Zero Trust Strikes a Balance Between Access and Security for Data

Managing the data lifecycle is a mission-critical task for all agencies.  

James Mersol  
Fri, 01/31/2020 - 14:06

The rise of data and the rise of remote users have happened in almost perfect unison in federal IT. The challenge becomes how to ensure that data is accessible by everyone who needs it whenever they need it, while at the same time ensuring the data is accessible only by those who need it and when they need it.
Traditional IT perimeter security restricts access to onsite employees, keeping the data protected but not particularly accessible in a cloud-driven environment. Agencies including the Department of Agriculture and Department of State are adopting the Zero Trust model as an improved system to provide both the access and security needed in an era when data is essential.

“For [the USDA], the driver becomes ‘how do I make sure that the data that I’m providing is, in fact, trusted?’,” said USDA CISO Venice Goodwine. “‘Have I classified my data properly, so that those who need access to that data have it relatively available?’, and then of course the general principles ... of cybersecurity still apply.”

Goodwine repeated, “It’s all about the data” throughout the discussion, each time explaining that this is one constant she sees in all agencies regardless of their individual missions.

“Where is the data actually located?” she asked. “What is the classification of the data? Who requires access to the data, and when they no longer require access, do we have policies in place ... to remove that access?”

Zero Trust makes “identity the new perimeter,” GSA Executive Director of Identity Phil Lam said. Tying access to an identity rather than a physical location removes the risk of dormant accounts maintaining access to classified data, a common threat vector that attackers exploit.

“It might be different data [between agencies], but the principle still remains the same,” said Goodwine. “I have to protect the data, I have to know the data, manage the lifecycle of the data. ... The missions are different, even maybe the funding type is different, but the principles still apply.”

When it comes to how to implement Zero Trust in agencies, Goodwine said USDA, like many other agencies, seeks public-private partnerships on identifying solutions. These conversations, she said, help her agency determine what solutions will deliver the greatest return on investment for its needs.
“When I meet with individual industry partners and vendors, I like to talk to them and ask them, ‘exactly what is the capability that you’re bringing to me?,’” she said. “Having that conversation then enables me to make better decisions about return on investment and make sure that what I have in my environment ... maximizes [my ROI].”

Goodwine also highlighted how important the federal CDO mandate is for data management.

“Having a CDO now as a requirement is important,” she said, “because now we have data stewards throughout our organizations that actually manage our data and the lifecycle of our data.”

“Data” means more than just access, said Gerald Karon, director of enterprise network management at the Department of State.

“At the end of the day, we’re trying to protect the data and a lot of people talk about ‘access,’” he explained. “I’m looking at it as continuous access and continuous conditional rules that apply ... We’re looking at making [access] transactional so we can understand what’s ‘normal' ... it’s not always a user that’s [accessing] that data — so what is accessing that data? Transactions, machines ... it’s got to be transactional, and it’s really got to be policy driven.”

Especially as an agency with employees and systems in every time zone, the Department of State looks at Zero Trust as more than just a system for data protection or even identity management.

“It’s not just identity, it’s not just endpoints, it’s not just data,” said Karon. “It’s the totality of it all.”