FORTINET FEDERAL®

Cyber EO One Year Later: Implementing Holistic Zero Trust Security

In May 2021, President Biden issued the sweeping Executive Order on Improving the Nation's Cybersecurity (cyber EO), which included 11 sections of information, guidance, and mandates designed to push Federal agencies to improve their cybersecurity posture and modernize their infrastructure to protect the American people and our nation's sensitive information and assets. Many of the mandates involve implementing a zero trust architecture. MeriTalk recently sat down with Fortinet's Jim Richberg, public sector CISO, Peter Newton, senior director, product marketing, and Fortinet Federal's Felipe Fernandez, senior director, system engineering, to gain their insights into how Federal technology teams can integrate all of the components of a zero trust architecture to achieve holistic cybersecurity in a cloud, hybrid, or closed environment.

MeriTalk: We are nearing the one-year anniversary of President Biden's cyber EO. What has been the biggest impact or change to Federal cybersecurity practices that you've seen over the past year as agencies work toward meeting the mandates in the EO?

Richberg: Based on my 35 years of working in the public sector, what is significant about the cyber EO is that it really got the agencies and the vendor community focused and aligned on technology solutions in a way that you don't typically see in government. While there are dozens of action items in the EO, most of them relate to building a zero trust architecture.

The government quickly put out a strategy, technical reference architectures, a maturity model, and shared capabilities information to guide agencies on the path to implementing zero trust principles. Those things also guided the vendor community to develop the technology solutions that would help agencies achieve the EO mandates.

Fernandez: The EO also addresses some of the questions raised by technology teams throughout the years that have worked through the National Institute of Standards and Technology (NIST) and Federal Information Security Management Act (FISMA) compliance.

Being compliant didn't necessarily equate to being secure. With the EO and its zero trust architecture, compliance now is security. Because of that, the vendor community and the user community – regardless of agency – are aligned with the solutions that need to be developed and deployed to be both compliant and secure.

MeriTalk: The cyber EO is moving Federal agencies to adopt a zero trust architecture quickly; some say too quickly. What should agencies prioritize as they implement zero trust security across their agencies?

Richberg: The Zero Trust Maturity Model released by the Cybersecurity and Infrastructure Security Agency (CISA) really demonstrates that the Federal government understands that each agency is on its own path. It even recognizes that all agencies don't need to get to the same level of maturity – maturity is based on their missions. The maturity model does a really good job at allowing agencies to prioritize the work of building zero trust security for themselves. It guides them, because everyone is moving in the same direction, but recognizes that each agency is starting from a different place and may stop at a different point along the pathway to fully mature, real-time zero trust capability.

Fernandez: Agencies do need to prioritize building a zero trust mindset within their workforce though. There may not be an understanding of what zero trust means – both in the technology organizations and with the end users. It may be hard for users to understand why they can't do whatever they want whenever they want with their IT assets. By helping them understand the need for proper cybersecurity – even drawing parallels to physical security such as the need for metal detectors when walking into some Federal buildings – they can become allies on the journey to zero trust.

Richberg: Zero trust is misleading language, especially for a workforce of public servants who were hired into positions of trust – and who may even have security clearances. Those of us who work with zero trust principles every day know what it means, but for the end user who may not, zero trust sounds like "I don't trust you" and has Orwellian implication of workplace surveillance. Employees may consciously or unconsciously push back. But zero trust is actually an enabler for employees, facilitating their ability to work from anyway in the 'new normal' operating environment. Zero trust simply means that security should not be determined solely by whether a validated user or device are connecting from within or outside of the network perimeter and that an appropriate level of trust is established prior to every transaction.

MeriTalk: A recent report from the National Security Telecommunications Advisory Committee said the government was in jeopardy of having zero trust become an incomplete experiment – a collection of disjointed technical security projects. What can Federal agencies do to ensure that doesn't happen?

Newton: This report really highlights the importance of taking a holistic approach during the assessment period. I've seen surveys of teams implementing zero trust and the single thing they find most challenging is to get all of the components to work together. To avoid that, agencies need to ensure they are selecting an ecosystem of products that work together. Having a platform-based approach to zero trust implementation will ensure it's not just a collection of point products that aren't integrated.

Fernandez: One of the issues that may be tripping up technology teams is that there are so many different zero trust strategies, guidelines, and roadmaps – CISA offers guidance; NIST, Department of Defense (DoD), and the National Security Agency released their zero trust architectures; Office of Management and Budget has a zero trust strategy. It is imperative to decide which framework they want to align with and run with that one. This flexibility, which as we said earlier is not typically seen in government, means that agencies can choose what framework is most appropriate for them instead of being stuck with something that isn't appropriate for their use case. That flexibility means it won't be an incomplete experiment as long as the agency stays on its roadmap.

