

# Wabbi Announces Findings of Annual Continuous Security Report

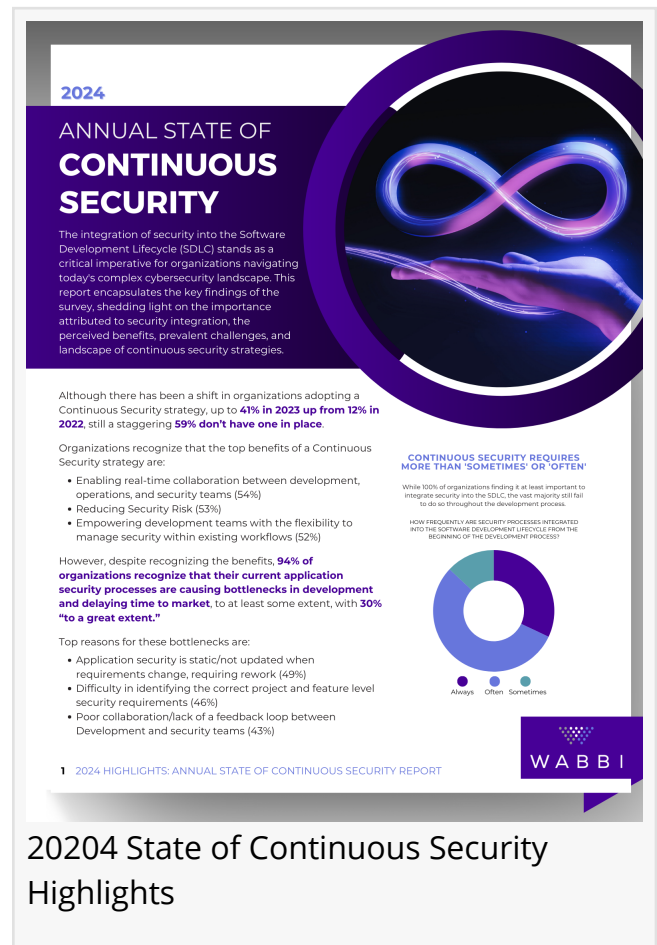
*Progress in Integrating Security into Software Development, Progress in Adoption, but Bottlenecks Persist*

BOSTON, MA, USA, May 6, 2024 /EINPresswire.com/ -- [Wabbi](#), the leading [application security posture management](#) platform, today announced the findings of its annual report on the state of [continuous security](#). The study surveyed over 100 security and development leaders at mid-market and enterprise organizations. The report reveals that while there has been significant growth in organizations adopting a Continuous Security strategy, many are still struggling with integrating security into the software development lifecycle (SDLC) due to persistent bottlenecks that hinder efficient development and security processes.

"While we've witnessed a significant shift towards Continuous Security adoption, with a remarkable 242% increase since our last report, this year's findings highlight the pressing need to address bottlenecks and inefficiencies that impede organizations from fully realizing the benefits of this approach," said Brittany Greenfield, CEO & Founder of Wabbi. "Closing the gap between security and development requires proactive collaboration, streamlined access to relevant security information, and a leveraging technology to break down silos between teams."

Key findings from the report include:

Organizations recognize the advantages of a Continuous Security strategy, with 54% emphasizing real-time collaboration between development, operations, and security teams as a primary benefit. Reducing security risk (53%) and empowering development teams with the flexibility to manage security within existing workflows (52%) are also recognized as valuable advantages.



**2024**  
**ANNUAL STATE OF CONTINUOUS SECURITY**

The integration of security into the Software Development Lifecycle (SDLC) stands as a critical imperative for organizations navigating today's complex cybersecurity landscape. This report encapsulates the key findings of the survey, shedding light on the importance attributed to security integration, the perceived benefits, prevalent challenges, and landscape of continuous security strategies.

Although there has been a shift in organizations adopting a Continuous Security strategy, up to **41% in 2023 up from 12% in 2022**, still a staggering **59% don't have one in place**.

Organizations recognize that the top benefits of a Continuous Security strategy are:

- Enabling real-time collaboration between development, operations, and security teams (54%)
- Reducing Security Risk (53%)
- Empowering development teams with the flexibility to manage security within existing workflows (52%)

However, despite recognizing the benefits, **94% of organizations recognize that their current application security processes are causing bottlenecks in development and delaying time to market**, to at least some extent, with **30% "to a great extent."**

Top reasons for these bottlenecks are:

- Application security is static/not updated when requirements change, requiring rework (49%)
- Difficulty in identifying the correct project and feature level security requirements (46%)
- Poor collaboration/lack of a feedback loop between Development and security teams (43%)

**CONTINUOUS SECURITY REQUIRES MORE THAN 'SOMETIMES' OR 'OFTEN'**

While 100% of organizations finding it at least important to integrate security into the SDLC, the vast majority still fail to do so throughout the development process.

