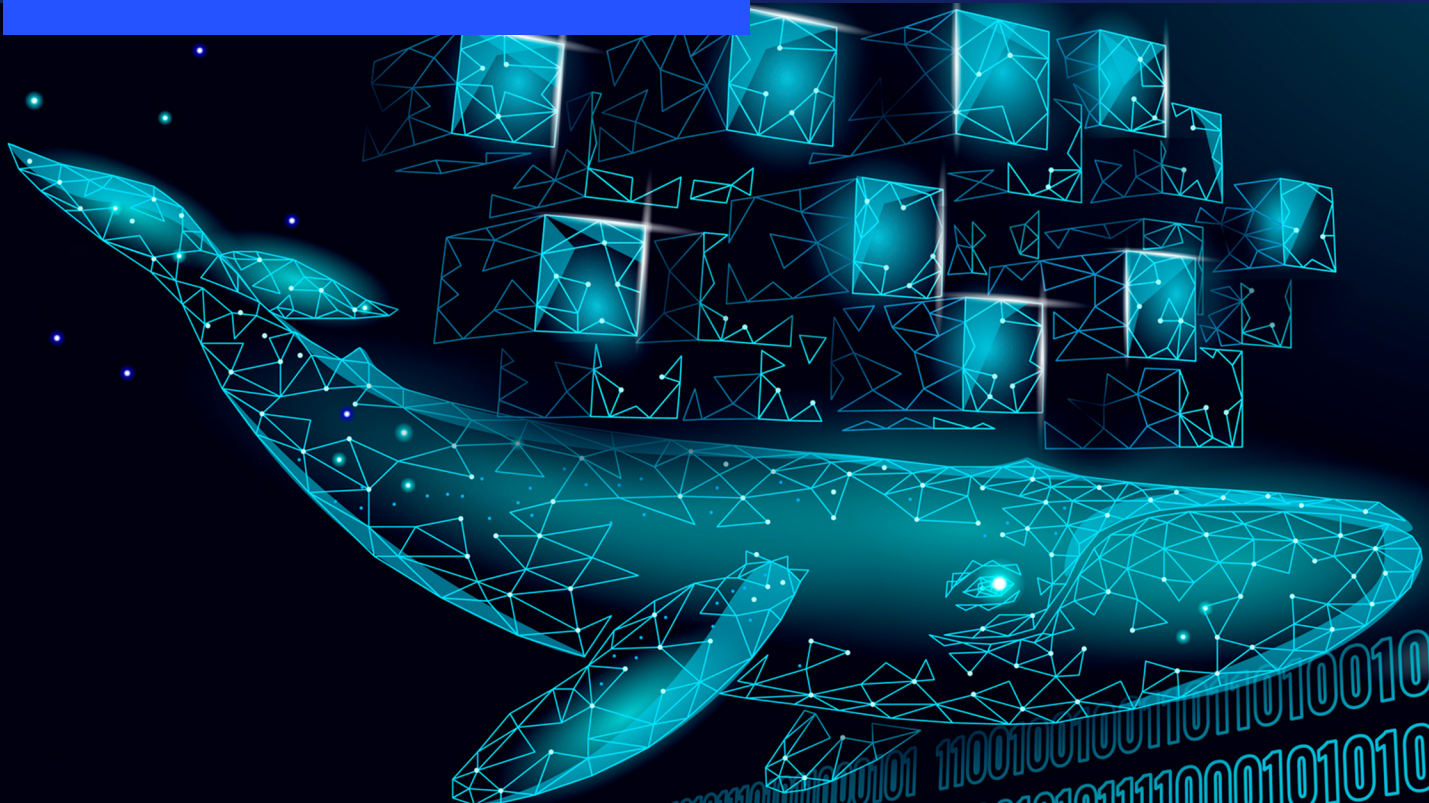


EXPERT EDITION

How to secure containerized applications



Insights from

- FAA
- NASA
- Software Engineering Institute

BROUGHT TO YOU BY

Driving Mission Success with Kubernetes.



Delivering secure, certified, open source and cloud-native solutions exclusively for the U.S. Government adopting containers and Kubernetes across the IT landscape.

