CISA | CYBERSECURITY AND INFRASTRUCTURE SECURITY AGENCY

HPE ARUBA NETWORKING FEDERAL SYMPOSIUM

Zero Trust Maturity Model (ZTMM)

Sean Connelly –
Office of the Technical Director (OTD), Cybersecurity Division (CSD), CISA, DHS

Acronyms, POCs, and References

- Acronyms, Points of Contact and References are provided at the end of the slide deck
- Slide deck made available to audience upon request:
  - Please email ZeroTrust@cisa.dhs.gov with the subject title: HPE Aruba Networking Federal Symposium

Sean Connelly's Background

- 10 years at CISA (and former CS&C)
- 15 years supporting and/or leading TIC PMO
- Also have supported CDM & NCPS/EINSTEIN PMOs
- Co-author of NIST Special Pub 800-207 Zero Trust Architecture
- TMF Board Member (alternate)
- ~20 years in the federal domain

The Basics: Zero Trust

Definition: An evolving set of cybersecurity paradigms that move defenses from static, network-based perimeters to focus on users, assets, and resources.

in other words…

Zero Trust is not about building higher walls – it's about designing better gates.

Traditional Network Security

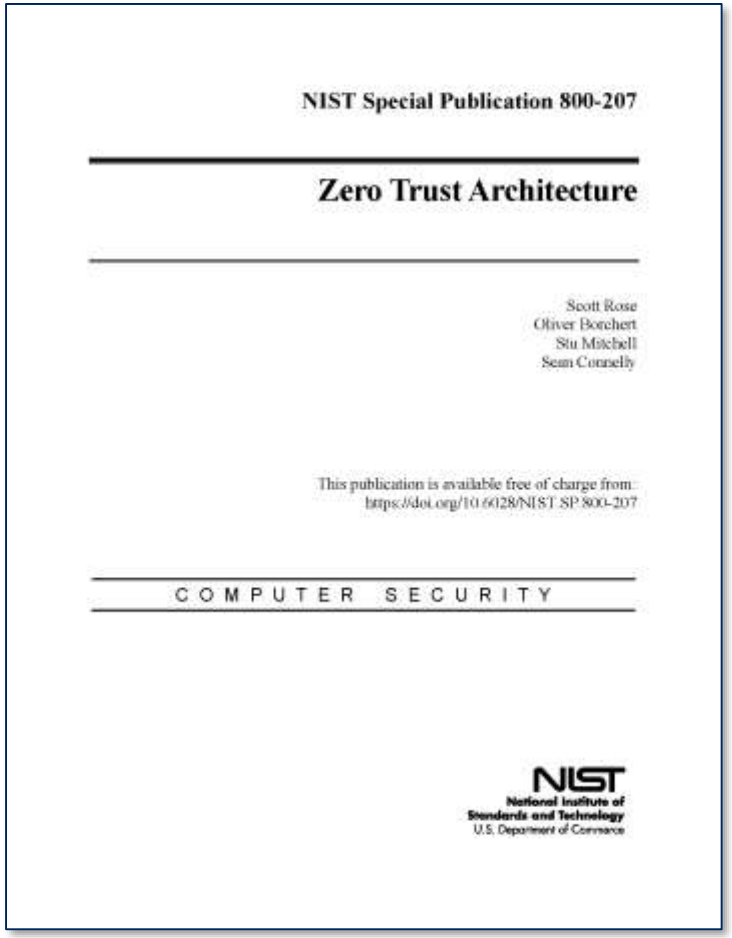
- Focus: perimeter security.
- Multiple, siloed perimeter sensors.

Zero Trust Network Security

- Focus: holistic security.
- Layered, integrated security systems.

NIST SP 800- 207 Zero Trust Architecture

- The National Institute of Standards and Technology (NIST) Special Publication (SP) 800-207 lays out seven tenets of Zero Trust Architecture (ZTA), such as:
    - Access is per-session and policy-determined,
    - Dynamic based Authentication & Authorization,
    - Extensive monitoring of assets, etc.
- Zero trust is a set of principles and not a single architecture or solution.
- ZTA is compatible with federal risk management guidance and cybersecurity initiatives including:
    - NIST Risk Management Framework,
    - Trusted Internet Connections (TIC),
    - National Cybersecurity Protection System (NCPS), and
    - Continuous Diagnostics and Mitigation (CDM).



NIST Special Publication 800-207

Zero Trust Architecture

Scott Rose
Oliver Borchert
Stu Mitchell
Sean Connelly

This publication is available free of charge from:
https://doi.org/10.6028/NIST.SP.800-207

COMPUTER SECURITY

NIST
National Institute of
Standards and Technology
U.S. Department of Commerce

Federal Zero Trust Efforts

National Security Agency | Cybersecurity Information

Embracing a Zero Trust Security Model

Planning for a Zero Trust Architecture: A Starting Guide for Administrators

NIST Special Publication 800-207

Zero Trust Architecture

Scott Rose
Oliver Borchert
Stu Mitchell
Sean Connelly

DoD Zero Trust Strategy

GSA

EIS and Zero Trust Architecture

How are you progressing on your Zero Trust Architecture journey?

Zero Trust Architecture (ZTA) Buyer's Guide

Executive Order on Improving the Nation's Cybersecurity

As the Federal Government continues to expand past the traditional network perimeter, it is paramount that agencies implement data protection measures around zero trust.

There are several other zero trust guidance documents that have been produced across the Federal Government.

FCEB Zero Trust Landscape

NIST Special Publication 800-207

Zero Trust Architecture

Scott Rose
Oliver Borchert
Stu Mitchell
Sean Connelly

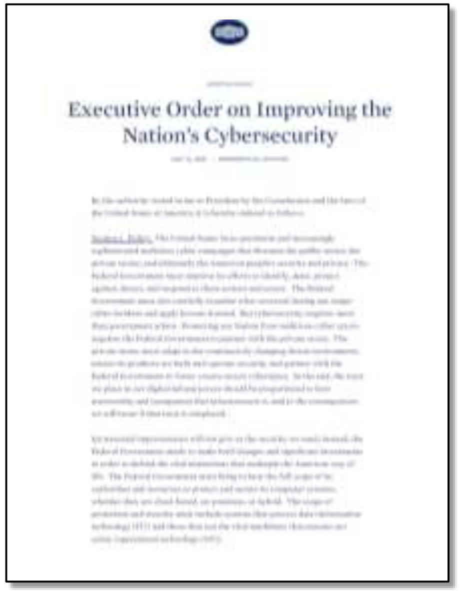
This publication is available free of charge from:
https://doi.org/10.6028/NIST.SP.800-207

COMPUTER SECURITY

NIST
National Institute of
Standards and Technology
U.S. Department of Commerce

The Principles

NIST SP 800-207
Zero Trust
Architecture



Executive Order on Improving the Nation's Cybersecurity

The Imperative

EO 14028
Improving the
Nation's
Cybersecurity

EXECUTIVE OFFICE OF THE PRESIDENT
OFFICE OF MANAGEMENT AND BUDGET
WASHINGTON, D.C. 20503

January 26, 2022

M-22-09

MEMORANDUM FOR THE HEADS OF EXECUTIVE DEPARTMENTS AND AGENCIES

FROM: Shalanda D. Young
Acting Director

SUBJECT: Moving the U.S. Government Toward Zero Trust Cybersecurity Principles

I. OVERVIEW

The Strategy

OMB M-22-09
Zero Trust Strategy

Zero Trust
Maturity Model

CISA Zero Trust
Maturity Model

Trusted Internet
Connections 3.0

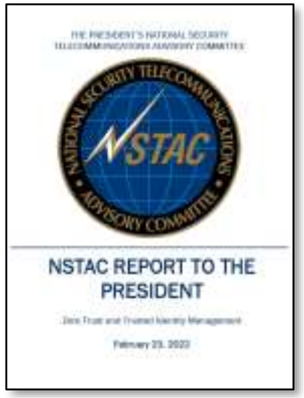
TIC Core Guidance Volume 3:
Security Capabilities Catalog

TIC Catalog

The Operational Guidance

Cloud Security
Technical Reference
Architecture

Federal Cloud
Security TRA



THE PRESIDENT'S NATIONAL SECURITY
TELECOMMUNICATIONS ADVISORY COMMITTEE

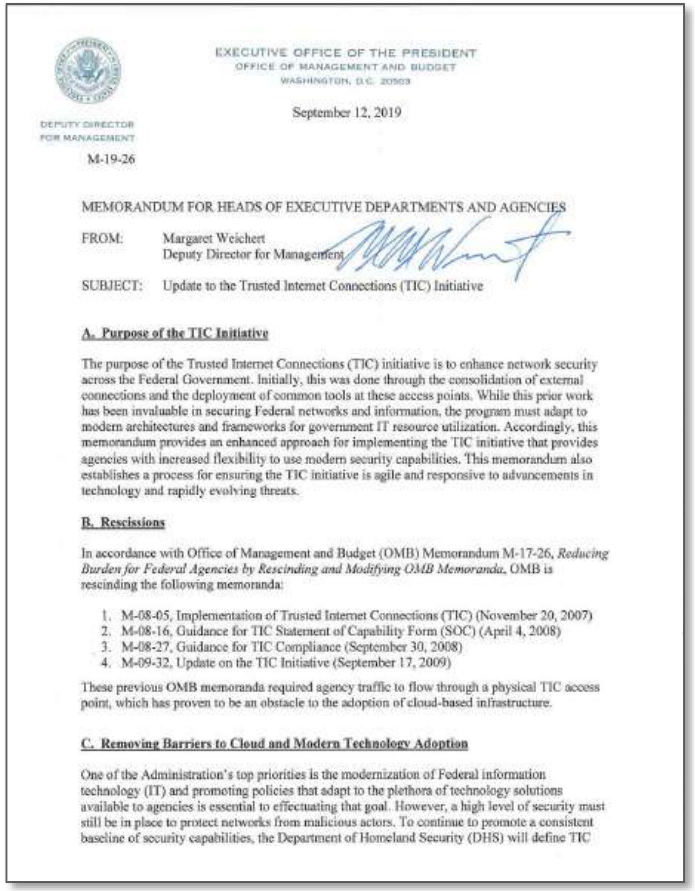
NSTAC REPORT TO THE
PRESIDENT

Zero Trust and Trusted Identity Management

February 23, 2022

NSTAC Report

TIC 3.0 M-19-26 & Core Guidance



EXECUTIVE OFFICE OF THE PRESIDENT
OFFICE OF MANAGEMENT AND BUDGET
WASHINGTON, D.C. 20503

September 12, 2019

DEPUTY DIRECTOR
FOR MANAGEMENT

M-19-26

MEMORANDUM FOR HEADS OF EXECUTIVE DEPARTMENTS AND AGENCIES

FROM: Margaret Weichert
Deputy Director for Management

SUBJECT: Update to the Trusted Internet Connections (TIC) Initiative

A. Purpose of the TIC Initiative

The purpose of the Trusted Internet Connections (TIC) initiative is to enhance network security across the Federal Government. Initially, this was done through the consolidation of external connections and the deployment of common tools at these access points. While this prior work has been invaluable in securing Federal networks and information, the program must adapt to modern architectures and frameworks for government IT resource utilization. Accordingly, this memorandum provides an enhanced approach for implementing the TIC initiative that provides agencies with increased flexibility to use modern security capabilities. This memorandum also establishes a process for ensuring the TIC initiative is agile and responsive to advancements in technology and rapidly evolving threats.

