Defensible Zero Trust: A Strategic Playbook

A White Paper by
Ross Foard, Foard Consulting LLC and
Kevin Brewer, Ping Identity

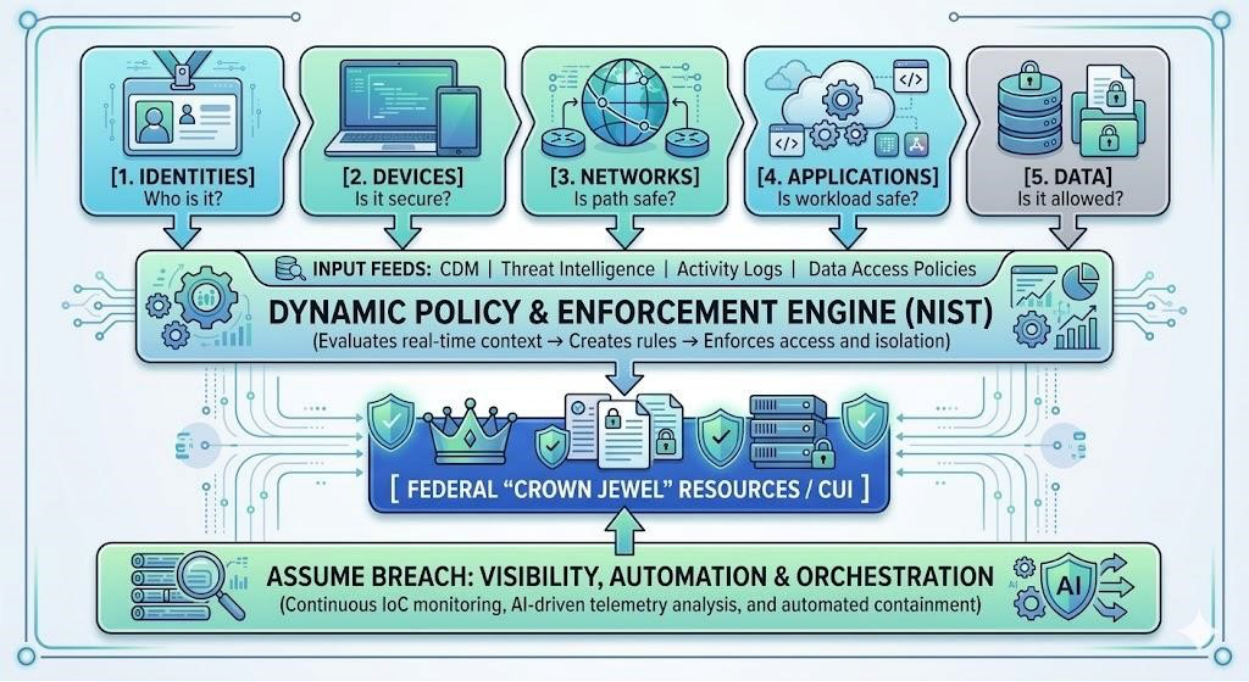
April, 2026

Executive Summary

Transitioning to a Zero Trust Architecture (ZTA) requires a cultural and technical shift, particularly for the US federal government and regulated industries. These sectors face a unique convergence of legacy technical debt and stringent compliance requirements.

Traditional perimeter-based metrics—such as the number of firewall blocks or static network zones or approved ATOs - no longer prove that an environment is secure or compliant. To demonstrate true progress, organizations must adopt Key Performance Indicators (KPIs) that continuously measure cybersecurity posture, micro-segmentation and containment, strong authentication, and provide visibility under an "assumed breach" reality.

A Zero Trust Architecture implements defenses for each of the ZTA pillars and relies on dynamic policies and policy enforcement to protect critical assets. A ZTA supports the “Assume Breach” mentality and responds to failures in defenses by orchestrating response through policy modification and automated actions.



