FEDERAL NEWS NETWORK

EXPERT EDITION

How to derive offensive benefits from AI-cyber convergence

Insights from

- Army
- GSA
- IARPA
- IRS
- Naval Postgraduate School

Brought to you by carahsoft.

carahsoft. The Trusted Government IT Solutions Provider®

Securing Government Systems with Trusted Cybersecurity Solutions

Explore Carahsoft's extensive portfolio of cybersecurity products and services designed to protect government infrastructures, networks, and assets. Our solutions empower agencies to mitigate risks and ensure compliance with proven technologies from leading vendors.

Discover which cybersecurity vendors align best with your organization's goals, offering solutions in Cloud Security, Supply Chain Risk Management, Identity & Access Management, and more.

Scan below to access case studies, contract vehicles, upcoming cybersecurity events, helpful resources, and more.

TABLE OF CONTENTS

Dynamic cyber

As agencies embrace the latest artificial intelligence tools and capabilities, cybersecurity initiatives — defensive but particularly offensive — are among the vanguard.

It makes sense for a few reasons. Chief among them though: U.S. peer competitors as well as cybercrime syndicates are all in on AI to fuel and sustain their attacks on federal agencies and targets.

"If you can simulate the threats faster than your opponents, this could give you a strategic edge over them that may potentially erode the adversary's first-mover advantage," points out Jason Rivera, field chief information security officer of SimSpace (*Read the full article on Page 13.*)

In the pages ahead, you'll hear from federal and industry cyber experts about tactics and technologies designed to gain an offensive upper hand in cyber through prescriptive AI use.

From an agency perspective, applying large language models to vast data stores suggests another possible plus-up from AI.

"AI has certainly made us much more effective and efficient in sifting through [IRS datasets] to find patterns, to identify fraud methodologies or typologies, to identify current threats or vectors that might be red flags of issues that we were not aware of prior," offers Jarod Koopman, executive director of cyber and forensics for IRS Criminal Investigations (*Read the full article on Page 16.*)

We hope that your organization finds the takeaways, advice and technology details shared in this e-book valuable. Finally, I want to personally invite you to reach out and share your own lessons learned and successes too. Send me an email at vroberts@federalnewsnetwork.com.

Federal News Network welcomes the opportunity to serve as a forum where leaders can build on the work that's come before.

Vanessa Roberts
Editor, Custom Content
Federal News Network

Commercial innovations drive FedRAMP’s new approach

BY JASON MILLER

Now more than ever, the cloud security program known as FedRAMP needs industry’s help.

That was the message from Pete Waterman, director of the Federal Risk Authorization Management Program at the General Services Administration.

“We’re going to transform FedRAMP. Instead of the government deciding what is best, we’ll collaborate with industry to drive the solution. We’ll start now and update our approach continuously. We’ve all been talking about automating the status quo for way too long. Everyone in this room knows that if it was that easy, we would have done it by now,” Waterman said at an event sponsored by the Alliance for Digital Innovation. “We need to drive this type of change together as a community. You bring the solutions; we’ll vet them with agencies and set standards to match.”

Waterman said infrastructure as a service and platform as a service vendors can make their systems secure by design — or at least provide some capability so customers using the services can validate their own security.

Array of possible third-party compliance tools

He said there are endless possibilities for third-party compliance tool vendors.

“Find your niche, and build something cool. If you build validation software, you won’t be excluded anymore. We’ll all work with you to figure out multiparty validation in a way that include you in the FedRAMP ecosystem without requiring a federal agency sponsor for everyone else,” Waterman said.

“All the other cloud service providers of varying scale and complexity, you can adopt these capabilities where, when and how. You can update your architecture to take advantage of them as they become available. Start small, go big, and get secure. For everyone else, figure out where you can add value and plug in. There’s plenty of room inside this for new ideas.”

This new vision, called FedRAMP 2025 and which looks to industry for innovations and to help lead the effort, is a drastic change from how GSA has managed the program over the last 12 years.

> We're going to transform FedRAMP. Instead of the government deciding what is best, we'll collaborate with industry to drive the solution. We'll start now and update our approach continuously.

Pete Waterman,
FedRAMP Director, GSA

Part of the reason for the new approach is the program management office is leaner with fewer contractor resources and a smaller budget. It also is getting out of being the centralized authority and provider of services and will instead focus on setting policies and standards.

GSA and the Office of Management and Budget have tried repeatedly over the last decade to fix long-standing complaints and concerns about the program. The program management office and the Joint Authorization Board created alternative approaches like FedRAMP Ready and FedRAMP Tailored, but the cost and burden of the authorization process still weighed heavily on agencies and vendors alike.

Waterman said the program has outpaced how GSA and OMB initially created the FedRAMP process and also the original Federal Information Processing Standard cyber guidance.

"FedRAMP is rooted in the past. FIPS 200, the government standard for the development, implementation and operation of secure information systems, was published way back in 2006. The approach outlined back then was based on the idea that systems were developed only until they were ready to be put into operation, like a building or a ship. You can use a paperwork-based process to evaluate the security of something that you won't change once it enters operation," he said. "That hasn't been how most of us built tech for a long time though. Modern services are continuously and simultaneously developed and implemented while being operated without downtime and without stopping."

Continuous validation is the goal

A common complaint about the current process is it's too burdensome and costly, and it's more of a checklist than a true security audit.

Instead, the retooled FedRAMP will work with industry to create continuous validation and verification processes as well as apply automation to those security controls.

"FedRAMP will set the standards that enable private innovation to create the solution. That's how we'll develop and continuously improve a standardized, reusable, cloud-native approach to security assessment and authorization for cloud services," Waterman said.

"We're going to build a different approach, starting with understanding the underlying security principles that will ensure government information is safe in a continuously evolving commercial environment with key security indicators. Then together, we'll build an assessment process to validate your choices about those key security indicators."

While Waterman didn't promise to have every answer to every question about how this approach would work, there are some initial ideas that seem to make sense.

For example, the key security indicators would shift the requirements from extensive descriptions about each individual control on a spreadsheet to continuous validation that the intent behind those controls has been addressed and there would be no need for extensive human reviews.

"We know the capability to rely on automated validation for many security controls already exists and that host providers often offer secure by design options to make this easier for their customers," Waterman said. "The vast majority of underlying security requirements for NIST SP 800-53 can be validated in the same automated way if we approach them in the abstract. No one should ever be manually reviewing an old spreadsheet that has some screenshots next to it and pretend that that's a security assessment."

