GovCIO MEDIA & RESEARCH

DeepDives

DevSecOps Enabling HYBRID CLOUD

INSIDE:

SPONSORED BY

maximus

GovCIO MEDIA & RESEARCH

From the writer's desk

Kate Macri, Deputy Editor

DevSecOps Isn't Enough for Hybrid Cloud

Reliance on open-source software or hybrid cloud often gets a bad rap for increasing security risks in an organization. But federal IT leaders across defense and civilian agencies believe open-source software and hybrid cloud aren't inherently riskier than legacy approaches to software development and IT management — ultimately, culture and operational imperatives will drive risk.

DevSecOps enables a secure shift to hybrid cloud across government, but tracking software components, changes and lines of code through a software bill of materials (SBOM) and configuration management are critical for maintaining a strong cybersecurity posture in hybrid cloud.

As federal agencies adopt hybrid-cloud solutions, network visibility and transparency will be paramount. DevSecOps is just the first step in a long journey toward an agile, security-first culture that develops new cloud capabilities responsibly.

Table of Contents

Kate Macri
Deputy Editor

Sarah Sybert
Senior Researcher

The Armed Services Wish List for Hybrid Cloud Security

Defense cloud leaders dissect cloud security myths and challenges, with DevSecOps and zero trust as the pillars of a secure hybrid cloud.

BY KATE MACRI

Special Operations Command (SOCOM) and the Defense Information Systems Agency (DISA) expect to roll out groundbreaking cloud capabilities next year, such as a SOCOM version of WhatsApp and a highly customizable DevSecOps platform to help the Fourth Estate shift to hybrid-cloud solutions more quickly and securely.

The impetus of these cloud initiatives includes improved user experience, network visibility and control to meet mission demands, according to DOD cloud leaders.

"We need hybrid cloud because we need to be able to move workloads anywhere and everywhere at any point in time," Army Enterprise Cloud Management Agency's Former Director Paul Puckett told GovCIO Media & Research in an interview.

Photo Credit: Senior Airman Christopher Stolze/DVIDS

The idea of hybrid cloud being more secure than legacy or on-premise IT infrastructure is a popular narrative in the IT community, but DOD cloud modernization leaders believe this is a myth.

For the defense community, hybrid-cloud migration is about improving efficiency and user experience. Hybrid cloud comes with a new set of cybersecurity risks, but also offers opportunities to strengthen cybersecurity posture in the long run and to capitalize on new capabilities and methods such as DevSecOps and zero trust.

(ctd.)

Improving User Experience Without Compromising Security

SOCOM Network Modernization Chief Operating Officer (COO) Col. Joe Pishock said commercial cloud is “giving us options that we haven’t had resident to SOCOM the last 15 years” with secure, cloud-connected communications in theater.

“The ability to extend, to go mobile, is greater because of cloud but then it presents challenges because I’m not really extending government services, I’m trying to extend collaboration tools or connect people with partners (not via SIPR or NIPRnet),” Pishock said in an interview with GovCIO Media & Research.

SOCOM’s cloud-enabled communications app — similar to Facebook Messenger, Signal or WhatsApp in the commercial market — intends to solve communication challenges between SOCOM and allied partners in theater. The app is currently in beta testing with U.S. Army Special Operations Command (USASOC) in the IndoPacific region after a successful deployment in Europe.

Pishock describes it as “a suite of collaboration tools coming out of a tactical mission network.”

“SOCOM exists for human-to-human interaction, and that is enabled by IT,” he said.

If SOCOM doesn’t create its own secure, collaborative communication tool, service members and allied partners will resort to those commercial apps, which come with a wealth of cyber and information security risks that the service can’t fully control.

“All of that is basically prohibited by regulations, but people are still going to do it,” Pishock said. “If we can do better than a third-party app, then we’re trending in the right direction — something that at least goes into an environment where we have the potential to control it or influence the data. No policy in the world seems to prevent third-party apps from emerging and that’s where (we need to) do better.” (ctd.)

Photo Credit:
whiteMocca/Shutterstock

Creating its own app allows SOCOM greater visibility and control while providing the user experience requested by service members and allied partners.

The app is successful because a limited number of people can access it and SOCOM can iterate the app across service components "with a lower level of risk … not at the level of NIPRNet (DOD's unclassified network)," Pishock added.