B. Rescissions

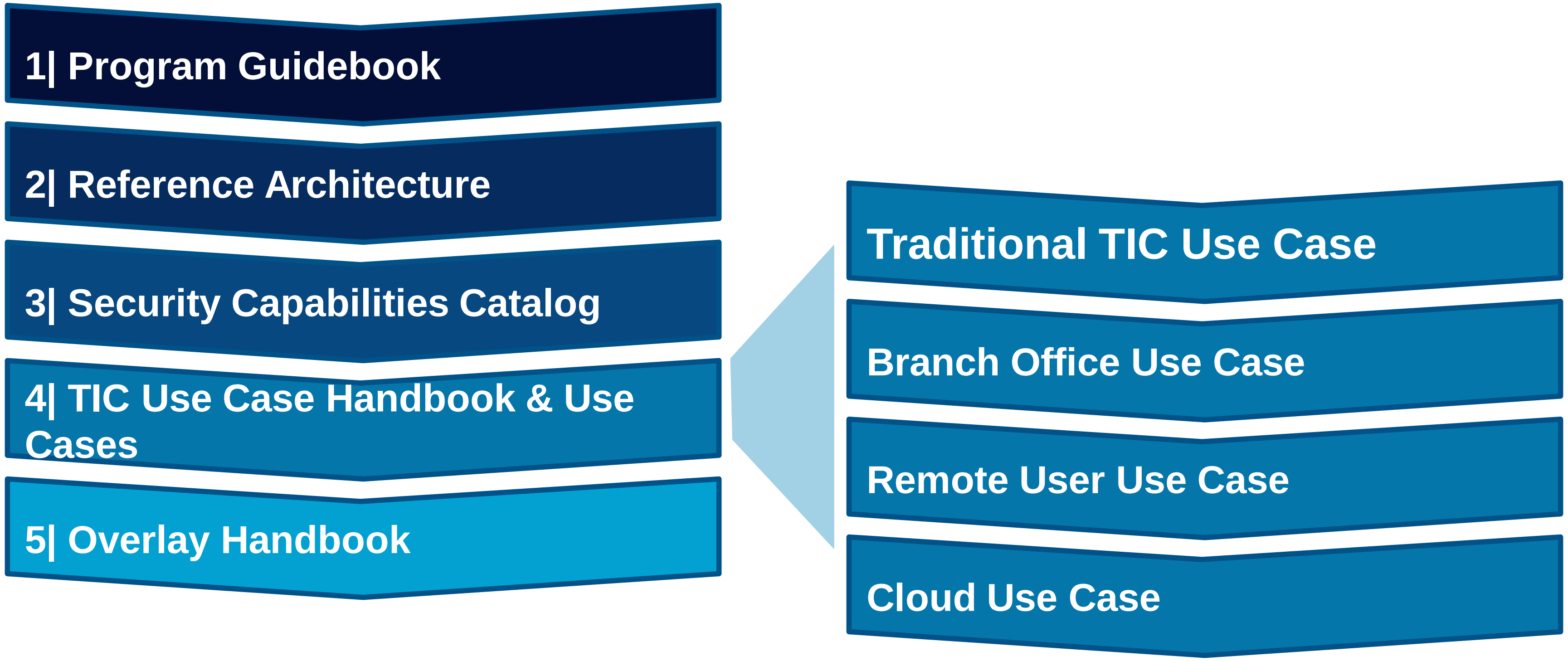
In accordance with Office of Management and Budget (OMB) Memorandum M-17-26, *Reducing Burden for Federal Agencies by Rescinding and Modifying OMB Memoranda*, OMB is rescinding the following memoranda:

1. M-08-05, Implementation of Trusted Internet Connections (TIC) (November 20, 2007)
2. M-08-16, Guidance for TIC Statement of Capability Form (SOC) (April 4, 2008)
3. M-08-27, Guidance for TIC Compliance (September 30, 2008)
4. M-09-32, Update on the TIC Initiative (September 17, 2009)

These previous OMB memoranda required agency traffic to flow through a physical TIC access point, which has proven to be an obstacle to the adoption of cloud-based infrastructure.

C. Removing Barriers to Cloud and Modern Technology Adoption

One of the Administration's top priorities is the modernization of Federal information technology (IT) and promoting policies that adapt to the plethora of technology solutions available to agencies is essential to effectuating that goal. However, a high level of security must still be in place to protect networks from malicious actors. To continue to promote a consistent baseline of security capabilities, the Department of Homeland Security (DHS) will define TIC



1| Program Guidebook

2| Reference Architecture

3| Security Capabilities Catalog

4| TIC Use Case Handbook & Use Cases

5| Overlay Handbook

Traditional TIC Use Case

Branch Office Use Case

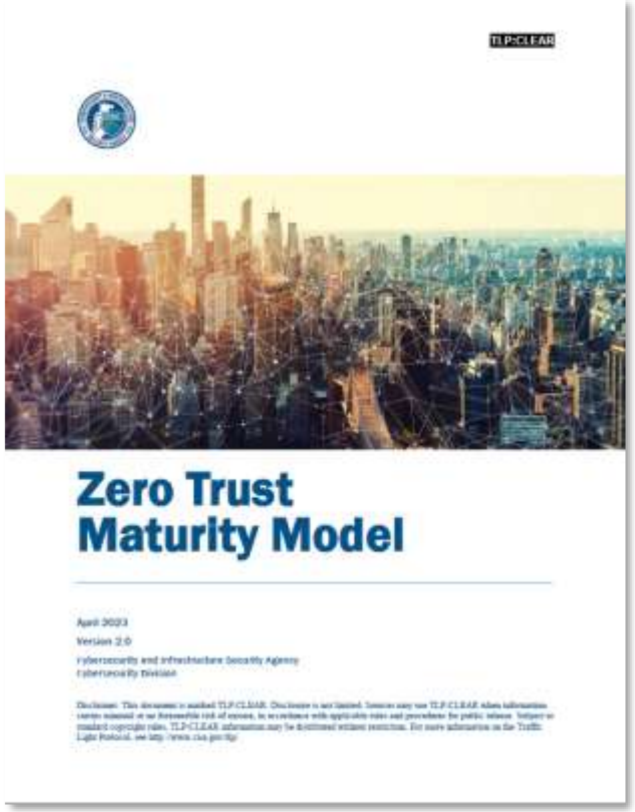
Remote User Use Case

Cloud Use Case

Zero Trust Maturity Model

CISA’s Zero Trust Maturity Model

- This Zero Trust Maturity Model (ZTMM) is one of many paths to support agencies
- Version 2.0 was released in April 2023
- Intent: Help agencies as they develop plans to implement Zero Trust Architectures (ZTA) in response to EO14028 Sec 3,b,ii (May 2021)
- OMB’s M-22-09 (January 2022) requires agencies to achieve specific zero trust security goals that are organized using the ZTMM



TLP:CLEAR

Zero Trust Maturity Model

April 2023

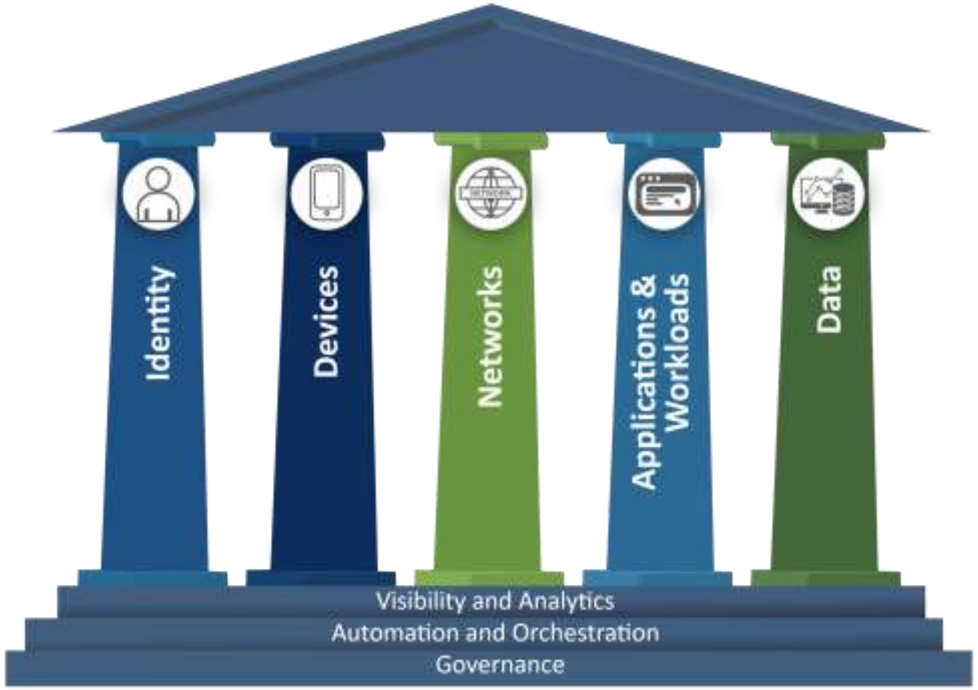
Version 2.0

Cybersecurity and Infrastructure Security Agency
Cybersecurity Division

Disclaimer: This document is marked TLP:CLEAR. Disclosure is not limited. Sources may use TLP:CLEAR when information carries minimal or no foreseeable risk of misuse, in accordance with applicable rules and procedures for public release. Subject to standard copyright rules, TLP:CLEAR information may be distributed without restriction. For more information on the Traffic Light Protocol, see http://www.cisa.gov/tlp/

