White Paper

Best Practices for Extending Zero Trust to Government Networks

Forescout As the Foundation of Your Agency's IT, OT & Iot Zero Trust Strategy

Table of Contents

In May 2021, President Biden issued the Executive Order on Improving the Nation's Cybersecurity (EO).[i] The order revamps how the federal government protects its digital infrastructure, leveraging Zero Trust.

Zero Trust is the foundation of a comprehensive security strategy for most civilian agencies, especially with an increasingly remote and mobile workforce. More work is being done outside office walls on devices that the agency may not have issued. That makes Zero Trust the ideal architecture for departments that need to protect digital assets and provide flexibility for employees and contractors working offsite.

By definition, Zero Trust assumes no asset is inherently trusted. It is rooted in the concept of "never trust and always verify" and requires users to prove they are who they say they are. Access is denied until a user or asset proves their identity.

It's important to remember that Zero Trust is a security design approach and not a single, fixed solution or technology that can be purchased and implemented. To implement Zero Trust effectively, agencies should think holistically about the strategy and practices across all areas of the agency's digital infrastructure, including network devices, and:

- Determine which resources and data should be accessible and which should not
- Understand potential vulnerabilities
- Identify potentially harmful software on connected devices
- Ensure all devices are compliant with regulatory requirements
- Take inventory of software and applications

Agencies can apply Zero Trust approaches to any cloud or on-premises environment through any device—desktop, laptop, or even Internet of Things (IoT).

The Federal Adoption of Zero Trust

There are several strategies and policies that agencies can use to find their way in their Zero Trust journey. Each of these strategies points out the

[i] The White House "Executive Order on Improving the Nation's Cybersecurity," May 12, 2021, https://www.whitehouse.gov/briefing-room/presidential-actions/2021/05/12/executive-order-on-improving-the-nations-cybersecurity/

importance of a comprehensive approach to Zero Trust and reinforces the need for managing down to the individual device level. In a modern Zero Trust Architecture (ZTA), the focus is on protecting "resources (assets, services, workflows, network accounts, etc.), not network segments, as the network location is no longer seen as the prime component to the security posture of the resource."[ii]

The White House Office of Management and Budget (OMB) on September 7, 2021, issued a draft of the Federal Zero Trust Strategy[iii] to help agencies adapt their enterprise security architectures based on Zero Trust principles. It includes:

- Consolidating identity systems
- Ensuring strong multifactor authentication
- Treating internal networks as untrustworthy
- Strengthening application security

In parallel, the Cybersecurity and Infrastructure Security Agency (CISA) released the Zero Trust Maturity Model.[iv] This is a roadmap for agencies to reference as they transition to ZTA. The model includes five pillars and three cross-cutting capabilities, all based on the foundations of Zero Trust. The pillars are:

- Identity
- Device
- Network/environment
- Application workload
- Data

CISA also operates the Continuous Diagnostics and Mitigation (CDM) program. CDM provides agencies with the tools and capabilities that find and prioritize risks and requires agencies to share data to the CISA dashboard. CDM-provided tools can help automate monitoring and threat identification to protect assets better and share data about those assets in an easier way. The program requires agencies to continuously monitor their environment and automate threat analysis for all devices. CDM is seen as a gateway to Zero Trust. It allows an agency to utilize trusted enterprise-grade tools to help establish policy decision controls that map back to both the CDM core tenets and future ZTA initiatives.

Securing Network Devices Is Essential

The proliferation of network devices and IoT devices has created a large and multiplying threat surface for attackers. IoT can include everything from sensors to security cameras to printers to smart thermostats. The increasing number of wearables like smartwatches, medical devices, or even car key fobs mean new potential paths of entry. The increase of IoT in the workplace or brought in from the outside introduces new and emerging threats. Adding to the threat, user and device interactions will often function as "shadow-IT," bypassing on-premises, perimeter-based defenses.

As a result, the biggest cyber threats aren't well-protected laptops or desktops, but the devices employees and contractors bring to work or use every

[ii] NIST SP 800-207, https://csrc.nist.gov/publications/detail/sp/800-207/final

[iii] The White House "Office of Management and Budget Releases Draft Federal Strategy for Moving the U.S. Government Towards a Zero Trust Architecture," September 7, 2021, https://www.whitehouse.gov/omb/briefing-room/2021/09/07/office-of-management-and-budget-releases-draft-federal-strategy-for-moving-the-u-s-government-towards-a-zero-trust-architecture/

[iv] CISA "Zero Trust Maturity Model," https://www.cisa.gov/publication/zero-trust-maturity-model

day in agency activities. The need for complete device visibility (along with agent-based and user authorization-based visibility) is a foundation of all cybersecurity practices. It will be no different for many as they move to a more robust ZTA. By applying "never trust and always verify" principles, requiring every device to validate its trust for every connection it wants to establish, agencies add another critical layer of cybersecurity protection. But how can agency teams do this efficiently and effectively?

Forescout Extends Zero Trust Capabilities to Network Devices

Pivoting from a perimeter-focused defense posture to Zero Trust requires a shift in thinking and tools. Enabling equal and continuous authentication and security on all devices can be difficult if you don't have the right platform to leverage.

Forescout understands government needs and the new federal security standards because we've been helping agencies build towards Zero Trust environments for years. In July 2021, the Forescout platform's capability was recognized and selected to serve on the National Institute of Standards and Technology's (NIST) National Cybersecurity Center of Excellence's (NCCoE) "Implementing a Zero Trust Architecture Project" to help shape and build Zero Trust design. Our emphasis is to help the federal government develop a practical Zero Trust strategy that extends protections to all devices and can stand up as the standard for the public sector to follow.

