



RESEARCH REPORT

The **Shift Left** Adoption Benchmark Report





RESEARCH REPORT

The Shift Left Adoption Benchmark Report

Table of Contents

How Are Companies Implementing Shift Left? And How Do You Stack Up?	3
Inside Our Research	4
KEY FINDINGS:	
How Shift Left is Being Implemented Today	5
THE STATE OF SHIFT LEFT:	
Adoption, Tools, and Challenges	6
THE DEVELOPER-SECURITY CONFLICT:	
A CISO's Dilemma	7
THE CORE CHALLENGE:	
Developer Resistance vs. Security Enthusiasm	8
SECURITY CHAMPIONS:	
Are They Making an Impact?	9
How Do You Stack Up?	10

How Are Companies Implementing **Shift Left**?

And How Do You Stack Up?

"Shift Left" has been a buzzword in application security for years, promising a proactive approach to catching vulnerabilities earlier in the software development lifecycle (SDLC). But how is it actually being implemented today? Are companies seeing the expected benefits, or are there major roadblocks slowing down progress?

Our research, based on responses from **250 security and engineering professionals**, provides a data-driven look at how organizations are implementing Shift Left, the challenges they face, and the impact on security posture. This benchmark report allows you to compare your own Shift Left journey with industry peers and answer the question:



How do you stack up?

Test

Release

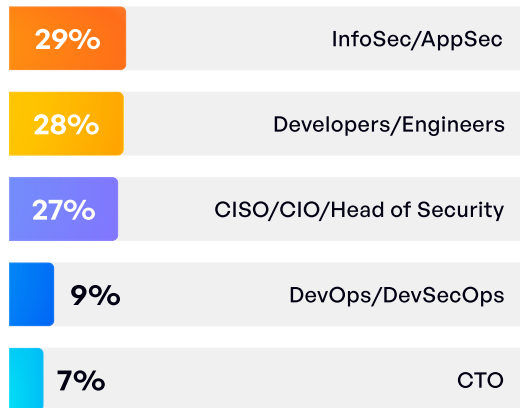
Inside Our Research

Study Methodology & Audience Breakdown

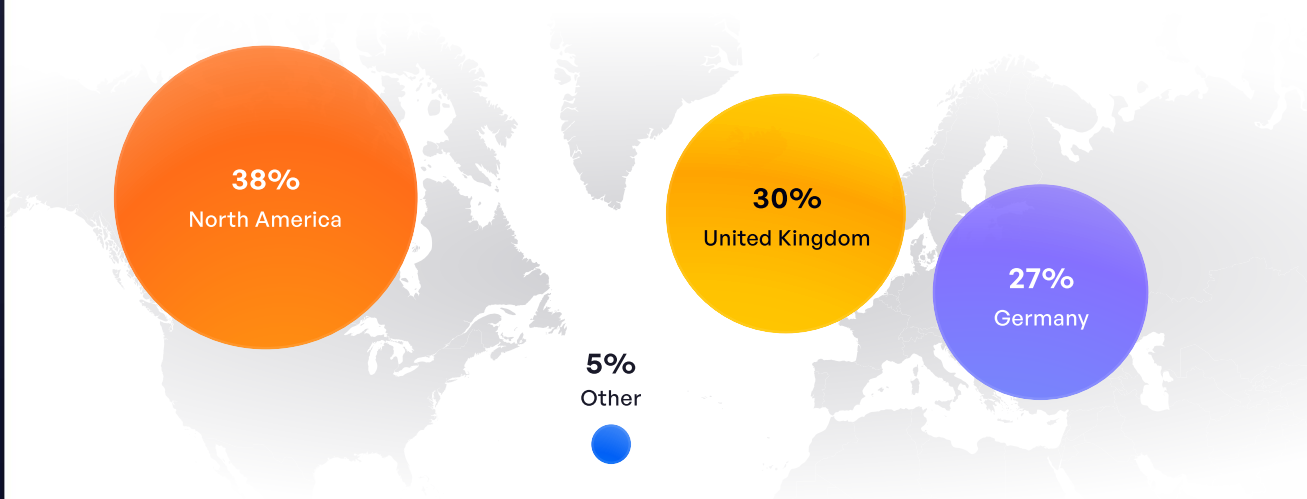
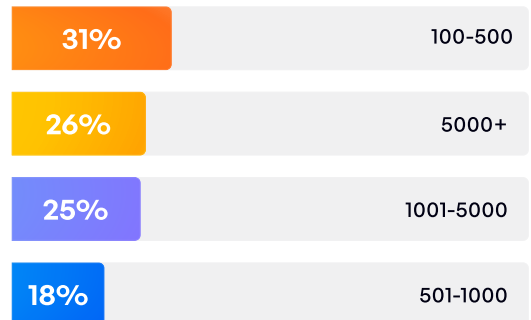
This research is based on a survey conducted among **250 professionals** across various industries, functions, and company sizes. The participants were specifically from technical and security-oriented roles.



