DevSecOps: Deploying Software at Speed of Operations

MARKET TRENDS REPORT

govloop Red Hat carahsoft

Introduction

To accelerate software development without sacrificing security, the Department of Defense (DoD) has turned to DevSecOps and its model of continuous testing, integration and delivery as the optimal way to get new tools into warfighters' hands as quickly as possible. Although DevSecOps may be the preferred method of development, it's still not the most widely practiced, with many IT shops tied to traditional waterfall methods and others struggling to implement what is sometimes a complex process.

Amid a fluid, asymmetric landscape of kinetic cyberthreats from adversaries who are themselves using automation and other advanced technologies, DoD recognizes the importance of keeping pace with software, which is at the core of practically every DoD system, from weapons and communications to procurement and personnel management.

DoD and other federal agencies need to combine the speed of DevOps software development — which emphasizes collaboration and continuous testing, integration and delivery — and the security that is essential to protecting networks and data. Last year, the department launched the DoD Enterprise DevSecOps Initiative to combine software development (Dev), security (Sec) and operations (Ops) to significantly shorten the time between the inception of new software and its deployment at scale.

The challenge for DoD and other organizations is ensuring that all moving parts work together seamlessly and effectively. To learn more about how agencies can implement a working DevSecOps culture, GovLoop teamed with Red Hat, the industry leader in enterprise open source software development. We gained insights from Kevin Griffith, Senior Director for DoD Sales at Red Hat.

BY THE NUMBERS

Legacy Software Development vs. DevSecOps

Comparison Point	Legacy	DevSecOps	Difference
Continuous Authorization *Average time to complete code deployment after initial assessment and authorization (A&A)*	23 days	6 hours	**92% faster**
Initial System Authorization *Cybersecurity risk assessment threshold determination for pipeline, including major system design and compliance with the DoD Risk Management Framework*	12 months	3 months	**75% reduction**
Mean Time to Provision *Average time that it takes to add additional services to an environment*	6 months	2 hours	**99.79% reduction**
Mean Time to Recovery *Average time from deployment failure to recovery*	15.5 minutes	4 minutes	**74% reduction**
Operating Costs *Change in operating costs based on using open source tooling vs. an architecture dependent on legacy commercial off-the-shelf technologies*	$1.8 million	$150,000	**91.66% reduction**

Source: Joint Improvised-Threat Defeat Organization, cited in the Defense Innovation Board's SWAP Study, May 2019

90%

of software development projects will claim to follow DevSecOps practices by 2022, up from 40% in 2019.

Source: Gartner

25%

of all software development projects will follow a DevOps methodology from conception to production by 2022, up from less than 10% today.

THE CHALLENGE
Mission Need Outpaces Development Practices

Like government agencies and organizations in other sectors, DoD in many ways runs on software. "Software has become one of the most important components of our nation's weapons systems, and it continues to grow in importance," according to a 2018 Defense Science Board report examining the design and acquisition of DoD software.

Software drives program risk on about 60% of acquisition programs, the report notes, which underscores the importance of incorporating security from the start. "Design and acquisition decisions at the beginning of the software development process frequently have far-reaching and long-term effects," the board said.

In one important way, time works against software's effectiveness. Traditional waterfall practices can take a year or more to deliver usable software, which can leave DoD far behind the curve in a fast-moving world. Agile development speeds things up, but not enough. The Enterprise DevSecOps Initiative states plainly that legacy processes lack the agility to deploy new software "at the speed of operations" and leaves security as an afterthought, sewn in after a software application has been developed.

In short, traditional software development methods just aren't good enough anymore. What DoD needs are programs with "the ability to rapidly field and iterate new functionality in a secure manner, with continuous oversight based on automated reporting and analytics, and utilize [DoD Information Assurance Certification and Accreditation Process]-accredited commercial development tools," according to the initiative's reference design document.

DevSecOps, which is now established as the "industry best practice for rapid, secure software development," presents the optimal path for DoD and other organizations, according to the document. Its continuous testing and delivery puts updates and new applications into use swiftly, potentially giving DoD a decided advantage over adversaries.