HOW FREQUENTLY ARE SECURITY PROCESSES INTEGRATED INTO THE SOFTWARE DEVELOPMENT LIFECYCLE FROM THE BEGINNING OF THE DEVELOPMENT PROCESS?

Always Often Sometimes

**1 2024 HIGHLIGHTS: ANNUAL STATE OF CONTINUOUS SECURITY REPORT**

**WABBI**

**2024 State of Continuous Security Highlights**

Despite these benefits, and while 97% of respondents assert the importance of integrating security into the SDLC, only 32% consistently integrate security from the outset of the development process. Consequently, access to accurate and relevant information on application-specific security and compliance requirements remains a challenge, with 56% reporting difficulties in obtaining such information.

Consequently, 94% of organizations recognize that their current application security processes are causing bottlenecks in development and delaying time to market, to at least some extent, with 30% “to a great extent.” These bottlenecks are a major pain point for organizations and can prevent them from delivering secure software quickly. Consequently, 62% of organizations have shipped vulnerable code in the last year.

The primary reasons for these bottlenecks include the dynamic nature of application security, requiring rework when requirements change (49%), difficulty in identifying the appropriate security requirements at the project and feature levels (46%), and poor collaboration or lack of feedback loops between development and security teams (43%).

“

Closing the gap between security and development requires proactive collaboration, streamlined access to relevant security information, and a leveraging technology to break down silos between teams.”

*Brittany Greenfield*

Greenfield added that, “By embracing continuous security practices and eliminating bottlenecks, organizations can not only enhance their security posture but also optimize their development processes, shorten time to market, and drive overall business agility. We’re encouraged by the progress that organizations are making in integrating security into the SDLC, however, the results of our report also show that there are still some challenges that need to be addressed.”

The State of Continuous Security is a valuable resource for organizations that are looking to improve their application security posture. The report provides insights into the latest trends in Continuous Security. Wabbi completes this study annually as part of its commitment to empowering organizations with the tools and expertise needed to achieve real-time security insights and collaboration, facilitating a secure and efficient software development journey.



For more information on the findings and recommendations from the report, please visit

<https://www.wabbi.com/continuous-security-report>

## About Wabbi

Wabbi is the industry's leading Application Security Posture Management Platform. A 2021 RSA Innovation Sandbox Finalist, Wabbi's Continuous Security solution orchestrates and correlates all components of an application security program to bridge the gap between security and development to meet the ever-escalating demands of deploying application security in the SDLC.

From policy deployment, vulnerability management, and secure release management, Wabbi's Continuous Security platform allows organizations to confidently ship code that meets their application-specific security standards, without sacrificing agility or velocity. By orchestrating each enterprise's unique application security program, security teams capture centralized, automated governance, while development teams are empowered to manage security as part of their day-to-day workflows, unifying processes between Development, Security & Operations teams.

With Wabbi, companies keep code shipping – securely.

Learn More at <https://www.wabbi.com>

Julie Boyer

Wabbi

+1 617-963-0186

[email us here](#)

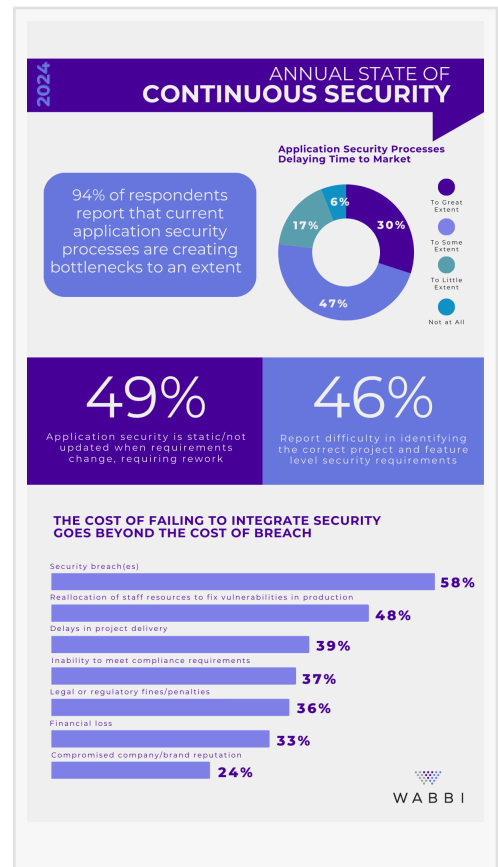
Visit us on social media:

[LinkedIn](#)

[YouTube](#)

[Twitter](#)

[Instagram](#)



This press release can be viewed online at: <https://www.einpresswire.com/article/707494003>

EIN Presswire's priority is source transparency. We do not allow opaque clients, and our editors try to be careful about weeding out false and misleading content. As a user, if you see something we have missed, please do bring it to our attention. Your help is welcome. EIN Presswire, Everyone's Internet News Presswire™, tries to define some of the boundaries that are reasonable

in today's world. Please see our Editorial Guidelines for more information.

© 1995-2024 Newsmatics Inc. All Right Reserved.