CISA | CYBERSECURITY AND INFRASTRUCTURE SECURITY AGENCY

930GOV

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: CISA 930gov

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

CYBERSECURITY & INFRASTRUCTURE SECURITY AGENCY

AMERICA'S CYBER DEFENSE AGENCY

Cybersecurity and Infrastructure Security Agency (CISA)

VISION

Secure and resilient infrastructure for the American people.

MISSION

CISA partners with industry and government to understand and manage risk to our Nation's critical infrastructure.

OVERALL GOALS

GOAL 1

DEFEND TODAY

Defend against urgent threats and hazards

seconds | days | weeks

GOAL 2

SECURE TOMORROW

Strengthen critical infrastructure and address long-term risks

months | years | decades

CYBERSECURITY & INFRASTRUCTURE SECURITY AGENCY

Cybersecurity Division

The Cybersecurity Division (CSD) assures the security, resilience, and reliability of the nation's cyber systems.

MISSION PRIORITIES:

Cyber Defense Operations - CISA detects and prevents cybersecurity risks where possible through information sharing and deployment of detective and preventative technologies and by providing incident response and "hunt" capabilities to minimize impacts of identified incidents.

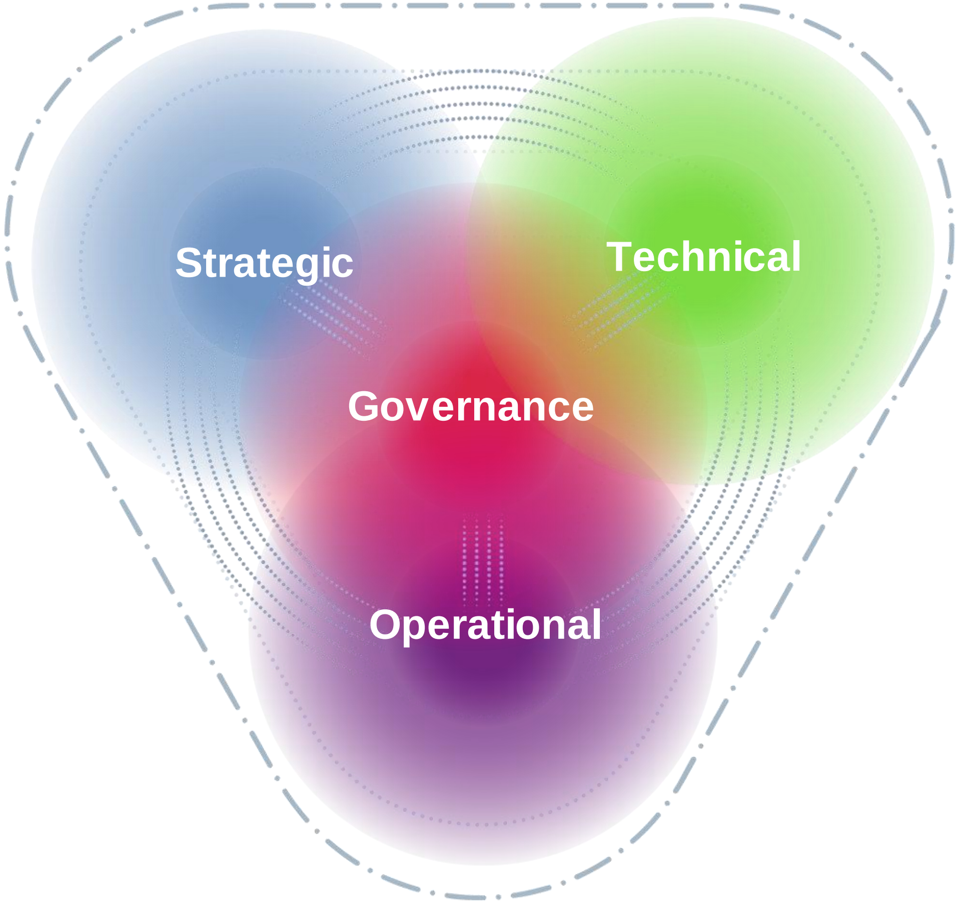
Federal Networks Governance and Capacity Building - To raise the federal cybersecurity baseline, CISA provides tools, services, expert guidance, and cybersecurity directives to drive cybersecurity risk management within agency defined risk tolerance and CISA's continuous analysis of cyber risks across the Federal enterprise.

Critical Infrastructure/SLTT Governance and Capability Building - CISA provides non-federal entities with cybersecurity information, assessments, and incident response assistance to enable more comprehensive cybersecurity risk management of the critical functions that underpin our national security, public health and safety, and economic security. Support and enable non-federal entities to better manage risk at an acceptable level commensurate with their own defined risk tolerance and national risks of national security, public health and safety, and economic security.

Long-term Cybersecurity - CISA drives national efforts to create a more secure cyber ecosystem through collaboration with the private sector, academia, and government partners to build a diverse cyber workforce, foster development and use of secure technologies, and promote cybersecurity best practices across all organizations.

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.

Federal Zero Trust Efforts

National Security Agency | Cybersecurity Information

Embracing a Zero Trust Security Model

NIST CYBERSECURITY WHITE PAPER (DRAFT)

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

October 21, 2022

GSA

EIS and Zero Trust Architecture

How are you progressing on your Zero Trust Architecture journey?

GSA

Zero Trust Architecture (ZTA) Buyer's Guide

June 2021

BRIEFING ROOM

Executive Order on Improving the Nation's Cybersecurity

MAY 12, 2021 • PRESIDENTIAL ACTIONS

By the authority vested in me as President by the Constitution and the laws of the United States of America, it is hereby ordered as follows:

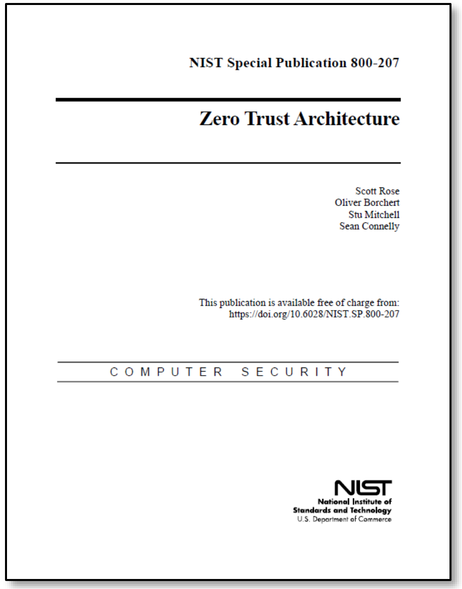
Section 1. Policy. The United States faces persistent and increasingly sophisticated malicious cyber campaigns that threaten the public sector, the private sector, and ultimately the American people's security and privacy. The Federal Government must improve its efforts to identify, deter, protect against, detect, and respond to these actions and actors. The Federal Government must also carefully examine what occurred during any major cyber incident and apply lessons learned. But cybersecurity requires more than government action. Protecting our Nation from malicious cyber actors requires the Federal Government to partner with the private sector. The private sector must adapt to the continuously changing threat environment, ensure its products are built and operate securely, and partner with the Federal Government to foster a more secure cyberspace. In the end, the trust we place in our digital infrastructure should be proportional to how trustworthy and transparent that infrastructure is, and to the consequences we will incur if that trust is misplaced.

