Zero Trust, How to understand the Paradigm

ITU-T workshop on “Zero Trust and SW Supply Chain Security”

Aug. 28th, 2023

Gachon University, Korea

Sokjoon Lee

CONTENTS

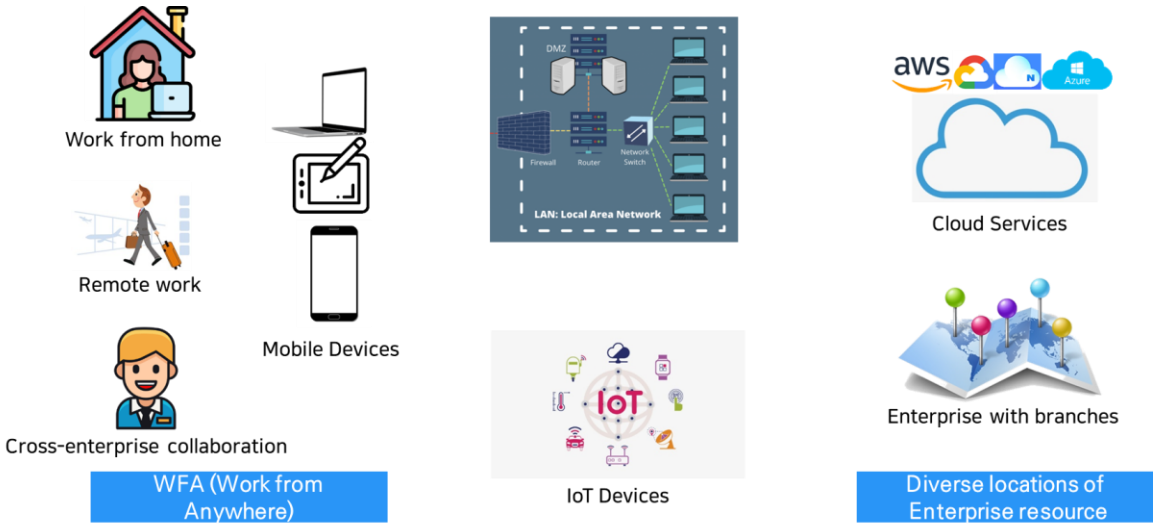
1. The concept of Zero Trust

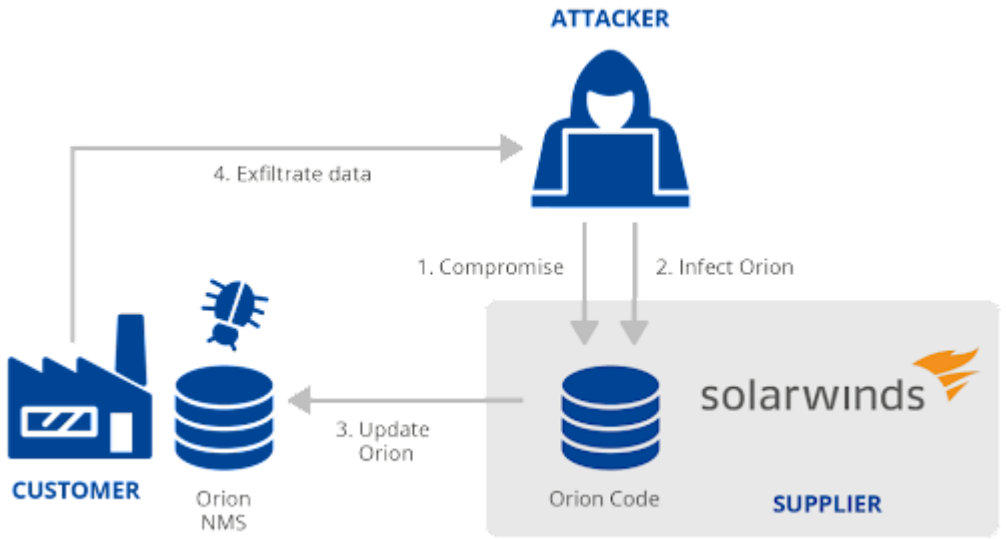
1) background

Security perimeters blurring with the mobile, cloud, and IoT technologies

Threats to national security/infrastructure due to advanced and continuous hacking cases

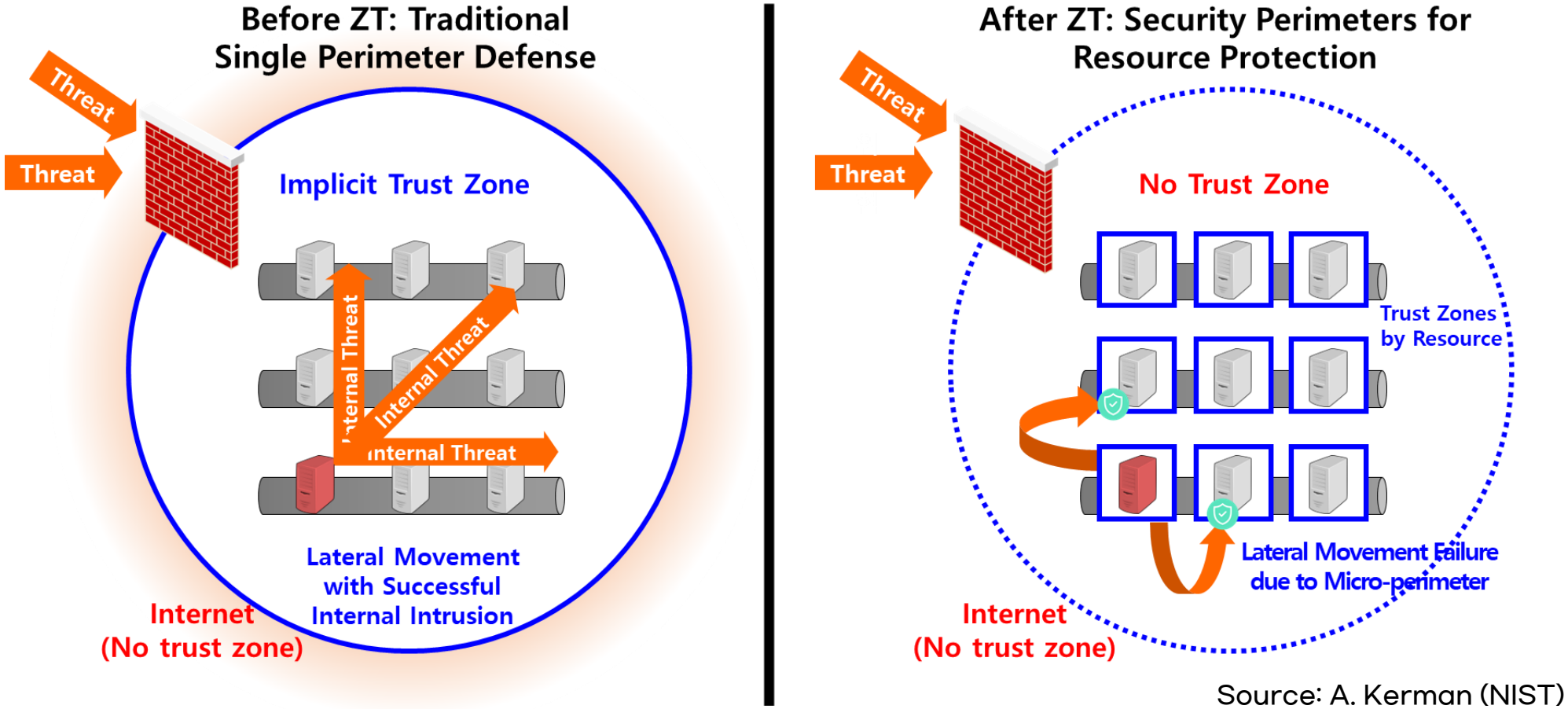
Difficulties to get internal network visibility





