BLACK & WHITE PAPER

DevSecOps Realities and Opportunities

APRIL 2018

COMMISSIONED BY

SYNOPSYS®

About this paper

A Black & White paper is a study based on primary research survey data that assesses the market dynamics of a key enterprise technology segment through the lens of the "on the ground" experience and opinions of real practitioners – what they are doing, and why they are doing it.

About 451 Research

451 Research is a preeminent information technology research and advisory company. With a core focus on technology innovation and market disruption, we provide essential insight for leaders of the digital economy. More than 100 analysts and consultants deliver that insight via syndicated research, advisory services and live events to over 1,000 client organizations in North America, Europe and around the world. Founded in 2000 and headquartered in New York, 451 Research is a division of The 451 Group.

NEW YORK
1411 Broadway
New York, NY 10018
+1 212 505 3030

SAN FRANCISCO
140 Geary Street
San Francisco, CA 94108
+1 415 989 1555

LONDON
Paxton House
30, Artillery Lane
London, E1 7LS, UK
+44 (0) 207 426 1050

BOSTON
75-101 Federal Street
Boston, MA 02110
+1 617 598 7200

EXECUTIVE SUMMARY

While many organizations are still in the early days of tearing down organizational silos to build DevOps teams and implementing continuous integration and continuous delivery (CI/CD) workflows, the benefits of streamlined, collaborative development approaches are clear: they enable organizations to bring more features and improvements to market faster. What is not so well understood is how application security is being included in these dynamic, fast-paced environments and how security testing tools and best practices must be augmented to stay relevant and keep pace. To better understand this emerging paradigm, also known as DevSecOps, we surveyed 350 IT decision-makers at large enterprises across a variety of industries. The results show that while half of DevOps teams are failing to incorporate application security into their CI/CD workflows, doing so is a high priority and presents many opportunities.

DevOps teams today are working with large-scale infrastructures, releasing software faster, and doing so with significant code changes in each release. Without a clear and informed strategy, this can make establishing and scaling application security testing within these processes complex and difficult.

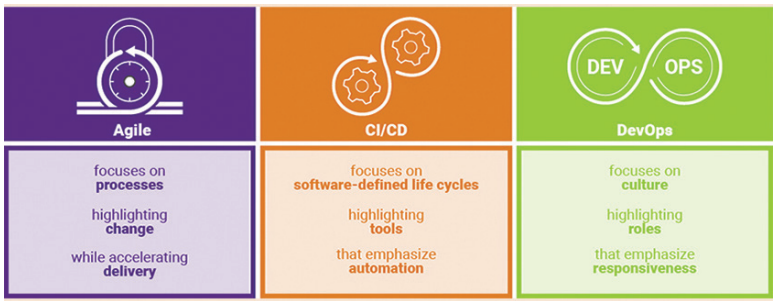
Even though the popular view is that security slows down software releases, we believe organizations can actually reduce risk and save themselves rework headaches and time by considering and injecting security early in the process and choosing security tools and elements that can be integrated and automated. This means integrating security at code commit and in pre-implementation processes, something our survey indicates is lacking for most organizations. While the early inclusion of security in rapid release processes is somewhat elusive among enterprise organizations, our survey did indicate an awareness of its importance when we asked when security should be integrated with CI/CD implementations.

In addition, more DevOps teams are folding security into their CI/CD workflows, driven by the priorities of software quality, compliance and avoiding risk. Despite increased awareness and these drivers, there is still a lack of understanding that when application security testing is integrated early and effectively, it results in more secure, faster releases and less rework.

Challenges of integrating security into CI/CD release processes center on a lack of automated, integrated security tools, inconsistency and the noise of false positives. These are real issues for enterprise organizations, but issues that can be addressed with the right technology choices, tools and providers. Collaboration and culture must also be included in DevSecOps efforts, and we see a growing number of stakeholders beyond developers and IT operations – including security teams – become increasingly critical.

Introduction

The maturation of the DevOps trend toward faster software iteration and efficiency through automation, combined with high-profile security incidents, has helped fuel the injection of security in CI/CD release processes. DevOps represents the cross-functional collaboration among developers and IT operations. CI/CD represents the workflows and toolchains that leverage automation. To get a sense of DevSecOps realities amid this crossover between CI/CD and security – two practices that have historically been and are often still viewed as antithetical – we surveyed 350 enterprise IT decision-makers at large enterprises across a variety of industries. What we found is that application security testing is, indeed, making its way into CI/CD workflows. However, it is not generally happening early enough in the process, such as with code commits, for organizations to fully benefit from reduced risk and rework headaches. We also discovered that, unsurprisingly, organizations are managing large infrastructures with hundreds of server nodes or more, as well as rapid release timelines, which can make managing and scaling DevSecOps even more challenging. According to our survey, DevSecOps is being driven by the priorities of software quality and security, compliance requirements and avoiding risk. The key DevSecOps challenges identified by respondents include lack of automated, integrated security tools, the noise of false positives and inconsistency. While there is a perception that security slows down CI/CD processes, we also believe that by seeking out the proper tools and vendor support and considering security early in the release process – ideally in pre-implementation – organizations can actually maintain velocity of software releases, lower their risk, and reduce required reworks and fixes.

