fedscoop

# Will agencies implement zero trust faster with TIC 3.0?

Written by Dave Nyczepir
APR 29, 2019

https://www.fedscoop.com/zero-trust-networks-tic/

Most agencies, if not all, will implement zero-trust networks to some degree within 18 months, aided by the overhaul of the Trusted Internet Connections guidance, predicts Stephen Kovac, vice president of global government and compliance at Zscaler.

Introduced in 2004, zero trust is a cybersecurity framework rooted in the notion that the network is always hostile and every device, user and flow must be continuously authorized whether they're local or not.

Meanwhile, TIC 3.0 — a draft of which was released by the Office of Management and Budget in December — introduces new use cases like Platform-as-a-Service (PaaS) or software-defined networking in a wide area network that can accommodate ZT solutions.

"TIC 3.0 is going to allow much speedier implementation of zero trust," Kovac said.

That's because federal procurement vehicles currently lag behind new technologies, he added.

Zero trust remains in the "research phase" at the Department of Labor, said Scott Davis, the department's deputy chief information security officer.

DOL is "pretty far along" implementing identity access management, centralized account management, and provisioning and deprovisioning of accounts, Davis said.

"Everything is based on resources. Whether something is brought from the [Continuous Diagnostics and Mitigation] program or we're able to make it something budgetary to focus on [ZT], that's a priority for our CIO," he added. "I don't know about timelines, whether it's 18 months or not."

Traditional security involves establishing a perimeter, often with a virtual private network, or VPN, where the user calls in, is placed on the network and can then go where they want. The process is a slow one, Kovac said.

Zero turst solutions vary, but Zscaler's involves the creation of "microtunnels" that stitch outbound calls to the user and the application together on an enforcement plane where neither has control and no IP address or user data is available — a dark connection. The internet is used to create the microtunnel, but people aren't placed on the internet.

"How do I take that user and put them where they should go without giving them access to anywhere else?" Kovac said.

That process is problematic for TIC 2.2, which mandates that open internet connections run back to the TIC. Fortunately, TIC 3.0 is "more focused on use cases than locking down the perimeter," Kovac said.

As a result, agencies will be able to use procurement vehicles like the Enterprise Infrastructure Solutions contract and Cloud Special Item Number to acquire zero trust technologies, he added.

"[T]here are currently no vendors in the market offering a complete and comprehensive ZT/SDN solution," according to a new ZT report from ACT-IAC. "Depending on what they seek, agencies may need to plan for a coordinated acquisition of products and services from multiple vendors to meet their requirements."

Some agencies will ultimately move to a full ZT network, while others will use ZT to compliment other cybersecurity tools and practices like a VPN or access control, Kovac said