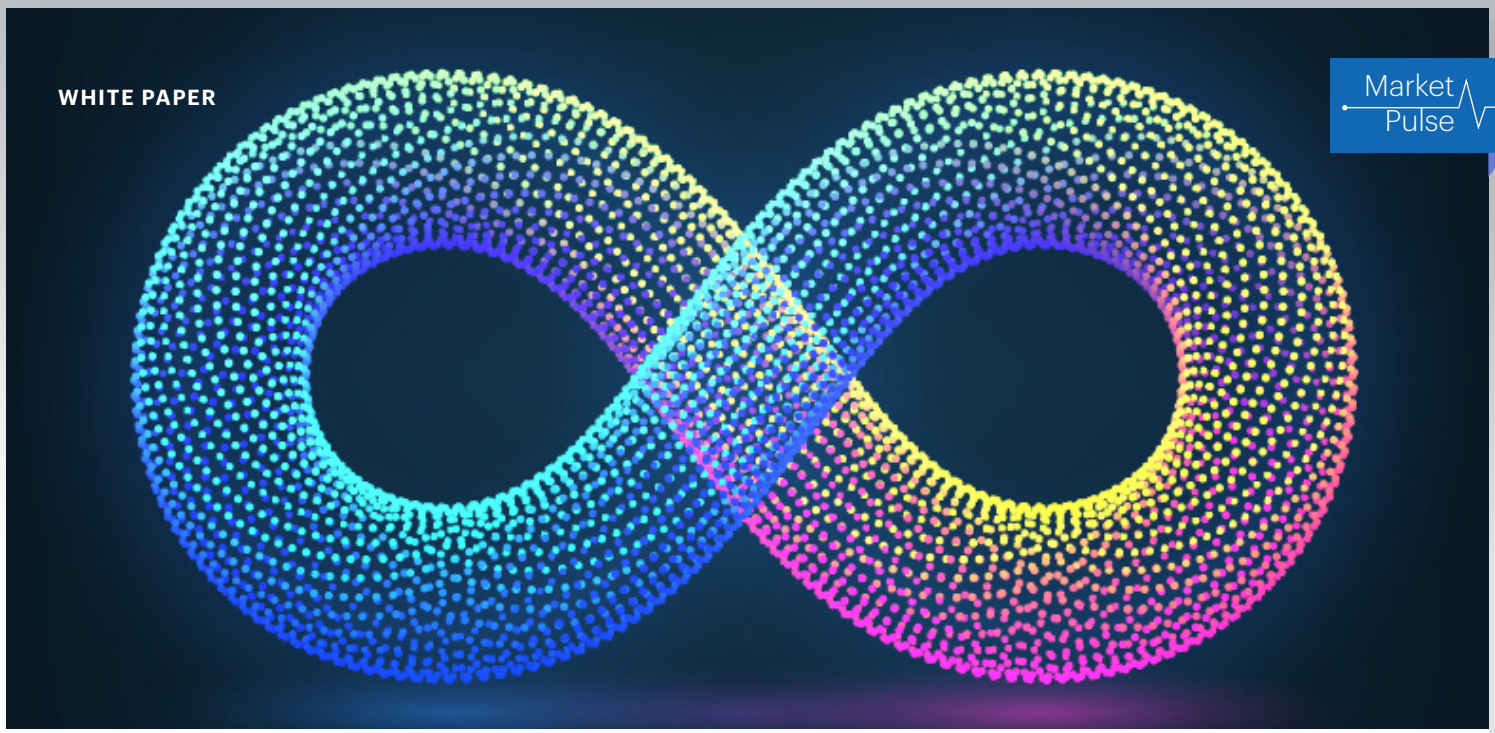
WHITE PAPER

Market Pulse



THE GREAT DISCONNECT: **Why DevSecOps has failed to fulfill its promise**

IT and security leaders recognize the critical need to integrate security into development. However, they're struggling to execute, according to IDG research. That's why a best-in-class approach—one that empowers the development team to take ownership—gives organizations a clear path to delivering secure code.

THE DEVSECOPS MODEL IS SUPPOSED TO HELP IMPROVE APPLICATION SECURITY. Nearly all respondents (98%) to a recent IDG research survey said it's "highly important" to integrate security across all stages of software development. But clearly, that isn't happening.

There is a fundamental disconnect between the integration of devops and secops teams and the processes currently in use. There are still too many silos and not enough developer engagement with security.

Only 15% of respondents said they "always" integrate security throughout the development life cycle. This gap in process opens the door to releasing vulnerable code. For example, 58% of respondents admit that their development teams have released apps that had security vulnerabilities, and 45% of these organizations subsequently reported a breach.

The IDG Market Pulse study, sponsored by Wabbi, focused on the integration of development and security, and the benefits of continuous security. Participants included 148 IT and security leaders, software/application development managers, and directors across industries at companies of various sizes. The survey examined priorities and trends around integrating security throughout the software development life cycle (SDLC).

