Implementing Zero Trust Architecture: A Methodical Approach

by Sarbari Gupta

Zero Trust Architecture

Federal agencies face a mandate to implement a Zero Trust Architecture (ZTA) across their systems and networks. Executive Order 14021 and Office of Management and Budget Circular M-22-09 set forth the specific requirements and establish implementation milestones. The transition, however well delineated, is anything but straightforward. The reason is simple: ZTA is not a technical shift. ZTA requires organizational and process changes within and across agencies.

As the name implies, ZTA is a security model that assumes all entities, both internal and external to an organization, are untrustworthy. Every user, device, or application must be authenticated, authorized, and continuously validated for its security configuration and posture before being granted access – or retaining access – to an agency's resources.

National Institute of Standards and Technology (NIST) Special Publication (SP) 800-27 sets forth seven tenets as underlying ZTA:

1. All data sources and computing services are considered resources.
2. All communication is secured regardless of network location.
3. Access to individual enterprise resources is granted on a per-session basis.
4. Access to resources is determined by dynamic policy.
5. The enterprise monitors and measures the integrity and security posture of all owned and associated assets.
6. All resource authentication and authorization are dynamic and strictly enforced before access is allowed.
7. The enterprise collects as much information as possible about the current state of assets, network infrastructure, and communications and uses it to improve its security posture.

Zero Trust Maturity Model, prepared by the Cybersecurity & Infrastructure Security Agency (CISA), offers a roadmap for ZTA transition. It includes five pillars: Identity, Devices, Networks, Applications and Workloads, and Data. Further, the following three cross-cutting capabilities are detailed for each pillar:

1. Visibility and analytics
2. Automation and orchestration
3. Governance

Implementation Challenges

Because ZTA affects extant policies, processes, and stakeholders as well as the entire information technology environment, the sheer scope of the effort can be overwhelming. It is a complex, multifaceted undertaking that will require multiple years to accomplish and extensive strategic planning, careful resource allocation, and continuous adaptation.

Thus, a phased, iterative approach is necessary, with multiple project phases envisioned. Each individual effort focuses on specific goals and objectives of the overall endeavor. Likewise, ZTA implementation

emphasizes the need for pilot programs wherein agencies can test new functionalities in a controlled environment, validate their effectiveness, and gather feedback for further refinements.

At its heart, the ZTA journey is characterized by evolving and adapting. Each phase and pilot program is seen to build on the lessons learned from previous efforts.

A Proposed Approach

Beyond a phased, iterative approach, the transition to ZTA demands a step-by-step process. I propose the seven-step methodology illustrated below.

1. ***Establish Governance and Assess Current State***

One of the first priorities in an effort of this magnitude is securing leadership buy-in. Staff must feel that implementation is a management priority and something agency leaders fully endorse. It is particularly helpful to have a "champion," an executive who both supports the change and advocates for it. Next, there must be a ZTA governance structure, that is, a framework that establishes responsibilities, authorities, roles, and more. Last, but not least, a Zero Trust Steering Committee must be formed to oversee the implementation process.

A prerequisite to organizational change is understanding the status quo. Thus, transition to ZTA must start with a thorough inventory of all IT assets, including users, devices, networks, applications, and data. Next, it is critical to understand current vulnerabilities in the inventory and prioritize them. Risk analysis is the best way to identify weaknesses and prioritize them based on mission-critical assets and vulnerabilities. A maturity model such as CISA's can be invaluable in evaluating an agency's current state.

2. ***Develop Zero Trust Strategy and Roadmap***

An overarching strategic vision should guide each agency's ZTA journey. This vision should incorporate an agency's distinct mission and strategic goals. Thus, each ZTA strategy will be unique to its creators.

Next, agencies must translate their strategy into a roadmap that includes a phased implementation plan with short-term, mid-term, and long-term goals. Planned actions should reflect established priorities: high-risk areas, critical resources, mission priorities, and federal mandates.

3. ***Prioritize and Plan Zero Trust Actions***

Prioritization and planning should focus on the following areas:

- Identity and Access Management (IAM): Implement multifactor authentication (MFA), least privilege principles, and continuous monitoring.
- Device Security: Ensure devices are compliant. Secure them with tools such as Endpoint Detection and Response (EDR).
- Network Security: Adopt microsegmentation and secure communications techniques.

- Application and Data Security: Implement encryption and monitor access.

Of course, automation is imperative for streamlining security processes and reducing errors.

4. ***Execute Pilot Programs***

The ZTA journey is wrought with challenges and unknowns. Pilot efforts offer an element of control by limiting testing to specific technologies and select user groups. By executing pilot projects for specific ZTA activities (e.g., MFA rollout or microsegmentation), implementers can identify and correct any problems prior to full-scale implementation.

Preestablished, well-defined metrics are needed to gauge the success of each pilot project. Stakeholder feedback is equally important, as the first-hand experiences of the ultimate end users are invaluable.

5. ***Continuous Monitoring and Iteration***

Regular assessment of ZTA implementation progress against the strategic roadmap enables adjustments based on new risks, lessons learned, and evolving guidelines. It cannot be emphasized enough that the ZTA journey demands an iterative process where analysis and evaluation inform next steps.

6. ***Scale, Document, and Share***

Building on previous success is paramount. Thus, a phased rollout where implementers gradually scale ZTA across the entire agency is recommended. Here, as elsewhere, it's key to maintain detailed records of strategies, challenges, and solutions. Moreover, as ZTA is a governmentwide effort, knowledge sharing will not just facilitate the process internally but also support broader ZTA adoption across agencies.

7. ***Align with Compliance and Plan for the Future***

Federal documents such as Office of Management and Budget Circular M-22-09 and Executive Order 14021 prescribe mandates for agency implementation including schedules. It is important to remain mindful of these requirements and abide by them.

I recommend "futureproofing" your ZTA strategy, that is, incorporating an element of adaptability to accommodate future technological advancements and emerging threats. Nothing in our IT environment is static, especially our enemies, and agencies must be capable of pivoting quickly.

Today, we are in the earliest stages of understanding the need for ZTA and defining its requirements. As the cybersecurity landscape changes – and it will – federal agencies must be able to evolve with the times to ensure efforts are responsive to the greatest extent possible.

Conclusion

Federal agencies can never underestimate the importance of cybersecurity. Federal systems collect and maintain data that requires the highest levels of protection whether in transit or at rest. Agencies perform critical activities on which the nation's citizens and indeed our global neighbors depend. Government must be capable of executing these actions without interruption or interference by outside cyber threats. ZTA is the best response in our arsenal today.