citrix | Public Sector

White Paper

Things to Consider Regarding the Executive Order on Cybersecurity

How it Works

We have recently seen several high-profile Cybersecurity breaches hit the news stands. The breaches vary from compromise of the supply chain that affected over 18,000 organizations, to compromise of a major pipeline provider which had an impact on fuel prices, to major exploits in enterprise software.

In response to these types of threats, on May 12, 2021, the Biden Administration released an Executive Order seeking to modernize the approach that government takes to cybersecurity. This order not only focuses on steps that government agencies must take to modernize their cybersecurity approach, but also puts pressure on suppliers to take measures to be more transparent and take actions to better protect the supply chain.

The serious impact of these incidents highlights that the existing approach to cybersecurity needs to change.

Things You Should Consider

The traditional security in depth approach where you harden around the network perimeter and layer security into your network infrastructure is not enough. The traditional approach is an approach based on trust, where as long as you have authorization, you have access to resources. This model is not effective from willing or unwilling internal threats.

How do agencies go about adopting a new approach when the variables are complex and ever changing?

Especially since:

- **Users:** Are located in physical offices, public locations, and at home.
- **Devices:** Can vary between mobile, GFE, Bring Your Own Device (BYOD).
- **Applications:** Are delivered in various ways such as Intranet/SaaS, browser, virtualized, mobile.
- **Data access and storage:** Are located in various locations—on-prem and cloud.

Enable remote access without VPN

Remote users need easy access to web applications but relying on traditional VPN solutions can create significant security risks. If bad actors can gain access through the SSL VPN, they have free reign over your entire network. You need a contextual security solution to meet zero trust requirements while enabling BYOD and access to apps deployed in a cloud. Citrix Cloud Government provides a secure space to work by enabling users to **remotely access web applications deployed on premises using any device**—without needing to access the entire network.

Adopt a contextual approach to Access and Identity

Citrix's identity approach allows agencies to preserve their investments. It allows them to use the native IdP security capabilities like MFA, Smart Cards, PIV/CAC, and biometrics to protect the user. It supports LDAP, RADIUS, TACACS, Diameter, and SAML2.0 authentication mechanisms, among others to provide **single sign on to Enterprise, SaaS, mobile, and Cloud-based applications**.

Your approach should provide provide **flexibility to balance user convenience with risk**. Based on the user context, a user can be granted full access, reduced access, quarantine, or no access at all. For example, a user who fails a device compliance check can get access to a reduced set of applications. Sensitive resources can have restricted functionality like blocking printing and downloading. Access can be restricted at the network layer before the user reaches the back-end resource.

Create a secure digital perimeter

By adopting digital workspaces, it becomes easier to create a **digital perimeter** around your valuable assets. This digital perimeter empowers agencies with insight and control into how users are interacting with apps and data so agencies can **better protect against data exfiltration**. The secure digital perimeter extends to the user, the edge, data centers, and clouds, making it easy to enforce continuous authentication and monitoring while restricting actions users can take depending on their state, like copying and pasting, printing, and downloading.

A secure digital perimeter:

- Manages and provides data to **assess device trust**.
- Configure **multiple authentication steps** to access confidential data based on user role, location, device state, and more.
- Create an containerized environment for providing **secure access to the internet**.
- Allows for **secure exchange of confidential agency data**.
- Provides **continuous monitoring** and assessment of risk.

Learn More

Articles

- What is Zero Trust Security?
- Tech Brief: Zero Trust
- Simplify your move to multi-cloud

Videos

- A Zero Trust Approach to Security for a Hybrid Work World (44 sec)
- A zero trust model: continuous security for remote digital technology users (49 mins)

Accelerate movement to cloud services

As agencies increase their speed of cloud services adoption, one of the challenges that they face is maintaining governance and compliance across multi-cloud architectures. To ensure operational and features consistency for all your applications across cloud and on-premises environments, agencies need an application delivery solution with a single code base. This empowers IT with holistic visibility for multi-cloud environments through a **single pane of glass** and gives you a **consistent and strong security posture**—all while providing a great application experience for end users.

Protect any application whether it is a **monolithic or microservices-based app**, anywhere, with a holistic security approach that combines security controls such as bot mitigation and volumetric DDoS protection with the proven Citrix web application firewall solution.

citrix | Public Sector

US Public Sector Sales
1-800-424-8749 x26603 | https://www.citrix.com/solutions/government/

Locations
Corporate Headquarters | 851 Cypress Creek Road, Fort Lauderdale, FL 33309, United States
US Public Sector Offices | 7735 Old Georgetown Road, Suite 300, Bethesda, MD 20814, United States