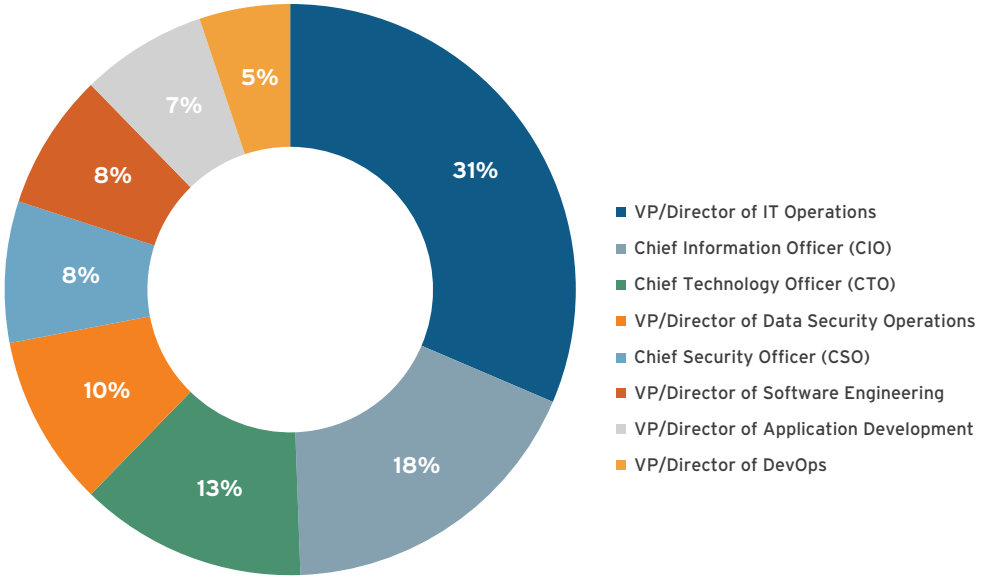


DEMOGRAPHICS

To get a better perspective on DevSecOps, we surveyed 350 enterprise IT decision-makers, primarily in North America and Europe. Our survey focused on organizations that had undertaken CI/CD implementations and on individuals who make decisions on sourcing, buying and managing software components and services (Figure 1).

Figure 1: Job title

Q. Which job title most closely corresponds to your role?

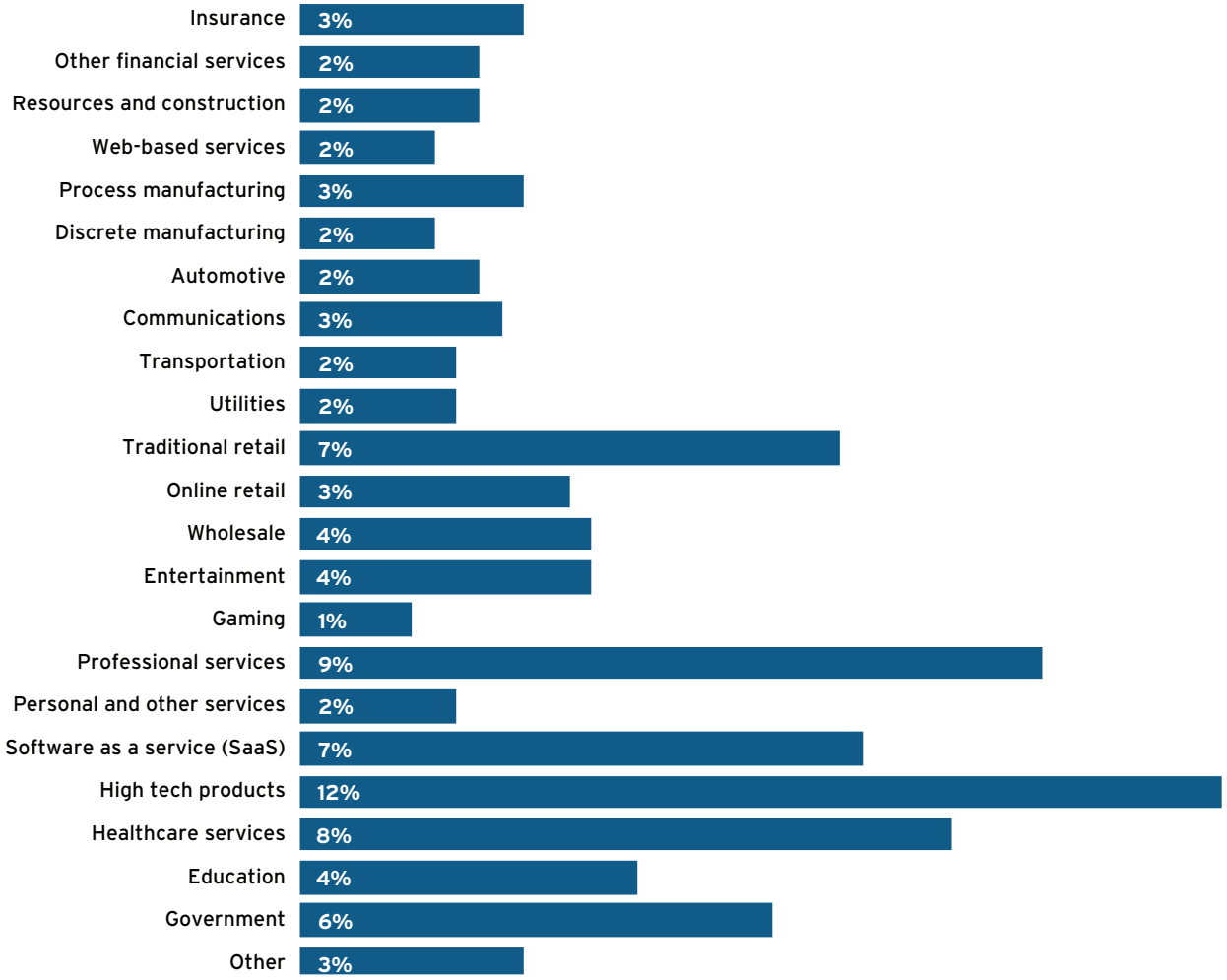


Source: 451 Research

Our survey also spanned several verticals: high tech, professional services, healthcare services, traditional retail, SaaS and government were the most heavily represented (Figure 2). In terms of size, our survey included enterprises of 1,000-50,000 or more employees (Figure 3).

Figure 2: Survey respondents by industry

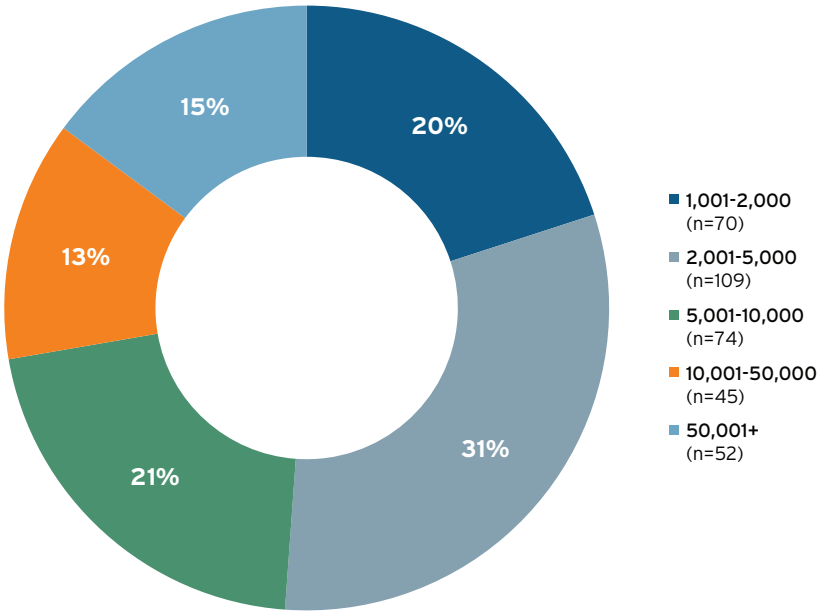
Q. What is the primary industry of your business?