> We know the capability to rely on automated validation for many security controls already exists and that host providers often offer secure by design options to make this easier for their customers.
>
> ***— GSA's Pete Waterman***

Simplifying a complex process by automating

Waterman added he believes the goal of automating everything is effectively a Boolean decision:

- Can I trust this company? True or false
- Is this cloud service secure enough for my specific needs? True or false
- Will I authorize its use? True or false

"It's that simple and that complex, but this should be our goal. My team has already done a lot of work … to get started. You all tell me how you can help such offerings to validate their configuration. You don't all have to agree on the approach or do it the same way. It's the outcome that matters," he said.

"If the approach is reasonable and the outcome is legit, we'll validate the approach, any approach. From there, we just keep going, continually adding key security indicators and pulling in various existing frameworks as we simplify more and more controls and solve more complex use cases."

Waterman acknowledged that the change won't be simple for the big IaaS and PaaS providers. "But we'll see it through, if you will. You can't keep pushing paper forever. I don't have all the answers to how to do this, but I'll bring the coffee and donuts."

But GSA has pressed forward, hosting meetings with new community working groups to bring everyone together. Some of the topics covered so far include:

- NIST SP-800-53, Rev 5
- Automating assessments
- Applying existing frameworks
- Continuous reporting

"Those groups are an attempt to create and establish a community where we work together and talk about things in public with each other, so there's no more ghost rules and regulations. There's just everybody having equal and fair access to all the same information, including me and my team, because my team wants to know what you all are doing," he said.

"Then, as we monitor that, as we see things that work, and as we see some generally good ideas. As we see standards that folks align toward, we will develop that standard that supports that, and then we'll send that through our formal request for comment process that is required by law to make sure that we standardize that."

Waterman said the FedRAMP PMO will use a GitHub discussion forum to post meeting notes and summarize the discussions and the progress of industry in addressing these challenges.

The growing role of AI in federal cybersecurity

As federal agencies create and collect more data, their cybersecurity needs are evolving rapidly. With attack surfaces expanding to include multiple cloud platforms, distributed endpoint devices and Internet of Things sensors, the priority of cybersecurity continues to increase.

Simultaneously, cyber adversaries are leveraging artificial intelligence to develop more sophisticated attack methods. These factors combine to make AI-driven cyber defenses crucial, as the sheer volume of data to monitor exceeds human capacity.

The data challenge and AI solution

VAST Data Federal, a company specializing in data storage and analysis solutions, is at the forefront of addressing these challenges. said Carmelo McCutcheon, the company's public sector chief technology officer. The approach involves processing data at the point of creation and using AI to manage and analyze vast amounts of information. This allows for near real-time event monitoring and response, crucial in an environment where cyberattacks occur frequently VAST's ransomware detection and prevention tool exemplifies this AI-driven approach, McCutcheon said. It examines previous behavior patterns to identify potentially malicious anomalies. Upon detection, it not only alerts but also proactively can revert to the last known-good system snapshot, created every 15 seconds. This rapid response is crucial as the time to breakout for cyber intrusions continues to decrease.

> The sheer volume of data our customers handle necessitates AI-driven analysis. We're integrating these AI tools and datasets directly into our platform because the amount of data being generated is staggering.

Carmelo McCutcheon
Public Sector Chief Technology Officer, VAST Data Federal

VAST FEDERAL

The VAST Data Platform

Data Infrastructure Engineered for the Federal Government

The VAST Data Platform unifies storage, database, and containerized compute into a single, scalable software platform to power AI & deep learning in modern data centers and clouds.

Visit us at:
vastfederal.com

SCAN ME

ZTA compliance

VAST's tools are designed to meet many controls under the data pillar of zero trust architecture (ZTA). The platform automatically labels incoming data and controls access through attribute-based authentication.

The VAST Data Platform's implementation of the data pillar within the ZTA framework exemplifies how advanced security features and compliance with regulatory standards can create a secure, compliant environment. By embracing the principles of zero trust and implementing the data pillar with precision and foresight, VAST ensures that sensitive data remains protected against the evolving threats of the digital age.

VAST's multitenancy abilities allow organizations to create and maintain multiple secure enclaves on a scalable data fabric. This helps federal agencies access and manage data using shared AI infrastructure resources without impacting performance or security, McCutcheon said. VAST's attribute-based and roles-based access control capabilities provide another layer of data security.

This integration eliminates the need for additional tools to gain insights, as everything is stored and accessible within the platform. VAST can track a data flow back to a specific user in real time, including the endpoint they're using.

Kafka Broker: Accelerating data analysis

VAST developed Kafka Broker, written in C++, which enables high-throughput ingest at 10 times the performance of a traditional Kafka cluster, McCutcheon explained. This innovation makes ingesting high volumes of event data 10 times faster. The broker

> We capture all the data, metadata and protocol information as it changes, and store it in queryable database tables. This allows for real-time access and analysis.
>
> ***— VAST Data Federal's Carmelo McCutcheon***

structures the data in a query-able table in the VastDB and uses a large language model AI to identify trends over time. What used to take multiple analysts weeks or months can now be accomplished in minutes, he said.

A component of the Energy Department has been using this functionality in beta. It faced challenges in storing NetFlow data for extended periods to meet zero trust architecture requirements, such as those outlined in Office of Management and Budget Memorandum M-21-31. VAST's solution allowed the DOE organization to collect and process both packet capture data and NetFlow data, which was previously unfeasible due to volume constraints.

"Our solution enables real-time and historical correlation across all data sets simultaneously, a capability that was previously out of reach," McCutcheon said. "Before, if an agency suspected a hack from two years ago, they lacked both the tools to investigate and the historical data to analyze — storage costs made long-term data retention prohibitive. With VAST, we've made it possible to store 18 months of data cost-effectively, all while preserving the familiar analyst workflow. This means agencies can now conduct thorough investigations into past events without disrupting their current operations."

As cyberthreats continue to evolve, AI-driven solutions are becoming indispensable for federal agencies. Recent developments highlight the growing importance of these technologies:

- Darktrace Federal achieved FedRAMP High authority to operate for its AI-powered cybersecurity platform in March 2025, enabling federal government access to advanced IT, operational technology and email security solutions.
- The MITRE Federal AI Sandbox, powered by the VAST Data Platform, now provides federal agencies with highly performant, AI-ready data infrastructure for cybersecurity and critical infrastructure protection.
- VAST Data and Superna have partnered to enhance cyber resilience with intelligent threat protection and instant recovery capabilities, addressing the increasing ransomware threats in the AI era.

These advancements demonstrate that AI-driven solutions not only manage vast amounts of data but also provide real-time analysis, threat detection and response capabilities, McCutcheon said. "They are crucial for maintaining robust cybersecurity in an increasingly complex digital landscape, where traditional methods are no longer sufficient to combat sophisticated cyberthreats."