WABBI

SPONSORED CONTENT

CSO

The disconnect creates challenges for the business

Organizations are still a long way from realizing the benefits they expect from devsecops. In many cases, their current approach doesn't go far enough to eliminate the siloed nature of development, which exacerbates the gap.

Disconnected development and security teams create other problems, such as project delays and bottlenecks. For example, 47% of respondents said the lack of application security process integration with development creates delays to a great extent, while another 53% said it does so to some extent. Another related issue: 72% of respondents cited poor collaboration/lack of feedback as a reason for stalled projects. Of significance, 88% said it is highly challenging for development and project teams to gain access to accurate, relevant security and compliance information. Only 28% of development teams are receiving application security requirements during the planning stages of the SDLC. This is concerning because "bolting-on" security after development is underway creates potential for vulnerabilities in code.

The results of this disconnect are tangible. When security processes are not integrated throughout the SDLC, organizations experienced project delays, financial losses, and compromised brand reputation (see Figure 1).

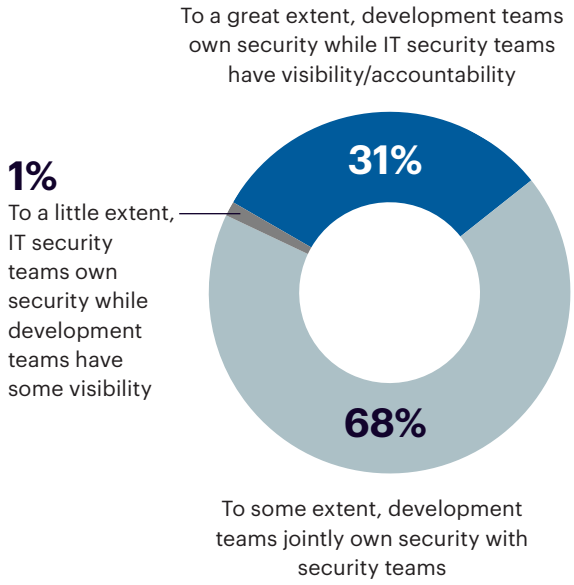
FIGURE 1. **TOP 3 IMPACTS WHEN SECURITY ISN'T INTEGRATED INTO SDLC**

Source: IDG

The path to continuous security

To gain the promise of devsecops and push through the disconnect, security must be integrated right from the beginning of, and throughout, the SDLC. This approach is known as "continuous security." It is the practice of automating and orchestrating the deployment of application security processes to enable dynamic management of security requirements in the SDLC. Code is always ready to ship in compliance with the security program, without delivery delays.

FIGURE 2. **EXTENT TO WHICH DEV TEAMS ARE EMPOWERED TO TAKE OWNERSHIP OF APP SECURITY**



Source: IDG

The IDG survey found that 31% of enterprises are starting to follow the concept of continuous security and are reaping the benefits. These best-in-class organizations have empowered their development teams to take ownership of security by integrating it into and throughout the SDLC (see Figure 2). They are experiencing greater alignment with business objectives and the issues facing modern IT.

For example, the best-in-class respondents reported substantial improvements in security:

	Best in Class	All Others
Have released apps with vulnerabilities	**50%**	**73%**
Have been provided with security requirements and given opportunities for feedback in the planning stage of the SDLC	**48%**	**16%**
Feedback sharing processes between development and security teams are fully automated	**49%**	**25%**

Automating processes across the development life cycle is a natural part of continuous security. Automation makes it possible to act at the speed necessary to meet project timelines and deliver new code as the organization demands it.

Although only 12% reported that their organizations have already adopted a continuous security strategy, the majority plan to do so within the next 12 months (see Figure 3).

The benefits of continuous security

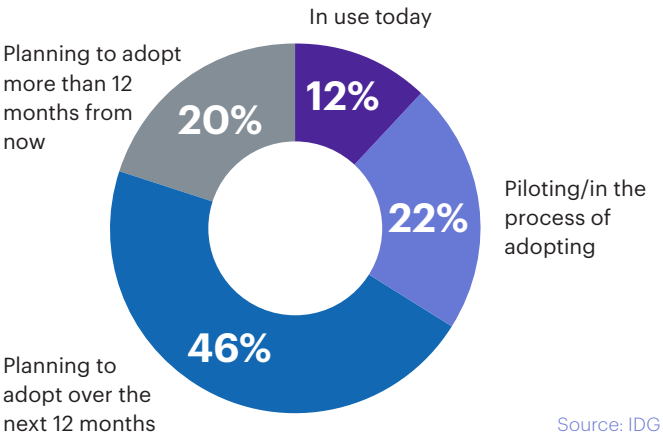
Respondents said that following a continuous security approach will result in more secure code, fewer breaches, less economic loss, reduced delivery delays, and shorter and fewer business interruptions. This strategy meets IT's needs as well as the needs of executive management.

