IDC

DevSecOps: Critical Risk Reduction Leads to Better Business Outcomes

RESEARCH BY:

Jim Mercer
Research Director, DevOps and DevSecOps, IDC

December 2021 | IDC Doc. #US48346521

Navigating this White Paper

Click on titles or page numbers to navigate to each section.

IDC Opinion

IDC forecasts that by 2025, up to a quarter of Fortune 500 companies will shift from simply being consumers of software to being producers as well (see *IDC FutureScape: Worldwide Future of Digital Innovation 2021 Predictions*, IDC #US46417320, October 2020).

Becoming a software producer leads to software innovation that empowers organizations to create evocative customer experiences, obtain intelligence, and create platforms for future products and services. The desire for such outcomes is compelling organizations to adopt DevOps practices to enable them to succeed with digital transformation by improving the speed with which digital solutions can be brought to market.

The ripple effect of organizations' creating more software is that the application attack surface is rapidly expanding, and it has become a favored target of bad actors. Today, hacking tools and guides are readily accessible via an internet search, so bad actors no longer need to be knowledgeable software security experts—they simply need to be opportunistic.

While bad actors only need to win once, a single security breach can have catastrophic impacts on a business. The effects can be severe and often include the loss of and/or tampering with customer data, which substantially damages customer trust and brand reputation. Further, application outages while the breach is remediated will result in considerable revenue losses as impatient customers take their business elsewhere. If there is a reason to believe that an organization did not properly protect consumer data, there may be lengthy litigation, financial penalties, or even restitution payments to affected parties.

This concern is pressing organizations to look at their DevOps practices to examine how they can maintain the velocity of new application updates while reducing the risk of a security breach. This has led organizations to start adopting DevSecOps practices and tools. IDC defines DevSecOps as a methodology that asserts that security needs to be prioritized at the beginning of the DevOps delivery pipeline. It enables DevOps teams to act as key stakeholders in defining and implementing security policies (see *IDC's Worldwide DevOps and DevSecOps Software Tools Taxonomy, 2021,* IDC #US48033621, July 2021).

This IDC white paper reviews the results of the *DevSecOps Assessment Survey* of organizations actively pursuing and embracing DevSecOps practices. This study provides insights and tips that can assist organizations at all levels of DevSecOps maturity with improving their security capabilities.

Situation Overview

Summary of Findings

- DevSecOps is more than security tools, and much like DevOps, there is an important cultural aspect. You need to have the security, application development, IT operations, and DevOps teams working together to achieve success.
- DevOps provides the foundation for DevSecOps, and DevOps attainment is a leading indicator of future DevSecOps success.
- DevOps teams that take on more security ownership in collaboration with the security groups show greater DevSecOps maturity. The key is shared ownership across development, IT operations, and information security.
- Organizations adopting DevSecOps are struggling with tool sprawl and building the right stack of security tools to enable proper security due diligence and DevOps efficiency.
- With so many workloads shifting to both cloud deployments and Kubernetes orchestration platforms, organizations today want more integrated security included in their deployment platforms.

- As DevSecOps practices take hold and scale up in use, organizations recognize significant benefits across all levels of DevSecOps maturity. While the benefits of DevSecOps are larger at higher levels of maturity, even those organizations in the initial stages of their DevSecOps journey are recognizing tangible benefits.

Key Business Discoveries

- Organizations using DevSecOps have realized improved operational efficiency and employee productivity.
- Organizations using DevSecOps indicated that it has resulted in stronger customer satisfaction and retention as well as helped accelerate the acquisition of new customers.
- DevSecOps is enabling organizations to reduce their operational risk and improve their ability to adhere to regulatory compliance.

Drivers for Adopting DevSecOps

We found that multiple factors were propelling organizations to shift security further to the left and adopt DevSecOps, such as DevOps efficiency, application security, and modernization of applications and platforms.

Predominantly, *DevSecOps Assessment Survey* respondents indicated that the primary factor for integrating security with DevOps — aka DevSecOps — was to improve the holistic security posture of their applications, with 48% overall selecting application security as a primary driver.

DevSecOps is all about improving security, but with faster speed and efficiency. Confirming that position, 45% of respondents identified faster development and deployments while maintaining security as a principal driver. The importance of not slowing down DevOps teams while upholding application security is an essential component of DevSecOps.

Shifting security to the left proposes introducing security checks and work during the development phase or even earlier.