But doing DevSecOps effectively involves more than just deciding to do it. "Current law, regulation, policy and internal DoD processes make DevSecOps-based software development extremely difficult, requiring substantial and consistent senior leadership involvement," the Defense Innovation Board's 2019 SWAP Study states. "Consequently, DoD is challenged in its ability to scale DevSecOps software development practices to meet mission needs." It requires a cultural change, which starts at the top.

The Solution: Delivering Incremental Value Through DevSecOps

DevSecOps offers dramatic advantages in the speed of development. "In a traditional waterfall scenario, delivered value is zero until the initial release of the product," Kevin Griffith, Senior Director for DoD Sales at Red Hat, said. "With DevSecOps, features, and thus value, are produced iteratively, in small increments. This means that, while the first iteration that can be released might not be as impactful as the first release from a waterfall release schedule, the value is fielded far sooner, and continues to add value through the iterative steps of additional releases."

The SWAP Study provided some examples of DevSecOps' advantages. For example, it found that the time for Initial System Authorization fell from 12 months under legacy processes to three months with DevSecOps.

In addition to software development, DevSecOps also supports the use of Other Transaction Authority (OTA) agreements, which allow DoD and other federal agencies to collaborate with non-traditional businesses on cutting-edge projects, so they can work together with industry partners on new, innovative capabilities.

"DevSecOps pairs perfectly with these goals," Griffith said. "Agencies can demonstrate the advantages of a leaner, more agile acquisition strategy for DoD through a DevSecOps engagement using an OTA vehicle."

Project leaders can home in on the most valuable aspects and more easily course-correct throughout development. "In the end, a DevSecOps methodology will show greater time to value and more focused value to DoD, which should naturally lead procurement and acquisition to prefer a leaner, more flexible process," he said.

BEST PRACTICES
for DevSecOps

I. Enlist leadership.

DevSecOps requires a cultural change, which needs leaders' support. Key steps — such as developing a comprehensive plan, educating developers and ensuring cooperation among IT, security and business teams — depend on their support.

2. But start small.

As with software development itself, it's a good idea to make changes iteratively, with a fairly small project that can fail, adapt and grow. The Air Force's software factories, which are at the forefront of DevSecOps among federal agencies, started small with a specific project in Qatar. Its success gave root to wider — and still expanding — use of DevSecOps.

3. Automate.

Security is essential, but speed is the goal. Automation can combine the two in software development with tools such as dynamic application security testing, static application security testing and automated configuration. With security controls embedded early in the process, automation can ensure the consistency and reliability of testing, and secure coding in a continuous integration, continuous deployment environment. Software can't be developed quickly without it.

4. Teach security.

In addition to having development and security teams working together, it helps to educate programmers on secure coding practices, which may not be something they're using now.

5. Test everything.

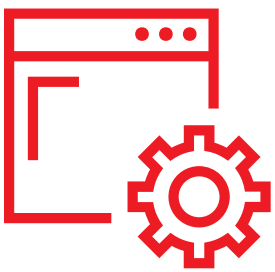
Continuous security testing is essential to DevSecOps, but it can't be limited to a few areas. Threats exist across a spectrum of techniques and tactics, and security controls must match the threat, covering areas including front and backend testing, unit testing, application programming interface testing, database testing, and passive security testing.

6. Adapt continuously.

One of the most important lessons in IT operations — whether involving security, cloud adoption or any number of applications — is that there is no finish line. Change is the only constant, so enterprises must be able to adapt to circumstances with policies and processes designed to shift gears quickly.

7. Build to scale.

Innovative software won't do much good if it can't reach the full expanse of federal agencies, whose operations often are worldwide. Agencies with DevSecOps initiatives also need to work with a cloud platform that ensures scalability.



CASE STUDY
DevSecOps in Action

DevSecOps has proven its value in DoD through projects such as the Air Force's software factories and the Navy's Compile to Combat in 24 Hours initiative, which changed how the Navy develops and deploys reliable, secure software to the fleet. Various civilian agencies, including the Homeland Security and Agriculture departments and the Environmental Protection Agency, have also adopted it.

Griffith said the experience of one defense command illustrates how DevSecOps delivers value quickly through an incremental approach. The command had been relying on a labor-intensive, spreadsheet-laden process for assessing soldier fitness and wanted to move to an automation and web-based system. Adopting DevSecOps, leaders initiated a modernization program that included three release cycles, or sprints.