Source: 451 Research

Figure 3: Company size

Q. Please check the box which best corresponds to the size of your company by number of full time employees.



Source: 451 Research

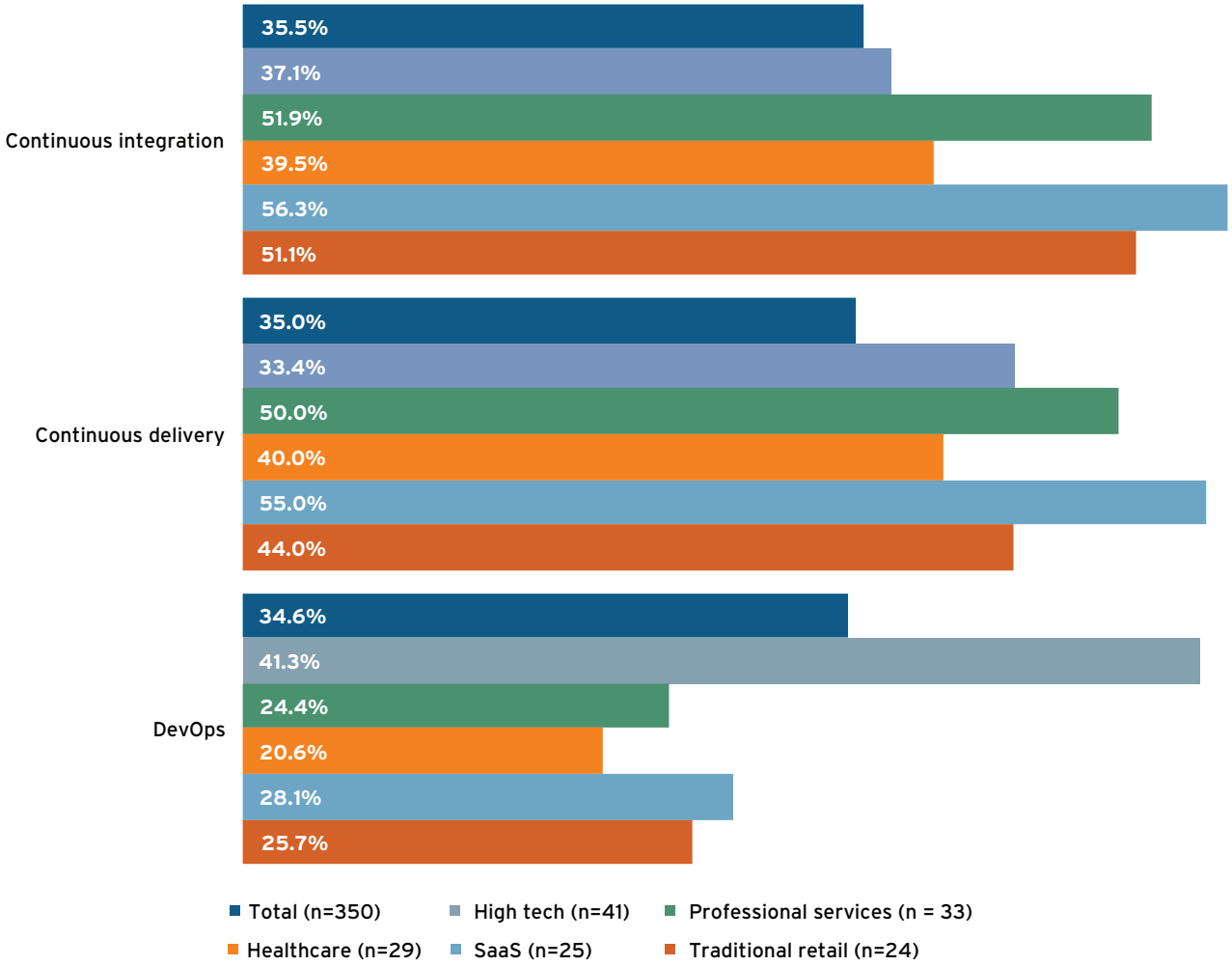
The Scope, Scale and Speed of DevSecOps

DevOps teams and CI/CD technology, methodology and use have grown in recent years as enterprise organizations seek to better serve both internal developers or lines of business and their customers. The early days of these releases were focused almost entirely on speed, but with more widespread enterprise adoption, they have evolved to include efficiency and security, where we see the genesis of DevSecOps.

Our survey indicated that while adoption of DevOps methodology and CI/CD technology is significant, not all teams within enterprise organizations are necessarily doing any of it. Of our survey respondents, 36% reported developer/administrator teams were focused on continuous integration. Another 35% of respondents stated teams focused on continuous delivery, and 35% also reported a DevOps focus, although DevOps was ranked lowest in most industries, including traditional retail, SaaS and healthcare. (Figure 4)

