

The AI Cyber Arms Race Is On

Introduction

Government agencies know what they are up against. They know that malicious actors are leveraging artificial intelligence to launch a higher volume of attacks and to make attacks more targeted and harder to detect. And they know the threats will only get worse. Given the constraints on their staffing and budgets, they also know AI is essential to strengthening their cyber posture.

The good news is that cyber experts across the public and private sectors are working furiously to help agencies keep pace in the AI cyber arms race. In this guide, the third in our 2025 three-part series, we will explore recent developments that will shape security strategies in 2026 and beyond.

We begin by looking at the current state of the arms race — where experts see AI giving an edge to defenders and where malicious actors are pressing their advantage. And heads up: Agentic AI is expected to make its presence felt in a big way in the year ahead.

Next, we look at the workforce. How can agencies help their cyber workers adapt to the demands of AI? The NICE Cybersecurity Workforce Framework could provide the path forward.

This won't be the last word on the intersection of AI and cybersecurity. If anything, next year is likely to bring developments we can't yet imagine. But when that happens, we'll be here to tell you about them.

Contents

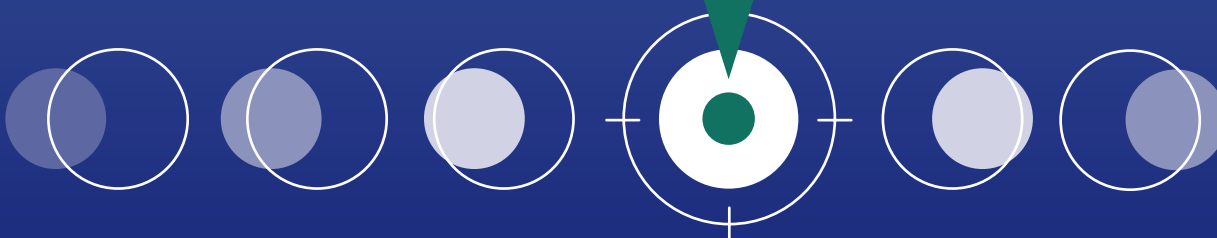
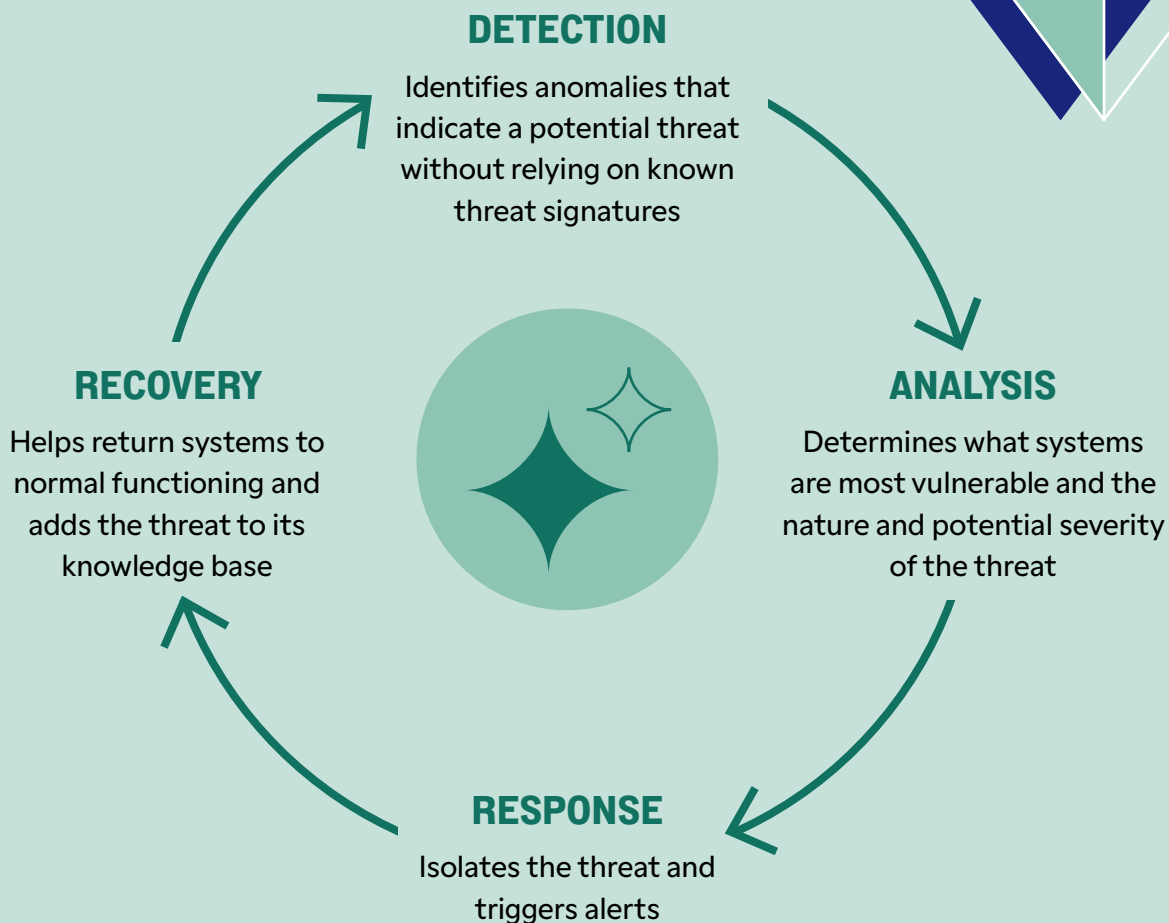
- 3 Dispatches From the AI Cyber Arms Race**
- 7 How Cyber Data Can Give You a New Edge on Malicious Actors**
- 8 How to Bring Greater Efficiency to Network and Cyber Operations**
- 9 How to Get More Value Out of CDM Cyber Data**
- 10 NICE Helps Agencies Rethink the Cyber Workforce for the AI Era**
- 13 How to Mitigate the Threat of Identity-Based Attacks**
- 14 How to Tackle Your Mobile Device Security Risks**
- 15 How Observability Fills Key Gap in Zero-Trust Architecture**
- 16 Fighting Fire With Fire: Cybersecurity in the Age of AI**
- 17 Conclusion**