1. The first provided the assessors with tablets loaded with the assessment application. The application's intuitive user interface allowed them to enter data in fields, replacing a process that had them entering data into a spreadsheet at the end of each day.
2. In the second sprint, data moved from the new information system directly into a database, replacing a process in which a data scientist had to input the assessment data.
3. The third sprint produced reports incorporating the fresh assessment data with the data scientist's historical reports, replacing a more labor-intensive process.

As a result, reports covering the full range of assessment criteria, which could take hours or even days to complete, were produced in a matter of minutes. It serves as a clear example of how leadership buy-in and a targeted use of DevSecOps can deliver value both immediately and incrementally throughout the development lifecycle, Griffith said.

HOW RED HAT CAN HELP

Red Hat has long been a leader in enterprise open source software, including Linux, cloud and Kubernetes container orchestration technologies, and has worked with DoD and other federal agencies on successful DevSecOps deployments. In addition to helping agencies gain the speed and security of DevSecOps, Red Hat also enables deployment at scale. The **OpenShift** Container Platform uses Kubernetes for its container orchestration layer, supporting a microservice architecture that enables innovation, easy integration and scalability in hybrid environments.

Red Hat OpenShift, based on the Red Hat Enterprise Linux (RHEL) operating system, enables a true hybrid cloud experience. Whether the workload needs to run on-premises or across a cloud provider, the OpenShift Container Platform can run anywhere that RHEL can run, and provides a consistent, infrastructure-agnostic experience for operators and system administrators.

OpenShift implements a defense-in-depth security strategy. The platform is based on a Security Technical Implementation Guide-hardened RHEL, but also provides a second layer of security through its own controls. And, lastly, Red Hat provides curated, security-audited container images that can be used as the base images for building hardened containerized applications.

To learn more, listen to a **recent podcast** featuring Michael Ducy, a Red Hat Transformation Specialist.

Conclusion

Federal agencies need three things for effective software development: speed, security and scalability. In a fast-moving, constantly changing threat environment, DevSecOps, combined with a comprehensive container orchestration platform for scalability in the cloud, offers the optimal path for achieving that goal. DevSecOps will help build a culture of collaboration, innovation and continuous delivery of software in a cost-effective model that consistently delivers value.

The traditional approach to software development is not designed to keep pace with the demands of the current IT environment. Not only is the pace — and the payoff — of development too slow, but security needs to be everyone's job, not just security teams' responsibility. Incorporating secure practices into development at the start of a collaborative process is necessary when producing reliable software at the speed of operations. And an orchestration platform designed for microservices ensures that new ideas get into the field quickly and at scale.

Red Hat

ABOUT RED HAT

Red Hat® is the world's leading provider of open source solutions, using a community-powered approach to provide reliable and high-performing cloud, virtualization, storage, Linux® and middleware technologies. Today, Red Hat is at the forefront of open source software development for enterprise IT, with a broad portfolio of products and services for commercial markets. That vision for developing better software is a reality, as CIOs and IT departments around the world rely on Red Hat to deliver solutions that meet their business needs. Solutions that provide technology leadership, performance, security, and unmatched value to more than 90 percent of Fortune 500 companies.

http://www.redhat.com/en/technologies/industries/government

carahsoft

ABOUT CARAHSOFT

Carahsoft Technology Corp. is The Trusted Government IT Solutions Provider®. As a top-performing GSA Schedule and SEWP contract holder, Carahsoft serves as the master government aggregator for many of its best-of-breed technology vendors, supporting an extensive ecosystem of manufacturers, value-added resellers, system integrators and consulting partners committed to helping government agencies select and implement the best solution at the best possible value.

Visit **www.carahsoft.com**, follow **@Carahsoft**, or email **sales@carahsoft.com** for more information.

govloop

ABOUT GOVLOOP

GovLoop's mission is to "connect government to improve government." We aim to inspire public-sector professionals by serving as the knowledge network for government. GovLoop connects more than 300,000 members, fostering cross-government collaboration, solving common problems and advancing government careers. GovLoop is headquartered in Washington, D.C., with a team of dedicated professionals who share a commitment to connect and improve government.

For more information about this report, please reach out to **info@govloop.com.**

1152 15th St. NW Suite 800
Washington, DC 20005

P: (202) 407-7421 | F: (202) 407-7501

www.govloop.com
@GovLoop