ANTEAN TECHNOLOGY

VENDOR AGNOSTIC ZERO TRUST ARCHITECTURE (ZTA)

PLANNING AND IMPLEMENTATION

ANTEAN TECHNOLOGY

Does your organization need a Vendor Agnostic approach to Implementing Zero Trust Architecture?

On January 26, 2022, the Office of Management and Budget (OMB) released M-22-09 “Moving the U.S. Government Toward Zero Trust Cybersecurity Principles” in order to provide agencies guidance on implementing a Zero Trust cybersecurity policy government-wide in direct support of President Biden’s Executive Order E.O. 14208 on Improving the Nation’s Cybersecurity.

OMB’s Federal Zero Trust Strategy requires government agencies to achieve specific Zero Trust security goals by the end of Fiscal Year 2024.

The OMB guidance describes a federal Zero Trust architecture that:

1. Bolster’s identity practices.
2. Relies on encryption and application testing instead of perimeter security.
3. Recognizes every device and resource the government has.
4. Supports intelligent automation of security actions.
5. Enables safe and robust use of cloud services.

The Federal Zero Trust Strategy requires Federal Civilian Executive Branch (FCEB) agencies to achieve specific ZTA-related goals by the end of fiscal year 2024. Those goals are grouped into five categories: identity, devices, networks, applications, and data. Specific goals for agencies include:

- Implementing enterprise-wide identity and authentication systems using single sign-on (SSO) and multi-factor authentication (MFA);
- Deploying endpoint detection and response (EDR) tools across the agency's computers, and developing the capability to share threat data with other agencies;
- Encrypting web traffic and email traffic;
- Segmenting agency networks around individual applications
- Retaining outside firms to perform security testing and assessment;
- Maintaining a public vulnerability disclosure program;
- Safely moving applications to be Internet accessible (and therefore not reliant on being behind a security "perimeter");
- Auditing access to sensitive data stored in commercial clouds; and
- Improving retention of and access to security logging.

But what does it take to move from a Zero Trust Strategy to active implementation?

Antean’s Security subject matter experts thoroughly understand the key elements of the OMB ZTA requirements and its implementation. We are available to work with, assist and provide oversight from a security perspective to enterprise architect, system/application developers, engineer and admins on the building, configuration and implementation of a secure Zero Trust Architecture.

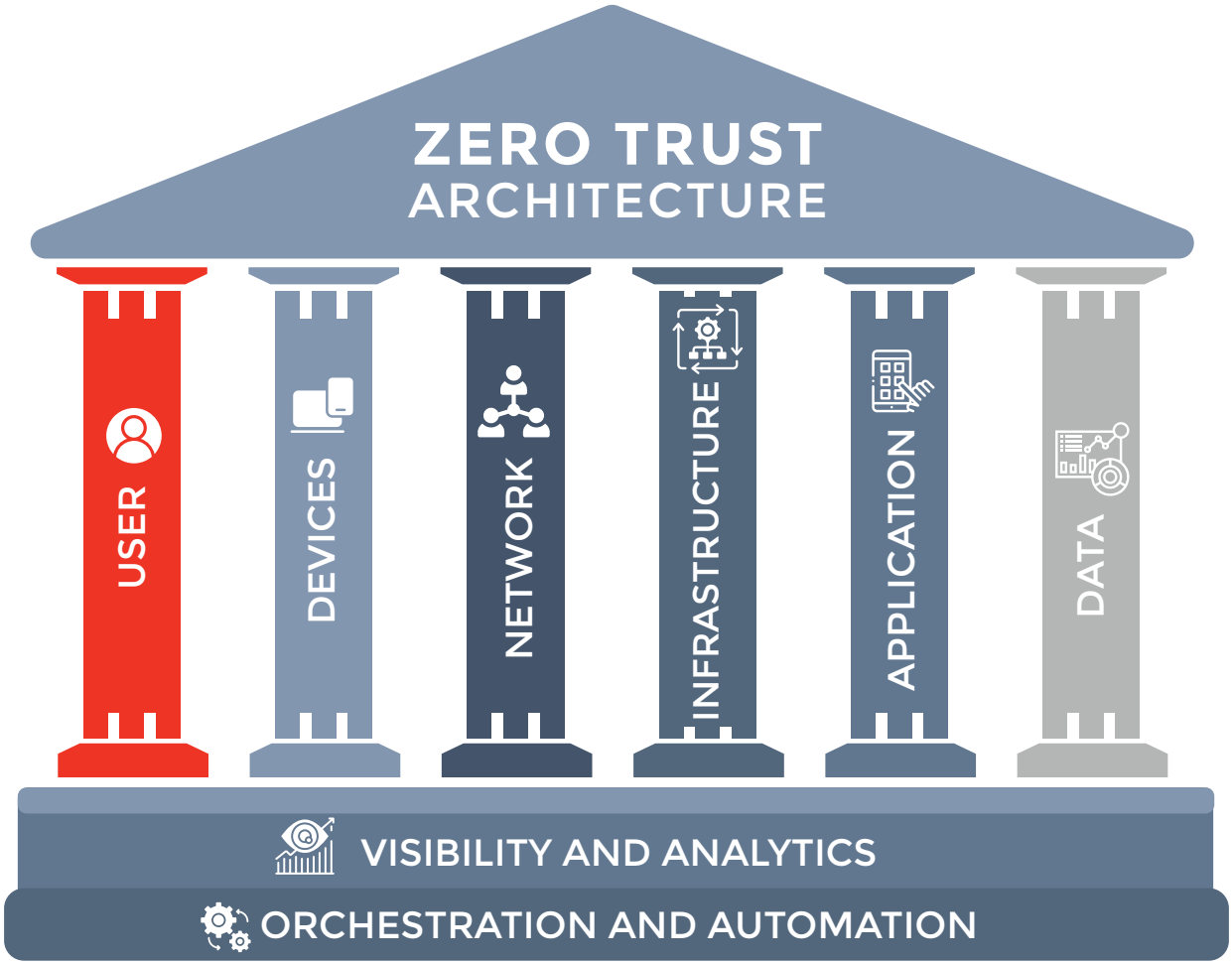
Make Zero Trust a reality at your organization with hands-on guidance from Antean’s Security subject matter experts. Permit us to a lead and coordinate your upcoming ZTA efforts.

