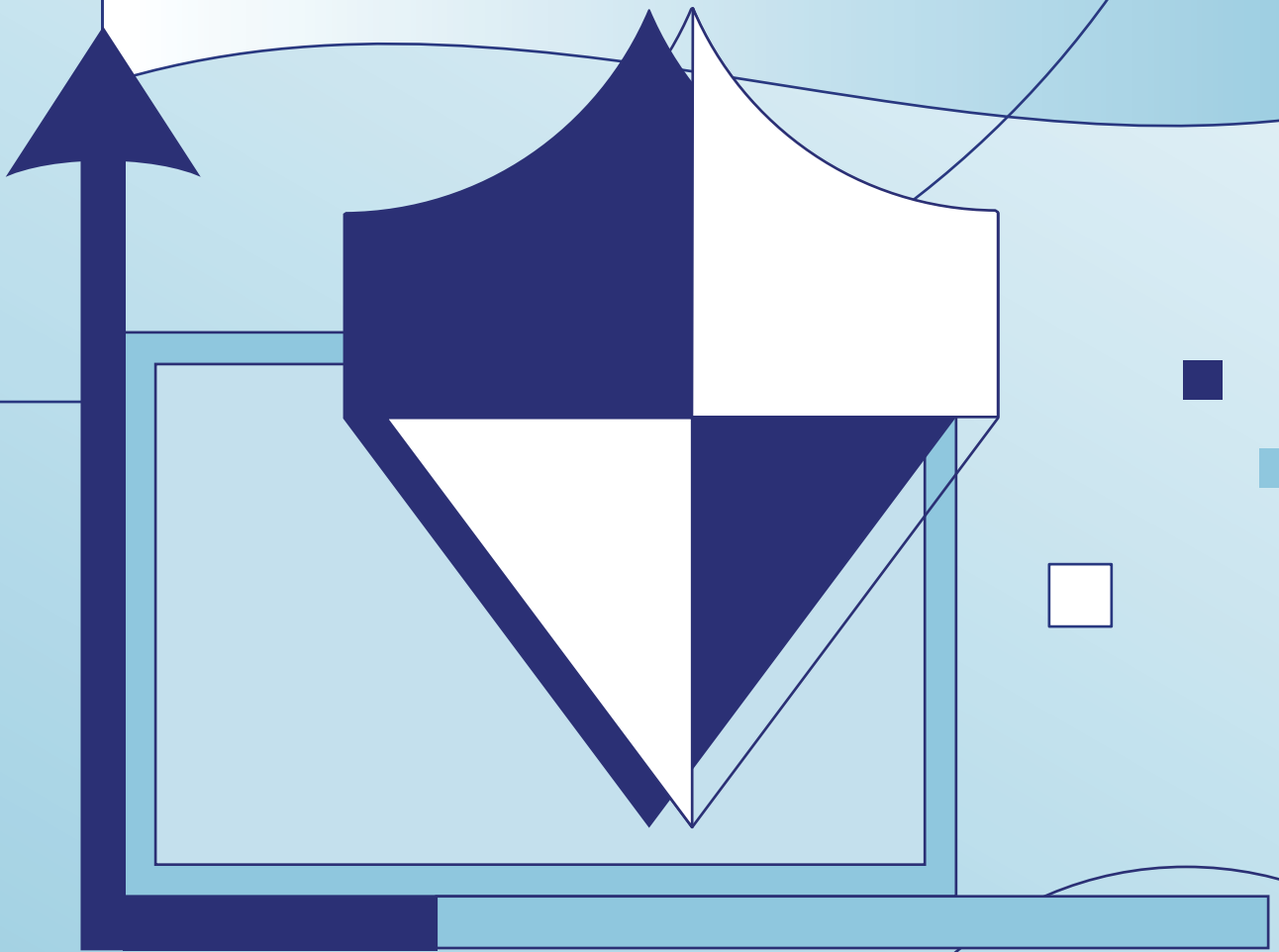


Focus on Cyber Force Multipliers



Introduction

Cybersecurity teams, like everyone in government, are dealing with increasingly constrained budgets and staffing limits. But to make matters worse, this is happening at a time when the IT environment is growing more complex and the cyber threats more sophisticated. In cybersecurity, “do more with less” is not a mindset. It’s a mandate.

In this guide, the second of a three-part series, we explore different technologies and tactics that can serve as force multipliers for cyber teams, helping them not only respond to the current threat landscape but prepare for whatever comes next.

We start by looking at cyber-related events of the past 12 months, in which agencies found themselves dealing with both landmark incidents (the discovery of Salt Typhoon, the infiltration of the nation’s telecommunications infrastructure) and the mundane (reducing security misconfiguration of cloud-based applications). We also hear from government cyber leaders about their top priorities, drawing on recent GovLoop virtual events.

All of this sets the stage for our look at four technologies and strategies that have emerged as potential cyber force multipliers, enabling agencies to strengthen their defenses working within their existing (and future) constraints.

Our third cyber guide, in October, will take a deep dive into artificial intelligence (AI) and its impact on cyber operations, for better and for worse.

Contents

- 3 Agencies Respond to Shifting Cyber Threats and Strategies**
- 5 How to Bring Greater Efficiency to Network and Cyber Operations**
- 6 How to Get Your Identity-Based Security Up to Speed**
- 7 4 Ways to Boost Cyber Efficiency**
 - 8 Predictive Analytics
 - 9 Secure Software Development Life Cycle
 - 10 Security Orchestration, Automation and Response
 - 11 Vulnerability Protection/False Positives
- 12 Meeting the Challenge of Insider Threats**
- 13 How to Mitigate the Threat of Identity-Based Attacks**
- 14 Cyber Risk Management? A Better Bet Is Danger Management**
- 15 3 Priorities to Elevate Cybersecurity in Adversarial Times**
- 19 State and Local Agencies Find Strength in Whole-of-State Cyber Strategy**
- 20 How to Tackle Your Mobile Device Security Risks**
- 21 The Essentials of Cloud Data Security**
- 22 Conclusion**

Agencies Respond to Shifting Cyber Threats and Strategies

Between the Salt Typhoon attack, AI-driven threats and more mundane risks, government agencies have spent the past year adapting to a new cyber reality.

JUNE 2024

In a study of 172 **open source-based projects**, the Cybersecurity and Infrastructure Security Agency (CISA) reports that 52% included code that left the software vulnerable to memory errors malicious actors could exploit.