Incremental improvements will not give us the security we need; instead, the Federal Government needs to make bold changes and significant investments in order to defend the vital institutions that underpin the American way of life. The Federal Government must bring to bear the full scope of its authorities and resources to protect and secure its computer systems, whether they are cloud-based, on-premises, or hybrid. The scope of protection and security must include systems that process data (information

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

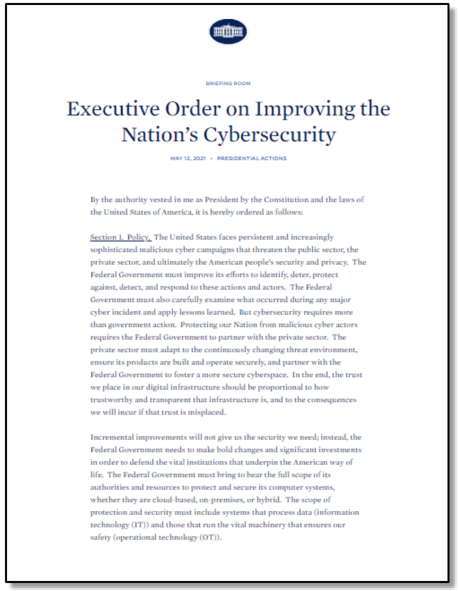
This publication is available free of charge from:
https://doi.org/10.6028/NIST.SP.800-207

COMPUTER SECURITY

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

The Principles

NIST SP 800-207
Zero Trust
Architecture



BRIEFING ROOM

Executive Order on Improving the Nation's Cybersecurity

MAY 12, 2021 • PRESIDENTIAL ACTIONS

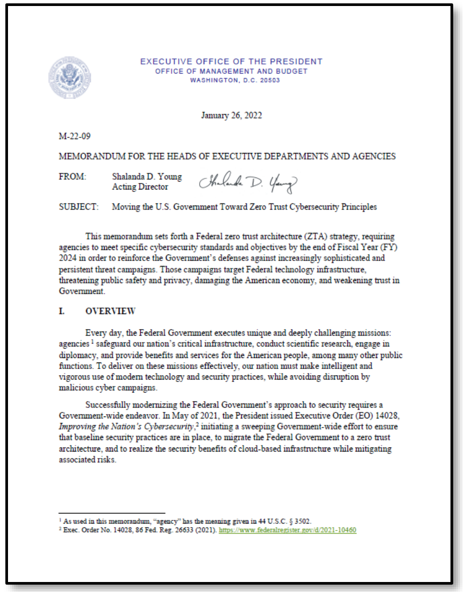
By the authority vested in me as President by the Constitution and the laws of the United States of America, it is hereby ordered as follows:

Section 1. Policy. The United States faces persistent and increasingly sophisticated malicious cyber campaigns that threaten the public sector, the private sector, and ultimately the American people's security and privacy. The Federal Government must improve its efforts to identify, deter, protect against, detect, and respond to these actions and actors. The Federal Government must also carefully examine what occurred during any major cyber incident and apply lessons learned. But cybersecurity requires more than government action. Protecting our Nation from malicious cyber actors requires the Federal Government to partner with the private sector. The private sector must adapt to the continuously changing threat environment, ensure its products are built and operate securely, and partner with the Federal Government to foster a more secure cyberspace. In the end, the trust we place in our digital infrastructure should be proportional to how trustworthy and transparent that infrastructure is, and to the consequences we will incur if that trust is misplaced.

Incremental improvements will not give us the security we need; instead, the Federal Government needs to make bold changes and significant investments in order to defend the vital institutions that underpin the American way of life. The Federal Government must bring to bear the full scope of its authorities and resources to protect and secure its computer systems, whether they are cloud-based, on-premises, or hybrid. The scope of protection and security must include systems that process data (information technology (IT)) and those that run the vital machinery that ensures our safety (operational technology (OT)).

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
Shalanda D. Young

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

This memorandum sets forth a Federal zero trust architecture (ZTA) strategy, requiring agencies to meet specific cybersecurity standards and objectives by the end of Fiscal Year (FY) 2024 in order to reinforce the Government's defenses against increasingly sophisticated and persistent threat campaigns. Those campaigns target Federal technology infrastructure, threatening public safety and privacy, damaging the American economy, and weakening trust in Government.

I. OVERVIEW

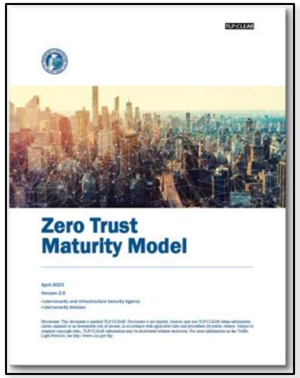
Every day, the Federal Government executes unique and deeply challenging missions: agencies [1] safeguard our nation's critical infrastructure, conduct scientific research, engage in diplomacy, and provide benefits and services for the American people, among many other public functions. To deliver on these missions effectively, our nation must make intelligent and vigorous use of modern technology and security practices, while avoiding disruption by malicious cyber campaigns.

Successfully modernizing the Federal Government's approach to security requires a Government-wide endeavor. In May of 2021, the President issued Executive Order (EO) 14028, *Improving the Nation's Cybersecurity*,[2] initiating a sweeping Government-wide effort to ensure that baseline security practices are in place, to migrate the Federal Government to a zero trust architecture, and to realize the security benefits of cloud-based infrastructure while mitigating associated risks.

[1] As used in this memorandum, "agency" has the meaning given in 44 U.S.C. § 3502.
[2] Exec. Order No. 14028, 86 Fed. Reg. 26633 (2021). https://www.federalregister.gov/d/2021-10460

The Strategy

OMB M-22-09
Zero Trust Strategy



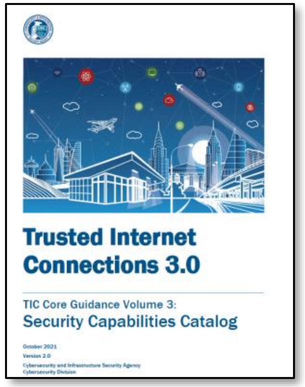
TLP:CLEAR

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.