Dispatches From the AI Cyber Arms Race

A look at how AI is reshaping the strategies of cyber defenders and attackers

A UBIQUITOUS DEFENSE

AI is emerging as a factor at each step of the cyber defense cycle, say experts at Syracuse University's School of Information Studies:



KEY USE CASES FOR AI-DRIVEN DEFENSES

Here is a more detailed look at the most promising use cases for AI in cybersecurity, according to experts:



Detecting external threats

Unlike traditional detection tools, AI-driven solutions get better over time at identifying threats and preventing false alerts.



Detecting internal threats

AI is expected to significantly improve behavioral analytics, which develops an understanding of individual users' normal network behavior (e.g., when people typically log in and from where, what they access, etc.) and then flags anything anomalous.



Phishing prevention

AI can catch phishing attempts by detecting indicators in network and email traffic and then analyzing the content of the email.



Protecting endpoint devices

AI should accelerate solutions' ability to detect and quarantine threats on user devices, keeping the rest of the network safe.



Optimizing access management

What access rights do users actually need? AI can study user behavior to learn which resources users typically access — and which they don't — and recommend tweaks to their permissions.

AN AGENTIC FUTURE

In time, agentic AI, which is designed to carry out complex processes with minimal human intervention, is expected to bolster cyber defenses, according to a [recent paper](#) by researchers at Oak Ridge National Laboratory.



