글로벌 ICT 표준 컨퍼런스 2023

Global ICT Standards Conference 2023

(세션5) 사이버보안: 신뢰성 있는 디지털 환경 구축

제로트러스트 기술과 보안 패러다임의 전환

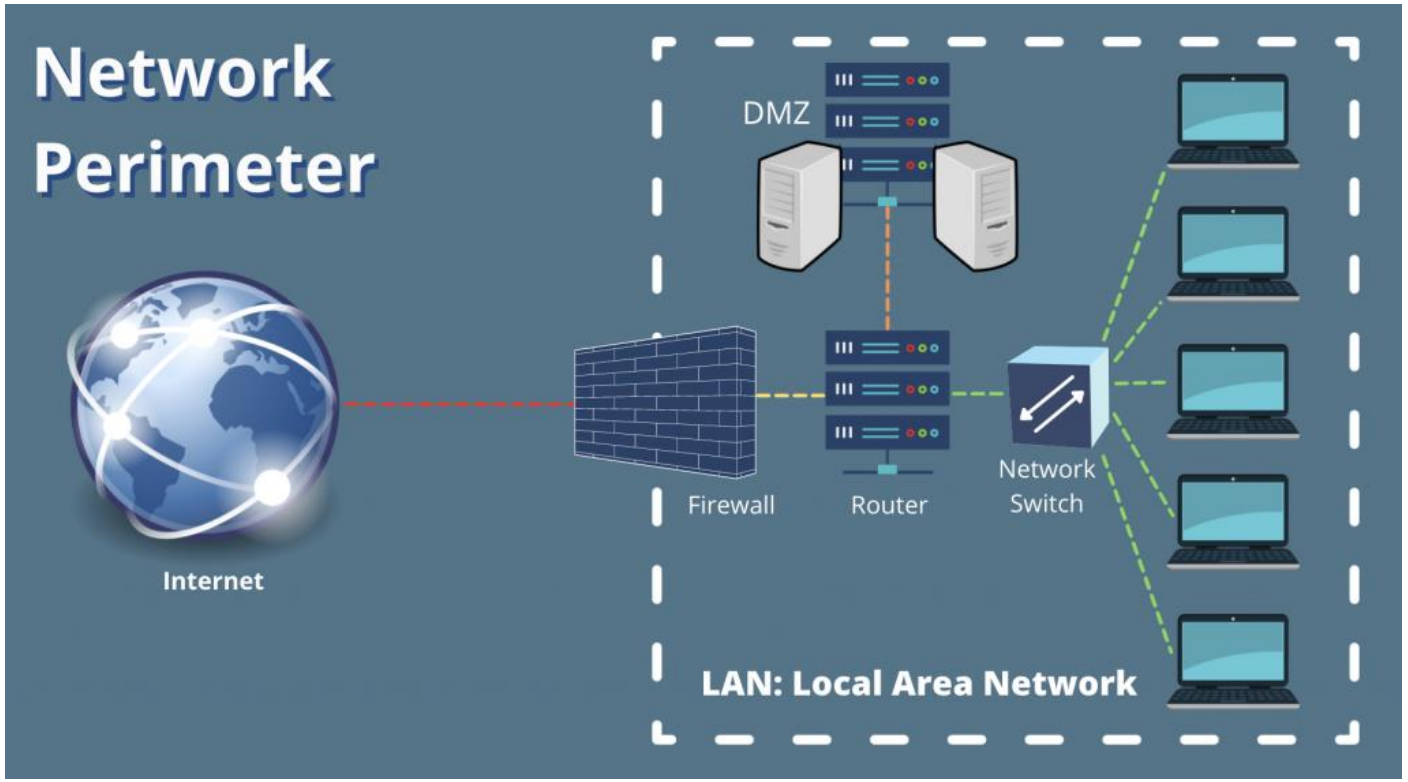
이석준 교수, 가천대학교

주최 과학기술정보통신부 Ministry of Science and ICT
특허청 Korean Intellectual Property Office
주관 국립전파연구원 National Radio Research Agency
TTA IITP KEA kista ETRI

