and maintaining visibility across the organization while collaborating closely with development and platform engineering teams. As budgets and decision-making increasingly shift to development teams, CISOs have the opportunity to redefine their role through governance rather than direct control. This requires prioritizing flexible security tools that seamlessly support both agile and legacy methodologies, ensuring consistent protection across all development processes. By establishing frameworks that integrate automated security controls throughout the development lifecycle, CISOs can enable comprehensive oversight while empowering teams to act decisively on security risks.

### Collaborative Influence

CISOs should opt for security solutions that are embedded directly into development workflows through continuous integration and automated controls, ensuring developers receive real-time feedback within their environments. Foster a culture of shared responsibility by empowering security champions and actively incorporating developer feedback to refine processes. Focus on integrating security seamlessly, making it an inherent part of workflows, rather than an afterthought or bolt-on addition.

### Business Alignment

Position security as a key business enabler by connecting technical challenges to tangible business outcomes. Highlight how addressing vulnerabilities, both immediate and long-term, protects revenue streams, builds customer trust, and strengthens competitive advantage. Engage with executive leadership by framing security investments in terms of their impact on growth, compliance, and reputation, ensuring alignment with organizational priorities.

### Tech-Driven Scalability

Eliminate gaps in security coverage by moving away from fragmented tools and adopting platforms capable of supporting diverse programming languages and development methodologies. Prioritize solutions that scale effectively across agile and legacy workflows while maintaining consistent security standards.