Figure 4: Application release approach by industry

Q. What percentage of developer/administrator teams in your organization are focused on the following?

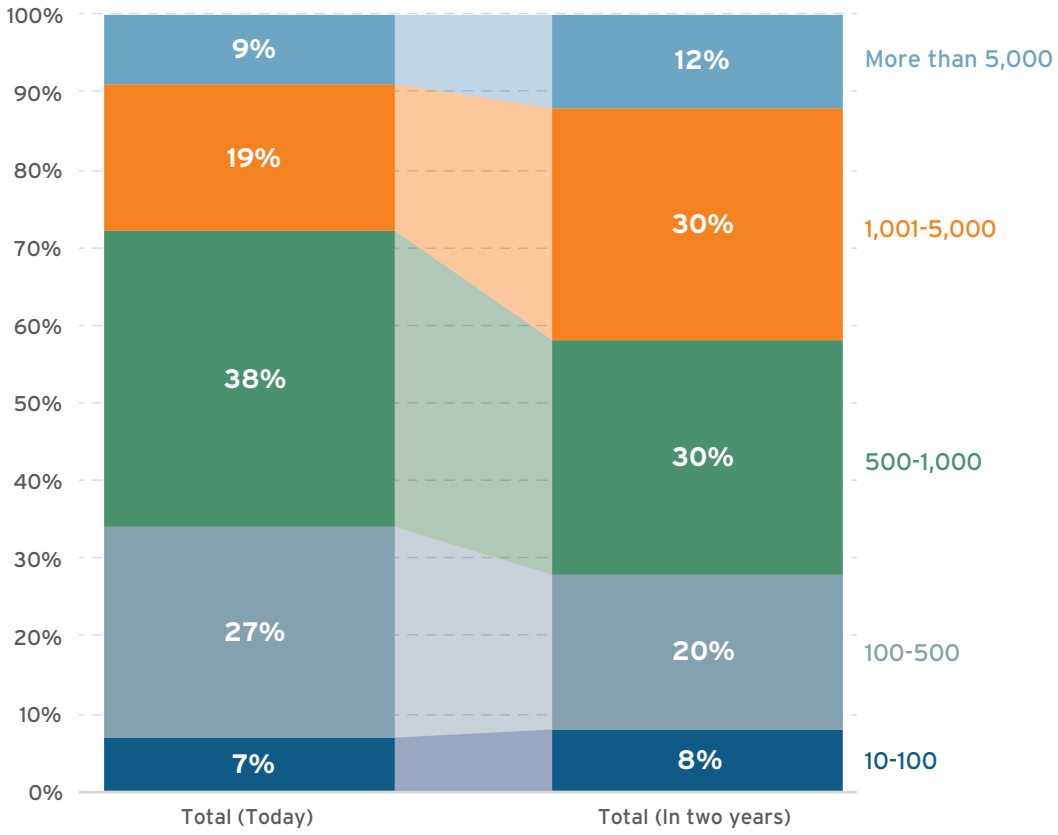


Source: 451 Research

Our survey highlighted the growing scale of enterprise CI/CD releases, with most respondents reporting they involve 500-1,000 servers or nodes today and a large number indicating deployments will grow to more than 1,000 servers or nodes in two years (Figure 5). This represents the significant size of infrastructure involved in enterprise CI/ CD workflows, making the scaling of DevSecOps even more complex and difficult.

Figure 5: Number of servers or nodes in CI/CD – today vs. expected in two years

Q. How many servers or nodes are included in your CI/CD toolchain implementation?
Q. How many servers or nodes do you expect to be included in your CI/CD toolchain implementation in two years?



Source: 451 Research

The challenges with scaling DevSecOps may help make the business case for other technologies, such as cloud computing infrastructure and application container software, which can help make releases and DevSecOps more scalable, consistent and repeatable.

Our survey also highlighted the increasing speed of enterprise software releases. Nearly half of respondents (49%) indicated code changes or releases were deployed in a matter of days. While 22% indicated a frequency measured in weeks, the same number (22%) said hours. Only 5% reported code changes or releases deployed in a matter of minutes, with 2% indicating it was down to seconds. Nevertheless, this is a faster pace for enterprise software releases compared to the monthly timelines that characterized traditional releases. With more frequent changes comes a need for more testing. Similarly, organizations polled said the size of code changes pushed in the CI/CD workflows was significant; 67% of respondents indicated regular, significant changes, 17% mentioned large, complex changes, and another 16% reported small, simple changes.

NEARLY HALF OF RESPONDENTS (49%) INDICATED CODE CHANGES OR RELEASES WERE DEPLOYED IN A MATTER OF DAYS. WHILE 22% INDICATED A FREQUENCY MEASURED IN WEEKS, THE SAME NUMBER (22%) SAID HOURS.

Our survey also indicated enterprise organizations expect significant factors of improvement from their CI/CD implementations. The most organizations (36%) sought a 4x factor of improvement in time to deploy from their CI/CD workflows. A significant number (15%) sought a 5x factor of improvement. Another 7% sought more than a 5x factor of improvement, and 5% were seeking a 10x or greater factor. These findings highlight how speed and iteration are typically prioritized, but sometimes at the expense of security measures that could actually contribute to faster releases by reducing bugs, downtime and maintenance. We believe that as organizations evolve these processes, the focus will naturally move from 'how fast can development teams iterate' to 'how reliably can we deploy high-quality, appropriately secure code each and every time.' That critical change in focus – that more mature view of risk management – will realign everyone's expectations on what '4x' really means.

OUR SURVEY ALSO INDICATED ENTERPRISE ORGANIZATIONS EXPECT SIGNIFICANT FACTORS OF IMPROVEMENT FROM THEIR CI/CD IMPLEMENTATIONS. THE MOST ORGANIZATIONS (36%) SOUGHT A 4X FACTOR OF IMPROVEMENT IN TIME TO DEPLOY FROM THEIR CI/CD WORKFLOWS. A SIGNIFICANT NUMBER (15%) SOUGHT A 5X FACTOR OF IMPROVEMENT.

Adding to the complexity of implementing CI/CD, organizations are also seeking to support a mix of on-premises and hosted deployments. Most organizations (41%) indicated a preference for a combination of on-premises and hosted software for the consumption and integration of security elements in their CI/CD workflows. Thirty-seven percent of respondents said they prefer licensed software, while 22% selected 'as a service.' When asked what drives their preference for on-premises or hosted security software for CI/CD deployments, most organizations (42%) cited security; 31% said scalability, availability and elasticity, and 22% cited compliance and regulatory needs. This reflects that today's enterprise organizations have legitimate reasons to support hybrid infrastructure scenarios that involve public clouds, private clouds and on-premises environments. It also highlights how security components and elements must support the different infrastructures if they are to be effectively integrated into CI/CD processes. We believe the 'Ops' portion of DevSecOps will become much more critical in these scenarios, and these teams may require a lot of training to ensure bad cloud, orchestration, container, API access, and other security configurations do not undermine application security.

