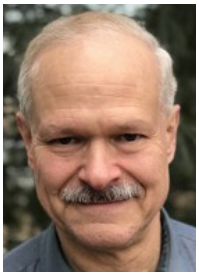
Modernizing Federal Cybersecurity

Organizations should consider using firewall-based Zero Trust because it consolidates and optimizes security operation and management in any environment, whether in the cloud, at the edge, or on-premises.

Jim Richberg
Public Sector Chief Information Security Officer
Fortinet



The United States Federal government is massive and doesn't typically make big changes with great speed, except in extreme situations. The fact that President Biden issued an Executive Order (EO) with specific timelines related to modernizing cybersecurity is an indication of just how critical changing and evolving the federal government's security posture has become.

Recent high-profile cybersecurity breaches like the SolarWinds intrusion have led to the EO, which is a comprehensive plan to better secure federal systems and protect critical infrastructure and data in the United States. Although the EO is focused on Federal systems and services the private sector provides to those networks, this infrastructure includes both public and private systems that are vital to national security and systems, which provide many essential services that underpin American society.

The EO accurately points out that "incremental improvements will not give us the security we need; instead, the Federal Government needs to make bold changes and significant investments." But even the most lofty and laudable goals have to be broken down into manageable steps before anything can happen. The old saying about eating an elephant one bite at a time isn't wrong. You have to start somewhere.

Start with Section 3

In the EO, Section 3 addresses modernizing Federal Government cybersecurity and cites a number of areas for improvement. Although the other sections of the EO are certainly important, taking the fundamental steps toward modernization outlined in Section 3 first can help move forward with progress on the requirements listed in the other sections as well.

At a high level, Section 3 of the EO states that agencies should accelerate migration to cloud technology, implement a Zero Trust architecture, improve cloud security, multifactor authentication and data encryption, centralize and streamline access to cybersecurity data to drive analytics, and improve communication and training.

Zero Trust Architecture

In Section 3, it states that agencies must move to a Zero Trust approach to security by implementing strong authentication capabilities, network access control technologies, and application access controls. Zero Trust Network Access (ZTNA) entails

Zero Trust verifies and authenticates user and device identify before every application session to confirm that they meet the organization's policy to access that application, and grants the least privilege necessary to perform the task at hand.

controlling access to applications. ZTNA verifies and authenticates user and device identify before every application session to confirm that they meet the organization's policy to access that application, and grants the least privilege necessary to perform the task at hand. A key element of the ZTNA concept is that access is independent of the location of the user. Users on the network should not enjoy any more trust than users who are located outside of the network perimeter or even working off the network. With ZTNA, the application access policy and verification process are the same in all cases.

Organizations should consider using firewall-based ZTNA because it consolidates and optimizes security operation and management in any environment, whether in the cloud, at the edge, or on-premises. This approach makes it possible to enforce a consistent access policy no matter where users, data, and computing resources may be located.

Modernization Needs to Happen Now

Meeting the requirements laid out in the EO isn't going to be easy, but it needs to happen. The best time to have modernized cybersecurity would have been years ago. The next best time is now. There's no time to waste because cyberattacks are becoming more aggressive and more damaging every day. Hackers certainly aren't delaying their activities and neither should we.

Learn more at www.fortinet.com/solutions/industries/government/federal. ■

About The Author

Mr. Richberg's role as a Fortinet CISO leverages his 30+ years' experience leading and driving innovation in cybersecurity, threat intelligence, and cyber strategy & policy for the U.S. Government and international partners.

Prior to joining Fortinet, he served as the National Intelligence Manager for Cyber, the senior Federal Executive focused on cyber intelligence within the $80B+/100,000 employee U.S. Intelligence Community (IC). He led the creation and implementation of cyber strategy for the 17 departments and agencies of the IC, set integrated priorities on cyber threat, and served as Senior Advisor to the Director of National Intelligence (DNI) on cyber issues.