Learn more at ranchergovernment.com



RANCHER



RKE 2



LONGHORN



K3S



HARVESTER



NeuVector
Full Lifecycle Container Security

TABLE OF CONTENTS

Is simplicity the secret to success in DevSecOps? 4

How FAA uses DevSecOps for mission support apps ... 7

NASA adopts SAFe to make dev more agile, secure 9

Why containers require novel approach to cyber 11



When it comes to dev — agencies seek the trifecta: agility, transparency, security

Containers just make sense for federal agencies.

For starters, they make it swift to launch cloud-native applications. But if you think about IT in the federal government and the need to maintain ongoing services that run legacy code, containers become really appealing. They create a way to rationalize an organization's legacy code, package code that needs to continue running in containers and then run those containers on modern cloud and hybrid platforms.

And legacy code is a reality for the foreseeable future. Consider the nation's space agency.

"NASA has been around for a long time. We do have quite a bit of legacy code on older platforms," points out Shenandoah Speers, the agency's director of application and platform services. Speers' team has begun rationalization work so that it can containerize needed legacy code to run on newer platforms and reduce NASA's technology debt.

The use of containers will also help the agency continue to become more agile and make the most use of its continuous integration and continuous deployment pipeline for software development.

The Federal Aviation Administration is on a comparable path. It's even created a container-specific CI/CD pipeline. The primary goal? Enable mobility between hyperscale cloud environments or even cloud and on-premise infrastructure so that apps can reside wherever they need to, explains Sean McIntyre, director of solution delivery at FAA.

But there is a rub. "The challenge with containers is there's really no place to put an endpoint detection and response agent on the container itself," McIntyre says. Containers require new cyber tactics.

With this ebook, we want to highlight efforts by agencies to gain visibility into containers and to ensure they can adequately provide cybersecurity through the latest tactics and tools.

We hope that the information proves helpful to your agency's work in using containers and implementing development, security and operations (DevSecOps) pipelines to support software development that's agile, transparent and secure.

Vanessa Roberts
Editor, Custom Content
Federal News Network

Is simplicity the secret to success in DevSecOps? SEI's Greg Touhill says 'yes'

BY ROBERT O'SHAUGHNESSY



Supporting an application only after its release isn't enough to keep it secure. Security must be top of mind throughout development.

That is core to the development, security and operations (DevSecOps) model. And it's also an important principle for federal agencies to bear in mind when making acquisition decisions, said Greg Touhill, director of the CERT Division at Carnegie Mellon University's Software Engineering Institute and a former federal security IT official in the White House, Homeland Security Department and Air Force.

"In the past, we've seen security relegated as an add-on by the requirements team and the folks who are doing acquisition," Touhill said during an interview with Federal News Network's Jason Miller for [Federal Monthly Insights – Securing Containerized Applications](#). "Security was never articulated upfront as a requirement in most government organizations. Ever since, we've seen some very active activities involving nation state

actors, as well as organized criminal groups, targeting government systems in particular."

Increasingly, customers want security to be a major consideration throughout the development process. This has led to changes in how developers build applications.

"We're seeing folks saying, 'Hey, we need to be incorporating security in our software acquisition as well as development.' So, there's a great deal of emphasis now on including security upfront as a requirement. And as a result, I think that folks who are incorporating DevSecOps as part of their software development process are discovering that, independent of the platforms that are out there, you're getting a better product that's going to require less maintenance, because it in fact has a disciplined engineering process behind the development of the code," Touhill said.

“It’s less art than science. And in the past, we would just basically have folks do a lot of artistic work in software but without the engineering rigor. Now we’ve got the engineering in place with DevSecOps.”

Containerization is an important part of the security piece when developing applications. Done correctly, containerization can make a system more mature and lower costs while accelerating operational capabilities, Touhill said. By spinning up a virtual machine and setting up containers to run certain processes, an administrator can take it apart electronically when those processes or apps are no longer needed, he explained. Plus, that saves time and money by negating the need to buy a big new computer.

“It’s very exciting. And the fact of the matter is that we see more and more folks investing in the security of containerization and the applications that are running within them,” Touhill said.

Less complexity helps improve security

Complexity is antithetical to security, meaning that systems should be simple to use for the intended users, Touhill said.

“When it comes to implementing these technologies, we want the complexity to be put on the back of the folks who are trying to attack us, not on the folks that are trying to leverage the technologies,” he said.