One persisting challenge involves determining the best way to secure the app. Because the app doesn't live on the Department of Defense Information Networks (DODIN), it's not subject to the same security regulations, despite security being a crucial component of communications with allied partners in a mission environment.

Typical cybersecurity measures such as scanning and patching don't really apply, Pishock said, so SOCOM must innovate to meet mission demands.

"How it's secured is what we're trying to figure out," he said. "How do we meet the intention of the information security and cybersecurity and do so in such a way that we can't follow the letter of the law because we don't have any law for these spaces yet? How do we do that, small scale?"

SOCOM CTO Mark Taylor believes a zero trust approach to cybersecurity will be the answer to some of these questions.

"Zero trust is the baseline principle of how we need to treat all networks, whether they be cloud-based or something internal moving forward," he said in an interview with GovCIO Media & Research. "DOD is still trying to figure out what it looks like. It's not a widget you buy, it's several tools you buy working in concert. Zero trust is the method. Having a strict identity management or ICAM strategy in place is the foundation for that. Zero trust is the Y2K of 2022 for the government."

How DevSecOps Can Optimize Hybrid Cloud Security

At DISA, the upcoming DevSecOps platform — called "Vulcan" — aims to maintain cybersecurity while enabling swift hybrid-cloud migration and improved collaboration for the Fourth Estate.

Alex McFarland, DISA's technical lead for the Vulcan program, said Vulcan

Photo Credit: Gorodenkoff/Shutterstock

"gives people what they need to level themselves up."

"We're trying to provide tools that make the work they're doing visible to ease collaboration across silos," he told GovCIO Media & Research in an interview. "The goal is to make change safe through automation … and by improving safety, improve velocity."

Dave Lago, a product manager at DISA's Hosting and Compute Center (HACC), described Vulcan as a set of "self-service tools" for DevSecOps to ensure DOD components integrate security policies into the beginning stages of software development, especially regarding configuration management.

"It's an economic play, all these teams need software development, DevSecOps tools, and it's cost-prohibitive to do it yourself," he told GovCIO Media & Research in an interview.

"This will be consistent and is consistent with what the Thunderdome team is doing," he added, referencing DISA's Thunderdome zero trust prototype.

One of the major goals of Vulcan is to increase visibility of network assets and applications and allow teams to respond quickly to known vulnerabilities and tweak lines of code within an infrastructure-as-code (IaC) environment to improve efficacy, efficiency and security.

"IaC allows for representation of the environment that's codified in text files, which can be checked for vulnerabilities before you deploy," McFarland said. "Surfacing all that knowledge and that collaboration, I think, is what really kind of addresses our largest issue. It will increase, it will improve visibility in terms of like an audit trail (of code changes) and what we're doing and how we deliver and improve sharing and all the rest."

Hybrid Cloud Security Challenges Come Down to Configuration

Improved user experience, network visibility and control are frequently cited as top cloud modernization goals for armed services and DOD components

as they explore hybrid-cloud solutions, including the U.S. Army, which will continue its aggressive cloud push in fiscal year 2023.

For Puckett, hybrid cloud isn't more secure than legacy or on-premise IT infrastructure and vice versa. The Army isn't interested in hybrid cloud for enhanced cybersecurity, but rather improved mobility, visibility and control over assets and users, which will allow the Army to develop more agile cybersecurity strategies and responses.

"Now we've got our cyber with visibility into the entire cloud ecosystem simply at the account level and now they can see and be able to manage risk in real time and how they defend the network," Puckett said. "But then part of that is us working with them, it's getting visibility turned into understanding, it's building those skill sets."

Like DISA's Vulcan leads, Puckett considers IaC and configuration-as-code (CaC) as "100% an imperative" for developing a sound hybrid cloud security strategy.

"For instance, the way that we deploy from a [secure cloud computing architecture] (SCCA) component in cArmy (the Army's global cloud environment managed by ECMA) is we are leveraging IaC and CaC to the greatest extent possible in order to have repeatability and high confidence in the configurations that we're putting out in the environment," Puckett said.

Puckett believes operational imperatives will drive risk in hybrid-cloud environments, which means authorizing officials and commanders need to evaluate cloud versus legacy IT tradeoffs and manage expectations about what a secure hybrid-cloud environment should look like.

Cloud security breaches often come down to poor configuration management, he added. In Puckett's view, breaches tend to happen at the same rate in the cloud as they do in on-premise infrastructure.

