

WHAT IS DEVSECOPS? THE ROLE OF SECURITY IN DEVOPS ARCHITECTURE



As the world continues its lightspeed advance into the future of tech, businesses scramble to develop new methods and tools for keeping pace. The cloud exploded onto the scene and new applications are being found for this technology every day. The same can be said for blockchain technology as well. The rate of change in the tech world is astounding and businesses need to keep up if they hope to keep their head above water in the days to come.

Enterprises had to find new approaches to aid them in maintaining the development speeds required by today's competitive environment. Organizations learned that switching over to software as a service (SaaS) structures allowed them to stay relevant and appeal to the new sensibilities of modern customers. With new tools and mentality, enterprises found means for achieving constant delivery (CD) and constant integration (CI) where software development lifecycles became much shorter.

The Basics of DevOps

The switch to CD/CI structures emphasized the importance of both faster development cycles as well as integrating deployment systems into the process. This is what gave rise to the adoption of DevOps as a solution for maintaining a constant stream of service updates that are stable and impactful on the customer's experience. DevOps merged once disparate teams of development and operations into single, cohesive units that utilize their cross-discipline backgrounds to enhance the success of the team.

DevOps is a mentality of collaboration as well as a collection of tools and systems that come

together to form more efficient teams, keeping up with the rapid pace of development and deployment expected of IT enterprises today. The tools necessary in a successful DevOps system's toolkit are ones that enhance collaboration and transparency. The strengths of the cloud in conjunction with the power of automation provided the necessary boosts that fuel this new structure of DevOps.

The cloud has proven invaluable in providing teams with the means of communicating efficiently at all times. Meanwhile, the automation of tasks drastically reduces the time that was previously spent manually handling work that could readily be offloaded through automation. These tools have proven themselves invaluable for the DevOps transformation many enterprises are finding necessary; however, new technologies that enhance collaboration and the speed of development also present new and more complex [security threats](#).

The Basics of SecOps

In acknowledgment of the massive importance of security in the new era, SecOps was developed as a seamless collaboration for IT security and IT operations teams to work together for managing risk and remediating vulnerabilities. Once again, the key aspect of these new systems is the collaboration of teams that had once siloed themselves off from one another. This time, the focus is on creating safe systems by making security a primary concern for all team members.

Security and compliance are the primary pursuits of a SecOps team as they search for the best ways to maintain safe servers, networks, and cloud environments. SecOps is especially important in multi-cloud environments where security issues become increasingly complex as the system grows in size to meet the new demands. SecOps tools look to enhance collaboration while also providing tools that give deep insight into preventing security threats and any means for remediating current potential risks existing within the system.

SecOps teams also utilize automation that aids in quickly remediating issues as they arise. Operational intelligence is a constant concern for the teams as they look to enhance their understanding of each system and its vulnerabilities. SecOps tools feed teams constant streams of insightful data that empowers them to maintain security standards while achieving continuous compliance. This intense focus on security can result in slower deployment rates but provides high levels of security for increased stability and mitigated risks.

Extending DevOps and SecOps into DevSecOps

You probably noticed that DevOps and SecOps had some key similarities. SecOps and DevOps both emphasize the importance of collaboration while also promoting the use of cross-discipline teams so that everyone can have a deeper understanding of the other aspects of the project on which they're working. This enhanced insight provides team members with a unique perspective that empowers them to focus on their tasks while also considering how their work will impact the work of teammates.

DevSecOps looks to combine DevOps and SecOps functions into singular teams that all work together to increase the rate of deployment while also ensuring compliance and security best practices are maintained. By making security a responsibility of every member of the team, development and operations take some of the load off of security. Armed with a deeper understanding of how each discipline functions, security team members can work alongside dev

and ops members to more quickly resolve issues or prevent them altogether.

This shared responsibility is incorporated as part of the culture of collaboration engendered by standard DevOps systems. Developers learn to adopt more secure coding practices while operations realize the importance of compliance. These aspects help to create products that are inherently more secure coming right out of the gate. Furthermore, modifications can be readily made in case of unforeseen security risks cropping up.

DevSecOps takes the culture of collaboration and the idea of cross-discipline teams a step further to bring everyone into the fold and integrate key security policies for each step of the process. DevSecOps tools are available to enterprises that help them perform automated code analysis, compliance monitoring, threat investigation, and vulnerabilities assessments. By integrating security into DevOps, more secure software is deployed from day one. This heavily influences the rate of recalls and rollbacks to save time, money, and face for the organization.

Embracing the power of a collaborative environment that utilizes cross-discipline teams and values the importance of transparency can help launch your enterprise to new heights. DevSecOps looks to combine the speed and stability of DevOps with the security and compliance of SecOps, creating a perfect recipe for software enterprise success.

DevOps: Solutions for You

If DevSecOps sounds like a good fit for your organization's needs but you want to make sure you get it right the first time, BMC is the IT solution partner you need. Read more about how automation and DevOps systems can help increase the rate at which you deploy products with BMC's free eBook: [*Automate Cloud and DevOps Initiatives*](#).

BMC provides DevOps and [SecOps](#) services and expertise to help your organization meet its goals. BMC expert consultants are available to work with you to bring their knowledge and expertise to your organization. BMC also provides custom-tailored [Implementation Services](#) for your organization to tackle the unique challenges you face. When partnering with BMC, you get:

- **Faster service delivery:** Agile releases that keep up with rapid demand
- **Visibility across data:** Ensure compliance and data accuracy
- **Cost-effective service:** Increased productivity and performance
- **Experienced DevOps professionals:** Equip you with the tools you need for success
- **Conversion or upgrade:** Seamless modernization or total replacement
- **All tailored for the specific needs of your organization.**

Download or view the [Solution Implementation Overview](#) online to learn more about how [BMC Consulting Services](#) can help you. Learn more about maintaining security and compliance in the [SecOps for Dummies](#) eBook from BMC. Then contact the experts at BMC to find out more about how to combine SecOps and DevOps practices into DevSecOps for enhanced building, testing, and deployment success.