In collaboration with more than 50 experts in AI, CISA conducts a four-hour tabletop exercise focused on understanding and mitigating **digital threats to AI systems**.

JULY 2024

A glitch in a routine update to a common security module causes many Microsoft Windows-based systems to crash, leading to **IT outages** across the public and private sectors.

The Institute for Critical Infrastructure Technology (ICIT), a nonpartisan think tank, launches the **ICIT Center for Federal Civilian Executive Branch Resilience**, which is intended to serve as a hub for research, education and collaboration around security technology and policy.

AUGUST 2024

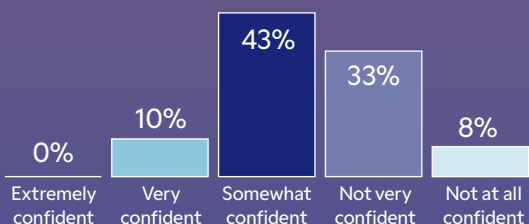
The National Institute of Standards and Technology (NIST) releases draft guidance on the use of **digital identity solutions**, such as passkeys and digital wallets, that people can use when accessing government services.

CISA publishes guidance to help agencies identify systems that rely on encryption tools that eventually could be vulnerable to **quantum computer-based attacks**.

“The rapid proliferation of online services over the past few years has heightened the need for reliable, equitable, secure and privacy-protective digital identity solutions.”
— **NIST**

STATE CISOS WARY OF AI-ENABLED THREATS

A September 2024 study by NASCIO and Deloitte finds that state-level chief information security officers lack confidence in their states’ ability to defend against AI-driven cyberattacks.



SEPTEMBER 2024

A report from the National Association of State CIOs (NASCIO) and Deloitte highlights how **CISOs** are spending less time in their roles: an average of 23 months now, down from 30 in 2022.

While the wide range of possible attack vectors has grown in recent years, a CISA analysis finds that malicious actors still rely heavily on one of the most basic: **stealing employee credentials**.

OCTOBER 2024

The U.S. Energy Department's Energy Threat Analysis Center went fully operational, becoming a new forum for **alerting industry to emerging threats** to energy systems.

The FBI and CISA announce that a cyberattack linked to the Chinese government has gained unauthorized access to the commercial telecommunications infrastructure. The attack becomes known as **Salt Typhoon**.

DECEMBER 2024

CISA directs agencies to adopt its Secure Cloud Business Applications (SCuBA) baseline to reduce the risk of security vulnerabilities due to **cloud misconfigurations**.

The 2025 National Defense Authorization Act is signed into law, requiring DoD's CIO to extend DoD's zero-trust strategy to wearable computers, sensors and other **Internet of Things hardware**.

After Salt Typhoon, Sens. Eric Schmitt (R-Mo.) and Ron Wyden (D-Ore.) called for the DoD OIG to investigate the department's reliance on **unsecured telecommunications networks**.

MARCH 2025

The U.S. General Services Administration announces that the Federal Risk and Authorization Management Program (FedRAMP) office will work with industry to **streamline and automate the process** for vetting the security of cloud-based applications.

As part of an executive order titled "**Achieving Efficiency Through State and Local Preparedness**," the Trump administration directs state and local governments to take the lead in preparing for and responding to a wide range of crises, including wildfires, hurricanes and cyberattacks.

NOVEMBER 2024

NASCI encourages states to take a **whole-of-state approach** to cybersecurity, including extending assistance to cities and counties that lack the staff or resources to defend their systems.

The Office of the Inspector General (OIG) for the Veterans Affairs Department reports that a VA office in Atlanta **failed to encrypt** the records of more than 3 million veterans.

JANUARY 2025

In an open letter to the new Trump administration, the Better Identity Coalition advocates for greater investments in identity technology to **reduce fraud** in government benefits programs.

CISA publishes the AI Cybersecurity Collaboration Playbook, which aims to improve collaboration across the public and private sectors around **cyber risks in AI systems**.

FEBRUARY 2025

The Office of the Comptroller of the Currency notifies Congress that malicious actors had compromised administrative email accounts and **gained access to "highly sensitive information"** about federally regulated financial institutions.

APRIL 2025

Karen Evans is nominated to serve as the **Undersecretary for Management at the U.S. Department of Homeland Security**, responsible for securing all federal infrastructure.

Just hours before funding was set to expire, CISA extends a contract with MITRE to manage the **Common Vulnerabilities and Exposures** program.

How to Bring Greater Efficiency to Network and Cyber Operations

WATCH VIDEO



“You can create a consolidated environment that provides the full breadth of required services but with highly efficient management.”

— Bill Lemons, Fortinet Federal

ABOUT FORTINET FEDERAL

Fortinet Federal, Inc., a wholly owned subsidiary of Fortinet, Inc., is dedicated to delivering trusted cybersecurity and IT modernization solutions to U.S. Federal government agencies. Fortinet Federal provides the public sector with a comprehensive cybersecurity platform that combines advanced threat protection, secure access, and integrated cloud and network security to anchor any agency Zero Trust architecture. Trust Fortinet Federal to safeguard your agency operations and mission-critical assets.

[Learn more about Fortinet Federal.](#)

**FORTINET
FEDERAL®**

Network and security modernization initiatives have taken on new importance in recent months. With return-to-office mandates, agencies are concerned about the ability of their legacy infrastructure to handle the surge in bandwidth requirements. At the same time, as the threat landscape continues to evolve, agencies also are looking to adopt advanced cyber capabilities, such as defense-in-depth, microsegmentation and zero trust.

Increasingly, agencies recognize they need to take a converged approach, integrating their network and cyber infrastructure in a common platform. This approach also helps improve the efficiency of IT operations, said Bill Lemons, Director of Systems Engineering at Fortinet Federal.

In this [video interview](#), Lemons discusses best practices in shifting to a converged approach. Topics include:

- Closing the knowledge gap that hinders cybersecurity efforts
- Reducing the total lifecycle costs associated with managing infrastructure
- Incorporating new and emerging technologies into the IT environment

How to Get Your Identity-Based Security Up to Speed

WATCH VIDEO



“Agencies are looking to adopt more modern identity solutions, especially because the demands of their organizations are increasing and they need more agility. And what users are expecting in terms of an experience is also rapidly moving forward.”