"If you look at the Capital One breach, people would blame the cloud service provider for the issue," he said. "It's like, well, the issue was a

Photo Credit: Natali_Mis/Shutterstock

misconfiguration on the user side of the house, not the provider side of the house. Oftentimes you get these labels of things being insecure or even go take it further and say this data is really sensitive, so I'm not going to put it in the cloud, I'm going to put it on premise. And that would imply that simply being physically located on premise makes it more secure. And I'd ask the question, have we ever had data breaches for services and data running on-premise? And the answer is yes, right? So is it inherently more secure? No. I'm able to physically touch the server, but when it comes to access to the data, the system as it's designed, if you're not patching or updating those capabilities and you're connected to any type of network, you are vulnerable. And so there's training that has to happen for people to understand."

Although cloud migration doesn't necessitate better cybersecurity, the key to holistic cybersecurity improvement is increased visibility and translating cybersecurity data to actionable knowledge.

"Part of our challenge even today, there's so many logs and alerts and all these different things," Puckett said. "How do you know what matters or what doesn't matter? I think that's a challenge that's always really existed, which is why you see so many companies that have tools or like we can help you make sense of all this information, we can help you make sense of it. It's not just visibility, it's understanding."

Puckett also believes zero trust can help translate knowledge of a hybrid cloud's security state into action.

"Hybrid cloud, if we're going to be thoughtful about it, requires we move on the zero trust journey," he said. "It's a journey of removing implicit trust over time. Moving to a hybrid-cloud environment is just another opportunity to get after that hard work."

Photo Credit:
Natali_Mis/Shutterstock

“Infrastrucure-as-code allows for representation of the environment that’s codified in text files, which can be checked for vulnerabilities before you deploy.”

— Alex McFarland, Vulcan Program Technical Lead, DISA

GovCIO MEDIA & RESEARCH

DeepDives

The Ultimate Cloud Modernization Checklist

A DevSecOps approach to software development can enhance cybersecurity in hybrid cloud architecture, but requires a new way of thinking about IT.

- ✓ **Zero Trust**
- ✓ **Software Bill of Materials**
- ✓ **DevSecOps**
- ✓ **Configuration Management**
- ✓ **Environment-as-Code**
- ✓ **Infrastructure-as-Code**
- ✓ **Data Governance**

GovCIO MEDIA & RESEARCH

PARTNER INTERVIEW

maximus

How DevSecOps Improves Cybersecurity in Hybrid Cloud

Collaboration, communication and good cyber hygiene are critical elements of the DevSecOps approach to software development.

Kynan Carver, DOD Cybersecurity Lead, Maximus

How is your organization building a culture of security with collaboration between security teams and developers?

Carver At Maximus, we believe everyone has a role in protecting the security and integrity of the systems and environments. Therefore, we establish a culture of security from the start, fostering a shared sense of responsibility between development, operations and security teams. We achieve this through educating all stakeholders. All teams undergo security training to understand the importance of a threat-driven approach to application development so that everyone understands and is prepared for their roles in attack prevention and incident response. Through continuing education and fostering a shared sense of responsibility, we help drive a culture of continuous improvement that ensures organizations stay ahead of evolving threats.

(ctd.)

“Through continuing education and fostering a shared sense of responsibility, we help drive a culture of continuous improve-ment that ensures organizations stay ahead of evolving threats.”

— Kynan Carver, DOD Cybersecurity Lead, Maximus

How can agencies increase visibility and detection of network vulnerabilities and threats?

Carver Shifting to a zero trust architecture will be vital for agencies to increase their threat visibility across hybrid and multi-cloud environments. As data plays a vital role in the success of zero trust environments, we help agencies implement advanced data analytics to continuously monitor and analyze data across the enterprise. Through the real-time analysis, we can proactively predict user behaviors, understand network traffic, and watch application logs to identify potential security threats and risks. With this critical information, we can quickly communicate and collaborate with development teams to enhance security during the application-development process and enable operations and security teams to better protect their systems and environments.

Where do you see opportunities across government to integrate DevSecOps principles?

Carver DevSecOps may be a good option for agencies producing government-owned code, as this has traditionally been built using waterfall development processes. With the waterfall methodology, agencies follow a linear development process, which makes it harder to quickly pivot when making security changes, updates or iterations. This can also slow the time to deliver new services. Another opportunity for agencies to integrate DevSecOps is when they are migrating to the cloud. Many cloud service providers incorporate technology like containerization and serverless deployment, and these cloud-native technologies enable developers to focus on the development of the actual code rather than focusing on the performance of the underlying infrastructure.