Index

01. 신뢰의 제거, 제로트러스트의 시작

기업 네트워크 환경의 변화



기업망의 내부 진입점에 대한 강력한 보안 (Firewall, IDS 등)

01. 신뢰의 제거, 제로트러스트의 시작

문제 1. 흐려지는 경계 – 점점 더 복잡해지는 기업망

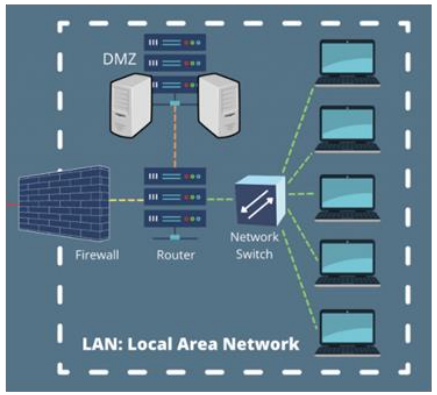
재택 근무

원격 근무

협력업체 직원

모바일 기기의 확산

WFA (Work from Anywhere)



각종 IoT 기기

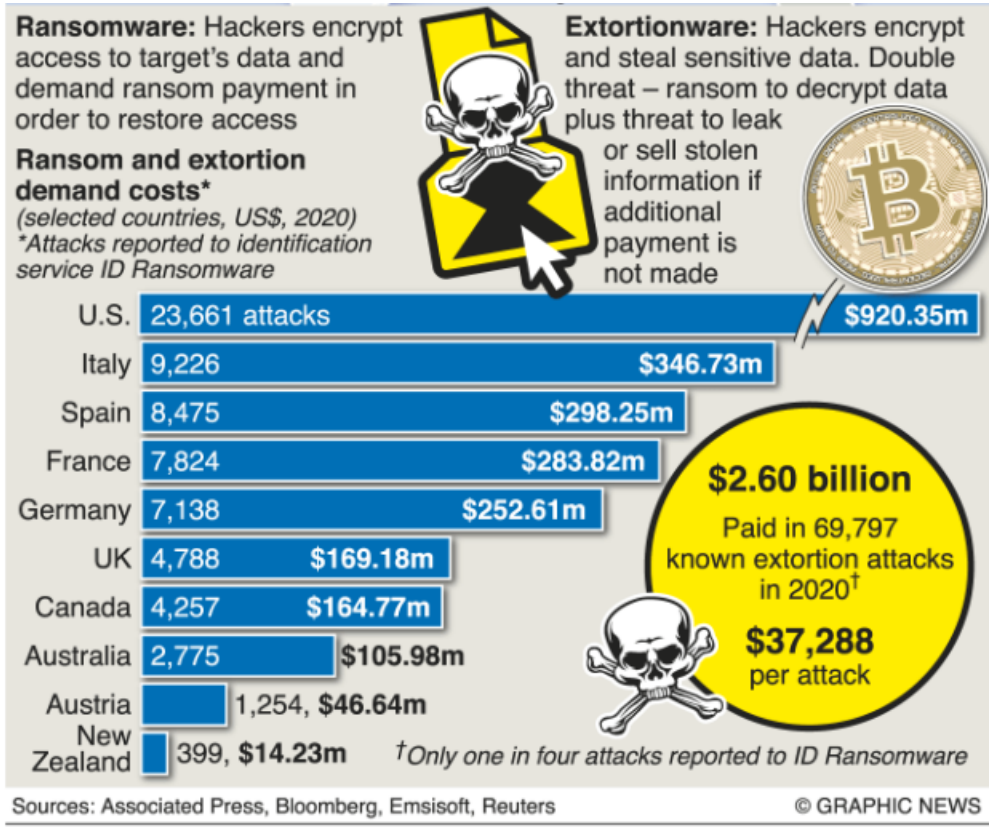