GenAI GETS THE CALL

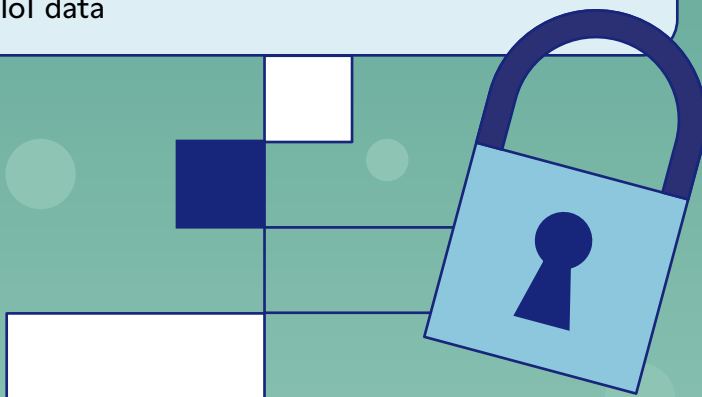
Although generative AI is unlikely to play a major role in the core cyber defense life cycle, it can still help. A paper that the Institute of Electrical and Electronics Engineers published recently highlights some [promising possibilities](#):

- + **Generating passwords** that are more difficult to crack
- + **Identifying phishing email messages** and flagging dangerous links embedded in email text
- + **Creating realistic phishing emails** for use in employee training
- + **Simulating adversarial attacks** on GenAI systems to identify potential vulnerabilities
- + **Simulating malware attacks**, based on real malware data, to test detection systems
- + **Creating fake websites and applications** (i.e., honeypots) to attract attackers so that cyber defenders can study their techniques

AI-DRIVEN CYBER THREATS

While GenAI may not be especially helpful to cybersecurity, it can play an outsized role in helping malicious actors because using it requires much less technical expertise or advanced tooling than, say, machine learning-based methods. Here are some ways GenAI could amplify cyber threats, according to ISACA, an IT professional association.

- **Social engineering:** Making phishing emails and fake websites more personal and more convincing
- **Malware:** Developing techniques that are more effective and adaptable to new defenses
- **Password cracking:** Developing algorithms that help attackers decipher passwords more effectively and quickly
- **Automated attacks:** Deploying numerous bots to detect and exploit network or system vulnerabilities
- **Data extraction:** Finding and stealing data on compromised networks
- **Ransomware attacks:** Automating the process of encrypting a target organization's files and folders
- **IoT attacks:** Detecting and exploiting vulnerabilities in Internet of Thing networks and network-attached devices (e.g., sensors, monitors and cameras), as well as compromising IoT data



A NEW CYBER CONCERN: THE SECURITY OF AI ITSELF

As AI becomes integral to so many aspects of an agency's operations, the security of those AI models becomes a mission-critical concern. Agencies need to monitor and protect their AI operations from start (gathering data and training models) to finish (ensuring model integrity). Here are the top concerns about cyber-related AI risks, according to a recent survey by McKinsey and Co.:

41% Observability (e.g., monitoring AI models)

35% AI governance

32% Sensitive-data scanning/ protection for AI models

28% Vulnerability monitoring of AI models

26% Preproduction code scanning of AI models

23% Data poisoning mitigation for AI models

FOUR STRESS POINTS WHEN BUILDING AI-DRIVEN CYBER DEFENSES

Although AI can go a long way toward strengthening cyber operations, it comes at a price. Recent research shows what challenges often catch organizations off guard:

INCREASED DEMANDS ON NETWORK/ HARDWARE INFRASTRUCTURE

As any data center operator would tell you, AI-based solutions require more computational power, processing capabilities and memory, and the bigger the model, the greater the implementation costs.

INCREASED CONCERNS ABOUT PHYSICAL SECURITY

Not every malicious actor will attack a data center through the internet. Some just break in through a back door. The risk is not just to the core hardware and software, but also to cooling systems, power backups and utility connections.

MORE COMPLEX DATA MANAGEMENT

Typical AI models require massive datasets, and that data must be high-quality, complete and error-free. Data quality has always been important, but now the stakes are higher because unreliable data translates into unreliable AI outputs.

EXACERBATED STAFFING CHALLENGES

An AI-based cybersecurity initiative is inherently a multidisciplinary affair, involving project managers and people with expertise in cybersecurity, AI and data. For organizations already struggling to staff technical experts, this can feel overwhelming. But there is an upside: Once in place, AI-based automation can ease the burden on security teams.

NEW HOPE FOR OPERATIONAL TECHNOLOGY?