Innovation flexibility without compromising security

We provide secure, agile delivery of modern applications that keep pace with the mission

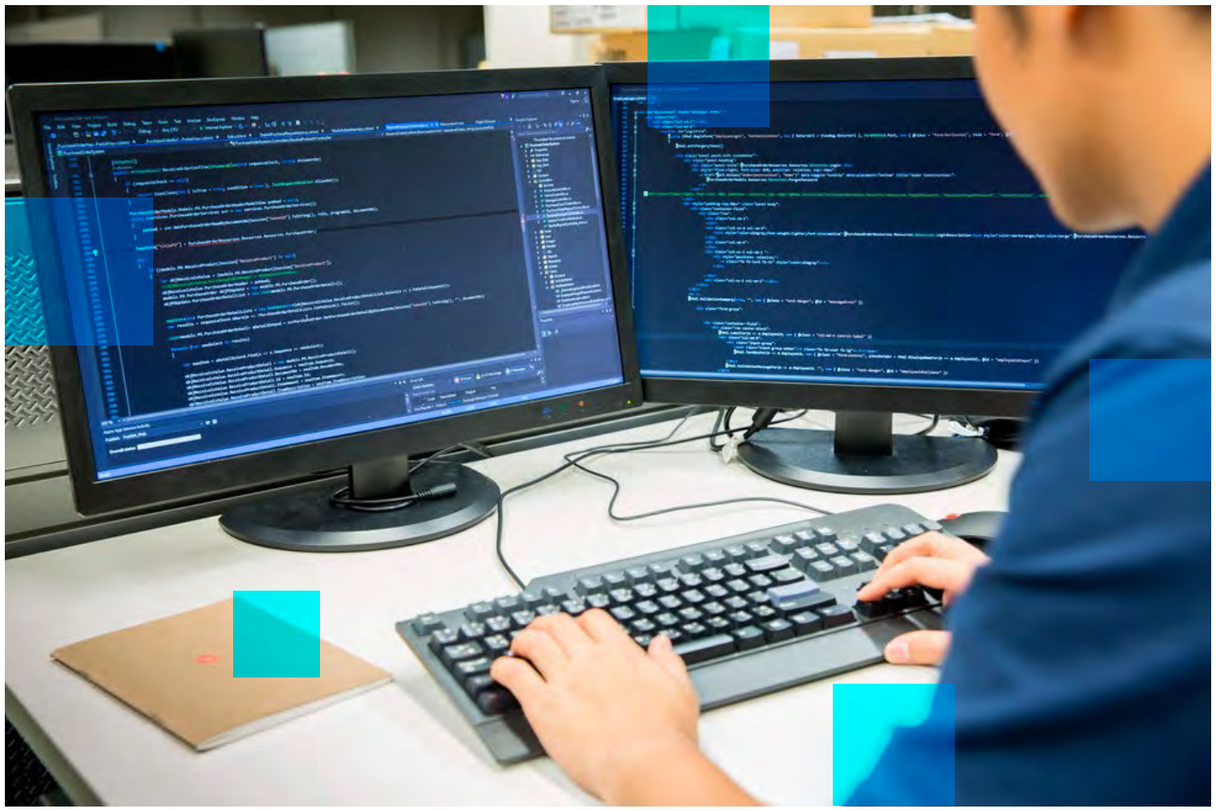
Learn more:
maximus.com/digital-modernization

maximus

Feds Working to Secure Open-Source Software

DevSecOps practices could secure open-source technology as new threats emerge.

BY SARAH SYBERT



Open-source software offers greater agility, flexibility and transparency to keep pace with the evolving threat landscape. Now federal agencies are honing in on boosting security in an open-software world.

President Biden's 2021 cybersecurity executive order catalyzed government's robust approach to cybersecurity and called for agencies to increase visibility into and detection of cybersecurity vulnerabilities and threats to agency networks.

"What the executive order does is it recognizes that fundamentally we are not going to make this space secure. What we are going to do is we're going to make it defensible. And so we're employing new policies and new ways of thinking about security so that you are no longer looking at just the perimeter. We are looking at everything inside that perimeter," Director of Federal Cybersecurity at the Office of the National Cyber Director Phil Stupak said during GovCIO Media & Research's Zero Trust event in September 2022.

