FORRESTER®

Zero Trust ≠ Zero Risk

Ron Woerner
Principal Consultant,
Forrester Research

19 February 2025

ISACA®
Minnesota Chapter

50 Years!

Ron Woerner

Principal Consultant,
North America Strategy Consulting
Forrester
https://www.linkedin.com/in/ronwoerner/

https://linktr.ee/cyberron

Education

Ron holds a Bachelor of Science in computer science from Michigan State University and a Master of Science in information systems management from Syracuse University. He received his CISSP in 2001 and CISM in 2015. His commitment to the industry is reflected in his desire to continue education through continuing education credit courses as well as vendor-specific technologies, network, and security-focused learning paths.

Background

Ron is a Principal Consultant supporting security and risk (S&R) professionals and focusing on Zero Trust strategy, architecture, implementation, and alignment to industry standards. He specializes in security transformation initiatives across industry verticals, focusing on risk, security, and privacy frameworks; organizational maturity; and Zero Trust strategies for empowering the business to meet the customer-driven challenges of cloud and mobile, identity and access, and automation and analytics.

Previous Work Experience

Before joining Forrester, Ron served as a virtual chief information security officer, security evangelist, and lead security analyst for numerous organizations, including Fortune 100 private equity firms, utilities, healthcare providers, government agencies, and service organizations. He has also been a university professor for more than 10 years, focusing on cybersecurity and IT curriculum, and he developed the LinkedIn Learning courses on the National Institute of Standards and Technology (NIST) Cybersecurity, Risk Management, and Privacy Frameworks. In the United States Air Force, Ron served as an intelligence and targeting officer.

What does Zero Trust mean to you?

Put your answer in chat or unmute your mic

What is *Zero Trust*?

FORRESTER®

"Zero Trust Is A Model For Information Security, Plain And Simple"

David Holmes, Sr. Analyst, Forrester

The Definition Of Modern Zero Trust

"You don't need to understand the granular details of Zero Trust security to understand why it's so effective or how it can help power a radical change in technology capabilities that creates the foundation for trusted business. "

Stephanie Balaouras, VP, Group Director, Forrester

Zero Trust Security: The Business Benefits And Advantages (forrester.com)

Core principles of Zero Trust

Explicit and Continual Verification

1. All entities are untrusted.
2. Least privilege access is enforced.
3. Assume breach; inspect and monitor everything.

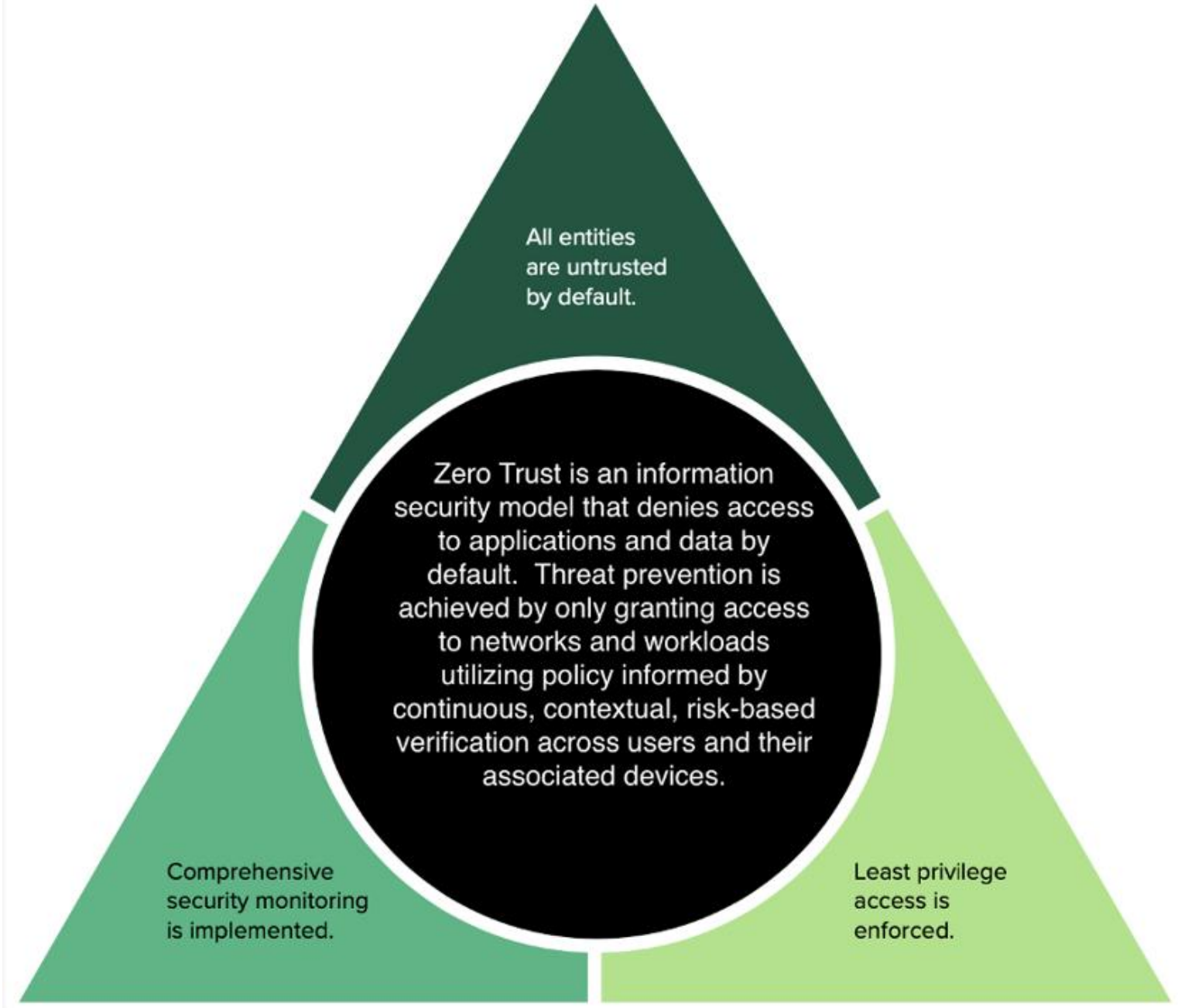
Connecting from a particular network must not determine which services you can access. Access to services is granted based on identity.

Reference: The Definition Of Modern Zero Trust (forrester.com)

Forrester Zero Trust Definition (2023)

Themes:

- Default deny
- Access by policy only
- For data, workloads, users, devices
- Least privilege access
- Security monitoring
- Risk-based verification



Source: Zero Trust Security: The Business Benefits And Advantages (https://www.forrester.com/zero-trust/)

