FEDInsider

Zero Trust Segmentation Is Strengthening Cyber Resilience Across Government

State leaders discuss containing threats, improving visibility and adapting security strategies as AI and cloud environments expand the attack surface.

The rising adoption of generative AI and cloud environments is transforming state and local government IT, but it is also widening attack surfaces and accelerating cyber risk. Traditional security tools are struggling to keep pace as adversaries leverage artificial intelligence. In response, agencies are shifting their focus from prevention to resilience. Zero trust segmentation is emerging as a critical layer of defense, enabling greater visibility into east-west traffic, enforcing identity-based controls and containing threats through microsegmentation and encryption.

During a recent **FedInsider webinar**, state and local government and industry experts shared how they are applying these tools to protect mission-critical assets, strengthen compliance, reduce costs and more.

An Evolving Security Approach for a Changing Threat Environment

"Our environment is changing so much faster than the traditional security models were designed to handle," said Assistant Commissioner and Chief Information Security Officer for the State of Minnesota John Israel.

Infrastructure and data used to be managed onsite or in data centers – in other words, secure facilities with little exposure to direct attacks. As the world evolved and transitioned to internet services, public-facing opportunities, cloud environments, software vendors, outsourced programs and AI-powered environments, traditional network perimeters disappeared.

"We have moved away from the castle-and-moat level of defense to where our critical data can be distributed across vast networks across many different providers," Israel added.

Attackers are also shifting their tactics. They're using automation and AI to scale phishing attacks and exploit vulnerabilities faster. Israel said they're targeting identities more than infrastructure, and legacy security tools meant to protect devices rather than networks are no longer cutting it.

Identity, data and cloud workloads have become targets, so government is shifting to a risk-based approach rooted in zero trust principles. This means that rather than trusting everything in the network, assume there's a breach and have processes in place to validate users, devices and access continuously. This can minimize the blast radius in the event of an attack.

That's where zero trust segmentation comes in. "To be effective, you have to contain," said the CISO for the North Carolina Department of IT Bernice Russell-Bond. "It is very important that you can see that the compromise — the lateral movement — has been really contained and is not able to move outside that segment." This way, security teams can focus on remediation by quickly identifying the indicators of compromise, updating rules impacting other segments within the environment and applying lessons learned to harden the environment in the future.

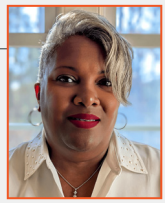
The Unexpected Benefits of Zero Trust Segmentation

Along with security, zero trust segmentation yields several benefits to users. For the State of Tennessee, one of those benefits is compliance readiness. "We touch a lot of federal data...and all those come with audits, so compliance is a big thing for us," said the Domain Information Security Officer for the Tennessee Department of Finance and Administration Brendan Taylor.

"Being able to show the way we have implemented zero trust, it automatically checks so many boxes... you get such a leg up on answering those audit compliance questions, instead of going to a bunch of different tools to show proof and evidence."

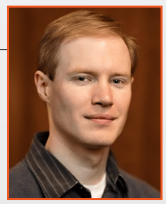
Featured Experts:

- **Bernice Bond**
  Chief Information Security Officer, North Carolina Dept. of Information Technology



- **John Israel**
  Assistant Commissioner & Chief Information Security Officer, State of Minnesota

- **Brendan Taylor**
  Domain Information Security Officer, Tennessee Department of Finance & Administration



- **Mark Gardner**
  Director of National State, Local & Education (SLED) Sales, Illumio

illumio | carahsoft

Visibility of applications, systems and how users communicate is another benefit — and has traditionally been a challenge for SLED agencies, said the Director of National SLED Sales at Illumio Mark Gardner.

"A lot of these SLED entities I've worked with have grown organically over decades, which has resulted in complex, flat networks without the ability to see a lot of the undocumented connections," Gardner added.

The first step is gaining a clear picture of how applications and workloads interact by mapping their dependencies and communication flows across the environment. This visibility helps define trusted, least-privilege pathways while also uncovering unknown connections and potential lateral movement paths that may have gone undetected.

With a better understanding of how systems truly communicate, agencies can make security decisions based on real behavior rather than assumptions. This is especially critical as attackers increasingly use AI and automation to quickly identify and exploit vulnerabilities.