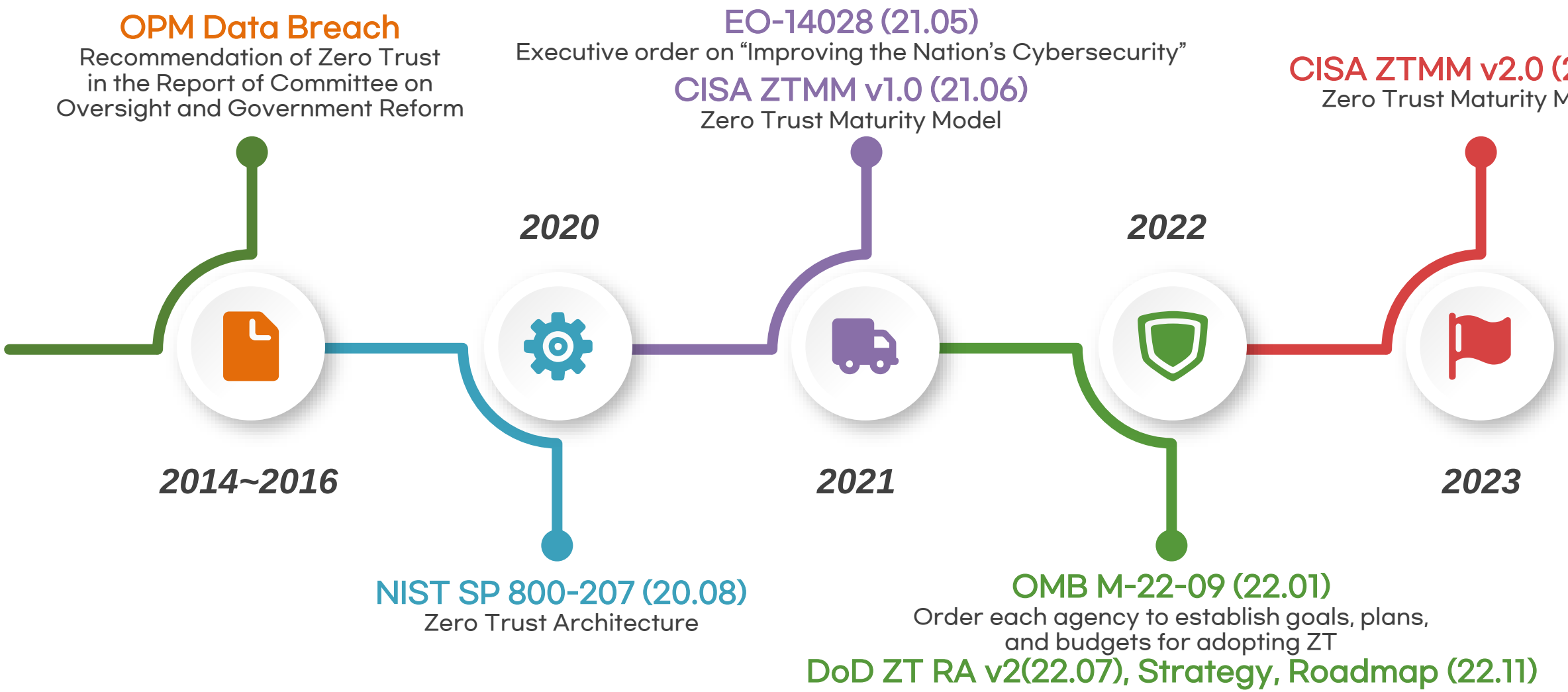
Source: ActiveState

2) Emergence of Zero Trust



Source: A. Kerman (NIST)

3) Introduction ZT in the US Federal Government



4) Definition of ZT in the US Federal Government

Definition of ZT

(NIST) 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.

(NIST, DoD) an evolving set of cybersecurity paradigms that move defenses from static, network-based perimeters to focus on users, assets, and resources.

(NSA) a security model, a set of system design principles, and a coordinated cybersecurity and system management strategy based on an acknowledgement that threats exist both inside and outside traditional network boundaries

Definition of ZT Architecture

(NIST) an enterprise's cybersecurity plan that utilizes zero trust concepts and encompasses component relationships, workflow planning, and access policies

5) Definition of ZT in other area

Definition of ZT

(CSA) a network security concept centered on the belief that organizations should not automatically trust anything inside or outside traditional perimeters and aims to defend enterprise assets.

(Gartner) a security paradigm that explicitly identifies users and devices and grants them just the right amount of access so the business can operate with minimal friction while risks are reduced.

6) Common Concept from all definition of ZT

Common Concept

- Possibility that the enterprise network has already been compromised
- Accurate and Continuous Access Control based on Trust Evaluation or Inference
- Security Concept, Paradigm or Set of Idea

Eliminate Trust	✗	✓	Evaluate Trust Accurately
Eliminate Perimeter	✗	✓	Move Perimeter to Each Resource

7) Tenets of Zero Trust

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—including the observable state of client identity, application/service, and the requesting asset—and may include other behavioral and environmental attributes.
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

- ZTA should be designed and deployed with adherence to the tenets (NIST SP 800-207)
- It may not be possible to implement all tenets in the purest form, taking into account organizational strategy. However, ZTA should be designed considering all tenets as much as possible.