# Demographics

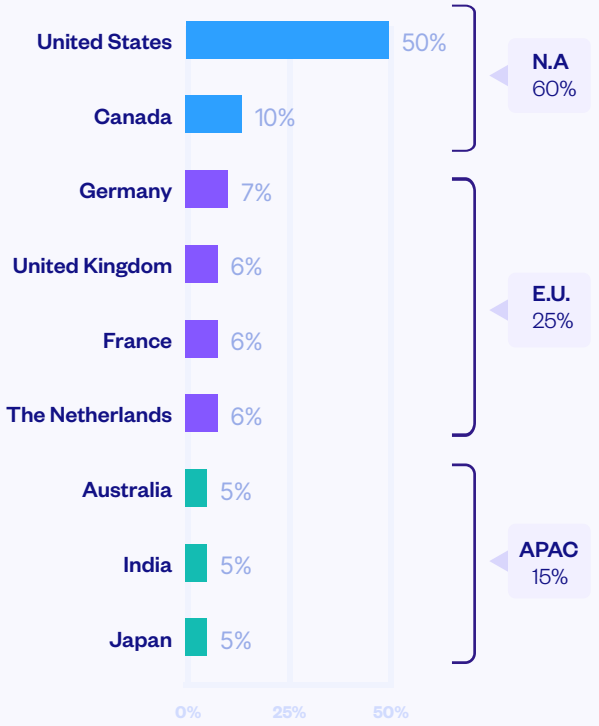



FIGURE 17
Country

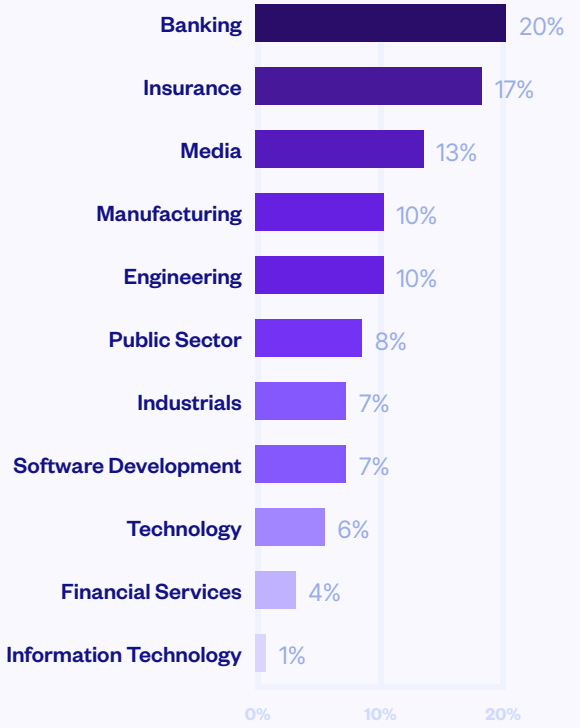



FIGURE 18
Industry

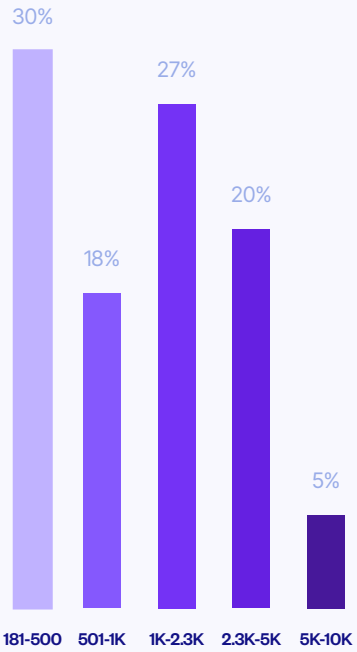



FIGURE 19
Number of Developers

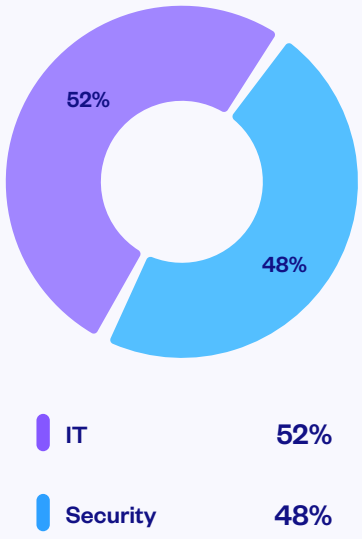



FIGURE 20
Department

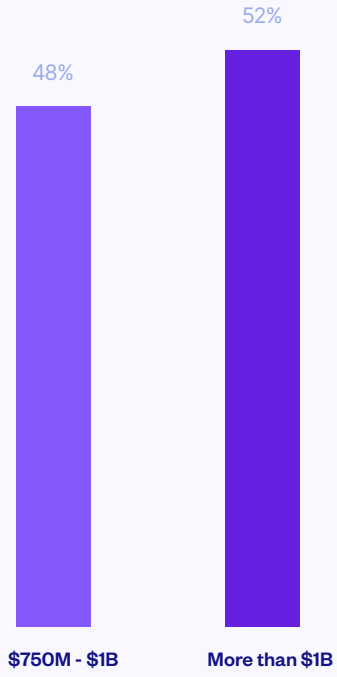



FIGURE 21
Annual Revenue

# Conclusion

As software continues to drive business innovation across industries, the responsibility for securing applications has evolved-and so must the role of the CISO.

To build a resilient, future-ready security strategy, CISOs must embrace a model of shared accountability, fostering transparency and alignment with developers and product teams. Rather than enforcing security from the top down, the focus shifts to enabling teams to integrate security seamlessly into their workflows. Developers and product teams are no longer just collaborators-they are key drivers in shaping the future of AppSec programs.

**Collaboration, alignment, and a complete view into risk**

will lead to better future security outcomes.

This new paradigm requires CISOs to lead through influence, establishing policies and KPIs that align security with development objectives. By leveraging tools like ASPM and championing a 'shift everywhere' approach, CISOs can address security gaps comprehensively, ensuring consistent protection from code to cloud.

The survey findings highlight the importance of engaging developers and development teams directly – through feedback, training, and shared ownership – to create a culture where security is embedded into every stage of development.

By aligning security initiatives with business objectives and customer expectations, CISOs can position security as a strategic enabler that drives measurable outcomes across the organization directly—through feedback, training, and shared ownership—to create a culture where security is embedded into every stage of development.

By aligning security initiatives with business objectives and customer expectations, CISOs can position security as a strategic enabler that drives measurable outcomes across the organization.