Federal Zero Trust Definitions

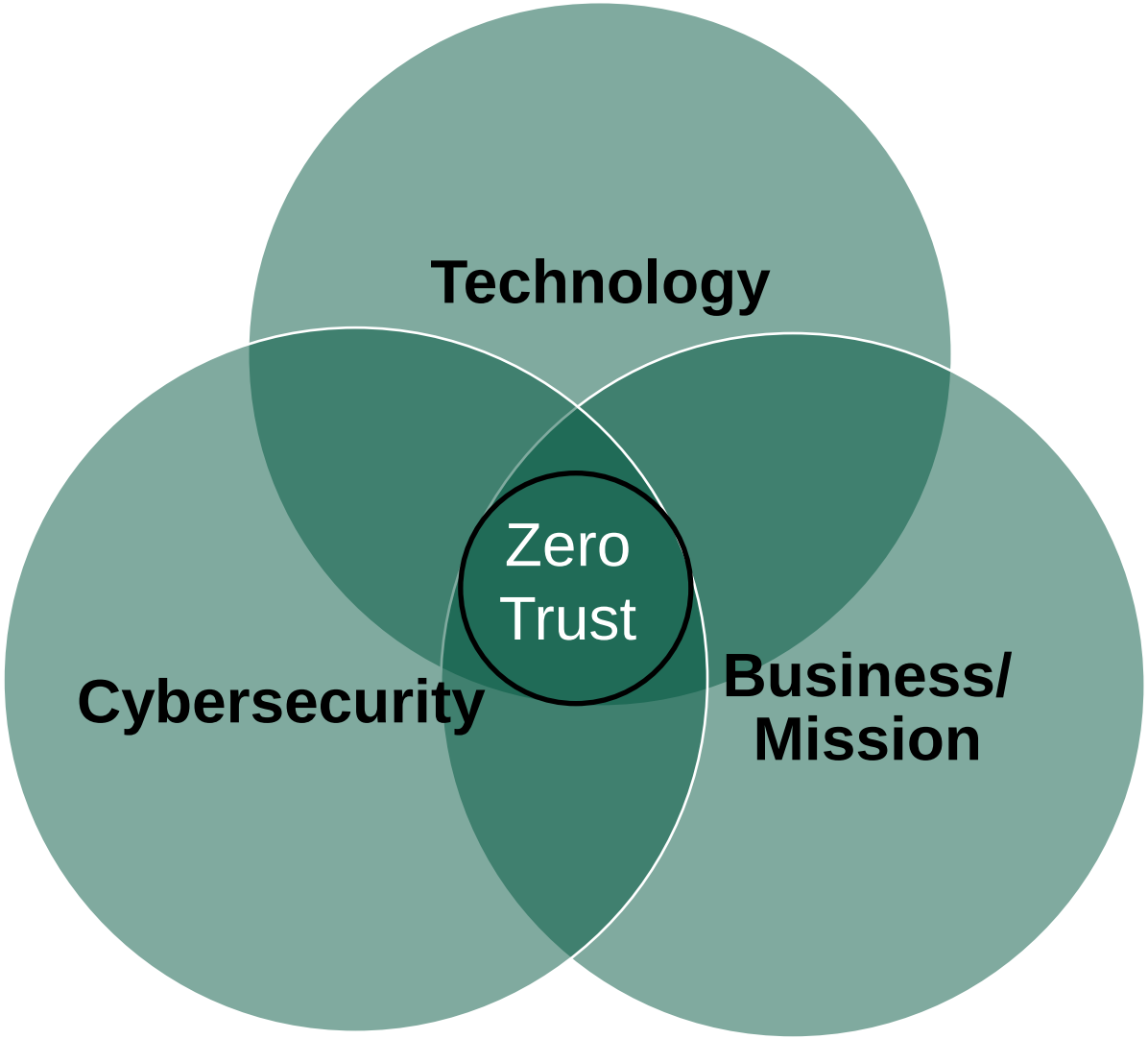
NIST SP800-207, Zero Trust Architecture & Zero Trust Maturity Model Version 2.0 (cisa.gov)

Zero trust (ZT) provides 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**.

Zero trust architecture (ZTA) is an **enterprise's cybersecurity plan** that utilizes zero trust concepts and encompasses component relationships, workflow planning, and access policies. Therefore, a zero trust enterprise is the **network infrastructure** (physical and virtual) and **operational policies** that are in place for an enterprise as a product of a zero trust architecture plan

The path to zero trust is an incremental process that may take years to implement.

Zero Trust Intersection



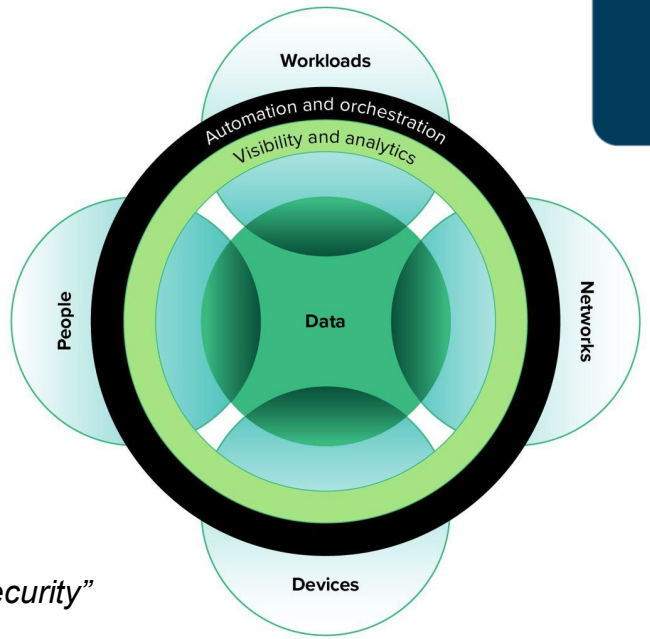
FORRESTER®

Why Zero Trust?

Zero Trust origin story: From 2009 to present

In 2009, Zero Trust was network-centric

Over ten years, it has evolved to encompass an entire ecosystem



Forrester's "No More Chewy Centers: The Zero Trust Model Of Information Security"
Forrester's "The Zero Trust eXtended (ZTX) Ecosystem"

Trust Based On Network Security FAILED

- Fails to address the current threat landscape
- Security policy enforcement ineffective
- Decreased agility & performance
- Fragmented architectures and networks
- Increased costs, complexity, & technical debt

Zero Trust has gained adoption

- Zero Trust (ZT) security is now mainstream in the US Government
  - Executive order on improving the Nation's Cybersecurity (May 12 2021)
  - OMB ZT Memorandum M-22-09 (January 26 2022)
- Zero Trust Adoption has significant momentum in the US and global private sector.

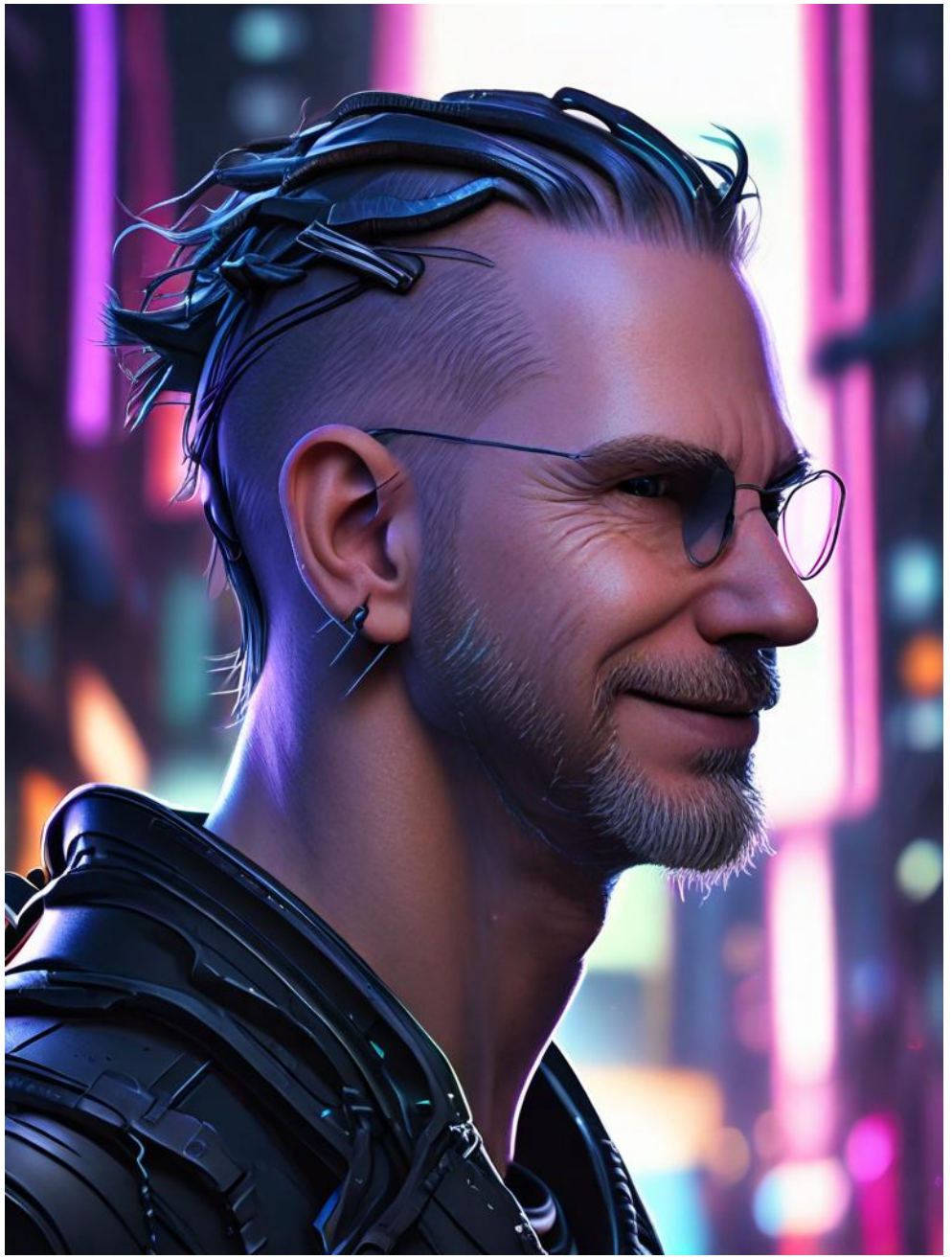
Common Zero Trust concerns and misconceptions