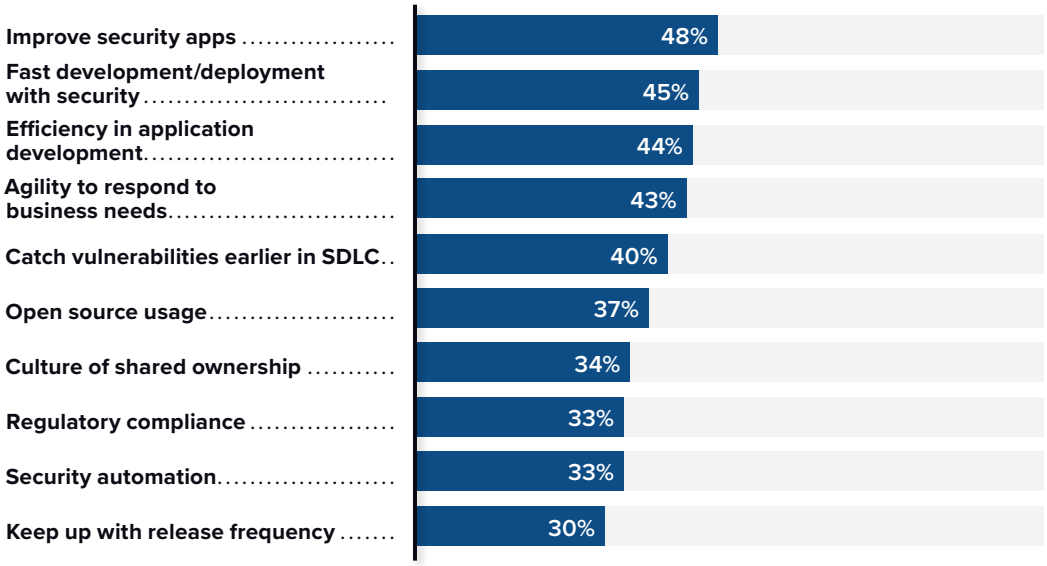
Survey respondents also called out the significance of shifting security further to the left as a key driver (see **Figure 1**), with 40% of respondents identifying that catching security vulnerabilities earlier in the software delivery life cycle (SDLC) is vital to their operations. Shifting security to the left proposes introducing security checks and work during the development phase or even earlier. The object is to ensure that the code base is designed to be secure from the start, rather than checking for security issues at the end of the development process, where it is more costly. This requires integrating DevSecOps tools into the DevOps pipeline in an automated manner.

FIGURE 1

Primary Drivers for Shifting Security Left

Q. What are the primary factors driving your organization to consider increasing the integration of security with DevOps? (Select all that apply.)

(% of respondents)



Source: IDC's *DevSecOps Assessment Survey, 2021*

The migration toward modern cloud-native applications is an important driver for expanding automated DevSecOps security processes, and regular scrutiny is vital to address the challenges of securing an ephemeral cloud environment that is in a state of perpetual change. Cloud security was called out as both a necessity and a threat for organizations as they increase their use of cloud-native technologies.

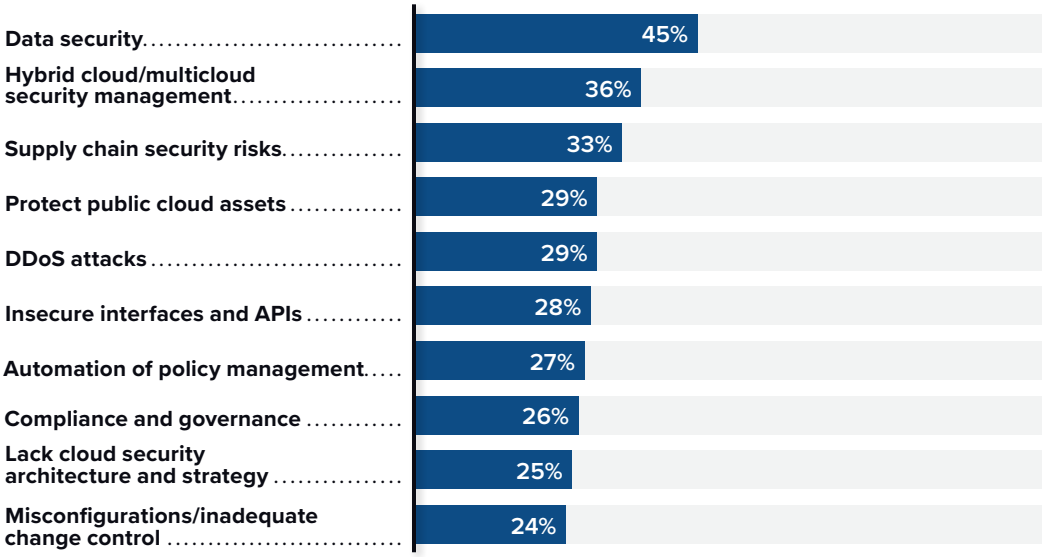
In **Figure 2** (next page), survey respondents called out key areas of security concerns as they shift their DevSecOps efforts toward the cloud. Overall top four areas of concern included data security (45%), hybrid cloud/multicloud security management (36%), supply chain security risks (33%), and protecting public cloud assets (29%).

FIGURE 2

Most Concerning Security Challenges

Q. What types of security challenges are you most concerned about as part of a shift toward running in the cloud (public, private, hybrid, or multi)? (Select all that apply.)