There is also business value to be gained from integrating security throughout the SDLC, including improved productivity (70%), cost savings (67%), and reduced risk of breaches (67%) (see Figure 4).

The future: The adoption and use of continuous security

Continuous security solves many existing problems and puts development teams in the position to meet future demands as they embark on the journey to digitization. The ability to quickly and securely deliver apps that power digital business processes is a competitive advantage. This development model fundamentally changes the game.

FIGURE 3. **ADOPTION RATES OF CONTINUOUS SECURITY**

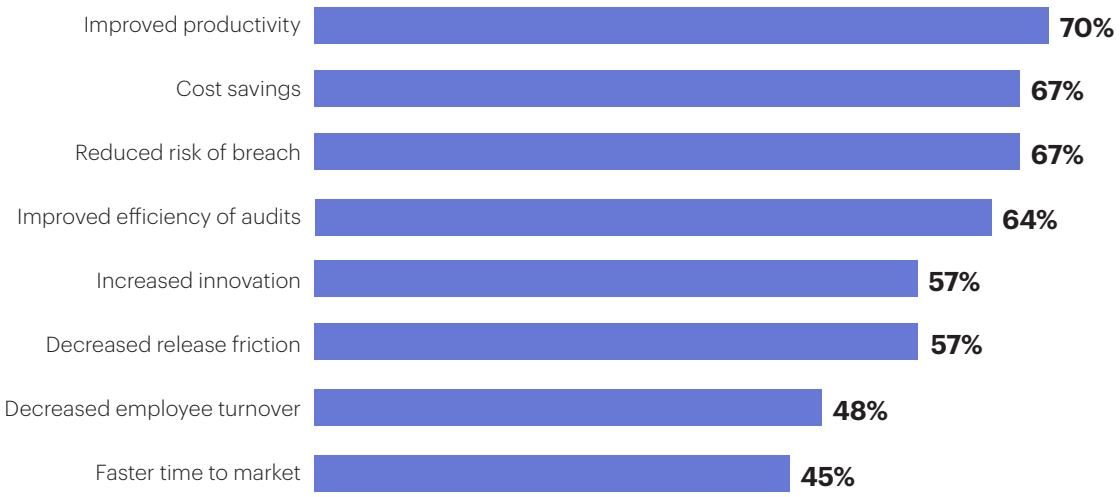


Source: IDG

Moving to continuous security enables teams to overcome key issues while meeting strategic requirements. Today, many organizations typically struggle with trying to balance three competing demands: mitigating known security vulnerabilities (66%); confirming that code meets necessary functionality requirements (61%); and accessing the security policies that are germane to a given development project (60%).

When an organization implements continuous security, development teams can effectively balance and simplify all three of these issues. On the flip side, incorporating security processes further into the SDLC is more difficult and time-consuming, causing additional work in the form of quality assurance and testing.

FIGURE 4. **BENEFITS OF INTEGRATING SECURITY INTO SOFTWARE DEVELOPMENT LIFE CYCLES**



Source: IDG

Processes like these should be automated at the planning stage so that developers have access to security policies that are in context with their work. They need security policies for the specific code modules currently being written, as well as across all stages of the development process to ensure updates occur in real-time.

Continuous security is the ideal way to remove common roadblocks that arise with manual approaches. It's not just about efficiency—it's about accuracy, consistency, the mitigation of security risks, and the ability to scale.

For the 89% of survey respondents who have just started or are interested in adopting continuous security, their path should include an automation platform. The right solution integrates with existing development workflows to empower development teams to own application security processes.

Continuous security solves many existing problems and puts development teams in the position to meet future demands as they embark on the journey to digitization.

For example, it automates and orchestrates security policies to ensure consistency and repeatability, while also making it easy to scale and adapt.

A continuous security platform allows organizations to take a significant step forward on the path to continuous security. Respondents cited several aspects of such a platform as highly valuable:

- **98%:** Dynamic management and deployment of security requirements
- **98%:** Creation and management of a clear audit trail
- **96%:** Project-level prioritization of vulnerabilities
- **96%:** Orchestration of security processes
- **94%:** Consolidation of security results across tools

Summary

Automation is essential to move at speed and scale. However, there is a disconnect between the need for automation and its relatively low adoption rate into devsecops processes. For example, only 38% of the respondents have automated the feedback sharing process between development and security. The amount of interaction between the two groups and the need to track and document it cry out for automation.

Continuous security is a catalyst for automated collaboration and the elimination of manual processes that create vulnerabilities and other roadblocks to innovation. A platform that pulls together devops and secops workflows throughout the SDLC is a major step in the right direction toward removing the great disconnect around security integration.