DevOps vs DevSecOps Approaches Which Amplify Automation and Security

In today's IT world, most software pros are willing to adopt the agile framework in the current market. As a result, the focus has shifted from transforming the process to prioritizing the roles. Agile spawned off multiple methodologies such as DevOps, SecOps, and DevSecOps. For instance, DevOps decreases the delivery time, whereas SecOps creates security, and DevSecOps create a balance between the two.

In recent years, **DevOps and DevSecOps** have transformed many companies' software development approaches. But both terms have become a euphemism for software development. At the same time, it is essential to understand the importance of both DevOps and DevSecOps concepts. They are not permanent paradigms, monolithic, or one-size-fits-all.

Both DevOps and DevSecOps sound similar terms. But their distinctions can impact your business effectiveness and the IT industry on a larger scale. Understanding the

Headquarters: Veritis Group, Inc , 1231 Greenway Drive, Suite 1040, Irving, TX 75038

Phone: 972-753-0022 | **Email:** connect@veritis.com

concepts will allow you to develop a productive work for your company's data by leveraging the weakness and strengths of each model.

The two terms DevOps and DevSecOps are perceived to be synonymous with each other. However, some industry experts suggest that DevSecOps isn't only compatible with DevOps but also vital for it to function optimally in a few circumstances.

Teams who understand the differences of DevOps Vs DevSecOps can make decisions that will improve the productivity of their app development pipeline. It also helps teams to make modifications to their process so that they may focus more on security, agility, and speed.

So, let's dive into understanding these approaches and how they differ from each other.

DevOps

Patricks Debois coined the term DevOps in 2007. He is known as the father of DevOps. He was an IT consultant who used agile methodologies to bridge the gap between project management and operations.

DevOps is a set of tools, practices, and a philosophy that automates and combine the process between software development and IT teams. It defines a change in IT culture to improve work throughout the software development life cycle (SDLC).

The development and operations teams are not the same as twins under the DevOps approach. Instead, these two teams combine a single group where developers work on the application lifecycle, from deployment to development test. As a result, they foster a broad range of skills that aren't limited to a single function.

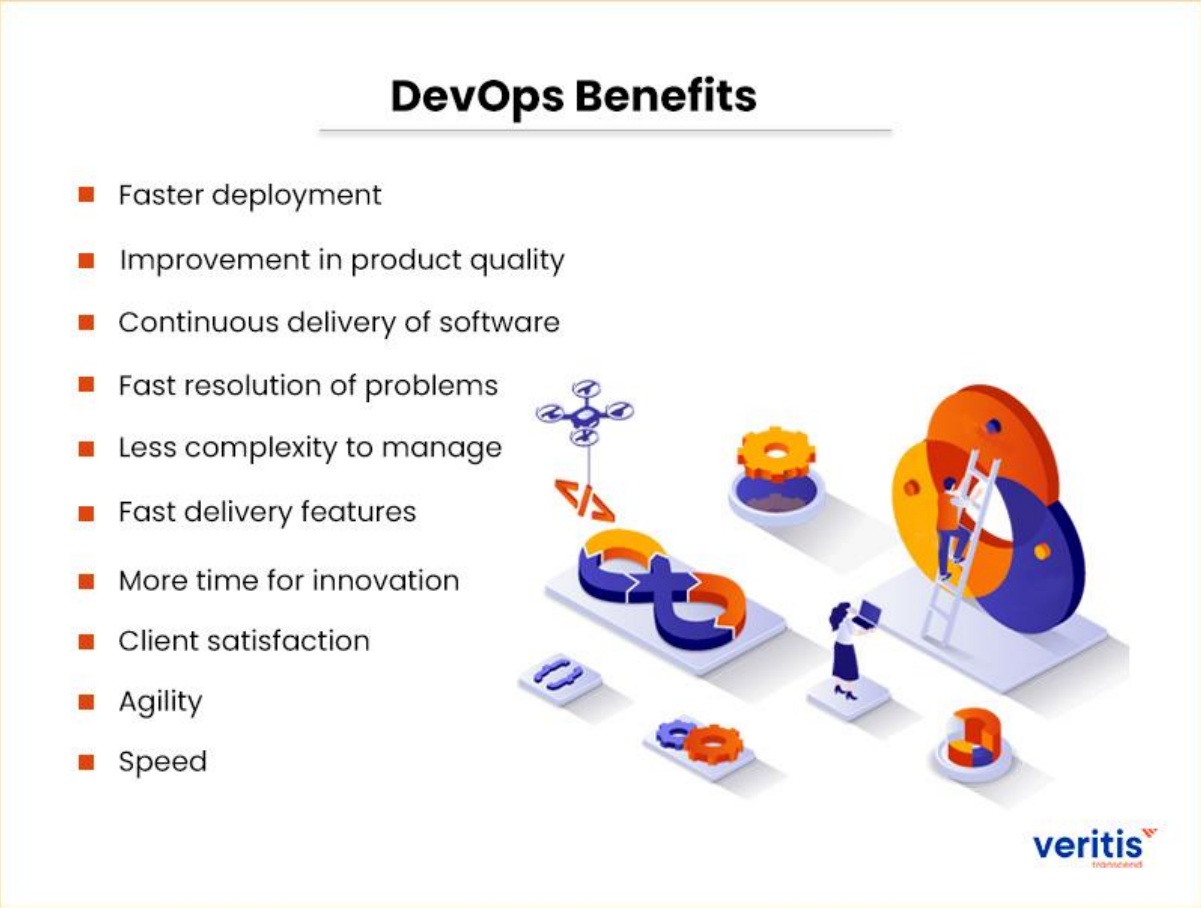
Transposit IT firm released the '2022 State of DevOps Automation' report and said IT firms adopted DevOps workflow more widely. 48.2 percent of IT pros pointed to automation, while 52.3 percent of IT pros stated that they would run new automation tools.