(% of respondents)

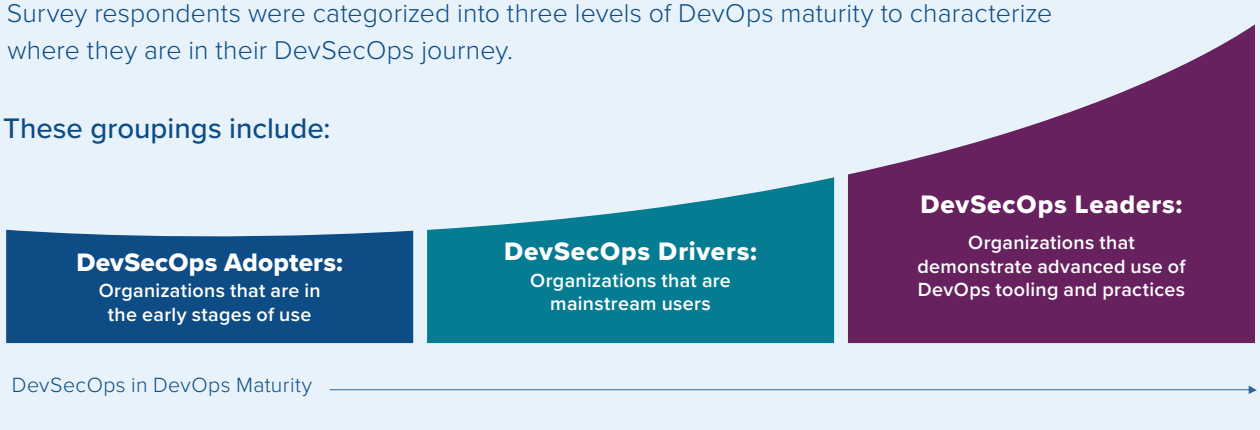


Source: *DevSecOps Assessment Survey,* 2021

Identified Levels of DevSecOps Maturity

This white paper is based on survey responses from organizations across the globe demonstrating various levels of DevSecOps proficiency. The survey responses were further analyzed to identify distinct DevSecOps maturity cohorts. This segmentation helped reveal what types of actions an organization might take at various stages of DevSecOps maturity to achieve higher levels of DevSecOps effectiveness and drive better outcomes. Survey respondents were categorized into three levels of DevOps maturity to characterize where they are in their DevSecOps journey.

These groupings include:



DevSecOps Adopters

Early-stage adopters of DevSecOps practices, described as DevSecOps Adopters, are more likely to be focused on the initial integration of security into the DevOps pipeline as part of an early shift-security-left effort and constitute 25% of organizations.

DevSecOps Adopters are less mature in their DevOps capabilities, with 70% indicating that they have 50% or fewer applications using DevOps for application development. These organizations are typically in the initial stages of DevSecOps maturity, with only 9% considering security as part of application design.

For these organizations, security tools are not well integrated into the DevOps pipeline, with 34% reporting low to moderate levels of security automation,

while 45% indicated that they see the security and operations teams as primarily responsible for application security testing. Also, just 17% indicated that they are concerned with governance and compliance, implying that this is not yet in their purview.

DevSecOps Adopters were less apt to be using cloud-native technologies, with 35% indicating that they have integrated containers into their application development and 41% indicating that their applications are using public cloud services.

DevSecOps Adopters were less apt to be using cloud-native technologies, such as integrating containers into their application development and using public cloud services.

DevSecOps Drivers

DevSecOps Drivers were the largest cohort and are made up of organizations that are further along in their DevSecOps journey when compared with the Adopters. For DevSecOps Drivers, application and operational security have become more pervasive, and there is generally an increased focus on improving software security and adopting secure coding practices (50% of organizations).

DevSecOps Drivers were already well along the DevOps and DevSecOps adoption path, with 91% rating their infrastructure-as-code (IaC) capabilities as intermediate to advanced. Analysis shows that 45% indicated that increased efficiency in software development along with faster deployments are driving them to expand the integration of security into their DevOps pipelines.

Drivers also demonstrated higher levels of automation, with 31% indicating that they are using automation to avoid human errors and 30% indicating that they are trying to automate the patching of security vulnerabilities to ensure swift remediation of reported vulnerabilities.

One of the distinguishing characteristics of the DevSecOps Drivers is their tendency to take greater ownership of the security of their applications, with 53% seeing developer and DevOps teams as primarily responsible for application security testing.

DevSecOps Drivers tend to take greater ownership of the security of their applications, seeing developer and DevOps teams as primarily responsible for application security testing.

DevSecOps Leaders

DevSecOps Leaders demonstrated higher levels of DevSecOps adoption and optimization, with progressively ambitious standards for secure software code and quality, along with a more focused approach to governance and compliance (25% of organizations).

Leaders have a sound DevOps foundation, with 71% indicating that 51–100% of their applications are using DevOps as a methodology for application development and 100% of their new applications in initial development are using DevOps.

DevSecOps Leaders showed deeper DevSecOps maturity, with 58% incorporating security before QA testing and 30% inserting security into the planning and design phases of application development. Also, 53% of this group attest that they have been on their DevSecOps adoption path for three-plus years.

DevSecOps is done at a greater scale among this group, with DevSecOps Leaders reporting the highest levels of automation within the DevOps pipeline across all of the tooling areas, for an overall average of 73% of DevSecOps tools being fully driven by automation.

DevSecOps Leaders are more concerned with higher-level issues such as protecting their applications in the public cloud (49%) and improving automation and controls around compliance and governance (38%).

DevSecOps Leaders are more concerned with higher-level issues such as protecting their applications in the public cloud and improving automation and controls around compliance and governance.

Organizational Learnings

Culture

Like DevOps, the most essential elements of DevSecOps are not tools and technologies but the fostering of a culture where security is important throughout the application life cycle, with ownership shared across teams and domains. Cultural resistance is, uniformly, the leading inhibitor of DevSecOps success. **Figure 3** (next page) shows that resistance from within the organization is the most significant impediment toward building a DevSecOps culture.

