Zero Trust Provides Remote Security for Government, IT Leads Say

Identity-based approach to verification moves beyond perimeters and VPNs.

James Mersol
Mon, 05/11/2020 - 18:17

The federal government’s shift to mass telework in response to the COVID-19 pandemic is unprecedented in its size, but the numbers are still remarkable and shed light on security needs moving forward.
In the weeks following guidance from the White House's Office of Management and Budget and the Office of Personnel Management, the Department of Homeland Security saw a 900% increase in telework, a 255% increase in “workplace as a service” usage and a 483% increase in VPN usage across the agency, said Bryan Forsythe, technical assessments branch chief for DHS. While there were some “low-hanging fruit” for remote security solutions, with the 'internet of things' coming, DHS realized a fortified perimeter approach to security wouldn’t work, Forsythe added. Instead, it needed a solution beyond VPNs, turning to the Cybersecurity and Infrastructure Security Agency (CISA) for guidance on Zero Trust.

“Revector where the perimeter is,” said CISA Chief Technology Officer Brian Gattoni, referring not only to the remote work applications for zero trust, but also for making Zero Trust work with DevOps. DevOps tends to rely on technologies such as containerization that work well within the perimeter, but are not designed for remote work, Gattoni said. Getting the most out of Zero Trust may require building multiple perimeters — in effect, multiple layers of security — and redesigning security checks to ensure “the same entity” is going through each layer of security to get to the DevOps environment.

Zero Trust has applications beyond allowing DevOps teams to continue working remotely, however. For the U.S. Marine Corps, Zero Trust is part of an organization-wide plan to divest from legacy systems and reinvest in new technologies. This plan was already in place before the pandemic, said the service's Cyber Technology Officer Renata Spinks, but the changing circumstances accelerated that plan. Already, a Zero Trust solution enhances verification across the Defense Department network for the Marines.

“We trust and verify, we monitor behavior,” Spinks emphasized. “Then we trust again, we verify again.”

Spinks does not consider Zero Trust — the concept of granting access to systems based on a user’s identity, with continuous authentication and verification — entirely new, pointing out that similar frameworks are already in effect.

“Zero Trust is already kind of happening,” Spinks said. “Users don’t get access to an entire network.”
Contractors, industry liaisons and health care providers with the DOD have access to segments of the networks — such as those working on the Defense Health Agency’s electronic health record management — without having access beyond that data. Taking that approach across the network is part of the next step. The Marines plans to incorporate Zero Trust as part of its move to an Agile, continuous service model as part of its modernization.

“We’re no longer building from the ground up,” Spinks said. “We’re integrating [these methodologies] into our environment.”

Gattoni added that Zero Trust’s goals "are in alignment" with CISA’s other programs, including the continuous diagnostics and mitigation (CDM) program and the trusted internet connection (TIC) 3.0 program. TIC 3.0, in particular, has a “really nice dovetail” with Zero Trust, Gattoni said. TIC pilots have used Zero Trust to assist with metrics and risk scoring for connections and network systems.

Government Zero Trust innovators have reminded those involved that there is no one solution or set of solutions that allow organizations to adopt Zero Trust. At the Small Business Administration, CIO Maria Roat has underscored that many agencies already have some of the tools they need to implement it.

Jim Russo, enterprise infrastructure technical solutions lead at the General Services Administration, added that the move to telework “heightened the need” for a continuous authentication solution. This need has led GSA to work with CISA and other agencies as well as industry to find applications for Zero Trust in related use cases, such as TIC.

“Zero Trust will probably be a solution from several of these use cases,” Russo said, although he noted at this point there are a lot of variables in play that make it hard to define those solutions.
Russo said he could even see a government version of how banks will freeze customers’ cards automatically when they spot unusual activity, where any user who accesses a government network outside of their usual location without prior approval would have their access temporarily revoked. Gattoni suggested that agencies could develop an AI/ML solution to make this solution work better with users, automatically registering travel on the backend rather than requiring an official exception.

The bottom line for agencies looking to implement Zero Trust is to sell it as a cost-effective solution to further the mission, Zero Trust leads agreed. Especially for agencies with budget constraints, shifting resources to the right approach is critical, Spinks said. Gattoni encouraged IT leaders to avoid limiting themselves in these conversations.

“Focus on the mission,” Gattoni said. “Be ambitious.”