CISA Zero Trust
Maturity Model



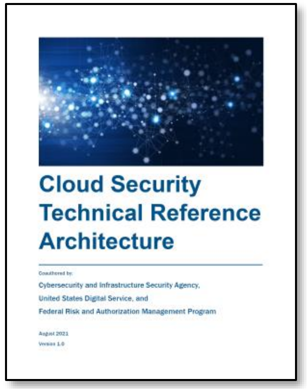
Trusted Internet
Connections 3.0

TIC Core Guidance Volume 3:
Security Capabilities Catalog

October 2021
Version 2.0
Cybersecurity and Infrastructure Security Agency
Cybersecurity Division

TIC Catalog

The Operational Guidance

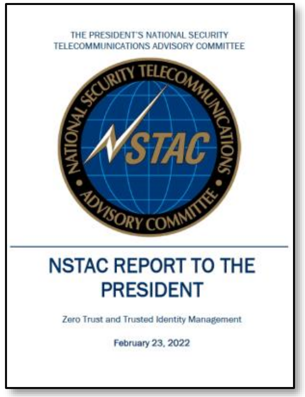


Cloud Security
Technical Reference
Architecture

Coauthored by:
Cybersecurity and Infrastructure Security Agency,
United States Digital Service, and
Federal Risk and Authorization Management Program

August 2021
Version 1.0

Federal Cloud
Security TRA



THE PRESIDENT'S NATIONAL SECURITY
TELECOMMUNICATIONS ADVISORY COMMITTEE

NATIONAL SECURITY TELECOMMUNICATIONS • ADVISORY COMMITTEE • NSTAC

NSTAC REPORT TO THE
PRESIDENT

Zero Trust and Trusted Identity Management

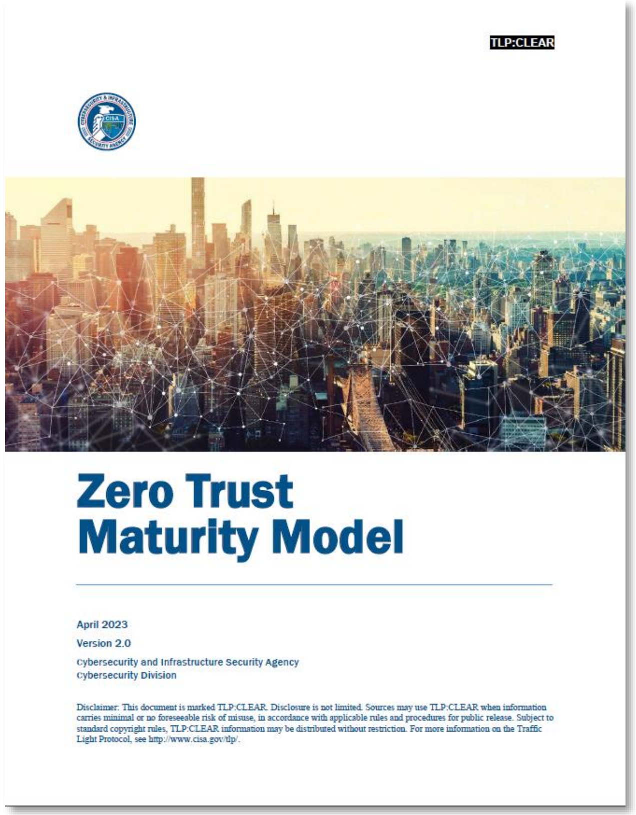
February 23, 2022

NSTAC Report

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

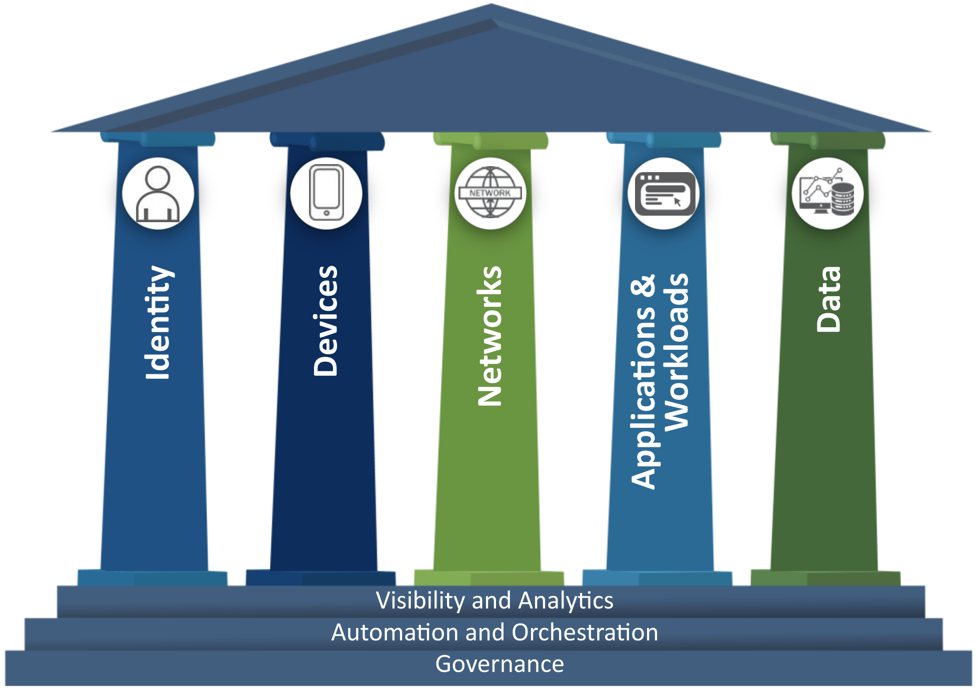
Version 2.0

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

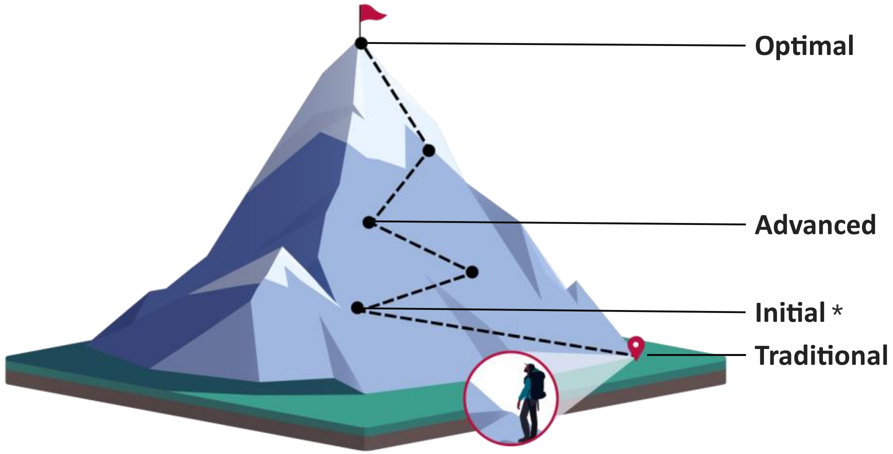
- The ZTMM represents a gradient of implementation across five distinct pillars and three cross-cutting capabilities
  - Functional areas where zero trust principles must be implemented in order to create a secure ZTA
  - Cross-cutting capabilities must be satisfied for each pillar
- Heavily influenced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