Security is a priority in the DevOps approach. As a result, the security team and quality assurance teams collaborate throughout the application lifecycle. They depend on a

technology stack and tools to guide them to produce applications consistently and quickly.

Useful link: Top 10 DevOps Tools to Pick for Your Business

DevOps Benefits



DevOps has multiple benefits that a company can have productive work after implementing the DevOps model in their workflow.

Headquarters: Veritis Group, Inc , 1231 Greenway Drive, Suite 1040, Irving, TX 75038

Phone: 972-753-0022 | **Email:** connect@veritis.com

Below mentioned are some of the benefits of DevOps:

- Faster deployment
- Improvement in product quality
- Continuous delivery of software
- Fast resolution of problems
- Less complexity to manage
- Fast delivery features
- More time for innovation
- Client satisfaction
- Agility
- Speed

DevOps Practices

Continuous automation and improvement are essential to DevOps practices. As a result, many practices concentrate on one or more levels of the development cycle. These are some of the practices

Continuous Development

The coding and planning phases of the DevOps lifecycle involve in this approach. In addition, it may involve version control techniques.

Continuous Testing

Continuous testing includes ongoing code tests, automation, and prescheduling of the application code to modify. Such tests can help to expedite code release to the production atmosphere.

Continuous Integration

It entails feedback between development and testing to discover and resolve code errors as quickly as possible. In addition, this method involves configuration management (CM) tools with other development tools to track how much code is ready for production.

Continuous Delivery

It automates the delivery of code changes to a preproduction stage after testing. A staff member may then opt to push such code changes into production.

Continuous Deployment

It automates the release of new or updated code into production, similar to continuous delivery. Continuous deployment allows an organization to release code or feature updates numerous times.

Continuous Monitoring

This method entails continuous monitoring of the infrastructure. A feedback loop in which bugs or problems are reported and reported to development.

Infrastructure as Code

Infrastructure as code uses to automate the provisioning of infrastructure required for a software release during multiple DevOps processes. Developers developed Infrastructure “code” using their existing development tools.

DevSecOps

DevSecOPs is a short form of development, security, and operations. It automates the security at every stage of the SDLC. It is a way to reach IT security with everyone responsible for a security mindset. The aim is to involve security at every level of the software development workflow.