IARPA looks to next round of AI cybersecurity research

BY JUSTIN DOUBLEDAY

The intelligence community already has plenty of challenges with unauthorized disclosures, and its lead research arm wants to make sure ChatGPT isn't the next leaker to make news headlines.

That's one of the challenges the Intelligence Advanced Research Projects Activity is considering under its next round of artificial intelligence research. IARPA's current program for AI cybersecurity, called TrojAI, is wrapping up this year. The effort was launched in 2019 to develop means of detecting adversarial attacks on AI systems. It was established prior to the widespread advances in large language models that power generative artificial intelligence.

Putting the focus on large language models

IARPA Director Rick Muller said LLMs will be a major focus area for the next program. "What we want to be able to do is understand in the next round, what kind of training skews are brought into a large language model that might give unintended consequences? What type of hallucinations are going on?" Muller said during an event hosted by the Intelligence and National Security Alliance. "And then how can we make sure that those models can be trained on classified data and not spew out that data if you ask them nicely?" Muller continued. "If you read the literature in jailbreaking large language models, sometimes it really just takes asking them in the right way."

In the world of LLMs, jailbreaking refers to convincing a system to ignore its built-in safeguards. A related concern are prompt injections that disguise malicious instructions as benign inputs, in order to manipulate a generative AI system into leaking sensitive data or taking other nefarious actions.

> If you read the literature in jailbreaking large language models, sometimes it really just takes asking them in the right way.

Rick Muller
Director, Intelligence Advanced Research Projects Activity (IARPA)

Adopting AI as an investigatory aid

Meanwhile, intelligence officials believe AI can be used to speed up intelligence gathering and analysis. An IT roadmap released by the Office of the Director of National Intelligence in 2024 called for adopting "AI at scale" across the intelligence community.

Defense and intelligence agencies have been exploring the use of generative AI to analyze open source information. And vendors like Microsoft and Palantir have said they are working to bring large language models to classified networks as well.

> If we're going to train it on classified data, how do we make sure that that data isn't compromised down the road in a way that that threatens our resources?
>
> ***— IARPA's Rick Muller***

IARPA's TrojAI program has focused on building defenses against Trojan horse-style attacks on AI systems. The program has worked on detecting attacks across a range of vectors, from training data to the AI model itself.

The research has focused on a range of AI domains, including image recognition, natural language processing, and reinforcement learning. IARPA has published much of the research in conjunction with the National Institute of Standards and Technology.

Building an AI cyber tool kit

Muller said the goal is to fill gaps in the market for AI safety.

"IARPA doesn't have the billions of dollars that are required to train a foundation model," he said. "What we want to be able to do is give the intelligence community tools to help them understand when these models are safe, when they've been compromised and so on."

While the TrojAI program is wrapping up, Muller said the last competition under the program focused on large language models. "The IC wants to be able to use these tools when people's lives are on the line. And so if we're going to train it on classified data, how do we make sure that that data isn't compromised down the road in a way that that threatens our resources?"

The AI arms race has begun — cyber ranges are the next step in deterrence

A cyberattack can be quantified across three variables: speed, volume and sophistication. How fast are attacks occurring, how many of them are there, and how sophisticated are they?

The biggest cybersecurity challenge that federal agencies will likely face in the future is that artificial intelligence will serve as an accelerant to all these variables.

Speed of a cyberattack can be measured via the term breakout time, a term coined by CrowdStrike. It refers to how long it takes an adversary, after breaching a system, to move laterally.

In 2018, the fastest average breakout time was 18 minutes and 49 seconds, achieved by Russian nation state hackers. In 2023, a breakout time of 2 minutes and 7 seconds was observed. Jason Rivera, field chief information security officer of SimSpace, said AI is pushing breakout time speeds closer and closer to zero.

> As a human, I have a limitation on what I can conceive of. Artificial intelligence? No. The only limitation is computing. AI is a force-multiplying accelerator. It will take everything that we are doing, and it will accelerate it faster than anything that we can comprehend or have experienced in the past.

Jason Rivera,
Field CISO, SimSpace

Similarly, he said, the number of phishing attacks is increasing, as AI writes and sends malicious messages faster than humans can. It also improves faster than any human could, essentially by applying the scientific method: Try something, see if it works, learn from it and apply what it learned to the next iteration. That's improving the quality of not only phishing attacks but all initial access tactics, as well as lateral movement and privilege escalation attacks too.
"As a human, I have a limitation on what I can conceive of. Artificial intelligence? No. The

only limitations are algorithmic capability and computing power," Rivera said. "AI is a force-multiplying accelerator. It will take everything that we are doing, and it will accelerate it faster than anything that we can comprehend or have experienced in the past."

An AI arms race

Because adversaries are using AI to improve their attacks, cyber defenders need to use it to improve their defenses as well. Rivera said the future state of cybersecurity is one where all security functions and all IT functions are joint hybrid human-AI. Because how do you defend against a breakout time near zero? You must predict it before it happens. Deterrence tends to become the answer during an arms race.

That's where cyber ranges come in. With a powerful enough capability, you can simulate faster than the adversary can attack. Cyber ranges simulate the three layers of a system — the operating systems and network; the data, applications and security logging tools inside the operating systems; and the users — to create what Rivera called a what-if machine.

"What is the future? You could argue that the future is a predictable series of quantized outcomes," he said. "What did Google just do with weather prediction? They made the most accurate 10-day weather forecast in human history. And they did it with artificial intelligence. Why were they able to do that, whereas all other human methods in the past were not able to do that? I would argue that the reason for that is they could quantize lots of different outcomes, test the outcomes, figure out which one is the most likely, apply statistical significance to certain ones, and then they get better and better."

Don’t be reactive, be predictive

It’s not enough to just simulate an environment. That simulation must assess potential future scenarios. Just like a soldier wants to know how many bad guys are in a room and how they are armed before entering it, a chief information security officer wants to know what tomorrow’s malware and hands on keyboard capabilities will look like. Just like a soldier wants to know how weapon systems will perform in every environment, a CISO wants to know how cyber tools will perform against attacks. That’s why testing on a cyber range is important.

Most large enterprises are investing in serious cybersecurity tools and disciplines, like anti-virus and endpoint detection and response (AV/EDR), cloud security, zero trust, disaster recovery preparedness and the like. How effective is their AV/EDR system at detecting and responding to threats? Will the company’s cloud security posture standup to modern day criminal and nation-state threats? Does their organization’s zero trust strategy work? What happens if the primary data center fails? What’s the failover solution?