Because most organizations seem to be dealing with larger and more significant and complex changes, as well as both on-premises and hosted deployments, they are likely to be encountering more security issues. This also highlights that while organizations seek performance and other benefits from their CI/CD workflows, they must not forget security as they release and change larger portions of code more frequently.

Status of DevSecOps Today

When we investigated the degree to which enterprise organizations are incorporating security in DevOps, we found across industries only about half of CI/CD workflow implementations include any application security testing elements (Figure 6), which shows there is ample room for improvement. When we asked which elements of application security testing were most critical, most respondents (61%) identified software composition analysis (SCA) and CVE scanning. We're not surprised to see this pointed out as most critical given recent security incidents – including Heartbleed and the Apache Struts vulnerability that caused the Equifax breach – have highlighted potential risks, particularly in open source software. Nevertheless, with cloud computing, containers, microservices and other leading-edge technology, open source software is typically a significant and meaningful part of CI/CD pipelines and workflows. We would also highlight that even though composition analysis was perceived as the most critical element of DevSecOps, nearly 40% of our survey respondents reported use of no tool to find vulnerabilities in open source software in use or that they didn't use open source at all (Figure 7), a somewhat dubious claim given the prevalence of open source in today's enterprise software releases and workflows.

WHEN WE INVESTIGATED THE DEGREE TO WHICH ENTERPRISE ORGANIZATIONS ARE INCORPORATING SECURITY IN DEVOPS, WE FOUND THAT ONLY ABOUT HALF OF CI/CD WORKFLOW IMPLEMENTATIONS INCLUDE ANY APPLICATION SECURITY TESTING ELEMENTS, WHICH SHOWS THERE IS AMPLE ROOM FOR IMPROVEMENT.

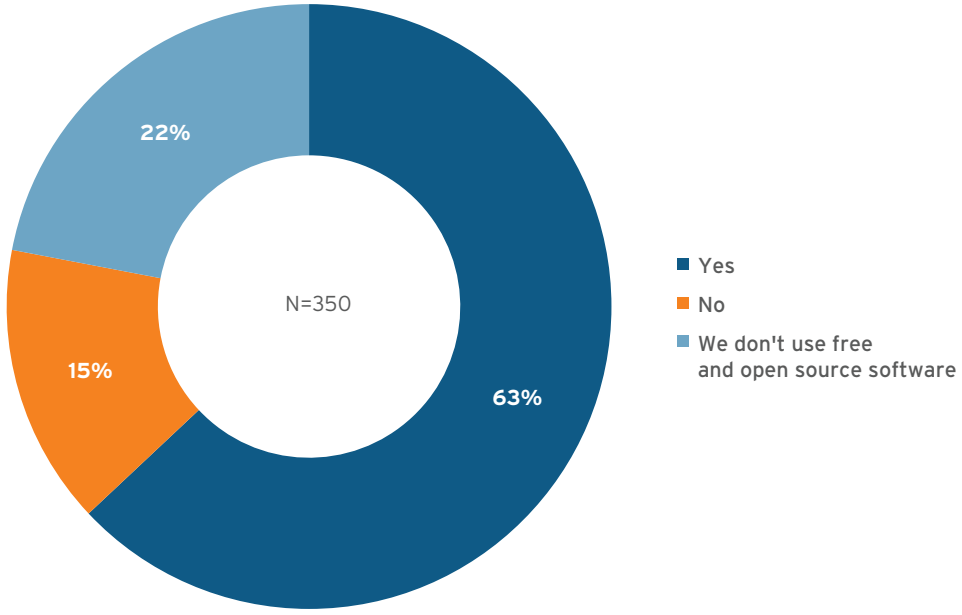
Figure 6: Security in CI/CD workflows by industry

Q. How many of your CI/CD workflow implementations include application security testing elements?

Source: 451 Research

Figure 7: Usage of tools to find vulnerabilities in open source software

Q. Are any tools used to find vulnerabilities in free and open source software in use?



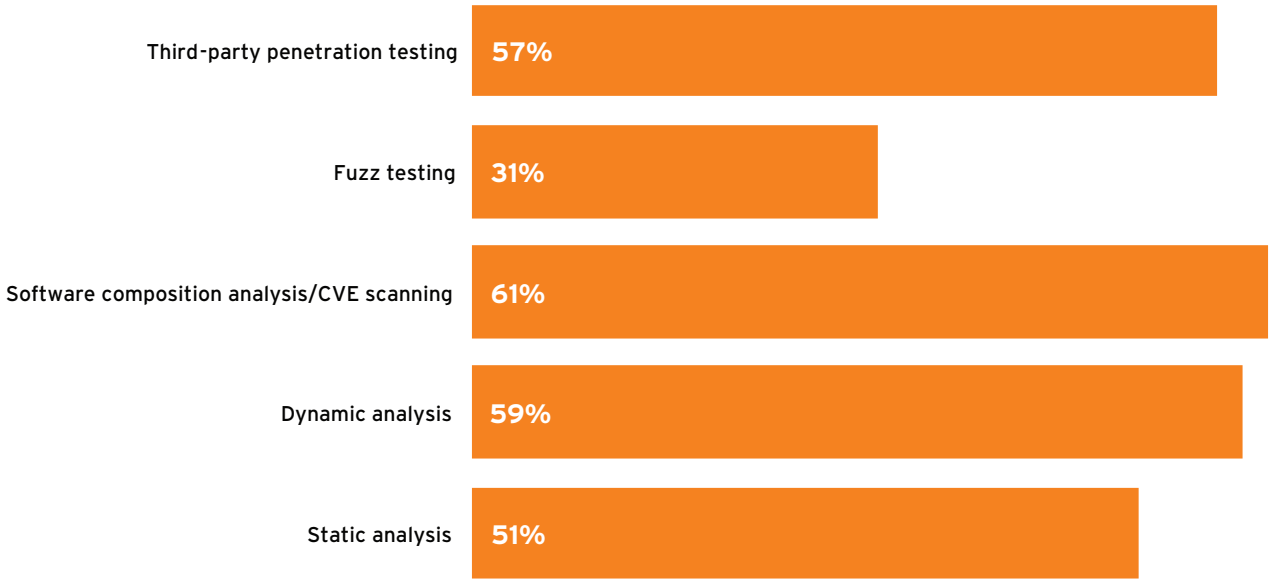
Source: 451 Research

The next most critical security element, according to our survey, was dynamic application security testing (DAST), pointed out by 59% of respondents (Figure 8). This also is not surprising given DAST is an established and popular component of security, but it does have its shortcomings, such as typically occurring late in the software development lifecycle (SDLC) when there is running code and lack of automation. Next, 57% of survey respondents identified penetration testing as critical. Again, this comes as little surprise given many organizations do penetration testing to comply with regulatory requirements such as PCI. We agree that penetration testing is a critical element, but alone, it is neither sufficient nor scalable in CI/CD releases because it also typically occurs as an out-of-band activity late in the software release process. Although it ranks lower as a critical element (31%) in our survey and in other research, there are benefits to fuzz testing, such as fewer

