Gigamon®

Guide to Zero Trust for Federal Agencies

How to Get Started with Your Zero Trust Journey

Table of Contents

Introduction 3

What Is Zero Trust? 4

Why Do You Need Zero Trust Now? 5

Zero Trust Is a Journey — with Benefits All Along the Way 6

Questions to Ask on the Journey to Zero Trust 7

Where Are You on Your Zero Trust Journey? 8

About Gigamon 8

Introduction

The frequency and relentlessly increasing sophistication of cybersecurity attacks on federal agencies has led to one simple truth: We can no longer implicitly trust the users, devices and applications on our networks. This is the concept behind the move towards Zero Trust, which is rapidly becoming the default position for federal chief information officers (CIOs) and chief information security officers (CISOs).

BACKGROUND READING
For background, read these two recent reports about Zero Trust.

- "The Road to Zero Trust" by the Defense Innovation Board
- "Zero Trust Cybersecurity Trends" by the American Council for Technology-Industry Advisory Council (ACT-IAC)

The Zero Trust model is built on these guiding principles:

- The network must always be assumed to be hostile
- External and internal threats exist on the network at all times
- Locality is not sufficient for deciding trust in a network
- Every device, user and network flow must be authenticated and authorized
- Security policies must be dynamic and determined from as many data sources as possible

This guide, written by Gigamon, the leader in networking and security, provides our recommendations on Zero Trust and demonstrates ways federal agencies can design and implement Zero Trust architectures around the key concepts of network and data visibility.

Federal agencies and networks often have specific needs:

- They rely on legacy applications and platforms that span multiple hardware and software generations
- They often house extremely sensitive data in secure facilities
- They are often under continuous attack from multiple actors, including hostile nation-states

What is Zero Trust?

The Zero Trust concept focuses on establishing effective perimeters around sensitive and critical data. The perimeters include traditional prevention technology, such as network firewalls and access control, but also authentication, logging and controls at the identity, application and data layer levels.

Many Zero Trust concepts are rightly compared to established best practices, such as defense-in-depth and assume breach. Zero Trust is, in fact, an evolution of those concepts and the resulting architectures, not a radical new approach.

Still, even as the concepts are familiar, implementing Zero Trust, especially in federal agencies, is complicated for a number of reasons, including:

- Many federal agencies rely on multiple generations of IT assets distributed across physical, virtual and cloud environments
- Many agencies are under continuous attack from bad actors, ranging from disgruntled individuals to well-organized and financially motivated criminal syndicates and hostile nation-states

A big challenge is that any progress toward Zero Trust must be done in flight without any degradation of the agency's current security posture and capabilities.

FALLING IN LINE WITH THE ACT-IAC REPORT
For government agencies, implementing a Zero Trust model helps meet the target outcomes identified by the ACT-IAC report:

- Creating more secure networks
- Making data safer
- Reducing the negative impacts of breaches
- Improving compliance and visibility
- Reducing overall cybersecurity costs
- Improving the security and risk posture of the organization

“Many Zero Trust concepts are rightly compared to established best practices, such as defense-in-depth and assume breach. Zero Trust is, in fact, an evolution of those concepts and the resulting architectures, not a radical new approach.”

Why Do You Need Zero Trust Now?

Just read the news to learn why Zero Trust has become so critical. We live in a world where security is breached and data is stolen daily. Those attacks are supremely disruptive, impacting everything from the privacy of an individual's financial and health data, to the integrity of our government operations and institutions, including national security.

We've reached a tipping point, where progressing toward Zero Trust must be a goal for federal agencies. The path to Zero Trust can vary, and no two agencies need to follow the same strategy, but it's important to take the first step now.

The good news is that regardless where you start, with every step you take toward Zero Trust you will bolster the security of your assets, data and mission.

> The purpose for a Zero Trust architecture is to protect data. A clear understanding of an organization's data assets is critical for a successful implementation of a zero-trust architecture. Agencies need to categorize their data assets in terms of mission criticality and use this information to develop a data management strategy as part of their overall ZT approach.