MeriTalk: Agencies implementing a zero trust architecture can choose from many technologies that are designed to meet the guidelines in NIST Special Publication 800-207 on building a zero trust architecture. Are agencies at risk of increasing security complexity as they pursue zero trust?

Fernandez: They aren't increasing complexity with zero trust; they are just now learning about different complexities with which they may not have experience. For example, a lot of the integrations between components of a zero trust architecture are done through application programming interfaces (APIs), and not every technologist has worked with APIs. The Fortinet Security Fabric helps with this by having out-of-the-box integrations within Fortinet products and third-party vendors. This platform approach ensures components work together correctly and securely, without placing undue pressure and risk on the security administrator.

Newton: The way to combat the complexity is to select an ecosystem and a platform of products that work together from the beginning and not try to get them to work together later down the line.

MeriTalk: Is it possible that zero trust implementation could reduce the number of security technologies that agencies deploy? How does it change the roles of security personnel?

Fernandez: Adopting zero trust absolutely could reduce the number of security technologies and ultimately change the role of security personnel. Here's why – over the past 15 years, security tools were built to address specific security vulnerabilities, such as databases, user web security, web application firewall, or mail security gateway. Technology teams ran out to get the latest security capability, but then had to get more personnel who were subject matter experts in that one capability.

Now, zero trust architecture enables us to focus on the outcome, not the capability. By restricting access to any resource on the network, the overall security effectiveness of deploying a zero trust architecture is higher than buying a security capability for each and every application, user, device, and server and then also having that subject matter expert manage that capability going forward.

And zero trust will allow us to address the cybersecurity skills gap because personnel roles can be more security outcome focused, not so much product capability focused. If we hire someone to be the subject matter expert of the firewall, we are not getting the most out of their talent. By up-leveling security talents' focus, we get teams full of people that understand the outcomes – and the appropriate knowledge of the components that lead to those outcomes will follow.

Newton: Implementing zero trust also reduces the amount of time spent on manual processes, as it relies on automation. Through automation, technology teams can redeploy their talent who were doing manual processing into much more productive uses to accomplish mission goals.

Richberg: Security teams may not realize that they are already doing some elements of zero trust. I used to hear it all the time: "Zero trust sounds really hard, and we can't devote the time or resources to doing it right now." When you start peeling back the layers though, most agencies already have network segmentation; they have role-based access control giving different levels of permissions to staff, contractors, and visitors.

This is a form of static zero trust; the goal of the Executive Order is to enable zero trust to be applied more dynamically and in real-time. With the right vendor partner, agencies can combine what they are already doing with new components to realize this dynamic zero trust security.

MeriTalk: What's often overlooked in the transition to zero trust?

Richberg: The biggest element overlooked in zero trust is education. Agencies need to help users understand that zero trust doesn't mean we don't trust you. Once you show the right credentials, you can get access to what you need. Zero trust is an enabler and a tool. Zero trust should be largely transparent to users, as opposed to the security and technology teams that have to implement it. But users are likely to hear or read something about their agency moving to zero trust architectures, and it's good to make resources like this available to explain to them what that means.

MeriTalk: Fortinet offers multiple solutions that can help agencies improve their cybersecurity and achieve a zero trust architecture. How are Fortinet solutions different than others on the market?

Newton: A lot of zero trust vendors are very cloud-focused in their approach. Fortinet understands and embraces the nature of hybrid environments. We know that agencies are not currently 100 percent in the cloud, and some never will be. Those agencies need a zero trust architecture that can be deployed everywhere, whether it's an on-premises resource or cloud-based resource.

Fortinet's zero trust solutions can operate in that hybrid environment. Through a combination of Fortinet-branded products and our third-party partners that are part of our security fabric, we offer a platform that encompasses everything that's necessary to achieve zero trust. The broad ecosystem of products that come together in our platform differentiates Fortinet from other solutions on the market.

Fernandez: We aren't just a viable solution for cloud or internet connected environments. I previously worked at DoD, so one of the things that is really important to me is that the Fortinet zero trust solutions can operate in a closed-area network. Especially in government, not all networks have unfettered access to the world wide web. Fortinet ensures that the products and solutions can still deliver zero trust network access, continuous monitoring, advanced malware analysis, and all of things that go along with complementing a zero trust architecture.

The other key differentiator is that Fortinet solutions were developed with unification in mind. We mean it when we say integrations work out of the box. The Fortinet Security Fabric is a unified platform to visualize and manage security in every environment.

Richberg: The other thing that matters is to make zero trust work at speed and scale. That includes using artificial intelligence and machine learning. That's what's going to drive automation. Fortinet has really been a pioneer in this area, having used the technology in our solutions for over 10 years.

FORTINET FEDERAL®