2. The Need for a Common Understanding of Zero Trust

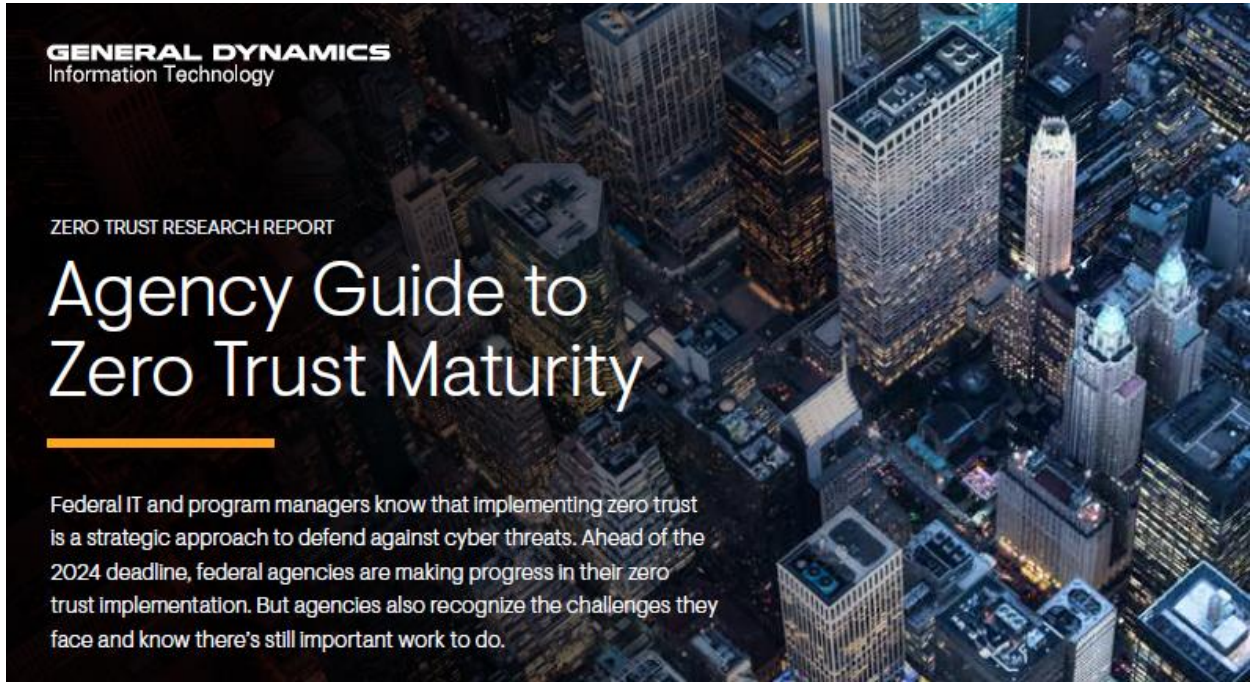
1) How can Zero Trust be adopted?

Can we “buy” Zero Trust?

No; Zero Trust may include certain products or technologies but cannot be achieved solely through introducing new technologies.

Source: T. Denman (DoD), Zero Trust - The Time is Now!

2) Agency Guide to Zero Trust Maturity (General Dynamics)



The 300 IT and program managers across the federal civilian, and defense agencies surveyed for this report

DEFENSE AGENCIES

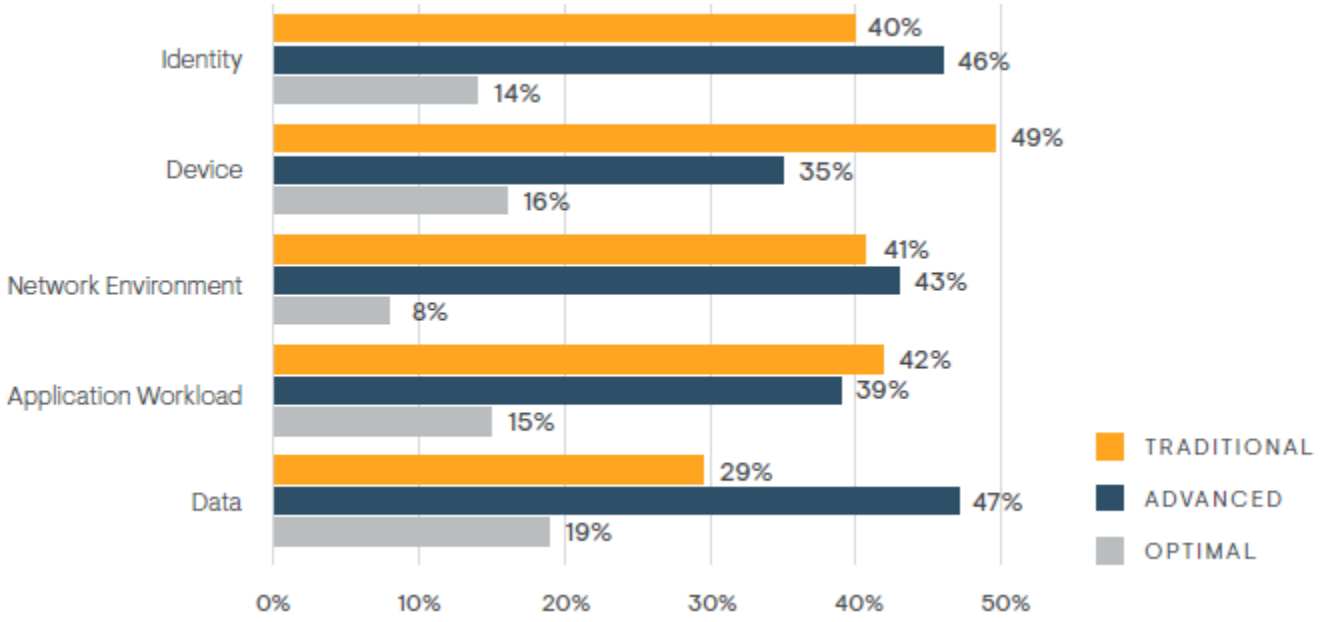
40%

FEDERAL CIVILIAN AGENCIES

60%

2) Agency Guide to Zero Trust Maturity (General Dynamics)