When they invest in cybersecurity tools like that, they need to know how they will function, Rivera said. Testing in the production environment is a no-go; there’s too much risk of breaking something important. Cyber ranges empowered by AI will enable enterprises to see how their tools work before real-world events. And they’ll enable them to do so faster, with more volume and sophistication than their adversaries, he said, which will lead the United States to a place where more powerful AI algorithms and faster computational power are what will provide the deterrence in an AI arms race.

> We’re headed to this arms race where you want the most powerful computational capability that can simulate in advance what is likely to happen. And if you have a powerful enough computational capability, and if you can simulate the threats faster than your opponents, this could give you a strategic edge over them that may potentially erode the adversary’s first-mover advantage.
>
> ***— SimSpace’s Jason Rivera***

“China just came out with DeepSeek, a model that allegedly is of the same performance capability of even the U.S. leading models like OpenAI. Some call it AI’s Sputnik moment. It came very unexpected,” Rivera said. “We’re headed to this arms race where you want the most powerful computational capability that can simulate in advance what is likely to happen. And if you have a powerful enough computational capability, and if you can simulate the threats faster than your opponents, this could give you a strategic edge over them that may potentially erode the adversary’s first-mover advantage.”

IRS deploys AI tools to combat emerging tech’s role in fraud schemes

BY JORY HECKMAN

The IRS is staffing up with investigators to go after all sorts of criminal activity, but criminals are using artificial intelligence tools to launch more sophisticated fraud schemes — and in greater volumes.

The agency’s criminal investigation branch, however, is also relying on AI tools to stay one step ahead of fraudsters.

Jarod Koopman, IRS Criminal Investigations’ executive director of cyber and forensics, said in an interview that online payment fraud now exceeds $360 billion annually, and that check fraud is “skyrocketing.”

Evaluating AI potential applications

“What used to take a significant amount of effort, going into some type of a social media-type exploit or a hack, they can now do this with AI that’s much more efficient, much more effective and certainly much more volume at high speed,” Koopman said. The IRS, under the Inflation Reduction Act, recovered more than $1.3 billion from about 1,600 millionaires who had not paid overdue tax debts or filed tax returns in recent years. Koopman said the agency isn’t currently using AI in these tax recovery cases, but IRS-CI is reviewing AI as a use case for “that exact scenario.”

“They want to make sure what they’re doing is implementing in a way that is very unbiased and done in a way that’s governed and utilized to ensure both the privacy but also the integrity of the application of the tax law,” Koopman said.

IRS enforcement operations, more broadly, are trying to keep up with emerging technology’s impact on criminal financial activity. AI tools are accelerating the development of deepfake schemes, as well as misinformation and disinformation campaigns that led to fraud.

Staying a step ahead of tax fraudsters

Meanwhile, a trillion-dollar global cryptocurrency market gives fraudsters more opportunities to hide criminal sources of revenue from federal law enforcement agencies.

“From a general standpoint, we’ve seen not only fraud continue on the rise but more sophisticated frauds in the way of AI cyber components, in addition to traditional financial fraud," Koopman said.

He estimates that about 50% to 60% of IRS-CI's casework relates to taxes. IRS-CI also investigates a wide scope of criminal activity with a financial component — including public corruption, terrorism funding, organized crime, drug trafficking and money laundering.

A recent [IRS-CI investigation of child exploitation material,] paid for through cryptocurrency transactions, led to 300 arrests worldwide.

IRS-CI is the sixth-largest law enforcement agency in the federal government but lacks the robust staffing of larger entities such as the FBI and Immigration and Customs Enforcement's Homeland Security Investigations (HSI).

"Some of these agencies have 30,000 to 40,000 employees, versus us coming in at 3,500. We're also a very small portion of the IRS as a whole," Koopman said. "We tend to be an agency that's very flexible and nimble. We're small enough that we can drive innovation. And that's really helped us, I think, in the long term."

IRS-CI is hiring law enforcement personnel with expertise in international banking, anti-money laundering, cybercrime and cryptocurrency. Nearly all its hires, however, are required to have a background in accounting.

Koopman said IRS-CI in recent years had the resources to bring its staffing up to levels not seen for more than a decade. In recent years, it's grown from about 2,700 employees to about 3,500. About 2,500 of them are frontline special agents, and the rest are professional staff.

> From a general standpoint, we've seen not only fraud continue on the rise but more sophisticated frauds in the way of AI cyber components, in addition to traditional financial fraud.

Jarod Koopman
Executive Director of Cyber and Forensics, Criminal Investigations, IRS

"Over the last couple of years, we've actually been able to increase our employees on roles a bit to help continue to meet the demands," he said. "This is just basically getting us back to staffing levels that we were back in the '90s and the early 2000s — so nothing of significant growth, but definitely something that's been helping."

Tapping AI to analyze current datasets

The IRS generally uses AI to make more effective use of the data already available to its workforce. This includes operational data from previous and ongoing casework, as well as third-party data from other financial institutions and open source intelligence.

"All of that data is pretty vast, and it's large volumes of data. AI has certainly made us much more effective and efficient in sifting through that to find patterns, to identify fraud methodologies or typologies, to identify current threats or vectors that might be red flags of issues that we were not aware of prior," Koopman said.

He added that AI, above all, is helping the agency flag and detect patterns in the data it has, then have employees investigate further. "It's like having AI and large language models be able to match up against our data internally to be able to give us the results and the outputs that we're looking for to make decisions, not for the AI to use the data to make decisions directly," he said.

Creating opportunities to share data

Koopman said the IRS is also relying on new privacy-enhancing technologies that allow the agency to share sensitive information with law enforcement partners and third-party financial institutions through encrypted channels and allow those organizations to run analytics or other models against those datasets without ever having access to the source data.

"If we want to correspond with a third party, we have to provide them with some type of a name or a Social Security number or something or handle to be able to get information back. There's a trust factor there, and there's also a risk tolerance that we have to provide something in order to get the information that we wouldn't readily have available otherwise," Koopman said.

"That's really a game changer when you start talking about some of these capabilities that we're looking to do internally because it just further enhances the security of the data that the government has — and that all of these other partners have — and not constantly shifting around information that's pretty valuable to criminals and others."

> AI has certainly made us much more effective and efficient in sifting through [our datasets] to find patterns, to identify fraud methodologies or typologies, to identify current threats or vectors that might be red flags of issues that we were not aware of prior.
>
> *— IRS' Jarod Koopman*

So you've automated application security testing — here's the next step

The development lifecycle has changed a great deal over the years, particularly with respect to application security, and it doesn't show signs of stopping any time soon.

