Ping Identity

Lay the Foundation for Zero Trust

Uplevel Federal ICAM for Continuous, Risk-Based Identity Security

EBOOK

Table of Contents

Introduction:

Zero Trust is No Longer an Option

Zero Trust has been a topic of discussion in the Federal Government for some time. However, the approach to these discussions has recently changed. Previously, conversations revolved around why you should implement Zero Trust. But especially with the release of the cybersecurity Executive Order and Memorandum M-22-09, it's now about why you must.

As an identity-centric security framework, a strong identity foundation is necessary for a successful Zero Trust implementation. Unfortunately, the legacy identity, credential, and access management (ICAM) technologies frequently found in Federal environments can't provide the foundation required.

This means you'll need to re-examine the capabilities of your identity infrastructure and enhance them wherever possible, as soon as possible. However, this doesn't mean you'll need to rip and replace your entire infrastructure.

Continue reading to learn more about:

- The use cases that elevated Zero Trust from a "nice to have" to a "must have"
- The infrastructure challenges standing in the way of many organizations' Zero Trust implementations
- How to overcome these challenges to lay the foundation for Zero Trust—without ripping and replacing

The Mission-Critical Use Cases Zero Trust Must Address

Use Case 1:
Supporting the Hybrid Workforce

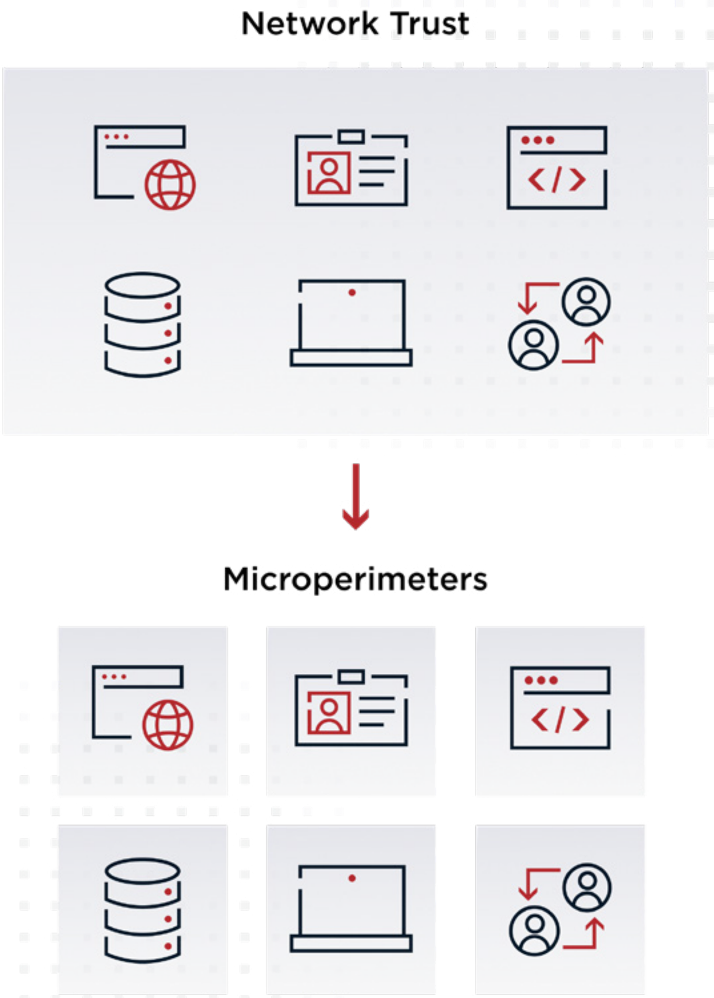
Due to the COVID-19 pandemic, the government's workforce transitioned to a hybrid model practically overnight. Now, it's clear that the hybrid workforce is here to stay.

Traditionally, an organization's security was based on a strong network perimeter. Generally, any user, resource or activity within the perimeter was considered safe while anything outside the perimeter was risky.