The Five Pillars of the CISA Zero Trust Maturity Model



DATA PILLAR

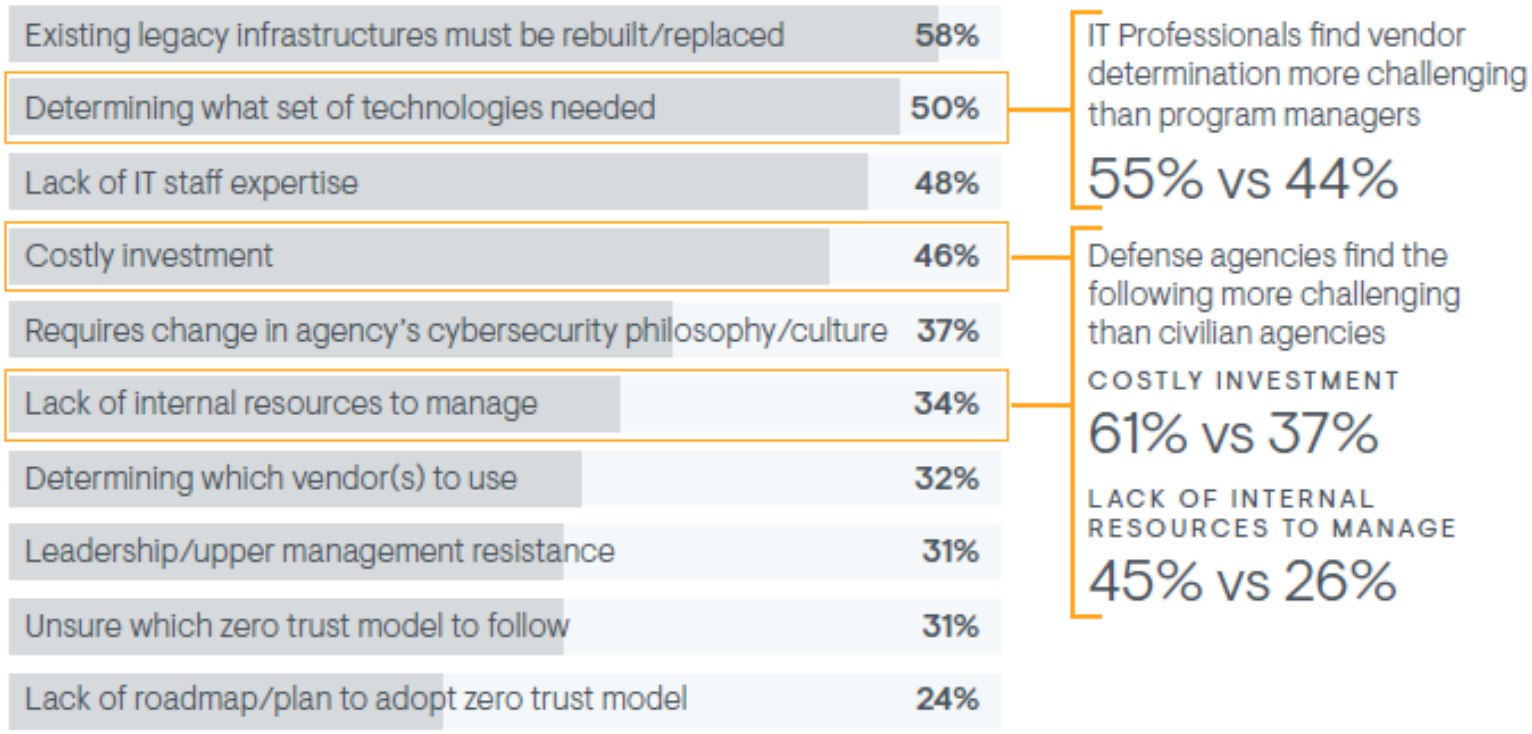
For the data pillar at the traditional maturity stage, federal civilian agencies are less mature than defense agencies.

34% vs 23%

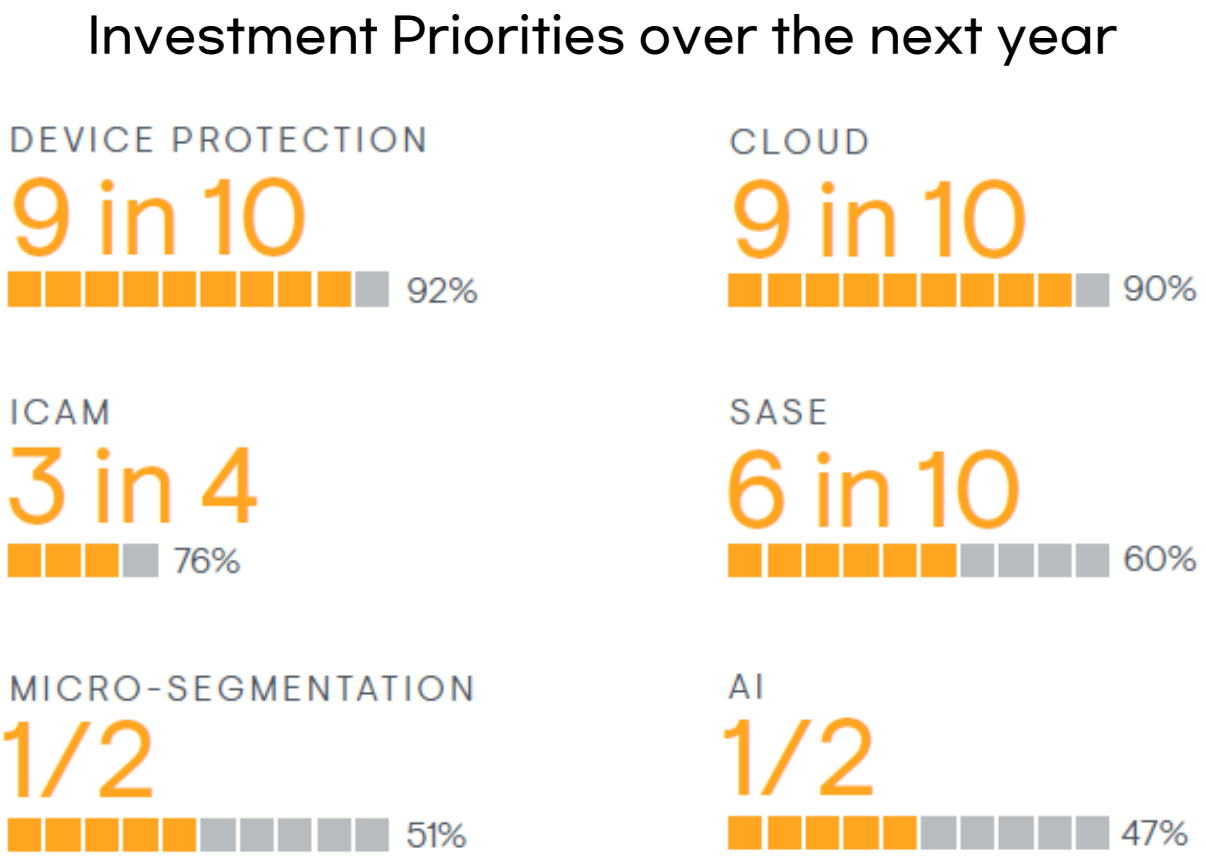
US federal IT and program managers regard **"Device"** as the least mature pillar in terms of zero trust maturity

