FERTINET®

WHITE PAPER

Federal Zero Trust Strategy and Maturity Model

Highlights from the Webinar "Hear from the Authors: Federal Zero Trust Strategy and Maturity Model"

Federal News Network reporter Nicole Ogrysko memorably described Executive Order (EO) 14028, "Improving the Nation's Cybersecurity," as having "aggressive" timelines and "detailed and lengthy" requirements but noted the Biden Administration's seriousness in delivering the "necessary shock to the system" to push federal agencies to secure their networks. While the EO is far-reaching, one of its most notable components was the requirement that agency heads "develop a plan to implement Zero Trust architecture" within 60 days of the EO's issuance on May 12, 2021.

In order to help put these plans into action, EO 14028 further stipulated that within 90 days of its issuance the Office of Management and Budget (OMB), the Cybersecurity and Infrastructure Security Agency (CISA), and the Administrator of General Services acting through the Federal Risk and Authorization Management Program (FedRAMP) would work together to "develop a Federal cloud-security strategy and provide guidance to agencies accordingly." As a result of these efforts, three guidance documents were produced: a draft Federal Zero Trust Strategy released by OMB, a Zero Trust Maturity Model developed by CISA, and a corresponding Cloud Security Technical Reference Architecture.

> *There are many ways to get to Zero Trust. There isn't just one path.*
>
> Sean Connelly
> CISA

As part of its mission to bring together government, industry, and academia, the Advanced Technology Academic Research Center (ATARC) recently held a panel discussion with the co-authoring agencies of the aforementioned guidance documents in partnership with Fortinet® (NASDAQ: FTNT), a global leader in broad, integrated, and automated cybersecurity solutions. The panel featured Sean Connelly, TIC Program Manager and Senior Cybersecurity Architect at CISA, Elizabeth Schweinsberg, Digital Services Expert at the United States Digital Service (USDS), John Simms, Senior Technical Advisor at CISA, Eric Mill, Senior Advisor to the Administrator/Federal Chief Information Officer, Office of E-Government and IT at OMB, and Jim Richberg, Chief Information Security Officer, Public Sector at Fortinet. Discussion was moderated by ATARC Founder and CEO Tom Suder.

During the spirited discussion that followed, panelists described their perceptions of Zero Trust, described the problems associated with legacy approaches to cybersecurity, and considered the barriers inhibiting agency adoption of a Zero Trust model. Panel attendees from across the federal government and private industry actively participated in the discussion by asking questions of panelists and taking part in a series of poll questions.

Understanding Zero Trust

While the term 'Zero Trust Architecture' is used liberally within the cybersecurity community, it is often misunderstood outside of it. Part of the confusion stems from the fact that Zero Trust refers to an architectural model, rather than a defined technology stack or a single set of products that can be purchased off the shelf. In EO 14028, the essence of a Zero Trust Architecture is defined as allowing "users full access but only to the bare minimum they need to perform their jobs." The idea being that "if a device is compromised, Zero Trust can ensure that the damage is contained."

Expanding on this notion, OMB's Eric Mill described Zero Trust as an attempt to move away from the old 'castle and moat' approach to cybersecurity, "where once you are logged into the internals of your organization you are broadly trusted within it." By contrast, in a Zero Trust model "you are constantly evaluating and reevaluating whether a person or device is authorized to do the thing they are trying to do."

In explaining the logic behind Zero Trust, Mill referenced the common saying among cybersecurity professionals that "you can never remove risk, you can just move it around." In his words, the goal of Zero Trust is not to completely remove risk from a system, which would be an impossible task, but rather "to move that risk into places where we know we can more effectively manage it and where it's explicit and known and protected, as opposed to having it sprawl throughout the enterprise."

Moving Beyond the Castle

Prior to the emergence of Zero Trust, the 'castle and moat' approach to enterprise security, where security teams were largely focused on defending the network perimeter, reigned supreme for a quarter century. However, as CISA's John Simms noted, this approach is no longer up to the task of defending a network that has become increasingly dispersed among an ever-growing array of devices and locations. Furthermore, according to Fortinet's Jim Richberg, the 'castle and moat' approach has the weakness of putting all of an organization's 'eggs into one basket.' For example, if the single-sign on system is compromised and a malicious actor tricks the system into thinking it is a legitimate user, that can have wide-ranging consequences.

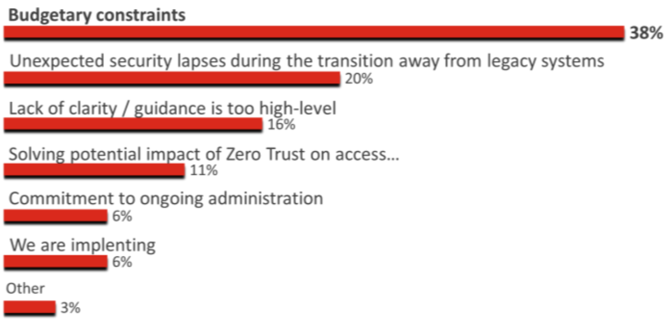
> *The 'castle and moat' architecture has been used for 25 years. It's not effective given the types of threats and the large attack surfaces that we have in our federal enterprise.*
>
> John Simms
> CISA

Yet, while Zero Trust is widely seen as the future by the cybersecurity community, panel participants were unanimous in their view that the work of moving to this model is not going to be completed overnight. In the words of Simms, "it's not a two-to-three year thing, it's a long-term endeavor." Mill added that he and his colleagues at OMB are "well aware that 99% of the work is yet to come. This is an architectural shift, not just turning on a particular security thing." USDS's Schweinsberg agreed and ended with a call for collaboration, saying "we will all get farther if we share what we learn over this Zero Trust journey… no one has to do this all alone."

The Audience Weighs In

The responses of panel attendees provides strong evidence of ongoing confusion among agency staff regarding how to actually put a Zero Trust approach into practice. While the vast majority of attendees, 76%, agreed that "all three" of the guidance documents co-authored by OMB, CISA, and FedRAMP impacted their agencies' plans, just 27% indicated that the documents were "clear and actionable." Nearly half of attendees indicated that they still hadn't had time to digest them and another 27% said they were still unclear about how the guidance documents intersected with one another or how they mapped back to EO 14028.

Webinar Audience Poll: What is the top challenge hindering your agency from implementing the guidance provided in these documents?



Audience participants were also asked what barriers they faced in implementing the guidance documents. Responses were varied but the most commonly cited challenges were budgetary constraints and fear of security lapses during the unwinding of legacy solutions, which together accounted for more than half of audience responses. A mere 6% of attendees indicated that they were already implementing the recommendations laid out in the guidance documents, suggesting that Schweinsberg and Mill were correct in their assessment that most of the work of putting Zero Trust into practice remains to be done.

How Fortinet Can Help

Based in Reston, Virginia, Fortinet Federal, Inc. is a wholly owned subsidiary of Fortinet, Inc., established to provide federal government customers with complete visibility and control across the expanding attack surface, and the power to take on ever-increasing performance requirements today and in the future. Fortinet solutions help address the federal government's most critical security challenges, from multi-domain network security to zero trust access.

Contact us today to learn more!