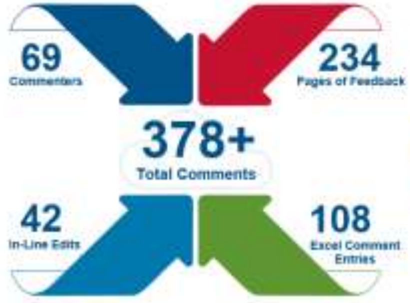
Zero Trust Maturity Model Overview

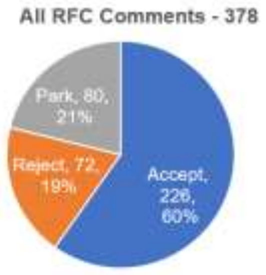
- The ZTMM represents a gradient of implementation across five distinct pillars and three cross-cutting capabilities
  - Functional areas where zero trust principles must be implemented in order to create a secure ZTA
  - Cross-cutting capabilities must be satisfied for each pillar
- Heavily influenced by NIST, DOD, GSA, and NSA's zero trust publications
- This is a general model and is intended to provide direction for Agencies

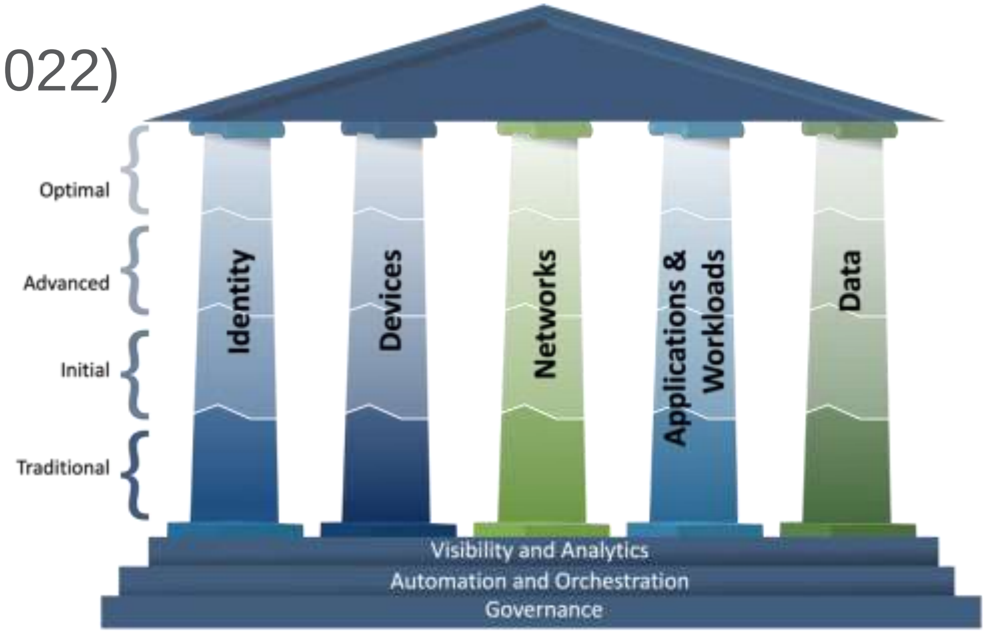


What’s New in ZTMM V2.0?

- Incorporated comments from ZTMM V1.0 Request for Comment (RFC) in 2021
  - Response to Comments published
- Revised Maturity Evolution
- Alignment to OMB M-22-09 (released January 2022)
- Expanded Content and Guidance across pillars
- Clarified Terms and Concepts





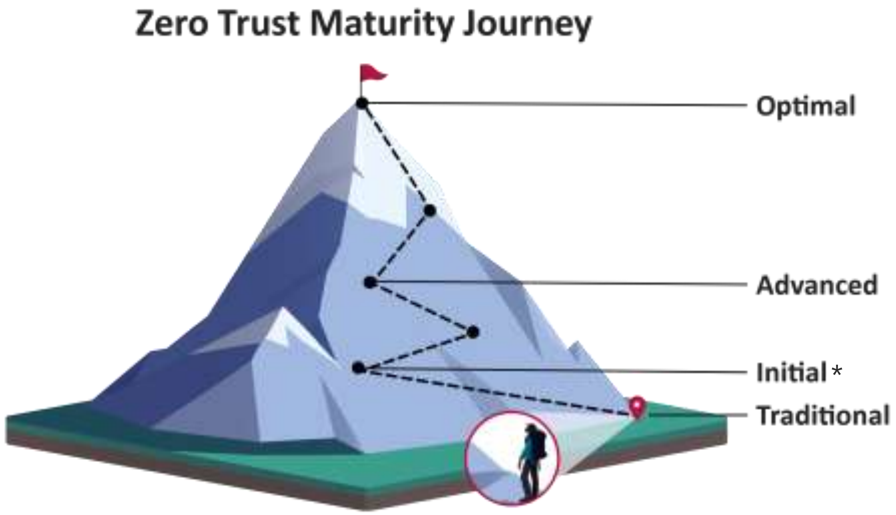


Additional Sources of Feedback

- A review of Zero Trust Implementation Plans with the Office of Management and Budget (OMB)
- Inputs from CyberStat Workshops
- Findings from National Security Telecommunications Advisory Committee (NSTAC) Meetings
- Modernization Deep-Dives
- Individual one-on-one meetings with agencies, international partners, and the greater IT community.

Zero Trust Maturity Journey

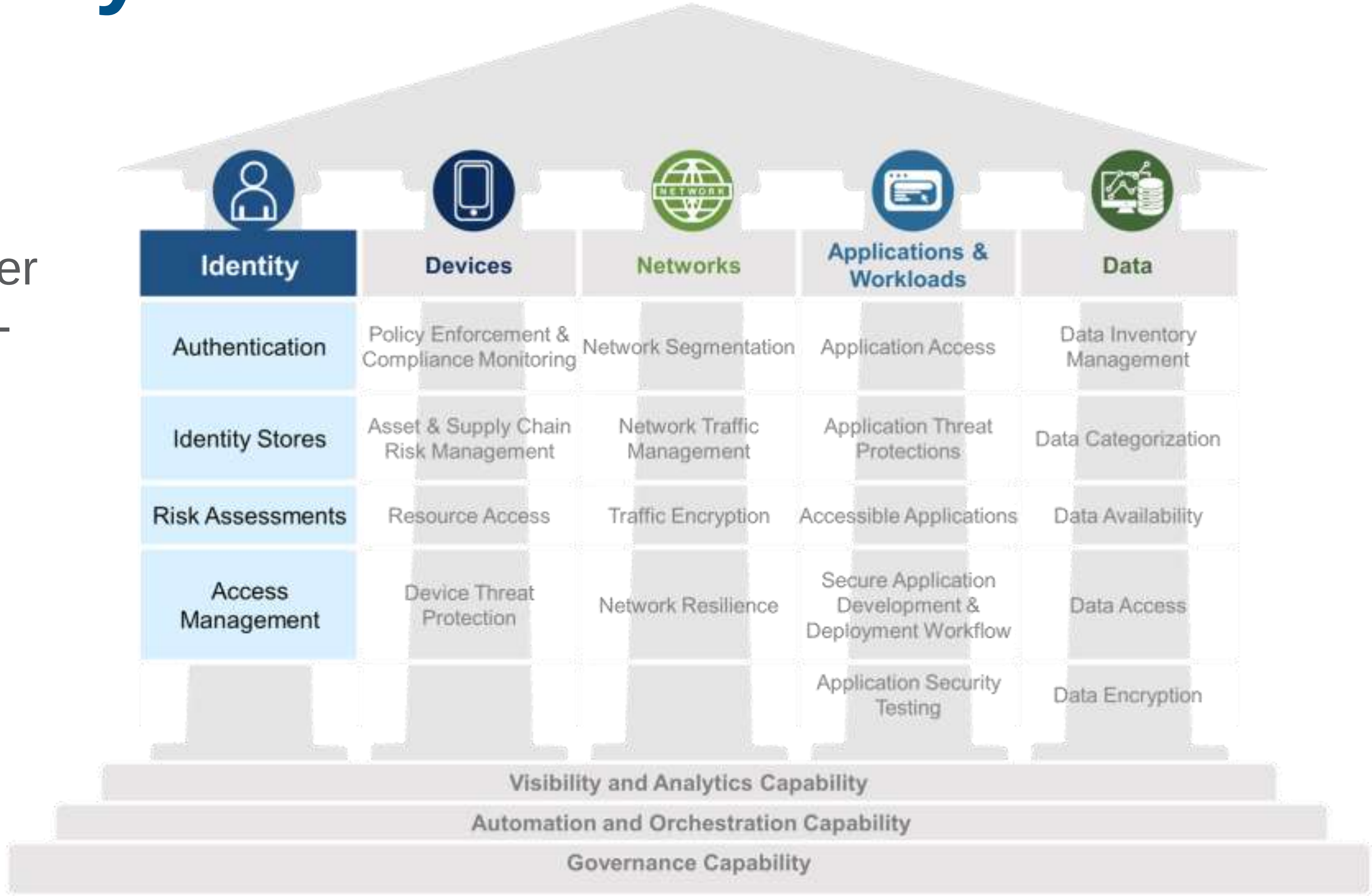
- Each stage on the Zero Trust Maturity Journey requires greater levels of protection, detail, and complexity for adoption, with exponential growth in efforts and benefits.
  - **Traditional:** Manual configuration, response, and mitigation; static and siloed policies and solutions
  - **Initial*:** Starting automation; initial cross-pillar solutions; some responsive changes to least privilege; aggregated visibility for internal systems
  - **Advanced:** Automated controls where applicable; cross-pillar policy enforcement; least-privilege changes based on risk/posture; response to pre-defined mitigations
  - **Optimal:** Fully automated, just-in-time, self-reporting; dynamic least privilege access; cross-pillar interoperability with continuous monitoring, centralized visibility



*New with ZTMM V2

Pillar 1: Identity

- An identity refers to an attribute or set of attributes that uniquely describe an agency user or entity, including non-person entities.



