WHITE PAPER

# How Can You Benefit from Webhead's DevSecOps Process

Webhead

Web-Hed Technologies, Inc. (dba Webhead)
1710 N. Main Ave • San Antonio, Texas 78212 • (210) 354-1661 • webheadtech.com

## How Can You Benefit from Webhead's DevSecOps Process?

**DevSecOps stands for development, security, and operations. It's an approach to culture, automation, and platform design that integrates security as a shared responsibility throughout the entire software development and IT lifecycle. While digital transformation is changing how IT operates, security concerns continue to be top priority for non-profit, government, and B2B organizations.**

**In the past, software, security and operations were developed in three separate silos. With the DevSecOps approach, cybersecurity is integrated from the beginning to the end of the entire software and IT development process.**

**The cybercrimes and legal battles reported over recent years prove just how essential security is for organizations. The hack involving SolarWinds showcases the significance of securing every aspect of the software and IT product life cycle.**

**In other words, it is no longer enough to rely on frequent software updates. Organizations must endeavor to incorporate continuous integration and continuous delivery of security best practices – verifying the integrity of the code/script every step of the way. (Overall migrate to DevSecOps.)**

**So, what's driving this change? And what does it mean for organizations embracing it? This whitepaper talks you through DevSecOps and offers guidance on how to institute the same into your organization.**

## What's Driving the Change? The Market Demand for Speed and Innovation

In a dynamic marketplace, agility makes the difference between success and failure for most organizations. If a firm cannot seize the moment, get its new product in front of clients promptly; a nimble competitor will.

**Webhead understands the need to innovate more quickly to:**

i. Differentiate their offers; and,

ii. Gain a competitive advantage.

If your organization is not innovating fast enough, it risks losing market share to innovative firms. And if it's not developing and gaining market share, the business can be perceived to be failing.

Understanding this, B2B organizations look to agile and DevSecOps methodologies to help them get to their desired destinations. Gartner analysts note that:

*"Through 2023, 75% of organizations will customize agile practices to match product and team contexts, resulting in increased application delivery cadence."*

### Unfortunately, Increased Innovation Speed Introduces New Risks.

To beat competitors, your organization or company must deliver products more rapidly. But the fast delivery comes at a price.

Transitioning from 12-, 6-, 3-month delivery cycles to a world of DevSecOps and continuous delivery, where your organization is expected to deliver new features daily or by the hour (or even minute), you're bound to encounter risks and challenges.

If you were used to building products as per careful, planned processes, now, you have to ensure your teams are dotting i's in the shortest time possible.

**The questions then become:**

- How do you maintain and perform audits that took months in just days or even hours?
- How do you ensure you run critical regression tests on your software when you have limited time to perform tests?
- How do you ensure your checks and balances are not skipped?
- How do you ensure the manager provides the needed approval on time?
- How do you ensure speedy delivery amid a wide-ranging portfolio, including Python, mobile, Java, Haskell, and cloud computing?
- Who will be accountable for what? Or who will ensure everything goes smoothly?
- What rules and policies will everyone involved in product development have to follow?

Now, there may be no clear-cut answers to these questions, seeing that change happens regularly. But the fact remains that the market environment is defined by continuous everything. So, you will be analyzing, integrating, testing, and deploying solutions on a loop; hence, the need for control procedures.

### Speed vs. Security

Non-profit, government, and B2B organizations must identify and address security holes and vulnerabilities at high speeds.

Yet, most compliance and security tools are lagging behind the fast-paced systems development. As such, security is an obstacle, with organizations continuing to face IP theft, data loss, increased expenditure, business disruption, and competitive disadvantage.

Recent security breaches showcase just how essential security is for the well-being of users, customers, and the entire organization. Data breaches at Equifax, Yahoo!, Uber, and Facebook exposed users' private information, costing the firms millions.

The Uber security breach, for instance, cost the company GBP $133M in legal settlements. The online transportation network also had to pay $100,000 for hackers to delete the stolen data.

Overall, open-source software bugs like Wanacry and Heartbleed are disrupting organizations, with losses accruing from these ransomware costing billions.

## The Security Problem

Traditionally, organizations relied on security teams to handle all their security issues.

A recent Sans Institute survey indicates that organizations still rely on a handful of job functions to perform security testing.

**Think of:**

- Internal security teams
- Security consultants
- Quality assurance
- Or DevSecOps (or cross-functional teams)

The development team is mainly responsible for corrective action, whereas the security team handles vulnerability testing. In such a space, the development team addresses security issues if they come. (And is likely to perceive the security team as blocking its ability to innovate and make progress.)

There is, therefore, a need for innovative ways to effectively integrate compliance and security in a mature DevSecOps lifecycle.

**When implementing secure application systems, organizations are likely to face the following challenges:**

- A lack of automated and integrated workflow
- A gap between application development security and compliance
- Lack of application security tools, methods, and skills

So, organizations are left in a situation where they want everybody to be accountable for security, yet the average developer does not truly comprehend cybersecurity. Or in a scenario where they want to automate the security testing process but don't understand how to do it.

## Webhead's Solution: DevSecOps (Technology Advanced to the Height of Self-Defense)

DevSecOps is an extension of DevOps. It secures the collaboration between the development process and security functions to check weaknesses and risks at every step of the software development life cycle (SDLC).

