How AI Could Help Federal Agencies With Their Zero Trust Strategies

DHS Deputy CTO Brian Campo said zero trust is all about how you control your data. Kate Macri
Tue, 10/20/2020 - 10:22

The heart of the zero trust approach to cybersecurity is proactive control over your data, according to Department of Homeland Security Deputy Chief Technology Officer Brian Campo.

In a virtual event hosted by NextGov last week, Campo said the first step in a zero trust strategy is recognizing there is no physical boundary anymore, just data, which security professionals must tightly control.
“Data can't be treated as an all-in-one asset, data is not equal,” he said at the event. “We can't give people all the access to all the data in an application. Zero trust is the really vital aspect that gives us more granular control over the endpoints you have access to as well as the data.”

A zero trust approach enables federal agencies to grant granular access to different data based on a user’s credentials and the user’s interaction history with other data sets.

“There is no predefined security. With zero trust, what you're doing is you're looking at every single request as a new request for a resource,” Campo said. “It's giving us different paradigms and different defense vectors. We've got these sets of criteria. We're doing policy enforcement not at the gateway anymore, we're doing it on the endpoint. We're doing it in different traversal points across the network. There's no [longer] just one access mechanism anymore. On the endpoint we might be looking at GPS location, or other things that are installed on that endpoint like software applications.”

With all this user information, security professionals can make educated decisions about what level of access to grant.

“We can really build these viable identity profiles at each stage of the policy decision,” Campo said. “The other aspect that's really interesting is we're seeing more people work from untrusted locations. Before we could say someone was only ever going to work in a controlled building or controlled access point. Now ... [they're] on the same network in their house as a damaged computer, or their router may be compromised. Zero trust is absolutely vital.”

DHS is focused on aggregating its components’ directories of singular identities to verify users at different levels of data access, Campo said, as part of the department’s zero trust strategy.

But zero trust is more than just users, it’s also about devices and what kinds of devices a federal agency will allow on its network, an especially pertinent question as federal agencies are teleworking.
"I think zero trust is about how it integrates into the overall infrastructure," said Kevin Finch, global security strategist for World Wide Technology, at the event. “You're trying to establish a source of truth. That user also needs to come from a trusted device.”

Because zero trust must verify users, systems and devices continuously, Finch said federal agencies and their IT contractors should think about ways to make that verification process as seamless as possible.

“It needs to be seamless in nature,” Finch said. “Now there's this common knowledge that we're going to do that on the initial request and the lifecycle of the question. If something changes at the endpoint, [we have a risk profile so] now we can ingest that into the policy orchestration and it's no longer a binary decision of yes or no. Maybe there's a judgment call on the level of access, maybe only read access.”

Campo expects artificial intelligence to play a large role in zero trust in the future to help predict, automate and streamline access-granting decisions.

“Zero trust is all about thinking proactively,” he said. “Where do I think the user needs to go and access? That's really where zero trust is focused. Being able to understand the types of scenarios your systems need to communicate at. Thinking proactively about what sorts of data should be traveling through my network.”