클라우드 서비스

지사 운영

기업 리소스 위치 다변화

01. 신뢰의 제거, 제로트러스트의 시작

문제 2. 경계기반 보안을 뚫는 해킹 – 랜섬웨어 공격 등 국가 안보·인프라 위협



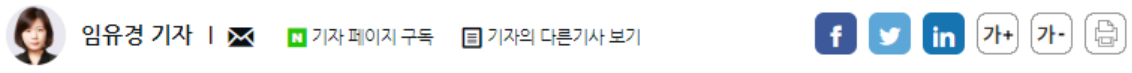
01. 신뢰의 제거, 제로트러스트의 시작

문제 2. 경계기반 보안을 뚫는 해킹 – 랩서스 해킹 사례

삼성·MS 뚫은 해커집단 랩서스, 공격수법 드러났다

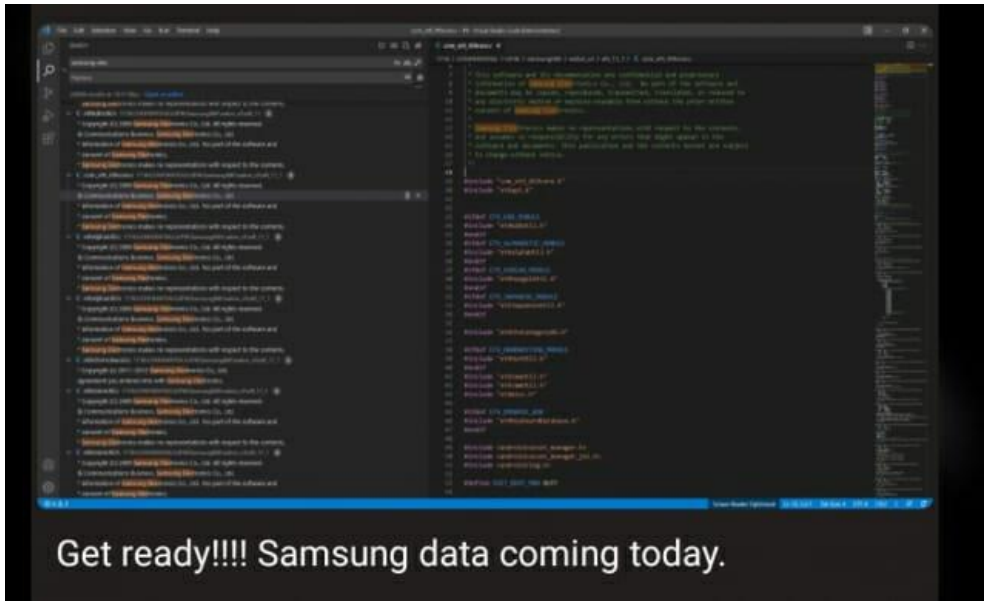
MS, 전술파악 성공…"SIM스와핑·유출계정 구매 수법 동원"

