

Top Five Takeaways:

Implementing Zero Trust Architecture for the Federal Government

Understanding how Executive Order 14028 Provides a Path to Improved Cybersecurity



A surge in breaches and ransomware attacks has pushed agencies to redefine their cybersecurity posture. Recent zero-day events—the SolarWinds and Colonial Pipeline incidents—uncovered by Mandiant, then a part of FireEye demonstrate the sophistication of today’s cyber attacks. Government security teams are also grappling with the blurred lines between operational technology (OT) and IT systems.

Recognizing this clear and immediate danger, President Biden issued Executive Order 14028 on May 12, 2021, titled “Improving the Nation’s Cybersecurity.” EO 14028 orders Civilian Executive Branch Agencies to aggressively implement cybersecurity-related activity and programs that will enhance government and industry’s ability to detect, respond and recover from cyber attacks.

Implementing EO 14028 requires an overarching cyber security strategy. Zero trust provides the underlying fabric. By adding layers of intelligence, validation and automation, federal agencies can ensure a modern approach that efficiently and effectively addresses the cyber attack landscape and meets the mission of the cyber security Executive Order.

Understand the Directives

The executive order directs all Federal Civilian Executive Branch (FCEB) agencies to dramatically improve their cyber capabilities in a variety of ways. Among the many directives are specific requirements for the adoption of technologies like endpoint detection and response (EDR), universal logging and threat hunting across all FCEB agencies. These capabilities leverage artificial intelligence and machine learning to improve threat detection and operate at scale.

With 74 actionable directives and a timeline of compliance spanning 30 days to a year, agencies have been hard at work changing their systems and processes in accordance with EO 14028. President Biden’s executive order also addresses the role of emerging technology in threat prevention and response. Section seven, “Improving Detection of Cybersecurity Vulnerabilities and Incidents on Federal Government Networks,” calls on agencies to deploy EDR solutions to monitor threats more proactively.

Take Stock and Understand Current Security Baseline

It’s important to understand what security practices and solutions your organization already has in place. Zero trust may seem daunting, but many federal agencies have already started down the path with capabilities such as single sign-on (SSO) or multi-factor authentication (MFA) for application access. There is no need to reinvent the entire wheel if you have pieces already in place.



Ask your security teams if you can leverage any cybersecurity solutions that you've already implemented to meet the EO requirements. If so, these investments will most likely also fit into your ZTA roadmap. Also ask your teams about the private sector vendors with whom your agency has relationships.

You'll want to know if they have the knowledge and government expertise to help you on your ZTA journey. Many providers offer Zero Trust-related solutions; however, they may not be aware of unique compliance and security requirements for government agencies.

Need for EDR

One of the directives that has many in industry paying attention is the mandate for all FCEB agencies to utilize EDR technology on their endpoints. The Cybersecurity and Infrastructure Security Agency (CISA) is working to help agencies that do not already have EDR deployed. CISA will soon be utilizing the deployed EDR solutions to facilitate its cyber threat hunting activities across agencies. This is one of the key elements of EO 14028 that can dramatically improve the government's cyber defense capabilities.

Need for Artificial Intelligence and Machine Learning

It's easy to see how various elements of EO 14028 will generate vast volumes of data. AI/ML tools will be required to derive additional insights from all the various data sets. Of course, successful implementation of AI/ML requires talented data scientists and access to the best data. Without these elements, AI/ML cannot effectively deliver on its promise.

When it comes to AI and ML, the quality and availability of data can make or break the entire mission.

If an agency's model is not based on real-world incident response, victim intelligence and artifacts the AI models won't be properly trained in detection and response, especially as some of the threat actors continue to become smarter. If agencies can't cross-correlate against their environment and train their AI to recognize threat signals from noise they will get into a cycle of false positives or false negatives.

Extended Detection and Response (XDR)

The need to combine and analyze so much attack data leads inexorably to an XDR solution. By quickly and effectively compiling and contextualizing threat data across multiple threat vectors, organizations achieve increased threat visibility, as well as rapid threat response and mitigation.

While the executive order does not specifically issue directives on the use of XDR solutions, the functional requirements called out in Section seven ("Improving Detection of Cybersecurity Vulnerabilities and Incidents on Federal Government Networks") and Section eight ("Improving the Federal Government's Investigative and Remediation Capabilities") map directly to XDR solutions — and the AI/ML capabilities embedded within.

About World Wide Technology

World Wide Technology (WWT), a global technology solutions provider with \$13.4 billion in annual revenue, combines the power of strategy, execution and partnership to accelerate transformational outcomes for large public and private organizations around the world. Through its Advanced Technology Center, a collaborative ecosystem of the world's most advanced hardware and software solutions, WWT helps customers and partners conceptualize, test and validate innovative technology solutions for the best business outcomes and then deploys them at scale through its 4 million square feet of global warehousing, distribution and integration space. For more information, visit wwt.com.

About FireEye

McAfee Enterprise and FireEye combined in October 2021, bringing together their portfolios and expert teams to create a market-leading security company. With proven technology and unrivaled experience, the company serves more than 40,000 enterprise, commercial, and government customers worldwide. The new company blends innovative technology, intelligence, and automation to help solve the most complex cybersecurity problems for its customers. For more information, visit freeeye.com

About Mandiant

Mandiant brings together the world's leading threat intelligence and frontline expertise with continuous security validation to arm organizations with the tools needed to increase security effectiveness and reduce organizational risk. For more information, visit mandiant.com