ANALYST BRIEF
Sponsored by: OpenText

**Through DevSecOps automation, organizations can develop and release higher-quality applications faster, seamlessly integrating security into the DevOps pipeline. This leads to the delivery of secure applications that mitigate the security risk to the business.**

# Achieving High-Velocity DevOps with Security Automation

*August 2024*

**Written by:** Jim Mercer, Program Vice President, Software Development, DevOps & DevSecOps

## Introduction

Software is fundamental to the success of modern digital businesses. It goes beyond being a mere backroom engine to becoming the backbone of operations, innovation, and customer engagement. Software drives efficiencies, automates processes, and enables the development of new products and services, making it an indispensable tool for achieving business goals.

In today's competitive landscape, software provides businesses with a crucial edge by allowing tailored solutions, enhanced data analytics, and customized experiences. This ability to adapt and innovate through software makes it an essential differentiator, helping digital businesses meet and anticipate market demands.

A recent IDC's *DevOps Survey* underscores the significant impact of DevOps on business value, with over 70% of respondents viewing it as a high or extremely high driver. This perception is supported by the frequency of software updates, reflecting the agility and efficiency that DevOps practices bring to organizations. Figure 1 shows that 39% of organizations release software updates weekly, while over 33% claim to release software daily/multiple times daily. These rapid release cycles enable businesses to quickly respond to market demands, fix issues promptly, and continuously improve their products, enhancing customer satisfaction in the fast-paced digital landscape.

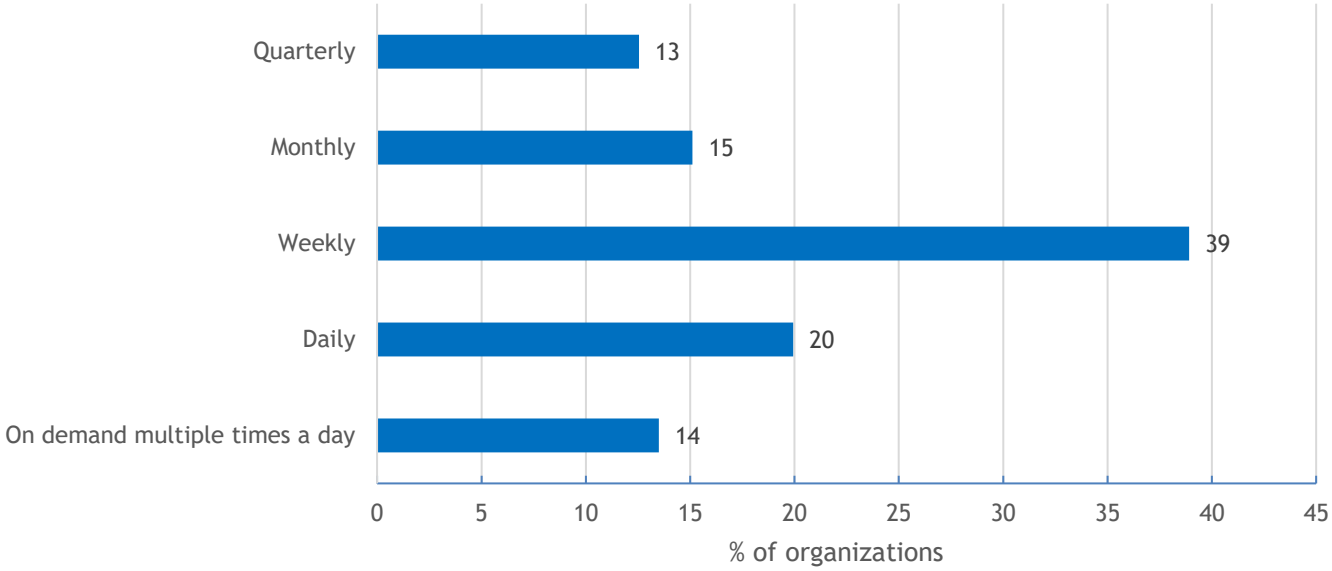
## AT A GLANCE

### KEY TAKEAWAYS

- As DevOps velocity grows, organizations are unable to evaluate software for security vulnerabilities, resulting in immature DevSecOps practices.
- The growing number of new applications fueled by end-user demand and generative AI (GenAI) coding assistants is only making the application security problem worse.
- With a modern DevSecOps automation platform, organizations can develop and release secure software while maintaining DevOps velocity.