Operational technology, such as industrial systems and controllers, utilities, and sensors, is a big vulnerability across government and the critical infrastructure sector. These systems are increasingly connected to the internet but often lack robust security measures. AI could help fill that gap, according to the SANS Institute. Potential uses include:

- Enhancing threat detection
- Guiding and accelerating response efforts
- Improving vulnerability management
- Helping engineers adapt to evolving cyber threats

REVISITING THE WEAKEST LINKS (I.E., US)

The market for AI-based security solutions is still taking shape, and organizations are exploring how AI might or might not help. But of all its potential benefits, perhaps the most tantalizing is this: reducing the damage resulting from simple human error.

“Whether it is a decision-based mistake, a skill-related oversight, or an error in task execution, intentional or not, eliminating the potential for human error is the initial step in establishing a well-protected cyber environment,” researchers say.

How Cyber Data Can Give You a New Edge on Malicious Actors



“For too long, cyber defenders have been operating in a world where they’ve got tools that are kind of strapped together with bubblegum and duct tape. You really have to have a proper data platform, like Cloudera’s Anywhere Cloud platform, to help those cyber defenders.”

— Carolyn Duby, Cloudera

As cyberattacks grow more sophisticated and increasingly disruptive, agencies need to level up their cyber game. In theory, data should give them an edge, improving their ability to detect and mitigate threats. Artificial intelligence can accelerate those capabilities, with agentic AI promising even greater advances.

But that whole vision hinges on agencies being able to gather, manage and analyze that data. In reality, many agencies find themselves with a wide array of tools that weren’t designed to work together. The data is there, but the experts can’t leverage it at sufficient speed or scale.

In this [video interview](#), Carolyn Duby, Field CTO and AI Strategist at Cloudera, discusses how agencies can bring better discipline to managing their cyber data and using it to strengthen their defenses.

Topics include:

- The connection between an open data platform and a security incident and event management tool (SIEM)
- An iterative approach to incorporating cyber data into your operations
- Best practices in managing a cyber data initiative

ABOUT CLOUDERA

Cloudera Government Solutions helps accelerate AI results throughout the life cycle, providing the flexibility to operate data workloads anywhere — whether on a public or private cloud, an on-premises data center, or at the Edge.

[**Learn more about Cloudera**](#)

CLOUDERA

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

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

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’s Zero-Trust architecture. Trust Fortinet Federal to safeguard your agency operations and mission-critical assets.

[Learn more about Fortinet Federal](#)

**FORTINET
FEDERAL®**

How to Get More Value Out of CDM Cyber Data

WATCH VIDEO



Matthew Shallbetter

Director of Strategy, Civilian, Armis

“This new model of cloud-first technology applied to this space is very powerful. Especially at this time when you have shrinking staffs, having the right data, the right information and the right tools is going to be really important.”

— *Matthew Shallbetter, Armis*

The Department of Homeland Security’s Continuous Diagnostics and Mitigation program, or CDM, was launched in 2012 to help agencies get better visibility into their risks and to improve their ability to detect and respond to threats. As implemented, the CDM solution has been successful in standardizing cyber risk operations and brought system owners more insight into their cyber posture. But in the ensuing years, cloud, mobility, the Internet of Things (IoT) and other technologies have led to an explosion of unmanaged devices and greatly expanded their attack surface area, and the original CDM solutions have not kept pace.

The extent of the current visibility and management gap is a serious threat to federal networks and our country. But in late 2024, DHS awarded a task order for a data services solution, which will provide a modern, cloud-based approach to harnessing CDM data.

In this [video interview](#), Matthew Shallbetter, Director of Strategy for Civilian at Armis, which is a subcontractor on the task order, explains how this new approach to data could reshape cyber efforts. Topics include:

