PLATINUM
BUSINESS SERVICES, LLC

Implementing Zero Trust Architecture (ZTA)

Platinum Business Services, LLC

Jody Venkatesan, CISA, CISM, CGEIT, CRISC, CDPSE
President & CEO

Email: jvenkatesan@weareplatinum.net
Phone: 301-651-1297
Fax: 301-483-0104
Website: weareplatinum.net

4SBA Certified 8(a) HUBZone, Service-Disabled Veteran Owned Small Business (SDVOSB), Veteran-Owned Small Business (VOSB), Small Business (SB), Small Disadvantaged Business (SDB)
4TIN/EIN: 26-3462811
4Cage Code: 59N47
4DUNS: 828491410
4UEI: PCNMDK3FLJB9
4CIOSP3 NIH CIOSP3 SDVO (Contract #HHSN316201800030W)
4GSA MAS Professional Services #GS00F344CA
4GSA MAS IT #GS-35F-0067Y
4GSA 8(a) STARS 3 #47QTCB21D0108

Implementing Zero Trust Architecture (ZTA)

Introduction

When the White House issued Executive Order 14028, "Improving the Nation's Cybersecurity," every Chief Security Officer in the Government went into a state of heightened activity, working quickly to quickly formulate a plan to become compliant with the Executive Order and the accompanying Office of Management and Budget (OMB) Strategy. Swift actions were taken to formulate novel policies, overhaul architectural frameworks, and devise streamlined procedures to implement this directive. Since then, the number of approaches and standards created to implement Zero Trust is, to be blunt, rather confusing. Platinum's staff has worked diligently to make sense of these sometimes-conflicting guidelines and design a practical approach to assisting our clients in enhancing their cybersecurity positions while meeting OMB objectives. Our strategy enables us to effectively aid our clients in elevating their cybersecurity postures while aligning with the strategic imperatives outlined by the OMB.

OMB's strategy can be encapsulated in five distinct statements, each of which can then be equated to specific actions that need to be taken to implement Zero Trust Architecture (ZTA).

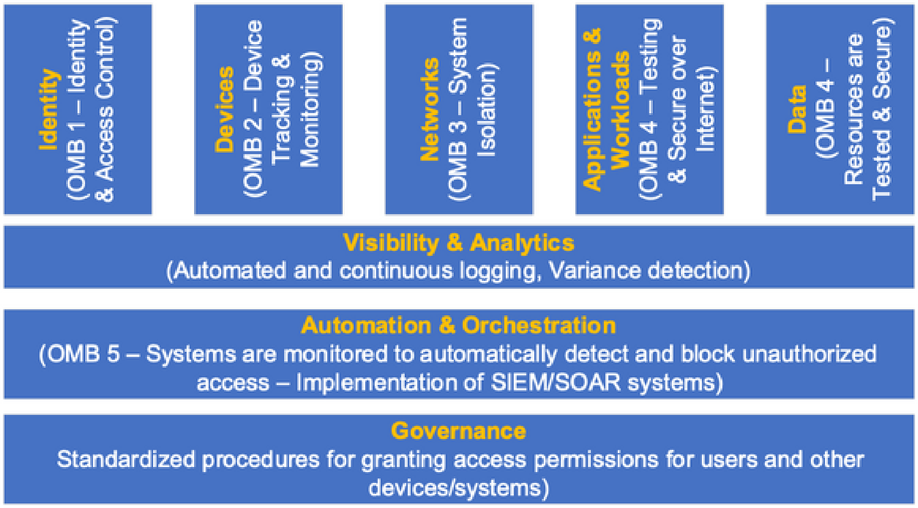
1. Federal Staff have enterprise-managed accounts protected from cyberattacks.
2. Devices are tracked and monitored, and device security is considered when granting access to the users.
3. Agency systems are isolated, and traffic between and within them is reliably encrypted.
4. Applications are tested internally and externally and are available securely over the Internet.
5. Systems are monitored to detect and block unauthorized access automatically.

While the strategic objectives seem reasonably straightforward, implementing them is not as simple as they seem. For many years, system architectures, cybersecurity policies, and Identity, Credential, and Access Management (ICAM) have all been based on having trusted networks. ZTA starts from the premise that no network can be trusted – that all networks have vulnerabilities that could allow unauthorized access.

