Zero Trust Provides Long-Term Solution for Remote Work

Federal IT leads say the strategy lets agencies ‘use the tools we have’ to modernize security.

James Mersol
Wed, 05/20/2020 - 14:09

Both public and private sector organizations supported the concepts of Zero Trust to enable a more remote workforce, providing employees access to mission-critical data and applications even when working out of the office. That approach is even more critical now that few, if any, employees are working onsite at federal agencies, and agency leaders see it as a long-term solution that does not require a total restructuring of networks and online environments.
“We’re not going to get to a new environment any time soon,” said Federal Chief Information Security Officer Grant Schneider. “We’re living in a Zero Trust environment.”

While several agencies were already implementing Zero Trust principles prior to the COVID-19 pandemic, others are experiencing “a little bit of everything” when it comes to IT challenges, Schneider said. Two months in, most agencies have a remote computer solution in place — and those that do not have a valid reason, such as concerns over handling Top Secret material — but applying that solution to other hardware, such as monitors and printers, is still in progress. Remote connections to printers, for example, raise questions over the “internet of things” and network vulnerabilities.

Zero Trust answers these questions by removing the traditional perimeter from the network, connecting users directly to the application based on identity and access credentials, instead of granting access to all or part of a network.

“You cannot hack a network you’re not on,” said Stephen Kovac, vice president of global government and compliance at Zscaler, a provider of trusted internet connection (TIC) and Zero Trust solutions. “[Zero Trust] ... can’t be hacked.”

For the State Department, protecting ‘data on the wire’ is especially important, given the number of remote and international connections the department uses on a day-to-day basis, said Acting Enterprise Network Management Officer Gerald Karon.

Karon explained that his office has used Zero Trust to manage identities based on several factors, including personal identity, device and location, as well as managing access based on the sensitivity of the information, moving away from a model that treats public-facing content as equal to personally identifying information.

“[We] distrust everything,” Karon said, “so when a breach happens [we] are as protected as can be.”
Advancements in artificial intelligence and machine learning can combine with human intuition to better protect networks and data, said Department of Education Chief Information Security Officer Steven Hernandez, one of the earliest adopters of Zero Trust in the federal government. In one hypothetical scenario, AI can flag when an employee’s download bandwidth spikes, then escalate it to a security team. The team could then cross-check with human resources to learn that the employee recently received a poor performance review and cap or shut off access to prevent a malicious insider incident.

The human element of developing a Zero Trust strategy is essential.

“You really have to get your mission folks on board with this,” Hernandez said. “[The new workforce] needs any data on any device at any time to execute our mission.”

Karon underscored how Zero Trust secures the data and networks behind agencies’ missions.

“It should be continuous,” he said. “[Identities] should be constantly evaluated until the user is logged off completely.

Many Zero Trust tools are already at agencies’ disposal, and federal leaders are at work with the National Institute for Standards and Technology (NIST) to release guidelines on how to implement those tools. Alper Kerman, Zero Trust technical lead at NIST, said that the draft for NIST Special Publication 800-207, “Zero Trust Architecture” is currently undergoing final review, with the final version expected by the end of May. At the same time, the National Cybersecurity Center of Excellence (NCCoE) has established a test lab, which is currently testing how to integrate technical components into a Zero Trust architecture. The lab will test Zero Trust scenarios and capabilities next, with a focus on undertaking a project on implementation in late 2020.

From an acquisitions perspective, the General Services Administration (GSA) is fast tracking Zero Trust and TIC solutions, Kovac said, with many agencies planning to use funds from the Technology Management Fund and CARES Act to transform their IT.
“I have a tremendous amount of respect for the FedRAMP office,” Kovac said, after Zscaler’s TIC platform went through the approval process in less than three months, a timeline far shorter than both official FedRAMP targets and typical timelines for certification. “Everyone’s stepping up ... [it’s] a true partnership.”

View printer friendly version
Federal Cybersecurity
Zero Trust
TIC
State Department
Department of Education
GSA
Standard