ZT Architecture, Dynamic Policies and Automation protect “Crown Jewels”

This white paper outlines a three-phase playbook for security consultants and agency leaders to baseline their current environments, align their metrics with the NIST SP 800-207 architecture and the CISA Zero Trust Maturity Model, and validate the real-time telemetry required to automate threat containment. The KPIs identified give an indication of the essential items in moving to a Zero Trust architecture and measurements organizations can use to gauge their progress.

Phase 1: Architectural Baseline and "Crown Jewel" Discovery

Before assigning metrics or deploying new technologies, an organization must clearly define what it is protecting and assess its current technological maturity. In federal and regulated sectors, data categorization is often well-defined by law but poorly tracked in practice. Therefore, traditional data discovery must be augmented with access-driven auditing.

1. Follow the Privileged Access

Because data tagging can be unreliable or incomplete, baselining is most efficient when aggressively auditing **Identity and Access Management (IAM)**.

- **The Methodology:** Inventorying who has access to what is a massive shortcut to finding critical assets. Discovery of access performed via a Identity Governance and Administration (IGA) is the quickest way to identify legitimate privileged user and is essential for cleaning up orphaned accounts. Users designated "Privileged Users" (e.g., system administrators, database managers, cloud architects) allows security teams to rapidly differentiate legitimate users who may be an insider threat.
- **Federal / DoD Context:** Mapping privileged access reveals the exact environments housing Controlled Unclassified Information (CUI), Classified data, and FISMA High/Moderate systems.
- **Regulated Industries Context:** Identifying the administrators pinpoints the databases containing Protected Health Information (PHI) for healthcare, Cardholder Data (CDI) for finance, or operational technology (OT) control systems.

2. Establish the Maturity Baseline

Using the CISA Zero Trust Maturity Model (ZTMM), agencies must establish where they currently sit across the Traditional, Initial, Advanced, or Optimal stages.

- **Identity Readiness:** Has the organization implemented phishing-resistant MFA (e.g., PIV/CAC, FIDO2), for ALL users, or are they reliant on vulnerable SMS/Push notifications?
- **Device Health:** Are devices known and uncompromised prior to allowing them to access the network?
- **Network Modernization:** Are they shifting away from legacy VPNs toward modern access proxies aligned with TIC 3.0 use cases?
- **Application Assurance:** Are applications developed and delivered using secure DevSecOps practices and with understanding of the supply chain of code components?
- **Data Sensitivity:** Does the organization have a clear understanding of the level of sensitivity and availability requirements of the data being protected?

- **Assume Breach:** Even the best architecture and careful defense will be breached. Can anomalies be detected and automated actions taken to isolate or remediate failures?

Phase 2: Framework Alignment and the KPI Matrix

Metrics are only effective if they map directly to established best practices and compliance mandates. Combining CISA's Zero Trust Maturity Model (ZTMM) and NIST SP 800-207 provides a robust, defensible approach:

- **NIST SP 800-207** provides the architectural blueprint (the "how"). It dictates how trust is evaluated using the Policy Engine (PE), executed by the Policy Administrator (PA), and actioned by the Policy Enforcement Point (PEP).
- **CISA ZTMM** provides the roadmap (the "where"). It dictates the organization's current stance across five distinct pillars: Identity, Devices, Networks, Applications, and Data. By mapping CISA's pillars to NIST's components, we generate a compliance-driven KPI matrix that proves architectural maturity.

The Defensible KPI Matrix

CISA Pillar	Key Performance Indicator (Metric)	Federal / Regulated Context
Identity	**Phishing-Resistant MFA Rate:** *% of authentications using FIDO2/PIV/CAC vs. weaker methods.*	Explicit mandate under **OMB M-22-09**; phases out vulnerable SMS/Push MFA.
Device	**Continuous Posture Validation:** *Frequency of endpoint health/EDR checks post-authentication.*	Moves agency from "Traditional" to "Optimal" under the **CISA ZTMM**.
Network	**Legacy VPN Depreciation Ratio:** *Volume of remote traffic routed via ZTNA access proxies vs. traditional VPNs.*	Tracks adherence to **TIC 3.0** remote user use cases and shifts away from implicit trust.
Application	**Micro-segmentation Coverage:** *% of critical workloads that can be isolated to deny lateral movement.*	Mitigates lateral movement risk, aligning with the core **DoD Zero Trust Strategy**.