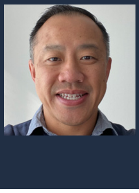
Artificial intelligence is automating many of the more difficult, time-consuming tasks in the process, vastly improving security and time to delivery.

As each new application of AI proves itself and becomes standard practice, it leads directly into additional new ways to use this tool to become more efficient and secure. That dynamic is playing out once again in application security testing.

In the early days of application development, developers primarily focused on getting the app functional. Then the security team would scan the app for vulnerabilities and send them back to the developers to be patched. This was a time-consuming, painstaking manual process that unnecessarily extended the development lifecycle. Then came DevSecOps, integrating the security testing process with the development process and baking security in rather than bolting on as an afterthought.

"So now we start to integrate that scanning, get that automated and integrated with the development lifecycle," said Victor Tham, cybersecurity chief technologist at OpenText. "But while that starts to become automated for a lot of different organizations, what still is a challenge is really what happens after you scan. You get a bunch of results, and you have to go in and audit those results. Then, you have to think about how you're going to fix those issues. That's still a really manual process for a lot of organizations."

> We're not removing the human from the loop. What we're doing is helping speed up the process of the auditing. You still want to have a human review the auditing results, as well as review the remediation recommendations.



Victor Tham
Cybersecurity Chief Technologist, OpenText

The challenges of automating the auditing and remediation processes

That's the next target use case for AI in the development lifecycle: automating the auditing and remediation processes. Tham said generative AI can help in terms of finding and understanding existing issues during security audits and determining their relevance. It can help determine whether an issue is a true or false positive, saving developers from chasing down nonissues and allowing them to focus on the real vulnerabilities. It can also recommend fixes and how to implement them.

This can help address several challenges currently faced by organizations involved in application development, Tham said. First, many development teams have large backlogs of security issues to both audit and remediate. Those are painstaking manual processes that push back application delivery. GenAI can speed up these processes, allowing developers to work smarter and faster, making more progress in reducing backlogs, Tham said.

"What we're really doing is taking the scan results that we're finding, using prompt engineering against some publicly available large language models and being able to recommend auditing as well as remediation based off of the engineering that we're putting into the prompts and reviews," he said.

"We're not removing the human from the loop. What we're doing is helping speed up the process of the auditing. You still want to have a human review the auditing results, as well as review the remediation recommendations."

> Agencies can take a look in terms of the number of issues that they're finding in their security scans, in terms of all the auditing and based off their human reviews. From those results, then they can figure out if it's something that is really helping them save time and improving accuracy, as well as the results in terms of recommendations for fixes.
>
> ***— OpenText's Victor Tham***

This can also help assist developers who might not have as much training in security and vulnerability remediation. Developers are often taught to write code in terms of functionality, rather than secure coding practices. They may not necessarily know how to securely patch a vulnerability even if it's flagged and sent back to them.

Having genAI recommend fixes saves developers time in having to find and learn the right fix on their own, Tham said. They can instead concentrate their time on evaluating the fixes recommended by the AI.

How to start implementing genAI for cyber

Agencies that want to apply this new use case for genAI may need to think through a few things before getting started. Tham said many government agencies have policies, procedures and guidelines that determine their interactions with AI and large language models. Because these tools are usually in the cloud, policies and restrictions surrounding that may apply as well.

Agencies should also evaluate the tools that they're using to see how much time and effort they're saving in their development lifecycle, specifically their application security audits and remediation processes.

"Agencies can take a look in terms of the number of issues that they're finding in their security scans, in terms of all the auditing and based off of their human reviews," Tham said.

"Off of those results, then they can figure out if it's something that is really helping them save time and improving accuracy, as well as the results in terms of recommendations for fixes. How many issues are they having based off the audit findings, what they're looking at with the fixes, and then what they are finding in terms of accuracy."

Addressing risk while using AI to shrink the visibility gap

Hybrid environments are the norm at most agencies these days, with combinations of public and private clouds, as well as some legacy on-premise systems. While that unlocks a slew of new capabilities for agencies, it also introduces a greater complexity when it comes to operating and managing those systems.

One key challenge they're facing is the data visibility gap: Because the data is isolated in these different environments, gaining full observability is difficult. Different signals are flowing into different monitoring tools that aren't integrated.

IT professionals need all of this to flow into a single pane of glass with unified alerting systems. At that point, the problem becomes one of sheer volume. There's so much noise that it's impossible to sort out the signal. That's where artificial intelligence comes into play, said Krishna Sai, chief technology officer at SolarWinds.

"If you think about where AI tools are getting used, they're essentially getting used to address predictive analytics and issue detection. Both are very important. If you're an IT operator, you want to know when things are going to go wrong before they actually go wrong, which means you need to have good forecasting and prediction models," Sai said.

> If you think about where AI tools are getting used, they're essentially getting used to address predictive analytics and issue detection. Both are very important. If you're an IT operator, you want to know when things are going to go wrong before they actually go wrong.

Krishna Sai
Chief Technology Officer,
SolarWinds

"From an issue detection perspective, it's a classic needle in the haystack problem, where data is flowing into your observability systems from a variety of different places. And when you get paged at 3 a.m. because of an incident, you need to have the right context to be able to pass through the data and quickly identify what went wrong."

Risks of AI adoption

According to a December 2024 survey of 200 IT decision-makers in the federal, state, local and education sectors, one-third currently have AI tools implemented, while another one-third are actively pursuing them. But 38% reported being extremely or very concerned about the risks of adopting AI, while another 44% expressed moderate concern. Of those who were concerned, data privacy and security topped the list of their concerns.

That said, Sai noted one way agencies are addressing those concerns is through the implementation of a zero trust architecture. When the basic principle of “trust nothing, verify everything” is applied to AI tools as well, Sai pointed out that agencies report significant improvements in security posture.

“That mindset is especially critical in government agencies when you begin integrating AI. Every request to access data or AI systems, make sure that they’re authenticated and authorized, often with multifactor authentication and strict access policies — things like least-privilege access. Everyone and everything only gets a minimal level of access to do the job,” he said.

“This is super important for AI workloads that pull data from multiple systems so that you can strictly limit the AI engines — whether that’s for training or inference — to permit access to only the specific area that it needs to have access to. It cannot roam or ingest information from places it shouldn’t. Microsegmentation, breaking down environments into small segments, is also important, especially when AI models live alongside other sensitive systems.”