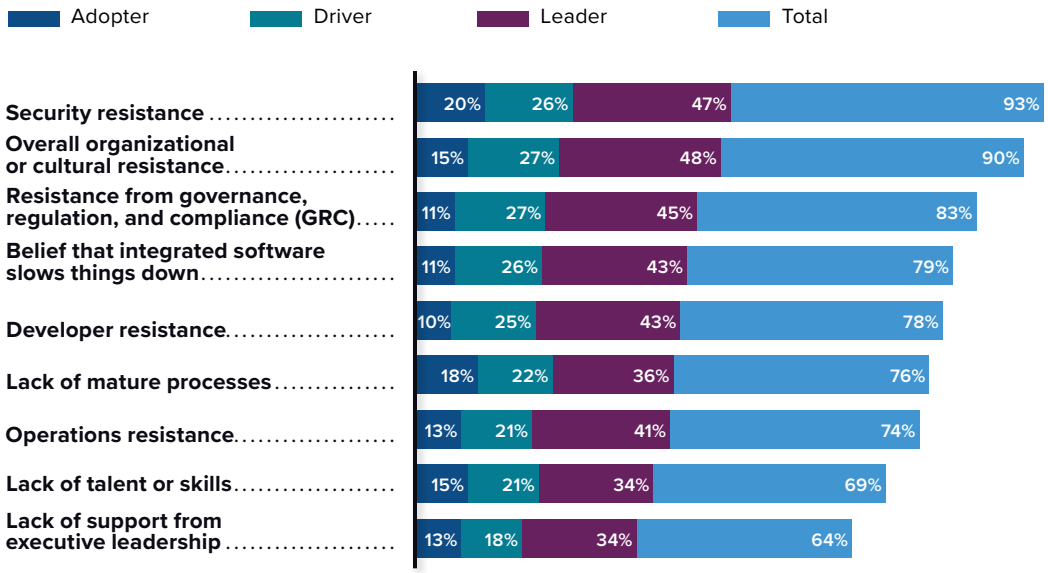
Cultural resistance is, uniformly, the leading inhibitor of DevSecOps success.

FIGURE 3

Significant Obstacles to Integrating Security with DevOps

Q. Which of these are significant obstacles to the organization's increasing the integration of security with DevOps? (Select all that apply.)

(% of respondents)



Source: *DevSecOps Assessment Survey,* 2021

Increasing cultural collaboration across silos is key, and 34% of *DevSecOps Assessment Survey* respondents identified building a culture of shared ownership between their application development and security teams as one of the primary factors for increasing the integration of security with DevOps.

Collaboration is enhanced by shifting security to the left and integrating security early in the DevOps pipeline. In **Figure 4** (next page), the *DevSecOps Assessment Survey* depicts how DevSecOps Leaders, at 72%, were more than five times more likely to have security completely integrated into the DevOps pipeline as compared with DevSecOps Adopters (14%).

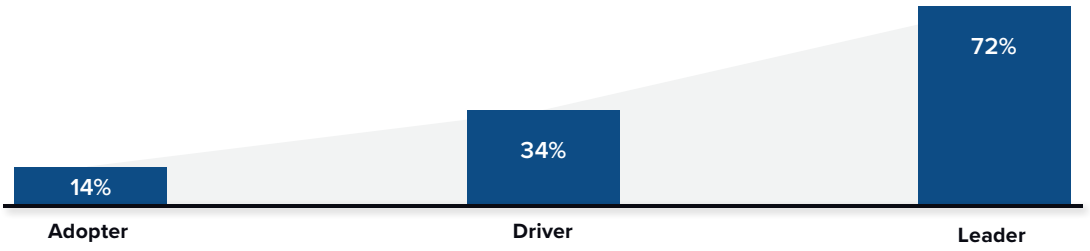
Integrating security into the DevOps pipeline, making it more visible to DevOps teams, can help organizations incent developers to get better educated on what it takes to write secure code.

FIGURE 4

Depth of Security Integration by DevSecOps Maturity Level

Q. Currently, how deeply does your organization integrate security with DevOps?

(Depth of integration)



Source: *DevSecOps Assessment Survey,* 2021

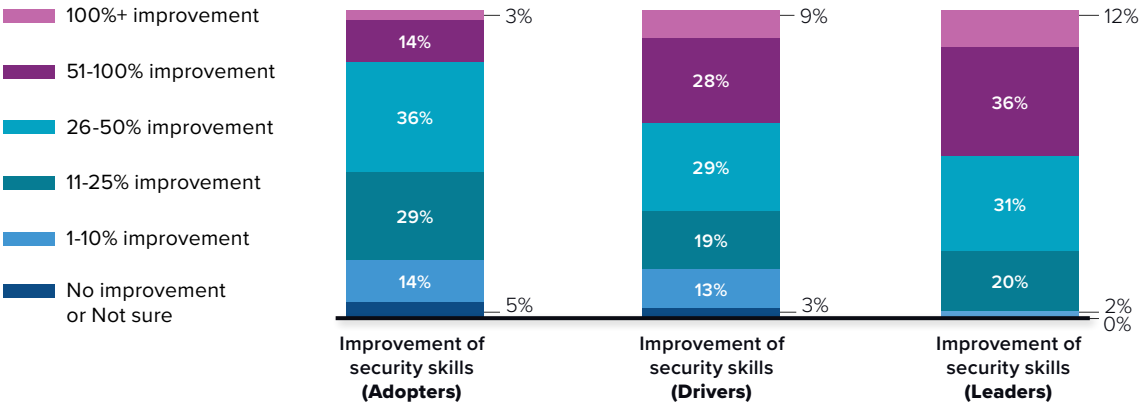
Integrating security into the DevOps pipeline, making it more visible to DevOps teams, can help organizations incent developers to get better educated on what it takes to write secure code. When asked for the levels of improvements that their organizational metrics had captured since adopting DevSecOps, in **Figure 5**, 66% of respondents indicated that the advancement of security skills has improved by 26% or more, and for the DevSecOps Leaders cohort, the improvement in security aptitude jumped to 78%.

