MARKETPULSE RESEARCH:

Benefits of Continuous Security

On Behalf of Wabbi

January 2022
Sample

Field Work
This survey was fielded in the U.S. between December 10, 2021 and December 22, 2021

Total Respondents
148 qualified

Method and Objectives

Data collection
Online questionnaire

Length
18 questions (excluding screeners and demographics)

Audience:
Respondents were qualified as follows:
- Manager or above with responsibility and/or oversight for application development
- Employed at a company with 500 or more employees
- Employed in one of the following vertical industries: Financial services, Healthcare, Manufacturing, Media/Entertainment, Pharmaceutical, Retail, Technology, or Telecom products and services

Research objectives
In this survey we seek to gauge the priority placed on integrating security throughout the software development lifecycle. We look at current levels of security integration and automation within the SDLC, the frequency and impact of releasing applications with security vulnerabilities, the extent to which security creates bottlenecks in application development processes, and the level of communication and information sharing between DevOps and security teams.

Lastly, we examine adoption and perceived benefits of continuous security strategy and explore the value of automating application security.
Respondent Profile

Job Title

<table>
<thead>
<tr>
<th>Role</th>
<th>%</th>
</tr>
</thead>
<tbody>
<tr>
<td>CIO</td>
<td>14%</td>
</tr>
<tr>
<td>CTO</td>
<td>3%</td>
</tr>
<tr>
<td>VP/SVP/EVP of IT/IT Operations</td>
<td>10%</td>
</tr>
<tr>
<td>Director of IT/IT Operations</td>
<td>26%</td>
</tr>
<tr>
<td>VP/SVP/EVP of Application/Software Development</td>
<td>1%</td>
</tr>
<tr>
<td>Application/Software Development Director</td>
<td>12%</td>
</tr>
<tr>
<td>Application/Software Development Manager</td>
<td>33%</td>
</tr>
<tr>
<td>Software Engineering Manager</td>
<td>1%</td>
</tr>
</tbody>
</table>

Number of Employees

<table>
<thead>
<tr>
<th>Employee Range</th>
<th>%</th>
</tr>
</thead>
<tbody>
<tr>
<td>2,500 - 4,999</td>
<td>17%</td>
</tr>
<tr>
<td>5,000 - 7,499</td>
<td>17%</td>
</tr>
<tr>
<td>7,500 - 9,999</td>
<td>22%</td>
</tr>
<tr>
<td>10,000 - 19,999</td>
<td>7%</td>
</tr>
<tr>
<td>20,000 or more</td>
<td>18%</td>
</tr>
<tr>
<td>1,000 - 2,499</td>
<td>15%</td>
</tr>
</tbody>
</table>

Primary Industry

- Financial services (banking, insurance, accounting, tax, etc.): 25%
- Manufacturing, Production, Distribution: 21%
- Technology (software): 18%
- Retail: 17%
- Healthcare: 11%
- Telecommunications products and services: 4%
- Media, Entertainment, Content: 3%
Summary of Findings

- Virtually all respondents (98%) place high importance on integrating security throughout the development lifecycle (30% rate as “critical” and 68% “very important”). Better productivity (70%), cost savings (67%), and reduced security risk (67%) are perceived as top benefits of integrating security into SDLCs.

- Just 15% report that security is always integrated from the beginning of the development lifecycle; more than half (51%) indicate this happens often.

- Not integrating security into the SDLC has often resulted in project delays (72%), financial loss (63%) and/or compromised brand reputation (57%) at respondents’ organizations.

- More than half (58%) report their organization has released applications with security vulnerabilities in the past year.

- All respondents indicate current application security processes are creating bottlenecks to at least some extent (47% “to a great extent” and 53% “to some extent”).
  - More than seven in ten respondents (72%) report poor collaboration between DevOps and security teams is one aspect of security that is delaying development projects. Respondents also cite difficulty identifying the correct project and feature level security requirements (71%) as a bottleneck.