Since the executive order was released, agencies have developed additional policies — like the Securing Open Source Software Act of 2022 and the memo on Enhancing the Security of the Software Supply Chain through Secure Software Development Practices — to continuously improve security and protect the supply chain.

As agencies move toward a more transparent approach for software development, they're turning to solutions like software bills of materials (SBOMs) and open source to provide a formal record containing the details and supply chain relationships of various components used in building software and make software more accessible.

Open-source software is code that is designed to be publicly accessible. This means anyone could inspect, modify or enhance it. The cross-government transition to open-source software provides flexibility to free agencies from vendor lock-in and enable them to scale and change with the environment.

"Open-source software brings added flexibility to government-off-the-shelf

Photo Credit: PW Photograph/Shutterstock

software production since government developers can now focus on the application of software rather than solving a problem that's already been solved," Defense Digital Service Expert Nicole Thompson told GovCIO Media & Research.

Introduced earlier this year, the Securing Open Source Software Act of 2022 would "establish the duties of the director of the Cybersecurity and Infrastructure Security Agency (CISA) regarding open-source software security," requiring CISA to assess open-source software components used directly or indirectly by federal agencies. SBOMs play a critical role in the bill as they enable CISA to assess the components of open-source software.

Sen. Rob Portman said during a Sept. 28, 2022 business hearing, "This bill (Securing Open Source Software Act of 2022) comes out of our hearing we had on this topic and months of discussion … it ensures that the U.S. government anticipates and mitigates security vulnerabilities in open source software to protect America's most sensitive data."

The bill adds to the cross-government push to secure supply chain and improve transparency of software products. In September 2022, the Office of Management and Budget (OMB) issued a memo on Enhancing the Security of the Software Supply Chain through Secure Software Development Practices, which calls for agencies to use software built with common cybersecurity practices.

The memo also set new deadlines for federal agencies to inventory software, develop communication processes and provide training for personnel, adding to the push for greater transparency across software development and move away from the traditionally siloed development approach.

"Open-source software has crowd-sourced software development, which is in contrast to closed-source single-team, single-product deployments," Thompson noted. "The diversity of thought that can be applied to a problem set by inviting a multitude of people to collaborate on a product enhances the final product."

(ctd.)

“DDS often quotes, ‘Open-source software is inherently more securable than closed-source software.’ This does not mean that open-source software is automatically more secure, but we have the ability to see the software supply chain and are able to take advantage of that.”

— Nicole Thompson, Expert, Defense Digital Service

While there is more transparency within development, that doesn’t mean there is more inherent security. A common misconception is that open-source is more secure than closed-source; however, this is not the case, Thompson said.

“DDS often quotes, ‘Open-source software is inherently more securable than closed-source software.’ This does not mean that open-source software is automatically more secure, but we have the ability to see the software supply chain and are able to take advantage of that,” Thompson said.

One way government could bake in security as it transitions to open-source is leverage DevSecOps practices. DevSecOps integrates application and infrastructure security seamlessly into Agile and DevOps processes and tools to address security issues as they emerge — when they’re easier, faster and less expensive to fix — often using automation. (ctd.)

DevSecOps makes application and infrastructure security a shared responsibility of development, security and IT operations teams, rather than the sole responsibility of a security silo. By automating the delivery of secure software, agencies aren't slowing the software development cycle.

In November 2022, the National Cybersecurity Center of Excellence announced a new project uniting software supply chain and DevOps security practices. The project will apply DevSecOps practices in multiple proof-of-concept scenarios that involve different technologies, programming languages and industry sectors. The center will use closed-source and open-source technology to demonstrate these use cases.

"The intention is to demonstrate DevSecOps practices, especially using automation, that would apply to organizations of all sizes and from all sectors, and to development for information technology, operational technology, 'internet of things' and other technology types," the project description states.

The project will produce actionable guidelines to help organizations integrate security practices into development methodologies. Organizations could then apply these guidelines when choosing and implementing DevSecOps practices to improve the security of the software they develop and operate.

"DDS values the open-source software community — it's a cultural tenet of DDS. We open source many of our products and our employees also contribute to open-source projects. We want to bring as many secure coders to the process to leverage the advantages of diversity of thought," Thompson said.

Photo Credit:
Chinnapong/Shutterstock