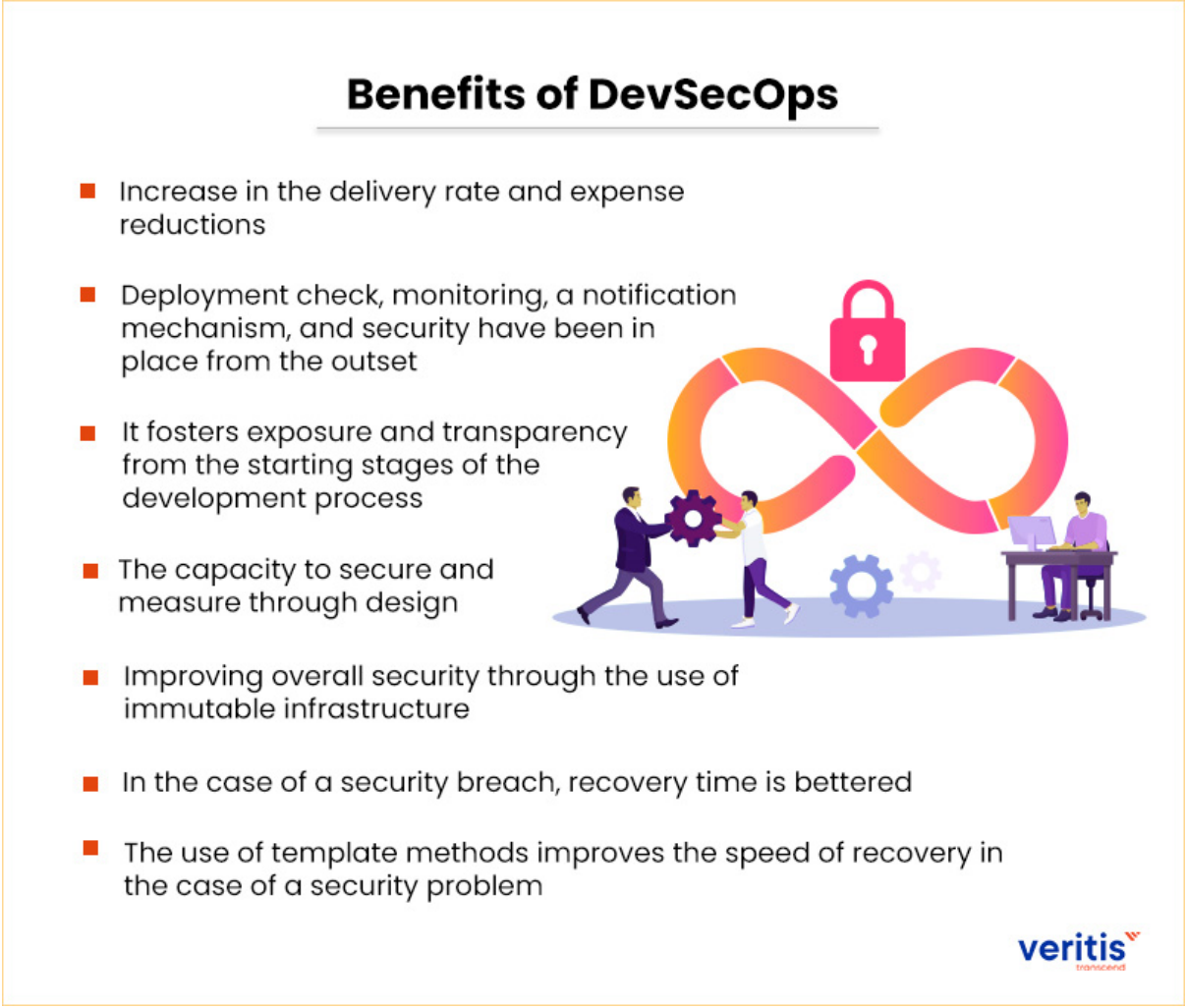
If your company has adopted DevOps, then it’s an excellent thought to shift towards DevSecOps. It depends on the principle of DevOps, which will enable the user to bring IT pros from technical disciplines to allow your existing security processes.

A CSA survey said that 30 percent of IT security pros are adopting the DevSecOps model. While 24 percent of companies are in the planning phase, 18 percent are in the designing phase, and 90 percent of companies are at some stage of their DevSecOps journey.

Applying security at every stage of the SDLC allows software products to deliver more quickly. In addition, it reduces the costs and continuous integration. In DevSecOps, every person and team is responsible for security. And they must make quick decisions and adopt them without compromising security.

Useful link: DevSecOps – A DevOps Savior to 'Cybersecurity' Challenge!

Benefits of DevSecOps



The two key advantages of DevSecOps are security and speed. Development teams produce cheaper, better, and more secure code.