- While DevOps processes are typically highly automated, 55% report moderate or low automation of security processes.

- Eighty-eight percent (88%) report it is highly challenging to gain access to accurate, relevant information regarding application security and compliance. It’s most difficult for development teams to gain access to prioritization of known security vulnerabilities (66%), assurance that code meets the necessary requirements (61%), and information about specific security policies that impact a given project (60%).

- Development teams are empowered to take ownership of application security at less than one-third (31%) of respondents’ organizations.

- Just one-quarter (28%) indicate development teams receive application security requirements during the planning stage of the development lifecycle.

- At 61% of organizations, the feedback sharing process between development and security teams is not fully automated. Most respondents (79%) report their security teams acknowledge and respond to feedback from development teams.

- Just 12% report that their organizations have adopted continuous security strategy; all others report interest in adopting (22% are piloting, 46% have plans to adopt in the next 12 months, and 21% are planning to adopt more than 12 months from now).

- Respondents cite empowerment of development teams (73%), enablement of real-time collaboration (72%), and reduced security risk (70%) as top potential benefits of continuous security strategy.

- Consolidation of security results across tools and the ability to prioritize vulnerabilities at a project-level are top attractions of a platform that can automate application security (63% and 62% rating as “extremely valuable”, respectively).
Results
Virtually all respondents (98%) place high importance on integrating security throughout the development lifecycle.

Q1: From your perspective, how important is it to integrate security throughout the software development lifecycle (SDLC)?
Better productivity, cost savings, and reduced security risk are perceived as top benefits of integrating security into SDLCs.

Q2: What do you perceive to be the most important benefits of integrating security into software development lifecycles?
Just 15% report that security is always integrated from the beginning of the development lifecycle; more than half (51%) indicate this happens often.

Q3. At your organization, how frequently are security processes integrated into the software development lifecycle from the beginning of the development process?
Not integrating security into the SDLC has most often resulted in project delays, financial loss and/or compromised brand reputation.

Q4: In which of the following ways has your organization been impacted when application security is not integrated into the software development lifecycle? (Please select all that apply.)

- Delays in project delivery: 72%
- Financial loss: 63%
- Compromised company/brand reputation: 57%
- Reallocation of staff resources to fix vulnerabilities in production: 47%
- Inability to meet compliance requirements: 47%
- Security breach(es): 45%
- Legal or regulatory fines/penalties: 41%
More than half (58%) report their organization has released applications with security vulnerabilities in the past year.

In the past 12 months, has your organization released an application into production with security vulnerabilities?

- Yes: 58%
- No: 41%
- Don’t know: 1%
All respondents indicate current application security processes are creating bottlenecks to at least some extent.

Q6. To what extent is your organization’s current application security process creating bottlenecks in development/delaying time to market?

Extent to Which Current Application Security Process is Delaying Time to Market

- To a great extent: 47%
- To some extent: 53%
More than seven in ten respondents (72%) report poor collaboration between DevOps and security teams is one aspect of security that is delaying development projects.

**Top Aspects of Application Security Causing Bottlenecks in Development**

- Poor collaboration/lack of a feedback loop between Development and security teams: 72%
- Difficulty in identifying the correct project and feature level security requirements (e.g., due to complex documentation): 71%
- Lack of security process orchestration as part of the SDLC/CI/CD: 68%
- Lack of the right information to act on testing results: 65%
- Application security is static/not updated when requirements change, requiring rework: 65%
- Manual processes: 30%
- Other: 1%
- None: 1%

Q7: Which of the following aspects of application security are creating bottlenecks in the development process at your organization? (Please select all that apply.)
While DevOps processes are typically highly automated, 55% report moderate or low automation of security processes.

How would you describe the level of automation within your **DevOps** processes?

- Very high (almost no human intervention is needed) - 8%
- High - 79%
- Moderate - 13%

How would you describe the level of automation of your **security** processes?

