FORTINET FEDERAL

ISSUE BRIEF

Zero Trust Integration: Taking a Holistic Approach to Cybersecurity

In May 2021, President Biden issued a sweeping Executive Order on Improving the Nation's Cybersecurity (cyber EO), which included 11 sections of guidance and mandates designed to push Federal agencies to improve their cybersecurity posture and modernize their infrastructure to better protect the American people and our nation's sensitive information and assets.

The cyber EO came on the heels of high-profile cyberattacks that plagued public and private sector organizations, including the Colonial Pipeline attack that caused gas shortages along the East Coast and several breaches of software widely used across both the public and private sectors. These incidents highlighted the cybersecurity vulnerabilities within government agencies and across our nation's critical infrastructure.

Aligning Cybersecurity Under the EO Mandates

The mandates laid out in the cyber EO focused attention on agencies' adoption of zero trust operating principles for on-premises, hybrid, and cloud-based operations. The EO established goals and aggressive timelines that drive action by agencies, IT and security technology providers, contractors, and employees. Government agencies, including the National Institute of Standards and Technology and Cybersecurity and Infrastructure Security Agency, released strategy documents, technical references, maturity models, and capability documents to help agencies develop their individual paths to meet the requirements set forth in the cyber EO.

Many of the mandates involve building a zero trust architecture. Zero trust is a network security philosophy that assumes access and privileges should not be granted to users or devices based solely on their physical or network location. A zero trust architecture requires users and devices to be authenticated and authorized before accessing the agency network, applications, and data.

When the connection is established, the user is monitored and must undergo new verification, and is only granted the level of privilege needed for the task at hand when moving around the network, accessing a new application, or upon a change in behavior or activity. The latter is an increasingly important aspect of zero trust architecture; technologies that monitor user and device behavior, and detect potential malware infections, are incorporated in the application access decision process.

Implementing a zero trust architecture involves people, process, and technology. Building zero trust solutions is a process rather than a single upgrade, and separate functions such as identity management, access control, and policy enforcement have interdependencies that agencies need to consider during implementation. For example, establishing controls and security policies that aren't matched with sufficiently powerful technology solutions for execution can result in slow performance, unhappy users, and even an inability to accomplish core agency functions.

Considering the Human Side of Zero Trust

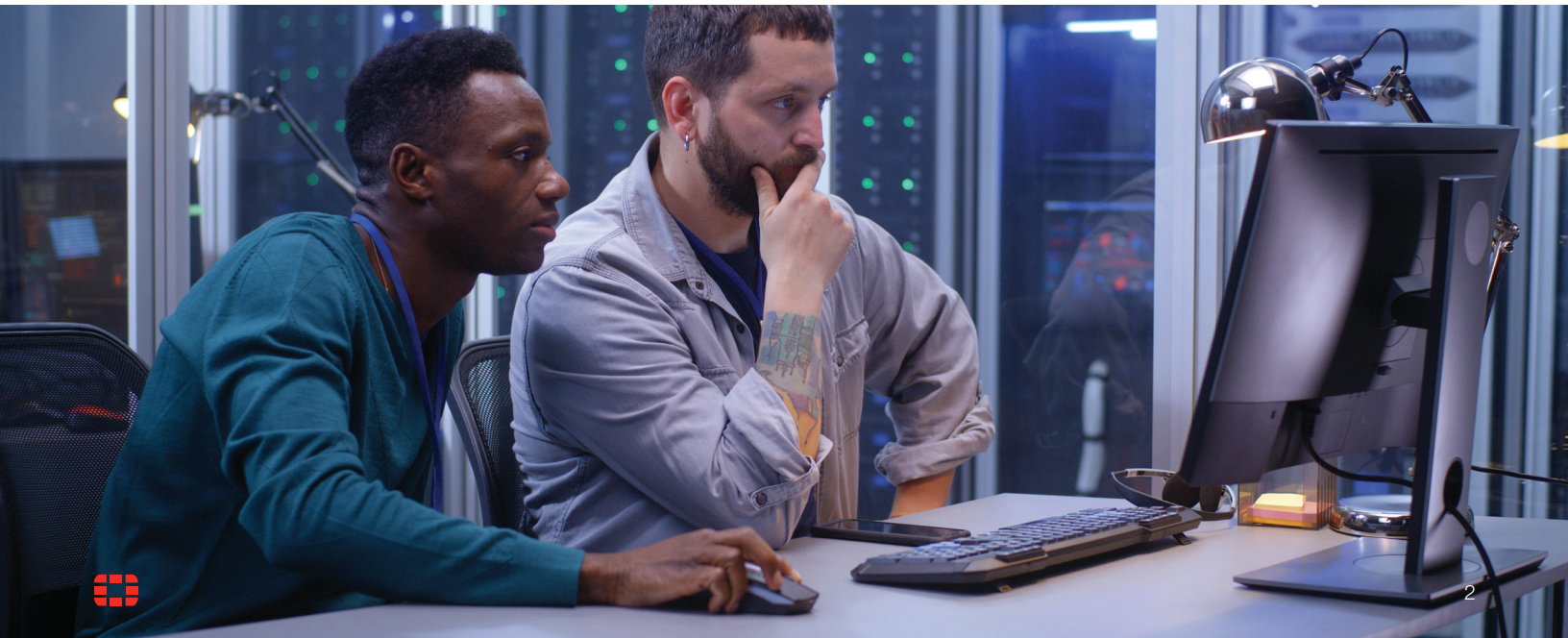
People are vital; both the user population and the workforce that builds and operates zero trust solutions are every bit as important as processes, architectures, and technologies. Federal agencies need to look at the human side of zero trust.