Containerization helps accomplish that simplicity goal by improving the user experience, Touhill said, adding that there



Folks who are incorporating DevSecOps as part of their software development process are discovering that, independent of the platforms that are out there, you’re getting a better product that’s going to require less maintenance.


— Greg Touhill, Director, CERT Division, Carnegie Mellon University’s Software Engineering Institute

remains a lot of progress to be made at improving user experience.

“As you take a look at the complexity and the impacts of complexity, I think we still have a ways to go,” Touhill said. “Because there is a measure of complexity, particularly with trying to interface and bind together all the different types of technologies and different products. If you almost get if you are going to pick a container, you only can pick one without having some unique interface issues. ... You still can use multiple types of container technologies. It just increases the degree of difficulty for the operators that are trying to get things done.”

Today, Touhill and his team are looking to continue innovating in the realm of DevSecOps. Areas of research include determining how to detect whether the firmware on a chip has

been altered or corrupted in the manufacturing or distribution process as well as the interconnectivity between enterprise IT and edge IT.

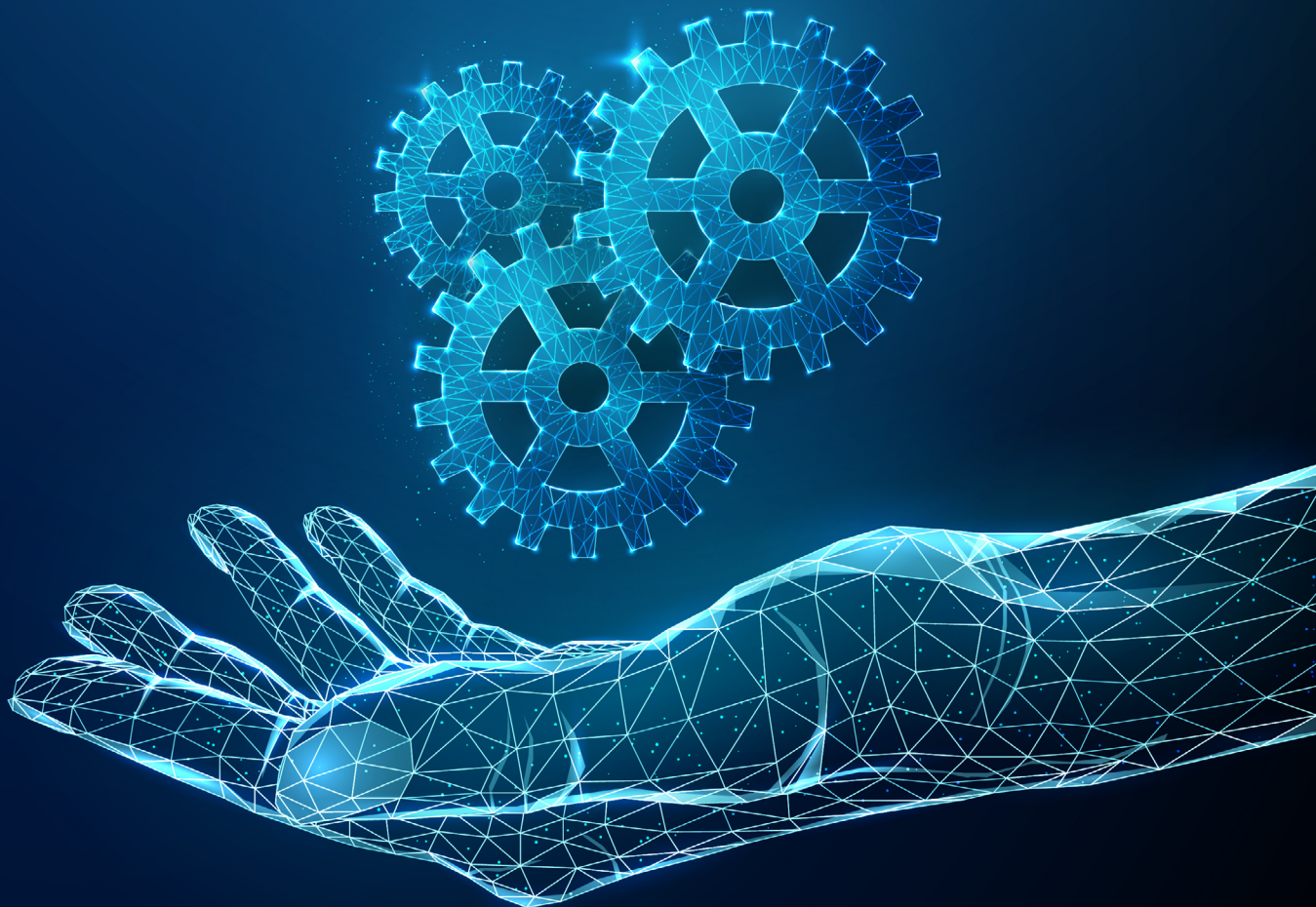
“Enterprise IT is not the sole definition of your cyber ecosystem,” Touhill said, “because you’ve got industrial control systems, operational technology, and Internet of Things and spectrum-enabled devices like your cell phones and mobile devices.” 