Sai said the AI by Design framework developed by SolarWinds is intended to address these concerns through four broad principles:

- Privacy and security: Through advanced access control protocols and sophisticated anonymization strategies, SolarWinds maximizes the safety of user data at all stages.
- Accountability and fairness: Keeping a human in the loop helps to ensure AI tools do not reinforce existing biases.
- Trust and transparency: A well-defined machine learning operations pipeline works to illustrate the rationale behind AI actions, helping foster trust by demystifying AI processes.
- Simplicity and accessibility: New tools and processes can be overwhelming. The systems need to be as seamless and intuitive as possible to drive adoption.

The importance of unified visibility

Sai stressed that everything comes back to observability. Operators need to be able to get all their data into a unified tool or platform to leverage AI for things like monitoring and analytics. This is key because not only is the data isolated in different systems but so are the teams. Accomplishing unified visibility also moves all teams across the enterprise into a consistent posture with the same security baseline. This has an additional benefit of increasing collaboration, Sai said.

> Paying proper attention to cybersecurity and AI while building on that foundation of digital transformation is so important. These are the things that keep us up at night, and these are why we pay a lot of attention to how we build our systems.
>
> ***— SolarWinds' Krishna Sai***

"Paying proper attention to cybersecurity and AI while building on that foundation of digital transformation is so important. These are the things that keep us up at night, and these are why we pay a lot of attention to how we build our systems, so that we're able to address these challenges more proactively in our customer environments."

Naval Postgraduate School seeks to balance open, classified research

BY JASON MILLER

Classified research and academic institutions often aren't mentioned in the same breadth. One is secretive, and the other thrives on openness and sharing.

The Naval Postgraduate School is trying to become the conduit that connects these two often divergent efforts.

NPS is planning to address these sometimes opposite goals through its new Naval Innovation Center, which former Navy Secretary Carlos Del Toro announced in December 2022.

"It's not NPS' Innovation Center, and that's very important to understand. The reason why it's going to take place at NPS and be co-located with NPS is because the secretary of the Navy understood the value of having our student population — the experienced officers that have come from the fleet or the Marine force and are going to go back into service — come in with problems, and then they're going to go back and try to address those problems," said Kevin Smith, the former vice provost for research and innovation who recently returned to his role as a physics professor, during an interview at the West 2025 conference sponsored by AFCEA and the U.S. Naval Institute.

"It's a very unique student body we have, in addition to our world class faculty. But they're all driven toward that common mission. It's a very unique institution that can really support the kind of innovation the Navy wants to see accomplished to address the capability gaps that we're currently seeing."

Expansive cyber plans

The Naval Innovation Center will host students and partners from across the Naval R&D ecosystem — from industry, other academic institutions and even allies.

This means the center will have to support multiple levels of access to data and research.

Scott Bischoff, chief information officer at NPS, said the underlying infrastructure will need to be in place to address those needs.

"I'm talking about multiple levels of classification, and we have to make sure that the building's set up for the room we need there. The basics with AV and collaboration are going to be very important. We want to build in adaptability and make sure we don't get stuck two years after we open the doors," Smith said during the interview.

"Not only is the Naval Innovation Center well down the planning stage, but we're also doing a big campus modernization, so we've kind of got it on both sides. But it's the same thought process with the buildings — we have to make sure we don't get stuck with old technology."

> It's a very unique institution that can really support the kind of innovation the Navy wants to see accomplished to address the capability gaps that we're currently seeing.

Kevin Smith, Physics Professor, Naval Postgraduate School

Research demands increasing

Smith said moving into the classified space brings a host of challenges, such as ensuring cloud services are at Impact Level 6 or higher.

"It's also about what resources do we need to keep everything cool that's on premise — there's more of that on the classified side. We're starting to run into heating and cooling issues in some of the older buildings. That is the big one," he said. "Researchers are bringing in hardware now, a lot of GPUs, and we've got a big high-performance computing center. It is very full right now."
Retired Navy Vice Adm. Ann Rondeau, NPS president, said striking the balance of access to information and ensuring classified data stays with the right people is a constant challenge for NPS.

Rondeau said the recent movie "Oppenheimer" is a good example of this challenge.

"There was a lot of discussion that was at high levels of great intellectual work in electrical engineering, physics and all those things. That was the dialog of the classroom and of the open conversations — and actually the arguments. There was lots of sharpening of the edge, and they had to work through the basics of it — the engineering and the concepts in the physics. Then they went over to the classified side as to what they were doing," she said.

"That upfront conversation is unique in the sense of the democratic world — of how you learn and educate. You have to have an exchange of ideas. That is part of the excitement of it — that there's energy behind it ... and that comes way before it is classified. Then, you go into the world that is classified as to how you apply it."

> Applications become a sensitive area, so you need to put that in a classified environment. The basic knowledge you must have. But once you start to practice that and put it into an applied form, that becomes, at times, very sensitive.

Retired Navy Vice Adm. Ann Rondeau, President, NPS

While NPS doesn't have a large student population working in the classified world, Rondeau said as the institution does more with cybersecurity or artificial intelligence, the need for classified capabilities may increase.

"If you're interested in an application, which is what I want to have our students think about all the time, then how are you applying your knowledge with open architecture and access to all kinds of information?

Applications become a sensitive area, so you need to put that in a classified environment. The basic knowledge you must have," she said. "But once you start to practice that and put it into an applied form, that becomes, at times, very sensitive. You need to have a classified environment to talk about the actual solutions and applications many times. That's really important."

A maturing concept for the Navy

This is where the new Naval Innovation Center can play a bigger role. While it remains in the planning stages, Smith said the building designs are mature at this point, and they're looking at budgets and final designs for how everything will fit into the building.

"The Naval Innovation Center itself is still a concept we're developing. The operating model — we're preparing for what that might look like at NPS, and how NPS can support it and leverage it as well for the education of our students," Smith said.

"Now, while that's going on, NPS has been looking for the last few years at: How do we start creating more of that innovation ecosystem within our own efforts? We're doing a lot more interdisciplinary types of work. We'll pull faculty and students from different communities, different departments, together to work on some problems that we've identified internally, that we have the capacity to work on. Now, we have an NPS innovation operating concept that goes from concept development through potential prototyping, some field experimentation, as well as what would the acquisition process look like to put something like that into practice."

Under the current plan, students will apply to the innovation center and, if accepted, be part of a team for six to 12 months that includes NPS faculty and staff and work on specific problems or challenges.

Smith said the innovation center, in many ways, is an entirely new concept.

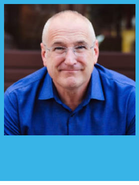
"It's really to take something that's already got a little bit of maturation to it and try to take that further," he said. "At the same time, we're not going to be building large programs or large prototypes in the center. It's really about, how do you take something from an early stage and mature it with the folks that have that understanding of how it's going to be used in actual practice and get it to a point where it is ready to scale? Then, hand it off to another organization, either within a Navy office or an industry partner, to scale it and then be able to provide that to the fleet."