bugs and greater software robustness. While only 51% in the survey mentioned static application security testing (SAST), we believe that because it can be integrated earlier in the process, it is one of the simplest, fastest routes to cost-effective application security testing for CI/CD releases.

Figure 8: Critical elements of application security testing

Q. What are the most critical application security testing elements to add to CI/CD workflows?

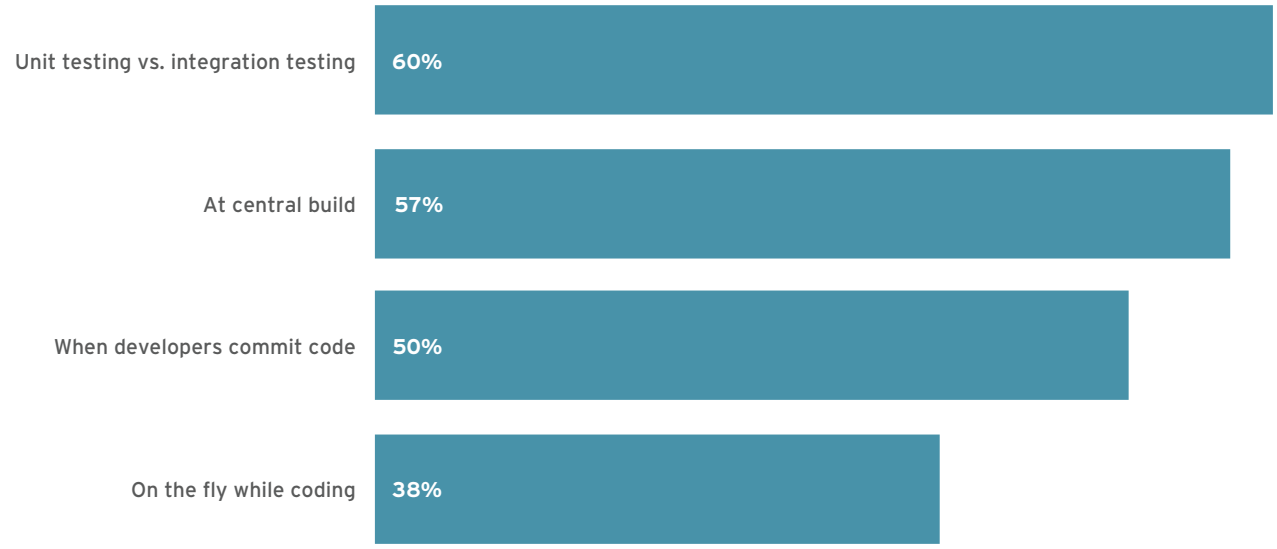


Source: 451 Research

Our survey also delved into scenarios when application security testing is integrated into CI/CD processes. What we found is that more organizations are injecting security through unit testing (Figure 9) vs. integration testing (60%) and at central build (57%) than when developers commit code (50%). This may represent a missed opportunity for organizations that want to improve the security of their more iterative releases because the integration of application security testing at code commit can save time and effort by preventing bugs and rework. When we asked about pre-implementation security measures, a higher number of organizations reported activities such as security control design analysis (74%), application risk assessment (61%), threat modeling (59%) and architectural risk analysis (58%). Even if organizations are reporting these activities in higher numbers than reality, it highlights the importance and awareness of the fact that roughly half of software vulnerabilities are flaws in design and architecture and thus can't typically be found through automated testing. Nevertheless, this out-of-band testing and the exertion of security diligence prior to programming will reduce trouble and save time.

Figure 9: Security testing integration with CI/CD

Q. Are you currently integrating security testing with CI/CD workflows?



Source: 451 Research

While fewer enterprise organizations are integrating application security testing at code commit, a greater number of them recognize the importance of security early in the process. When we asked organizations when application security testing should be integrated with CI/CD workflows, the percentages of 'When developers commit code' and 'On the fly while coding' were both high (67% and 44%, respectively) compared to what is actually being done. We see that even though organizations are aware it would be beneficial to align application security testing with CI/CD workflows earlier in the process, they are currently focused mostly on doing so at central build or unit testing vs. integration testing, demonstrating that there is still ample room for improvement. Much of this challenge centers on enterprise IT inertia and the fact that DevSecOps is still in its early days of evolution. Still, the growing awareness is consistent with separate survey data, such as our Voice of the Enterprise: Information Security, Budgets and Outlook 2017, which surveyed 600 enterprise IT decision-makers in North America, Europe and Asia from December 2017 through February 2018. Respondents to that survey highlighted securing emerging architectures, including the cloud, improved application security and automation of common security tasks among top strategic security objectives.

WHEN WE ASKED ORGANIZATIONS WHEN APPLICATION SECURITY TESTING SHOULD BE INTEGRATED WITH CI/CD WORKFLOWS, THE PERCENTAGES OF 'WHEN DEVELOPERS COMMIT CODE' AND 'ON THE FLY WHILE CODING' WERE BOTH HIGH (67% AND 44%, RESPECTIVELY) COMPARED TO WHAT IS ACTUALLY BEING DONE.

Our DevSecOps survey produced some interesting results in terms of who is responsible for application security testing in CI/CD processes. IT operations was the most popular response at 71%, ahead of security teams (61%) and developers (49%). This makes sense since we consistently see most of the disruption from DevOps happening on the IT operations side of the organization. Developers tend to have been more exposed to tenets such as transparency and collaboration given their work with open source software and agile practices. IT operations, on the other hand, faces a more dramatic shift from the command-and-control, stability priority of traditional software releases. Lower-ranked for security in CI/CD workflows were leadership and management (43%) and testing and QA (42%). One key takeaway here is that no single person or team can or should be responsible for security in CI/CD releases. In these environments, the continuous and constant flow of code, data and activity means all stakeholders need to be involved in securing the process.