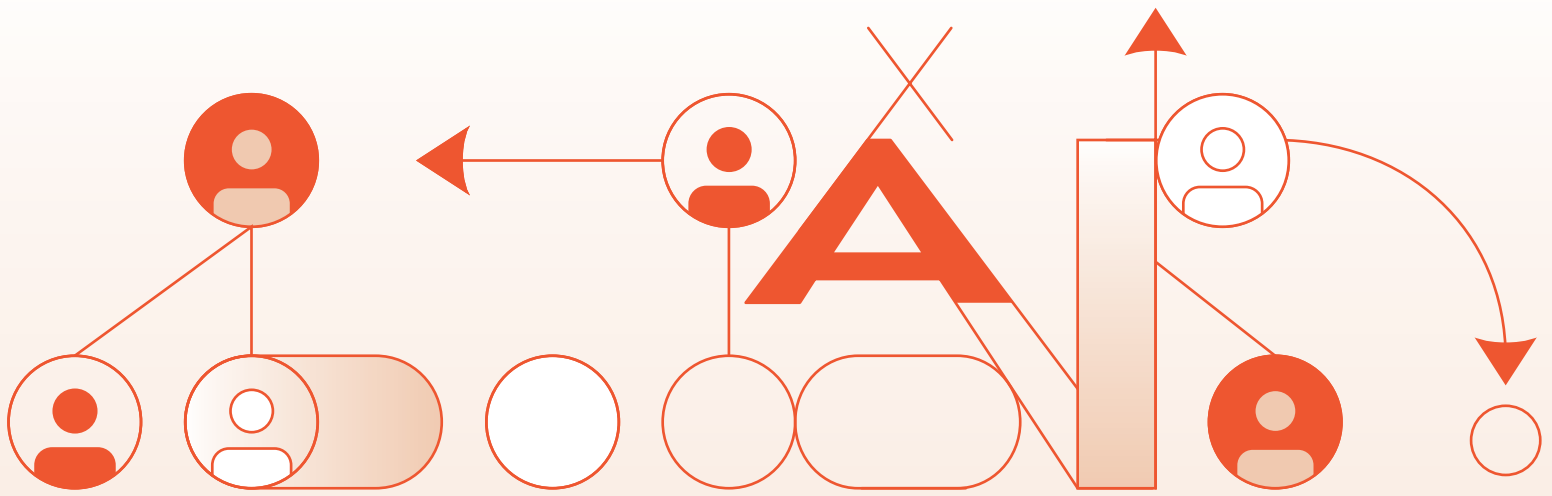
- Governing data from the data center to the edge
- Gaining better visibility into the IT environment through AI and machine learning
- Turning cyber data into actionable insights

ABOUT ARMIS FEDERAL

Armis Federal empowers U.S. government agencies and Tribal Nations to continuously see, protect, and manage all critical assets — from the ground to the cloud. Its cyber exposure management platform, Armis Centrix™, is FedRAMP- and DISA IL-authorized and helps agencies protect their entire attack surface and manage cyber risk exposure in real time.

[Learn more about Armis Federal](#)





NICE Helps Agencies Rethink the Cyber Workforce for the AI Era

The NICE Cybersecurity Workforce Framework, spearheaded by the National Institute of Standards and Technology (NIST), is one of those initiatives that will never be complete — and that’s a good thing.

The goal of the framework, which is under the purview of the National Initiative for Cybersecurity Education program, is straightforward: **to provide a standard approach and common language for describing cybersecurity work and cyber workers.** Organizations across the public and private sectors use the framework to assess their cyber workforces and shape recruiting and training strategies.

The challenge is that cybersecurity work is constantly evolving. AI is a recent case in point: It can strengthen cybersecurity in myriad ways, but only if cybersecurity workers have the necessary skills. Other emerging issues include quantum computing, operational technology (e.g., industrial systems) and supply chain security.

“So, we’re really trying to make certain that we are regularly adjusting for change, regularly making improvements, both to its content and how it can be applied,” said Karen Wetzel, Lead of the NICE Workforce Framework for Cybersecurity at NIST.

A WORK IN PROGRESS

The idea for the framework dates to 2007, when the U.S. Department of Homeland Security proposed creating the IT Security Essential Body of Knowledge, or EBK. First, the U.S. Federal CIO Council, then the NICE program office, took up stewardship of the framework.

