THE GREAT DISCONNECT

Annual State of Continuous Security Report

IDG surveyed IT and security leaders, across industries to examine priorities and trends around integrating security throughout the software development lifecycle (SDLC).

You Say Integrating Security is Important, So Why Don't You Do It?

Continuous Security

/kənˈtinyo͞oəs /səˈkyo͝orədē/

Noun

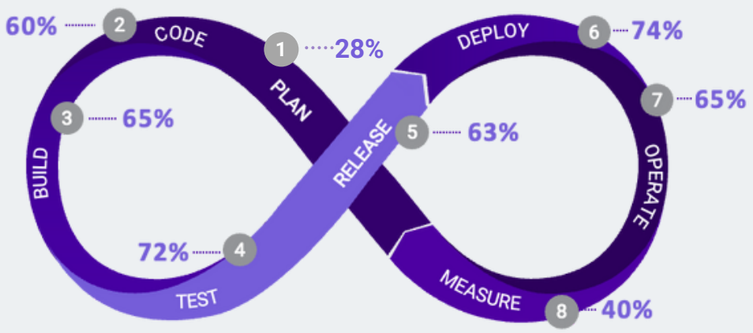
The practice of automating and orchestrating the deployment of application security processes to enable dynamic management of security requirements in the SDLC in response to internal and external changes, so code is always ready to ship in compliance with the security program without creating delivery delays.

98% placed high importance on integrating security throughout the development lifecycle

15% reported that security was always integrated from the beginning of the development lifecycle.

Just one-quarter indicated development teams receive application security requirements during the planning stage of the development lifecycle.

Stages of SDLC Where Dev Teams Were Offered Security Reqs/Opportunities for Feedback



88% Report it is very difficult to access accurate, relevant AppSec and compliance information.

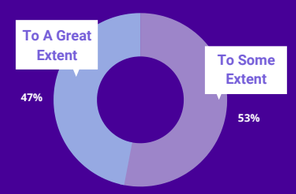
Report that it's most difficult to access to prioritization of known security vulnerabilities **66%**

61% Have difficulty understanding if code meets the necessary security requirements

Struggle to access information about the specific security policies that impact a given project **60%**

What's The Cost?

Application Security Process is Delaying Time to Market



100% of respondents indicate current application security processes are creating bottlenecks to at least some extent.

72%

72% report poor collaboration between DevOps and security teams in development projects

71%

71% cite difficulties identifying the correct bottleneck on project/feature level security

Failure To Not Integrate Security Is About More Than Just Breach Risk

Delays in Project Delivery	72%
Financial Loss	63%
Compromised Reputation	57%
Reallocation To Fix Issues	47%
Inability To Meet Compliance Reqs.	47%
Security Breach(es)	45%
Legal or Regulatory Fines	41%

What You're Missing Out On...

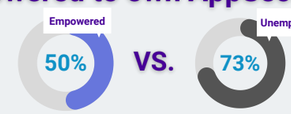
Integrating Security isn't Just About Better Security, It's About Better Business Outcomes

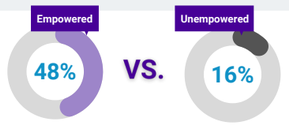
45%	Faster Time To Market
48%	Decreased Turnover
57%	Decrease Release Friction
57%	Increased Innovation
64%	Improved Efficiency of Audits
67%	Reduced Risk of Breach
67%	Cost Savings
70%	Improved Productivity

Take Ownership Of Your Security

When DevOps teams were empowered to own AppSec...

Respondents were less likely to report their organizations had released applications with security vulnerabilities in the past 12 months

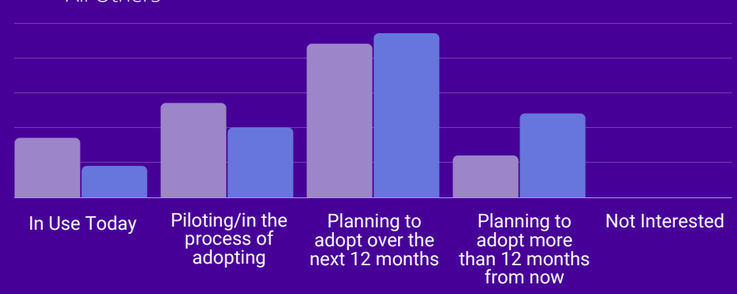




Dev teams were more likely to have been provided with security reqs and given opportunities for feedback in the planning stage .

Respondents more often reported feedback sharing processes between development and security teams being fully automated

Organizations That Have Empowered Dev Teams To Own Security Are More Likely To Have Adopted A Continuous Security Strategies



Continuous Security Is The Future

Most Attractive Potential Benefits of Continuous Security Strategy

73%	Empowering development teams with the flexibility to manage security within existing workflows
72%	Enabling real-time collaboration between development, operations, and security teams
70%	Reducing security risk
61%	Dynamic management of security requirements in line with business needs and concerns
55%	Removing bottlenecks
50%	Eliminating manual security processes/increasing automation
49%	Improving time to market
45%	Centralizing security governance
1%	Other

WABBI

Website: https://wabbisoft.com/
Email: info@wabbisoft.com

@Wabbi @HiWabbi