ANTEAN TECHNOLOGY

How Can Antean Assist?

- Develop and document a Zero Trust Architecture (ZTA) Implementation Strategy
- Assist you agency in determining what it takes to move from a Zero Trust Strategy to active implementation?
- Develop and document ZTA Plans, Polices, Processes and Procedures
- Conduct a gap analysis of the existing/as-is environment to identify gaps, coordinate on deployment, and establish information sharing capabilities
- Assist with budget/investment plan estimation for ZTA implementation
- Assist is selecting the correct ZTA deployment scenario based on NIST SP 800-207
- Ensure agency endpoint detection and response (EDR) tools meet CISA's technical requirements and are deployed and operated across the agency
- Develop a set of initial categorizations for sensitive electronic documents within your enterprise
- Assist in identifying agency assets (i.e., data, application, assets, and services)
- Assist with implementing a centralized identity management system
- Deploy phishing resistant methods and training

ZERO TRUST ARCHITECTURE PILLARS



USER

This pillar focuses on user identification, authentication, and access control policies which verify user attempts connecting to the network using dynamic and contextual data analysis.

DEVICES

This pillar performs system of record validation of user-controlled and autonomous devices to determine acceptable cybersecurity posture and trustworthiness.

NETWORK

This pillar isolates sensitive resources from being accessed by unauthorized people or things by dynamically defining network access, deploying micro-segmentation techniques, and controlling network flows while encrypting end-to-end traffic.

INFRASTRUCTURE

This pillar ensures systems and services within a workload are protected against unintended and unauthorized access, and potential vulnerabilities.

APPLICATION

This pillar integrates user, device, and data components to secure access at the application layer. Security wraps each workload and compute container to prevent data collection, unauthorized access or tampering with sensitive applications and services.

DATA

This pillar focuses on securing and enforcing access to data based on its categorization and classification to isolate the data from everyone except those that need access.