However, the shift to hybrid work rendered this approach insufficient. Users, resources and activity increasingly moved outside the perimeter, so proximity to the perimeter would no longer serve as an adequate measure for determining trustworthiness.

To address this challenge, Zero Trust calls for the end of the traditional network perimeter and the establishment of micro-perimeters. Micro-perimeters group resources by risk level, so the higher the resources' risk level, the stricter the micro-perimeter's security measures.

This means that user requests need to be deemed low risk before accessing the resources, based on what's considered "low risk" for that micro perimeter. Therefore, organizations need to transition from static, network-based trust to dynamic, identity-based trust, which of course necessitates a strong identity foundation.



Use Case 2:

Keeping Up with the Threat Landscape

After a number of high-profile cybersecurity attacks on the Federal Government and critical infrastructure (e.g., SolarWinds and Colonial Pipeline), it became clear that cybersecurity must be recognized as an issue of national security. But the government won't be able to do that if it doesn't modernize its IT infrastructure.

The Office of Management and Budget (OMB) made that clear in its analysis of President Biden's Fiscal Year 2022 budget. It identified three areas of modernization at the center of the President's cybersecurity investments, stating:

> **"These investments will, in alignment with the Administration's priorities, focus on addressing root cause structural issues, promoting stronger collaboration and coordination among Federal agencies, and addressing capability challenges that have impeded the Government's technology vision."**

[1]OMB, *Analytical Perspectives, Budget of the United States Government, Fiscal Year 2022*

Let's take a closer look:

1. ROOT CAUSE STRUCTURAL ISSUES

Many Federal Government IT foundations include legacy identity systems that vendors have stopped investing in. To make matters worse, codependent stack components are tied to these (potentially end-of-life) solutions. Therefore, upgrading these systems is inherently risky and leaves agencies vulnerable to the latest threats and attack vectors.

2. INTER-AGENCY COLLABORATION

The Federal Government has historically struggled with interoperability, in large part because of incompatible authentication systems. This means that agencies cannot accept or verify each other's credentials, preventing the collaboration necessary to exchange vital security intel and launch coordinated response efforts.

3. ENHANCING TECHNOLOGY CAPABILITIES

Legacy identity systems do not provide the modern security capabilities needed to support the current threat landscape, such as native X. 509 certificate support for phishing-resistant PIV authenticators. Without enhancing IT environments with these capabilities, agencies will not be able to move forward with Zero Trust.

Use Case 3:

Complying with Federal Mandates

In under a year, the Federal Government went from having no Zero Trust mandates to three mandates on the books. Today, impacted agencies must comply with the following:

May 12, ‘21: EXECUTIVE ORDER 14028

Executive Order (EO) 14028, “Improving the Nation’s Cybersecurity,” elevated Zero Trust from “optional” to “required.” It calls for all impacted agencies—which, upon initial release, only included Federal Civilian Executive Branch (FCEB) agencies—to develop plans for Zero Trust and abide by subsequent Zero Trust policy issued in support of the EO.

Jan 19, ‘22: NATIONAL SECURITY MEMORANDUM-8

National Security Memorandum (NSM)-8, “Improving the Cybersecurity of National Security, Department of Defense (DoD), and Intelligence Community Systems (IC),” requires these additional entities to comply with EO 14028. This means the DoD and IC also need to plan for Zero Trust and abide by subsequent policy.

Jan 26, ‘22: OMB MEMORANDUM M-22-09

OMB Memorandum M-22-09, “Moving the U.S. Government Toward Zero Trust Cybersecurity Principles,” is the subsequent policy that outlines specific requirements for FCEB, DoD, and IC agencies’ Zero Trust implementations. Notably, this includes employing a centralized identity management system, phishing-resistant MFA, and attribute-based access control.