The next great existential digital crisis and how to start preparing for it

The Y2K crisis of the late 1990s was the first existential digital threat the IT industry faced. It threatened every major computerized enterprise, especially global communications, and it required massive, coordinated efforts to overcome successfully. Some experts believe the industry now faces an equivalent challenge, to the point where they've called it — in homage — Y2Q. That challenge is quantum computing, and the implications it has for data security.

Every single communication accomplished by computers, from text messages to emails to data transfers between systems, uses known encryption methods like the RSA-256 algorithm. Some of these have been in use for more than 50 years. And quantum computers can crack those encryptions with ease. As those capabilities become more commonplace and available, all data — from personally identifiable information to corporate secrets and national security files — will be vulnerable.

> The post-quantum computing era is a real threat to classical encryption, and organizations need to start thinking about how that encryption — the same things and standards that they've had and been comfortable with for decades — is no longer viable.



Jim Walker
Product Manager for Quantum Cryptography, Tychon

"The post-quantum computing era is a real threat to classical encryption, and organizations need to start thinking about how that encryption — the same things and standards that they've had and been comfortable with for decades — is no longer viable," said Jim Walker, product manager for quantum cryptography at Tychon. "Because they are vulnerable to the capabilities of quantum computers to cracking classical encryption, and this is something that people need to pivot to planning for and start to move out on today."

Automated cryptographic discovery and inventory

The scale of the challenge isn't the only similarity to Y2K; organizations know the threat is inevitable but have time to prepare for it. That's why Walker said it's imperative to begin now by running an automated cryptographic discovery and inventory (ACDI) lifecycle.

Much like the first step on the path to a zero trust architecture, identifying the endpoints and data that must be secured is step one in becoming quantum cryptography–ready. Organizations must know what encryption is being used across an enterprise and where, he said. That includes the entire network, all endpoints and devices that are connected to it, even Internet of Things sensors and printers.

The ACDI approach must be two-pronged. Organizations need tools on the endpoints that can listen, interrogate and gather the necessary data, and they need the capability to harvest that data and inventory it at the socket layer.

"The reality is that there are very few discovery and inventory tools that cover both surfaces, meaning endpoint and network," Walker said. "It needs to be intelligent, where it will help the customer understand risks. It will prioritize those risks for the customer — think of a stoplight: red, yellow, green. It needs to paint that picture and then provide some decision-making ability for an organization to decide which encryption they're going to improve upon first." He said it should also have third-party integrations with major existing federal environments, ecosystems and tools, such as Elastic and Splunk.

> Industry experts have said they believe nation states are already leveraging quantum computers to crack encryption and get to secrets. I think we'll start seeing more research and things coming out between now and the end of the year, like an academic institution claiming that they've achieved it.
>
> ***— Tychon's Jim Walker***

Prioritizing encryption upgrades

Walker said agencies will need to prioritize quantum-resistant encryption upgrades based on the value of each system. For example, the U.S nuclear stockpile will probably be at or near the top of the Energy Department's list. This prioritization will be important because these upgrades will be a massive, time-consuming and expensive undertaking.

Agencies will have to go system by system, database by database, Walked advised. Some enterprises will have to invest billions of dollars to fully complete this migration.

But the first step, ACDI, doesn't have to be expensive or time consuming, he said. Organizations can accomplish discovery and inventory instantaneously and at low cost. Having that complete picture will let agencies then make better decisions about what order to approach the much bigger and more expensive task of performing the system-by-system migration, Walker said.

The need for urgency

The government has already put out multiple mandates that agencies begin the work toward achieving quantum read- encryption. Unfortunately, many of the deadlines have passed without substantial improvement on the situation. But Walker said he's optimistic about what agencies will soon be able to accomplish.

He said the government is finally starting to devote funding to this, meaning line items will probably begin appearing in fiscal 2026 budgets.

And it won't be a moment too soon, Walker said.

"Industry experts have said they believe nation states are already leveraging quantum computers to crack encryption and get to secrets. I think we'll start seeing more research and things coming out between now and the end of the year, like an academic institution claiming that they've achieved it. But in the cyber world, common thinking is that some nation states have already accomplished this.

Army readies new AI guidance based on lessons learned

BY JARED SERBU

The Army plans to issue guidance on how its various organizations should and shouldn't make use of artificial intelligence, based on lessons learned from a series of pilot efforts over the last several months. But at least one thing is already clear: Cost considerations will be a significant factor going forward.

Under the auspices of Project Athena, which officials launched in November 2024, the Army has been examining AI use cases that can deliver capability to broad swaths of the service, largely in back office–type business functions. Technology and acquisition leaders have been looking at different deployment architectures, the potential utility of various AI tools and cost models.

One goal is to find ways to deliver AI capabilities that can serve 80 percent of the Army, rather than letting "a thousand flowers bloom," said Leonel Garciga, the Army's chief information officer.

"These efforts are hyper-focused on back office and on capabilities that are ready to go. There's not a lot of [government R&D] work happening here. We're seeing them in commercial space, a lot of us are using them personally, and it's stuff that we can deploy on the network today," he told reporters during a briefing.

These efforts are hyper-focused on back office and on capabilities that are ready to go. There's not a lot of [government R&D] work happening here.

Leonel Garciga
CIO, Army

"We started with an initial memo that said, 'Hey, commanders, go do this. Run as fast as you can. Here are some guidelines, here's some things you need to think about. Think about cybersecurity, think about resourcing.' I think in this next phase, we'll mature that and say, 'Here's what we learned over the last couple of months, and here's where you're best postured to use this capability against this resourcing profile and this cybersecurity profile.' "

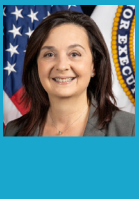
Cost guardrails for AI implementation

One of those lessons? The Army will need to be deliberate about creating guardrails around commands' use of commercial AI capabilities, mainly for cost reasons. Since most of the tools they'll be employing use cloud consumption-based pricing models, bills can add up quickly.

In at least one recent case, the on-demand billing associated with an AI platform put an Army program at financial risk, Garciga said.

"One of our army commands was asked to look at a national-level data problem, and they needed a response very quickly. And within 48 hours, we had the database, we had analytical work that was ready to go, and we unleashed the power of some of these tools in the cloud. It was a real fast spin-up. But all of a sudden, I needed GPUs that weren't in my budget," he said. "That was done in a very unconstrained manner, so it really pushed the limits of their resourcing for their base cloud bill because we didn't have these guardrails in place at that time."