Listen to the full discussion between Federal News Network’s Jason Miller and the [Software Engineering Institute’s Greg Touhill on keeping DevSecOps simple.](#)

“

When it comes to implementing these technologies, we want the complexity to be put on the back of the folks who are trying to attack us, not on the folks that are trying to leverage the technologies.

— Software Engineering Institute’s Greg Touhill



FAA embraces DevSecOps for mission support applications



BY DAISY THORNTON

The Federal Aviation Administration has more than 700 applications that support its mission, from human resources and finance to aircraft safety. It's been working to leverage a development, security and operations (DevSecOps) approach for those applications, though it hasn't gotten to all its legacy apps yet.

But the agency has gained great portfolio insight by following the Chief Information Officers Council's application rationalization playbook, said Sean McIntyre, director of solution delivery at FAA.

Initially, there was some confusion about what it meant for an application to be on the DevSecOps tool chain, he said.

"When I first came to the FAA in 2018, I was told that 80% of our legacy apps were on the DevSecOps tool chain, which sounded pretty great," McIntyre said on [Federal Monthly Insights – Securing Containerized Applications](#).

"But when I dug deeper, it became clear that my teams thought that merely using our code repository qualified for being on the tool chain. And given that criteria, it wasn't so great."



We created a repeatable process we call 'four factoring' an app and, since then, we've made a lot of progress applying DevSecOps — even to our legacy portfolio.

— Sean McIntyre, Director of Solution Delivery Service, Federal Aviation Administration

To solve this, FAA adopted a clear definition of what constitutes tool chain integration by turning to the Heroku 12-Factor App model and identifying four minimum factors for tool chain integration. "We created a repeatable process we call 'four factoring' an app and, since then, we've made a lot of progress applying DevSecOps — even to our legacy portfolio."

The four-factor approach enables security governance to be built into the tool chain.

The platform handles logging, monitoring and sending everything to the security operations center. It also performs automated vulnerability scans, because McIntyre said FAA wants the platform to handle as much as possible, so the developers don't have to worry about it.

Many of FAA's applications are in the cloud in legacy form, he said. The team therefore is primarily focused on refactoring them for containerization but leaving them monolithic. That abstracts the business logic from the operating system and makes the applications more mobile. The primary goal is to enable mobility between different hyperscale cloud environments or even cloud and on-premise infrastructure. McIntyre wants applications to be able to go wherever they make sense.

Creating comparable dev experiences

Toward that end, FAA is building a container-specific DevSecOps pipeline so that the development experience is the same, and the workloads can be moved wherever they're needed.

"The challenge with containers is there's really no place to put an endpoint detection and response agent on the container itself," McIntyre told [The Federal Drive with Tom Temin](#). "And so we've invested in tools that are able to scan – in real time, in production – the containers while they're running. So, it is a special case with containers once it's in production because you're not going to put something right on it."

McIntyre's primarily concerned about the supply chain of the containers FAA uses. If the agency accepts a container image from somewhere else, it doesn't always know what's



The challenge with containers is there's really no place to put an endpoint detection and response agent on the container itself. And so we've invested in tools that are able to scan – in real time, in production – the containers while they're running.