- It’s just a buzz word
- It’s like old wine in a new bottle
- There isn’t an agreed-upon definition of Zero Trust
- It’s impractical in most real-world scenarios
- It’s too hard to know where to start and how to gain adoption
- Zero Trust is costly and requires an operations overhaul
- The “zero” in Zero Trust sounds counterintuitive to organization’s trust initiatives and culture

AI & Zero Trust

TL;DR: AI Lies

Trust
&
Verify



FORRESTER®

Implementing Zero Trust

A wholistic approach for protecting critical assets

Zero Trust Components:

1. Data
2. People
3. Devices
4. Networks
5. Workloads
6. Visibility and analytics
7. Automation and orchestration
8. Governance

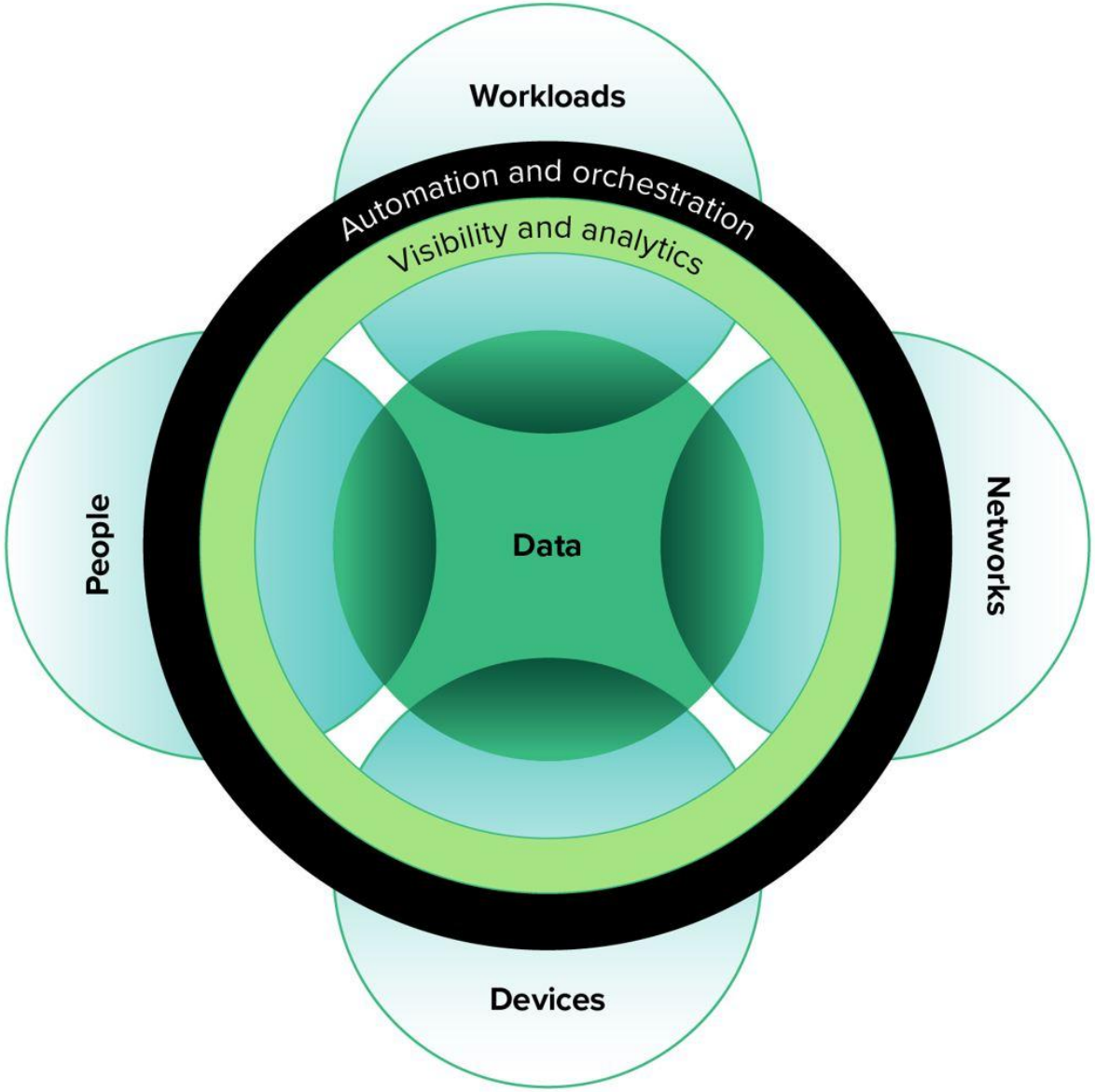
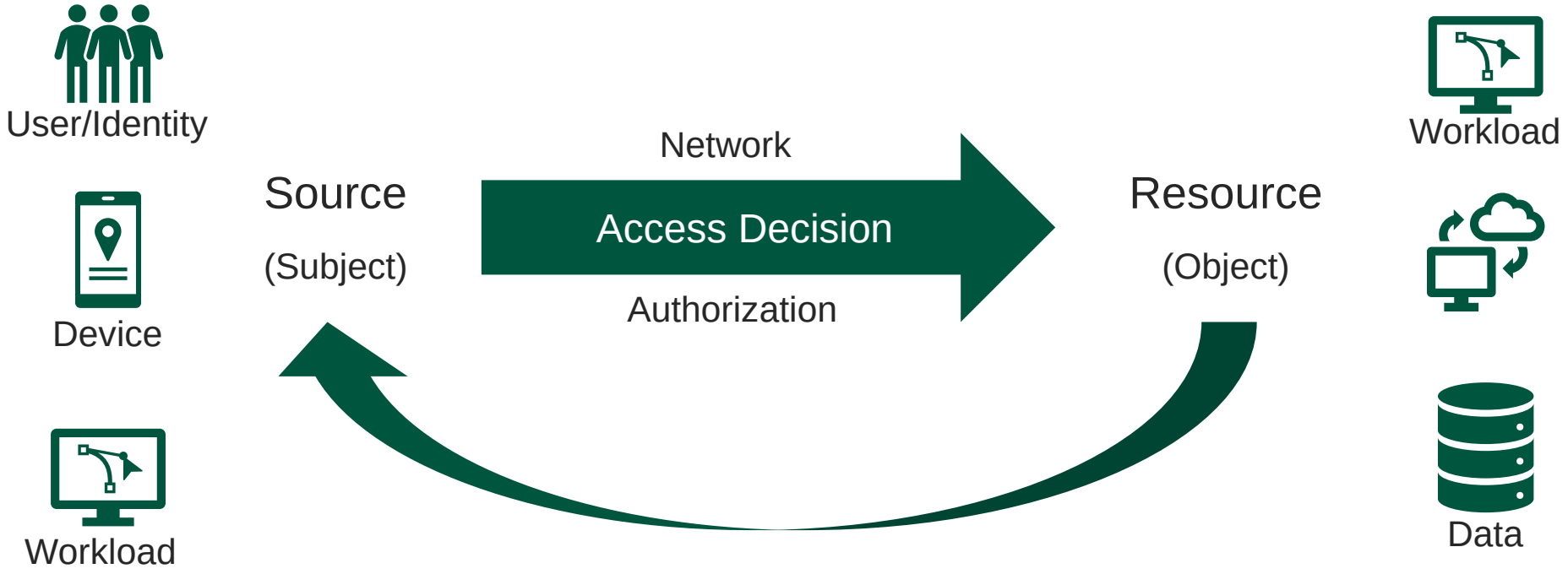


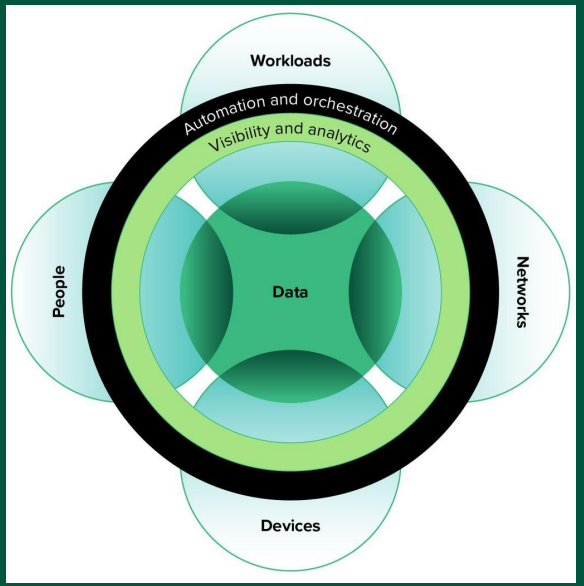
Image source: Zero Trust Security: The Business Benefits And Advantages (forrester.com)