ONE KEY TAKEAWAY HERE IS THAT NO SINGLE PERSON OR TEAM CAN OR SHOULD BE RESPONSIBLE FOR SECURITY IN CI/CD RELEASES. IN THESE ENVIRONMENTS, THE CONTINUOUS AND CONSTANT FLOW OF CODE, DATA AND ACTIVITY MEANS ALL STAKEHOLDERS NEED TO BE INVOLVED IN SECURING THE PROCESS.

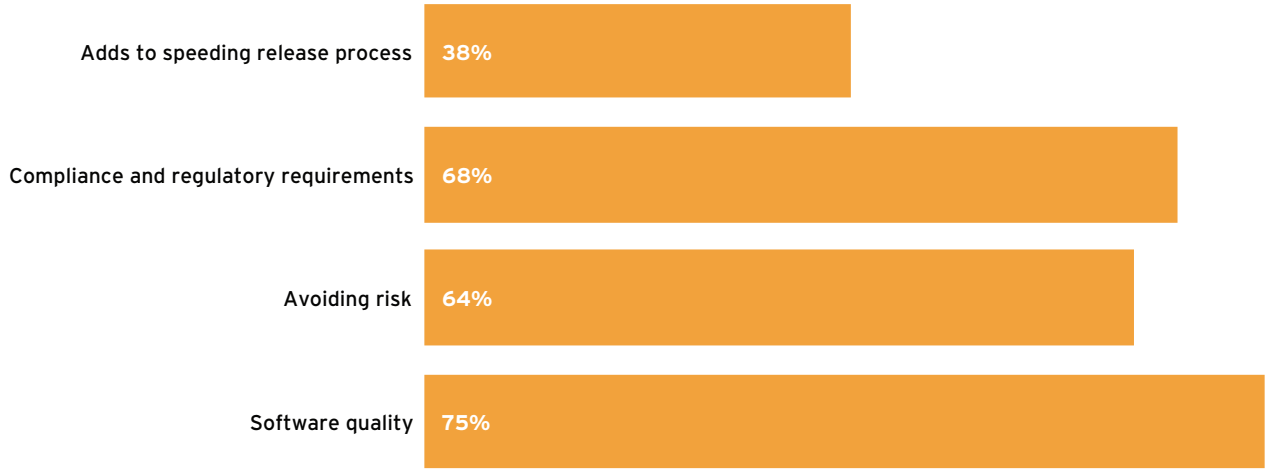
With the growth and maturation of DevOps, we have also seen a number of significant stakeholders beyond developers and IT operations teams pulled into the process, including database administrators, data scientists and analytics teams, and also security. Given this, we asked in our survey what other stakeholders are involved in IT management and DevOps initiatives. Security led the way at 66% across the board and was reflected in most respondents' job titles. 'Technology center of excellence' and similar groups also garnered 66% of responses, with database administrators and data analytics teams close behind at 64%. Line-of-business managers ranked lower at 46%, but the focus on adding security and data experts is encouraging. The earlier that security teams and individuals are collaborating with developers and IT operations, the earlier security will be integrated into the software development lifecycle – again, advantageous to reduce risk and rework.

Drivers of DevSecOps

When considering what is driving DevSecOps and the injection of security elements into CI/CD processes, our survey indicated that software quality was ranked highest at 75% (Figure 10). This validates the idea that companies are prioritizing high-quality, functional software. It may also mean that in the minds of enterprise IT decision-makers, quality and security go hand in hand. We've also seen historically how organizations may focus on the quality of certain software components, typically open source, and then realize the value of scrutinizing the quality for all of their code. The next biggest driver according to our survey was compliance and regulatory requirements (68%), which is always a priority for regulated industries. This is consistent with our other research that indicates security and compliance are top of mind in the enterprise adoption of cloud computing infrastructure and application container software. Another driver, avoiding risk, also ranked fairly high in our survey (64%), and this makes sense as we see high-profile security breaches and incidents consistently generating interest in and attention on software security. Lower-ranked on the survey was that application security testing can add to speeding the release process (38%). This is consistent with the misconception that security always slows things down, a mistaken belief that is often perpetuated by suboptimal tools that are difficult to integrate or automate, as well as both untrained tool users and untrained consumers of tool output. However, real-world enterprise use cases indicate that with the proper technology, experts and support, organizations can architect a secure process and toolchain for velocity.

Figure 10: Drivers of application security testing in CI/CD workflows

Q. What are the biggest drivers of incorporating application security testing into your CI/CD workflow?



Source: 451 Research

Challenges of DevSecOps

We also peered into the challenges of DevSecOps in our survey. The biggest issue identified by respondents was a lack of automated, integrated security tools for CI/CD (61%). This comes as little surprise because, again, it is still early days for the injection and integration of security in these faster software releases. We also note that not all security tools are equal, and the less software testing tools can be integrated and automated into enterprise workflows, the less effective they will be in securing CI/CD pipelines.

Also identified among the biggest challenges was inconsistent approach at 56% (Figure 11). We suspect this is because many security tools and services are difficult to integrate and do not report consistently into the workflow. One possible solution to this inconsistency is application container software, which must still be secured, but is beneficial in providing standardization of development environments and consistent development lifecycles, according to our Voice of the Enterprise: Servers and Converged Infrastructure, Organizational Dynamics 2017 survey.

The idea that security slows the release process down also ranked fairly high (48%) among challenges in our DevSecOps survey, but we believe this is a misconception. We believe organizations that take the right approach and apply the proper tools, integration, automation and methodology can include security and still maintain velocity in CI/CD releases.