Using the framework, as described in NIST Special Publication 800-181, agencies define cybersecurity work by writing task, knowledge and skill (TKS) statements. Each statement includes:

- **Task:** An activity that supports organizational objectives, such as conducting security reviews
- **Knowledge:** Information and concepts that a worker needs to retain, such as sources of vulnerability, to complete a task
- **Skill:** A worker’s capacity to perform a task, such as skill in patching system vulnerabilities

But cybersecurity is not that simple. In many organizations, some cybersecurity tasks are carried out by individuals who don't have cybersecurity jobs. Organizations need to map out those responsibilities and ensure that those workers can carry out those tasks. With that in mind, NICE has developed three additional framework components:

- **Work roles:** A grouping of tasks for which someone is responsible, such as database administration or incident response (work roles are not necessarily synonymous with specific job titles or occupations)
- **Work role categories:** A high-level grouping of common cybersecurity functions, such as oversight and governance or design and development
- **Competency areas:** Clusters of related knowledge and skill statements that correlate with one's capability to perform tasks in a particular domain, such as cyber resiliency or AI cybersecurity

Agencies can use the framework to more closely align their workforce development programs with their current and emerging cybersecurity requirements, Wetzel said. Indeed, NICE works closely with the entire cyber workforce ecosystem, from education and training organizations to employers, to support that alignment.

"We're seeing [the framework's] use in career discovery for education and training, in hiring and workforce management, in career planning and development," she said, "so, really across all of the different stakeholders and everything that happens in the workforce."

THE NICE CYBERSECURITY WORKFORCE FRAMEWORK: A HISTORY

- **2007**
DHS develops the IT Security Essential Body of Knowledge (EBK) as a way to define and assess the federal cybersecurity workforce.
- **2008**
The Federal CIO Council decides to build a standard framework that expands on the EBK, later expanding its work to include the private sector.
- **2012**
The council publishes the first version of its framework.
- **2013**
NICE takes on the work of further developing the framework.
- **2015**
The Federal Cybersecurity Workforce Assessment Act of December 2015 directs the federal government to use the framework to support cyber workforce planning.
- **2017**
NIST publishes the third version of the framework as Special Publication 800-181.
- **2024**
NICE publishes Version 1 of the NICE Framework Components, which includes work roles, work role categories and the first competency areas.



THE AI PIVOT

The growing adoption of AI has added new urgency to cyber workforce planning.

As agencies deploy AI, they “need to ensure that individuals across an organization have the skills and knowledge needed to create key innovations, take advantage of these new opportunities, and to secure organizational data and systems to mitigate and minimize organizational risks,” Wetzel said.

To support these efforts, NICE is working with its partners to apply the framework to the strategic and workforce implications of AI. A big part of this is the new **AI Security Competency Area**, which covers a foundational set of knowledge and skills that can help agencies both use AI securely and leverage it to improve cybersecurity work. In developing the content, NICE drew heavily on the NIST AI Risk Management Framework, in addition to the [Department of Defense Cyber Workforce Framework](#), the National Science Foundation’s [AI Scholarship for Service initiative](#) and other resources.

NICE is also updating the **work roles** and their associated tasks to reflect AI’s impact. For example, in the case of incident response, how are the tasks changing, and what knowledge and skills are needed to support the new approach?

The goal of this work, said Wetzel, is not to create a new AI-specific framework but to build on the existing framework to help organizations understand the ramifications of AI for their cyber workforce. “And that, hopefully, will make it easier for organizations to start shifting in this direction,” she said.

MORE TO COME

Although AI is dominating the cyber field now, the NICE team is already looking ahead to future disruptions, such as quantum, which will bring its own challenges. But NICE’s basic approach will be the same, working with its partners in the cybersecurity workforce ecosystem to strengthen talent acquisition and workforce management practices.

“Technology is always evolving, and this is just another shift,” Wetzel said. “It’s a massive one, but it’s one that we’re addressing through being able to be more responsive to some of these changes.”

How to Mitigate the Threat of Identity-Based Attacks

WATCH VIDEO



Cristian Rodriguez

Field Chief Technology Officer for the Americas, 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 legitimacy of 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

“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

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](#)



How to Tackle Your Mobile Device Security Risks

WATCH VIDEO



Michael Riemer

SVP Network Security Group and Field CISO, 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 endpoints 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 endpoints 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 endpoints

“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

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.