컴퓨팅 | 입력 :2022/03/24 19:30 수정: 2022/03/25 09:12



임유경 기자 | 기자 페이지 구독 기자의 다른기사 보기

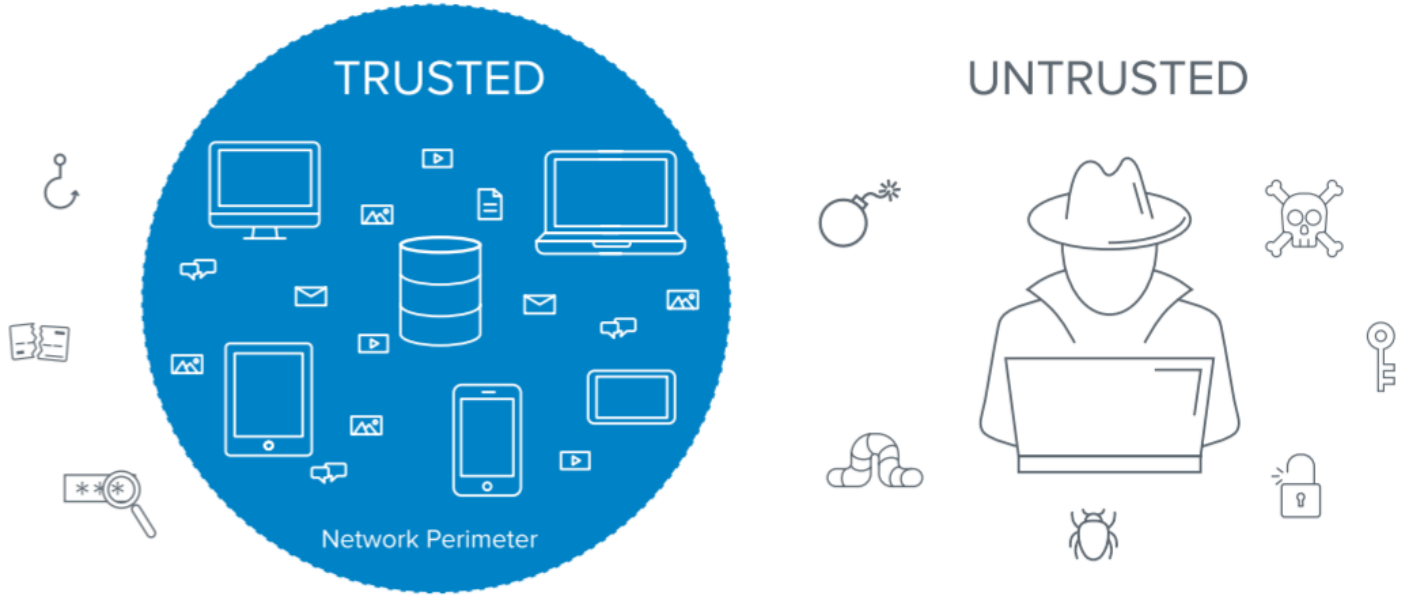
마이크로소프트가 최근 몇 달 사이 글로벌 IT 기업 여러 곳을 해킹해 악명을 높인 해커집단 '랩서스(Lapsus$)'를 쫓고 있다. 마이크로소프트도 랩서스에 뚫려 검색 엔진 빙·인공지능 비서 코타나 소스코드를 탈취당하는 수모를 겪은 만큼, 설욕을 위해 단단히 벼르고 있는 모양새다.