FIGURE 5

Improvement of Security Skills by DevSecOps Maturity Level

Q. What level of improvement has the organization seen in each of these metrics or KPIs over the past two years?

(% of improvement)



Source: *DevSecOps Assessment Survey,* 2021

Further, DevOps and security teams that have a culture of strong organizational support for integrating security into their DevOps processes are better positioned for success. In IDC's *DevSecOps Assessment Survey*, 70% of the DevSecOps Leaders stated that they had complete organizational support for DevSecOps compared with only 16% of DevSecOps Adopters.

Key Business Discoveries

While the technical and security aspects of DevSecOps adoption and maturity may be well understood, the *DevSecOps Assessment Survey* also revealed key business benefits realized by organizations that adopt DevSecOps.

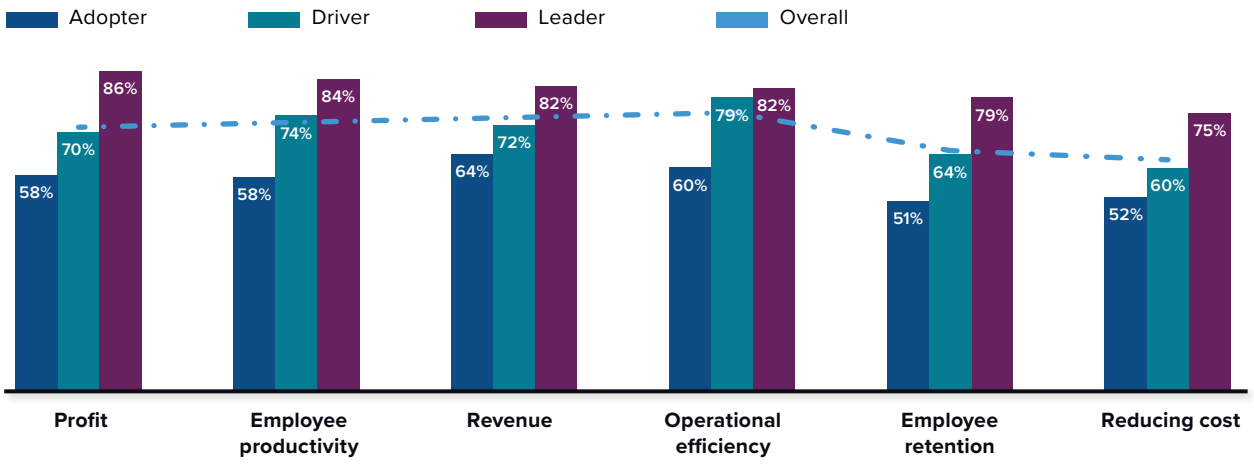
Commercially, survey respondents attributed their investments in DevSecOps security to bottom-line improvements in operational efficiency (75%) and profits as well as top-line increases in business revenue (73%).

Figure 6A presents benefits that organizations experience from the adoption of DevSecOps, parsed by adoption maturity. Further, DevSecOps was attributed to improvements in employee productivity (73%), and a likely ripple effect of enhanced productivity is a more content workforce. Amid a tight labor market for software developers and security professionals, maintaining talent is vital for business success and creativity. In addition, 65% of survey respondents indicated that investments in security supporting DevSecOps improved employee retention, and for DevSecOps Leaders, that metric jumped to 79%.

FIGURE 6A

Business Benefits by DevSecOps Maturity Level

Q. As a result of investments in security, has your organization improved each of the following?
(% of improvement)



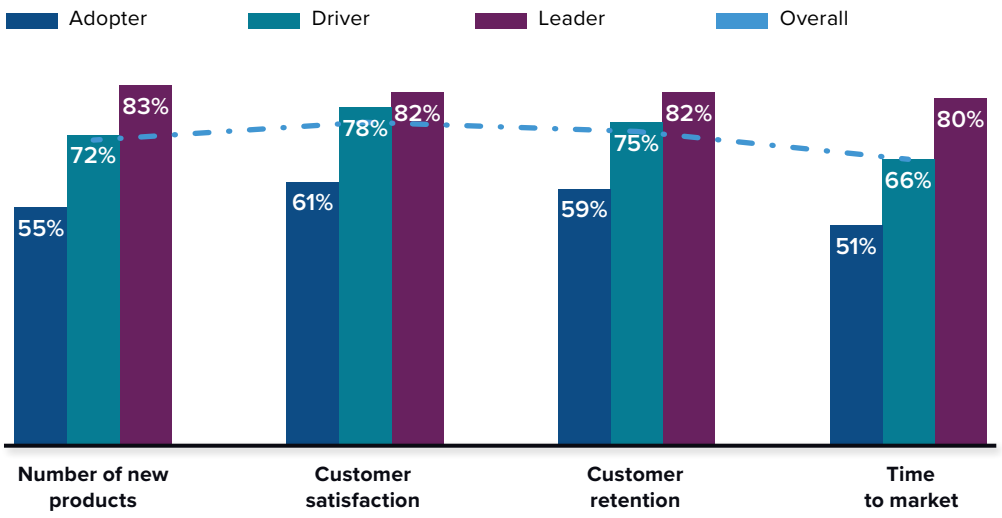
Source: *DevSecOps Assessment Survey,* 2021