— Khizar Sultan, CyberArk

Many agencies are realizing that their legacy identity-based security solutions are beginning to age out. It shouldn't be a surprise. Identity solutions have played an essential role in cybersecurity for more than 20 years, with an evolving set of tools and tactics for identity and access management (IAM), privilege access management, governance, and more. But the earlier generations were not designed to address the complexity of today's IT environment.

That's because security capabilities are just one aspect of an identity solution, said Khizar Sultan, Vice President of Workforce and IGA Solutions at CyberArk. As agencies increasingly rely on cloud- and software-as-a-service-based offerings, they need to address concerns around scalability and productivity, in addition to the governance of artificial intelligence tools, such as AI agents. Legacy systems don't measure up.

In this [video interview](#), Sultan discusses how agencies can adopt an identity-first approach to cybersecurity. Topics include:

- The key attributes of an identity-first approach
- The connection between identity security and the user experience
- The importance of identity security to the use of AI solutions

ABOUT CYBERARK

CyberArk is a cybersecurity company specializing in privileged access management (PAM) and identity security solutions. Its primary focus is to help organizations protect privileged accounts, credentials, and sensitive data from cyber threats, insider attacks, and compliance risks. CyberArk is widely used by financial institutions, government agencies, healthcare organizations and enterprises to secure their most sensitive data and systems.

[Learn more about CyberArk.](#)

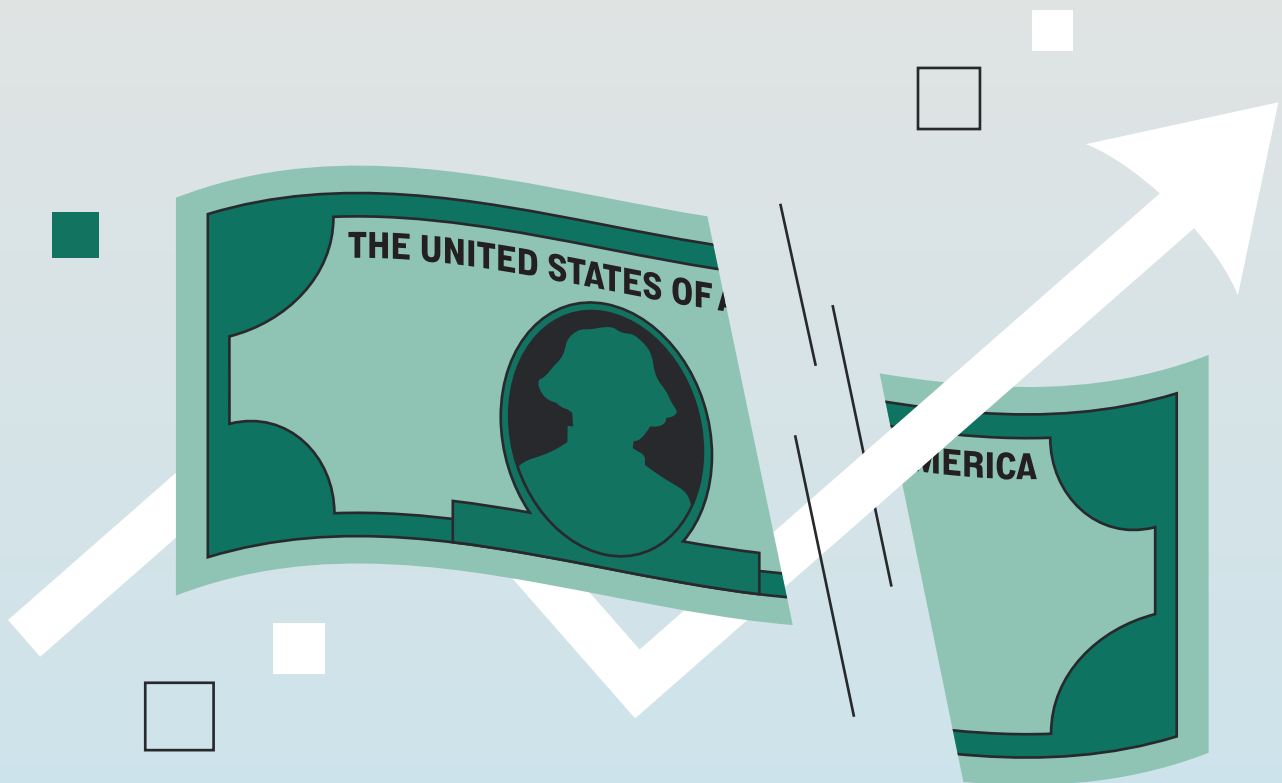


4 Ways to Boost Cyber Efficiency

A perennial threat, cyberattacks continue to grow in sophistication and number. In fact, “there has been an increase in most types of cyberattacks across the United States,” the Government Accountability Office reports.

At the same time, cybersecurity funding presents its own challenge. For instance, in March 2025, the Trump administration cut about \$10 million from two U.S. Cybersecurity Infrastructure Security Agency (CISA) programs: the Elections Infrastructure Information Sharing and Analysis Center and the Multi-State Information Sharing and Analysis Center.

Fortunately, government agencies are well-versed in finding ways to do more with less, and this situation is no different. Here are four effective, budget-friendly ways to boost cyber operations’ efficiency.



PREDICTIVE ANALYTICS

THE CHALLENGE

One of the biggest challenges in cybersecurity is getting ahead of the type, timing and target of the next cyberattack.

THE SOLUTION

Predictive analytics can help. It uses advanced tools and analysis, such as data mining, AI, statistical models and big data analytics, to identify patterns in historical data to forecast outcomes. It can learn risks and threats to the enterprise IT environment without manually inputting data, according to the Center for Cybersecurity Analytics and Automation, which is crucial when resources are tight. Exposure management, threat intelligence and cybersecurity validation techniques are key to predictive security, Gartner says.

HOW IT HELPS

“Predictive models can help organizations anticipate new attack vectors, understand adversary behaviors, and prioritize defensive measures effectively,” a 2024 research report states. For example, intrusion-detection systems use predictive models to find unusual patterns and behaviors that signify an attack, according to an article in the World Journal of Advanced Research and Reviews. One clue might be someone who always logs into the network from the office starting to log in from remote locations.

“By anticipating and addressing potential vulnerabilities in advance, predictive analytics helps in reducing the likelihood of successful attacks and enhancing overall cybersecurity resilience,” the article states.