2) Agency Guide to Zero Trust Maturity (General Dynamics)

Challenges Implementing a Zero Trust Architecture

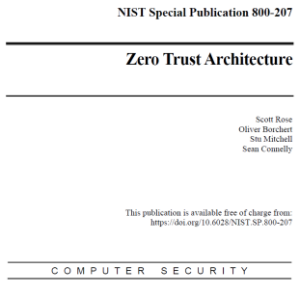


2) Agency Guide to Zero Trust Maturity (General Dynamics)

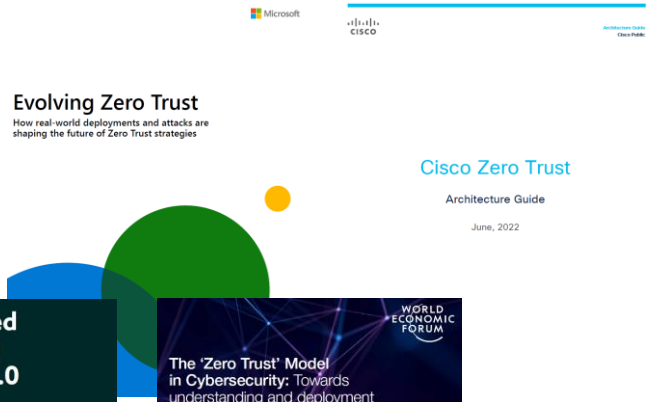


3) Difficulties in adopting Zero Trust

Numerous Zero Trust guidelines, reference architectures, and strategy documents

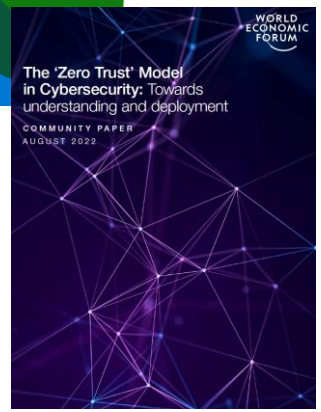


Department of Defense (DoD)
Zero Trust Reference Architecture



Zero Trust Cybersecurity
Current Trends
April 18, 2019

Applying Zero Trust
Principles to Enterprise
Mobility
Version: DRAFT FOR PUBLIC COMMENT
March 2022
Cybersecurity and Infrastructure Security Agency



3) Difficulties in adopting Zero Trust

☑ Understanding of ZT	What is Zero Trust?
☑ Adoption effect	Why should Zero Trust be adopted?
☑ Adoption method	How and with which technologies should enterprise adopt ZT?

The Need for a Common Understanding of Zero Trust

4) Korea Zero Trust Guidelines 1.0 (‘23.06)

4) Korea Zero Trust Guidelines 1.0 (‘23.06)

Purpose

To support the adoption of zero trust architecture suitable for the Korean ICT environment

by quickly and easily understanding the concept of zero trust architecture by Korean government, public, and business sector

Summary version

- from non-professionals to experts
- Helps policy makers involved in the decision-making process, corporate executives and employees to understand Zero Trust

Full version

- Security strategy manager and staff
- Helps security personnel in charge of establishing cyber security plans within the organization using zero trust

4) Korea Zero Trust Guidelines 1.0 (‘23.06)

Publishing Principle

① Since the background and basic principles of Zero Trust, which have been discussed mainly in the United States, do not differ from country to country, US documents were referred to as much as possible, and the basic philosophy was maintained.

② Addition of the new pillar (system) and introduction reference model (remote work and network separation) in consideration of the Korean environment

③ Since the network structure, policies and regulations within the organization are all different, the document is written at a higher level to cover them all

④ It is also written so that the concepts can be understood more easily, considering non-experts involved in the decision-making process and all members of the organization who need to understand the philosophy

3. Misconceptions and How to understand the Paradigm

1) Zero Trust Technology and Solutions

Zero Trust

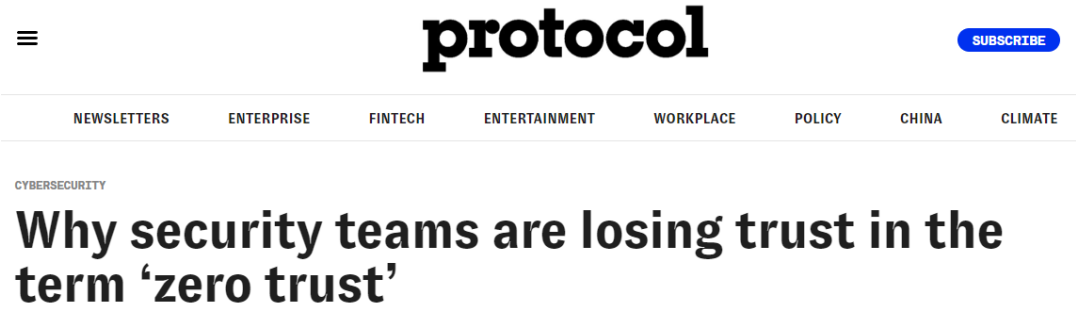
Zero Trust Architecture

Zero Trust Technology

Zero Trust Solutions

- (element) technology/solution that (partially) satisfies the Zero Trust philosophy
- Can the Zero Trust philosophy be satisfied by adopting a specific Zero Trust technology/solution or combining the ones?
- Can cyber attacks be prevented perfectly by adopting specific Zero Trust technologies/solutions?
- Do Zero Trust technologies/solutions have better security than legacy technologies/solutions?