ROLES IN THE ORGANIZATION



NUMBER OF EMPLOYEES



This diverse respondent pool ensures a well-rounded representation of Shift Left adoption trends across different organizational contexts.

KEY FINDINGS:

How Shift Left is Being Implemented Today

1

Shift Left adoption is widespread, but execution and enforcement is inconsistent

47% of organizations claim they have implemented Shift Left strategies, yet many still struggle with execution gaps and security inefficiencies.

2

False positives are the #1 challenge

High rates of false positives create alert fatigue and wasted cycles for security teams and developers.

3

Companies who still implement shift left are Stuck at WIP

Top issue for those companies who are still implementing is integration issues. Shift left tools and processes are a major roadblock to shift left success.

4

Shift Left overburdens developers

One of the top frustrations among developers is the overwhelming volume of vulnerabilities they must address, even beyond false positives.

5

Security Champions are a major enabler

67% of respondents report having Security Champions within their Engineering or QA teams, but adoption varies—75% of European companies have security champions, compared to just 50% in U.S. organizations.

Adoption, Tools, and Challenges

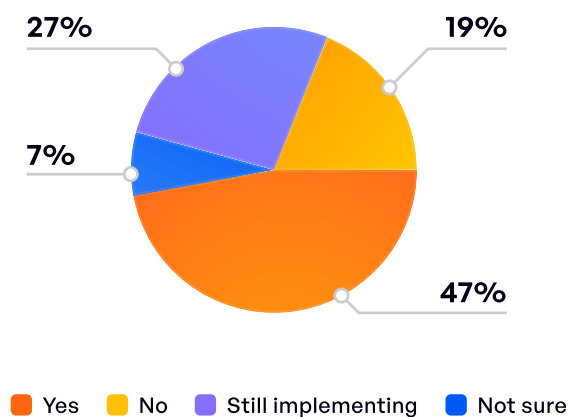
While many companies claim they've implemented Shift Left, our research shows that a significant portion are either struggling with it or have no plans to implement it at all. While 97% of respondents implement tools to enforce a shift left strategy, there's a clear gap between intention and execution, with a variety of factors hindering true adoption.

Regional trends also play a role. Our data reveals that European organizations are ahead in adopting Shift Left compared to the U.S.—with Germany and the UK reaching 52% implementation, while the U.S. lags at 42%. The future outlook follows a similar trend: 36% of German respondents and 25% of UK respondents plan to implement Shift Left soon, compared to only 20% in the U.S.

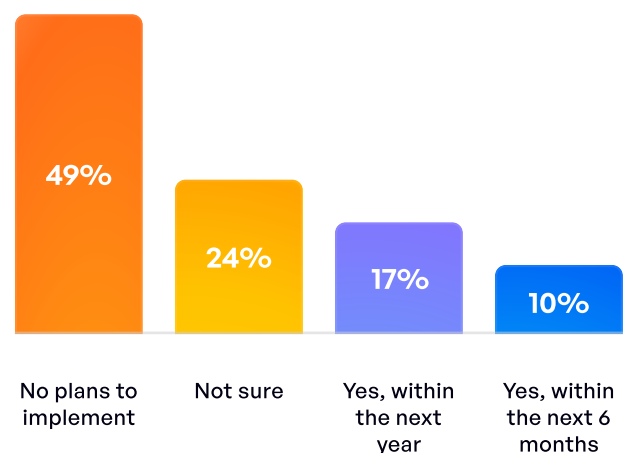
Many Are Implementing, But Many Are Not

- While 47% of organizations claim to have fully implemented Shift Left, a large portion are still in the process or have only partially implemented it.
- Of those who haven't implemented Shift Left, half of them have no plans to do so at all, showing a stark divide in adoption rates.
- **Europeans lead in Shift Left adoption** – Respondents from Germany and the UK show a higher Shift Left adoption rate (52%) compared to the U.S. (42%). Furthermore, 36% of German organizations plan to implement Shift Left soon, compared to only 20% in the U.S.

Q2 Has your organization implemented a 'shift left' approach in its software development lifecycle?