Turning to **Figure 6B**, we consider metrics that directly affect the customer experience. DevSecOps was attributed to improving customer experience, retention, and value delivery. A majority of the total pool of respondents (75%) indicated that their adoption of DevSecOps security was improving customer satisfaction, and 73% of respondents indicated that it has enhanced their ability to retain their existing customers. In addition, using DevSecOps was attributed to helping organizations deliver more value to their customers via faster time to market (66%) and improving their ability to bring new products and services to market (71%).

FIGURE 6B

Customer-Facing Improvements by DevSecOps Maturity Level

Q. As a result of investments in security, has your organization improved each of the following?
(% of improvement)



Source: *DevSecOps Assessment Survey,* 2021

Using DevSecOps was attributed to helping organizations deliver more value to their customers via faster time to market and improving their ability to bring new products and services to market.

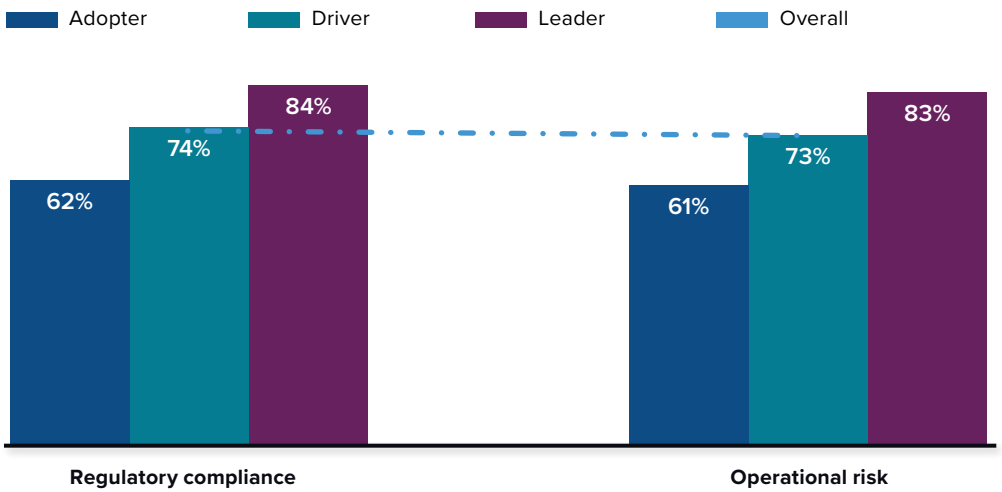
Likewise, **Figure 6C** shows that survey respondents identified that DevSecOps played a role in improving their business risk and compliance, with 72% of the total survey sample indicating that DevSecOps reduced operational risk and 74% indicating that it enabled better regulatory compliance.

FIGURE 6C

Risk and Compliance Improvements by DevSecOps Maturity Level

Q. As a result of investments in security, has your organization improved each of the following?

(% of improvement)



Source: *DevSecOps Assessment Survey,* 2021

Quantifiable Business Benefits at All Levels of Maturity

Organizations that have demonstrated DevSecOps leadership are gleaning the most benefits from their investments; however, respondents in the Adopter and Driver groupings also reported measurable progress in multiple business dimensions. Often, organizations in the initial stages of DevSecOps adoption presume that tangible benefits from their early efforts in adopting DevSecOps will not be realized until some later date. However, this survey data strongly suggests that presumption is incorrect, as the data collected across the different maturity levels indicates that organizations in each group reported measurable DevSecOps benefits.

As DevSecOps practices take hold and scale, organizations recognize significant benefits across all three levels of DevSecOps maturity.

Driving DevSecOps Across Your Organization

Although we have categorized survey respondents into three distinct levels of DevSecOps maturity, organizations should tailor their approach to DevSecOps adoption so that it aligns with their culture, current capabilities, and identified security gaps and risks impacting their business. Organizations in the DevSecOps Adopter and Driver cohorts reported some of the same attributes of DevSecOps Leaders, but the remaining gaps constrict overall maturity and attainment.

There are well-documented models for building maturity across the security community, such as the Capability Maturity Model Integration (CMMI) and the Building Security in Maturity Model (BSIMM), but organizations still struggle to get their DevSecOps journeys started. However, *DevSecOps Assessment Survey* revealed that there are some common key ingredients for successfully driving a DevSecOps initiative that can be used by any organization.