- Very high (almost no human intervention is needed) - 6%
- High - 39%
- Moderate - 51%
- Low - 4%

Respondents who indicate DevOps is highly automated are also the most likely to report that security processes are highly automated (70% of this group versus 21% among other respondents).

Q8: How would you describe the level of automation within your DevOps processes?
Q9. How would you describe the level of automation of your security processes?
Eighty-eight percent (88%) report it is highly challenging to gain access to accurate, relevant information regarding application security and compliance.

Q10: How challenging is it for development and project management teams at your organization to access accurate, relevant information about application specific security and compliance requirements?
At two-thirds of respondents’ organizations (66%), it’s difficult for development teams to gain access to prioritization of known security vulnerabilities.

**Q11: What security-related information is most difficult or time consuming for your DevOps and/or project management teams to access? (Please select all that apply.)**

- Prioritization of known vulnerabilities that need to be remediated: 66%
- Assurance that code meets the security requirements necessary to be compiled: 61%
- The specific security policies that impact a given project (instead of broader policies that might not be applicable): 60%
- Alerts regarding new security vulnerabilities and expected impacts post-production: 57%
- Assurance that a given feature has been developed in accordance with security policies: 55%
- Knowledge of whether the application has been approved to be released in production: 44%
- Security scan/test results: 39%
Just one-quarter (28%) indicate development teams receive application security requirements during the planning stage of the development lifecycle.

Q13: At What stages of the SDLC is the development team provided with security requirements and the opportunity to provide feedback? (Select all that apply)
Most respondents (79%) report their security teams acknowledge and respond to feedback from development teams.

Q14: Does the security team typically acknowledge and respond to feedback provided by the development team?

- Yes: 79%
- No: 21%
At 61% of organizations, the feedback sharing process between development and security teams is not fully automated.

Q15: How much of the feedback sharing process between the development and security teams is automated?
Development teams are empowered to take ownership of application security at less than one-third (31%) of respondents’ organizations.

Q12: To what extent development teams at your organization empowered to take ownership of application security in their processes?
At the 31% of organizations where DevOps teams are empowered to take ownership of application security...

- Respondents are less likely to report their organizations have released applications with security vulnerabilities in the past 12 months (50% versus 73% among others).

- Development teams are more likely to be provided with security requirements and given opportunities for feedback in the planning stage of the SDLC (48% vs. 16% among others).

- Respondents more often report feedback sharing processes between development and security teams are fully automated (49% vs. 25% among others).
Just 12% report that their organizations have adopted continuous security strategy; all others report interest in adopting.

Adoption of Continuous Security Strategy

In software development, **continuous security** is 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.

Q16: How would you describe your organization’s adoption of continuous security strategy?
Organizations where developers have the most ownership of security are more likely to have adopted continuous security strategy.

**Adoption of Continuous Security Strategy**

*In software development, continuous security is 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.*

Q16: How would you describe your organization’s adoption of continuous security strategy?
Respondents cite empowerment of development teams, enablement of real-time collaboration, and reduced security risk as top potential benefits of continuous security strategy.

<table>
<thead>
<tr>
<th>Most Attractive Potential Benefits of Continuous Security Strategy</th>
<th>Percentage</th>
</tr>
</thead>
<tbody>
<tr>
<td>Empowering development teams with the flexibility to manage security within existing workflows</td>
<td>73%</td>
</tr>
<tr>
<td>Enabling real-time collaboration between development, operations, and security teams</td>
<td>72%</td>
</tr>
<tr>
<td>Reducing security risk</td>
<td>70%</td>
</tr>
<tr>
<td>Dynamic management of security requirements in line with business needs and concerns</td>
<td>61%</td>
</tr>
<tr>
<td>Removing bottlenecks</td>
<td>55%</td>
</tr>
<tr>
<td>Eliminating manual security processes/increasing automation</td>
<td>50%</td>
</tr>
<tr>
<td>Improving time to market</td>
<td>49%</td>
</tr>
<tr>
<td>Centralizing security governance</td>
<td>45%</td>
</tr>
<tr>
<td>Other</td>
<td>1%</td>
</tr>
</tbody>
</table>

Q17. What are the most attractive potential benefits of continuous security strategy? (Please select all that apply.)
C-level respondents are more likely to cite enablement of real-time collaboration, the ability to reduce security risk, and improving time to market as attractive benefits.