EO 14028

- Released May 2021
- Initially impacts FCEBs
- Requires planning for Zero Trust adoption

NSM-8

- Released Jan 2022
- Impacts DoD / IC
- Requires EO 14028 compliance

OMB Memorandum M-22-09

- Released Jan 2022
- Impacts all EO followers
- Specifies Zero Trust implementation requirements

The Challenge

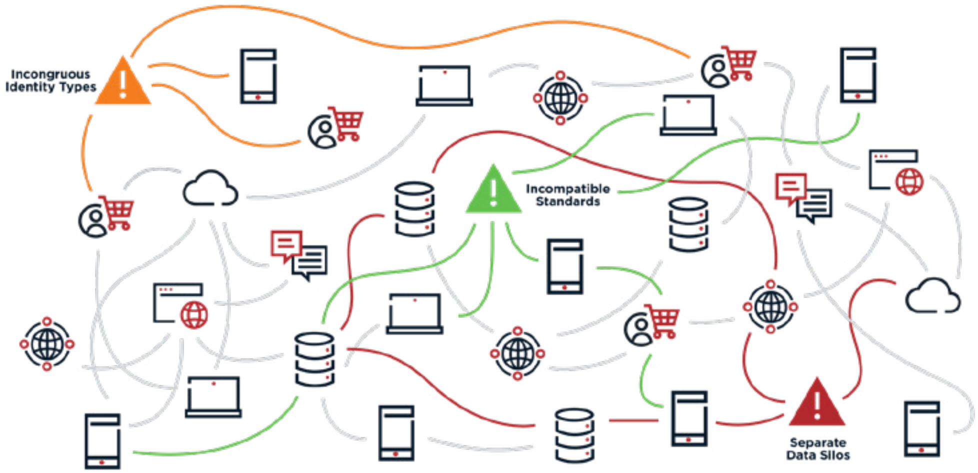
Fragmented Identity Infrastructures

It's clear now that identity-centric, Zero Trust environments are the path forward for the Federal Government. That being said, a common obstacle blocks that path for many agencies, and that is fragmented identity infrastructures.

This is due to the traditional ICAM approach that required agencies to build distinct identity systems to support four different "levels of assurance." These levels were based on how confident the agency needed to be in an asserted identity's validity before granting access to the requested resource:

- Level 1: Little or no confidence
- Level 2: Some confidence
- Level 3: High confidence
- Level 4: Very high confidence

While it was necessary to architect digital identity systems that interoperated with other systems that applied to the same LOA, it was not necessary for them to interoperate with systems that applied to a different LOA; whether that system resided within the same agency or a different agency. This led to a siloed development process, resulting in distinct identity ecosystems that were completely separate from one another. Or put another way: agencies wound up with fragmented identity infrastructures that look like the one to the right.



Forced Rip and Replace

Of course, agencies are aware of the challenges these types of infrastructures pose. So why have they persisted for so long?

The legacy identity systems these infrastructures were built on at the time make modernization a challenge, due to:

- Their tendency to force vendor lock-in
- Their connection to co-dependent stack components

Historically, this meant that agencies wanting to upgrade their infrastructures couldn't simply swap out a legacy component for a modern component.

Vendor lock-in prevented agencies from incorporating components designed by anyone but their existing vendor(s). And even if they could get around the vendor lock-in, co-dependency risked the entire environment going down if something went wrong when replacing a legacy component.

Therefore, incremental changes weren't an option. The only solution was a full rip and replace, which many agencies don't have the time or budget to afford.

But today, there's a different solution.

The Solution

Modernize Federal ICAM

Today, there are flexible, standards-based identity solutions that make it possible for agencies to uplevel their ICAM infrastructures, without ripping and replacing. This is because technologies built on open standards easily integrate with other components, even if they were developed by other vendors. As a result, agencies can simply augment their environments with select components to deliver the modern capabilities they need. They don't need to overhaul their entire infrastructure.

So how do you decide which ICAM components to augment to lay the foundation for Zero Trust? Let's look to the definition of ICAM itself:

> **ICAM is the set of tools, policies, and systems that an agency uses to enable the right individual to access the right resource, at the right time, for the right reason in support of federal business objectives.**[2]

To accomplish this, you must be able to:

- Break down identity silos
- Make risk-based access decisions
- Adjust access permissions as needed

While this might sound like a significant undertaking, you only need to modernize three ICAM components to attain these capabilities. In the next section, we'll provide an overview of these components and their benefits.