- This starts with explaining to users what zero trust is – and is not, as well as demonstrating how zero trust can empower and enable them. For those not steeped in cyber jargon, the label 'zero trust' can have Orwellian connotations of surveillance and distrust that are especially off-putting to workers focused on public service, many of whom have security clearances. Explaining zero trust in clear terms and showing how it can provide capabilities to enable work from anywhere while providing a safety net to minimize the consequences of user error can go a long way to making the concept more user friendly and easing its adoption in the workplace.
- Government technology teams accustomed to fixing problems reactively may find it difficult to step back from their day-to-day work to approach zero trust from a holistic perspective. Addressing an individual component of zero trust, such as multifactor authentication, fixes an immediate issue – or meets an individual mandate – but often doesn't achieve an integrated zero trust architecture.
- Similarly, some in government may not even realize they are already doing elements of zero trust. Educating procurement teams on what zero trust is, how each piece works, how the pieces connect, and why achieving zero trust is important will support agencies in acquiring the commercial capabilities they need to implement zero trust.

Achieving Integrated Zero Trust Security With a Cybersecurity Mesh Architecture Approach

The approach to security based on network locations and perimeters was often characterized by numerous point products, each focused on solving a separate problem in a non-integrated fashion. By contrast, a cybersecurity mesh architecture – or as Fortinet calls it, a Security Fabric – integrates capabilities across the breadth of the computing environment of an agency, providing broad threat coverage, protection, and even automated response. This approach turns the size and complexity of the digital attack surface of an agency from a liability into a potential advantage. It becomes a smart sensor platform that uses artificial intelligence and machine learning to understand normal and abnormal network activity in real time and determines what abnormal behaviors are malicious or potentially harmful. A cybersecurity mesh zero trust-based architecture can both minimize the likelihood and the consequences of a breach.

The cyber EO sets the end goals, but agencies can build their own unique roadmap to reach holistic cybersecurity with a zero trust architecture. Fortinet partners with technology teams to help them make cybersecurity upgrades in a way that makes sense for each agency based on its current environment, needs, and mission. Fortinet's platform-based approach offers an open ecosystem that not only incorporates Fortinet zero trust security technologies that protect more than 50 aspects of networking, computing, and connectivity, but also interoperates with more than 480 products from other vendors.



Hybrid Environments

To ensure consistent security, improve visibility, and streamline management across the enterprise, agencies need solutions that operate in multiple environments, from public clouds to on-premises data centers, and that are connected via a cybersecurity mesh architecture. The cyber EO pushes agencies toward the cloud, but not all Federal agencies are ready, willing, or able to move all of their applications and operations to the cloud. Technology teams operating on-premises environments may not fully understand that a zero trust architecture can be applied to all environments, including hybrid ones.

Fortinet's Security Fabric offers the same identity and access management capabilities for applications and networks in the cloud and on-prem environments. Technology teams benefit from the ability to provision the same security rules across all environments and to monitor enterprise-wide operations through a centralized dashboard. End-users benefit from seamless access to all of their data and applications.

Component Integrations

The first step to full zero trust security is to understand the zero trust functions that an agency's security capabilities already offer and then to fill in any gaps. Fortinet partners with technology teams to move cybersecurity solutions that are already working for them into its cybersecurity mesh, and then adds and integrates other components to meet zero trust outcomes. This approach saves time and budget. Technology teams aren't starting from scratch; they are using tools they already have and adding capabilities and technologies as needed to their portfolio, making the move to a zero trust architecture less daunting.

Trusted Users

End users and devices are allowed to access data and computing resources based on validated security policy permissions that are automated and centrally managed. With a cybersecurity mesh-based approach, security policies can be matched with the needed security capability, ensuring that the user experience is seamless.

Embracing Zero Trust With Fortinet

With Fortinet's platform approach, agencies can get teams across the organization onboard with zero trust security and build a logical path to integrated implementation to achieve the spirit of the cyber EO in a way that makes sense for them. Approaching zero trust from this perspective enables agencies to:

- Implement best-of-breed solutions from multiple vendors
- Approach technology upgrades incrementally, which ensures integration of each component
- Manage cybersecurity from a centralized dashboard that provides enterprise-wide visibility into trusted access – and abnormal behavior
- Reallocate security operations staff from routine to high-level activities, speeding response to real threats
- Provide agency employees with a seamless – yet secure – user experience
- Create a virtuous circle by adding more solutions to a common platform, reducing the need for specialized training on every new solution, and closing gaps in cybersecurity coverage

Learn how your agency can accelerate its implementation of the cyber EO and achieve fully integrated zero trust security at Fortinet Federal.

FORTINET FEDERAL®

www.fortinet.com

April 23, 2022 8:42 AM