Data	**Dynamic Revocation Time:** *Mean time to severely limit access to CUI/PHI when risk context indicates attack.*	Tests the architecture's ability to ingest threat intel from **UEBA and Shared Signals Events** and dynamically protect crown jewels.
Visibility *(Cross-Pillar)*	**Centralized Log Ingestion:** *% of required ZTA telemetry successfully ingested into SIEM.*	Measures compliance with **OMB M-21-31** (Event Logging) to ensure accurate policy decisions.
Automation *(Cross-Pillar)*	**Automated Containment Rate:** *% of compromised identities/devices isolated automatically vs. manual intervention.*	Essential for defending against machine-speed/AI attacks and scaling SecOps capabilities.

Phase 3: Real-time Signals Orchestrate Automation

Today's modern environments face dynamic, AI-driven attacks, and telemetry is the active nervous system of the architecture. This phase replaces legacy periodic query-based IT auditing in favor of auditing the **data feeds** that fuel the NIST Policy Engine. Without real-time signals, the Policy Administrator cannot trigger the Automation and Orchestration required to contain a breach.

1. Continuous Diagnostics and Mitigation (CDM) Audit

Federal agencies must feed asset data into the CDM dashboard. This audit maps how that data specifically feeds the Zero Trust Policy Engine to ensure decisions are dynamic, not static.

- **The Validation Check:** Is the Policy Engine actively ingesting real-time device health (EDR status, patch levels) prior to allowing devices to connect?
- **Consultant's Metric:** *Real-Time Signal Ratio* (The percentage of access decisions made using live context versus static credentials).

2. User Entity and Behavior Analysis Actions

Federal agencies must analyze user data within their control boundaries. These actions enable dynamic, not static adjustment of use access based upon expected actions.

- **The Validation Check:** Is the UEBA Policy Engine actively ingesting real-time user activity and analyzing accounts, groups and role information to detect anomalies?
- **Consultant's Metric:** *Shared Signal Events Ratio* (The percentage of access decisions made which consider live Shared Signal Framework Information vs static information).

3. Signal-to-Automation Pathway

Manual analyst review fails against machine-speed attacks. Organizations must verify the technical pathway from signal detection to automated enforcement and notification.

- **The Validation Check:** Can the Security Orchestration, Automation, and Response (SOAR) platform communicate directly with the Policy Administrator via APIs to instantly sever access upon detecting an Indicator of Compromise (IoC)?
- **Consultant's Metric:** *API Enforcement Coverage* (The percentage of Policy Enforcement Points - like firewalls, proxies, and IAM tools—that can accept automated configuration changes from the Policy Administrator).

3. OMB M-21-31 Maturity Alignment

OMB M-21-31 dictates strict logging tiers (EL1 through EL3) for federal agencies. These requirements must be mapped directly to the Zero Trust pillars to ensure the Policy Engine is not operating blind.

- **The Validation Check:** Are critical events (like decrypted traffic flows or DNS queries) retained and formatted in a way the Policy Engine can computationally parse for anomalous lateral movement?
- **Consultant's Metric:** *Signal Parsing Success Rate* (The percentage of required logs that are actively ingested and successfully parsed by the analytics engine, rather than just dumped into cold storage data lakes).

Conclusion

Building a Zero Trust Architecture in the federal government or heavily regulated private sector industry is not a product installation; it is a fundamental architectural and cultural overhaul. While shifting discovery to focus on privileged access, rigorously aligning KPIs with NIST and CISA standards, and relentlessly auditing the telemetry that feeds automated enforcement are critical technical steps, true success requires a commitment to continuous evolution.

Zero Trust is a journey, not a destination. By embracing the "assume breach" reality and prioritizing dynamic, machine-speed orchestration, agencies move beyond static compliance checklists. Ultimately, this proactive posture ensures mission continuity and builds a resilient defense that remains operationally formidable against increasingly sophisticated adversaries.