## Solidify DevSecOps, implement security at scale

and reduce business risk with Checkmarx ASPM

Learn More ↗

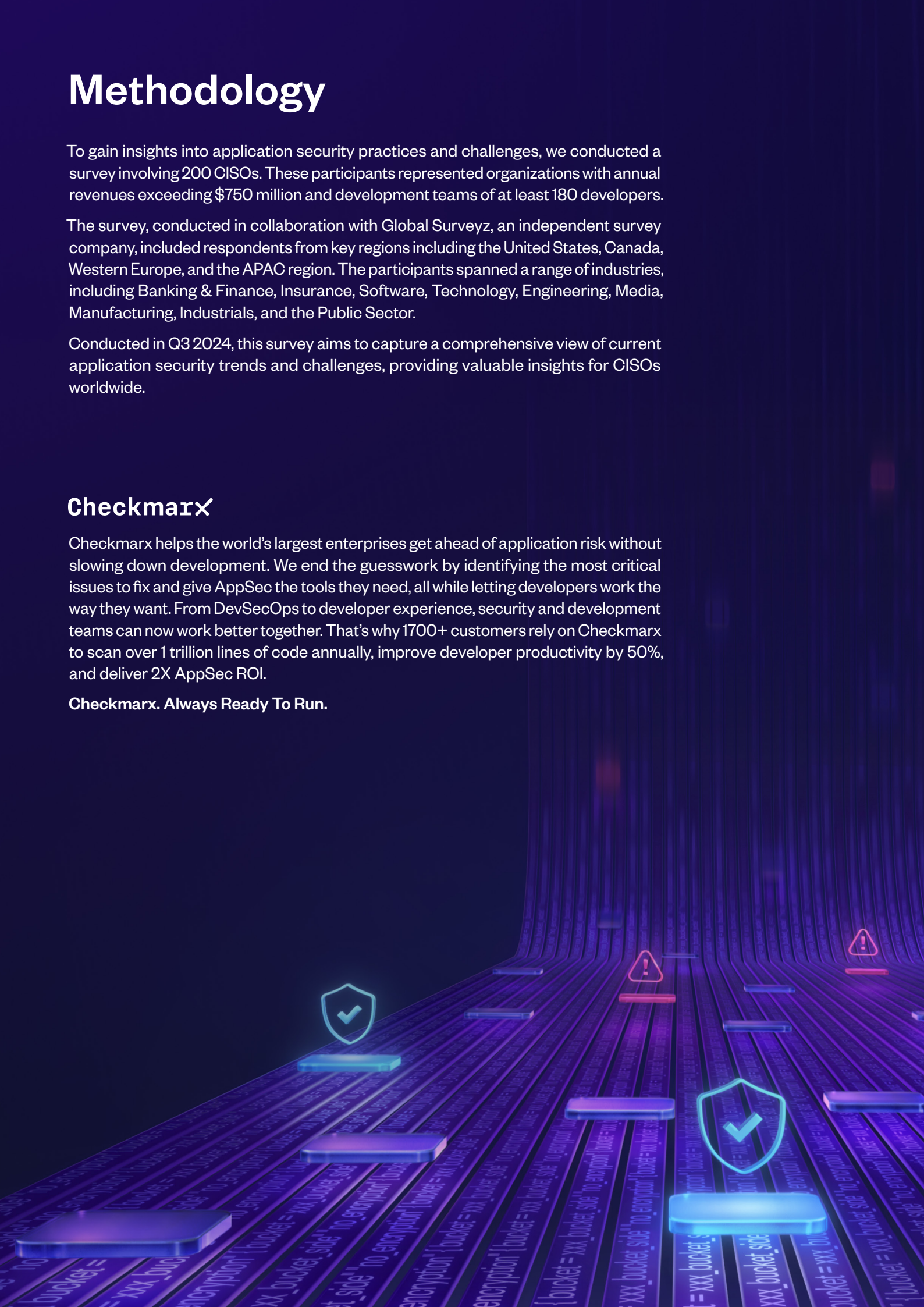
# Methodology

To gain insights into application security practices and challenges, we conducted a survey involving 200 CISOs. These participants represented organizations with annual revenues exceeding $750 million and development teams of at least 180 developers.

The survey, conducted in collaboration with Global Surveyz, an independent survey company, included respondents from key regions including the United States, Canada, Western Europe, and the APAC region. The participants spanned a range of industries, including Banking & Finance, Insurance, Software, Technology, Engineering, Media, Manufacturing, Industrials, and the Public Sector.

Conducted in Q3 2024, this survey aims to capture a comprehensive view of current application security trends and challenges, providing valuable insights for CISOs worldwide.

## Checkmarx

Checkmarx helps the world's largest enterprises get ahead of application risk without slowing down development. We end the guesswork by identifying the most critical issues to fix and give AppSec the tools they need, all while letting developers work the way they want. From DevSecOps to developer experience, security and development teams can now work better together. That's why 1700+ customers rely on Checkmarx to scan over 1 trillion lines of code annually, improve developer productivity by 50%, and deliver 2X AppSec ROI.

**Checkmarx. Always Ready To Run.**