With this fundamental change in the underlying assumption that we make about the security of our systems, we are faced with the need to make wide-sweeping changes in how we design and manage our IT systems. According to the National Institute of Standards and Technology (NIST) Special Publication 800-207, ZTA requires that we shift our focus from securing the network to securing the resources within the enterprise – data, assets, services, workflows, network accounts – instead of focusing solely on the network boundaries. Per NIST, ZTA is a collection of "concepts and ideas designed to minimize uncertainty in enforcing accurate, least privilege per-request access decisions in information systems and services in the face of a network viewed as compromised." So, the real question is, how do we protect an environment that is ALWAYS considered vulnerable?

Implementing Zero Trust Architecture (ZTA)

While OMB has stated what outcomes must be considered, and NIST has defined the controls to be implemented, the Cybersecurity and Infrastructure Security Agency (CISA) has defined a ZTA maturity model. Please note that a number of other organizations, ranging from Gartner to the Central Intelligence Agency, have also defined models for ZTA, each of which has advantages. Still, the CISA model is the most commonly used by Government agencies. CISA breaks ZTA into five pillars and three cross-cutting capabilities. These pillars collectively form the bedrock of a holistic ZTA framework tailored to bolster cybersecurity within the governmental environment.



Identity (OMB 1 – Identity & Access Control)

Devices (OMB 2 – Device Tracking & Monitoring)

Networks (OMB 3 – System Isolation)

Applications & Workloads (OMB 4 – Testing & Secure over Internet)

Data (OMB 4 – Resources are Tested & Secure)

Visibility & Analytics
(Automated and continuous logging, Variance detection)

Automation & Orchestration
(OMB 5 – Systems are monitored to automatically detect and block unauthorized access – Implementation of SIEM/SOAR systems)

Governance
Standardized procedures for granting access permissions for users and other devices/systems)

Like any significant change to the architecture, systems, and user experience that Zero Trust Architecture will require, we recommend adopting an organizational change management model to implement this now-required architecture incrementally – and, more importantly, to implement the organizational changes it implies.

During the first phase, establishing a clear "as-is" baseline and evaluating the current state of the enterprise architecture is paramount. As Watts Humphrey pointed out in Managing the Software Process, "If you don't know where you are, a map won't help." We evaluate the current condition against the OMB objectives and the CISA model, creating a gap analysis to identify if any ZTA elements are already in place and create a baseline for mapping out a roadmap for change.

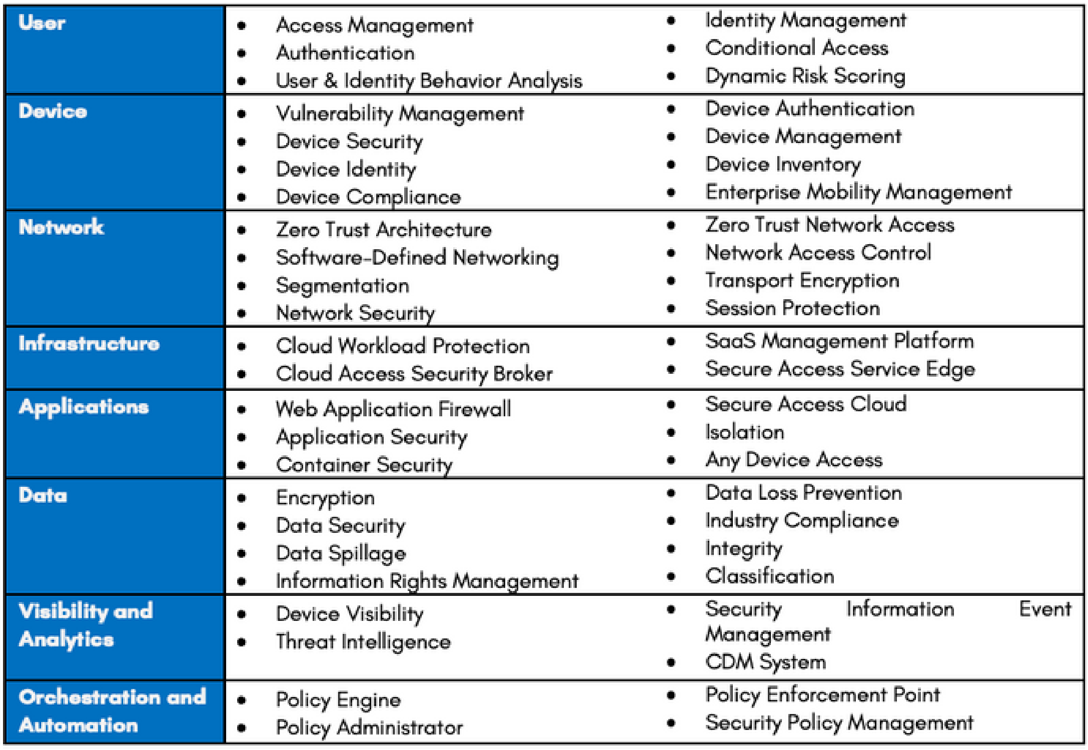
As with any change management process, the next step is defining the "to-be" condition you want to achieve. Mapping the status of each element as "met," "partially met," or "not met" allows you to identify low-hanging fruit and plan your path to achieving the ZTA goals.