<table>
<thead>
<tr>
<th>Most Attractive Potential Benefits of Continuous Security Strategy (By Job Title)</th>
<th>C-level</th>
<th>All others</th>
</tr>
</thead>
<tbody>
<tr>
<td>Empowering development teams with the flexibility to manage security within existing workflows</td>
<td>72%</td>
<td>73%</td>
</tr>
<tr>
<td>Enabling real-time collaboration between development, operations, and security teams</td>
<td>88%</td>
<td></td>
</tr>
<tr>
<td>Reducing security risk</td>
<td>84%</td>
<td>84%</td>
</tr>
<tr>
<td>Dynamic management of security requirements in line with business needs and concerns</td>
<td>68%</td>
<td>68%</td>
</tr>
<tr>
<td>Removing bottlenecks</td>
<td>64%</td>
<td>54%</td>
</tr>
<tr>
<td>Eliminating manual security processes/increasing automation</td>
<td></td>
<td>54%</td>
</tr>
<tr>
<td>Improving time to market</td>
<td>53%</td>
<td>40%</td>
</tr>
<tr>
<td>Centralizing security governance</td>
<td>51%</td>
<td>28%</td>
</tr>
<tr>
<td>Other</td>
<td>16%</td>
<td>16%</td>
</tr>
</tbody>
</table>

Q17. What are the most attractive potential benefits of continuous security strategy? (Please select all that apply.)
Consolidation of security results across tools and the ability to prioritize vulnerabilities at a project-level are top attractions of a platform that can automate application security.

### Valuable Aspects of a Platform to Help Automate Application Security

<table>
<thead>
<tr>
<th>Aspect</th>
<th>Extremely valuable</th>
<th>Very valuable</th>
<th>Somewhat valuable</th>
<th>Not very valuable</th>
<th>Not at all valuable</th>
</tr>
</thead>
<tbody>
<tr>
<td>Consolidation of security results across tools</td>
<td>64%</td>
<td>30%</td>
<td>6%</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Project-level prioritization of vulnerabilities</td>
<td>63%</td>
<td>33%</td>
<td>3%</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Orchestration of security processes</td>
<td>59%</td>
<td>37%</td>
<td>3%</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Dynamic management &amp; deployment of security requirements</td>
<td>55%</td>
<td>43%</td>
<td>2%</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Creation/management of a clear audit trail</td>
<td>55%</td>
<td>43%</td>
<td>2%</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Continuous monitoring and notification regarding application security posture</td>
<td>53%</td>
<td>43%</td>
<td>3%</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Automated security approval</td>
<td>49%</td>
<td>47%</td>
<td>3%</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Understanding compliance with security frameworks &amp; standards</td>
<td>46%</td>
<td>52%</td>
<td>1%</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Guided, informed decision-making on security issues &amp; procedures</td>
<td>39%</td>
<td>58%</td>
<td>4%</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Q18: How valuable are the following aspects of a platform that could help your organization automate application security?
Research Team at IDG Communications, Inc.

Aran Bride  
Senior Director, Research  
*IDG Insight and Performance Marketing*  
IDG Communications, Inc.  
aran_bride@idg.com  
508-766-5604  
IDG.com

Jen Garofalo  
Research Director  
*IDG Insight and Performance Marketing*  
IDG Communications, Inc.  
jen_garofalo@idg.com  
508-766-5605  
IDG.com