Evolving Agency Cybersecurity Practices to Meet Executive Order Goals

At the highest levels of the Federal government and the private sector, officials have recognized that cybersecurity is a national security issue. A series of policy and technical documents and high-level meetings this year have reinforced this notion. Chief among them is President Biden's cybersecurity executive order (EO), which outlines a wide-ranging and ambitious series of actions Federal agencies must take to better secure government operations. MeriTalk recently talked with Jim Richberg, field chief information security officer at cybersecurity firm Fortinet, who is uniquely qualified to assess the potential impact of the cybersecurity EO and the actions that agencies must take to realize its promise. Prior to joining Fortinet, Richberg was the senior federal executive focused on cyber intelligence within the U.S. intelligence community. He helped build the discipline of cyber threat intelligence analysis and is an innovator in measuring cyber performance, risk, and return on investment.

MeriTalk: The Executive Order on Improving the Nation's Cybersecurity sets out an ambitious plan for improvement – establishing up front that incremental change won't get us the security we need. Before we get into the nitty gritty, let's look at the big picture. How has the order changed the national conversation around cybersecurity?

Jim Richberg, CISO, Public Sector, Fortinet

Jim Richberg: The executive order is a brick in a much larger cybersecurity structure we're trying to erect as a nation. It establishes cybersecurity as a 'whole of nation' activity. It acknowledges that the government needs better technical security and that government's vulnerabilities extend to its dependencies on private-sector IT. Therefore, the government's private-sector partners must be involved in efforts to improve the security of government networks. We saw growing emphasis on public-private partnerships at the president's cybersecurity summit with industry in August, where major tech companies committed billions of dollars to improve IT supply chain security, which is one of the main themes of the EO.

MeriTalk: The EO set some aggressive deadlines for agencies, some of which have already passed. How are agencies balancing their existing cybersecurity obligations with the requirements of the EO?

Richberg: The EO focuses on a lot of really important issues that the government must address in order to improve cybersecurity. The requirements outlined in the EO were added on top of a fully booked budget, at a time when agencies are already juggling limited resources and limited personnel.

Truthfully, sometimes agencies simply must report, "I recognize this is a priority I'm obligated to meet, but I do not have the people or money to complete it." In this case, should agencies slow down other projects to initiate what's outlined in the EO? I think that's the direction many agencies are going. That said, the short-term deliverables set out in the EO are entirely consistent with things agencies were already working on. Essentially, the EO just pushed the gas pedal further on a lot of these priorities and asked agencies to start thinking about how to accomplish them.

MeriTalk: You've noted that some of the requirements of the EO are more immediately actionable – for example, multifactor authentication. Tell us more about that. What is the low-hanging fruit, so to speak?

Richberg: The low-hanging fruit – although it's heavy and expensive fruit – are things like endpoint detection and response (EDR) and multifactor authentication. Products and services on the market today meet these requirements, and the Federal government is already using many of them. The EO simply says agencies need to implement these solutions universally.

Accelerating the migration to the cloud can also be considered low-hanging fruit, because agencies have had private clouds, hybrid clouds, relationships with the public cloud, and special clouds within the public cloud for some time. The EO directs agencies to accelerate what they are already doing, and to do it in a way that implements zero trust as well.

To help with that, the National Institute of Standards and Technology has published multiple pieces of guidance on zero trust, and one more – essentially a how-to guide for administrators – is almost final.

MeriTalk: Agencies already have many cybersecurity solutions in place. As they evaluate their next steps toward meeting the goals of the EO, how should they go about deciding what solutions stay, and which must go?

Richberg: Agencies are going to want to break the mindset of saying "I'm replacing a firewall; I'm replacing a SIM device," because the new solutions today will likely offer the capability to do a whole lot more. Consolidation of security devices means that a next-generation firewall may perform the functions of a half dozen legacy devices. Of course, that doesn't mean agencies need to decommission the tools that are already performing those roles, but it's always worth considering the options.

Industry has been moving toward platform approaches to cybersecurity that emphasize the ability for devices and solutions in the environment to exchange data, and do it in an automated fashion, even across vendors. Several independent studies have shown that this platform-based approach to cybersecurity outperforms best-of-breed point solutions. Federal IT teams are used to making procurement decisions based on price and performance. They should add a third P, "platform," to their list of important criteria, because it essentially offers free synergy.

MeriTalk: We touched on the move to secure cloud services, which was kickstarted by the pandemic. Multicloud environments can introduce new security challenges. Tell us about those, and how agencies can overcome them.

Richberg: Cloud environments typically have different native security offerings. In cybersecurity, different often means inconsistent, inconsistent means gap, gap often translates into vulnerability, and that's what gets exploited. End-users in agencies want to access data seamlessly, regardless of whether it's in an on-premises data center or in a public or private cloud. At the same time, administrators know they need consistent security. They want security solutions that enable them to provision the same firewall rules in any cloud environment, for example. If that's not possible, they want to at least be able to feed the same threat intelligence to each environment.

MeriTalk: One of cybersecurity's biggest challenges is the growing size and complexity of the attack surface. How can agencies turn it into a net advantage?

Richberg: The platform ecosystem approach turns liability – the size, complexity, and sheer volume of endpoints and connections – into an advantage. It's truly transformational. If agencies can instrument the key parts of the network and apply artificial intelligence and machine learning (AI and ML) in real time, they can have a barometer of what normal activity looks like. ML enables agencies to see not only what's abnormal, but also what matches the confirmed characteristics of malicious activity.

Attackers typically try and fail innumerable times before they get into a network. Without the benefit of AI and ML, their attempts to look at something may not be noticed, because the defender can't be looking everywhere, all the time. Even if the defender did happen to note activity that could be malicious, there's no way of telling if it's a minor or existential threat. Consequently, the defender doesn't know what the attacker is trying to do.

However, if the network is instrumented and AI and ML are running behind the scenes, agencies will be able to sense a disturbance in the force before it's significant, to use a Star Wars analogy. Agencies can then react to it, wherever it's occurring, and inoculate everyone globally against it. That's why I view the evolution of this platform-based approach to cybersecurity, powered by increasingly mature AI and ML, as transformational.

MeriTalk: Fortinet offers multiple solutions that can help agencies improve their cybersecurity and, by extension, meet the requirements of the EO. How does Fortinet stand out from other providers in the market?

Richberg: Fortinet was a pioneer, if not the pioneer, of the platform-based approach, so it has first-mover advantage. The big OEMs in the security industry each have their own version of a security platform, but Fortinet is the most mature, and it's the broadest. Fortinet offers solutions that protect more than 50 aspects of networks that are part of the attack surface, and they can all be connected via Fortinet's platform. In addition, Fortinet consciously opted to make its platform an open ecosystem, and today, more than 400 best-of-breed solutions comprise the ecosystem, from the edge, to the core, to the cloud.

Fortinet also designs our own chips from scratch, which provides performance advantages compared to going commercial off the shelf. During my time in government, I got used to scenarios in which some commercial solutions could offer the highest performance, and other solutions that were the most cost-effective. The unique thing about most Fortinet solutions is that they're the highest performing and they're often the most cost effective.

Fortinet also has a large global threat intelligence organization that draws on more than 6 million devices around the world. Even if agencies aren't using Fortinet technologies, they can take advantage of Fortinet's threat intelligence. Like our platform, our threat intelligence is highly interoperable with other security solutions.