The "Sec" in DevSecOps emphasizes security to identify and mitigate vulnerabilities early and often. DevSecOps automates security functions, eliminating obstacles to help achieve security with speed.

Like DevOps, Webhead's DevSecOps approach strives to drive more productivity and efficiency through team collaboration. However, DevSecOps integrates security principles into the product development process.

Here, developers and security leaders work together, every step of the software development process. Instead of security teams providing input at the end. Security leaders are still required to offer expertise, but the overall security of the product in question becomes the responsibility of everyone involved in its delivery.

DevSecOps also represents a cultural shift, where stakeholders must be aligned to deliver products with both speed and security.

In a nutshell, Webhead uses its DevSecOps process to consider security as an integral part of the product development lifecycle. Think of the "Sec" in DevSecOps as the Robin to your organization's DevOps Batman – a trusted sidekick enhancing continuous backup.

### Webhead's DevSecOps Approach Encompasses these Concepts:

**Security as code**. DevSecOps integrates tests, vulnerabilities, and scans as code or scripts. These scripts can be replicated and automated, enabling continuous security verification throughout the software lifecycle.

**Shift security left**. DevSecOps not only starts security activities earlier in the development but also incorporates them throughout the process. That involves addition of security experts in an agile team at project inception and ensuring other members are educated on security issues.

**Empower teams**. DevSecOps makes security everybody's responsibility – with security experts serving as overseers: recommending methods, tools, and processes. The entire organization, quality assurers, and developers must learn security best practices and integrate them into their daily tasks. That calls for B2B organizations to empower their teams with the knowledge and tools required to enforce security.

**Security visibility**. DevSecOps makes security a priority instead of an afterthought – allowing it to be tracked and monitored like other DevOps tasks.

**Continuous security**. Security is incorporated throughout the product development process to help the organization identify and respond to cyber threats at any stage in the product development. Checkpoints are set up in the continuous loop to track changes, test for flaws, and activate mitigation measures continuously.

## How Webhead Checks Security for Your Organization

- Regular security audits help organizations stay ahead of cyber threats. As such, suspicious activities can be tracked and mitigated. That presents a chance for innovation with respect to the best security measures against cybercrime.
- Security personnel employ templates to deal with cyber threats promptly, nurturing or replacing servers to keep the organization running.
- Security automation comes in handy, especially for large Non-Profit and Government organizations where developers push different codes to production every other hour.
- By incorporating security principles throughout the product lifecycle and aligning them with the organization's risk strategies, DevSecOps helps minimize security issues.
- As organizations are now realizing, moving faster can boost security. Because then, delivery teams are forced to standardize, automate, and collaborate their workflows. When the delivery cycles and development pipelines become standardized, teams get more visibility into their practices and processes – enabling them to exercise more governance and control.
- DevSecOps also boasts continuous delivery, where developers make incremental changes and deliver updates frequently. This approach makes it easier to detect and mitigate any security flaws in the product development process.
- Moving faster with frequent incremental changes, changes the attack surface continuously – providing more security protection for the application system. (That makes it hard for hackers to identify vulnerabilities, let alone exploit them.)
- DevSecOps also employs rigid infrastructure to reduce insecure defaults and vulnerabilities, while enhancing automation and increasing code coverage. In case of an attack, your organization can tear down the infrastructure and rebuild the same with new credentials.
- DevSecOps also makes every individual responsible for security. By encouraging a culture of openness, DevSecOps establishes more collaboration among teams, further enhancing the approach to security enhancements. This "all the stakeholders" approach can boost the security firewall against cyber breaches.
- Overall, DevSecOps enhances security through different approaches, including automated code tests, application security testing, and encouraging the adoption of secure design patterns.

## How Webhead Implements DevSecOps

**Organizations looking to move to DevSecOps will need to:**

- **Change their process**. DevSecOps efforts need open lines of collaboration and communication to succeed. Organizations should, therefore, put measures in place to unify teams across different functional silos. That calls for reliable communication and collaboration tools, reporting metrics, and tools. Organizations must also create feedback loops to promote and embrace a continuous improvement approach.
- **Adopt new technology**. Organizations need to add tools that automate security testing. That means integrating tools that perform composition analysis, scripting, and static and dynamic analysis to detect weaknesses early and often.
- **Overhaul their culture**. Organizations need to embrace and create an atmosphere of cooperation and trust. They need to commit to training, learning, empowering security champions, establishing feedback loops, and promoting decision-making across business units.

## Webhead Bridges Gaps Among Innovation, Speed and Security

**Overall, bridging the gaps among innovation, speed, and security in product delivery requires commitment and collaboration. It also demands the establishment of new processes and workflows.**

**To succeed and find a balance between innovation, speed, and security, businesses must: i. adopt effective testing across the product development cycle, ii. build cross-functional teams, iii. automate end-to-end workflows, iv. integrate IT tools, and v. encourage communication across functional silos.**

**If your organization is looking to implement an innovative and secure software and IT solutions, the experts at Webhead can help. We understand how DevSecOps improves communication and collaboration, ensuring alignment across all aspects of the development process with security at the forefront.**

**Contact us today to learn more about our services and to start developing your DevSecOps transformation.**