Identity	Devices	Networks	Applications & Workloads	Data
Authentication	Policy Enforcement & Compliance Monitoring	Network Segmentation	Application Access	Data Inventory Management
Identity Stores	Asset & Supply Chain Risk Management	Network Traffic Management	Application Threat Protections	Data Categorization
Risk Assessments	Resource Access	Traffic Encryption	Accessible Applications	Data Availability
Access Management	Device Threat Protection	Network Resilience	Secure Application Development & Deployment Workflow	Data Access
			Application Security Testing	Data Encryption

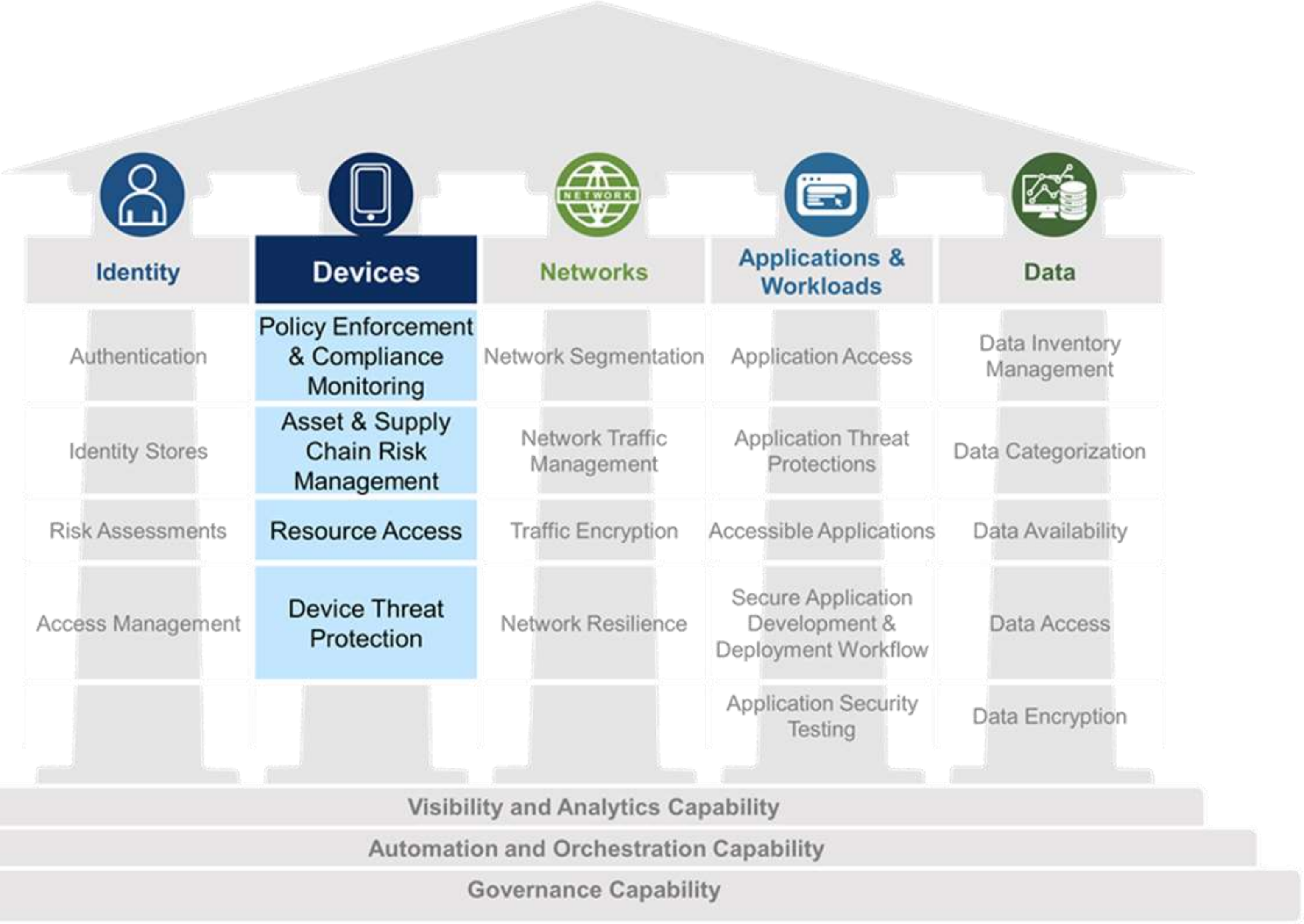
Visibility and Analytics Capability

Automation and Orchestration Capability

Governance Capability

Pillar 2: Devices

- A device refers to any asset (including its hardware, software, firmware, etc.) that can connect to a network, including servers, desktop and laptop machines, printers, mobile phones, IoT devices, networking equipment, and more.



Identity	Devices	Networks	Applications & Workloads	Data
Authentication	Policy Enforcement & Compliance Monitoring	Network Segmentation	Application Access	Data Inventory Management
Identity Stores	Asset & Supply Chain Risk Management	Network Traffic Management	Application Threat Protections	Data Categorization
Risk Assessments	Resource Access	Traffic Encryption	Accessible Applications	Data Availability
Access Management	Device Threat Protection	Network Resilience	Secure Application Development & Deployment Workflow	Data Access
			Application Security Testing	Data Encryption

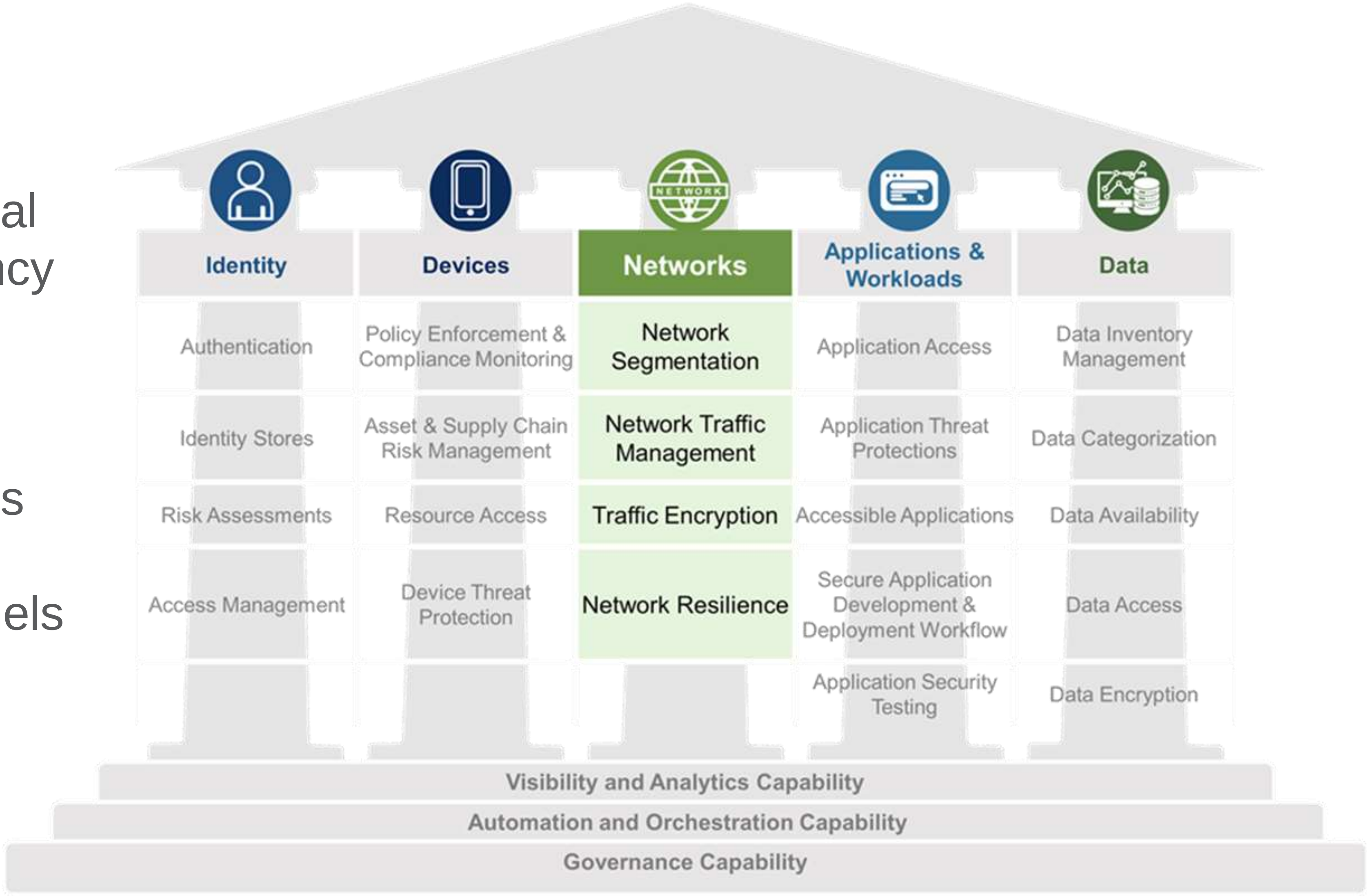
Visibility and Analytics Capability

Automation and Orchestration Capability

Governance Capability

Pillar 3: Networks

- A network refers to an open communications medium including typical channels such as agency internal networks, wireless networks, and the Internet as well as other potential channels such as cellular and application-level channels used to transport messages.