How Observability Fills Key Gap in Zero-Trust Architecture

WATCH VIDEO



Brian Chamberlain

Head of Business Development, SolarWinds Federal

Travis Galloway

Senior Advisor for Government Affairs, SolarWinds

“Observability is a key component of a greater zero-trust architecture, because it’s the platform that provides visibility and analytics into the entire IT environment.”

— Brian Chamberlain,
SolarWinds Federal

The concept of zero-trust architecture has been around for a long time, yet many agencies still struggle to put it into practice. The problem is that ZTA is not a specific solution but a system-of-systems approach to securing the network environment. And that environment is complex, encompassing both advanced cloud solutions and aging legacy technology. When it comes to aligning their systems with the pillars of ZTA, the pieces just don’t fit together.

What’s missing is observability. ZTA is based on the assumption that the network has already been breached and that the task is to contain and mitigate that threat. To do so, agencies need to look across the network environment and identify and diagnose issues, as well as anticipate future problems and optimize performance. That’s what observability provides.

In this [video interview](#), Brian Chamberlain, Business Development Manager at SolarWinds Federal, and Travis Galloway, Senior Advisor for Government Affairs at SolarWinds, discuss how observability and related capabilities can help agencies make progress on ZTA. Topics include:

- The critical differences between network monitoring and observability
- Best practices in modernizing with observability in mind
- The principles of a Secure by Design approach

ABOUT SOLARWINDS

SolarWinds provides simple, powerful, and secure IT management software to customers worldwide, including virtually all civilian agencies and branches of the military. Its products are easy to buy, install, use, scale, and maintain, and provide the power to resolve your toughest IT management problems.

[Learn More about SolarWinds](#)



carahsoft.

Fighting Fire With Fire: Cybersecurity in the Age of AI

WATCH VIDEO



“Where things like optimization, efficiency, resource constraints, or resources are at a premium ... the more that we can address [cybersecurity] systems and operations through automation, the better.”

— Bart Larango, Splunk

Artificial intelligence is the double-edged sword of cybersecurity, both raising the risks and providing new and more effective defenses. As the majority of adversaries are now organized, industrialized and backed by nation-states, attacks have grown too sophisticated for people to combat unassisted.

Automation and AI can improve your odds in the fight. AI can recognize anomalies far more quickly and effectively than any human, helping you keep up with the pace of incursions. Automating time-consuming basic tasks, such as installing updates and applying patches, frees up employees to focus on more complex cyber issues.

In this [video interview](#), Bart Larango, Strategic Industry Advisor, Federal, at Splunk, and Michael Saintcross, Senior Vice President of Revenue for Optiv + Clearshark, discuss the impact of AI and automation on cybersecurity. Topics include:

- How AI is changing the threat landscape.
- Why humans remain both a critical vulnerability and an essential safeguard.
- How automation and AI improve cybersecurity response.

ABOUT SPLUNK

Splunk, the cybersecurity and observability leader, helps build a safer and more resilient digital world. Organizations trust Splunk to prevent security, infrastructure and application incidents from becoming major issues, remediate threats and disruptions faster, and adapt quickly to new opportunities.

[Learn more about Splunk](#)

ABOUT OPTIV + CLEARSHARK

Optiv + ClearShark is a new federal powerhouse, with added resources, capabilities and value-added services that serve as a force multiplier for driving cybersecurity and IT adoption in the federal government.

[Learn more about Optiv + ClearShark](#)

Conclusion

To catch up on all the cybersecurity developments in 2025, check out the first two parts of our 2025 Cyber Guide series:

January 2025: Agencies Accelerate Cyber Advances

→ Topics include public-private partnerships in cyber innovations and recent advances in such areas as incident response and software bills of material.

June 2025: Focus on Cyber Force Multipliers

→ Topics include strategies for boosting cyber efficiency and emerging cyber priorities for government agencies.

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 Armis Federal, Carahsoft, Cloudera, CrowdStrike, Ivanti, Fortinet Federal, Optiv + Clearshark, SolarWinds 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
Kelly Boyer, Motion Graphics Team Lead



**Look for our first 2026
Cyber Guide in February!**

govloop.com
@govloop