FIGURE 1: ***Increasing Software Release Frequencies***

**Q *How often, on average, does your organization deploy code releases to production today?***




*n = 311*

*Source: IDC's DevOps Perceptions, Practices, and Tools Survey, November 2023*

Adopting GenAI code generators significantly accelerates the development of new applications and releases. By automating and enhancing coding processes, GenAI can reduce development time, leading to software being developed more quickly and with less human oversight. An IDC's *GenAI Survey* revealed that 46% of respondents are either expanding their use or piloting GenAI within their DevOps pipelines, underscoring the growing recognition of its value.

As the reliance on software applications intensifies, IDC forecasts that over 1 billion net-new applications will be developed by 2028. This explosive growth in the application landscape presents a lucrative target for bad actors that are becoming increasingly sophisticated in their methods. With more applications comes a larger attack surface, providing more opportunities for cyberthreats, vulnerabilities, and breaches.

From 2022 to 2023, IDC survey data revealed a 21% increase in security breaches and a 241% rise in reported software supply chain attacks, with 64% of respondents affected by open source software vulnerabilities. Even the most technically capable companies are susceptible, exemplified by AT&T's 2024 acknowledgment that hackers accessed six months of customer call data. Almost every day, we learn about a company that has been breached, and many of us have already received notifications from companies we do business with that our data has been compromised.

## *Prevailing Lack of DevSecOps Maturity*

The harsh reality is that most organizations struggle to keep up with the demands of modern digital business. IDC data shows that only 24% of organizations have automated code scans to ensure they are run before production, and only

41% of applications utilize DevSecOps. This lag in application security maturity results in software regularly being released into production with known security defects to meet end-user demand.

The lack of DevSecOps maturity and an expanding application attack surface significantly increase business risk. Innovations and new applications are undermined if they carry security vulnerabilities and potential compliance violations. These security concerns pose substantial risks, potentially halting digital innovation and jeopardizing business integrity and objectives.

Consequently, robust security measures become paramount as organizations strive to protect their data and systems. Security is critical to maintaining trust and protecting against disruptions and losses from malicious activities.

Modern digital organizations require access to advanced tools that facilitate DevSecOps automation. These tools ensure robust application security while maintaining the rapid pace of software updates.

The harsh reality is that most organizations struggle to keep up with the demands of modern digital business. IDC data shows that only 24% of organizations scan code before production, and 41% of applications utilize DevSecOps.

## Benefits

### Security That Enables DevOps Velocity

DevSecOps automation allows organizations to develop and release higher-quality applications more swiftly by integrating security seamlessly into the development process. This approach automates security checks, code analysis, and vulnerability assessments throughout the DevOps pipeline, ensuring potential issues are identified and addressed early without slowing down the development cycle. By embedding security into every stage of the development and deployment process, automation enhances the efficiency and reliability of software releases, enabling teams to maintain velocity while ensuring security and compliance. Ultimately, it results in faster delivery of secure, high-quality applications that meet market demands and mitigate risk.

Automating security involves integrating automated security measures into the DevOps CI/CD pipeline and treating security checks akin to automated unit tests or integration tests. By embedding security testing into this workflow, organizations can ensure that security measures are consistently applied throughout the development life cycle, identifying vulnerabilities early and enabling rapid remediation.

By using an automated approach to application security, DevSecOps becomes an integral part of the development process rather than a separate phase, ensuring that security checks and remediation happen concurrently with development activities. This approach enhances overall system security and promotes a proactive stance toward addressing potential threats before they impact production environments. As a result, organizations can still maintain accelerated software delivery while ensuring that security standards are consistently met and potential vulnerabilities are addressed promptly.

For example, automating static or dynamic analysis streamlines the process of detecting security vulnerabilities in source code, significantly reducing the manual effort required for security assessments. This automation shortens code reviews, security assessments, and testing times while lowering remediation costs by identifying vulnerabilities early in the development cycle when addressing them is significantly less costly.

### *Business Optimization*

DevSecOps automation offers significant intrinsic benefits to businesses by integrating security measures directly into the development process, such as:

False negatives are more concerning, as genuine security threats are overlooked, leaving applications, businesses, and customers vulnerable to attacks.