Identity	Devices	Networks	Applications & Workloads	Data
Authentication	Policy Enforcement & Compliance Monitoring	Network Segmentation	Application Access	Data Inventory Management
Identity Stores	Asset & Supply Chain Risk Management	Network Traffic Management	Application Threat Protections	Data Categorization
Risk Assessments	Resource Access	Traffic Encryption	Accessible Applications	Data Availability
Access Management	Device Threat Protection	Network Resilience	Secure Application Development & Deployment Workflow	Data Access
			Application Security Testing	Data Encryption

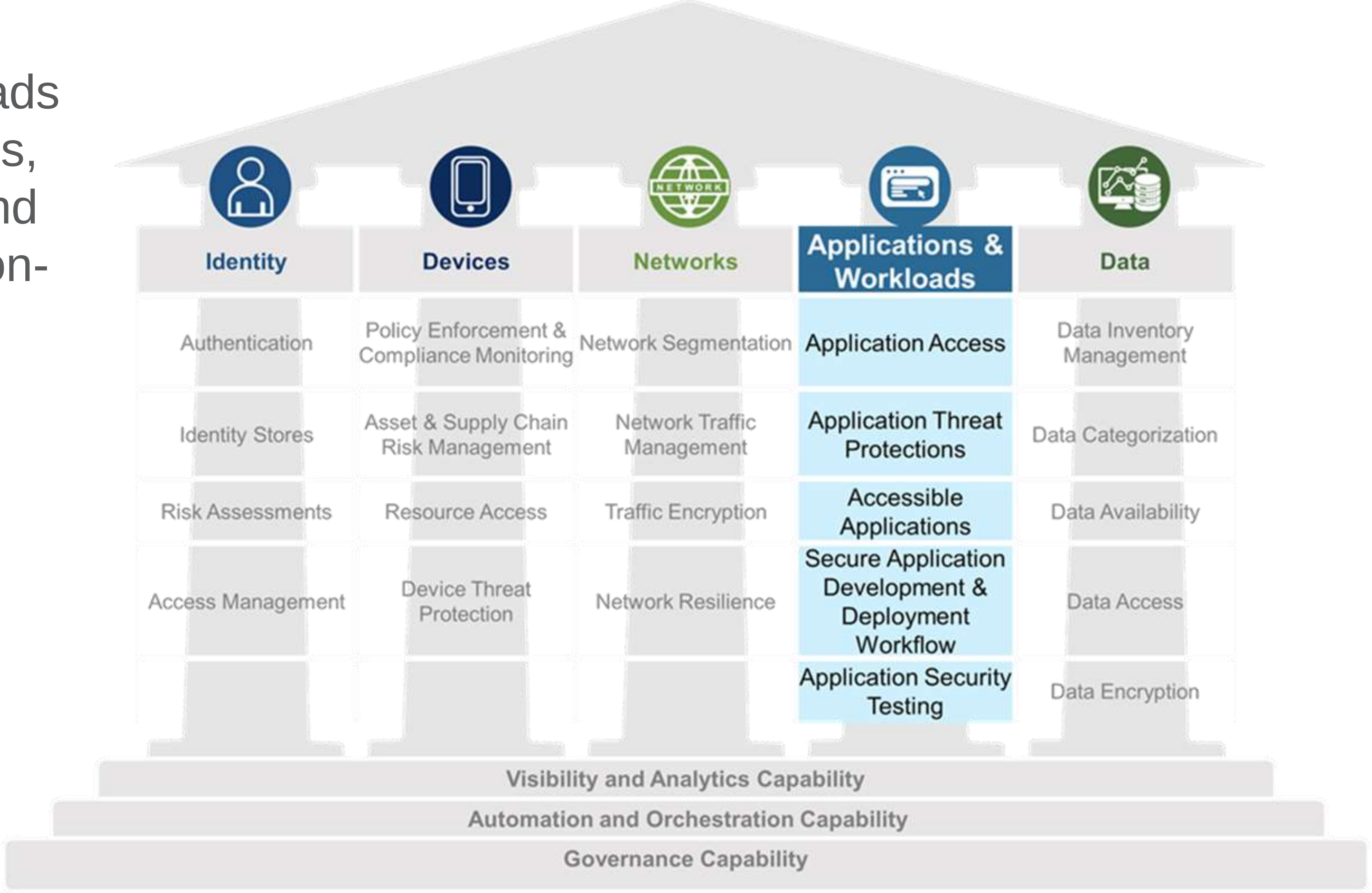
Visibility and Analytics Capability

Automation and Orchestration Capability

Governance Capability

Pillar 4: Applications & Workloads

- Applications & Workloads include agency systems, computer programs, and services that execute on-premise, on mobile devices, and in cloud environments.



Identity	Devices	Networks	Applications & Workloads	Data
Authentication	Policy Enforcement & Compliance Monitoring	Network Segmentation	Application Access	Data Inventory Management
Identity Stores	Asset & Supply Chain Risk Management	Network Traffic Management	Application Threat Protections	Data Categorization
Risk Assessments	Resource Access	Traffic Encryption	Accessible Applications	Data Availability
Access Management	Device Threat Protection	Network Resilience	Secure Application Development & Deployment Workflow	Data Access
			Application Security Testing	Data Encryption

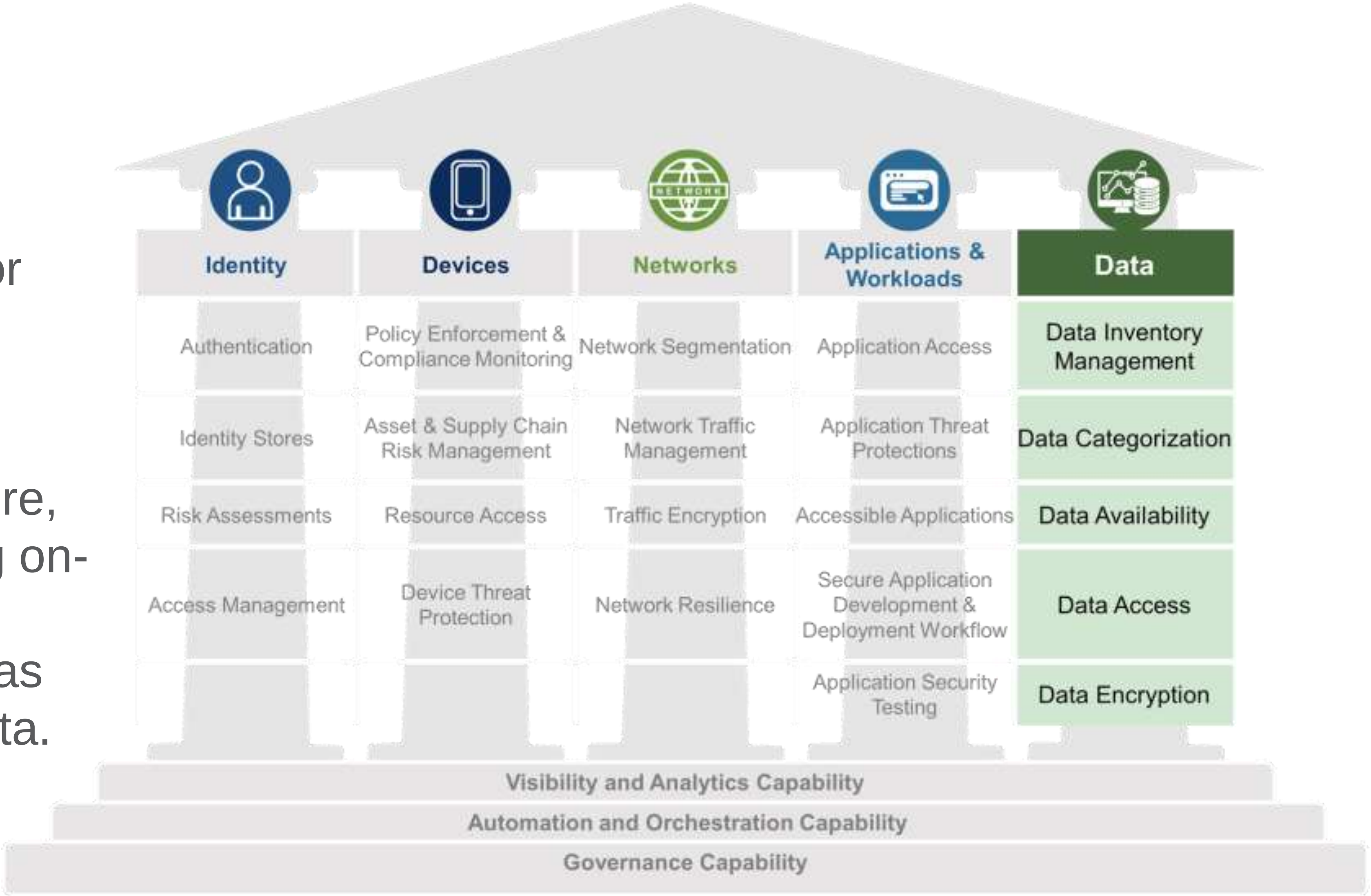
Visibility and Analytics Capability

Automation and Orchestration Capability

Governance Capability

Pillar 5: Data

- Data includes all structured and unstructured files and fragments that reside or have resided in federal systems, devices, networks, applications, databases, infrastructure, and backups (including on-premises and virtual environments) as well as the associated metadata.



Identity	Devices	Networks	Applications & Workloads	Data
Authentication	Policy Enforcement & Compliance Monitoring	Network Segmentation	Application Access	Data Inventory Management
Identity Stores	Asset & Supply Chain Risk Management	Network Traffic Management	Application Threat Protections	Data Categorization
Risk Assessments	Resource Access	Traffic Encryption	Accessible Applications	Data Availability
Access Management	Device Threat Protection	Network Resilience	Secure Application Development & Deployment Workflow	Data Access
			Application Security Testing	Data Encryption