– FAA's Sean McIntyre

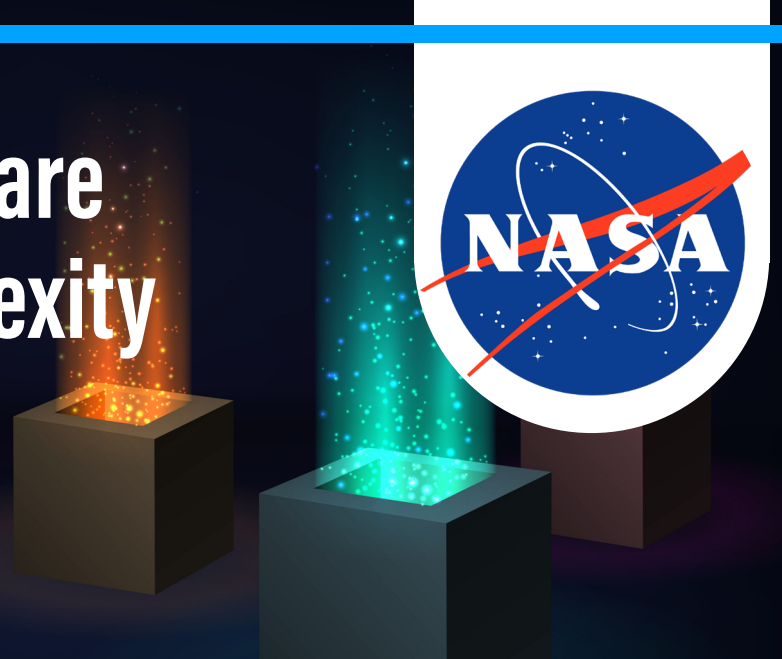
in that container. FAA uses tools to ensure container images are only from trusted sources and scans them constantly, he said. That way the team can inject code into clean, hardened containers rather than accepting complete packages that could be compromised.

"I've always said that the culture of an organization reflects its mission, and the FAA needs to be meticulous in their mission. And that's the culture of the agency," McIntyre said. "And a lot of times it seems like the FAA is slow to move forward. But it's because they're thinking about it. They want to make sure that the moves and decisions that they make are the right ones. But once they make them, they really get going on it."

Listen to the full discussion between The Federal Drive's Tom Temin and [FAA's Sean McIntyre on embracing DevSecOps for mission support.](#)

NASA reduces software development complexity through use of SAFe

BY ROBERT O'SHAUGHNESSY



Like most federal agencies now, NASA runs on software. Rockets are what the space agency may be known for, but controlling those rockets and interpreting data, even handling human resources and finances, all require software.

Currently, NASA has over 1,000 software features in development that leverage an agile dev process.

“We’ve been on a journey to embrace the agile mindset. As part of this journey, we have adopted that Scaled Agile Framework for Lean Enterprises, or SAFe, as part of the software system development lifecycle,” said Shenandoah Speers, NASA’s director of application and platform services in the Office of the CIO for [Federal Monthly Insights - Securing Containerized Applications](#).

SAFe has helped the agency align its strategy to execution, Speers said. The framework lets NASA visualize and prioritize its workload so that it can understand the capacity of its dev teams to handle that workload and deliver value incrementally, he said. SAFe “also provides us a way to get fast feedback from our stakeholders and our business partners through system

“

We’ve been on a journey to embrace the agile mindset. As part of this journey, we have adopted that Scaled Agile Framework for Lean Enterprises.

— Shenandoah Speers, Director of Application and Platform Services, NASA

demos, and program increment planning events,” Speers added.

Speers’ team has created a development, security and operations (DevSecOps) pipeline platform that supports on-demand continuous integration and continuous deployment (CI/CD) using containerization to automate the build security, scanning and deployment process.

Integrating cyber in dev

A lot has changed over the last decade to make sure that cybersecurity is part of what Speers' team releases, he said. The DevSecOps model is critical in helping ensure cybersecurity during development.

"We've kind of shifted our cybersecurity to the left ... where we try to automate the security scanning at the beginning of the software development, and that allows our software developers to get a better understanding of those security vulnerabilities ahead of time," Speers said on [The Federal Drive with Tom Temin](#).

All of the team's code and associated code configurations are stored in Git repositories, which control and track versioning. The use of the CI/CD pipeline provides built-in triggers throughout the build process for things like static application security testing. The pipeline also automatically deploys code images throughout the dev process.

"Once the developer is ready, these images are then submitted through the deployment phase of the pipeline and then go through the dynamic application security testing, and that's performed, as well as auto deployment through our staging environment. And then once all of that is successful, it is finished. It's deployed to a production environment," Speers said.

As automation becomes more prevalent in software development, NASA still wants to have humans involved when needed.