Zero Trust Context

Policy Decisions for finer-grained access controls

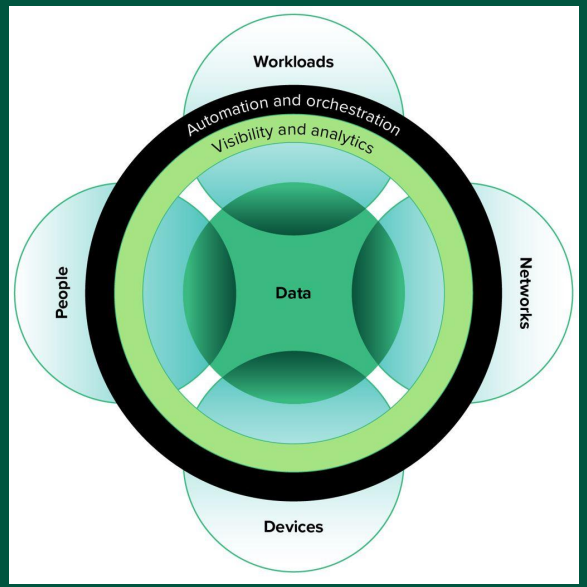


Identity – *People, devices, systems, applications, …*



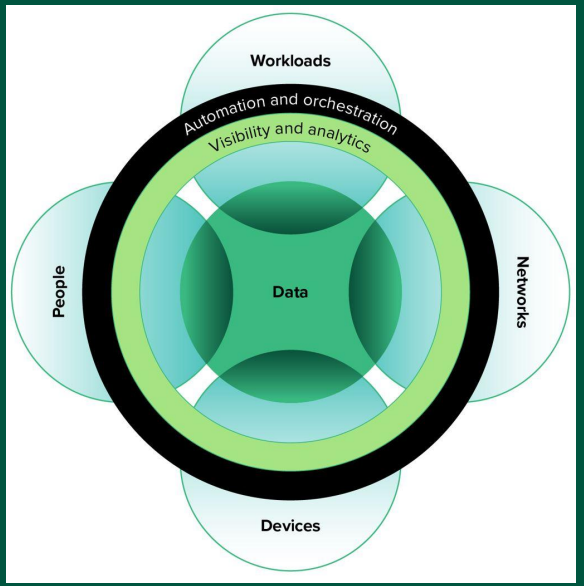
- Single source of truth for all accounts
- Identity and Access Management (IAM) solutions
- Apply least privilege universally
- Risk-based access controls

Devices – *End-point computers (e.g., workstations, laptops, mobile, BYOD, IoT, etc.)*



- Establish an inventory
- Isolate, secure, and control every device on the network at all times
- Unified Endpoint Management (UEM)

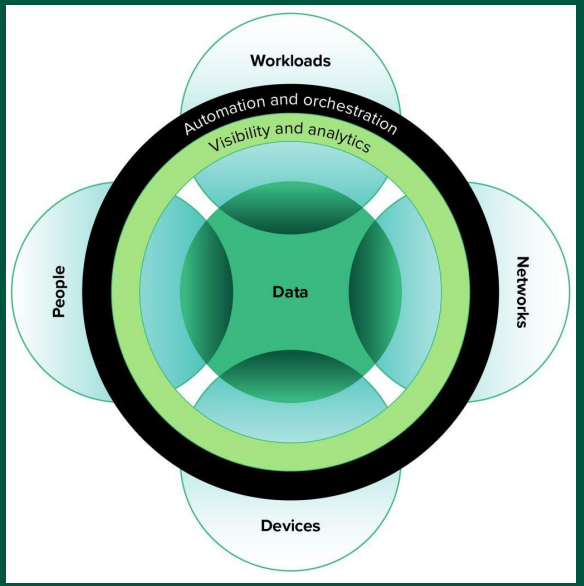
Workload – *Logical functions that do "work" on the endpoint.*



- Applications, Operating Systems, Cloud processors (hypervisors, containers, virtual machines)
- Workload discovery and inventory
- Standardize configuration and compliance
- Vulnerability and patch management
- Host-based security (EPP/AV, FW, threat detection)

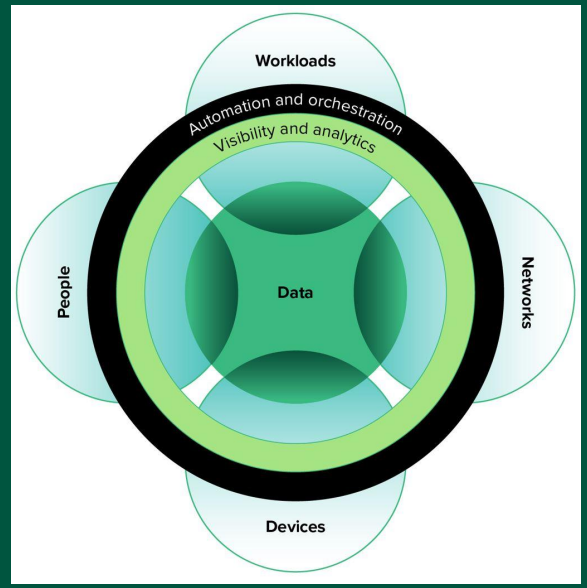
Network –

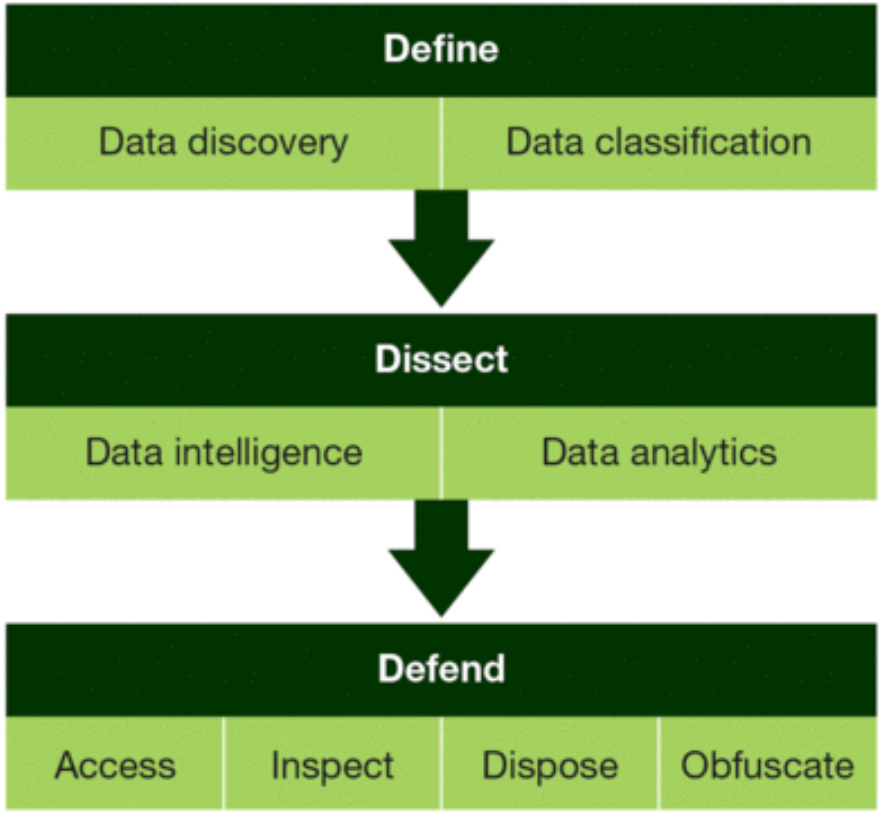
Connects devices and other networks



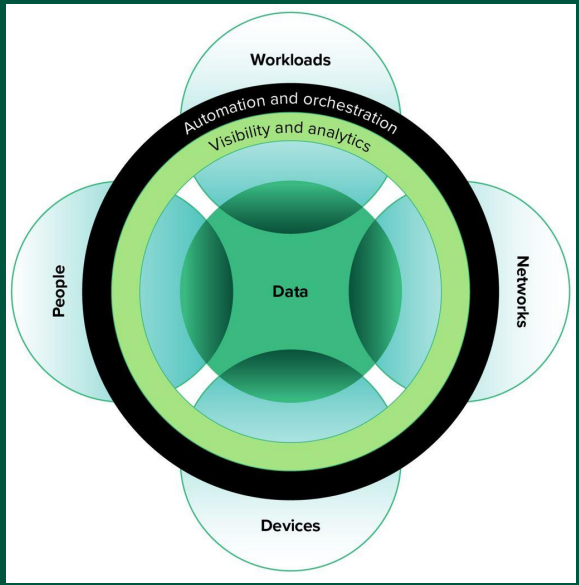
- Build towards host, application, or data-level enforcement
- Isolation and separation based on use, sensitivity
- Enable Zero Trust Network Access (ZTNA), microsegmentation, and microperimeters
- Centrally manage network policy
- Analyze network traffic for threats