Visibility and Analytics Capability

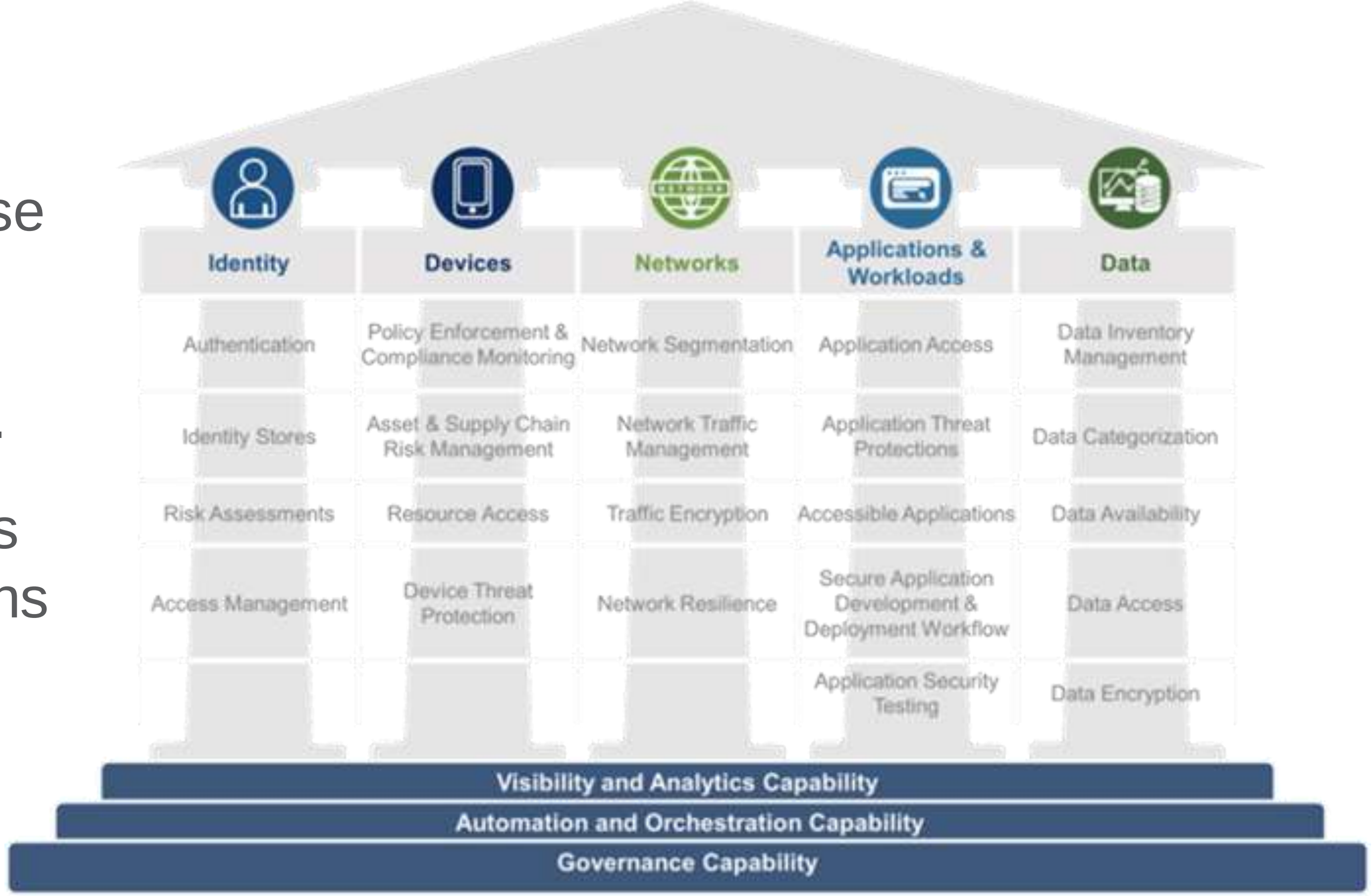
Automation and Orchestration Capability

Governance Capability

Cross-Cutting Capabilities

- These cross-cutting capabilities provide opportunities to integrate advancements across each of the five pillars. As agencies mature these capabilities with respect to a given pillar, they can also mature each capability independent of the pillars.

- These capabilities highlight activities to support interoperability of functions across pillars. As agencies mature these capabilities within each pillar, they can mature each capability independent of pillars as well.



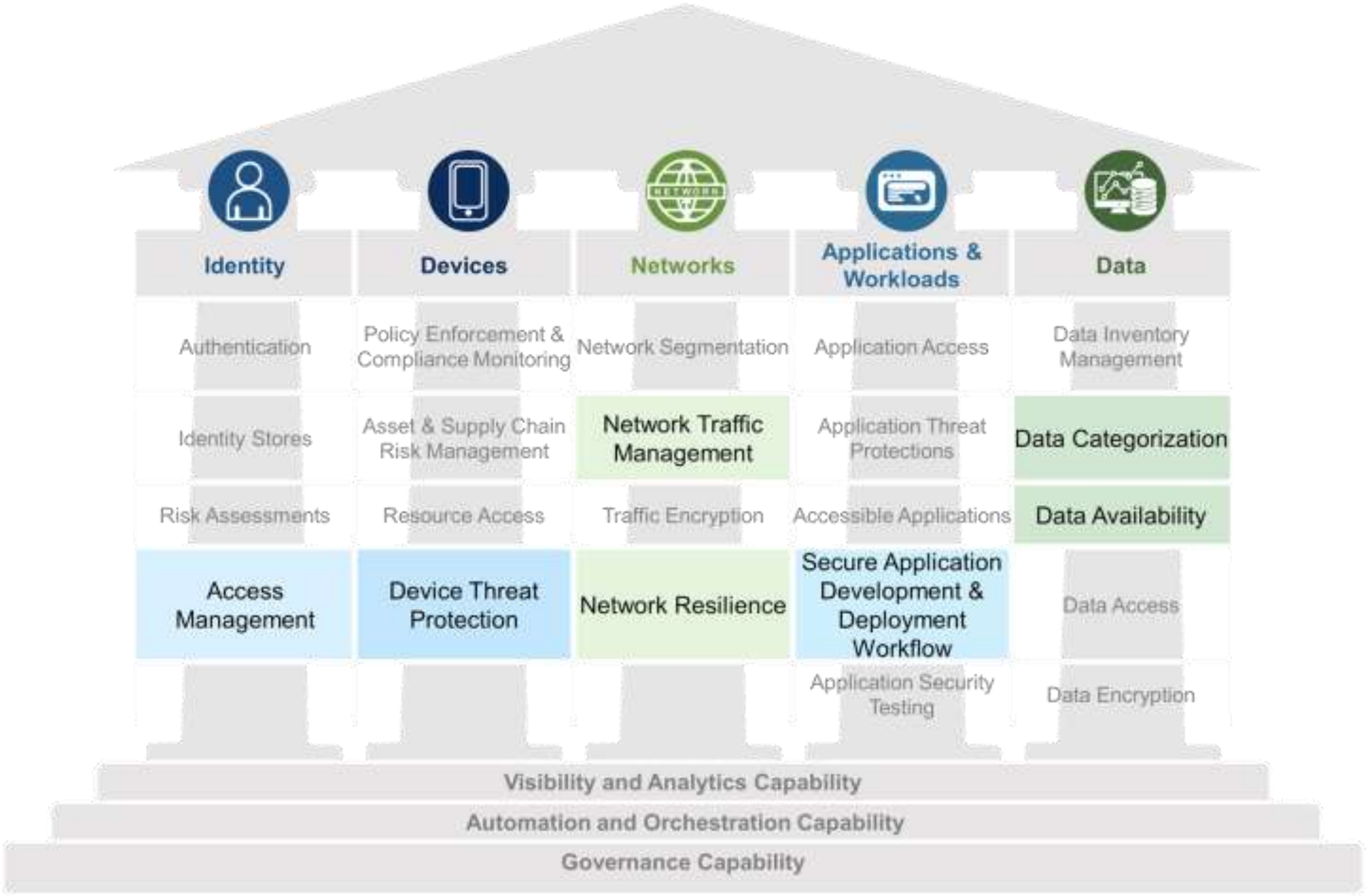
Identity	Devices	Networks	Applications & Workloads	Data
Authentication	Policy Enforcement & Compliance Monitoring	Network Segmentation	Application Access	Data Inventory Management
Identity Stores	Asset & Supply Chain Risk Management	Network Traffic Management	Application Threat Protections	Data Categorization
Risk Assessments	Resource Access	Traffic Encryption	Accessible Applications	Data Availability
Access Management	Device Threat Protection	Network Resilience	Secure Application Development & Deployment Workflow	Data Access
			Application Security Testing	Data Encryption

Visibility and Analytics Capability

Automation and Orchestration Capability

Governance Capability

ZTMM V2 New Functions



Identity	Devices	Networks	Applications & Workloads	Data
Authentication	Policy Enforcement & Compliance Monitoring	Network Segmentation	Application Access	Data Inventory Management
Identity Stores	Asset & Supply Chain Risk Management	Network Traffic Management	Application Threat Protections	Data Categorization
Risk Assessments	Resource Access	Traffic Encryption	Accessible Applications	Data Availability
Access Management	Device Threat Protection	Network Resilience	Secure Application Development & Deployment Workflow	Data Access
			Application Security Testing	Data Encryption