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

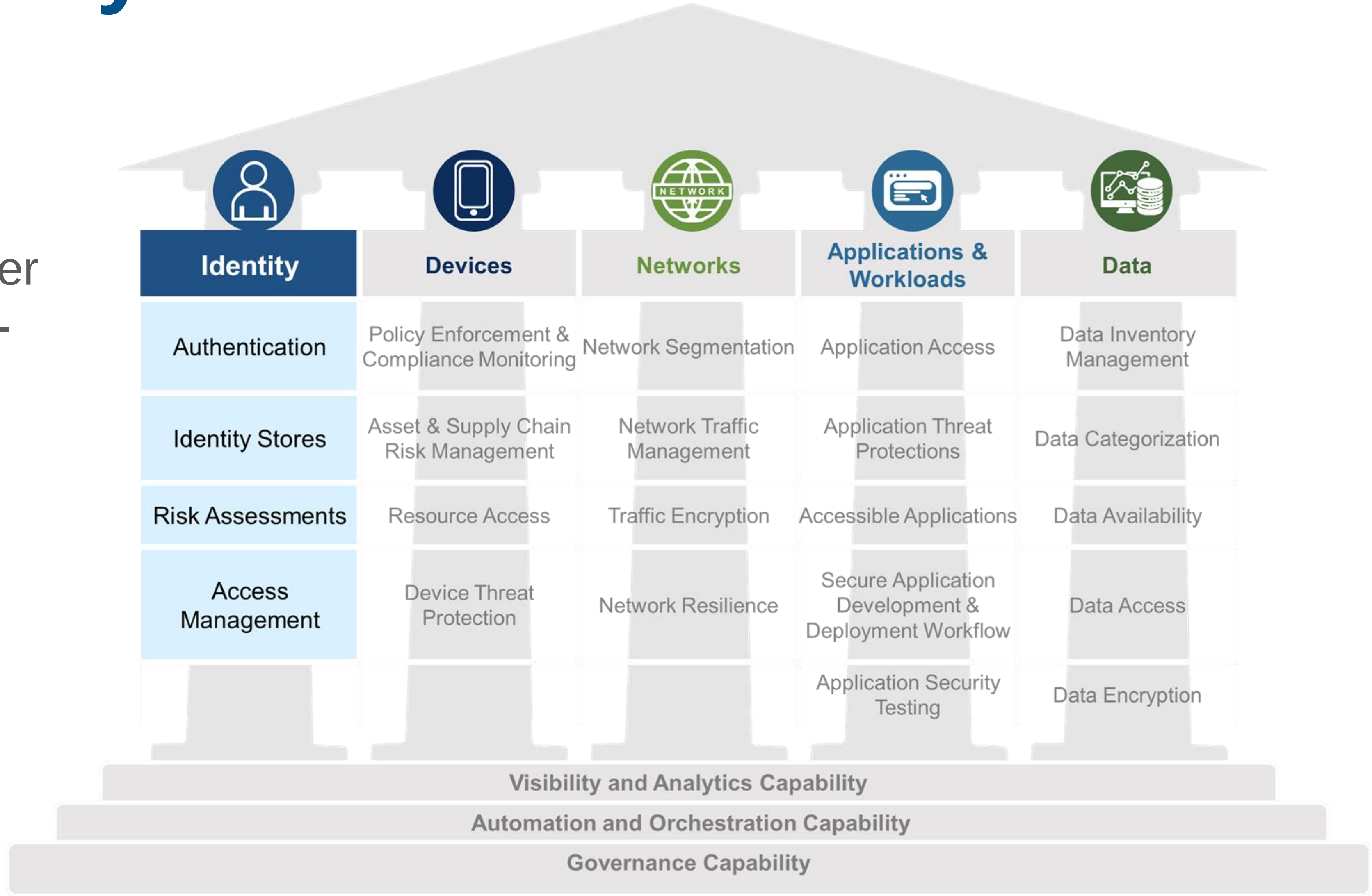
Zero Trust Maturity Journey



*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

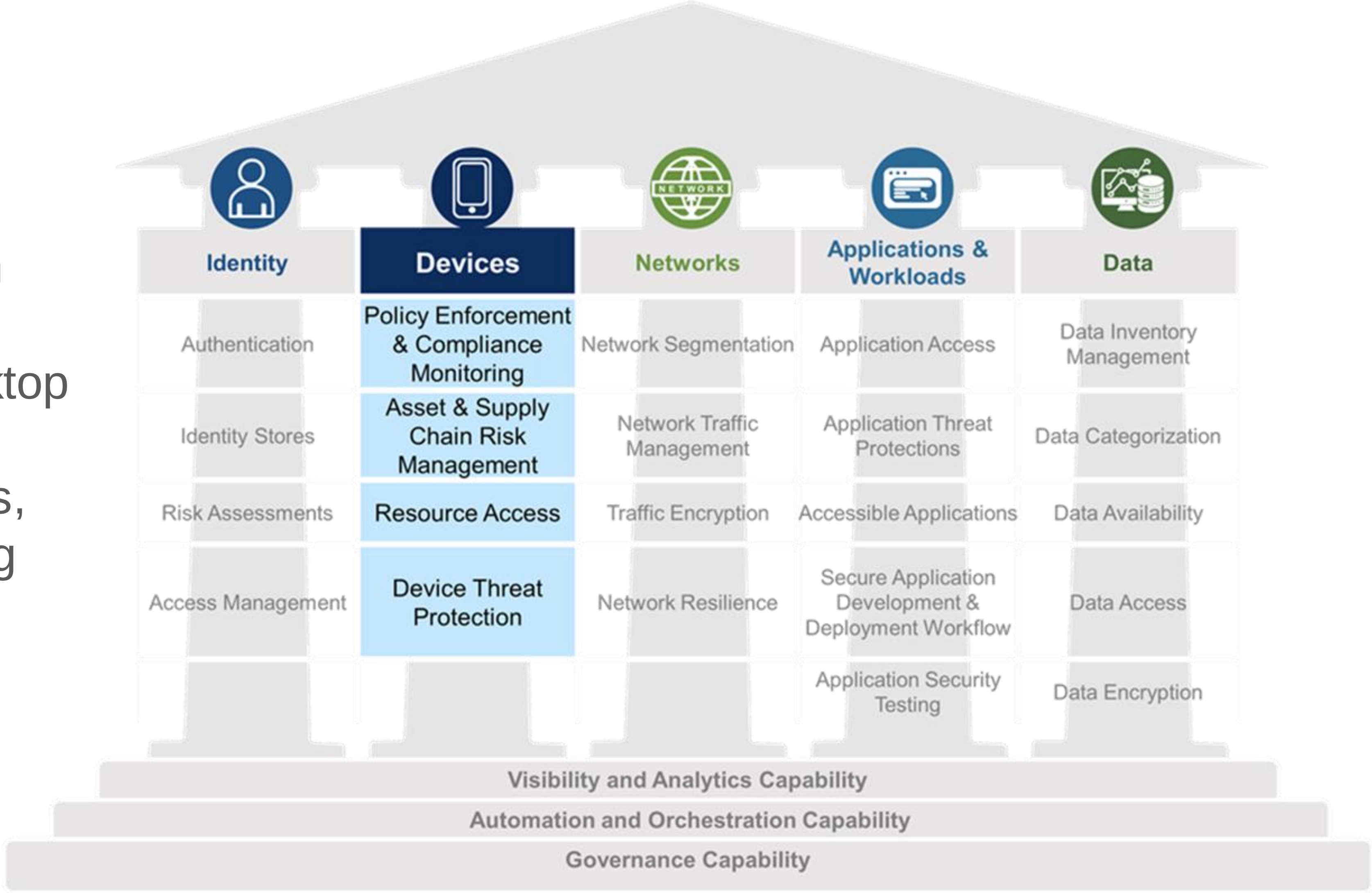
Visibility and Analytics Capability

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

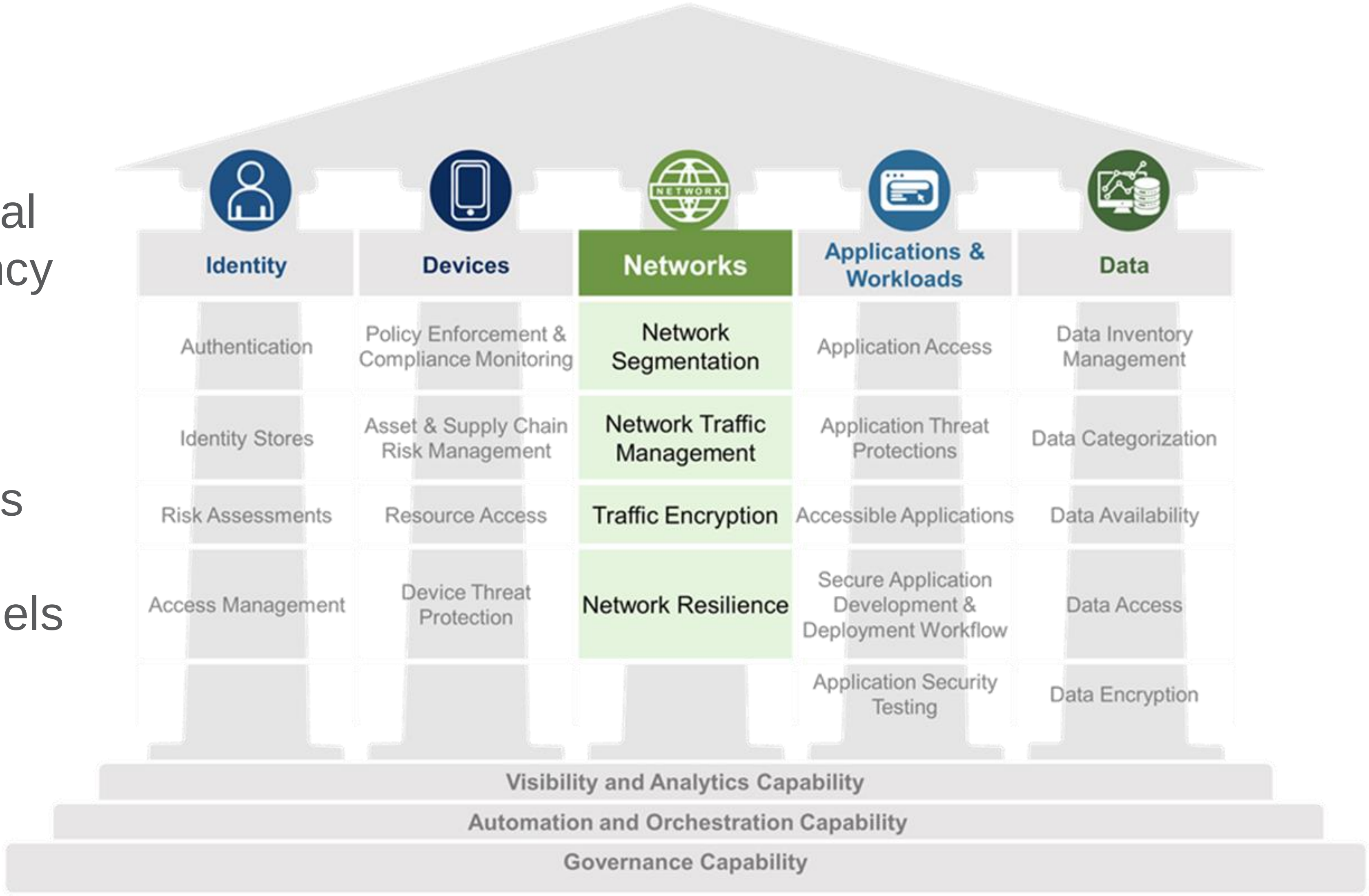