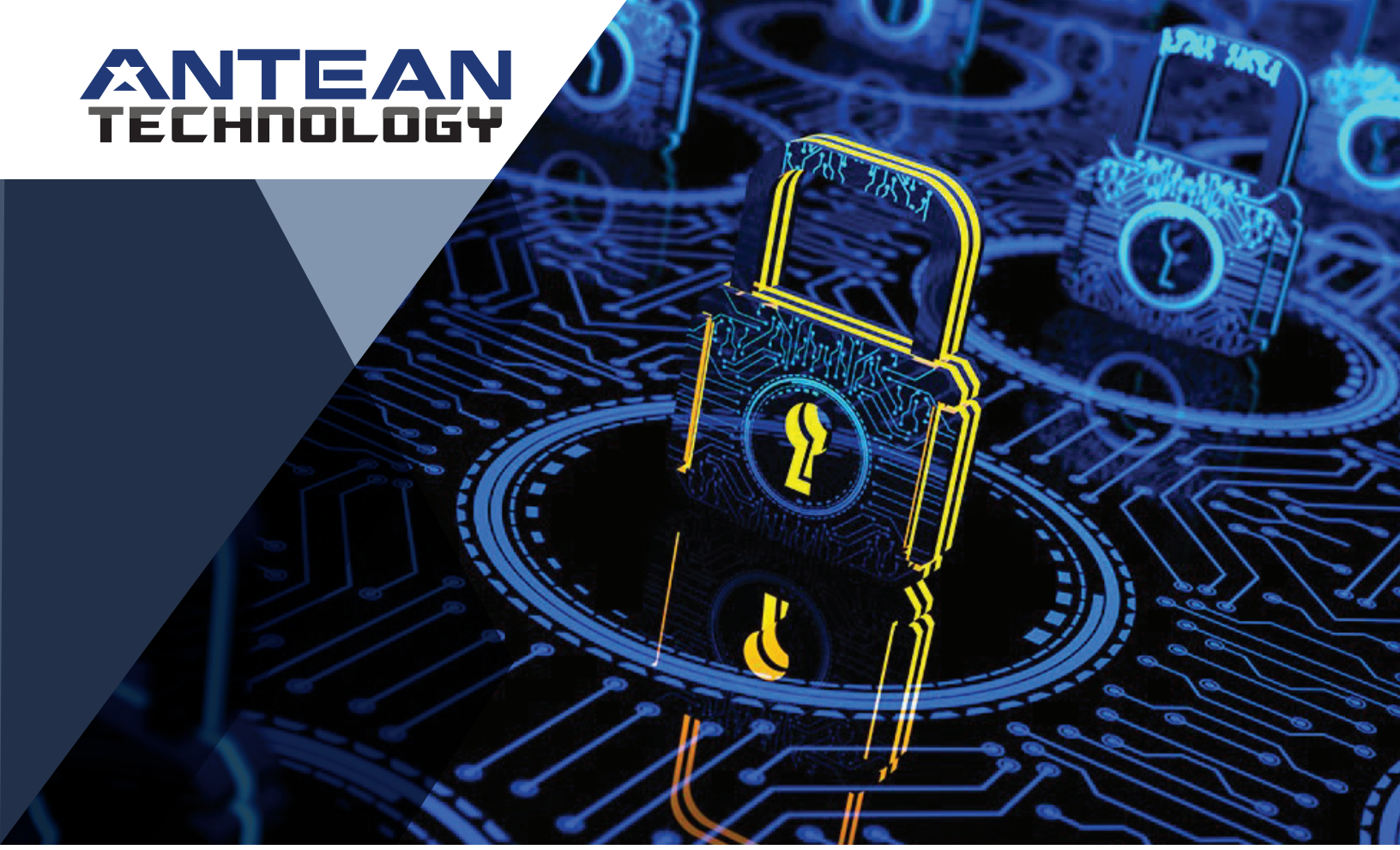
VISIBILITY AND ANALYTICS

This pillar provides insight into user and system behavior analytics by observing real-time communications between all Zero Trust components.

ORCHESTRATION AND AUTOMATION

This pillar automates security and network operational processes across the Zero Trust Architecture by orchestrating functions between similar and disparate security systems and applications.

ANTEAN TECHNOLOGY



ABOUT US

Antean Technology is deeply rooted in the design, development, implementation, and delivery of cybersecurity, systems engineering, executive administrative, and program management solutions. Our understanding of technology as it relates to time, cost, and performance allows us to quickly navigate through the nuances and challenges of organizations to provide bespoke solutions.

Cyber Security

- Security Architecture Design & Implementation
- Zero Trust Planning and Implementation
- Cloud/hybrid Systems Migration & Support
- Assessment & Authorization
- Security Compliance & 3rd Party Assessments
- Penetration Testing and Audit
- ISSM/ISSO Support
- Security Documentation Development
- System Hardening/Vulnerability Management

Systems Engineering

- Network Architecture Analysis & Design
- Network Architecture Development & Integration
- Infrastructure and Technology Evaluation
- Technical Strategy & Cost Savings Planning
- Cloud Based Virtualization
- Systems Integration
- Testing & Evaluation

CONTACT US

SIA FLOYD
President
Email : siafloyd@anteantech.com

SEAN FLOYD
Chief Operating Officer
Email : seanfloyd@anteantech.com

Website: **https://anteantech.com/**
SBA 8(a) and EDWOSB
TOP SECRET Facility Clearance
UEI: K2ZEQM1YTTV3
DUNS Number: 080011379
Cage Code: 7HPX4