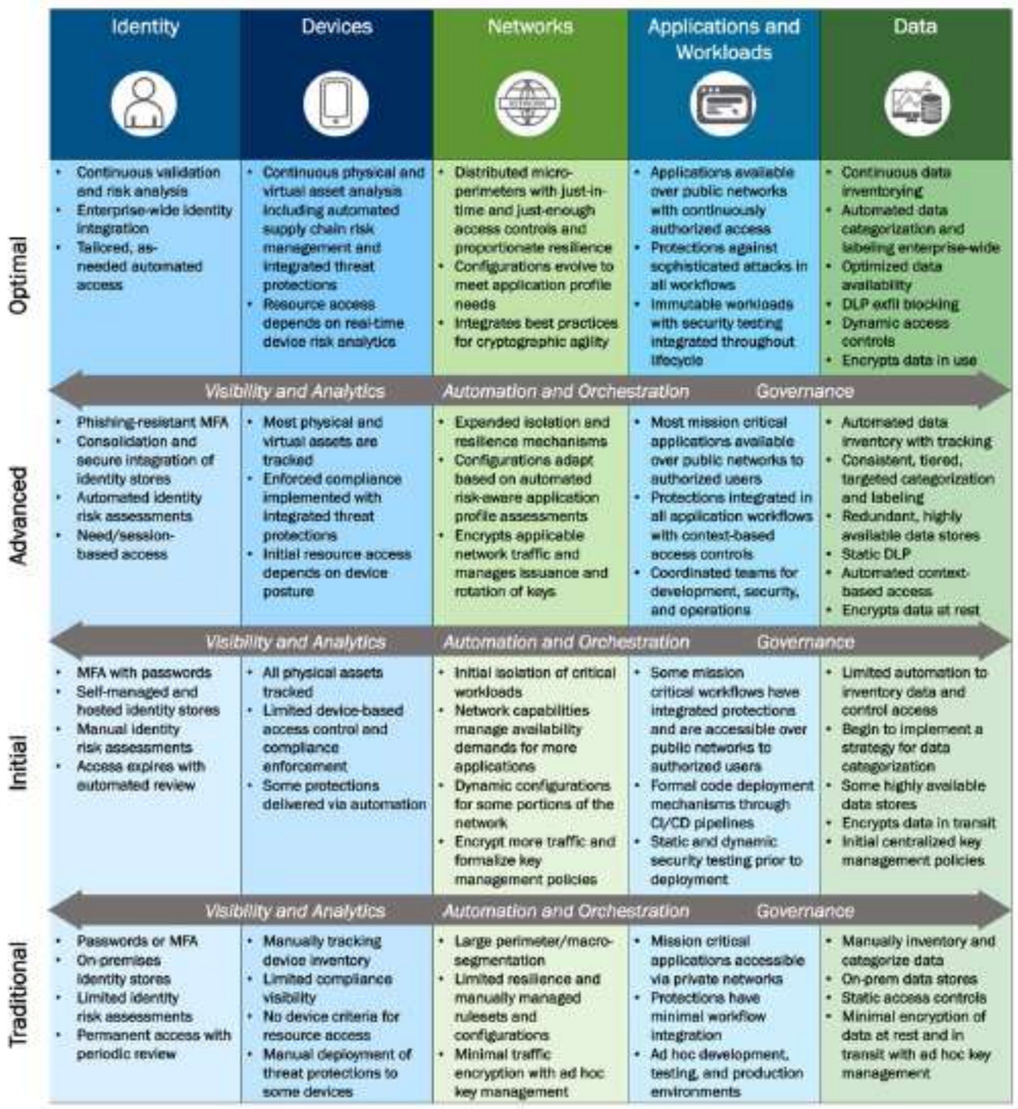
Visibility and Analytics Capability

Automation and Orchestration Capability

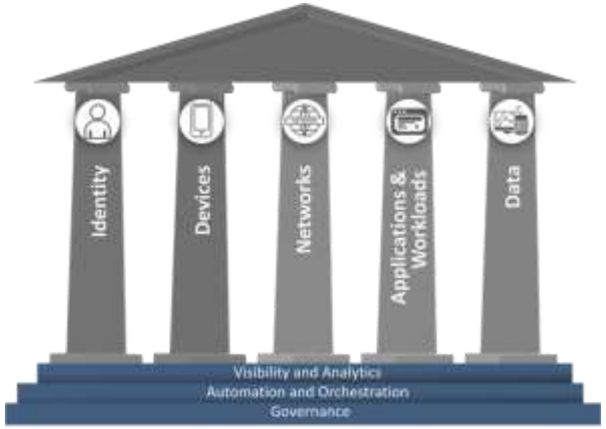
Governance Capability

Cross-Cutting Capabilities are Matrixed

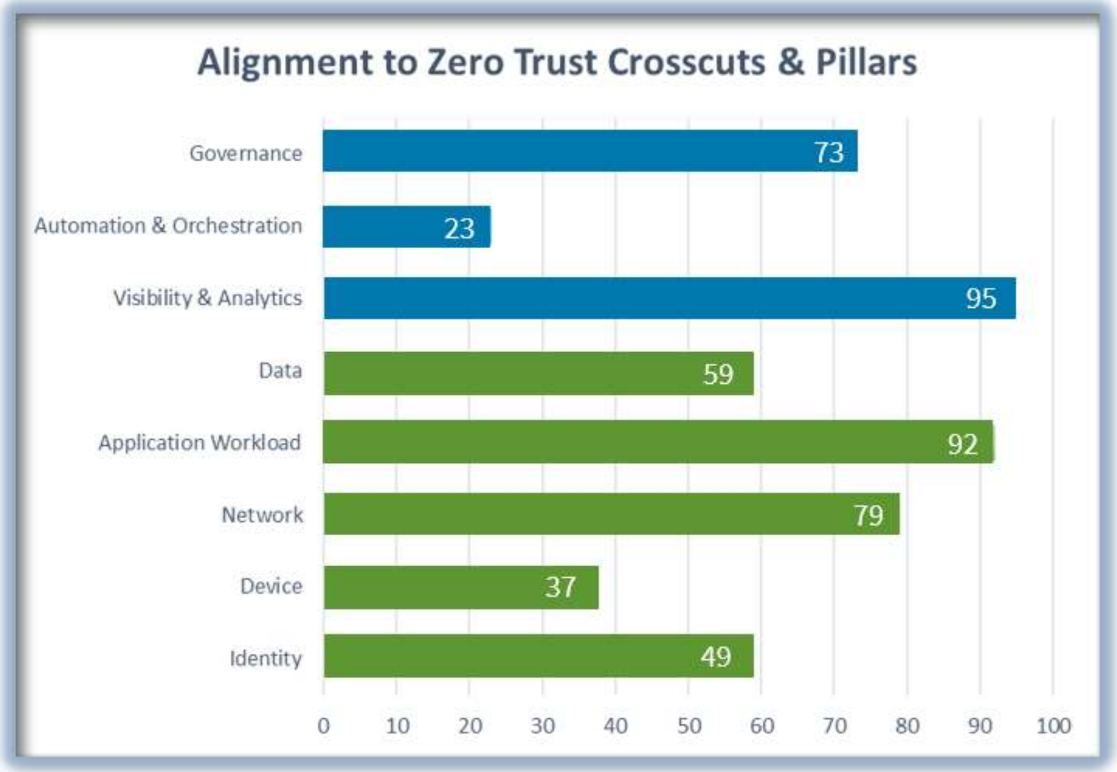
- The three capabilities are woven into each of the pillars.
- Each capability also has distinct maturity levels.



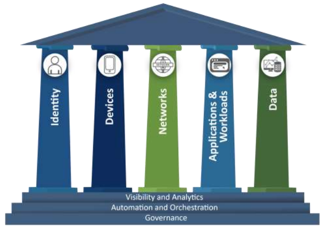
	Identity	Devices	Networks	Applications and Workloads	Data
Optimal	• Continuous validation and risk analysis • Enterprise-wide identity integration • Tailored, as-needed automated access	• Continuous physical and virtual asset analysis including automated supply chain risk management and integrated threat protections • Resource access depends on real-time device risk analytics	• Distributed micro-perimeters with just-in-time and just-enough access controls and proportionate resilience • Configurations evolve to meet application profile needs • Integrates best practices for cryptographic agility	• Applications available over public networks with continuously authorized access • Protections against sophisticated attacks in all workflows • Immutable workloads with security testing integrated throughout lifecycle	• Continuous data inventorying • Automated data categorization and labeling enterprise-wide • Optimized data availability • DLP exfil blocking • Dynamic access controls • Encrypts data in use
	Visibility and Analytics		Automation and Orchestration		Governance
Advanced	• Phishing-resistant MFA • Consolidation and secure integration of identity stores • Automated identity risk assessments • Need/session-based access	• Most physical and virtual assets are tracked • Enforced compliance implemented with integrated threat protections • Initial resource access depends on device posture	• Expended isolation and resilience mechanisms • Configurations adapt based on automated risk-aware application profile assessments • Encrypts applicable network traffic and manages issuance and rotation of keys	• Most mission critical applications available over public networks to authorized users • Protections integrated in all application workflows with context-based access controls • Coordinated teams for development, security, and operations	• Automated data inventory with tracking • Consistent, tiered, targeted categorization and labeling • Redundant, highly available data stores • Static DLP • Automated context-based access • Encrypts data at rest
	Visibility and Analytics		Automation and Orchestration		Governance
Initial	• MFA with passwords • Self-managed and hosted identity stores • Manual identity risk assessments • Access expires with automated review	• All physical assets tracked • Limited device-based access control and compliance enforcement • Some protections delivered via automation	• Initial isolation of critical workloads • Network capabilities manage availability demands for more applications • Dynamic configurations for some portions of the network • Encrypt more traffic and formalize key management policies	• Some mission critical workflows have integrated protections and are accessible over public networks to authorized users • Formal code deployment mechanisms through CI/CD pipelines • Static and dynamic security testing prior to deployment	• Limited automation to inventory data and control access • Begin to implement a strategy for data categorization • Some highly available data stores • Encrypts data in transit • Initial centralized key management policies
	Visibility and Analytics		Automation and Orchestration		Governance
Traditional	• Passwords or MFA • On-premises identity stores • Limited identity risk assessments • Permanent access with periodic review	• Manually tracking device inventory • Limited compliance visibility • No device criteria for resource access • Manual deployment of threat protections to some devices	• Large perimeter/macro-segmentation • Limited resilience and manually managed rulesets and configurations • Minimal traffic encryption with ad hoc key management	• Mission critical applications accessible via private networks • Protections have minimal workflow integration • Ad hoc development, testing, and production environments	• Manually inventory and categorize data • On-prem data stores • Static access controls • Minimal encryption of data at rest and in transit with ad hoc key management



Mapping TIC Capabilities to ZTMM



117 Total TIC Security Capabilities



- **Stronger alignment:**
  - Visibility & Analytics Crosscut
  - Network Pillar
  - Application Workload Pillar

- **Weaker alignment:**
  - Automation & Orchestration Crosscut
  - Identity Pillar
  - Device Pillar

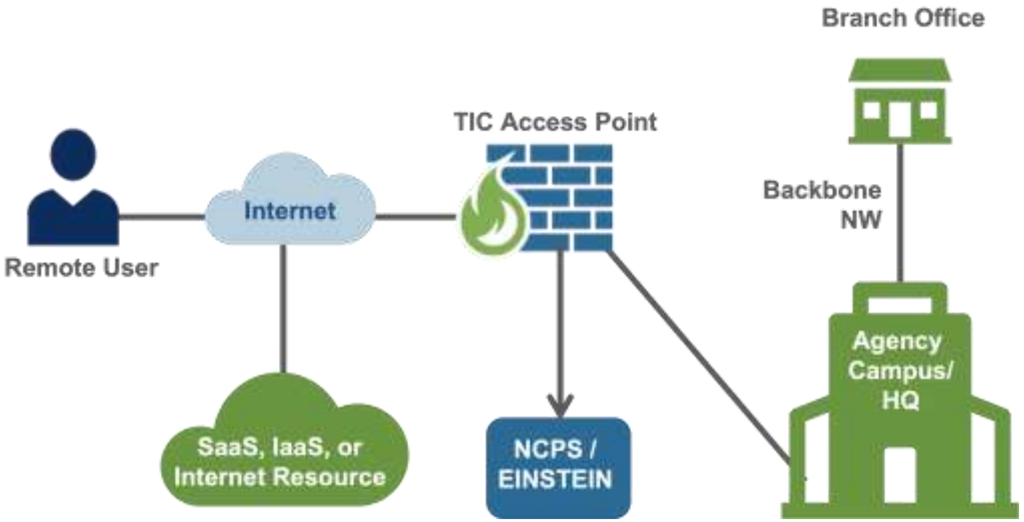
Findings are unsurprising given history of TIC