Comprehensive Device Visibility

Zero Trust requires clear visibility into network devices to understand what they are and what users are doing with them. The Forescout platform provides monitoring with a full suite of capabilities that enable and enhance Zero Trust security by:

- Providing visibility and assessing devices connected to your network
- Monitoring devices for real-time risk management
- Quickly deploying segmentation across your network
- Enforcing security policies for all devices
- Sharing data across your security infrastructure

The Forescout platform operates on agency-issued devices and guest devices to provide a clear view of every endpoint that touches a system. The platform quickly identifies the user, what device they're using, the version of the device's operating system, and what security platform is being used. Devices that meet internal standards can connect. Those that don't are flagged and remediated.

How Forescout Protects Agencies as IT and OT Converge

As IT (information technology) and OT (operational technology) become increasingly integrated and reliant on off-the-shelf technology, managing the convergence and the associated risks is now critical for agencies to become more efficient, reliable, and secure. Forescout helps protect the data, networks, devices, and services, called Enterprise of Things (EOT), that agencies rely on to service the workforce and citizenry by addressing these common public sector use cases:

Agency Need	Forescout Capabilities	Benefits	Use Case
Access Control	Detect all endpoints connected to a network, including rogue devices, and assess, enforce access policies, and monitor activity	Limit access to data, systems, and applications and identify devices that should and shouldn't be connected	Personal smartphones brought into the workforce are unable to connect to the workplace Wi-Fi
Incident Response	Provide a full understanding of a device to determine potential vulnerabilities; an automated response can block a device in seconds	Policy-driven remediation is done immediately to stop rogue devices before they get started and save staff time and resources	A laptop running an old, unpatched version of Windows is blocked from network access
Supply Chain	Understand software–and malware–running on connected devices	Identify potentially harmful software or scripts and block devices running them	An employee downloads questionable software and is automatically blocked from access
Compliance	Ensure that all devices are running prescribed software and are configured correctly to meet government directive needs	All devices are approved before connection, meeting Zero Trust and NIST 800 compliance recommendations	Agencies will mitigate cybersecurity threats and attacks by meeting compliance standards set by NIST and CISA
Software Inventory	Identify unused applications or gain visibility of unauthorized applications, operating systems, or unpatched software	Find unnecessary or underutilized software that can be removed to save money and resources	A long-forgotten SaaS platform is removed due to lack of use

Table 1: How Forescout helps government agencies

Start with a targeted use case

Know what is on your network

Baseline existing traffic

Automate policy creation

Monitor and enforce compliance

Learn more at Forescout.com

Forescout Technologies, Inc.
190 W Tasman Dr.
San Jose, CA 95134 USA

Toll-Free (US) 1-866-377-8771
Tel (Intl) +1-408-213-3191
Support +1-708-237-6591

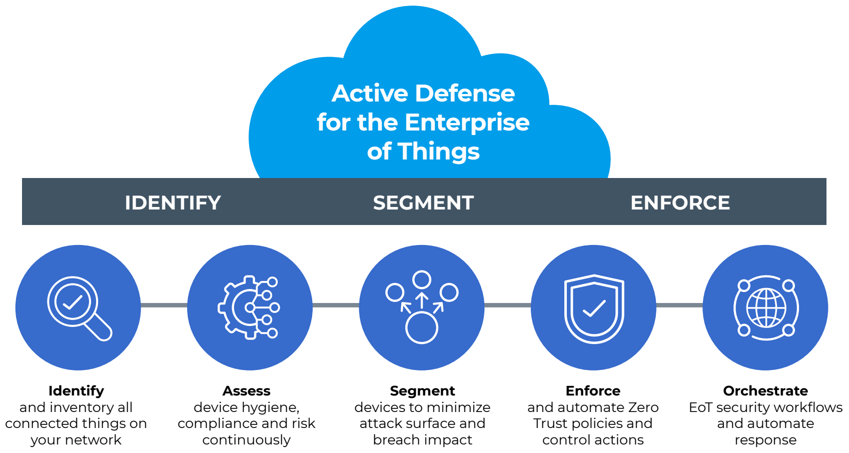
Active Defense for the Enterprise of Things
IDENTIFY
SEGMENT
ENFORCE
Identify and inventory all connected things on your network
Assess device hygiene, compliance and risk continuously
Segment devices to minimize attack surface and breach impact
Enforce and automate Zero Trust policies and control actions
Orchestrate EoT security workflows and automate response

Figure 1: Forescout as a Zero Trust platform

Forescout Is the Right Solution for Extending a Zero Trust Environment

Zero Trust cannot be fully implemented without absolute visibility into devices that are connected—or attempting to connect—to your network. All must be identified and classified so that governance policies can immediately be applied. Data moves with devices, meaning that the focus must be on endpoints and devices. And a single layer isn't enough. Multiple layers of security should be standard—integrated with network security—and multifactor authentication a requirement.

The Forescout platform is a holistic and comprehensive device visibility and management solution that protects networks from the devices traditional platforms cannot. Guest devices, BYOD, machine sensors, IoT products, and virtual machines are all handled seamlessly by the Forescout platform.

Forescout is working with agencies and departments to establish best practices, which include:

- Establishing device identification and fingerprint
- Determining access parameters
- Understanding potential risks from configuration or vulnerabilities
- Identifying harmful and outdated software
- Ensuring devices are compliant with government directives and policies
- Keeping an active real-time inventory of software and applications

Forescout has helped government IT and security professionals protect data and secure access to government resources to keep the lives of citizens free from disruption all over the country. We can help your agency successfully implement a modern Zero Trust environment to keep government operations available, secure, and compliant too. Experience the difference the Forescout platform can make for your agency. Schedule a demo today to get started.