» **Efficiency**

- **Reduces manual work:** Automating repetitive security checks throughout the DevOps pipeline frees up developers and security professionals to focus on more strategic tasks, leading to faster development cycles and quicker time to market for new features.
- **Swivel chair effect:** Automation eliminates the need for manual context switching between security and development tools, improving developer flow, minimizing delays and bottlenecks in the development process, and contributing to developer satisfaction.
- **Human error:** Automation minimizes the chance of a human error that can often be overlooked.
- **Improved collaboration:** Developers and security teams get a shared view of security risks, promoting a culture of "security by design," where security is an integrated part of the development process, not an afterthought. This application security mindset leads to a more security-conscious development team.

» **Cost reductions**

- Early detection and remediation of vulnerabilities diminish the likelihood of costly security breaches and data leaks.
- The increased productivity of development and security teams allows them to focus on the most critical security issues without getting overwhelmed.

» **Reduced risk**

- Integrating security checks into early development stages helps ensure vulnerabilities are identified and addressed sooner and prevents them from propagating to later stages, reducing the risk of costly exploits.

## *Considerations*

### *Achieving DevSecOps Automation*

Planning application and infrastructure security from the outset is crucial for building resilient systems. By incorporating security considerations early in the design and development phases, organizations can proactively identify potential vulnerabilities, establish security policies, and implement protective measures before they become significant issues.

A proactive approach involves designing secure architectures and integrating security controls into development workflows. By embedding security into the planning stage, organizations can avoid costly retrofits and disruptions, ensure compliance with regulatory requirements, and create a strong foundation that supports long-term security and operational integrity throughout the application's life cycle.

Fostering a culture of close collaboration among development, operations, and security teams is essential, as technology alone cannot guarantee adoption without people's engagement. Emphasizing security as a collaborative effort rather than a roadblock is crucial for success.

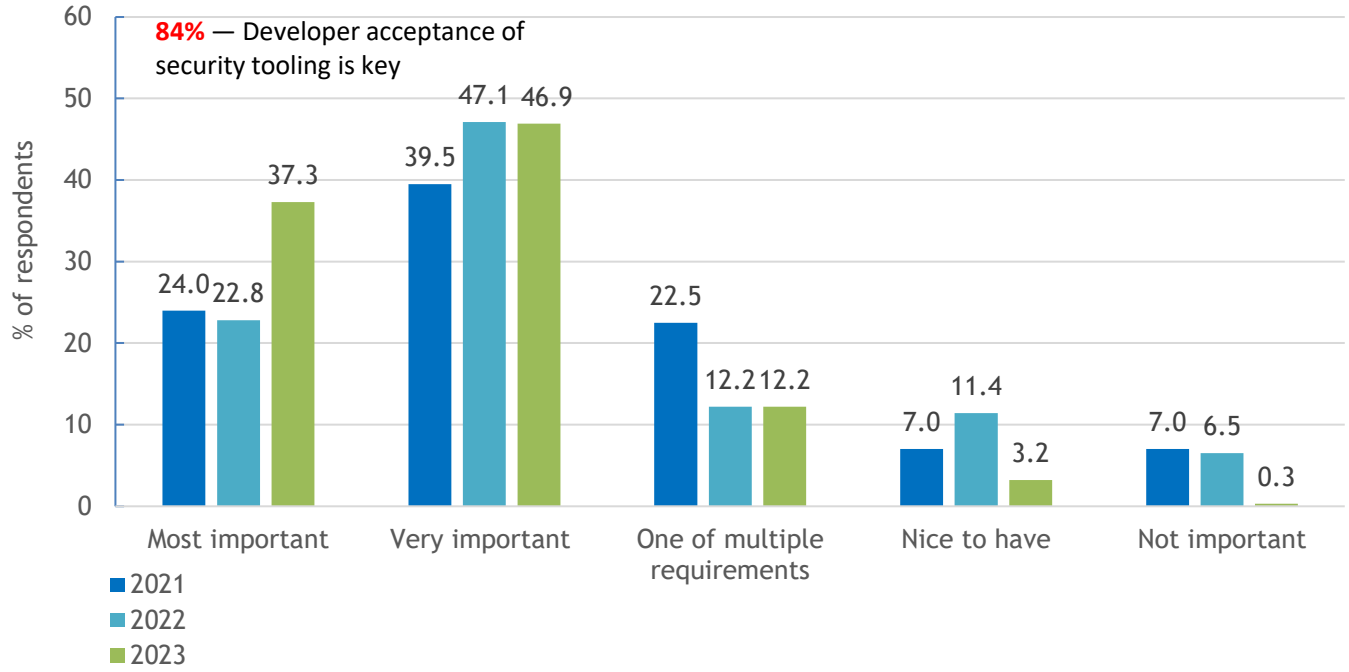
The emerging focus on using platform engineering teams can help facilitate this shift via secured paved paths for developing applications, ensuring that security is prioritized throughout the development life cycle and seamlessly integrated into processes.