Other Zero Trust Efforts

TIC2 vs.TIC3 with SSE/SASE

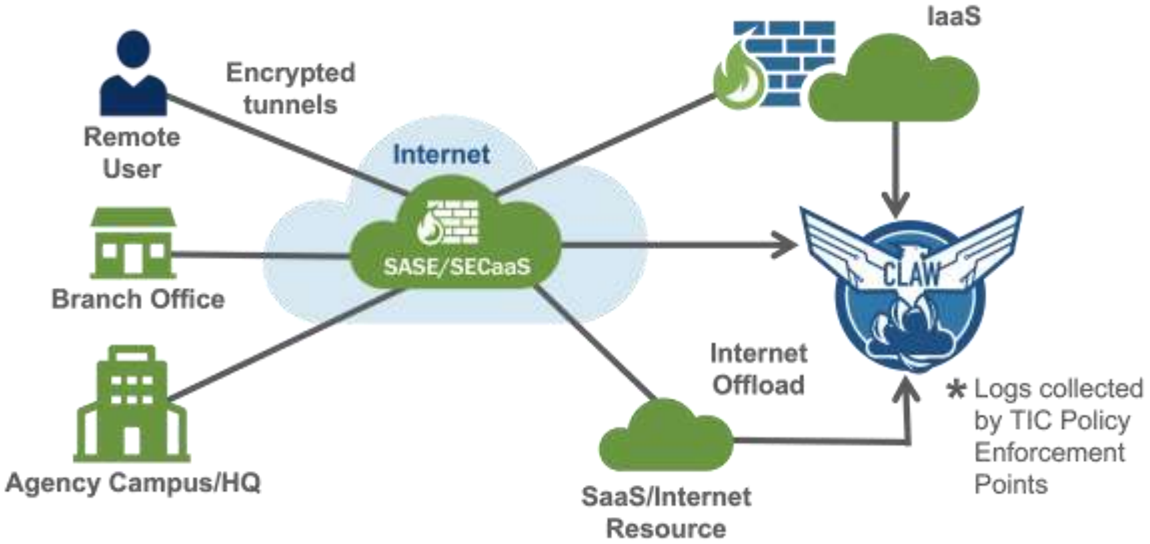
TIC 2.0 - Traditional TIC/Managed Trusted Internet Protocol Service (MTIPS)

- Acceptable architecture to meet TIC 3.0 requirements
- Defined by the Traditional TIC Use Case
- Provides perimeter security by funneling all incoming and outgoing data through TIC Access Points



TIC 3.0 –Secure Access Service Edge (SASE)/ Security Service Edge (SSE)

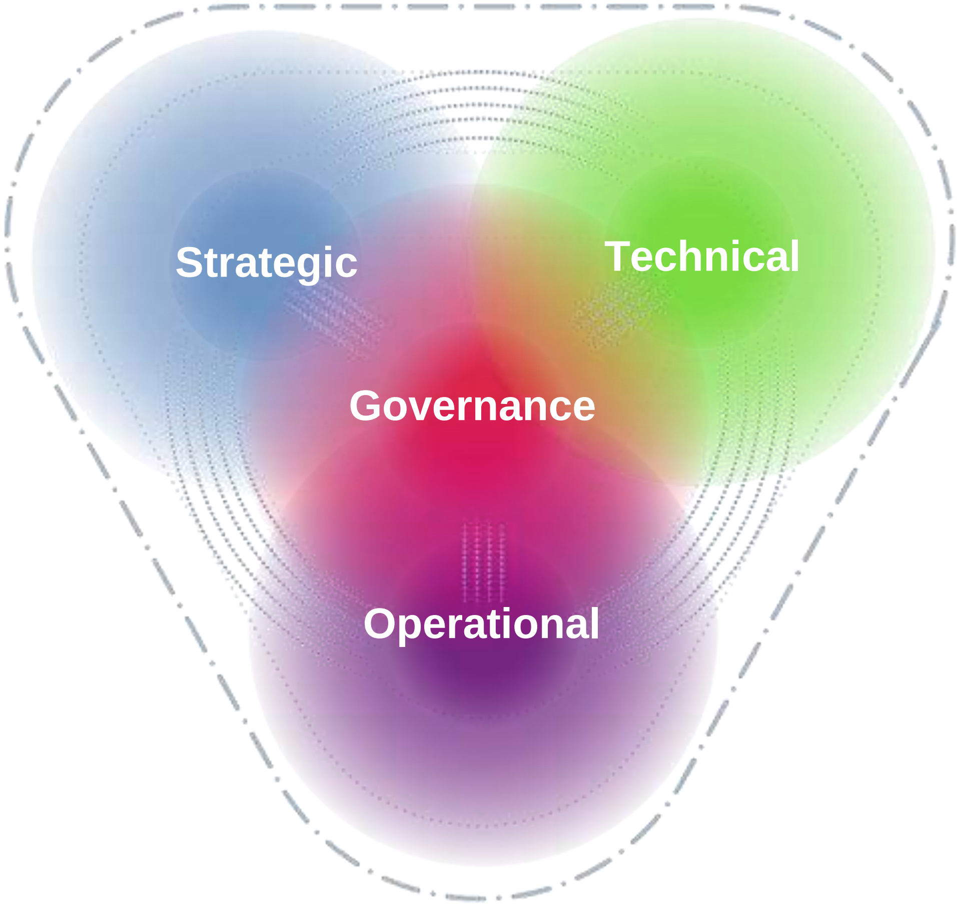
- Acceptable architecture to meet TIC 3.0 requirements with greater flexibility than traditional TIC2/MTIPS model to account for multiple and diverse architectures rather than single perimeter approach
- Zero Trust Network Access (ZTNA) provided through policy enforcement parity with TIC Access Point



* Logs collected by TIC Policy Enforcement Points

Related Efforts

To address gaps, CISA has produced strategic, technical, and operational documents.



- Federal Zero Trust Strategy: Serves as the official zero trust strategy for the federal government with the goal of accelerating agencies towards a shared baseline
- Zero Trust Maturity Model: Supports Federal Civilian Executive Branch (FCEB) in designing zero trust architecture (ZTA).
- Cloud Security Technical Reference Architecture (CSTRA): Illustrates recommended approaches to cloud migration and data protection for agency data collection and reporting.
- Trusted Internet Connections (TIC) Document Set: Defines the concepts of the program (Trust Zones, PEPs, MGMT) to guide and constrain the diverse implementations of the security capabilities.
- NCPS Cloud Interface Reference Architecture (NCIRA): Accommodates collection of agency data from cloud environments.
- Secure Cloud Business Applications (SCuBA): Highlights development of methods for ingesting and processing multiple types of cloud-based threat information.
- Extensible Visibility Reference Framework (eVRF): Expands coverage for CISA CSD visibility requirements and provides measures for coverage of CSD visibility.

CISA Efforts towards Zero Trust – CLAW

CISA's Cloud Log Aggregation Warehouse (CLAW)

- As agencies move to modern, distributed architectures and from TIC 2.0 to TIC 3.0, participation in CLAW will be critical
- CLAW is a distributed log ingest service – AWS (2022), Microsoft Azure (now available), GCP next
- Initial telemetry of interest
  - Microsoft Azure Active Directory logs
  - M365 Unified Audit Logs
  - AWS Cloud Trail access and authentication logs
  - GCP & GWS logs
  - SASE type logs
  - Other logs – stay tuned

Why is moving to Zero Trust important?

- Some of the Zero Trust benefits that are important to CISA:
  - Reduce the Attack Surface
  - Improve the User Experience
  - Improve Incident Management
- Where we need help?
  - Education & training
  - Guidance (Use Cases and Playbooks)
  - Interoperability of solutions
  - How to measure Zero Trust progress

Acronyms

- Amazon Web Services (AWS)
- Asset Management Baselining (AMB)
- Cloud Log Aggregation Warehouse (CLAW)
- Cloud Security Posture Management (CSPM)
- Continuous Diagnostics and Mitigation (CDM)
- Cybersecurity Division (CSD)
- Cybersecurity and Infrastructure Security Agency (CISA)
- Cybersecurity Technical reference Architecture (CSTRA)
- Department of Defense (DoD)
- Department of Homeland Security (DHS)
- Domain Name System (DNS)
- EINSTEIN 3 Accelerated (E3A)
- Endpoint Detection & Response (EDR)
- Enterprise Infrastructure Solutions (EIS)
- Executive Order (EO)
- Extensible Visibility Reference Framework (eVRF)
- Federal Civilian Executive Branch (FCEB)
- General Services Administration (GSA)
- Google Cloud Platform (GCP)
- Identity Lifecycle Management (ILM)
- Internet of Things (IoT)
- National Cyber Protection System (NCPS)
- NCPS Cloud Interface Reference Architecture (NCIRA)
- National Institute of Standards and Technology (NIST)
- National Security Agency (NSA)
- National Security Telecommunications Advisory Committee (NSTAC)
- Office of Management and Budget (OMB)
- Office of the Technical Director (OTD)
- Persistent Access Capability (PAC)
- Policy Enforcement Point (PEP)
- Program Management Office (PMO)
- Risk Management Framework (RMF)
- Secure Access Service Edge (SASE)
- Secure Cloud Business Applications (SCuBA)
- Special Publication (SP)
- The Technology Modernization Fund (TMF)
- Trusted Internet Connections (TIC)
- Zero Trust (ZT)
- Zero Trust Architecture (ZTA)
- Zero Trust Maturity Model (ZTMM)

Questions?

For CISA Media inquiries:
Contact CISA Media at
CISAMedia@cisa.dhs.gov
or 703-235-2010

Zero Trust Maturity Model Webpage:
https://www.cisa.gov/zero-trust-maturity-model

Zero Trust Mailbox:
zerotrust@cisa.dhs.gov

CYBERSECURITY & INFRASTRUCTURE SECURITY AGENCY

CISA