> I don't think that financially, over time, it makes any sense to do this on prem because we are going to have to buy GPUs. We're going to have to maintain that facility and that infrastructure.



Jennifer Swanson
Deputy Assistant Secretary for Data, Engineering and Software, Army

One possible answer is to implement hard limits, enforced by commercial cloud service providers, so that commands and program offices don't inadvertently run up huge bills. But Garciga said policing those cloud costs in the Army's IT ecosystem is potentially more challenging than in purely commercial environments.

"Most CIOs in the commercial space would say that they're building these guardrails to make sure that they don't push on cloud costs so much that they price themselves out of the market through analytical work," Garciga said.

"The more important question is: How do we get to a business model that allows us to do guardrails in an environment where sometimes it's cloud-native but sometimes we're using cloud compute and storage with an organic large language model on top? How do we build guardrails into that? That's the place where we're spending a lot of time exploring. We need to understand whether we have enough fine-grained control to make sure that we don't inadvertently price ourselves out when we're running analytics."

On-prem AI hosting will be rare

But even in cases where the Army is using its own AI models and algorithms, in most instances, it's likely to use commercial clouds for its computational and other infrastructure needs. Running large AI tasks in government-owned data centers will be fairly rare.

On-premise hosting "will be for those models that we need to have behind the fence line," said Jennifer Swanson, deputy assistant secretary of the Army for data, engineering and software. "I don't think that financially, over time, it makes any sense to do this on prem because we are going to have to buy GPUs. We're going to have to maintain that facility and that infrastructure. And three years from now, when those GPUs are no longer sufficient for the model we want to run, we're going to have to buy new GPUs. From the standpoint of back office, cloud is the way to go. They're going to be able to keep up, and we're not, so we should leverage what they're providing."

As for the outcomes of Project Athena, Swanson said most of what the Army will issue will be new policies and guidance — not necessarily new ways of contracting for AI.

"There will be some contracts that we have that we can make available, but we're definitely not going to say these are the only contracts you shall use," she said.

"There's going to be other options for commands, if they so choose, and there probably will be some policy that comes out based on what we learn. It will constrain if you are going to solicit for some other capability, you shall do this or shall not do this, and it's really going to be based on what we learn as we proceed."

How to identify opportunities for consolidation in pursuit of efficiencies

The way government works is changing rapidly, with agencies across the board downsizing their workforces, returning employees to their offices and seeking technological solutions to improve efficiency. All those efforts put together are creating ripple effects across the federal space, and the private sector partners who support those agencies. One of those effects is heightened scrutiny on agencies' modernization efforts and their attempts to move forward on modernization initiatives.

"There's been an enormous amount of compartmentalization or siloing of responsibilities across IT infrastructure as a whole. Whether it's defining process owners or component owners, operational segregation of duties, if you will, to create these highly focused groups of resources to support both developing and operating the missions and evolving the missions over time, or the systems that support the missions," said Bill Lemons, director of systems engineering for Fortinet Federal.

"When it's met with the challenge of getting a high degree of scrutiny with regards to efficiency, it brings to light the possibility that some of that highly compartmentalized approach to these solutions may not be the most efficient."

> There's been an enormous amount of compartmentalization or siloing of responsibilities across the IT infrastructure as a whole.

Bill Lemons
Director of Systems Engineering, Fortinet Federal

But the current shake-up in operations among federal agencies presents an opportunity for them to adopt some of the philosophies of the private sector, particularly in the area of consolidation. If these compartmentalized teams can adopt the mindset that certain siloes may share complimentary and interrelated knowledge, they may be able to benefit from working more closely together.

Doing so may enable them to enrich the overall solution; this can prove especially true of consolidating network and security teams.

Network and security are traditionally siloed operations, but artificial intelligence initiatives may enable them to gain greater shared insights by culling data from diverse sources and examining it through different lenses. Wherever there are complementary services, consolidation can provide additional efficiencies and cost savings.

Identifying opportunities for consolidation

IT modernization efforts have been ongoing for some time now. Newer mandates like zero trust adoption and return to office have placed a particular focus on continuous improvement of agencies' infrastructure. But much of that infrastructure has been mostly dormant or lightly used for years as agencies pivoted during the pandemic to remote work. These new requirements are applying massive stress, laying the foundations for greater consolidation between network and security.

"Looking at those two things together and trying to find ways of bringing efficiencies, it's a conversation with your partners, the groups that are providing you either complete solutions, point products or any number of combinations of those things, and really trying to understand whether or not they're looking at trying to provide that consolidation," Lemons said.

"Because when it comes to the spending piece, there's additional scrutiny being put in play to ensure that we're driving high levels of efficiency with all of the spending that's done as well. So that confluence all coming together really creates that demand for efficiency."

FORTINET FEDERAL®
Trusted Cybersecurity for Government
Simplifying Security, Enhancing Efficiency
www.fortinetfederal.com

That communication with industry partners can help agencies understand what's available to support those efforts.

Efficiencies from consolidation

Networks rife with point products generate data from a vast number of devices. That data can provide situational awareness on what's working well in the environment and where the challenges lie.

But the more sources of data there are, the harder it is to glean insights and separate the signal from the noise, Lemons noted. Consolidation through a shared platform can reduce the number of devices producing data and requiring updates and maintenance. It also makes the user interface consistent across all those pieces, standardizing the syntax for multiple functions, allowing them to interoperate more easily, he said.

Third-party integrations also allow agencies to consolidate products and services from various vendors across multiple teams and locations. That allows streamlining both management and operation of the hardware into a single pane of glass, while still providing the necessary functions across a building or even a campus.

"As agencies start to look toward their modernization effort, they really need to take a look at and follow the guidance that's getting put in place right now with regards to focusing on consolidation as a way to gain efficiencies. That technology has been proven in the commercial world to be very successful. And obviously it needs to be vetted and appropriate for federal consumption as well," Lemons said.

> Look both at the cost of operations as well as the cost and value of the product itself. Don't sacrifice performance. And, if consolidation can't be provided in a single platform of complimentary capabilities, then really look for opportunities where a platform approach ... can exist across multiple point products.
>
> ***— Fortinet Federal's Bill Lemons***

"Look both at the cost of operations as well as the cost and value of the product itself. Don't sacrifice performance. And, if consolidation can't be provided in a single platform of complimentary capabilities, then really look for opportunities where a platform approach — a highly integrated, potentially singular user interface, singular operating system — can exist across multiple point products and provide an agency with many benefits from a cost and operations perspective."

carahsoft.

FORTINET FEDERAL

opentext™

SOLARWINDS Public Sector

SIMSPACE

TYCHON

VAST FEDERAL