

## **EXECUTIVE BRIEFING SERIES**

# **How automation can help defend against mounting cyberthreats**



# Red Hat Solutions

**Provided by Emergent**

We are dedicated to tackling the world's toughest technology challenges.

We are a proven, customer-focused solutions provider with a team of trusted subject matter experts, steadfast in our commitment to delivering dynamic solutions for a proactive approach to transforming your IT environment.



Elite Red Hat Partner with 16+ years of industry experience



Successful Deployment and Adoption through Expert-led Workshops and Consulting Offerings



Contract vehicle access is Impressive

**Learn more today!**

[emergent360.com/red-hat](http://emergent360.com/red-hat)



See all of our  
upcoming events



**Red Hat**

**Connect With Us Today**

[sales@emergent360.com](mailto:sales@emergent360.com) | (800) 292-1000

[emergent360.com](http://emergent360.com)



# How automation can help defend against mounting cyberthreats

BY TOM TEMIN

As agencies add new applications or modernize existing ones, they often target increased automation of software development and IT processes as a goal. But what about automating cybersecurity?

It's a question that resonates with federal cybersecurity leaders given the increasing complexity of agency infrastructures, particularly with the expanded use of commercial cloud services and edge computing.

Plus, there's the advent of zero trust. Zero trust has supplanted the perimeter-and-moat approach to cybersecurity by requiring every device — including those that exist only as software, such as bots — undergo continual authentication.

A Federal News Network panel of government and industry cybersecurity practitioners discussed a range of practical approaches to cybersecurity automation. The panelists identified the types of tasks that agencies want to consider automating: reviewing logs; tracking, compiling and loading software; failing over or restarting when applications hang up; and maintaining access controls and other system administration functions.

## PANEL OF EXPERTS



**Paul Blahusch**  
Chief Information Security  
Officer, Labor Department



**Gary Buchanan**  
Chief Information  
Security Officer, National  
Geospatial-Intelligence Agency



**Jerry Cochran**  
Chief Information Security  
Officer, Pacific Northwest  
National Laboratory



**Rob Thorne**  
Chief Information Security  
Officer, U.S. Immigration and  
Customs Enforcement



**Jason McDonald**  
Technical Team  
Manager, Emergent



**Russ Pavlicek**  
Senior Solutions  
Architect, Red Hat Software

## Common cyber needs, varied missions


The panel discussion revealed that while agencies share a high degree of cloud adoption, the similarities end there. Agencies operate in a wide range of situations, none of them simple.

For instance, take the Labor Department. Chief Information Security Officer Paul Blahusch described an infrastructure at Labor that comprises 18,000 users, 30,000 endpoints and 400 applications under 75 systems with authority to operate. Meanwhile, behind the scenes, Labor is at work on a 10-year modernization effort largely dependent on moving updated applications to the cloud. And on the security front, Labor wants to simplify sign-on using a database of users not tied to any single application, he said.

Over at the National Geospatial-Intelligence Agency, the IT team supports users throughout the world with systems at multiple levels of classification, CISO Gary Buchanan said.

“We have what I would say is a healthy mix of cloud and on-premise infrastructure,” he said.

Since the 9/11 terrorist attacks, NGA has revised its infrastructure to support more information sharing across the Intelligence Community. NGA uses a zero trust approach to cybersecurity because of how IC networks have become interconnected.



Our zero trust efforts are focused on making our applications more in line with zero trust principles to support things like conditional access or modern authentication.

— Jerry Cochran, CISO, Pacific Northwest National Laboratory

“Zero trust really brings us back to that pre-9/11 of locking it back down, after we’ve already opened the floodgates,” Buchanan said.

To supplement its zero trust architecture, NGA uses a robust identity and credential access management (ICAM) solution to maintain data sharing consistent with meeting the cybersecurity mandate of [National Security Memorandum 8](#), he said.

At U.S. Immigration and Customs Enforcement, 30,000 users use up to 60,000 devices, each of which can gather, store and process data, CISO Rob Thorne said.

“What we want is security to be an easy choice for users” at ICE, he said. The agency’s goal is to have cybersecurity policy, enforcement points and access decisions embedded into the architecture.





“I believe zero trust will enable that and have that positive experience for employees,” Thorne said. “Of course, automation is key.”

Jerry Cochran, CISO at the Pacific Northwest National Laboratory, described a government-owned, contractor-operated IT infrastructure that includes thousands of laboratory measurement and process control devices. The lab hosts its enterprise services entirely with one of the major commercial cloud providers, and “in the past year, we completed movement of our 300-plus internal lines of business applications to the cloud,” Cochran said.