What’s more, prediction can mean defense. Predictive tools can be configured to automatically isolate networks, computers or other IT experiencing anomalies for evaluation. That keeps the issue contained until someone can verify whether the behaviors are safe.



SECURE SOFTWARE DEVELOPMENT LIFE CYCLE

THE CHALLENGE

As new cybersecurity approaches emerge, it's important to patch software with the latest protections. But patching has downsides, such as disrupting business operations, making systems unstable and relying on humans to hit the “update” button. That's why it doesn't always happen. “A third of ransomware attacks start with an unpatched vulnerability,” [research by Sophos](#) shows.

THE SOLUTION

A better approach is software with security built in. That's the crux of the Secure Software Development Life Cycle (SSDLC). “It involves planning, designing, coding, testing, deploying, and maintaining software while consistently addressing security concerns at each step,” according to [GeeksforGeeks](#), an educational portal. “It is an essential practice in the ever-changing landscape of cybersecurity.” Examples of SSDLC efforts include static analysis (an automated process for identifying known patterns of insecure code), scanning apps and their infrastructure for vulnerabilities and misconfigurations, code reviews, penetration testing, and bug reviews.

HOW IT HELPS

The benefits of including cybersecurity in software development from the get-go are a no-brainer. The result is better software quality, risk management and even cost efficiency, especially if agencies don't have to pay the exorbitant costs associated with data breaches.

Use of SSDLC is growing. [Forrester's Developer Survey 2024](#) found that 24% of executive-level respondents said that in the next 12 months, they would use AI and generative AI (GenAI) across the entire software development life cycle. Specifically, Forrester predicts that 30% of organizations will use TuringBots, AI- and GenAI-infused development tools, to accelerate software development.

Organizations looking for a starting point with SSDLC can use the National Institute of Standards and Technology's [Secure Software Development Framework](#), which aims to “help software producers reduce the number of vulnerabilities in released software, mitigate the potential impact of the exploitation of undetected or unaddressed vulnerabilities, and address the root causes of vulnerabilities to prevent future recurrences.”



SECURITY ORCHESTRATION, AUTOMATION AND RESPONSE

THE CHALLENGE

Cybersecurity is often piecemeal, with each element of IT, each department and even individual incident responders working in their own vacuums. That separation hinders coordination, collaboration and ultimately security, slowing response. “Monitoring security across a growing and changing attack surface was cited as the most significant security operations challenge by approximately 53% of participants” in The State of Automation in Security Operations: A SANS Survey.

THE SOLUTION

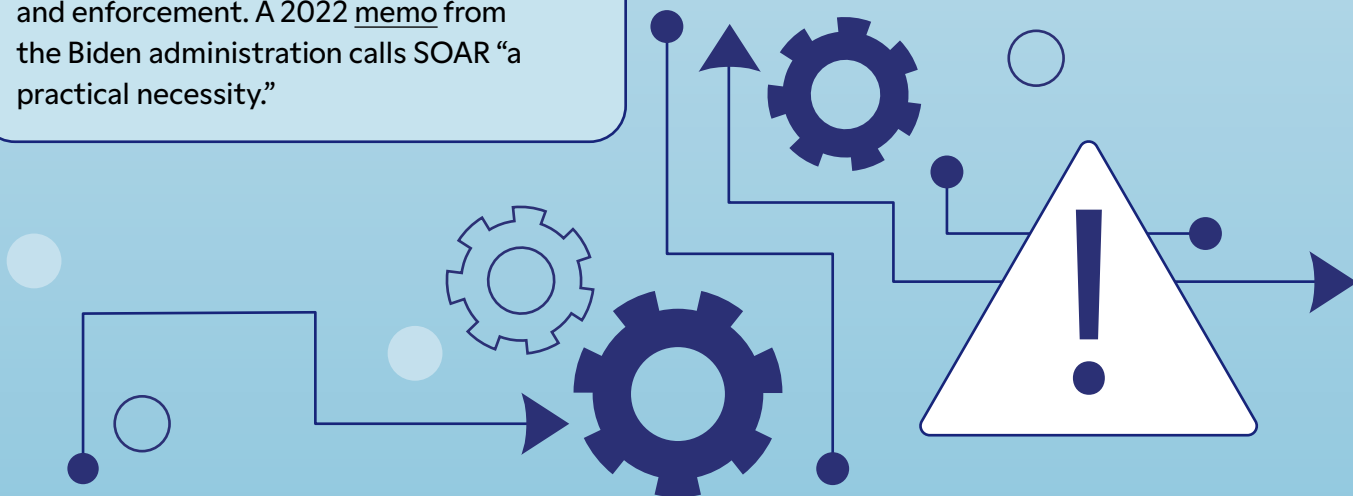
Security Orchestration, Automation and Response (SOAR) unites several foundational elements of cybersecurity, including zero trust, identity management, device and data security, and network segmentation, and automates monitoring and enforcement. A 2022 memo from the Biden administration calls SOAR “a practical necessity.”

HOW IT HELPS

Besides automating security, SOAR facilitates information sharing so that multiple automated tasks can work together. This can happen at a team or user level, according to SANS, and can take several forms, from externally maintained, system-specific automation, such as a local script running in a home directory, to fully autonomous systems.

Some organizations have already embraced SOAR. For instance, about 52% of survey respondents said they have already automated phishing response. Priorities for the future focus on detection and response, with breach response, malware forensics, threat intelligence, user and remote access management, and cloud security and configuration among the most cited items on respondents’ wish lists.

“SOAR can help teams find efficiencies in a variety of operational tasks,” SANS states.



VULNERABILITY DETECTION/FALSE POSITIVES

THE CHALLENGE

As much as we want to think technology is perfect, it's not. The speed at which new IT, especially AI, is released makes it particularly susceptible to having vulnerabilities and returning false positives, or identifying problems where there are none. These vulnerabilities can be exploited quickly but often remediated slowly, according to a [study](#) from the University of Illinois Urbana-Champaign.

