FEDInsider

Strengthening Your Network Security: Balancing Outer & Inner Defenses

As cyber threats rise in size and sophistication, agencies are looking to zero trust to protect data and reduce the attack surface.

In 2022, the White House released a federal zero trust architecture strategy, requiring agencies to meet certain cybersecurity standards by the end of FY 2024 to secure federal networks from increasingly sophisticated threats. These cyber practices include microsegmentation, a method intended to reduce the attack surface and stop cyberattacks from permeating through an entire network.

Enhancing cyber hygiene with zero trust and microsegmentation will provide agencies with real-time visibility into application activity and catch anomalies. Members of government and industry recently spoke at a **FedInsider panel** to discuss adopting these cyber practices and the role that zero trust and microsegmentation plays in securing government networks.

INTRODUCING MICROSEGMENTATION TO GOVERNMENT

"Zero trust is actually a godsend for us, and it's pushing the need for more microsegmentation," said Rob Thorne, chief technology security officer for U.S. Immigration and Customs Enforcement. According to Thorne, the benefit of microsegmentation versus network segmentation is that it moderates lateral traffic between network services, giving agencies greater and more holistic visibility into network activity. Security perimeters can even be put around each server in network segments, reducing lateral movements and shrinking the attack surface.

"I think that in government, we have always done a really good job of network segmentation, but what we haven't done is gone down to that next level of microsegmentation," Thorne said. When agencies begin mapping out their zero trust strategy, microsegmentation should be a part of the conversation – especially considering the techniques and behaviors of current bad actors and recent breaches.

Plus, IT systems supporting federal agencies are inherently at risk. They're complex, dynamic and geographically dispersed, Thorne said. They are also federated, even more now that the shift to remote work prompted by the pandemic still has many federal workers teleworking.

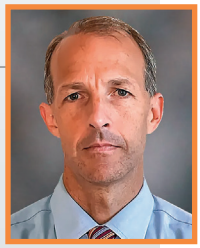
"It really has become increasingly more difficult for our agencies to protect our networks, systems and resources using the traditional perimeter security strategy," said Jennifer Franks, director of the Information Technology and Cybersecurity Team at the U.S. Government Accountability Office.

This is why it is critical that agencies look at microsegmentation as a strategy for reducing that attack surface, securing past the perimeter level and broadening enterprise-wide network efforts. "Providing an opportunity to restrict lateral movement involves the IT environment and the threat actors that could be maliciously impacting our environment. That is what is happening with the cybersecurity incident or data breaches that are impacting us," Franks added.

Featured Experts:

- **Jennifer Franks**
  Director, IT & CS Team,
  U.S. GAO

- **Rob Thorne**
  Chief Information Security Officer,
  U.S. Immigration & Customs Enforcement



- **Gary Barlet**
  Federal Chief Technology Officer,
  Illumio

VISIBILITY IS KEY

As enterprises are becoming more and more spread out, applications are sprawling. Agencies must see how applications are communicating, and what they're interacting with to properly secure an enterprise.

illumio

To discover vulnerabilities, Gary Barlet, federal chief technology officer at Illumio, uses a tool that creates a map of applications that displays the individual pieces of each application, what is in use, how they are communicating and who is accessing what.

This type of visibility can't be done in a traditional way for today's complex environments. "Ideally, it is done in a way that is easy for humans to consume, and we encourage the use of label-based monitoring and label-based rulesets so you can track things in a way that humans can consume and understand," Barlet said. "Having a map to visualize that is absolutely crucial."

Visibility is the first step in identifying vulnerabilities or threats in a network. "You have to acknowledge a problem before you can actually fix it. You have to be able to see the problem and see what you are dealing with and how to address it afterward," Barlet said.

EARLY STAGES OF ADOPTION

There are five pillars to zero trust: Identity, device, network/environment, application workload and data. When done correctly, adopting zero trust means layering security so that if an attacker reaches the network level, microsegmentation protects the next layer. It's important to take adoption pillar by pillar.

So, Thorne said agencies are beginning to invest in microsegmentation and look at the tools and programs they can put in place to isolate access to applications on a "need to" basis. "Organizations don't know what apps are talking to what apps and who is accessing what, and that is very important. I think you are going to see a lot of investments in this area. I believe if you are not, then you are not looking in the right areas," he said.

Considering federal funding processes, knowing what to invest in requires looking at the technology services an agency already has in-house and leveraging existing opportunities and resources before buying additional tools.

"But additional resources are often needed, and the advancements of technologies that are often needed are outside of the appropriations cycle," Franks said. "We are going to have to be proactive in thinking ahead of what we will need to do to really stay ahead of the curve."

To meet the 2024 zero trust requirements within federal budget cycles, agencies must properly assess resources and make the appropriate investments in those zero trust pillars. Modernization funds are provided, but it is each agency's responsibility to be creative with existing funds.

ZERO TRUST AND MICROSEGMENTATION BEST PRACTICES

Cyberattack attempts will happen regardless of what security measures are in place – and occasionally, they'll breach. The use of microsegmentation in environments is not a silver bullet to reducing attack surfaces, but it is one of the many layers that agencies can employ to improve cybersecurity protections.

The proper zero trust architecture is also dependent on agency business needs, but lateral movement tactics are highly used by threat actors. So, Franks recommends starting by limiting those lateral movements with microsegmentation, because it's a clear risk to agencies. Then, start thinking of authentication procedures at a greater level.

"Organizations can drive policies and procedures around this in a manner that moves that implicit trust for users on the network and devices that commonly have had more traditional style perimeter security," Franks said.

Yet the most important thing is getting started. Start with the five pillars, find the biggest risks in the organization's network, begin at the application level and then layer defenses. Having the right security in place is the difference between responding to a minor breach and needing to recover from a full-out disaster.

"If you are breached, part of the response you want is to be able to continue your operations and still be able to shut down segments," said Thorne. "That is the goal, and [with] microsegmentation, you can achieve a lot of those continuing operations."

FEDInsider

Hosky Communications Inc.
3811 Massachusetts Avenue, NW
Washington, DC 20016
Contact: **John Hosky**

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

illumio

Illumio, Inc
920 De Guigne Drive
Sunnyvale CA 94085
Contact: **Nestor Kassaraba**

(301) 335-8480
Federalsales@illumio.com
www.illumio.com
Facebook.com/illumio
Linkedin.com/company/illumio
@illumio