1 단계 : 초기 접근권한 확보
2 단계 : 정찰 및 권한 상승
3 단계 : 유출과 갈취

01. 신뢰의 제거, 제로트러스트의 시작

경계기반 보안의 약점

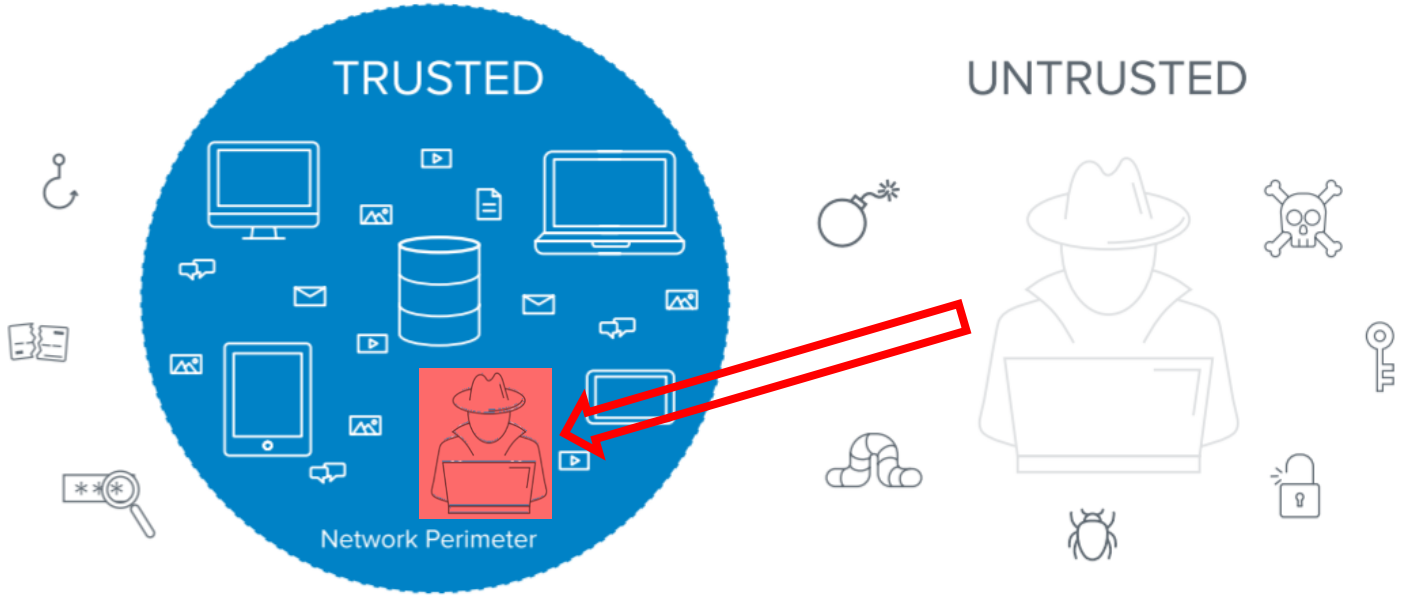


보안 경계를 둔다는 것:

내부자에게 더 높은 신뢰 부여

01. 신뢰의 제거, 제로트러스트의 시작

경계기반 보안의 약점



사이버 공격의 1차 목표:

내부 침투

01. 신뢰의 제거, 제로트러스트의 시작

신뢰의 위험성

사전적 의미

- 굳게 믿고 의지함
- 타인의 미래 행동이 자신에게 **호의적이거나 또는 최소한 악의적이지는 않을 가능성에 대한 기대**와 믿음

Trust (신뢰, 信賴)

보안 관점의 의미

- 악의적이지 않을 것이라는 기대감으로, 상대방의 행위에 **취약**해지는 당사자의 의지
- 신뢰를 부여할수록 **위험 증가**

01. 신뢰의 제거, 제로트러스트의 시작

보안 패러다임의 변화: '제로트러스트'

FORRESTER® Making Leaders Successful Every Day

September 14, 2010 | Updated: September 17, 2010

No More Chewy Centers:
Introducing The Zero Trust Model
Of Information Security

by John Kindervag
for Security & Risk Professionals

Never Trust,

Always Verify

목표: 기업과 정부의 위험(Risk) 최소화

- 모든 종류의 접근을 신뢰하지 말 것 (지속적인 신뢰도 검증)
- 일관되고 중앙집중적 정책 관리·접근 제어 실행 및 최소 권한 부여
- 사용자·기기 관리 및 강력한 인증, 암호화

02. 미 연방정부 제로트러스트 도입 전략

미 연방정부 관련 제로트러스트의 첫 등장 ('16.09)

연방 인사관리처(OPM) 개인정보유출사고(2014, 2015)에 대한
미 하원 감독개혁위원회 보고서: 연방정부 보안을 위한 제로트러스트 모델 권고

The OPM Data Breach: How the Government Jeopardized Our National Security for More than a Generation