The *DevSecOps Assessment Survey* shows an unequivocal correlation between DevOps adoption and DevSecOps success. The hallmark of DevOps is a collaborative agile software development methodology that breaks down boundaries between domains and leverages automation to improve efficiencies, repeatability, quality, and velocity. In fact, 55% of DevSecOps Leaders indicated that building a culture of shared ownership between application development and security teams was critical. DevSecOps builds upon DevOps, expanding on the collaborative culture and shifting security to the left of DevOps by integrating security scanning and automation into established DevOps processes.

The hallmark of DevOps is a collaborative agile software development methodology that breaks down boundaries between domains and leverages automation to improve efficiencies, repeatability, quality, and velocity.

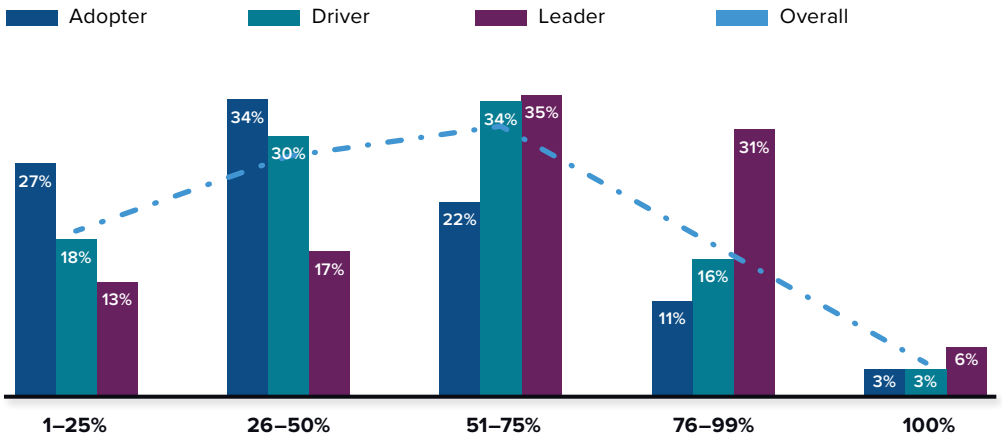
The foundational requirement of an established DevOps platform became clearer in the *DevSecOps Assessment Survey* results (see **Figure 7**). When survey respondents were asked about how deeply DevOps had been integrated into their production applications, almost 71% of the DevSecOps Leaders cohort and 53% overall indicated that over 50% of their production applications were using DevOps.

FIGURE 7

Production Applications Using DevOps by DevSecOps Maturity Level

Q. Apps in production: What proportion of each of these types of applications uses a DevOps methodology?

(% of improvement)



Source: *DevSecOps Assessment Survey,* 2021

Achieving organizational support for DevSecOps across the leadership of the development and security teams is critical. Sixty-four percent of survey respondents called out the lack of support from leadership as a key inhibitor to success.

The survey data demonstrates an understanding that DevSecOps adoption is a continuous process that is iterative and takes time to fully achieve. For example, 72% of DevSecOps Leaders responded that security, developers, IT, and business stakeholders continually work together to ensure security by design and throughout the software development process, while only 9% of DevSecOps Adopters are incorporating security into the design phase of the overall SDLC. However, these increased levels of maturity come with time as organizations hone their DevSecOps capabilities. The survey data shows that 53% of DevSecOps Leaders have been using DevSecOps for three-plus years, compared with just 20% of DevSecOps Adopters.

Future Outlook

The proliferation of new applications and application updates has made the application attack surface a preferred target for hackers.

According to the *2021 Mid-Year Data Breach QuickView Report* by Risk Based Security (the owners of the vulnerability database VulnDB), there were 1,767 publicly reported breaches in the first six months of 2021 alone. Every day, cybersecurity threats increase, while modern cloud-native application technologies are adding new complexities and endpoints.

For security and DevOps teams, the rate of change is outstripping their ability to stay ahead of the risks. Fifty-four percent of *DevSecOps Assessment Survey* respondents indicated that they are not confident or somewhat confident that their organization has selected the best security tools to use in a modern DevOps environment—and this lack of confidence grows to 62% for DevSecOps Leaders, indicating a need for better tooling to fight the growing security threats.

The market is being flooded by new DevSecOps tools, and the *DevSecOps Assessment Survey* indicates that organizations are finding the cacophony of different security tools to be intractable. They want their security tools to be more seamlessly integrated into the cloud platforms where they will be running their workloads. When asked whether their primary cloud container platform provides enough security tools for DevOps, 28% responded that it did not and 45% indicated that more security tools need to be incorporated into the platform.

Increased Focus on Security

With increased and more impactful cybersecurity breaches taking place routinely, we are seeing more pressure for tighter security controls from governments and partners. Most recent is the U.S. Cybersecurity Executive Order 14028, which states that the prevention, detection, assessment, and remediation of cyberincidents are a top priority and are essential to national and economic security. This executive order directly affects U.S. government agencies and will have a trickle-down effect on the private sector. Not surprisingly, 34% of *DevSecOps Assessment Survey* respondents called out the challenges of meeting regulatory compliance as a driving factor for integrating security into their DevOps processes.

The ability for organizations to keep up with cyberthreats will only get more complex as more applications are shifted to the cloud using cloud-native technologies. The inability of organizations to handle security policy management along with the failure to quickly patch security vulnerabilities is creating potential gaps and exposures in their application security.