Implementing Zero Trust Architecture (ZTA)

Taking the transition to ZTA one step at a time, rather than attempting to implement it all at once, is a more economical and lower-risk method. Some elements that can be implemented early in the process include the following.

- An appealing first step toward ZTA is implementing an ICAM system that operates within a hybrid environment, provides single sign-on for all systems (both within the cloud and mounted on on-premises servers), and uses multi-factor authentication. Such systems can also manage machine-to-machine sign-on and authentication. While most organizations have implemented single sign-on ICAM solutions that work within hybrid systems and are, therefore, partially compliant with ZTA, adding multi-factor authentication is a compliance step that is relatively simple since most ICAM systems can support MFA reasonably easily.
- Another option is migrating from the Trusted Internet Connection 2.0 (TIC 2.0) framework to TIC 3.0, mapping the new capabilities met by implementing Secure Access Service Edge (SASE) solutions to an updated Zero Trust capability model version.
- Yet, another option is to implement encryption for transit and rest data, which provides endpoints, including mobile devices and BYOD devices, with certificates supporting point-to-point encryption.

Regardless of where you start, the objective is to achieve 100% compliance with ZTA standards within the next 3 to 5 years. During this time, a number of issues must be addressed across the entire enterprise, as shown in the following table.



User	• Access Management • Authentication • User & Identity Behavior Analysis	• Identity Management • Conditional Access • Dynamic Risk Scoring
Device	• Vulnerability Management • Device Security • Device Identity • Device Compliance	• Device Authentication • Device Management • Device Inventory • Enterprise Mobility Management
Network	• Zero Trust Architecture • Software-Defined Networking • Segmentation • Network Security	• Zero Trust Network Access • Network Access Control • Transport Encryption • Session Protection
Infrastructure	• Cloud Workload Protection • Cloud Access Security Broker	• SaaS Management Platform • Secure Access Service Edge
Applications	• Web Application Firewall • Application Security • Container Security	• Secure Access Cloud • Isolation • Any Device Access
Data	• Encryption • Data Security • Data Spillage • Information Rights Management	• Data Loss Prevention • Industry Compliance • Integrity • Classification
Visibility and Analytics	• Device Visibility • Threat Intelligence	• Security Information Event Management • CDM System
Orchestration and Automation	• Policy Engine • Policy Administrator	• Policy Enforcement Point • Security Policy Management

Implementing Zero Trust Architecture (ZTA)

To assist in mapping the as-is model to the standards needed to meet ZTA requirements, it is possible to require vendors to report on their compliance status. For example, cloud providers typically meet ZTA standards already.

The following actions can efficiently be completed in parallel. They include creating use cases describing how connections are made to applications in the cloud and on-premises. Validating the accuracy of the configuration management database is used to confirm your configuration model. It can also evaluate what applications currently mounted on-premises can be moved to a ZTA-compliant cloud platform. This may have the beneficial side effect of reducing operating costs if the net book value of the on-premises assets is less than the cost of the cloud implementation.

With this information in hand, a clear definition of the current cybersecurity posture can be created, and a plan for achieving full ZTA compliance can be devised and implemented in reasonable increments.

Platinum brings the full range of cybersecurity experience and architectural expertise needed to support the implementation of ZTA in manageable increments – and the agile methodology to do so collaboratively with your IT and security teams. As part of the process of successfully implementing ZTA, you may also find additional benefits with a far more effective security posture and potential reductions in overall lifecycle costs for your IT systems.