Source: ACT-IAC, Zero Trust Cybersecurity Current Trends, April 18, 2019

Zero Trust Is a Journey — with Benefits All Along the Way

Many vendors claim that achieving Zero Trust is as simple as buying their products. The reality is much more complex. A Zero Trust model simply cannot be designed and implemented overnight. It is a journey toward an outcome that in some of the most complex federal environments may never be fully realized.

However, developing a Zero Trust Architecture (ZTA) will build an extensive set of foundational capabilities that deliver security and operational benefits all along the way.

1

Foundational Capabilities

First up, foundational capabilities, which are identified as:

- Asset inventory and management of network assets, including:
  - Application inventory, including legacy applications
  - Data inventory
  - Remote access methods
- Continuous data identification and classification
- Two-factor authentication (hardware device or token-based)
- Central Identity Credential Access Management (ICAM) for both users and applications
- Fine-grained user groups and permissions, based on job role and data access needs

2

Application Capabilities

Once you have inventoried your assets, develop the following application capabilities:

- Integration between applications and central ICAM
- User groups and role-based permissions at both application and data layers
- Application developer training to leverage ICAM
- Robust access logging to the central log-management platform
- Continuously updated development standards and architectures
- Development plans to phase out or migrate legacy applications

3

Security Capabilities

Next, overlay security capabilities on the application capabilities, for example:

- Data architectures and schemas to support visibility & security
- Application visibility through decrypted network traffic, access gateway (proxy) and application logs
- Security Information and Event Management (SIEM) to write rules and detection on top
- Network-layer visibility
- Device or endpoint visibility
- Application logging and visibility
- Identity logging and visibility
- Data-layer logging and visibility

4

Training and Support Capabilities

Finally, develop and implement robust and continuous training and support capabilities to strengthen the human element of Zero Trust, which too often proves to be the weakest link.

- Classify users into role- and level-based groups and identify training requirements for each group
- Then provide training and support for each group, new users, existing users and application developers

Questions to Ask on the Journey to Zero Trust

As we have said, there is no right or wrong path to Zero Trust. However, there are questions you should be asking at every stage of the journey.

1

How Well Do You Know Your Network Assets?

Every Zero Trust initiative must start with understanding the hardware and software assets within your organization. Gaining that understanding — and maintaining it in an ever-changing IT landscape — maps to Phase 1 of the DHS Continuous Diagnostics and Mitigation (CDM) program, namely, the automation of hardware and software asset management and configuration settings.

Once the management of your assets has been automated, you will have a real-time, accurate register of the assets you must safeguard.

2

How Is Data Managed in a Zero Trust World?

Unlike traditional, user-centric data management strategies (for example, the user's role defines their level of data access), in a Zero Trust world, this strategy must become data-centric.

In this model, based on the sensitivity of the data, you would build concentric defenses starting with data access controls at the storage layer that enforce strong authentication of the devices, users and locations that attempt to access this data.

3

Who Has Network Access and Why?

Historically, most network threats have come from its users who were implicitly trusted by their agency. In a Zero Trust model, in contrast, every user, device, application and network flow must be authenticated and authorized.

At the user level, it is critical to know what level of data access has been granted to employees, contractors or third parties, and to continuously review, update and, where necessary, revoke that access.

4

Does Zero Trust Mean Perimeterless?

In a word, no. Zero Trust Architectures apply the concept of perimeters to what is often called the micro-segmentation level. In this model, it is no longer just the network perimeter that needs to be secured. The Zero Trust Architecture also needs to secure the application layer and associated data and the compute containers and virtual machines that are typically the foundation of this layer in non-legacy IT environments.

5

Do You Have the Data Visibility You Need to Support a Zero Trust Architecture?

End-to-end visibility across the network, in order to segment, isolate and control network data, is critical for Zero Trust Architectures. Visibility must be informed, governed and enforced, and it requires you to develop security policies that are both dynamic and built from many data sources.

Gaining visibility into encrypted traffic presents a particular threat because encrypted traffic can conceal a malicious payload. Use whatever approach to manage encrypted traffic that works for your agency.

