Advancing DevSecOps

Government needs an open source approach to development.

The Department of Defense recently signaled a new direction in federal applications development. Having released its design guidance for DevSecOps in August 2019, DoD sent a clear message that this emerging methodology would be the way of the future in federal government.

By integrating the development, security and operations elements of software development, IT can reduce the time to develop new software features; increase the frequency of new releases; and automate risk characterization, monitoring, and mitigation across the application lifecycle. In announcing its guidance, DoD cited these benefits as potentially attainable with a well-designed DevSecOps strategy.

In order for federal agencies to seize the value of an integrated development strategy, they'll need to embrace two key ideas. The first is that DevSecOps works best in an open-source environment. Second, even in an open-source world, vendor selection matters.

Many government IT professionals have discovered that open source alone doesn't guarantee lower cost or alleviate vendor lock-in. Successful DevSecOps requires the support of a vendor with a cloud-native platform that can offer true interoperability. The vendor's support personnel should be aligned with the federal mission, as well. In short, federal agencies need a strong solution to help them take full advantage of the DevSecOps approach.

A new approach

Within government IT organizations, change often can be a challenge. Agency IT offices must keep pace with the scale and complexity of digital transformation, meet the demands of a user base accustomed to private-sector innovation, and deliver security in an increasingly hostile digital environment.

In the realm of software development, DevSecOps offers a means to meet these challenges. In part, that's why the Federal Cloud Computing Strategy, released in June 2019, calls for inclusion of DevSecOps in the government's modernization efforts.

This approach makes it easier and faster to add a function or feature to an application, taking security into consideration as well.

PRODUCED BY: FCW | SPONSORED BY: ORACLE Linux

It may leverage containerization as a way to provide portability and increase resource efficiency – with orchestration delivering the ability to deploy, manage and dynamically scale the outputs. Overall, DevSecOps supports continuous integration and continuous delivery to speed release of new features.

The optimal DevSecOps environment for this kind of development is an open-source platform.

The federal government is already moving in the direction of open source. In 2016, the administration announced a policy requiring 20 percent of the federal government's software projects to be open source. As adoption of open source has grown, its cost has declined. Many DevSecOps initiatives, for instance, take advantage of Linux container technology, enabling federal IT to leverage existing Linux investment in support of the DevSecOps environment.

Moreover, open source gives developers more eyes on the problem. There is input from the global, open-source user community and support from commercial vendors.

There is a caveat: not all open source is equal.

Federal IT leaders who turned to open source to break free of vendor lock-in haven't always attained that level of freedom. Vendors may require small, idiosyncratic adjustments for applications to run on their stack. The tweaks seem minor, yet they can prevent portability and tie a developer's hands – an outcome that runs counter to the fluid and agile spirit of DevSecOps.

Federal IT, therefore, needs to align itself with a vendor that can deliver open-source tools and support in a legitimately open and robust environment.

Improving the bottom line

The Oracle Linux Cloud Native Environment is a curated set of open source projects aligned with the standards and framework of the Cloud Native Computing Foundation (CNCF) that can be easily deployed. The curated projects have been tested for interoperability, and enterprise-grade support is available. Users can leverage integrated builds of several projects including Kubernetes, Kata Containers, Istio and Prometheus which can allow containers

Why are agencies moving to DevSecOps?

By integrating software development, security and operations on a single platform, the DevSecOps approach can help government to:

- break down patterns of siloed development
- create more stable and secure operating environments
- speed up delivery of software and features with security in mind
- drive continuous release and deployment, continuous testing and monitoring
- improve operational support and deliver faster fixes
- free up time for IT to innovate, with less fixing and maintaining
- achieve better coordination across IT and teams

to be easily portable between environments, whether on-prem or in-cloud, managed or non-managed. This helps to ensure integration with legacy and modernized systems.

A strong solution for DevSecOps can also have an impact on the bottom line. Compliance testing is among the biggest cost drivers in development — in some cases more than $500,000 for a single test. A solution provided by a trusted industry partner can leverage capabilities to reduce substantially that cost.

In addition, the right solution can help developers to overcome scalability issues that have, at times, plagued open-source projects. In a typical scenario, a federal agency embarking on a low-cost, open source project might discover that costs rise exponentially when the time comes to scale up. Vendors may layer on costs by server, by CPU, per call or per thread.

A robust solution ensures that contracts with agencies are more transparent. All parties know, at the outset, where and how costs accrue. That level of visibility makes it less likely that nasty surprises will emerge when taking an application into production.

Predictability is significant in the federal space, where a single piece of legislation can create a massive new requirement. Should the call come to onboard 280 million new Medicare users, for example, issues of scale and affordability will be substantial.

What to look for

Given the importance of a vendor-supported approach to DevSecOps, what are the attributes of a strong open-source partner?

