MeriTalk
cisco SECURE | DUO
digicert
PLURALSIGHT

SPECIAL REPORT

ZERO TRUST: The Next Federal Frontier

The Federal government is nearing the halfway point of a three-year plan to move agencies toward zero trust cybersecurity to better protect the nation from cyberattacks. With its recent National Cybersecurity Strategy, the Biden administration reinforced the commitment to zero trust made in last year's memo from the Office of Management and Budget (OMB), which required agencies to meet specific zero trust goals by the end of fiscal year 2024.

With Federal leaders working to carry out the mandates, how is the zero trust landscape evolving across the government? And what is the road ahead for accelerating zero trust implementation?

A key official overseeing zero trust, Federal Chief Information Security Officer Chris DeRusha, said at an event in March that the plan initiated by the January 2022 OMB memo is aimed at getting "everybody prepared and ready for this massive, long-haul migration and transformation that they're going to need to make."

Looking ahead to what they see as a 10-year modernization campaign, he said, officials are now writing an operational plan and homing in on specifics such as developing shared IT services across the government to heighten cybersecurity. "Over the next decade, we're going to strive to modernize legacy IT that cannot implement zero trust principles, and if you can't get there with that IT then you shouldn't be operating it," DeRusha said.

Zero trust is an approach to cybersecurity that "treats all networks and traffic as potential threats" and incorporates technologies that authenticate and validate user identities in an effort to control and manage data flows within networks. Zero trust is not a single technology, product, or service; rather, it is "a set of guiding principles for workflow, system design, and operations that can be used to improve the security posture of any classification or sensitivity level."

Amid warnings of an increasingly ominous cyber threat landscape, there has been a rush of recent activity as agencies move toward zero trust architectures. The Biden administration's fiscal year 2024 budget request contains $12.7 billion for Federal civilian agency cybersecurity, a 13 percent jump from 2023, and budget documents said a top priority is using that money to make Federal systems "more defensible by adopting zero trust principles."

In mid-April, the Cybersecurity and Infrastructure Security Agency (CISA) released the second version of its Zero Trust Maturity Model that is guiding Federal agencies on the path to zero trust. The updated document expands the range of zero trust maturity stages for agencies from three to four by incorporating a new "initial" stage. The four stages of maturity are now Traditional, Initial, Advanced, and Optimal.

CISA said it added the additional stage because "organizations begin their journey toward zero trust architectures from different starting points."

The new cybersecurity strategy, released in March, is also spurring Federal agencies to move faster as they seek to reach their zero trust goals. "The National Cybersecurity Strategy stands as a catalyst for accelerating the adoption of zero trust security architectures across the Federal government," said Mike Nelson, vice president of digital trust at DigiCert. "By providing a clear framework and guidance for implementing zero trust principles, it requires and empowers agencies to modernize their security infrastructures and better defend against today's advanced threats."

Across the government, agencies are reporting varying stages in their zero trust evolutions. State Department Chief Information Officer Kelly Fletcher, for example, said the move to zero trust has been hard because the agency is still "operating with a lot of legacy technology."

"We could hit zero trust out of the park if I was in a greenfield, but I'm not," Fletcher said in March. "So, what we're trying to do is really couple modernization with zero trust."

At the General Services Administration (GSA), which began its zero trust journey in 2016, the agency has made progress in tackling CISA zero trust pillars such as identity, device, and network, and is now moving on to application-level security. "We've made a lot of headway in our zero trust implementation," GSA Chief Information Officer David Shive said in March.

Other agencies, DeRusha said, are making progress in implementing centralized logging, single sign-on, and phishing-resistant multifactor authentication. "We're all in different places of maturity" in adopting zero trust, he said.

To achieve success with zero trust, experts recommend a comprehensive, integrated approach to protect users and their devices against stolen credentials, phishing, and other identity-based attacks; secure hybrid, multicloud workloads; and identify and act on cyber threats.

"Zero trust helps by taking an integrated approach to an agency's security, networking, and applications," said Andrew Stewart, a senior Federal strategist at Cisco Systems. "We think of it as four steps of a continuous cycle: establishing trust, enforcing trust-based access, continuously verifying trust, and responding to changes in trust in the relationship between users and devices and data, applications, and workloads. By taking these steps, agencies are realizing better security resilience."

Also important in the path forward is training – upskilling and reskilling the broader Federal IT workforce for zero trust – especially amid a continuing cybersecurity workforce shortage. Brandon DeVault, senior security author at Pluralsight, said cybersecurity training "must be embedded in agencies' overall zero trust strategies in order to have a fully realized cybersecurity framework. Gone are the days of ad hoc training once or twice a year. Federal cybersecurity teams must prioritize the education of their workforces so that they can be prepared to take on any new threat that their agency may face."

As agencies move ahead, experts also recommend that they integrate the concept of digital trust – centralized visibility and control over a broad range of digital needs including securing websites, enterprise access, software, and identity. Putting a zero trust policy into place is one way of achieving digital trust.

One Federal organization that has stood out in its adoption of zero trust principles is the Department of Defense (DoD), which last year issued a Zero Trust Strategy emphasizing that everyone in DoD must urgently adopt "a zero trust mindset" to "make certain that when malicious actors attempt to breach our zero trust defenses, they can no longer roam freely through our networks and threaten our ability to deliver maximum support to the warfighter."

Some experts have called DoD's quick action a model for civilian Federal agencies, and DeRusha said the strategy is "a fantastic kind of larger, comprehensive zero trust migration plan for defense." DoD officials have said they are already working on the next iteration of the strategy.