Simplifying and Securing DevSecOps

More federal agencies are taking advantage of DevSecOps than ever before to deliver secure applications more quickly and economically. DevSecOps, which uses an agile development approach, can significantly reduce the time it takes to create and update applications, allow developers to more efficiently develop cloud-native applications, and enable IT professionals to balance innovation with security requirements. For many, the fastest way to a secure, validated solution that maximizes developer productivity and speed is by deploying OpenShift.

While DevSecOps holds tremendous promise for federal agencies, security and complexity issues often hold agencies back from realizing its full benefits. One recent survey, for example, found that half of public sector organizations with mature DevOps practices consider application security a top concern.

The complexity of development environments also can hold agencies back from realizing the benefits of DevSecOps, because they often involve multiple pieces and systems. Too many pieces from different sources can lead to confusion and frustration, which can keep developers from being more productive as they deal with the complexities of automation, infrastructure and security.

And then there is compliance. Ensuring that all components are fully compliant with applicable standards, such as FIPS 140-2 (soon to be FIPS 140-3) and IPv6, isn't as easy as it might seem and is a great case study to explore how to build secure systems. These standards can be very confusing, leading many to believe that their systems and data are fully protected and compliant when they actually are not. This can result in gaps that attackers can use to infiltrate systems or create friction or incompatibilities within systems.

To avoid these problems, many agencies prefer a more integrated approach—securing the entire stack, from the operating system to the workflows and components layered on top, including container orchestration, as automated as possible.

That's the approach Red Hat has taken with OpenShift, a Kubernetes distribution platform that supports DevSecOps and is fully approved for government use. Each release of OpenShift pairs with a specific version of RHEL CoreOS and incorporates FIPS-validated cryptography, immutable file system constructs, and refined container runtimes and tools.

These issues are precisely the reason why so many public sector agencies choose OpenShift. One representative federal organization turned to OpenShift after previous efforts with an unsupported platform became unwieldy. As a result, the organization was able to ramp up DevSecOps in a big way. It went from having no in-house developers or in-house developed applications at all to solving big mission challenges

with DevSecOps. For example, the in-house development team used OpenShift to build a tracking application that shifted what was once a series of human-based time intensive processes into a fully automated process.

Compliance is key

Before committing to any DevSecOps technology, it's important to verify that all components are fully compliant with applicable standards. Complying with FIPS, for example, protects agencies against many vulnerabilities related to processing data. The best way to ensure compliance is by insisting on employing technology that has built compliance and security in, from the ground up, and keeps current with it.

"If you had to ensure compliance and accreditation for every single piece of software and infrastructure in your agency, it's easy to make mistakes that can be exploited," noted Michael Epley, Chief Architect at Red Hat's North American Public Sector Group. "Providing compliance at the common operating system level where everything above that can then use or inherit the common FIPS accreditation and validation ensures consistency. And as standards improve, it also ensures that agencies can update to these newer standards in a reliable way."

> **Security throughout the application development process** has never been more important than it is today.

Full compliance gives you confidence your systems are secure. Make sure your vendors take the right steps and have implemented one or more approved cryptographic algorithms in its software, firmware or hardware. FIPS-validated cryptographic modules should give agencies more confidence that cutting-edge tools like the Kubernetes distributed application management system won't leave them open to attacks or vulnerabilities.

But mistakes happen, which is why it's important to rely on a provider that is laser-focused on ensuring that users can't inadvertently bypass or misconfigure the underlying cryptography.

"Take the ingress controller, a component inside Kubernetes that allows external traffic into your system," explained Matthew Bach, a Senior Specialist Solutions Architect at Red Hat. "All of the traffic that goes through it has to be FIPS-enabled and accredited. It's a key component, but it's also easy to skip FIPS encryption of the ingress controller if you're not paying attention."

It's also important that the containerized components that make up the Kubernetes platform take advantage of the FIPS-validated cryptography instead of bypassing it.

"Containers, in particular, can create a false sense of security because of the high degrees of process isolation available, but useful containers must interact with the network, other applications, cluster services, persistent storage, monitoring and alerting systems, and many other components," Bach explained.

In other words, just because an application runs on Kubernetes doesn't mean it's inherently secure. "Does your orchestrator run with SELinux enforcing and is it FIPS enabled? Does it block ROOT workloads by default?" Bach asks. "Does it run on a tried and tested operating system and actually make your developers more productive, or are you left grabbing several GitHub projects as your production Kubernetes strategy? OpenShift allows your developers to get to work on a compliant system faster."

Get ready, set, CODE!

Security throughout the application development process has never been more important than it is today. That means that everything in the ecosystem matters—the supply chain, operating system, components that run on top of Kubernetes—in addition to a focus on standards compliance and a commitment to reducing risk wherever possible. When evaluating vendors, look for one with a deep bench of engineering expertise that takes the time to ensure security in every part of the solution stack. A good vendor will also work with the open source community to further the technology by triaging and patching systems as vulnerabilities arise.

Before committing, take the time to test the distribution you're considering, to make certain, for example, that key workloads actually work on top of a FIPS-enabled cluster. Don't bypass this step, Epley warned. Assuring that both the design side and supply chain side are using FIPS-capable and certified components is important throughout the entire software lifecycle. Of course, FIPS is just an example, and only one of many concerns.

Once deployed, system auditors should continuously verify and validate the use of FIPS for all workloads. Careful control of the workload's supply chain must be maintained to prevent reversions or regressions from being introduced, which could cause FIPS validation to be lost. Anything that can affect workloads or the underlying cluster infrastructure could affect FIPS compliance of the entire system.

With a secure, integrated DevSecOps infrastructure, agencies can reap the benefits of containers and agile development without major security concerns. A well-implemented DevSecOps process and infrastructure, along with a comprehensive approach to compliance, also positions agencies for the development of tomorrow, in whatever form that may take.