THE SOLUTION

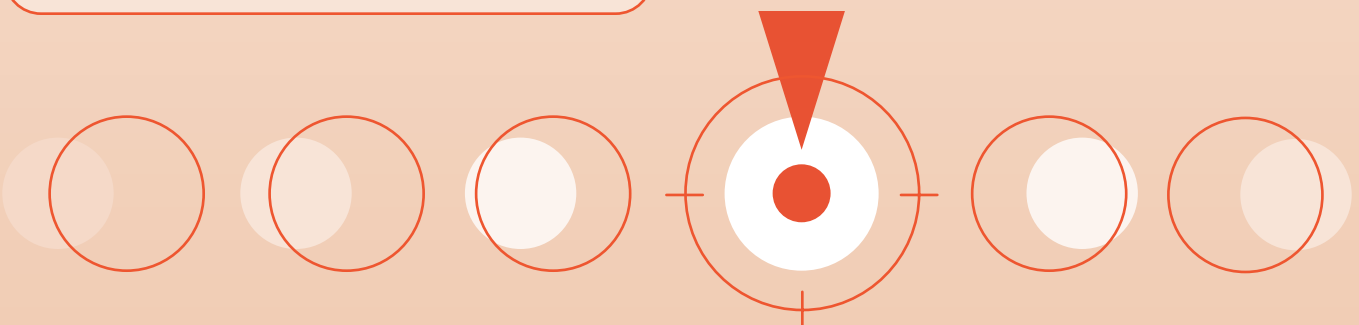
Sometimes the best answer is the simplest: Detect vulnerabilities and minimize false positives. AI, especially GenAI, can be a boon here, working much faster — and cheaper — than humans could. Purse-string pressures to show value from security investments mean a greater emphasis on meeting key performance indicators (KPIs), including detection fidelity and mean time to respond, according to a [report](#) from NST Cyber. “[GenAI is not just enhancing these KPIs; it’s fundamentally transforming how organizations manage vulnerabilities and exposures,” the report states.

HOW IT HELPS

Integrating GenAI into vulnerability management can make detection more accurate and reduce false positives, NST Cyber states, because its advanced pattern recognition capabilities and real-time analysis of data from diverse sources let it analyze vast amounts of information quickly.

Several big tech firms, such as Microsoft, Google, SentinelOne, CrowdStrike and Cisco, have already applied GenAI to their security operations tools, and code-generation tools from GitHub Copilot and Amazon CodeWhisperer use it to scan source code for vulnerabilities and as a “confirmation layer” to explain why a finding might be a false positive.

By 2027, GenAI will contribute to a 30% reduction in false positive rates for application security testing and threat detection, [Gartner predicts](#). But that doesn’t mean traditional approaches should be tossed: After pilot testing software that uses AI, [CISA concluded](#) that it works best when supplementing and enhancing, not replacing, existing tools.



Meeting the Challenge of Insider Threats

WATCH VIDEO



Tieu Luu

Chief Product Officer, Qmulos

“[Agencies] have to make sure that we have a synoptic picture of what’s going on in our networks, weaving together a great amount of data to identify anomalous activities.”

— Paul Kurtz, Splunk

Insider threats have always been with us but new technologies, including artificial intelligence, have made it easier for network users to access and expose sensitive data.

To minimize those risks, agencies must focus on controlling authentication, access and permissions. They need to implement least privilege models, separation of duties and comprehensive auditing. The auditing part is key to track those events and synthesize that information to determine when — or whether — there is a threat within the system, said Tieu Luu, Chief Product Officer at Qmulos.

User activity monitoring is a critical piece of this, said Paul Kurtz, Chief Cybersecurity Advisor at Splunk, but it requires weaving together a great amount of data to identify those anomalous activities.

In this [video interview](#), Luu and Kurtz discuss strategies for identifying and mitigating insider threats. Topics include:

- Establishing behavioral baselines for assessing user activity
- Using AI and machine learning to detect potential threats
- Protecting the privacy of individuals during the threat assessment process

ABOUT QMULOS

Qmulos applications improve operational security through real-time risk management and compliance automation. It makes evidence-based risk management decisions possible by providing real-time insights on overall enterprise risk posture. Qmulos ensures agencies and their partners adhere to critical security compliance regulations.

[Learn more about Qmulos.](#)

ABOUT SPLUNK

Splunk Inc. turns data into doing with the Data-to-Everything Platform. Splunk technology is designed to investigate, monitor, analyze and act on data at any scale. Splunk’s powerful platform and unique approach to data have empowered companies to improve service levels, reduce operations costs, mitigate risk, enhance DevOps collaboration and create new product and service offerings.

[Learn more about Splunk.](#)



How to Mitigate the Threat of Identity-Based Attacks

WATCH VIDEO



Cristian Rodriguez

Field Chief Technology Officer for the Americas, CrowdStrike

“In our 2025 Global Threat Report, the numbers are substantially increasing where identity is the focal point of the adversary because it does represent the path of least resistance.”

— Cristian Rodriguez,
CrowdStrike

Identity is at the heart of the modern cyber ecosystem. Whether implementing full-blown zero-trust security or not, a growing number of agencies authenticate the identity of users or applications before permitting them to access network resources. But here’s the catch: How do you know if an identity has been compromised?

This is not a hypothetical question. Malicious actors recognize that the easiest way to evade an agency’s defenses is to steal an employee’s identity and work as an insider threat.

In this [video interview](#), Cristian Rodriguez, Field Chief Technology Officer for the Americas at CrowdStrike, discusses how agencies can reduce the risk of identity-based attacks on network resources. Topics include:

- The importance of establishing baselines for activity on the network
- The role of continuous monitoring in identifying potential security gaps
- The value of automating enforcement to mitigate potential threats

ABOUT CROWDSTRIKE

CrowdStrike protects the people, processes and technologies that drive modern enterprise. The company provides a single agent solution to stop breaches, ransomware and cyberattacks—powered by world-class security expertise and deep industry experience.

[Learn more about CrowdStrike.](#)



Cyber Risk Management? A Better Bet Is Danger Management

WATCH VIDEO



John Kindervag

Chief Evangelist, Illumio

Risk management, a concept that originated in the financial sector, has proven to be a poor fit for cybersecurity, according to one industry thought leader.

John Kindervag, Chief Evangelist at Illumio, says the basic premise of risk management — that you can calculate the probability of a particular risk materializing — might be feasible in finance, where analysts work with finite datasets. But in cybersecurity, the number of variables involved, if not infinite, is simply unknowable, making it impossible to quantify risks in any meaningful way.

Kindervag, who is credited with defining the concept of zero-trust security in 2010, when he was a principal analyst at Forrester Research, recommends a new approach: danger management.