According to Gardner, "Visibility is no longer optional; it is a key component of the five-step zero trust process. The central concept is to look at the workload and application-level dependencies."

Protecting Critical Assets in a Complex Environment

Encryption plays a critical role in protecting precious assets. In Minnesota, Israel said they're taking a risk-based approach by prioritizing encryption everywhere possible while still balancing operational priorities. "There are always trade-offs in security controls, whether it's performance of the system or application compatibility, complexity or cost," Israel explained, "and the intent is to focus those resources and capabilities where we actually have sensitive data."

Managing that encryption can be complex. Encrypting data and traffic between all systems can be costly, so users must manage the certificate lifecycle effectively. "We need to know what we have to best protect it," Israel said.

Knowing your assets, the rules applicable to those assets and the identities associated with them will allow IT teams to secure them more efficiently, and in a tailored approach.

While organizations continue strengthening encryption, they must also prepare for the long-term implications of quantum computing. Although practical quantum computers capable of breaking today's widely used public-key encryption are not yet available, security leaders are planning for the possibility that adversaries are already collecting encrypted data with the expectation that future quantum capabilities could eventually decrypt it. This strategy is commonly known as "harvest now, decrypt later."

That makes zero trust even more important. Zero trust assumes that attackers may eventually gain a foothold and focuses on limiting what they can reach through continuous verification, least privilege access and network segmentation. By preventing unauthorized access to sensitive information in the first place, agencies can significantly reduce the amount of valuable data available to attackers, both today and in a future shaped by quantum computing. Combined with a transition to post-quantum cryptography, zero trust provides an important layer of defense against evolving threats.

This also rings true for visibility into east-west network traffic. Traditional security architecture was built to monitor north-south traffic, but as systems became increasingly complex, those walls expanded and securing them became more challenging.

According to Gardner, organizations were left with limited visibility into communications between internal systems. Today, they might have extensive visibility at the perimeter of their network, but limited visibility into the communications occurring within it.

"The way to address this is by focusing on workload-level telemetry and application dependency mapping, rather than relying solely on network infrastructure," Gardner said. This provides a more accurate view of reliable data because networks are not static. Every time a change is made to the network, a lateral path can be created, so focusing on workload and application-level dependencies gives a more accurate view of where unnecessary risk exists.

The Here and Now of Addressing an Evolving Threat Landscape

Emerging technology is being used to enhance cybersecurity. AI can exploit vulnerabilities much faster than humans, and given the increasing sophistication of attackers, organizations should shift to an "assume-the-breach" mindset. One key to keeping data safe in this new AI saturated environment, according to Gardner, is to use workload and application-level dependency microsegmentation instead of more traditional network-centric solutions that are more vulnerable to attacks using frontier AI.

Zero trust segmentation is also helping IT teams contain lateral movement during an attack. "Segmentation plays a key part in making sure that essential services are kept online because it allows me to put in some rules that may be related to quality of service," Russell-Bond said. "It really allows you to customize and update who has access and the flow of traffic at times when you're dealing with a crisis."

When an attack comes into a zero trust-protected environment, being able to address the most critical data and systems first is key, Taylor added. This significantly improves response time. "By only allowing the things you need, the volume of logs goes down substantially, your SIEM [Security Information and Event Management] platforms will run better, your alerts will run more efficiently and the people on the ground solving the problem don't have to sift through tens of millions of logs," Taylor said.

"Cyber is no longer an IT function as we adopt all these cloud services and generative AI. It has to become part of every technology and business decision from the start," Israel added. Attacks are bound to happen in today's changing threat environment, so containing the blast radius is more important than ever. And zero trust is a key way to accomplish that critical task.

FEDInsider

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

illumio

Illumio
920 De Guigne Drive
Sunnyvale, CA 94085

(669) 800-5000
Sales@Illumio.com
Illumio.com
Facebook.com/Illumio
Linkedin.com/company/Illumio
@Illumio

carahsoft

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

(703) 871-8500
Info@Carahsoft.com
Carahsoft.com
Facebook.com/Carahsoft
Linkedin.com/company/Carahsoft
@Carahsoft