6

Are You Using Tools That Free Up Your People?

To ensure that an agency can continuously monitor the Zero Trust network, use tools to automate as many of the routine network management tasks as possible.

It's important to note, however, that such tools must do more than simply automate tasks. They must also be able to quickly identify, isolate and analyze exceptions to expected traffic patterns or behaviors. With the increasing number, variety and sophistication of threats, automation and analytic tools are essential components that save time and effort that you can then apply to higher value functions, such as threat detection and response.

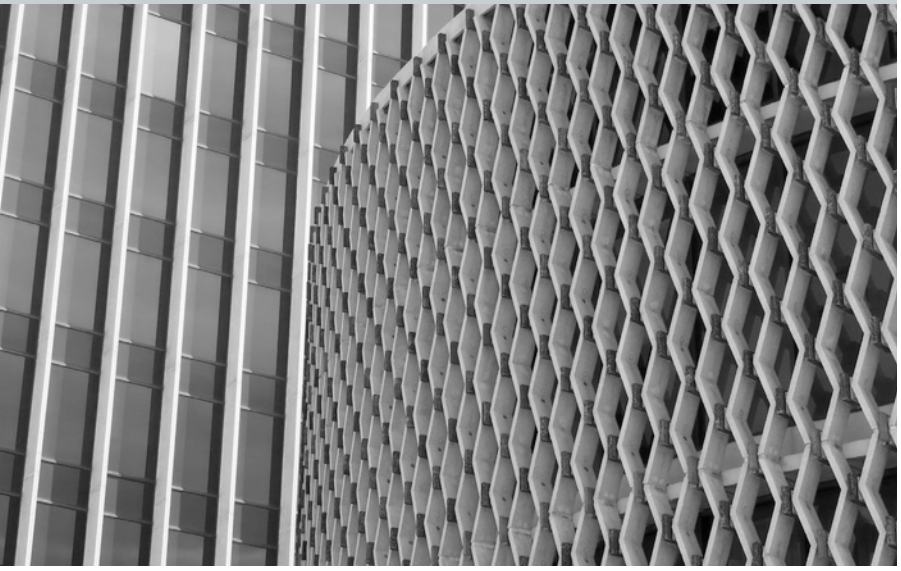
Where Are You on Your Zero Trust Journey?

While almost all agencies are considering Zero Trust models, only about 35 percent have started to implement this approach. Have you taken those first critical steps?

If you haven't yet started the implementation process, many models and resources are available to help you on your way. Many of the federal CIOs and CISOs who were early adopters of Zero Trust are already sharing information on how best to deal with some of the complexities that they have encountered.

And regardless of where you are in the implementation process, Gigamon can help you on your way. In fact, many of the leading federal agencies already rely on Gigamon to support their public-service missions, and we stand ready to support your efforts too.

The Gigamon Deep Observability Pipeline, including capabilities such as SSL/TLS Decryption, can accelerate and de-risk your Zero Trust efforts. Contact Gigamon to learn how we can help your agency establish a solid foundation for your Zero Trust journey. Please visit the federal government section of our website for more information.



About Gigamon

Gigamon offers a deep observability pipeline that harnesses actionable network-level intelligence to amplify the power of observability tools. This powerful combination enables IT organizations to assure security and compliance governance, speed root-cause analysis of performance bottlenecks, and lower operational overhead associated with managing hybrid and multi-cloud IT infrastructures. The result: Modern enterprises realize the full transformational promise of the cloud. Gigamon serves more than 4,000 customers worldwide, including over 80 percent of Fortune 100 enterprises, nine of the ten largest mobile network providers, and hundreds of governments and educational organizations worldwide. For more information about the Gigamon Platform or to contact a local representative, please visit: gigamon.com.

NIAP

TAA COMPLIANT

COMMON CRITERIA

DODIN

LEVEL 2

NEBS

Gigamon®

Worldwide Headquarters
3300 Olcott Street, Santa Clara, CA 95054 USA
+1 (408) 831-4000 | gigamon.com

06.23_02