In this [video interview](#), Kindervag explains the concept of danger management and how it can help agencies bring greater urgency to their cybersecurity efforts. Topics include:

- Building a strategy around protecting high-value assets
- Thinking in terms of mitigating threats, rather than accepting risks
- Applying danger management within the zero-trust framework

“There’s no way to say there’s a 10% chance you’re going to get hacked, or 0% or 100%. There’s just no way to know that. And what it causes people to do is to accept risks that they shouldn’t.”

— John Kindervag, Illumio

ABOUT ILLUMIO

Illumio, the breach containment leader, stops breaches and ransomware from spreading across the hybrid attack surface. The Illumio Zero Trust Segmentation Platform visualizes how workloads and devices are communicating, creates granular segmentation policies which allow only necessary communication, and automatically isolates ransomware and breaches.

[Learn more about Illumio.](#)

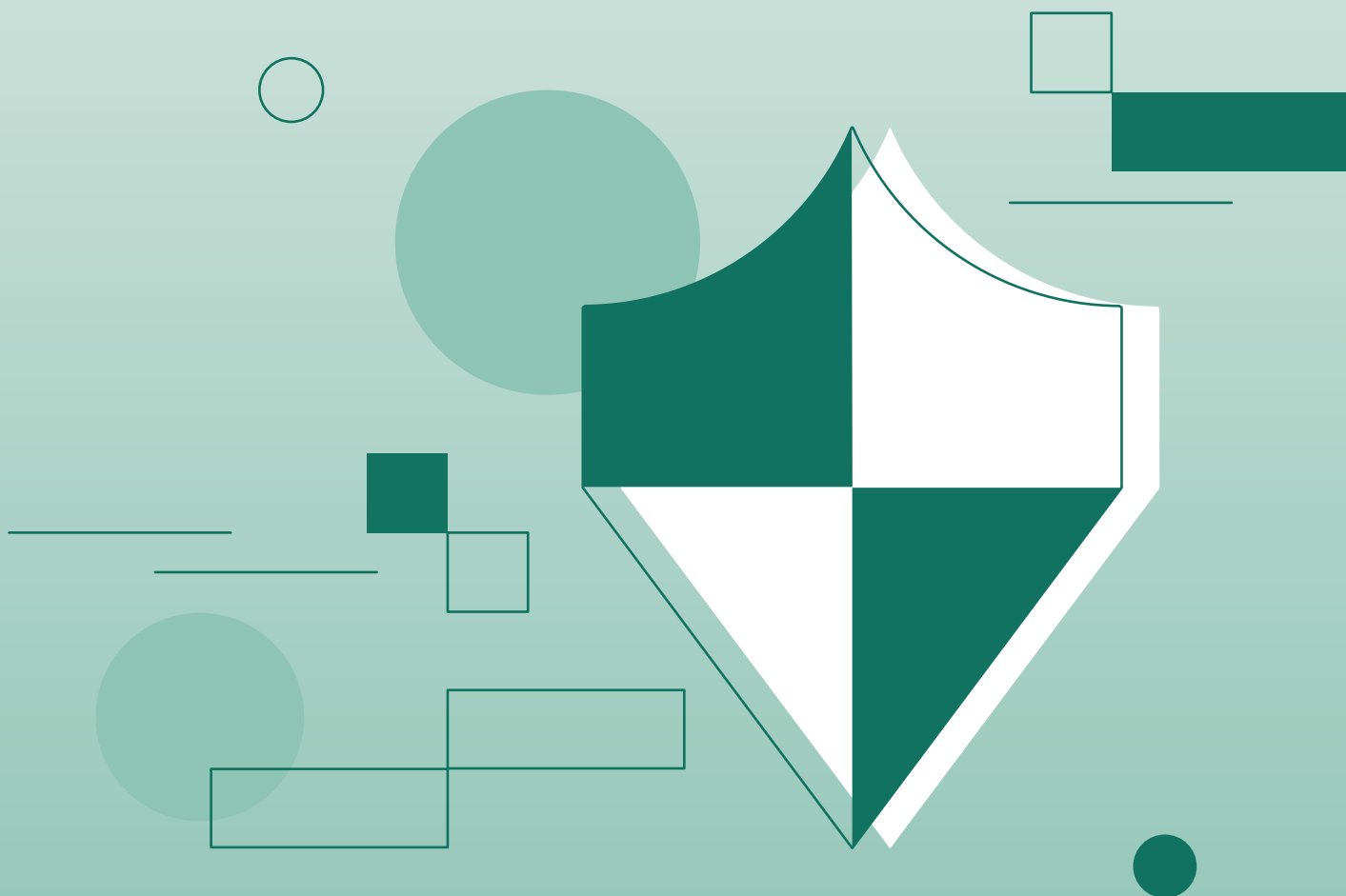


3 Priorities to Elevate Cybersecurity in Adversarial Times

Cybersecurity is an increasingly adversarial arena in which criminal gangs and nation-state actors target all levels of U.S. government. Plenty of tools and technology aim to safeguard agency systems, but to remain effective in their cyber defenses, government IT leaders must prioritize their efforts.

Rather than fall for the latest shiny solution, agencies need a risk-based approach to cyber tooling and measurable goals for managing user identities. Additionally, leaders should adopt a forward-looking security posture to keep pace with today's fast-changing threat landscape, including AI-driven risks.

Government leaders weighed in on these priorities during recent GovLoop events and offered the following insights.



1 – ALIGN THE TOOLS TO THE RISK

Although the right cybersecurity solutions are key to resilience, tools are just a part of the overall picture, said Bryce Carter, Chief Information Security Officer (CISO) for Arlington, Texas. By prioritizing a thoughtful approach to risk management, IT teams can make the most of those tools.







Government IT sometimes leans toward “just tossing more tools at the problem,” he said, but without the proper strategic thinking, “you’re throwing darts at a dartboard.”

It makes sense to deploy tools based on actual threat. “At the end of the day, is [cyber defense] really hitting your major risk points?” Carter asked. “It’s going to be a little bit different for every local government, depending on what you have. Some have power utilities, and that’s a very different risk profile than some other things. You need to be taking a risk-based approach.”

That risk-focused mentality encourages IT teams to **think beyond the typical emphasis on checking boxes around compliance.** “Truth be told, pretty much everyone who has had a data breach, even in the private sector, has checked every single compliance box,” he said. But all that emphasis on compliance “didn’t actually do anything to their operational security.”