[2] *IDManagement.gov, Federal ICAM Architecture Introduction*

The 3 ICAM Components to Modernize for Zero Trust

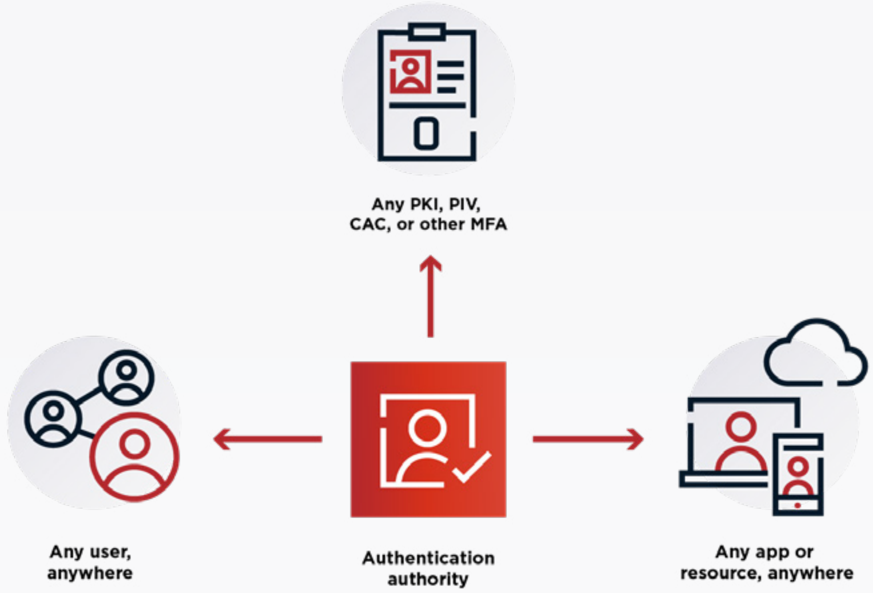
Component 1: Authentication

As previously mentioned, many Federal environments are made up of distinct identity systems that do not interoperate with one another. They feature disparate authentication systems that stand in the way of establishing consistent, secure, identity-centric access across the entire environment.

To overcome this, you need to consolidate these systems. It's important to note: you don't necessarily need to get rid of each individual system entirely. Rather, you need a way to facilitate visibility and management over all of the systems in your environment.

You can accomplish this by employing a centralized authentication authority which consolidates all of your disparate systems into a central identity control plane. This breaks down the identity silos in your environment so that you can:

- Integrate existing authenticators with all of your resources whether they're hosted on-premises or in the cloud
- Enable secure access to these resources by any user no matter whether the user resides inside or outside of the network perimeter
- Employ consistent authentication practices to users — regardless of which system initially issued their authenticators



