FEDInsider

Government Is Implementing Zero Trust for a More Secure Future

Federal agencies are working with the private sector to meet Zero Trust mandates while modernizing legacy systems.

The Office of Management and Budget issued its federal Zero Trust architecture strategy nearly two years ago, outlining specific goals for agencies to reach by the end of fiscal year 2024. Not only will a Zero Trust framework help agencies stop data breaches, but it will also modernize and enhance traditional network designs.

While agencies remain at different stages of their adoption journeys, thought leaders from government and industry spoke at a recent FedInsider webinar to discuss their experiences implementing a Zero Trust framework and what they've learned so far.

THE BENEFITS OF ZERO TRUST

Adopting Zero Trust will help agencies protect their networks, and starting with high-value assets is key for those looking for ways to begin that transition. "Start with defining the Protect Surface, which is kind of the inversion of the old attack surface concept, and then you map the transaction flows in order to move towards Zero Trust. You need to understand how everything works as a system, and then you can architect the technology," said John Kindervag, chief evangelist at Illumio.

Because of all the requirements and mandates for systems operating within government, compliance can sometimes seem like security, but that is not necessarily the case. Zero Trust, however, allows agencies to "become secure as well as compliant," Kindervag said. He added that because of the state of modernization projects within government and the continued need to secure legacy systems, for many agencies moving to Zero Trust means really having to rethink their entire security posture and mindset.

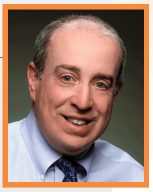
It's about appropriately designating what agencies are trying to protect, rather than trying to protect everything by a single, legacy system like a firewall, said Federal Zero Trust Architect and TIC 3.0 Program Manager at CISA Sean Connelly. And as agencies implement Zero Trust and modernize in general, they'll also find business modernization advantages.

As an alternate board member of the Technology Modernization Fund – an investment program for federal technology modernization projects – Connelly noted that several agencies recently awarded funds for projects that combined Zero Trust with business modernization, something that can be seamless if done right. Some examples Connelly noted included a program to help farmers complete forms faster, one that assisted an agency in building online records to improve customers' importing and exporting services, and one that helped veterans and their families to electronically request service records so they could access their benefits. "Each of those proposals, embedded in them, were cybersecurity Zero Trust principles," Connelly said.

Featured Experts:

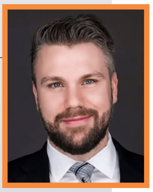
- **La Monte Yarborough**
  Acting DCIO, CISO & Executive Director, Office of Information Security, HHS

- **Dr. Robert Roser**
  Chief Information Security Officer, Idaho National Laboratory



- **Sean Connelly**
  Federal Zero Trust Architect, CISA

- **Robert Wood**
  Chief Information Security Officer, Centers for Medicare & Medicaid Services



- **John Kindervag**
  Chief Evangelist, Illumio

OVERCOMING ZERO TRUST ADOPTION CHALLENGES IN GOVERNMENT

For an agency as large as the Department of Health and Human Services, meeting Zero Trust mandates have their own challenges. "We continue to establish clear governance processes and measures that hopefully outline our roles and responsibilities in the decision-making processes related to the Zero Trust implementation," said La Monte Yarborough, acting deputy chief information officer, chief information security officer and executive director in the Office of Information Security for HHS.

That requires collaboration with representatives from all participating agencies, and assures alignment and accountability for HHS' discrete and collective activities. "Collaborative efforts are critical to developing standard Zero Trust policies, procedures and guidelines," Yarborough added. That collaboration helps HHS to ensure Zero Trust principles are embedded in all aspects of agency operations.

This collaborative approach of sharing best practices and lessons learned fosters a culture of knowledge sharing, too, which can accelerate the adoption and integration of Zero Trust principles. "Training promotes a unified understanding approach to Zero Trust as we align our technology strategies and engage in joint assessments and monitoring efforts to hopefully evaluate the effectiveness of Zero Trust measures across settings," Yarborough said.

For Robert Wood, chief information security officer for the Centers for Medicare and Medicaid Services (CMS), implementing Zero Trust means doing so in stages. "You need to look at the different elements of it," he said. "You can't really work on data security or application workloads and identity at the same time, because you're probably not going to address it with the same people, technologies, policy or process changes."

Due to the federated environment of CMS, there are different pockets of self-managed IT infrastructures or applications. Some parts of the agency are heavily leveraging centralized IT resources, while others are not. And nobody is mandated to use or consume any of the centrally managed IT resources, which can make Zero Trust decisions more complicated for large and complex government agencies like CMS.

"There's a lot of choose-your-own-adventure type of self-managed tech decisions that can end up getting made," Wood said. "And inevitably, it makes things more difficult to implement. If we want to achieve a certain level of maturity against the Zero Trust maturity model or reference architecture, we have to ask ourselves the question, are we achieving that for the entire agency? Are we achieving that on a certain component of centrally managed IT or just within certain programs?" The goal is to implement those things in a way that benefits the majority of systems within the agency.

The Idaho National Laboratory is already well into its Zero Trust implementation journey. It is now focused on securing its data and adjusting the data pillar, according to Dr. Robert Roser, chief information security officer for Idaho National Laboratory.

"You cannot protect the data if you do not know whether it is sensitive or not," Roser said. "The first step that you have to do is to label, classify or categorize data as to whether it contains sensitive information."

The lab, for instance, has large amounts of legacy data that has yet to be categorized or labeled, and is deploying algorithm-based and machine learning-powered technology to help automate the entire process. "Once categorized, we can potentially move it where we have better visibility for certain types of data and protect it at a different level," Roser said.

LESSONS LEARNED THROUGH IMPLEMENTATION

One of Roser's top takeaways from the Idaho National Laboratory's journey with Zero Trust is to train the entire IT team. "Make sure they understand [Zero Trust] so that they can't live without it moving forward," he said.

And Wood then emphasized the importance of starting with identity for most agencies, as it acts as the foundation to the other pillars of Zero Trust. CMS' federated environment results in different pockets of identity management preferences. "We really have to go the extra mile to make sure that any work that we do there is complete," he said. Because identity needs to be central core of everything related to Zero Trust, and is something that can be achieved even if the agency has a large or complex infrastructure.

For Yarborough, a key is also being able to track the effectiveness of Zero Trust programs as they are being implemented against expected metrics or best practices. "Analyzing user behavior and perhaps trying to assess incident response while also evaluating access control measures helps to monitor the effectiveness of segmentation and even our threat intelligence capabilities," Yarborough said.

That practice, coupled with the understanding of how the agency and its 1,250 systems are advancing with respect to meeting Zero Trust needs, allows HHS to know how it's progressing towards Zero Trust, and whether or not it needs to devote additional resources to that effort.

Ultimately, all panelists agreed that it's best to begin moving towards Zero Trust by classifying data, knowing what needs to be protected and starting small while learning about adding Zero Trust components to the environment. "Being intentional and focusing on the processes and organizational dynamics is just as important, if not more so, than the tool selection you ultimately go with," Wood added.

FEDInsider

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

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

carahsoft.

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

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

illumio

Illumio, Inc
920 De Guigne Drive
Sunnyvale CA 94085

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