1) Zero Trust Technology and Solutions


protocol

SUBSCRIBE

NEWSLETTERS ENTERPRISE FINTECH ENTERTAINMENT WORKPLACE POLICY CHINA CLIMATE

CYBERSECURITY

Why security teams are losing trust in the term 'zero trust'

exaggerated promotion of Zero Trust technology and solutions

- "with all of the hype and misappropriation of the idea, information security practitioners are pretty burned out on the term at this point.", "Literally every vendor is saying, 'We do zero trust'." - Matthew Prince (Cloudflare CEO)
- "It(Zero Trust) means whatever the person on the other side of the table is trying to sell." - Alex Weinert (Microsoft Vice President)
- "Don't listen to a vendor when they talk about [the definition of] zero trust. It is going to be biased." - Kapil Raina (CrowdStrike Vice President)
- "There's nobody out there that does everything.", "Anybody who claims they can deliver zero trust quickly or easily should also be treated as suspect." - Heath Mullins (Forrester)

2) Misconception 1: Having all the technologies that meet the ZT philosophy will ensure perfect security.

Threats Associated with Zero Trust Architecture (NIST SP 800-207)

- Subversion of ZTA Decision Process
- Denial-of-Service or Network Disruption to Policy Decision/Enforcement Point
- Stolen Credentials/Insider Threat
- Difficulties in obtaining network visibility
- Attacks on Storage of System and Network Information
- Reliance on Proprietary Data Formats or Solutions
- Use of Non-person Entities (NPE) in ZTA Administration (true negatives and false positives)

1) ZT can mitigate risks, but **it cannot eliminate all security risks or attacks.**
2) The threats above do **not mean that the ZTA has fundamental weaknesses.**
3) **Security vulnerabilities can be embedded** in the process of implementing and operating Zero Trust technology

2) Misconception 1: Having all the technologies that meet the ZT philosophy will ensure perfect security.

"However, CISOs and risk management leaders should not assume that zero trust will eliminate cyberthreats. Rather, zero trust reduces risk and limits impacts of an attack."

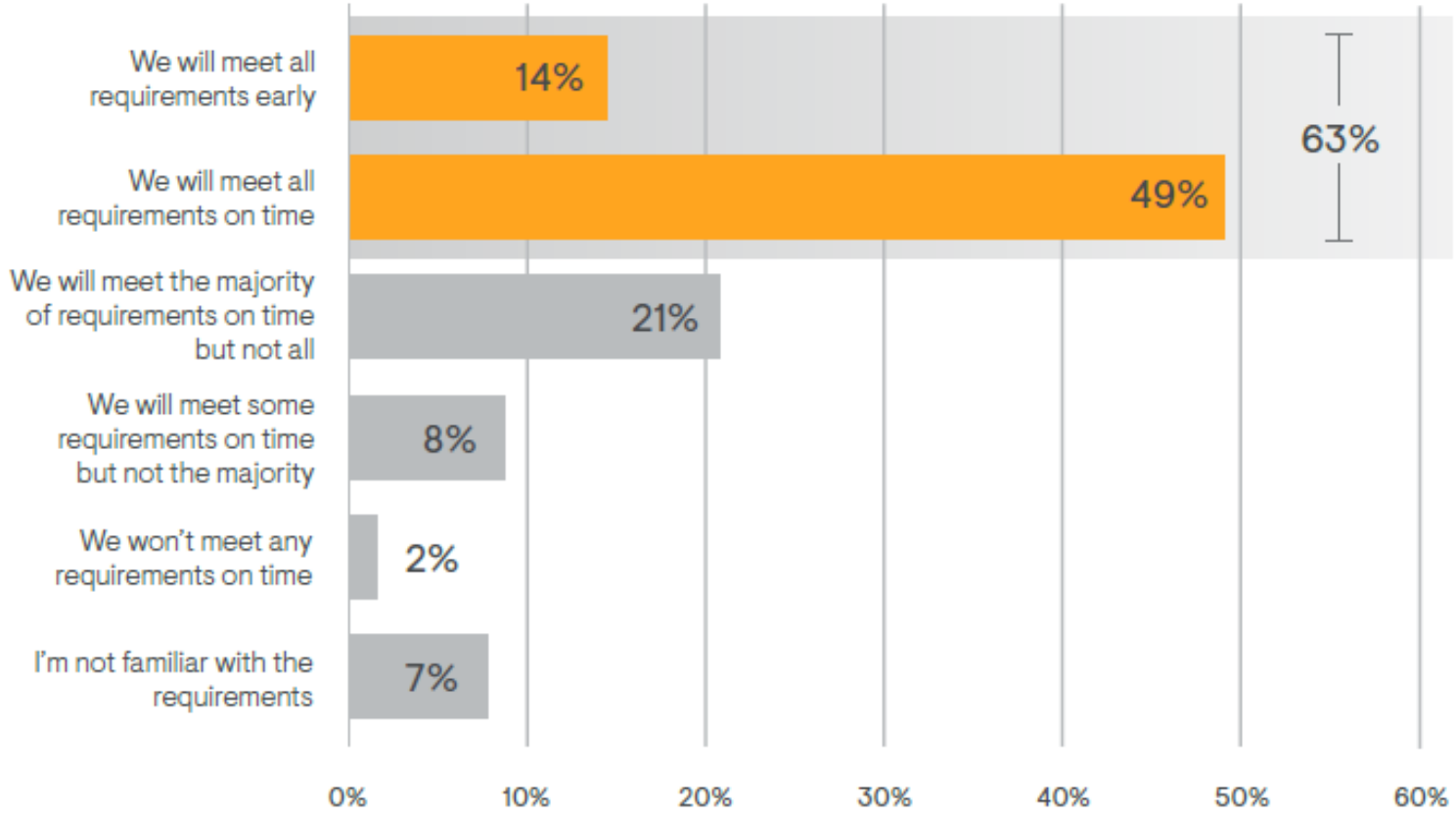
Source: Gartner, "Gartner Predicts 10% of Large Enterprises Will Have a Mature and Measurable Zero-Trust Program in Place by 2026"

3) Misconception 2: ZT can be implemented adopted in a short period of time.