There are multiple advantages of adopting DevSecOps, and some of them are:

- Increase in the delivery rate and expense reductions
- Deployment check, monitoring, a notification mechanism, and security have been in place from the outset
- It fosters exposure and transparency from the starting stages of the development process
- The capacity to secure and measure through design
- Improving overall security through the use of immutable infrastructure
- In the case of a security breach, recovery time is bettered
- The use of template methods improves the speed of recovery in the case of a security problem

---

Useful link: DevSecOps Process, Benefits, Tools and Implementation

---

DevSecOps Practices

The human aspect will always be the weakest link in the chain, yet of how many technologies you choose to combine. However, it is the start point for any DevSecOps adoption. One of the essential factors of DevSecOps is that it challenges traditional security teams' integration with the rest of the business.

Let's go through some of the specific DevSecOps practices

Encrypt Sensitive Data

Any data that could harm or identify an individual, both at transit and in rest, should encrypt. It includes medical records, social security numbers, and credit card numbers.

Headquarters: Veritis Group, Inc , 1231 Greenway Drive, Suite 1040, Irving, TX 75038

Phone: 972-753-0022 | **Email:** connect@veritis.com

Make Your Application Development Process More Secure

The starting step to secure your DevOps process is to assure the security of your application development process. It involves limiting access to your code repositories to authorized developers. It ensures all code changes to evaluate and approved by a qualified reviewer before merging into the main branch.

Protect Your Production Environment

Your application will deploy and use by your clients in your production pro. As a result, it’s essential to make sure this process is more secure.

Use Two-Factor Authentication

Two-factor authentication (also known as 2FA) is a security measure that safeguards access to DevOps resources. A user must supply two components of evidence to validate their identity with 2FA. The first component is something they know, such as a password. At the same time, the second component is something they possess, such as a mobile phone.

Operate Secret Management Tools

Secret management tools can let you handle secrets from a central location while providing access control and auditing. AWS Secrets Manager and Hashicorp’s Vault are the most famous secret management tools available in the market.

Perform Regular Security Audits

Security audits should be performed regularly as part of DevOps security. It may help you identify system flaws and make sure that your security policies are effective.

Useful link: DevSecOps Solution to Cloud Security Challenge

Difference Between DevOps Vs DevSecOps

The below mentioned points are the major difference of **DevOps Vs DevSecOps**.

Parameters	DevOps	DevSecOps
Philosophy	DevOps is a set of tools, practices, and a philosophy that automates and combine the process between software development and IT teams	DevSecOPs is a short form of development, security, and operations. It automates the security at every stage of the SDLC
Purpose	The primary goal is to bridge the gap between teams so that the entire process of code development and	The primary goal is to deliver security of the whole development while it improves

Headquarters: Veritis Group, Inc , 1231 Greenway Drive, Suite 1040, Irving, TX 75038

Phone: 972-753-0022 | **Email:** connect@veritis.com

	deployment can complete more quickly	process speed, scalability, and accessibility.
Emphasis	Emphasizes the software development	Emphasizes the importance of developers to create secure and compliant code. It is their role to ease data loss and downtime.
Team skillset	Fundamentals of Linux and scripting. It understands the basic concepts of multiple DevOps tools	Engineers in DevSecOps must be capable of identifying vulnerabilities by running automated security tools
Security	It starts at the development pipeline	It starts with the development process
Benefits	It supports end-to-end roles	It reduces the price of resource management

Final Thoughts on DevOps Vs DevSecOps

Don’t Devops Vs DevSecOps, as both approaches have the most common features. It includes automation and continual processes to generate shared development cycles. DevOps emphasizes delivery speed, while DevSecOps emphasizes more security. Although DevOps and DevSecOps concepts are not mutually exclusive, their objectives are distinct.

Instead of picking DevOps Vs DevSecOps, opt for multiple approaches. Which gives you multiple benefits for your business. Adopting both DevOps and DevSecOps strategies is a laborious process; this is why where companies seek Vertis’s services.

Veritis, the Stevie Awards winner, has awed its customers with its outstanding solutions. **Veritis** understands its clients' needs aptly and offers the best DevOps services for your business with cost effective solutions.

Services

Headquarters: Veritis Group, Inc , 1231 Greenway Drive, Suite 1040, Irving, TX 75038

Phone: 972-753-0022 | **Email:** connect@veritis.com