Data –
Assets with value



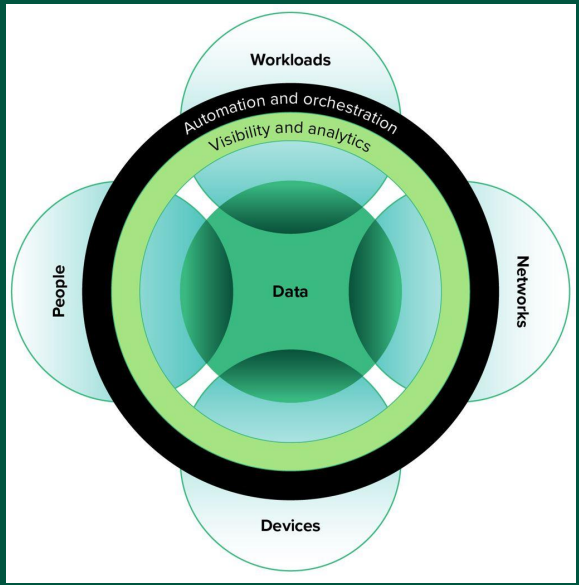


Visibility and Analytics – *You can't combat a threat you don't see or understand.*



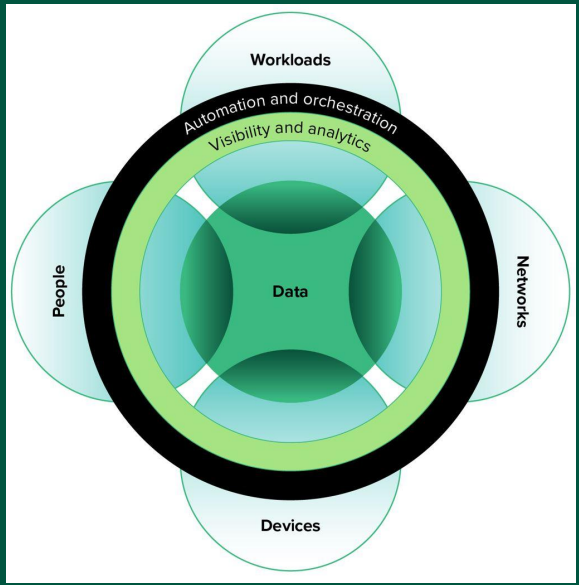
- Logging and monitoring
- How, when, where assets are used
- Security Information and Event Management (SIEM)
- Speed detection and response to cybersecurity threats
- Enable threat hunting and forensic
- Accelerate investigations
- Support compliance initiatives

Automation and Orchestration – *Command and control of technology assets*



- Identify, triage, investigate, and respond to threats
- Coordinating efforts
- Improves efficiency and accuracy
- Reduces the human element
- Security orchestration, automation, and response (SOAR)

Governance – *Policies, standards, regulations, requirements, etc.*

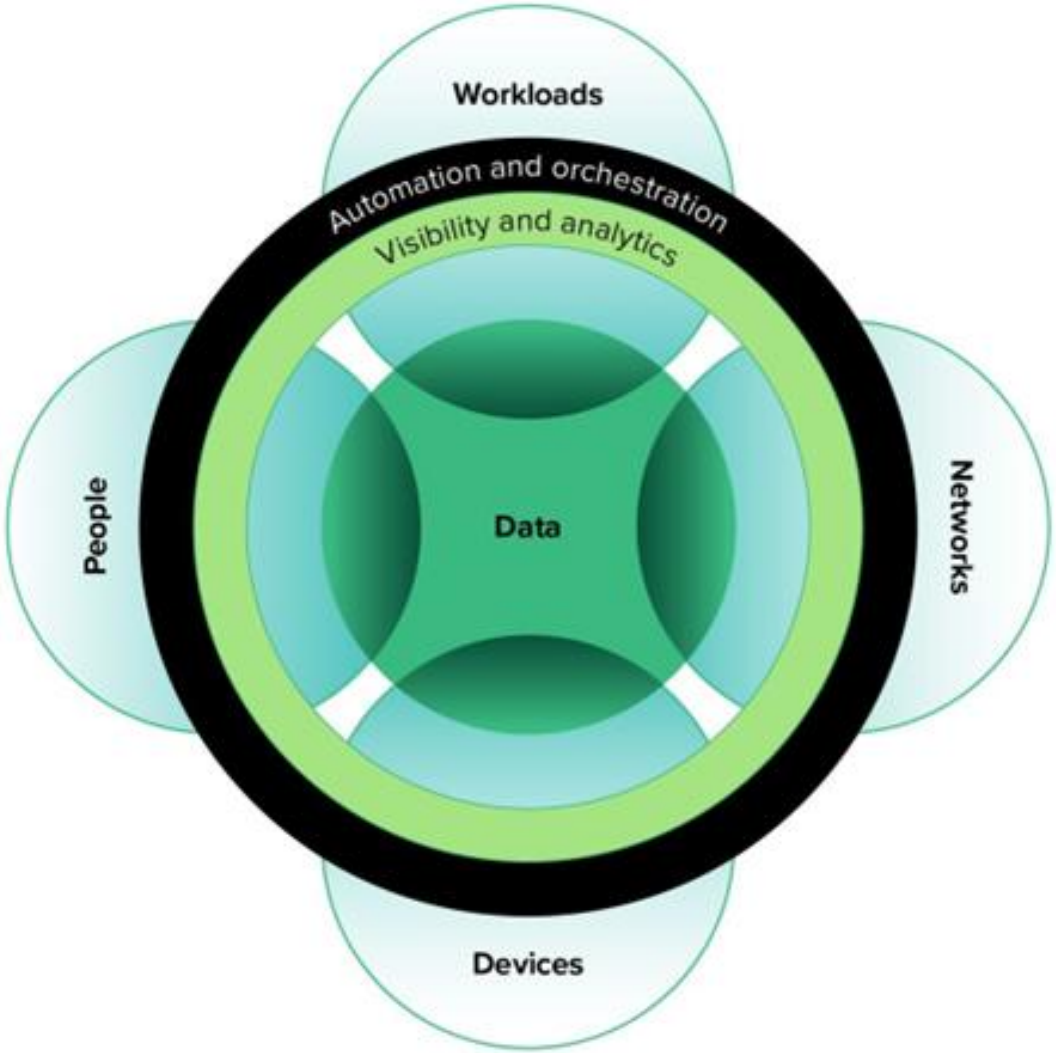


The policies, frameworks, and processes that facilitate risk management, resource allocation, prioritization, funding, and measurement necessary to deliver effective technology strategies.

Zero Trust Risk Analysis

Kipling method

Who
What
Where
When
How
WHY



Connecting with your business / mission

Decoding The New Zero Trust Terminology

Acronym	Forrester Term	Quick Description	Associated Technology
ZTE Solutions	Zero Trust Edge	Convergence of networking and Zero Trust, delivered as a service.	Equivalent to SASE. SD-WAN + SSE SSE = (SWG, CASB, DLP, ZTNA).
ZTE Services	Zero Trust Edge Services	Outsourced management and deployment of SD-WAN and the security-related functions of ZTE solutions.	Provider owned infrastructure and ZTE solutions Enterprise owned infrastructure and ZTE solutions
ZTP	Zero Trust Platform	A unified offering of core security technologies that support other tools, applications, or technologies that enable Zero Trust.	Replaces ZTX ecosystem. Identity management Zero Trust access Zero Trust segmentation Privilege management
ZTNA	Zero Trust Network Access	Replace VPN with Zero Trust.	VPN

Source: Forrester Research, Inc. Unauthorized reproduction, citation, or distribution prohibited.