☑ Technical difficulties	Need to implement high-level zero trust functions (AI-based trust verification, real-time risk management, etc.)
☑ Inter-operability	Requires API integration of zero trust functions (authentication, asset management, various logs integration, monitoring, etc.)
☑ No best practice	No case of successfully implementing and operating high-level zero trust
☑ DoD ZT Roadmap	The US Department of Defense roadmap plans to implement Advanced ZT by FY 2032
☑ NSTAC Report	NSTAC Report notes that government-wide implementation of ZT is a journey measured in years to decades

3) Misconception 2: ZT can be implemented adopted in a short period of time.

Timeline to Meeting EO-14028 and OMB M-22-09 Requirements (by 2024)



3) Misconception 2: ZT can be implemented adopted in a short period of time.

STAMFORD, Conn., January 23, 2023

Gartner Predicts 10% of Large Enterprises Will Have a Mature and Measurable Zero-Trust Program in Place by 2026

1) Gartner predicts that by 2026, 10% of large enterprises will have a mature ZT. (currently less than 1%)

2) 63% of US federal agencies said they would achieve the ZT goal set by OMB by FY2024.

3) The U.S. DoD set 10 years (until 2032) for the implementation of advanced ZT.

4) While the situation would be different for organizations, it is reasonable to assume that a high level of Zero Trust is difficult to achieve in a short period of time.

5) There would be unintended problems in the Zero Trust transition process.

4) Misconception 3: ZT requires removing all legacy security technologies and solutions.

☑ Legacy vs ZT

For example, is (next-generation) firewall a legacy technology?
If so, should we remove it?

Perimeter	De-Perimeterization
Static Access Control	Dynamic Access Control

1) there are cases in which ZT philosophy is embedded in the legacy technology currently in use.

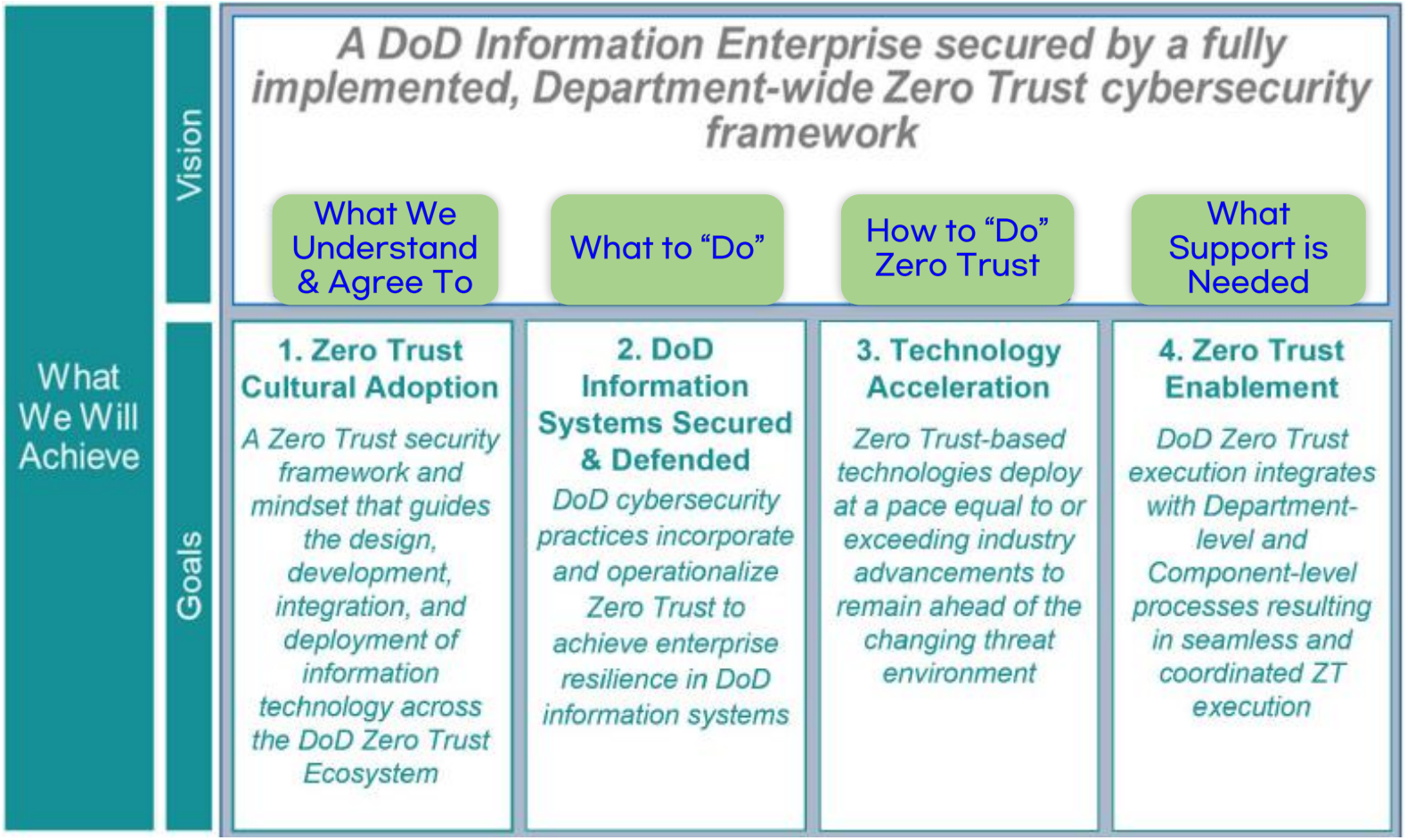
2) In general, legacy technologies have high performance and are stable, so retaining them can be considered if there is little benefit compared to the cost of ZT technologies.

3) Legacy technology generally has simple rules, so side effects are small and results are easy to predict.

4) When transitioning to ZT, an approach that minimizes side effects is needed rather than removing all legacy security technologies.

5) Misconception 4: The core goal of the ZT strategy is the adoption of ZT technology and solutions.

US DoD, Zero Trust Strategy (Nov. 2022)



5) Misconception 4: The core goal of the ZT strategy is the adoption of ZT technology and solutions.

Zero Trust Cultural Adoption

- Commitment
- Outreach
- Awareness
- Workforce
- Training

Zero Trust Support

- Policy
- Programming
- Planning
- Funding
- Acquisition
- Performance
- Zero Trust PfMO

For the enterprise, **cultural adoption and support** are also important goals in the long-term operational perspective of Zero Trust.