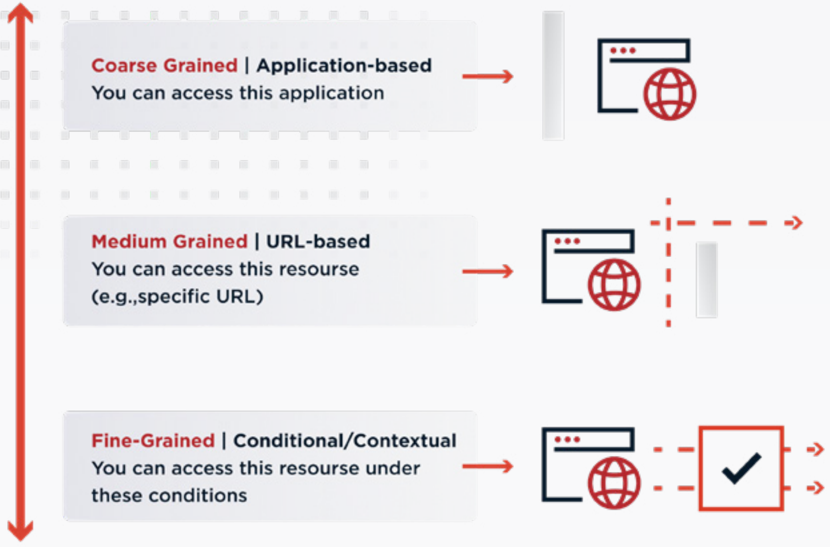
Component 2: Authorization

As a result of legacy identity systems, many organizations today have static, coarse-grained authorization processes in place. They rely on role-based access control (RBAC), which only allows you to grant access based on a user's position in the organization (i.e., their role).

Employing fine-grained, attribute-based access control (ABAC) allows for a more sophisticated authorization process. It takes additional context into consideration to determine how risky a user's access request is, such as:

- Does the user typically access this type of information?
- Is the request coming from a trusted device?
- Does the request originate from an abnormal location for this user?

This additional context helps you determine if the request is risky and whether or not it should be authorized. As a result, you can make risk-based access decisions to ensure that only users that meet the micro-perimeters' security measures are granted access to the resources it contains.



Coarse Grained | Application-based
You can access this application

Medium Grained | URL-based
You can access this resourse
(e.g.,specific URL)

Fine-Grained | Conditional/Contextual
You can access this resourse under these conditions

Component 3: Monitoring

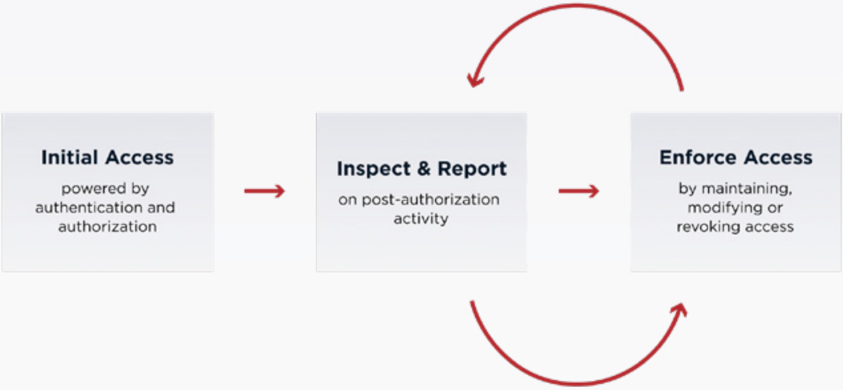
In a Zero Trust environment, initial access does not guarantee indefinite access. Why? Just because you deem a user's initial access request low risk, that doesn't mean their future requests will always have that same risk level.

For example, perhaps upon initially requesting access to a resource, it was confirmed that:

- The user does typically access this type of information
- The request is coming from a trusted device
- The request originates for a normal location for this user

The user receives initial access, so everything that happens moving forward is considered post-authorization activity. But what if post-authorization, the user attempts to access the same resource, but this time from an abnormal location? In that case, you may want to partially or completely revoke the user's access to that resource or require step-up authentication before reinstating the user's access.

However, legacy identity systems weren't designed to support post-authorization monitoring like this. Therefore, you need a monitoring component that can continuously inspect and report on post-authorization activity and adjust access permissions. This allows you to take real-time context into consideration when authorizing user access and making adjustments as needed to protect your assets.