Ongoing education and training for all teams involved in the DevSecOps process is crucial for maintaining security standards. Training should be interactive and available on demand, focusing on explaining security issues in terms developers can understand and related to the code they are working on. Developers and operators must have foundational knowledge of security best practices and know how to use automated security tools effectively.

DevSecOps tools should cater to developers' needs. By default, developers perceive that integrating security will slow their code delivery and waste time, forcing them to comb through verbose security findings and chase false positives. Figure 2 shows that 84% indicate that developer acceptance of DevSecOps tools is vital for adopting DevSecOps, and this sentiment has grown year over year.

FIGURE 2: ***Developer Acceptance of DevSecOps Tools Is Critical***

**Q** ***How important has developer acceptance of security tooling been as part of your adoption of DevSecOps?***




*n = 311*

*Source: IDC's U.S. DevSecOps Adoption Survey, January 2023*

So developer acceptance of application security tools is essential for effective security integration and should be prioritized to maintain security and development efficiency. This is not a nice to have, but a must-have to ensure DevSecOps success.

In the same way that legacy tooling impacts developers, security teams find themselves outnumbered and ill-equipped to keep pace with and ensure developers adhere to application security policies. Without an automated DevSecOps toolbox that allows them to set rules and security guardrails that can encompass the SDLC, they are fighting a losing battle. In response, they will work to slow things down, making it difficult to get buy-in from developers.

### *Automation-Enabled Tools*

Effective DevSecOps integrates security practices into the DevOps workflow, emphasizing automation to enhance software security. However, this approach to automation requires a DevSecOps platform of tools purpose built for integration into a modern DevOps pipeline.

DevSecOps tools must be easily automatable and seamlessly integrated into developer workstreams and the broader DevOps pipeline. Many organizations have utilized traditional security tools such as static application security testing

(SAST) and dynamic application security testing (DAST) for years. However, these legacy tools often lack integration with modern DevOps processes, leading to friction and inefficiencies.

Moreover, the accuracy and depth of security findings are crucial to the effectiveness of DevSecOps tools. Tools that generate many false positives can waste valuable developer time, leading to frustration and potential oversight of important security alerts. False negatives are more concerning, as genuine security threats are overlooked, leaving applications, businesses, and customers vulnerable to attacks.

DevSecOps tools must offer comprehensive security analysis that balances speed with thoroughness, precision, and actionable insights to maintain robust application security without compromising efficiency.

A modern automation-enabled DevSecOps platform should include the following:

- Documented APIs using OpenAPI Specs ensure comprehensive and easy-to-understand documentation. APIs enable developers and platform teams to integrate DevSecOps with custom tools and workflows within the DevOps pipeline and customize them to fit the organization's specific security needs.
- Out-of-the-box integrations with common DevOps tools (e.g., Jenkins and Jira), version control systems (e.g., Git), major cloud providers, and developers' integrated development environments (IDEs).
- Security policy management enables the creation and enforcement of security policies within the DevSecOps pipelines that align with the organization's overall security posture. For example, the organization's compliance and security standards define custom rules that map to and enforce specific security checks.
- Modern application environments are often polyglot, so the platform must support various programming languages and package managers.
- Data fidelity between security testing domains should provide a true picture of risk rather than just a myopic view of reality.