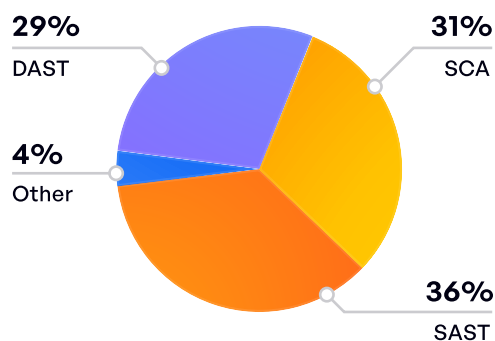
Q3 If your organization has not implemented a 'shift left' approach, do you plan to do so in the future?



“Shift left” teams implement “Shift left” tools

- For most companies, Shifting left means checking the box of implementing tools as our study finds 97% have implemented either SAST, DAST, SCA, or other tools.
- While SAST tools are the most adopted with 36% of respondents claiming to use it, SCA is fairly close with 31% and DAST with 29%.
- Among the top challenges reported by respondents regarding Shift Left, the high rate of false positives stands out and the leading issue.
- The second leading issue is “integration issues” which really applies to the struggle usually to implement tools in shift left mode. Shift right is easier since it doesn’t require extensive coordination between multiple teams, whereas Shift Left demands a collaborative effort across development, security, and testing teams.
- The third top issue adds frustration to the dev team, talking about how overloaded they are with vulnerabilities. Even if it’s not false positives, it’s still hard to keep up with the amount of vulnerabilities they ought to fix, gearing us up to the next section.

Q5 Which tools were implemented as part of the 'shift left' approach?



Q6 Which issues do you experience when it comes to the 'shift left' approach?

PLACE	ISSUE	PERCENT	
1	High rate of false positives	35%	The leading issue, overwhelming security teams and developers.
2	Integration issues	31%	A significant pain point, making it difficult to fit security tools into existing workflows.
3	Overloaded with vulnerabilities	25%	Even when vulnerabilities aren't false positives, developers report struggling to keep up with the volume of security issues.
4	None of the above	8%	
5	Other	1%	

THE CORE CHALLENGE:

Developer Resistance vs. Security Enthusiasm

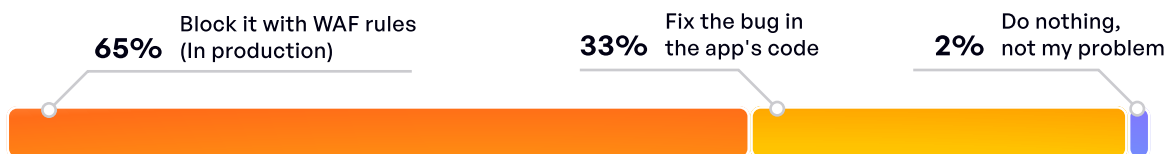
A significant friction point exists between **developers and security teams** when it comes to fixing security vulnerabilities. Developers often prioritize feature development and view security tasks as an added burden, while security professionals advocate for remediation.

The results highlight a clear **disconnect between developers and security teams**, which leads to delays and inefficiencies in security improvements.

65% of respondents prefer to fix bugs in the app's code, rather than block with WAF rules in production. Of course, it makes sense, no one wants to be that bad guy.

But looking closer to the results, when asking CISOs and security professionals this question, 42% prefer to block with WAF rules.

Q8 If you discovered an internet-facing security flaw in your application, would you rather...



SECURITY CHAMPIONS:

Are They Making an Impact?

Security Champions programs have become a key strategy for embedding security into engineering teams. Our research found:

- **67% of organizations have Security Champions** in their Engineering or QA teams.
- **Europe leads the way**, with **75% of European companies** adopting Security Champions, compared to **50% in the U.S.**
- Organizations with Security Champions report better adoption of security testing within their SDLC and more proactive security collaboration.

Does your organization have a Security Champions program? How do you compare?

Q7 Do you have Security Champions within the Engineering/QA departments?



Given the fact that so many organizations train security champions, making the **embedding of security testing in the testing process much easier**. Organizations can **crush security bugs earlier, without relying on unmotivated developers**. This approach could improve security posture and reduce friction between teams.

How Do You Stack Up?

This report provides a benchmark of how companies are implementing Shift Left today—both the successes and the struggles. Whether your organization has fully adopted Shift Left or is still figuring out the best way forward, the insights from this research can help you evaluate your current strategy.

Are you using the same tools as your peers?

Are you experiencing the same challenges?



Are you ahead or behind in adoption?

To address the challenges of Shift Left adoption, organizations should consider the following strategies:

- **Embed Security into Testing:** Relying solely on developers isn't working. Security testing should be part of the QA process.
- **Improve Collaboration Between Teams:** Bridge the communication gap between developers, security teams, and testers.
- **Automate Security Testing:** Reduce friction by integrating automated security testing tools within CI/CD pipelines.

Integrate **Shift Left Security**
Where It Works

With Pynt's Proactive Testing

Get a Demo >