With too much focus on the tools, “we’re bringing our technical game in, which is good, but that’s not necessarily aligned with the way the organization is aligned,” Carter said. “It all starts with culture, and then the technical side comes along afterwards. It’s about elevating your security teams, your IT teams to being more of a strategic partner [and] ensuring their representation at all the different levels of decision-making.”

TYPES OF CYBERSECURITY TOOLS

-  Network Security Monitoring
-  Security Compliance
-  Web Vulnerability Scanning
-  Wireless Network Defense
-  Encryption
-  Firewalls
-  Packet Sniffers
-  Antivirus Software
-  Managed Detection and Response Services
-  Public Key Infrastructure Services
-  Penetration Testing

2 – IDENTITY DEMANDS MEASURABLE STANDARDS



Identity is the new front line in cybersecurity, and effectively managing it requires clear and measurable standards, believes Kansas CISO John Godfrey.

When tightening up identity and access, agencies can prioritize “adopting standards and practices that you can start to show progress against,” Godfrey said. That means **establishing best practice benchmarks.**

One approach is to document progress toward microsegmentation, which divides a network into small, isolated segments to reduce the impact of potential breaches. With microsegmentation, “we start to carve up and split up and really create smaller zones, so that we can limit the lateral movement the threat actors may take,” Godfrey said.

IT staff likewise can measure how well they implemented multi-factor authentication across key systems, he said, adding that “you’d be surprised at how many areas still don’t have it deployed.”

Another potential benchmarking standard: continuous adaptation, or the IT team’s ability to continuously evolve its security strategies. That involves ongoing monitoring and the willingness and ability to adapt as appropriate.

Facing a dynamic threat landscape, government has a “constant need to focus on what our technology stacks look like” and to adjust accordingly, said Godfrey. “As technology evolves, it creates new opportunities, both good and bad. But it also gives us the opportunity to really look at solutioning and architecture, and to phase in new things to help us on this journey.”

IDENTITY MANAGEMENT LIFE CYCLE

Source: [Innominds](#)

PROVISIONING

- Create user IDs & identities
- Define user group membership
- Define systems

AUTHENTICATION

- Validate user identities using SSO services

AUTHORIZATION

- Determine the rights to access the systems
- Manage the systems

START OF USER IDENTITY

END OF USER IDENTITY

SELF-SERVICES

- Password changes and resets
- Update personal information
- User attributes sync with other systems as required

DEPROVISIONING

- Revoke permissions and unauthorize user identities to enterprise systems

GOVERNANCE

- Define organizations IAM guidelines to write rules/policies

PASSWORD MANAGEMENT

- Define password dictionary
- Enable password policies
- Sync password with end points

3 – ALWAYS LOOK FORWARD

Cyber defense can't afford to wait as technology advances. For instance, AI's rapid rise could expose cybersecurity gaps and aid malicious actors, said Sean Flowers, Executive Director of Ready Force Cyber, which supports cybersecurity workforce development.



"How do we ensure that the AI isn't able to have too many permissions? How do we ensure that people are using it correctly? Those are some of the challenges that we have with the emerging technology," Flowers said.

To tackle those issues effectively, IT leaders must commit to planning ahead. "We should be thinking about the next step: What do you need next, not what do you need now," he said. "If we're thinking about security that we have now and...the technology we have now, then [we're] probably already behind."

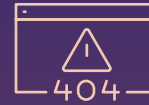
People are an agency's first line of cyber defense and its weakest link, so a **forward-looking strategy emphasizes employee training** — and not just generic don't-click-on-a-phishing-email education. Tailor training to an agency's culture, objectives, and relevant processes and tools, Flowers said.

"Everybody is mandated to have a cybersecurity awareness program [but] it's a lot of 'check the box,'" explained Flowers. "If you have programs that resonate with what the mission is...people tend to pay attention...and they'll take a little bit more pride in protecting information because now they know it's not some random scenario."

"If you are a government organization and you're thinking to yourself, 'there are a lot of evolutions happening right now in the cybersecurity realm,' [know that] there are always new threats on the horizon," Flowers said, and that will never change.

THINKING AHEAD: CYBER TRENDS TO WATCH

Attacks against cloud services



Growing IT skills gap and soft skills demand

Multi-factor authentication



Continuously evolving ransomware

Rise in IoT devices with 5G connectivity



Mobile cybersecurity

Generative AI and machine learning



Connected cars

Zero-trust cybersecurity



Rise in insider threats

International state-sponsored warfare



Cybersecurity to cyber resilience

Evolving social engineering attacks



State and Local Agencies Find Strength in Whole-of-State Cyber Strategy

WATCH VIDEO



“By joining forces, by leveraging limited resources, you can establish and create a more robust, comprehensive, and cogent cybersecurity posture.”

– Thomas MacLellan, Palo Alto Networks

For state and local governments and educational institutions, the threat landscape can seem increasingly daunting. Even as malicious actors grow more sophisticated and lethal, agencies continue to face significant obstacles in their efforts to defend their systems and data: cyber workforce shortages, a proliferation of point solutions that don’t interoperate and stringent budgets that limit access to much-needed resources. As it stands, it’s not a fair fight.

To change the odds, agencies need to change how they approach cybersecurity. One emerging concept is whole-of-state security, in which state and local agencies collaborate on their defenses, sharing information and resources.

In this [video interview](#), Thomas MacLellan, Director of Government Affairs and Strategy at Palo Alto Networks, discusses how whole-of-state security and related measures can help state, local and educational organizations strengthen their cyber posture. Topics include:

- The benefits of establishing joint security operations centers
- The opportunity to scale up orchestration and automation tools
- The importance of gaining visibility into all resources accessible through the public internet (i.e., your attack surface)

ABOUT CARAHSOFT

As the Master Government Aggregator® for its vendor and reseller partners, Carahsoft delivers a portfolio of secure IT solutions that enable the public sector to implement telework and online learning initiatives, support collaboration, ensure seamless operations, scale communications, and more.

ABOUT PALO ALTO NETWORKS

Palo Alto Networks is the global cybersecurity leader, committed to making each day safer than the one before with industry-leading, AI-powered solutions in network security, cloud security and security operations.

[Learn more about Carahsoft and Palo Alto Networks.](#)

How to Tackle Your Mobile Device Security Risks

WATCH VIDEO



Michael Riemer

SVP Network Security Group and Field CISO, Ivanti

“Whether it’s government-issued or government-furnished equipment or it’s a personally owned device, if it’s going to be connected [to the network], it needs to be secured. And that’s what a mobile device management solution does for you.”