Source: [Decoding The New Zero Trust Terminology (forrester.com)]

FORRESTER®

Federal Direction in Zero Trust

Federal Direction on Zero Trust

Moving the U.S. Government Toward Zero Trust Cybersecurity Principles (https://zerotrust.cyber.gov/)

Lots of "cooks in the Zero Trust kitchen

Executive Order & OMB detailed guidance

- Executive Order on Improving the Nation's Cybersecurity (EO 14028)
- OMB – Federal Zero Trust Strategy
- OMB – M-22-09
- Federal Zero Trust Data Security Guide

NIST guidance

- NIST Special Publication 800-207: Zero Trust Architecture
- NIST SP 1800-35 (Draft), Implementing a Zero Trust Architecture
- NIST Definition of Critical Software

DHS CISA guidance

- DHS CISA – Zero Trust Maturity Model
- DHS CISA – TIC 3.0 Telework Guidance
- DHS CISA – Cloud Security Reference Architecture

GSA guidance

- GSA - Zero Trust Architecture Buyers Guide

DoD guidance

- Chief Information Officer > Library (defense.gov)
- DoD Zero Trust Reference Architecture
- DoD Zero Trust Strategy

NSA - Embracing a Zero Trust Security Model

Federal ZT Vision and Strategy Statements

We envision a Federal Government Agency where:

- Federal staff have enterprise-managed accounts, allowing them to access everything they need to do their job while remaining reliably protected from even targeted, sophisticated phishing attacks.
- The devices that Federal staff use to do their jobs are consistently tracked and monitored, and the security posture of those devices is taken into account when granting access to internal resources.
- Agency systems are isolated from each other, and the network traffic flowing between and within them is reliably encrypted.
- Enterprise applications are tested internally and externally, and can be made available to staff securely over the internet.
- Federal security teams and data teams work together to develop data categories and security rules to automatically detect and ultimately block unauthorized access to sensitive information.

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

7 Tenets of Zero Trust

NIST SP 800-207, Section 2.1 (p. 6)

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.

NIST SP800-207 Zero Trust Architecture

OMB guidance for Zero Trust Strategy

M-22-09 Federal Zero Trust Strategy (whitehouse.gov)

This memorandum requires agencies to achieve specific zero trust security goals by the end of Fiscal Year (FY) 2024. Grouped using the five pillars that underpin the Zero Trust maturity model of the Cybersecurity and Infrastructure Security Agency (CISA), those goals include:

1. **Identity**: Agency staff use an enterprise-wide identity to access the applications they use in their work. ***Phishing-resistant MFA*** protects those personnel from sophisticated online attacks.
2. **Devices**: The Federal Government has a ***complete inventory*** of every device it operates and authorizes for Government use and can ***detect and respond*** to incidents on those devices.
3. **Networks**: Agencies encrypt all DNS requests and HTTP traffic within their environment and begin ***segmenting networks around their applications***. The Federal Government identifies a workable path to encrypting email in transit.
4. **Applications**: Agencies treat ***all applications as internet-connected***, routinely subject their applications to ***rigorous testing***, and welcome ***external vulnerability reports***.
5. **Data**: Agencies are on a clear, shared path to deploy protections that make use of ***thorough data categorization***. Agencies are taking advantage of cloud security services to monitor access to their sensitive data and have implemented ***enterprise-wide logging and information sharing***.

Mapping Forrester to CISA Zero Trust Model

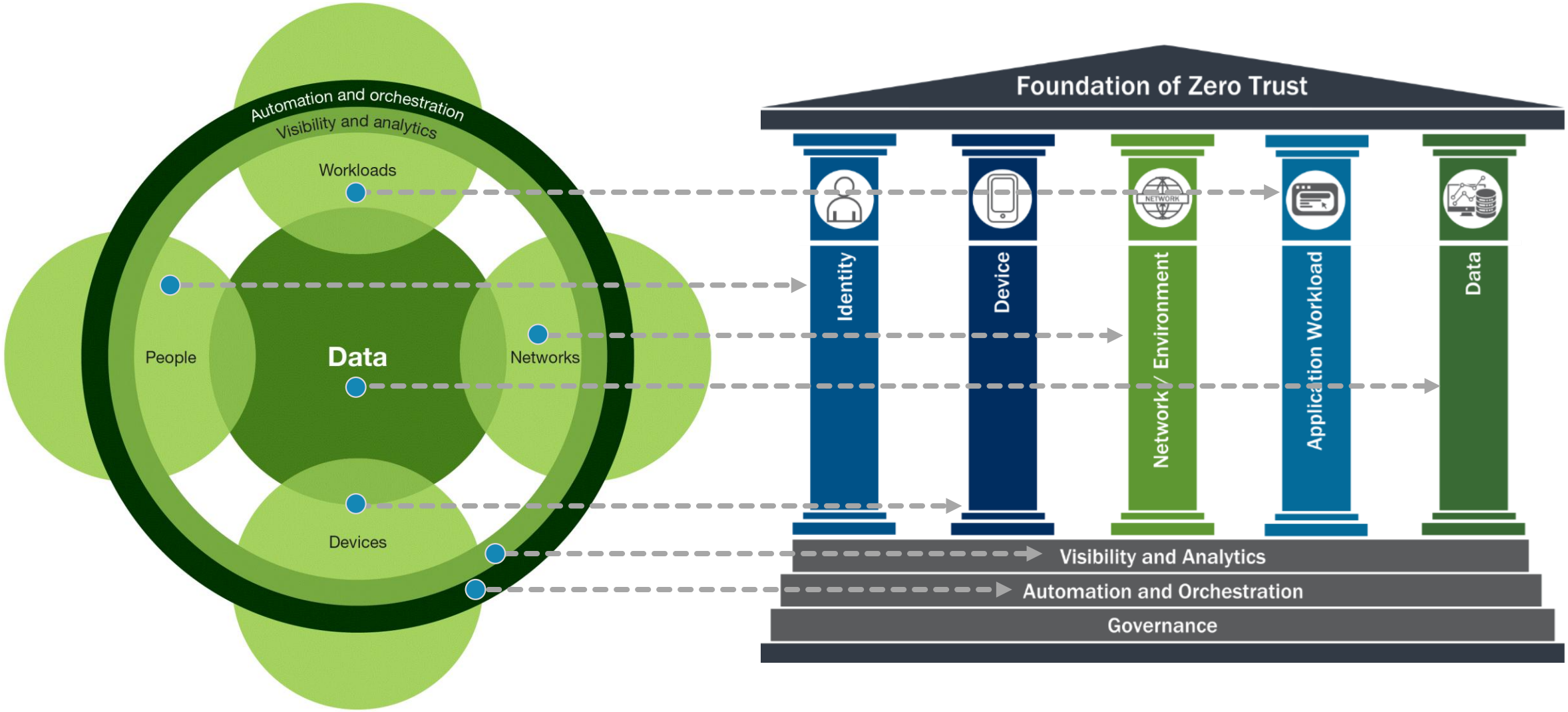
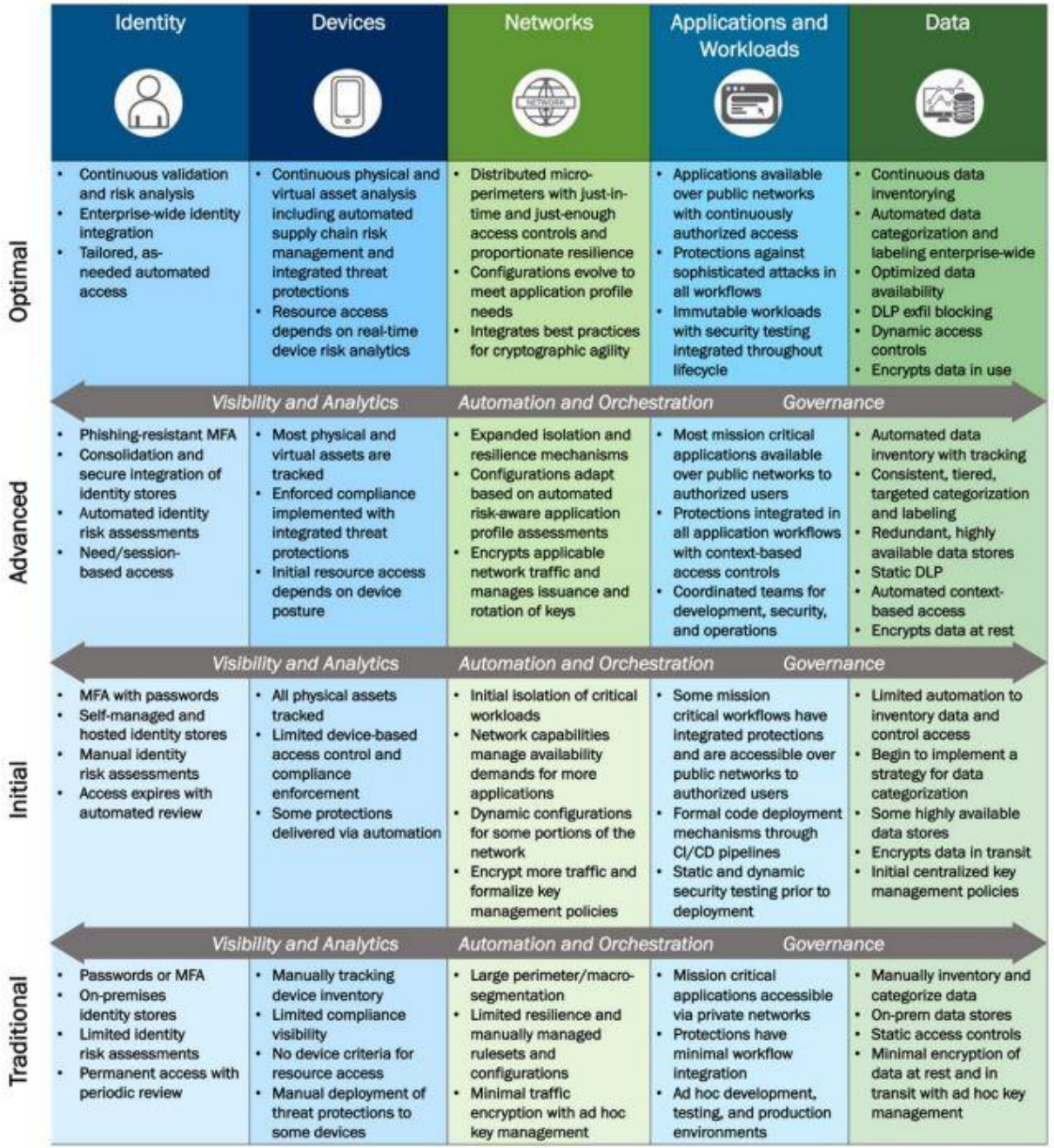