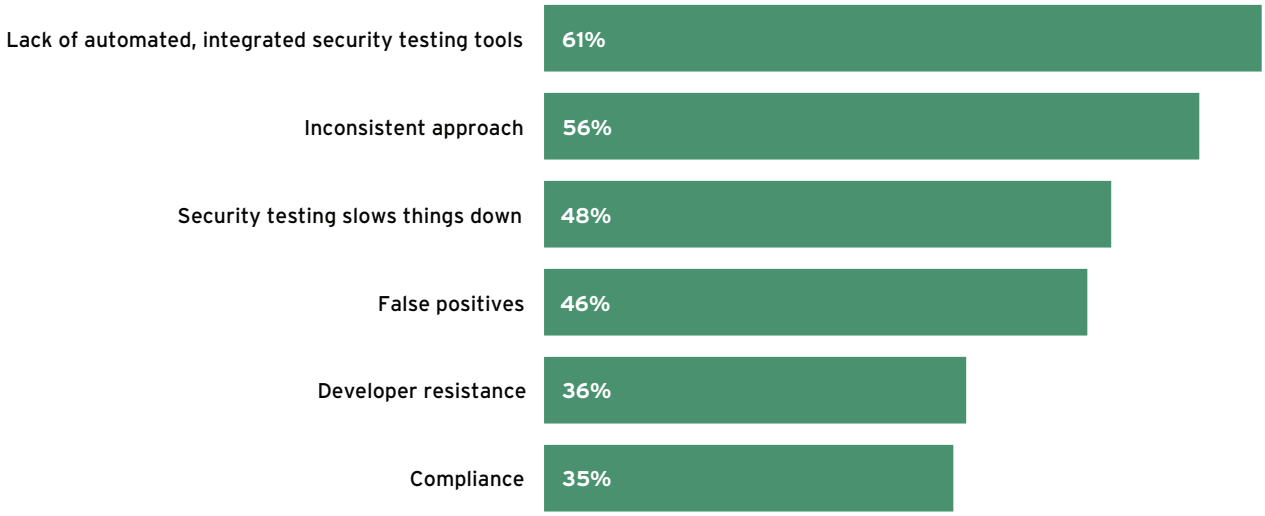
WE BELIEVE ORGANIZATIONS THAT TAKE THE RIGHT APPROACH AND APPLY THE PROPER TOOLS, INTEGRATION, AUTOMATION AND METHODOLOGY CAN INCLUDE SECURITY AND STILL MAINTAIN VELOCITY IN CI/CD RELEASES.

Another key challenge highlighted in our DevSecOps survey was false positives (46%), consistent with anecdotal research and conversations that suggest the noise of false positives can drown out the benefits of security scanning and other elements in CI/CD processes. We believe organizations can help address this issue by choosing security software and services that specialize in effectively reducing false positives and the noise that comes with them. In SAST, for example, this will likely require writing custom rules tailored to the organization's technology stacks and software.

WE BELIEVE ORGANIZATIONS CAN HELP ADDRESS THIS ISSUE BY CHOOSING SECURITY SOFTWARE AND SERVICES THAT SPECIALIZE IN EFFECTIVELY REDUCING FALSE POSITIVES AND THE NOISE THAT COMES WITH THEM.

Figure 11: Security testing challenges in CI/CD workflows

Q. What are the most significant application security testing challenges inherent in continuous integration/continuous delivery (CI/CD) workflows?



Source: 451 Research

Conclusion

Despite an awareness that integration of security elements early in the software development lifecycle – ideally when developers commit code – is advantageous, enterprises are still focused more on in-band application security measures, such as unit testing vs. integration testing. To act on this awareness, enterprises will need security tools that can be both integrated and automated across the SDLC and across hybrid infrastructures that include public clouds, private clouds and on-premises environments. Of course, it's also important to improve the ability of developers and testers to create unit tests that truly demonstrate correct operation of or uncover weaknesses in implemented security features.

Cloud computing and application containers can also help, but just as penetration testing alone does not make software releases secure, clouds and containers bring with them unique security issues that must be addressed.

The stakeholder spread of DevOps, whereby database administrators, security teams and others get pulled into the process, is also helping to drive the DevSecOps trend. This has already been a factor in enterprise deployment of DevOps, which tends to start with a developer or line-of-business team and then spread more broadly throughout the organization. Our survey results showing security among the biggest group of additional stakeholders is consistent with anecdotal input from enterprise end users and providers that are increasingly including security in their CI/CD plans and processes.

Looking ahead, we see that software and infrastructure complexity, as well as the scale of deployments, show no signs of slowing, and this can expose enterprise organizations to a growing number of – and more types of – security issues. To respond effectively, organizations need to include security in more of their CI/CD deployments because roughly only half are currently subject to application security testing. Enterprises will also benefit from injecting security elements earlier in the software development lifecycle – most effectively at code commit. They must also support integration and collaboration that includes security elements and personnel. Thus, they stand to maintain the velocity and growing scale of CI/CD releases, but do so in a secure manner that reduces risk and rework and, thus, contributes to greater speed.

TO RESPOND EFFECTIVELY, ORGANIZATIONS NEED TO INCLUDE SECURITY IN MORE OF THEIR CI/CD DEPLOYMENTS BECAUSE ROUGHLY ONLY HALF ARE CURRENTLY SUBJECT TO APPLICATION SECURITY TESTING. ENTERPRISES WILL ALSO BENEFIT FROM INJECTING SECURITY ELEMENTS EARLIER IN THE SOFTWARE DEVELOPMENT LIFECYCLE - MOST EFFECTIVELY AT CODE COMMIT.

Note that this survey and report focused on adding security testing to CI/CD toolchains and DevOps processes in the software development lifecycle. We believe each organization should strive to improve its agility, implement CI/CD toolchains that decrease time to market, and implement DevSecOps processes that remove barriers to success. We believe each organization should tightly integrate at-speed security testing into those SDLC components. Security testing in the SDLC is a great start to an overall application security program.

From the corporate risk management perspective, many aspects of application security will exist outside the SDLC, such as having an application security team (security champions that work directly with development teams on security choices), harmonized compliance requirements, non-functional security requirements, training and vendor management. In addition, some application security efforts that do happen in the SDLC cannot be automated. Security review of application design and manual penetration testing are good examples here.

While the benefits of getting more features to market faster are very clear to everyone, fewer organizations will accept the risk of using in-SDLC testing alone to ensure software moved to production is appropriately secure and compliant, and also meets users' privacy expectations. It will take a broader application security program to ensure that consistently meeting those objectives becomes a 'business as usual' capability. Everyone must plan accordingly and cooperate in improving each stakeholder's ability to accelerate their part of the overall application security program.