Recognizing these issues, IDC forecasts that the DevSecOps tools market will continue to grow with a 24% CAGR over the next five years (see Worldwide DevSecOps Software Tools Forecast, 2021–2025, IDC #US48052421, July 2021).

The market is being flooded by new DevSecOps tools, and the *DevSecOps Assessment Survey* indicates that organizations are finding the cacophony of different security tools to be intractable.

Challenges and Opportunities

Integration of Security with DevOps Team

Challenge: Forty-eight percent of DevSecOps Leaders and 29% overall called out overall organizational or cultural resistance as a significant obstacle to the organization's increasing the integration of security with DevOps teams.

Opportunity: Ninety-nine percent of DevSecOps Leaders rated their overall level of support across the organization for the integration of security with DevOps as strong or complete support, and 34% indicated that lack of support from executive leadership would be a significant obstacle for their DevSecOps success. This signifies that support from executive leadership is vital for overcoming the organizational and cultural resistance that can stall efforts to integrate security into DevOps pipelines.

Selecting the Right Security Tools for the DevOps Team

Challenge: Ninety-four percent overall responded that when DevSecOps was first adopted, it was challenging to select the right security tools for the DevOps teams to use, and 55% overall indicated that they still lack confidence in the assortment of security tools they are using as part of their DevSecOps adoption.

Opportunity: Twenty-one percent overall responded that they prefer to consume DevSecOps tools from their cloud provider, and 17% indicated that they are looking to their container/Kubernetes platform for DevSecOps security tools. This demonstrates that organizations running workloads in the cloud and using DevSecOps want to leverage platform-provided tools to help standardize and modernize security tooling. This is an opportunity for platform providers to be more aggressive about providing DevSecOps capabilities across the DevOps pipeline, which will make it easier for consumers as they shift more workloads onto cloud platforms.

Absence of Security Talent and Skills

Challenge: Twenty-three percent overall called out the absence of security talent and skills as a significant obstacle as they scale out DevSecOps, and 32% indicated that this lack of security skills in the organization is the biggest exposure as application development shifts toward the public cloud platforms and cloud-native applications.

Opportunity: Thirty-four percent overall stated that they are actively empowering DevOps teams to take on more ownership of security. Twenty percent indicated that they are increasing secure coding training and awareness for development and DevOps teams, and 32% indicated they are tracking improvement of staff security skills as a KPI. Forty-six percent stated that as part of DevSecOps adoption, they have seen improvements in the security skills of their teams. This demonstrates that the combination of increased security ownership and training in secure coding leads to greater security awareness, culminating in improved security skill levels for developers and DevOps teams.

Conclusion

In today's digital economy, where bad actors are both better equipped and more emboldened than ever, organizations can benefit by adopting DevSecOps technologies and practices.

The benefits are not isolated to DevOps and security teams but extend to your customers, with measurable improvements to the business bottom and top lines along with reduced risk, improved agility, employee satisfaction, and product quality. Shifting security to the left of the DevOps pipeline, via DevSecOps, is now essential due diligence for competing in the modern digital economy.

Today, many organizations in the initial stages of DevSecOps adoption are still moving too slowly and are not prioritizing the maturity of their application security capabilities. The findings of this study suggest that they should be accelerating DevSecOps adoption. Ironically, once these same organizations experience a security breach, they tend to move with a maniacal sense of urgency.

Organizations operating in the digital economy need a strong application security defense and should be improving their DevSecOps maturity with the same speed and urgency as if they had suffered a security breach: Bad actors are opportunistic, and the risk of a cyberattack is real—they only need to win once for your business to be debilitated.

Methodology

This white paper is based on the *DevSecOps Assessment Survey* conducted by IDC on behalf of Red Hat. The survey participants came from across the globe and included respondents from the following countries: Australia, France, Germany, India, Malaysia, New Zealand, Singapore, the United Kingdom, and the United States. Participants hailed from the following industries: financial services, government, healthcare, infrastructure, manufacturing, telecom, and utilities. A cross section of 806 survey respondents served in roles such as IT architecture, application development, cloud infrastructure/operations, DevOps, and security. All survey participants reported that they are decision makers or influence decisions surrounding IT security.

About the Analyst

Jim Mercer
Research Director, DevOps and DevSecOps, IDC

Jim Mercer is a research director within IDC's DevOps Solutions research practice. In this role he is responsible for researching, writing, and advising clients on the fast-evolving DevOps market. Jim's core research includes topics such as rapid enterprise application development, modern microservice-based packaging, application security, and automated deployment and life-cycle management strategies as applied to a DevOps practice. In addition, he examines how the move to DevOps methodologies impacts enterprise use of open source and preferences for using on-premises computing and development platforms versus public cloud services. He looks at how organizations are prioritizing DevSecOps and using automation to insert security assessments at the beginning of the DevOps delivery pipeline (i.e., shift left). Jim advises senior IT, business, and investment executives globally in the creation of strategy and operational tactics that drive the execution of digital transformation and business optimization.

More about Jim Mercer

IDC Custom Solutions

This publication was produced by IDC Custom Solutions. As a premier global provider of market intelligence, advisory services, and events for the information technology, telecommunications, and consumer technology markets, IDC's Custom Solutions group helps clients plan, market, sell and succeed in the global marketplace. We create actionable market intelligence and influential content marketing programs that yield measurable results.