— Michael Riemer, Ivanti

Government employees make ample use of cellphones, tablets, laptops, wireless printers and other mobile endpoints that connect to agency networks from locations near and far. The devices improve access and efficiency and can make workers more productive. But faced with a dramatic increase in nation-state and other cyber threats, agencies have come to realize that these off-premises devices are a significant vulnerability.

Mobile device management (MDM) gives agencies visibility into the number and types of end points connected to their networks — so that IT teams ultimately can block malicious activity. And by adopting “secure by design” principles — that is, considering security at the very start of a project — and automation, agencies can boost their cyber resilience. Think about the benefits of automatic updates on your cellphone, for example. Why give an end user the chance to remain less secure?

In this [video interview](#), Michael Riemer, Ivanti’s Senior Vice President of the Network Security Group and Field CISO, explains how to safeguard mobile end points efficiently and cost-effectively. Topics include:

- What to prioritize when modernizing your mobility operations
- What “secure by design” principles are, and why they’re vital
- How automation helps secure mobile end points

ABOUT IVANTI

Ivanti provides government organizations with scalable IT and security solutions to reduce costs, improve productivity and enhance risk management. By leveraging automation, integration and consolidation, Ivanti empowers IT teams to optimize budgets, eliminate redundancies, and focus on strategic goals, ensuring secure, efficient operations and seamless collaboration across IT and security functions

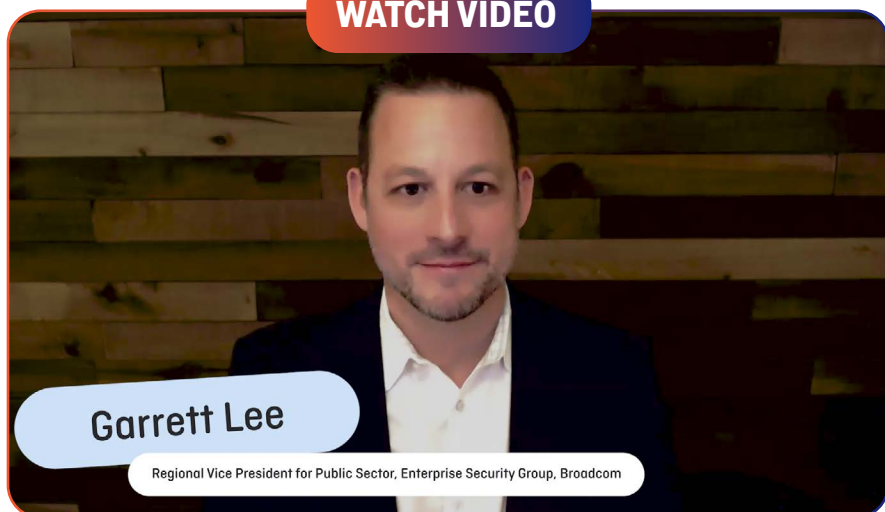
[Learn more about Ivanti.](#)

ivanti

carahsoft

The Essentials of Cloud Data Security

WATCH VIDEO



“Agencies have to comply with stringent regulations ... so that means they need a really robust [security] framework, all while managing the complexities of the cloud environment. Cloud, you know, solves some problems, but it also creates some others.”

— Garrett Lee, Broadcom

Cloud technology, for many years, enticed agencies looking for savings and efficiencies. Organizations pursued “cloud-first” policies that migrated data and applications away from onsite infrastructure and into the control, at least in part, of cloud service providers. But the cloud was too-good-to-be-true for agencies that faced cost overruns — and many did. And lately, malicious actors have gotten exceptionally good at exploiting cloud vulnerabilities.

There isn’t one way to secure your cloud platform, unfortunately. You need a holistic, zero-trust approach that combines security controls with cyber policies and procedures. Strong encryption and access rules, automated updates, clear visibility, and detailed incident response plans are all critical. Knowing who’s responsible for what should go without saying. And repatriating data — bringing it back on premises, for example — is often a commonsense answer.

In this [video interview](#), Garrett Lee, Regional Vice President for Public Sector in Broadcom’s Enterprise Security Group, explores both the opportunities that cloud computing offers and how to confront its security challenges. Topics include:

- What a holistic approach to cloud security entails
- The cost and security drivers behind data repatriation, and why they matter
- What tools agencies can use to strengthen their cloud security

ABOUT BROADCOM

The most targeted organizations in the world secure their environments with Symantec and Carbon Black, which now form the Broadcom Enterprise Security Group. Fueled by Broadcom’s commitment to R&D, the company aims to always innovate its solutions to keep you ahead of the next novel assault or sophisticated attack.

[Learn more about Broadcom.](#)



carahsoft.

Conclusion

This guide is the latest look at an ongoing shift in the cyber threats that agencies face and the technologies and tactics that can counter those threats. Be sure to check out the preceding guides:

May 2024: How to Build a Cyber-Savvy Workforce

- How One Agency Wove Zero Trust Into Its Culture
- Building a Culture of Cyber Literacy

September 2024: Government Gears Up for A Better Cyber Future

- AI's Impact on Cyber Operations
- Connecting Investments to Better Cyber Outcomes

January 2025: Agencies Accelerate Cyber Advances

- Four Key Areas of Cyber Innovations
- How NIST Fosters Deeper Engagement With Industry

ABOUT GOVLOOP

GovLoop's mission is to inspire public-sector professionals by serving as the knowledge network for government. Govloop connects more than 300,000 members, fostering cross-government collaboration, solving common problems and advancing government careers. GovLoop is headquartered in Washington, D.C., with a team of dedicated professionals who share a commitment to the public sector.

For more information about this report, please reach out to info@govloop.com.

THANK YOU

Thank you to Broadcom, Carahsoft, CrowdStrike, CyberArk, Fortinet Federal, Illumio, Ivanti, Palo Alto Networks, Qmulos and Splunk for their support of this valuable resource for public-sector professionals.

AUTHORS

John Monroe, Director of Content
Candace Thorson, Managing Editor
Lauren Walker, Senior Staff Writer

DESIGNERS

Kaitlyn Baker, Senior Creative Manager
Julia Blurton-Jones, Motion Graphics Designer



Register now to receive the next installment of our 2025 Cyber Guide Series: Winning the AI Cyber Arms Race

govloop.com
@govloop