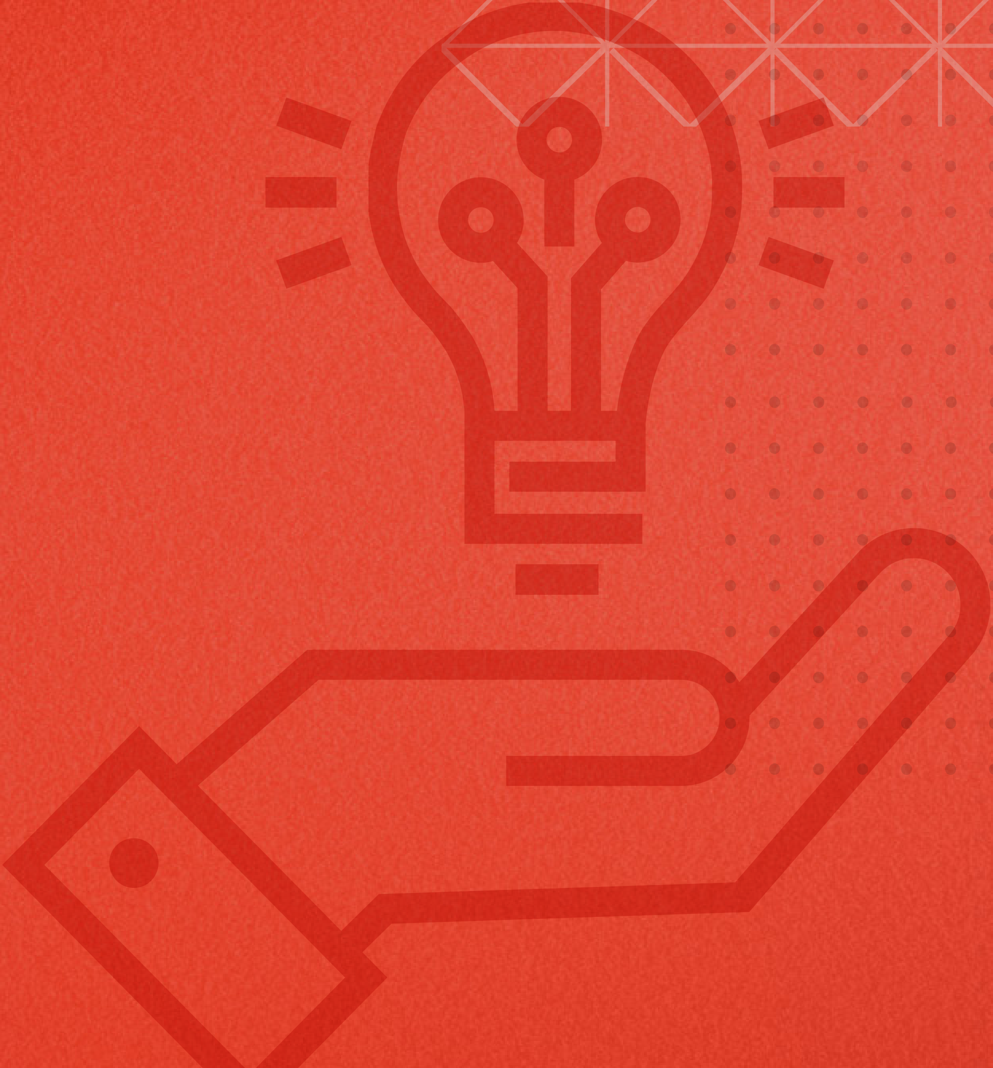


Initial Access powered by authentication and authorization

Inspect & Report on post-authorization activity

Enforce Access by maintaining, modifying or revoking access

Choosing a Solution



Flexible, Standards-Based Identity Solutions

With Zero Trust now a requirement for the Federal Government, agencies need to prioritize enhancing their ICAM foundations as much as possible, as soon as possible.

To avoid a rip and replace situation, look to flexible, standards-based identity solutions that can easily plug into your existing environment. This will allow you to lay a solid foundation for your Zero Trust environment while still making the most of your existing investments.

Ping Identity helps facilitate the move to a Zero Trust architecture with modern identity components, solutions, and services that can be deployed in any environment, including:

- Private, public, or multi-cloud environments
- Air-gapped or disconnected environments
- Hybrid IT environments

To learn more about overcoming legacy identity infrastructure challenges with the components reviewed in this eBook, read our white paper: Zero Trust Architecture Starts with Modern ICAM.

To learn more about Ping's solutions for the government, visit our website.