## Trends

DevSecOps automation is evolving rapidly, with two key trends enhancing the integration of security into development workflows. The first trend addresses tool sprawl and DevSecOps reporting toil by adopting full-featured DevSecOps platforms. This is closely followed by the impact AI is having on the capabilities of DevSecOps tools and what a DevSecOps platform will need to be able to secure.

### DevSecOps Platforms

The consolidation of DevSecOps tools into a unified DevSecOps platform represents a significant advancement in application security. Organizations can streamline their security efforts by integrating various security tools and processes into a single platform, reducing complexity and improving efficiency.

With a DevSecOps platform, visibility is usually enhanced using the available security dashboards, which are actionable by role and focus area. These dashboards provide tailored insights to various stakeholders and ensure that developers, security teams, and operations personnel can quickly identify and address security issues. This role-based customization streamlines the process of monitoring and mitigating risks, making security management more efficient and targeted.

This level of integration sets the foundation for improved prioritization of risk or what has been labeled application security posture management (ASPM).

### *The Impact of AI on DevSecOps*

AI-powered code fix suggestions and remediation tools revolutionize how developers handle security issues. By automatically identifying vulnerabilities and proposing fixes, these tools significantly reduce the time developers spend on remediation. They integrate seamlessly into their workflows for a frictionless experience, allowing them to focus more on innovation and less on manual security checks.

We are seeing increased interest in using GenAI to correlate and prioritize security findings and vulnerabilities. GenAI can analyze vast amounts of security data, identify patterns, and prioritize threats based on their potential impact, thereby enhancing the accuracy and efficiency of vulnerability management. Organizations can use this capability to allocate resources more effectively and address security issues more quickly. In addition, as machine learning operations (MLOps) and the development of large language models (LLMs) become more widespread, there is a growing need to protect these processes through MLSecOps.

## *Conclusion*

Software is fundamental to the success of modern digital businesses, serving as the underpinning of operations, innovation, and customer engagement. In a competitive digital landscape, software provides a crucial edge by enabling tailored solutions, enhanced data analytics, and superior customer experiences. However, security concerns pose substantial risks, potentially halting digital innovation and jeopardizing business integrity and objectives.

To move at the pace of DevOps, organizations need to embrace DevSecOps automation to reduce business risk and identify and address potential vulnerabilities early. Integrating modern DevSecOps security tools into the CI/CD pipeline allows businesses to detect and remediate issues quickly, reducing the downtime and costs associated with manual security fixes and incident responses. This continuous vigilance and rapid response capability helps maintain business continuity and safeguard against disruptions, further mitigating risks. By automating these processes, businesses can ensure their applications remain secure and compliant, defending against evolving threats and ensuring application resilience.

# About the Analyst

***Jim Mercer,*** *Program Vice President, Software Development, DevOps & DevSecOps*

Jim Mercer is a program vice president managing multiple programs spanning application life-cycle management (ALM), modern application development and trends, emerging generative AI software development, DevOps, DevSecOps, open source, PaaS for developers, and cloud application platforms. His focus areas are DevOps and DevSecOps Solutions research practices. In this role, he is responsible for researching, writing, and advising clients on the fast-evolving DevOps and DevSecOps markets.

## MESSAGE FROM THE SPONSOR

In today's fast-paced development environment, integrating security into every phase of the software development lifecycle is crucial. OpenText Fortify empowers organizations to seamlessly incorporate security within their DevSecOps practices, ensuring robust protection without compromising agility.

OpenText Fortify offers comprehensive application security testing solutions, including Static Application Security Testing (SAST), Dynamic Application Security Testing (DAST), and Software Composition Analysis (SCA). These tools help identify and remediate vulnerabilities early in the development process, reducing risk and enhancing code quality.

With automated code fix suggestions and automated SAST auditing, OpenText Fortify enables development teams to address security issues proactively. Our platform integrates smoothly with leading CI/CD pipelines, fostering a culture of shared responsibility for security across development, operations, and security teams.

Choose OpenText Fortify to secure your applications efficiently, ensuring your DevSecOps workflows are both agile and resilient against evolving threats.

IDC Custom Solutions

The content in this paper was adapted from existing IDC research published on www.idc.com.

**IDC Research, Inc.**
140 Kendrick Street
Building B
Needham, MA 02494, USA
T 508.872.8200
F 508.935.4015
Twitter @IDC
blogs.idc.com
www.idc.com