"We also support humans in the loop," Speers said. "As we go through this pipeline that we've

developed, some of our stakeholders still want humans to be in that loop. And so we do support humans in the loop, as well as fully automated deployment."

Like automation, open source is also prevalent. A concern some share is that open source software can be insecure. But Speers said the opposite is true.

"One good thing about open source is typically it is very secured, because you've got multiple people reviewing it and looking at it," he said. "And so we do utilize that open source, and we ensure that the open source is secured itself."

Finally, NASA has a long, storied history, meaning that there is legacy code that must be managed and maintained.

"NASA has been around for a long time. We do have quite a bit of legacy code on older platforms," Speers said.

To manage and run necessary legacy code in new environments, NASA is in the process of conducting application rationalization. That will reduce the technical debt of the older code, Speers said. Ultimately, the plan is to move critical legacy code to containers to run on the newer platforms. 🚀

Listen to and watch the full discussion between The Federal Drive's Tom Temin and [NASA's Shenandoah Speers on the space agency's agile evolution](#).

Cybersecurity in the containers age requires a new strategy



BY TOM TEMIN

Federal agencies – along with most large organizations – are steadily moving to a new generation of technology in the deployment of software applications. Regular run-time code gave way to virtual machines, and now virtual is yielding to containerization managed under frameworks like Kubernetes.

The use of containers enables more agile code deployment in the hybrid, multicloud environments that characterize the information technology setup at many agencies.

Here's how Tom Hance, director of container security at [Rancher Government Solutions](#) put it: "Use of containers, specifically Kubernetes, is kind of exploding in the marketplace. It's recognized as just a much more effective method for DevOps teams to produce applications. They're more agile. They can deliver on time and with a higher-quality product, using microservice-based containers, than they could with, let's say, a hardware or VM environment of the past."

This methodology brings a new set of cybersecurity risks that IT staffs must mitigate, Hance said. Standard scanning and monitoring tools cannot see what is inside of containers, for instance. What happens when they combine functionally via application programming interfaces (APIs)?

Network administrators and security operators "really have no idea what application protocols or what packet content is flowing across their cluster" without that visibility, Hance said. "And if you have security in your title, that is a big issue."

Reframing security requirements for containerized apps

Traditional layered security approaches that scan software images and runtimes don't



That's really our differentiation. We can stop malicious code execution in line before it can damage a container, a pod, an application or the system kernel.

— Tom Hance, Director of Container Security, Rancher Government Solutions



Our adversaries are extremely sophisticated. They're much more sophisticated than just looking for an open common vulnerability or exposure that hasn't been patched.

— Rancher Government Solutions'
Tom Hance

equate with security in the containerized world, he said.

Defense-in-depth techniques “don't actually have the ability to protect your containers because they don't sit in line with live traffic in between container pairs and govern what is allowed to cross that demarcation point,” Hance said.

This is where Rancher's NeuVector comes in. It's designed specifically to protect containerized workloads, he said.

“We not only hold the position between each container pair, but we have visibility into the application and packet levels to make accurate decisions on what gets to pass in live traffic,” Hance said. The product doesn't scan images or logs after something might have occurred. Instead, it halts execution of malicious code, he said.

“That's really our differentiation,” Hance said. “We can stop malicious code execution in line before it can damage a container, a pod, an application or the system kernel.”

Hance noted that the same vectors for malicious code exist for containerized development as for traditional development methods. Phishing, something coming in from social media, something in open source software or something in an image a developer has downloaded to incorporate. Once malicious code becomes incorporated into a container, then you need a specific tool like NeuVector to detect and stop it, he said.

The product itself is architected as a Kubernetes-native container, so it can run at wire speed and will not degrade application performance, Hance said. Because deep packet inspection can see application protocols, packet content and payload, it results in what Hance called contextual security for containers. He said that's a level of security that agencies can't obtain with scanning products running at the network layer (Layer 3).

“I think our adversaries are extremely sophisticated,” Hance said. “They're much more sophisticated than just looking for an open common vulnerability or exposure that hasn't been patched and applying that to gain access to our nation's critical assets. Agencies should be migrating to this new type of protection.” 🤖

[Listen to the full discussion between The Federal Drive's Tom Temin and Rancher Government Solutions' Tom Hance on how to best secure containerized apps.](#)