Visibility and Analytics Capability

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

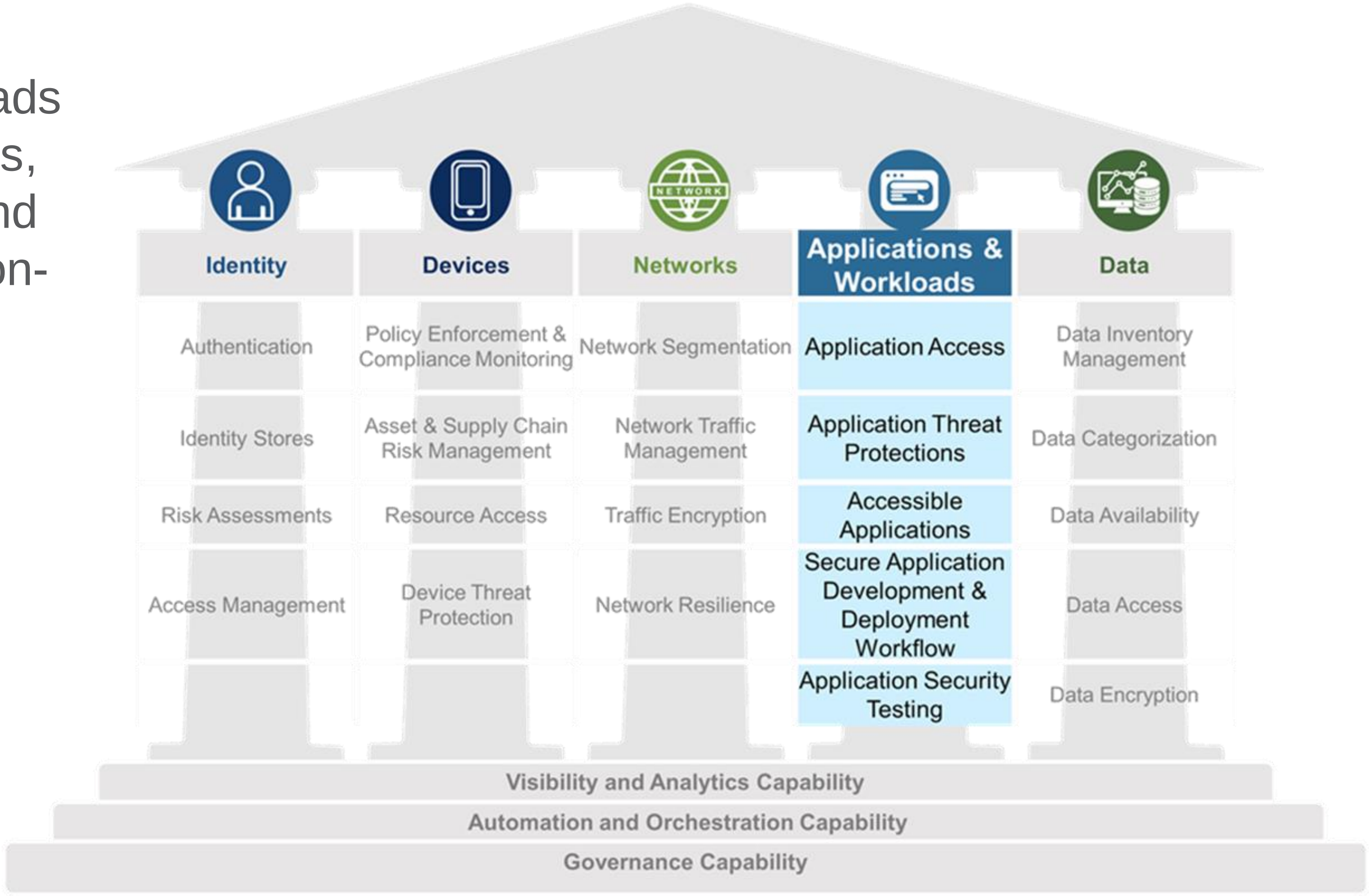
Visibility and Analytics Capability

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

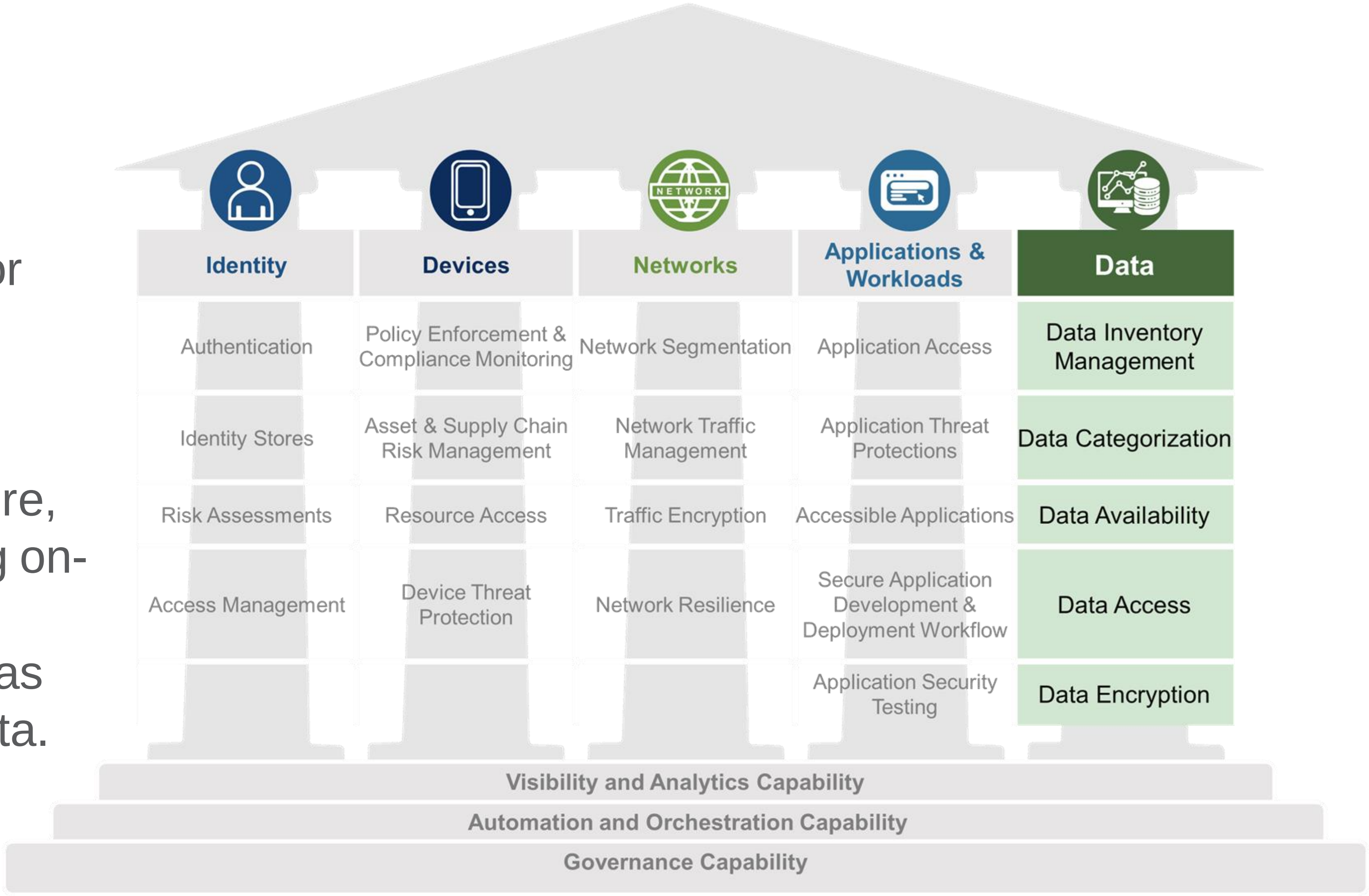
Visibility and Analytics Capability

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