Image (right) source: [CISA Zero Trust Maturity Model]

CISA Zero Trust Maturity Model

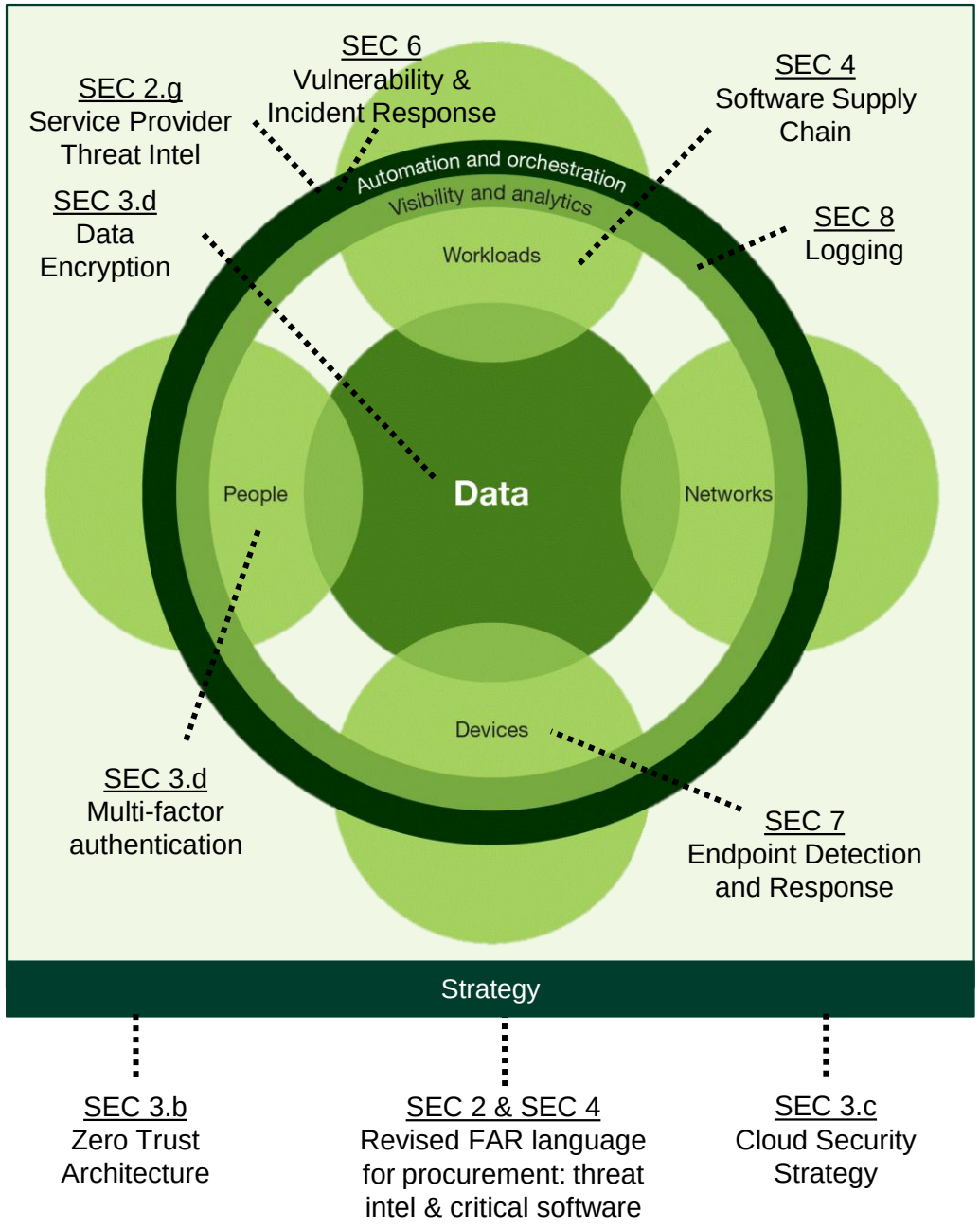
[Zero Trust Maturity Model Version 2.0 (cisa.gov)]



	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

Figure 4: High-Level Zero Trust Maturity Model Overview

Aligning the Executive Order to the Zero Trust (ZT) ecosystem model



NIST SP 800-207 Zero Trust Architecture (ZTA)

(an integrated set of solution architectures must aim for a unified policy mgmt suite)

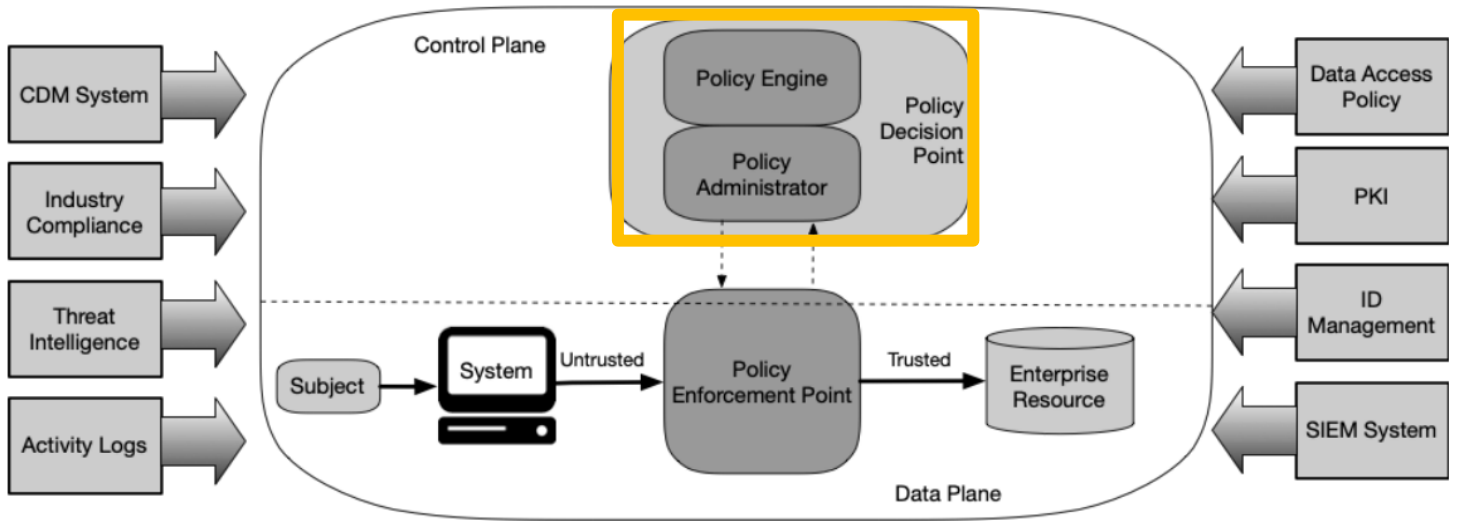


Figure 2: Core Zero Trust Logical Components

Image source: csrc.nist.gov
[NIST SP800-207 Zero Trust Architecture]