A DevSecOps platform should be optimized and complete, supporting everything from the hardware up to the application. It should be optimized for cloud scale, powering very large public and private clouds. It should include support for the complete range of needed tools: Linux, virtualization, cloud native, high availability, and management tools.

A robust solution ensures that contracts with agencies are more transparent.

The vendor should also be well-versed in the nuanced requirements of the federal government, where mission-specific needs combine with legal and regulatory constraints to drive development. A vendor seeking to support a federal DevSecOps platform should be fluent in these areas.

In addition, federal agencies will likely come to the table with some mix of legacy technologies and legacy applications. When it comes to DevSecOps, they'll want to work with a vendor that supports current technologies and past iterations, as well. Oracle Linux Premier, for instance, supports Linux versions 5 through 8, thereby helping to ensure the smooth functionality of legacy applications.

An ideal solution provided by a trusted industry partner also will be designed from the ground up for hybrid and multi-cloud environments, allowing agencies to derive maximum value from the solution. By shifting workloads seamlessly among all available resources, a ground-up hybrid and multi-cloud solution can offer greater resilience, enabling IT systems that go down to recover more quickly.

It makes sense to look for a cloud-native solution. This ensures a high level of portability, which in turn drives cost-effectiveness. Moreover, cloud is ideally suited to deliver the speed, scalability and ready availability at the heart of the DevSecOps approach. It's a natural fit in support of continuous integration and continuous deployment.

In addition, a strong solution should have uninterrupted support, especially for federal users doing mission-critical work. Oracle Linux Premier, for example, offers around-the-clock telephone and online support, as well as continuous access to enhancements, updates, and errata. Moreover, these support personnel have depth of expertise in the federal space, savviness that often surpasses knowledge of particular products.

Going forward

As federal IT shifts toward open-source DevSecOps, it's important to keep in mind that software development ultimately is a means to an end. The aim of DevSecOps is not just to accelerate applications development, it's to further the agency mission.

Taken together, Oracle Linux Cloud Native Environment and the Oracle Linux Premier service offering can help federal agencies to realize the cost savings and high productivity associated with DevSecOps, in an environment that is truly open, readily portable and cloud native.

Toward Open-Source DevSecOps

A conversation with Avi Miller, director of product management, Oracle Linux at Oracle.

Q: Why are federal agencies moving to DevSecOps?

A: They want to reduce the time it takes to get software into production. They want to work in the style of Facebook, Netflix and Airbnb, where they're pushing to production not once every three months but several thousand times a day.

They want increased deployment frequency, and they want automated deployments. They want to know that before a piece of code goes into production, it has been tested all the way through the lifecycle without requiring manual intervention to achieve that.

Q: Why is open source the best way to get to DevSecOps?

A: First, you have the many-eyes option, more people looking at the problem. Then there's affordability. As open source has become more popular, the ability to get resources has become cheaper.

There's also ubiquity. The DevOps space has been won by Linux containers and Kubernetes orchestration: Even if you go into the Windows side of DevOps, you're still running in containers. It's the same technology. It came from Linux, and you can even run it via a Windows Subsystem for Linux as well. So, your resource cost is lower with Linux, because this is the standard.

Q: Where has open source come up short for federal IT in the past?

A: One of the things that they're pushing back on is vendor lock-in. Some vendors have little tiny individual tweaks that you have to make to get your application to run on their stack. At an individual level, they don't seem that invasive, but when you add them all together, it means that once you've built your stack on their infrastructure, shifting it to somebody else becomes that much more difficult.

With Oracle Linux Cloud Native Environment, we're giving you the upstream builds of things like Kubernetes, and Istio, and Prometheus and all the rest of the good components, and at no point do we prevent you from adding your own stuff. If it runs on Kubernetes, you can run it on Oracle Linux Cloud Native Environment.

Q: How does the Oracle Linux Cloud Native Environment address security?

A: The Oracle approach gives you things like Ksplice, which can help to keep development compliant with the Common Vulnerabilities and Exposures (CVE) program by patching the kernel of master and worker nodes with no down time. It gives you things like NIAP and FIPS certification on the underlying hosts. We have security and compliance built into our operating environment to begin with.

Also, we can pay for the compliance testing that is required for federal agencies. Getting tested for security compliance costs a lot of money. You need a vendor backing you to make the ongoing costs of security and compliance testing affordable.

Q: Overall, what should government look for in an open-source solution?

A: Vendor-managed solutions are a good idea if they don't lock you into a high cost, and this is where most of those solutions unfortunately fall down.

Ideally, a vendor-supported solution lowers complexity, it addresses multi-cloud, and is easy for contracting. At Oracle we include the support of Oracle Linux Cloud Native Environment in your underlying OS support cost, so after you've paid Oracle for your support – for your underlying OS – you get everything else included.