As it modernizes applications to a cloud-native state, as opposed to simply moving virtual machines from a data center to the cloud, zero trust sits high on the priority list, he added.

“In the device and identity space, where we have the most work to do is in the application networks and data pillar space,” Cochran said. “Our zero

trust efforts are focused on making our applications more in line with zero trust principles to support things like conditional access or modern authentication.”

On the network side, the lab is moving to network as code, “where you can support technologies and approaches like microsegmentation or software-defined networking,” he said.

## **More complex infrastructures, more cyber demands**

Cloud-hosted applications, data and networks — it all adds up to thousands of elements requiring tracking and security, more than human operators can hope to keep up with, said Russell Pavlicek, senior solutions architect at [Red Hat Software](#). He said Red Hat uses a playbook approach to infrastructure as code, in which IT architects describe the required network behavior at a high level and then the coding occurs automatically.

“You have to end up with automation that can check, maneuver, flag and restart — basically do whatever is needed,” Pavlicek said. “It doesn’t matter how many physical operators you put in the room. You can’t stay ahead of that stack. It’s too big.”

Within Red Hat’s OpenShift product group, Pavlicek pointed to development of automated operators. With an operator running, network and security operation center staffs receive notices of what requires attention, he explained.

“You have all these health checks and other checks that are automatically being handled, so that your people can focus on the real job, the job that you hired them for: to do intelligent things with data,” he said.

Asked what specific functions federal IT shops want to automate, Labor’s Blahusch pointed to “those activities that are tedious for that human to do or that they can’t keep up with.”

I want to automate those activities that are tedious for that human to do or that they can’t keep up with.

— Paul Blahusch, CISO,  
Labor Department

He added that the things he worries about as a federal CISO drive his automation goals, particularly the increasing sophistication and automation of adversaries.

“I need to automate to make sure everything’s secure and right because the adversary could find the one thing that I missed,” Blahusch said.

“The other thing I worry about as a federal IT executive is recruiting and retention,” he said. “Those people I hire don’t want to be checking those 1,000 things. They want to be doing something that’s engaging for them.”

## A place for AI/ML in cyber automation?

The panelists agreed that artificial intelligence and machine learning will play a role in cybersecurity and infrastructure automation.

“If the AI can learn about rote or repeatable tasks or validated options, if something happens — whether it’s a security alert or whether it’s an infrastructure kind of alert — there can be certain levels of intelligence that you put into responding to those alerts,” Cochran said. “Maybe there’s auto remediation that needs to happen.”

Added Blahusch, alerts mostly happen automatically now. “Is the action taken on that alert? That’s what we might have matured to now.”

Going forward, said Jason McDonald, technical team manager for [Emergent](#), “we have to find ways to scan code faster. We have to automate that. We have to use ML to determine whether something is a normal kind of thing or not and then use AI for some of the decision-making.”

## Pushing cybersecurity to the left

ICE’s Thorne also sees a need for security to move left in the development, security and operations (DevSecOps) cycle.

“I want to automate the security in that software development lifecycle,” Thorne said. “If I get greater visibility within that lifecycle, then I can keep up with the increased speed to production of these new applications, which seem to be spinning up and pushed out to production much quicker.”

Red Hat’s Pavlicek described a scenario in which development pipelines automatically call on cloud-hosted tools for vulnerability and error checks. This frees coders from

You have to end up with automation that can check, maneuver, flag and restart — basically do whatever is needed.

— Russ Pavlicek, Senior Solutions Architect, Red Hat Software

routine tasks, letting them focus on coding and on collaboration within the organization.

When automating the transfer of security measures to updated versions of an application, an IT shop can speed up obtaining that critical authority to operate, said NGA’s Buchanan.

“Otherwise, an ATO becomes shelfware as soon as you deliver it because we know things change immediately after any application is delivered,” he said. “Automation is key here.”




Plus, advised PNNL's Cochran, automation needs to go a step further than sorting out alerts. He envisions the orchestration of security investigations and analysis when a system detects a security breach.

"Wouldn't it be better, when the alert fires, for that analysis and those queries already to have been performed," Cochran said, "so that they are presented to the analysts rather than the analysts doing them after the alert fires?"

For the same reason, automation should integrate the numerous activity updates and alerts coming in from an agency's multiple cloud sources, he said.

Cochran suggested that the automation that currently applies to code development and checking for flaws be applied to operation of the network infrastructure. That way, as in app development, automation could reduce errors, he said.

"How do you automate the telemetry and alerts and intelligence that all those panes of glass provide into a single source of truth?" 

We have to find ways to scan code faster. We have to automate that. We have to use ML to determine whether something is a normal kind of thing or not and then use AI for some of the decision-making.

— Jason McDonald, Technical Team Manager, Emergent