NIST SP 800-207 Zero Trust Architecture (ZTA)

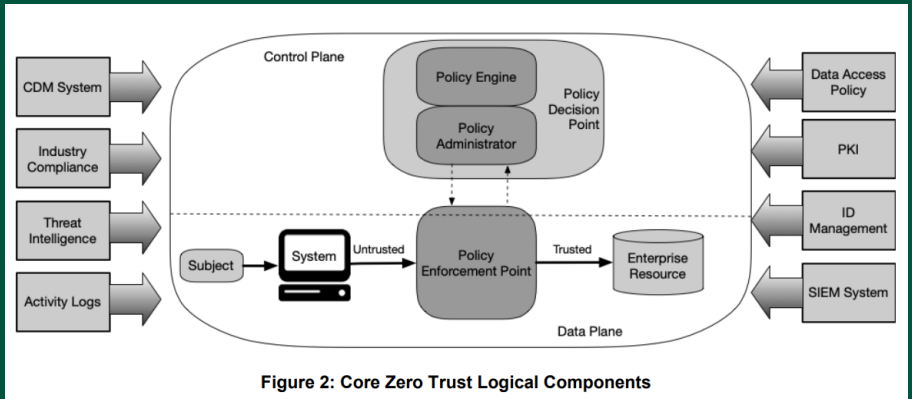


Figure 2: Core Zero Trust Logical Components

Policy Engine (PE): Responsible for the ultimate decision to grant access to a resource.

Policy Administrator (PA): Responsible for establishing and/or shutting down communication between a subject and a resource.

Policy Enforcement Point (PEP): Responsible for enabling, monitoring, and eventually terminating connections between a subject and an enterprise resource.

Multiple Data Sources: Several data sources (SIEM, CDM, PKI, etc) are needed to provide input and policy rules which are used by the policy engine when making access decisions.

Image source: csrc.nist.gov
[NIST SP800-207 Zero Trust Architecture]

Accelerating Your Zero Trust Journey

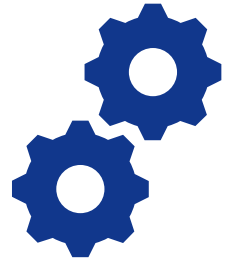
Develop a Single Strategy for Long Term Success

Being Compliant – not a strategy

Risk-based approach

Being Secure – not a strategy

Tie to business / mission goal



Implementing Controls and Tech – not a strategy

Include people & process (User Experience)

Zero Trust – One Strategy, Multiple Avenues, Long Lifecycle

Assess Your Zero Trust Maturity

Zero Trust Maturity Model Version 2.0 (cisa.gov)

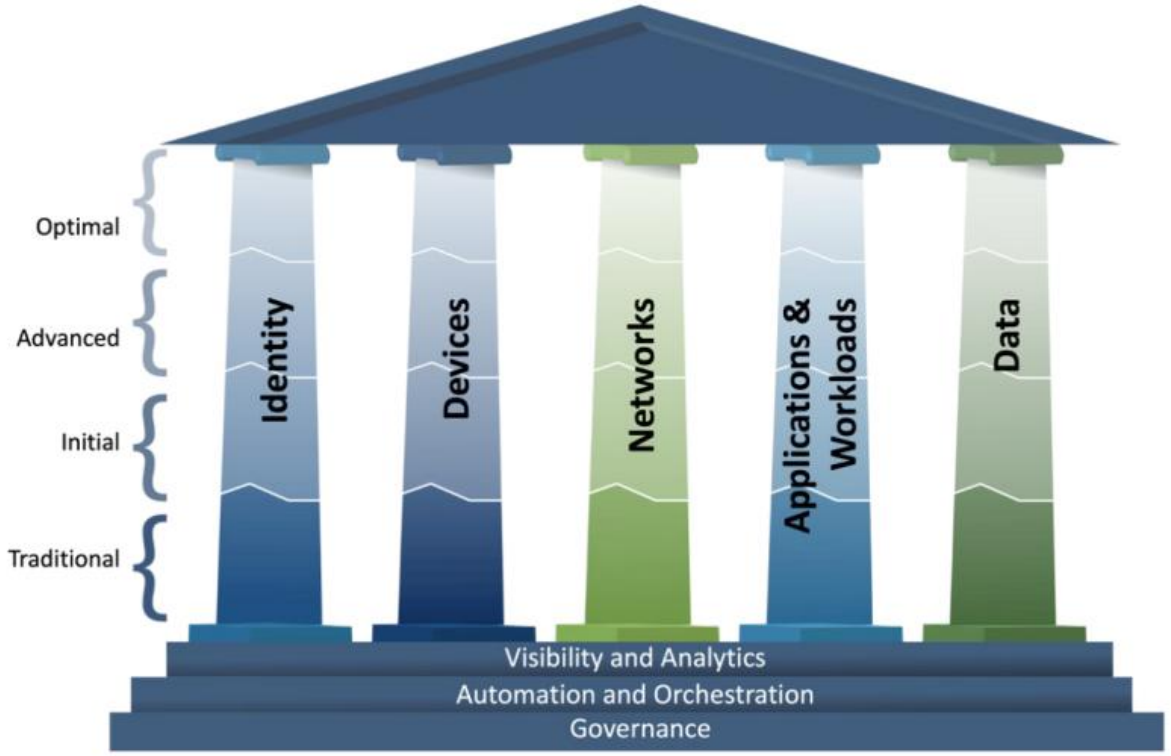


Figure 3: Zero Trust Maturity Evolution

	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

Figure 4: High-Level Zero Trust Maturity Model Overview

CISA's ZTMM is one of many paths to support the transition to zero trust.

Preparing for Zero Trust

Zero Trust as a security culture initiative for improved risk management

There is no “right” way to Zero Trust.

Zero Trust is both a blueprint for security architecture and a strategy to guide you.

Zero Trust is a mindset and a path for digital protection transformation.

Take advantage of what you already know, have, and are doing

Where do you start? Take advantage of what you already know and the tools you already have.

Be opportunistic and take advantage of current initiatives.

Integrate people and process with technology

Zero Trust cannot be implemented with technology alone.

Understand how user experience and operations are affected by Zero Trust.

Zero Trust Capability Transformation Model

AN ILLUSTRATIVE MODEL

Implementing Your Zero Trust Strategy

FORRESTER®

1. Join or help charter a Zero Trust steering committee / champions
2. Identify use cases and customer journeys for Zero Trust transformation
3. Develop a Zero Trust enablement plan / Chart your course
4. Starts with (high-risk/value) inventory (identity, device, workload, data)
5. Focus identity and access management (IAM)
6. Weave Zero Trust into companywide security enhancements (new initiatives)
7. Continually track improvements
8. Communicate the good news and sell the business value of Zero Trust (efficiency)
9. Keep your program and messages pragmatic

Source: Zero Trust Security: The Business Benefits And Advantages (forrester.com)

Source: [Zero Trust Security: The Business Benefits And Advantages (forrester.com)]

FORRESTER®

Zero Trust Is Good for Business

Reasons to implement

1. Support anywhere-work models
2. Accelerate cloud modernization
3. Pilot emerging technology with less risk
4. Better tech debt management
5. Reduce friction / improve UX/EX
6. Improves visibility and decision-making
7. Increases data awareness and protection
8. Enables digital business transformation

Forrester References

- Zero Trust Security: The Business Benefits And Advantages (forrester.com)
- The Definition Of Modern Zero Trust (forrester.com)
- Success With Zero Trust Lives And Dies By Executive Support (forrester.com)
- A Zero Trust Paradox: Which Comes First, Microsegmentation Or Microperimeter? (forrester.com)
- Why Asset Management Mastery Is Core To Zero Trust (forrester.com)
- Decoding The New Zero Trust Terminology (forrester.com)

FORRESTER®

Thank You.

Zero Trust ≠ Zero Risk

Ron Woerner
Principal Consultant,
Forrester Research

BOLD AT WORK