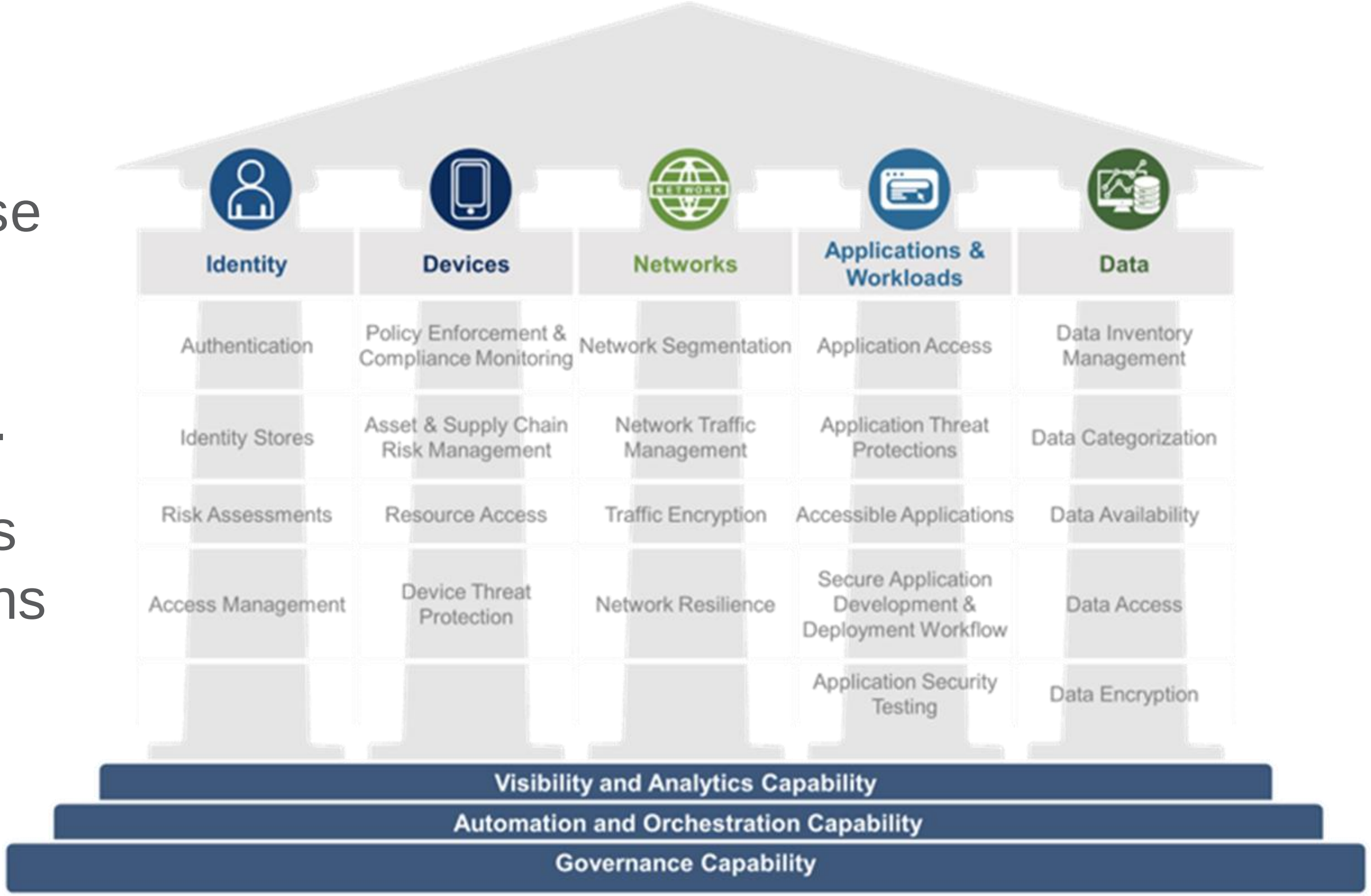
Visibility and Analytics Capability

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

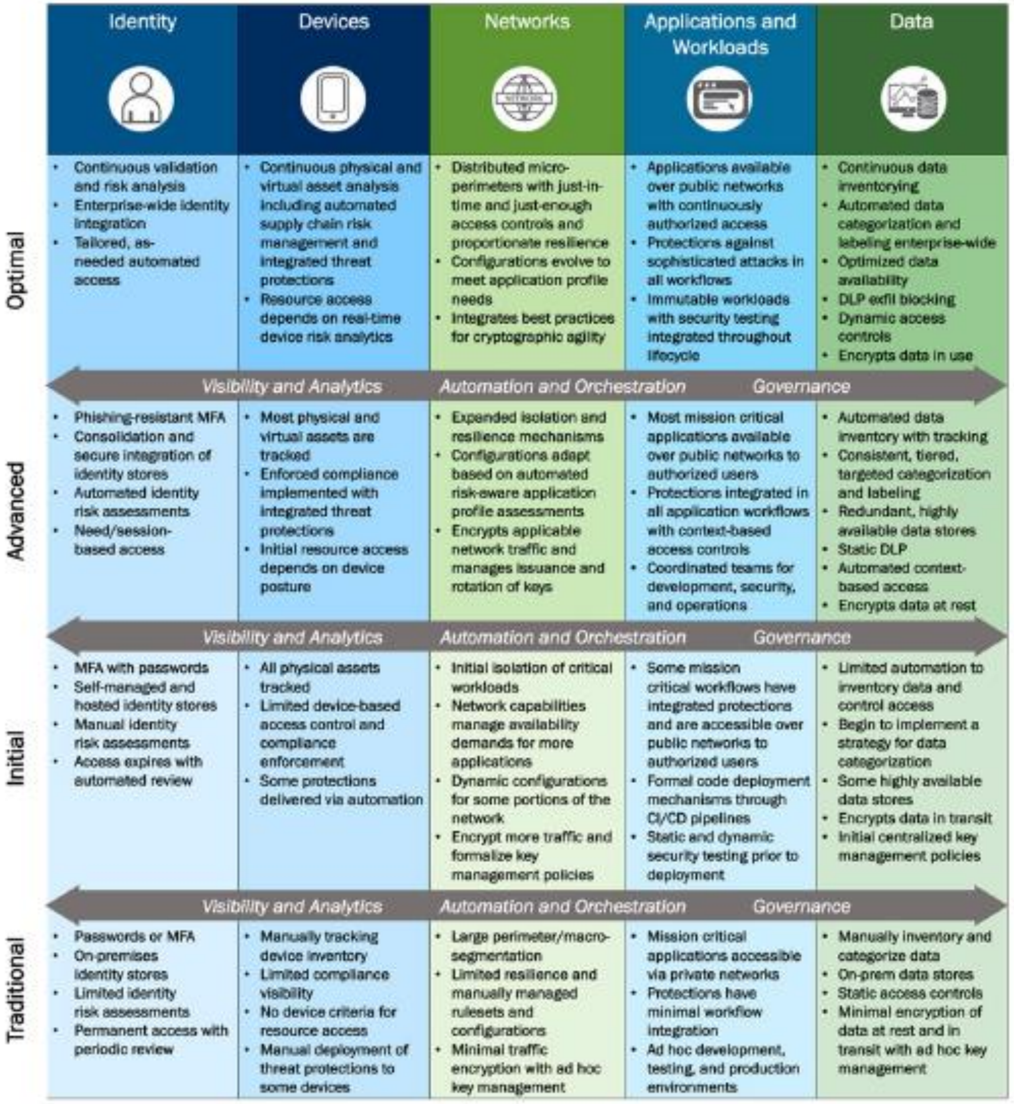
Visibility and Analytics Capability

Automation and Orchestration Capability

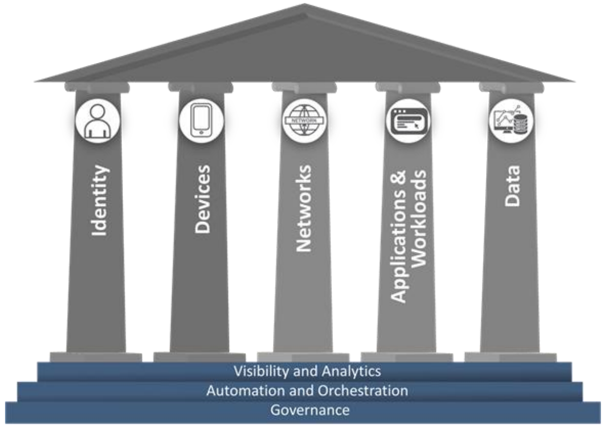
Governance Capability

Cross-Cutting Capabilities are Matrixed