6) Misconception 5: When adopting Zero Trust, employees will be happy not to use inconvenient VPNs.

☑ New inconvenience	Possibility of hindering work performance due to the least privileges and strict access control
	Troubles such as compulsory business devices, device hygiene checks, and updates
	Possibility of falsely detecting normal user activity as suspicious due to mis-configured dynamic access control engine
	Possibility of requiring procedures such as asset and ID registration even for use of temporary devices
☑ Privacy Issues	status monitoring such as the user's location, using programs, etc.

Requires a strategy to maintain security while minimizing employee inconvenience in the adoption and operation of Zero Trust

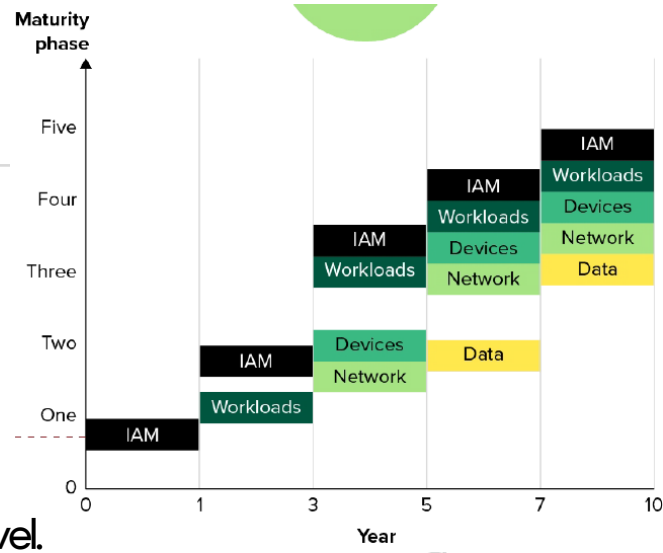
7) Enterprise Strategy: How to adopt Zero Trust?

☑ Identify the current security solution	Which security solutions are currently in use, and how can they be replaced or supplemented?
	For example, will the current network separation solution be maintained?
☑ Identify data and service	What resources (network, application services, data) need to be protected?
	Which cloud services are you currently using? Or do you have any transition plans?
☑ Identify user and device	What about identity management and authentication schemes?
	Is the device (asset) inventory made? Are all devices managed?
	Which security technologies are used or necessary for user and device access control and security?

7) Enterprise Strategy: How to adopt Zero Trust?

Adopting a specific pillar in the enterprise network

- Example) A plan to focus on the adoption of identifier-centric ZT
  - ✓ DoD regards integrated ICAM as a basic function of zero trust
  - ✓ Enhanced Identity Governance (NIST SP 1800-35, ZT implementation)
  - ✓ Roadmap of Starting from IAM (Forrester)
- When intermediate goals are reached, move on to other pillars and increase your maturity level.



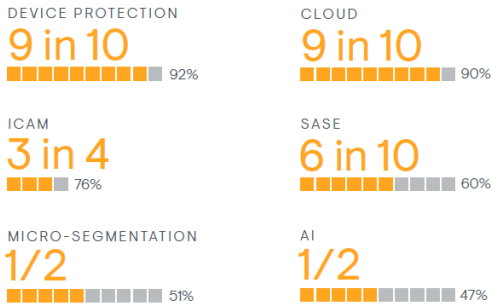
Starting with specific business processes

- Organizations performing specific military tasks in the military (ex. specific units, ships, etc.)
  - ✓ Clearly identify process-related users, devices, resources, and policies
  - ✓ Define required functions such as enhanced authentication, micro-segmentation, and SDP
  - ✓ Establish workflow scenarios for processes
  - ✓ Implementation and validation after adopting a security solution including defined functions
- Extending to other processes, continuously verifying all ZT functions

7) Enterprise Strategy: How to adopt Zero Trust?

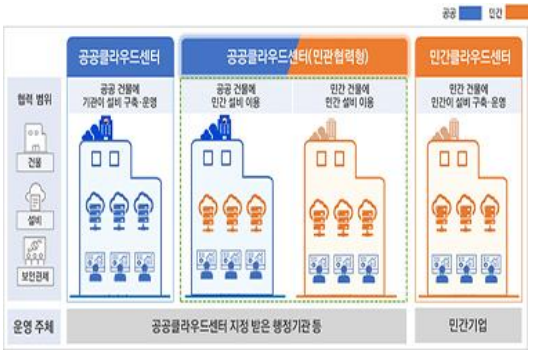
Investment Priorities in US Government

- Endpoint Security Solution (EDR, MDM, etc)
- Cloud Security (CASB, CWPP, SASE, etc.)
- Enterprise-Wide ID Management, MFA, PAM, etc



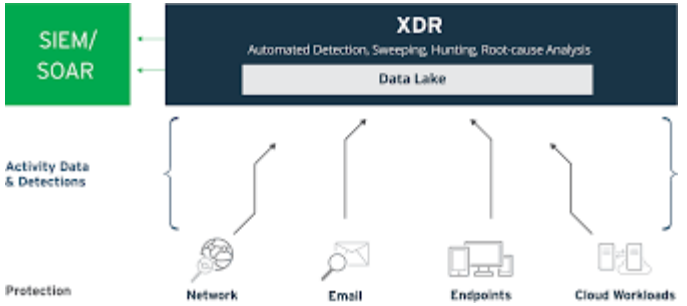
Korean Business Enterprise

- Financial institutions: network separation regulations
  → Complement network separation through NAC and SDP
- Government Sector: Use of public cloud, API opens to private services
  → Cloud security, API access control



RSA Conference 2023

- Topic: Stronger Together **(collaboration between companies or private and public sectors)**
- XDR (eXtended Detection and Response)
- AI and security, Threat intelligence, Zero Trust



Conclusion

How to understand Zero Trust

- Zero Trust is a security philosophy (not technology or solution) that eliminates trust and minimizes risks to establish high security through strong authentication, least privilege, and context-aware dynamic access control.
- It may take a long time (more than 10 years) to technically adopt and implement a high-level Zero Trust Architecture, and it is necessary to set intermediate and final goals according to the enterprise situation and current maturity level.
- Zero Trust is a security philosophy that must be adopted throughout the enterprise, and it is not desirable to emphasize only partial principles or specific security technologies and solutions.