FEDInsider

DOD Is Meeting Cyber Threats Head-On

Department of Defense agencies are adopting zero trust, commercial-based technologies and modernizing IT to meet evolving cyber threats.

As the cyber threat landscape constantly evolves, bad actors grow in numbers and become increasingly sophisticated in their tactics and techniques. To prevent, detect and thwart emerging threats, the Pentagon is steadfast in its efforts to implement a zero trust strategy to protect the nation's most critical systems.

Thought leaders from military agencies and industry spoke at a **recent series of FedInsider webinars** to discuss implementation progress, cybersecurity challenges and best practices for dealing with challenges to critical infrastructure.

Modernizing the DOD for Resiliency

Accelerating and modernizing technology is a critical component of meeting cybersecurity strategies. For example, the Army's "Knights Watch" campaign, named in honor of the West Point Black Knights, is a program designed to quickly deliver a unified network for the Army based on zero trust principles. The challenge, said Maj. Gen. Jan C. Norris, cybersecurity director and chief information security officer in the Office of the CISO for the U.S. Army, is pivoting a large existing global infrastructure to a zero trust solution.

"We've got to take our existing infrastructure, migrate that, while we're also migrating tools and services to the commercial cloud," he said. The Army is starting with federating and integrating identity, credential and access management tools. "This is a foundational concept within the zero trust framework."

The Air Force is tackling similar short-term goals, focusing on identity, credential and access management (ICAM), plus endpoint management as it pertains to the DOD's objectives in the zero trust strategy. Yet, the next step for the Air Force is local area network functionality, according to Aaron Bishop, Air Force CISO. Today, the Air Force oversees 150 global bases, but those bases may turn into expedition bases in the future. And because the Air Force relies on data, it must understand its networks.

"How do I get the data I need, at the place I need, at the time I choose and be able to do that securely through zero trust modalities – and be able to do that fast and effectively in order to meet operational requirements?" Bishop asked.

Securing such a dynamic environment like the DOD requires identity, redefining access and minimizing privilege, and lateral communication within the network. Modernizing with software can help, especially when it comes to visibility, said Patrick Sullivan, chief technology officer of security strategy at Akamai. "Ideally, you get yourself to zero trust where you understand every request and every flow and only those that are explicitly allowed are permitted," he said. "You want to be able to ensure that you have very strong visibility and

Featured Experts:

- **Randy Wood**
  Senior Vice President, North American Sales, Akamai

- **MG Jan C. Norris**
  Cybersecurity Director & CISO, Office of the CISO, U.S. Army

- **Aaron Bishop**
  CISO, U.S. Air Force

- **Patrick Sullivan**
  Chief Technology Officer, Security Strategy, Akamai

- **Maj. Cory Dombrowski**
  Army Functional Mgmt. Office, Zero Trust, Army Cyber Command

- **Rob Gordon**
  Director of Engineering, Akamai

- **COL Joseph Pishock**
  Director, Global Networks & Services, U.S. Special Operations Command J63

- **COL William Uhrig**
  Offensive & Defensive Cyberspace Operations Chief, U.S. Special Operations Command

- **Jeffrey Lush**
  Chief Information Officer, Air University, U.S. Air Force

- **Brian Dennis**
  Principal Technologist, Public Sector, Akamai

carahsoft | Akamai

proactive monitoring so that if you need to give some latitude to your operators, you're not doing so by generating additional risk."

Extending Zero Trust to the Edge

Computing from the edge has changed how agencies look at protecting data while implementing zero trust. Maj. Cory Dombrowski of the Army Functional Management Office for Zero Trust in the Army Cyber Command said this starts by identifying the users at the edge, which "will enable us to provide them the data that they need at the edge. If we don't do that effectively, we're not going to be able to authenticate users correctly, and we're not going to be able to make sure that they get the data they need."

Making sure users are only able to see what they need to do their jobs is critical to implementing a zero trust environment, and to the DOD's zero trust strategy. It's also about knowing everything about a transaction – who is making it, where they're coming from, and whether the endpoint they're using is trusted. This will make data and systems available securely, according to Rob Gordon, director of engineering at Akamai.

"The way that we do that is by using all of that to make intelligent, risk-based decisions," Gordon said. "If I'm coming from an untrusted network, that doesn't mean I can't access the systems, it means that the other burdens of access that I need to be able to prove in order to show that I should be able to access that system are higher."

ICAM and network visibility are applied to the risk score, so if a user is coming from an untrusted network but is a securely authenticated user from a vetted, known endpoint device that is managed and secured, they can access the data they need. This, however, requires keeping up with technology at the same pace as cyber threats are evolving – and adopting dynamic, rule-based configurable tools.

Cybersecurity Tools of Today & Tomorrow

Software-defined segmentation is being explored to provide granular control over a network, enabling segmentation based on data sensitivity levels, device types and user roles. "By limiting the access to these specific resources and devices, only authorized users will have access; cybercriminals are then forced to hack into multiple segments within the environment making it more difficult to move laterally across the network," said Jeffrey Lush, CIO of Air University.

This is critical to the resiliency and recoverability of defense-based networks. Col. Joseph Pishock, director of global networks and services for U.S. Special Operations Command in J63, said that starts with understanding what the network looks like, then adopting tools to protect it.

"J6 is really focusing on figuring out what we actually look like, eliminating what we can and placing resiliency inside of our own data centers," Pishock said. Once J6 knows what needs to be locked, removed or discovered within the infrastructure, it can pursue the services and tools it needs and restore routes.

Network visibility is also the start of building resiliency, said Col. William Uhrig, offensive and defensive cyberspace operations chief for U.S. Special Operations Command. "If you do not know what communication is allowed, it becomes very difficult to determine if something is nefarious or not," Uhrig said. "It has an incredible impact on the cybersecurity posture."

Secure access service edge technology can also come into play here. Brian Dennis, principal technologist for the public sector at Akamai, said SASE can provide consistent, flexible security that can keep up with evolving threats. "If there are multiple appliances spread throughout the castle [network], that are running services all at once, what a SASE network can do is really break down that appliance sprawl. You're replacing that with a single software stack that can really reduce those capital expenditures and operating expenditures," Dennis said.

The DOD also receives support from the DOD Cyber Crime Center, and unifying efforts cross-industry is critical. "Our strategy for the next two to four years is what we call purposeful partnerships...engaging in a complimentary way to other components of the Department of Defense and the U.S. government as well as the private sector," said Dr. Jude Sunderbruch, executive director of DC3. "We want to work responsibly with the leadership of the Department of Defense, other leaders in federal cybersecurity and really do everything we can to focus our efforts in a way that brings maximum value to the department."

Hosky Communications Inc.
3811 Massachusetts Avenue, NW
Washington, DC 20016

(202) 237-0300
Info@FedInsider.com
FedInsider.com
Facebook.com/FedInsiderNews
Linkedin.com/company/FedInsider
@FedInsider

Carahsoft
11493 Sunset Hills Road, Suite 100
Reston, VA 20190

(703) 871-8548
Info@Carahsoft.com
Carahsoft.com/Akamai
Facebook.com/Carahsoft
Linkedin.com/company/Carahsoft
@Carahsoft

Akamai Technologies
11111 Sunset Hills Road, Suite 250
Reston, VA 20190

(617) 444-3000
Info@Akamai.com
Akamai.com
@AkamaiTechnologies
Linkedin.com/company/Akamai-Technologies
@Akamai