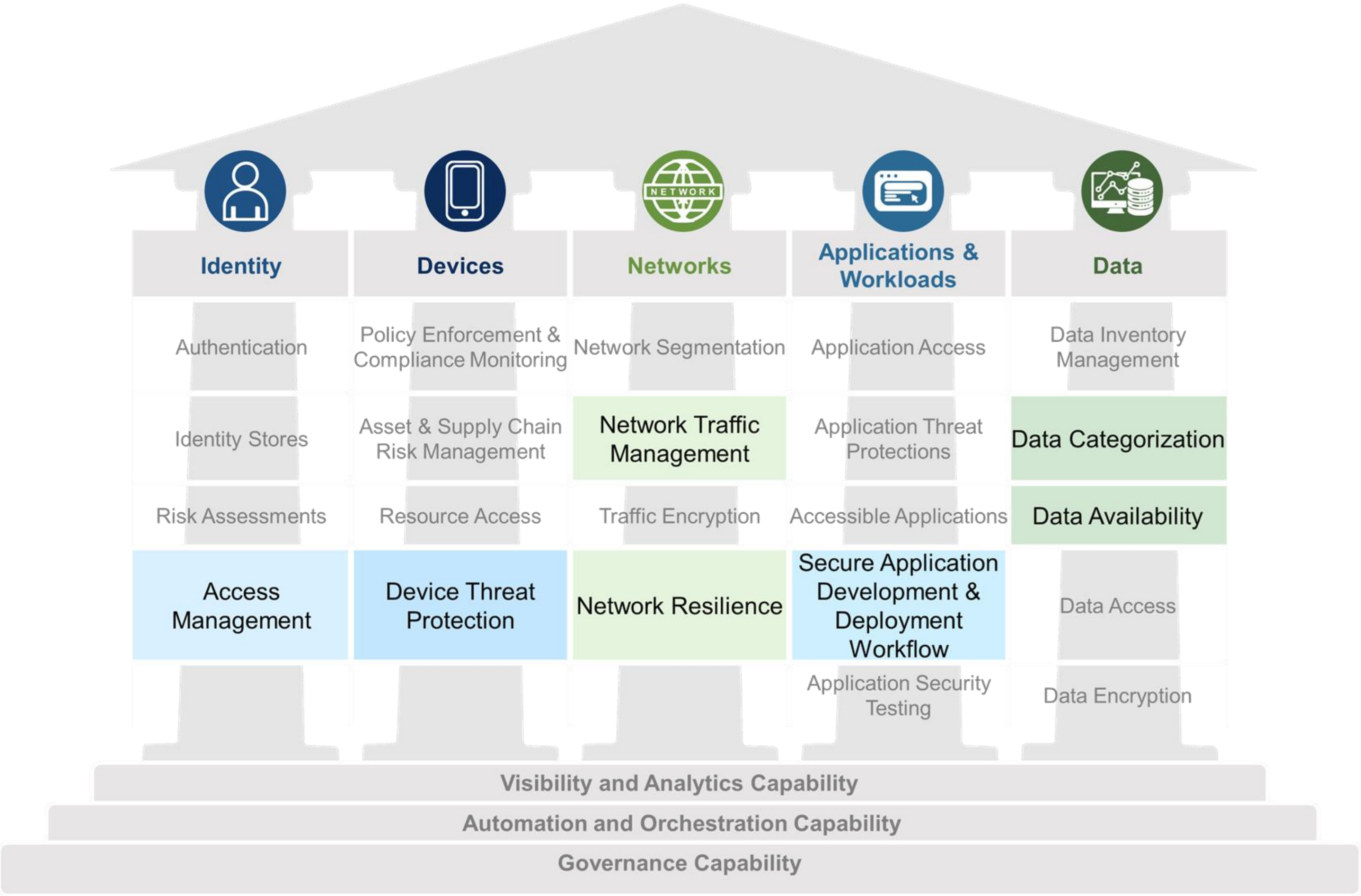
- The three capabilities are woven into each of the pillars.
- Each capability also has distinct maturity levels.



	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	• Expanded 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



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

Acronyms

- 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)
- Executive Order (EO)
- Extensible Visibility Reference Framework (eVRF)
- Federal Civilian Executive Branch (FCEB)
- General Services Administration (GSA)
- 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)
- Policy Enforcement Point (PEP)
- Program Management Office (PMO)
- 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