Majority Staff Report

Hon. Jason Chaffetz, Chairman
Committee on Oversight and Government Reform

Hon. Mark Meadows, Chairman
Subcommittee on Government Operations

Hon. Will Hurd, Chairman
Subcommittee on Information Technology

September 7, 2016

www.oversight.house.gov

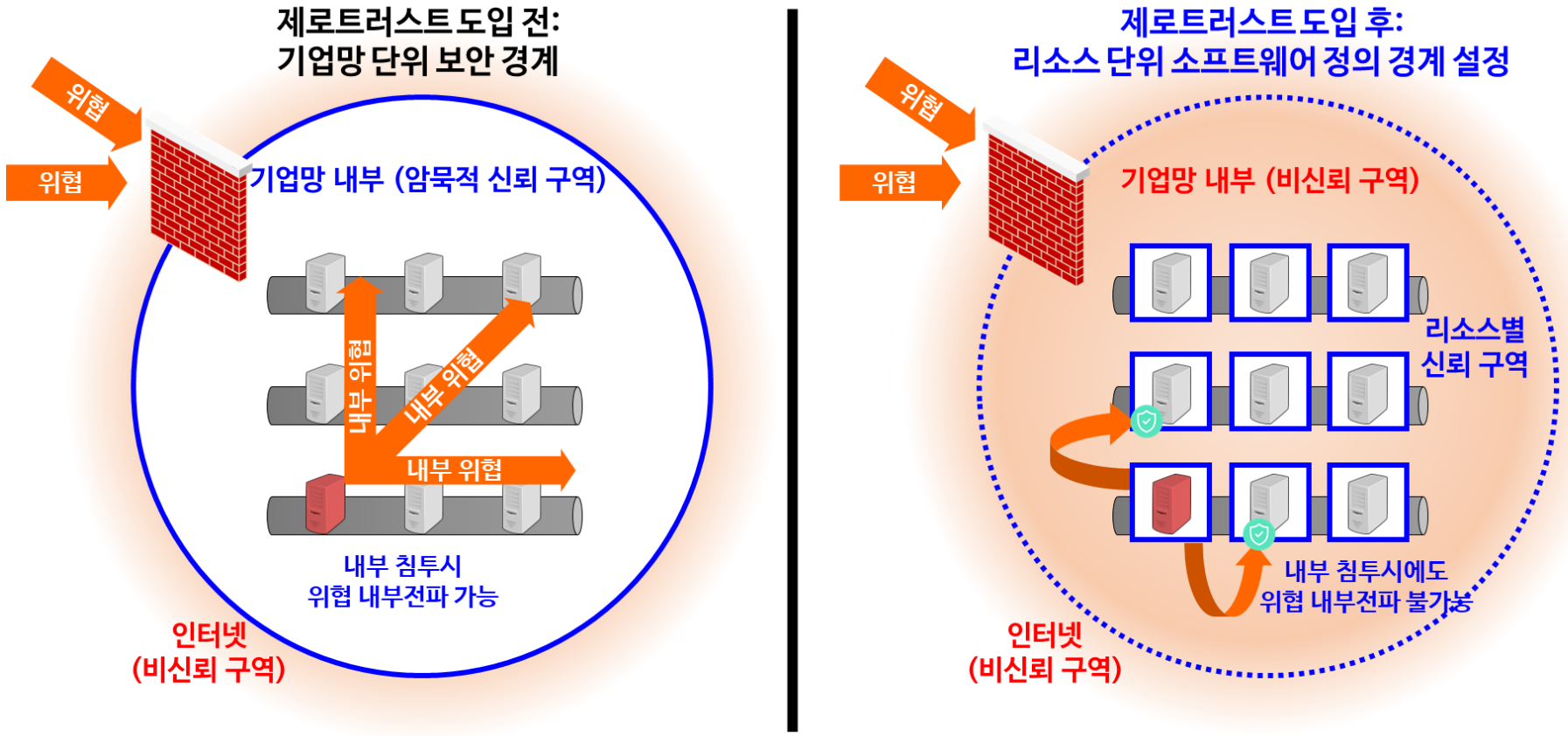
Recommendation 2 – Reprioritize Federal Information Security Efforts Toward a Zero Trust Model

OMB should provide guidance to agencies to promote a zero trust IT security model. The OPM data breaches discovered in 2014 and 2015 illustrate the challenge of securing large, and therefore high-value, data repositories when defenses are geared toward perimeter defenses. In both cases the attackers compromised user credentials to gain initial network access, utilized tactics to elevate their privileges, and once inside the perimeter, were able to move throughout OPM's network, and ultimately accessed the "crown jewel" data held by OPM. The agency was unable to visualize and log network traffic which led to gaps in knowledge regarding how much data was actually exfiltrated by attackers.

To combat the advanced persistent threats seeking to compromise or exploit federal government IT networks, agencies should move toward a "zero trust" model of information security and IT

02. 미 연방정부 제로트러스트 도입 전략

Zero Trust in NIST SP 800-207 ('20.08)



A. Kerman (NIST)의 그림 재구성

02. 미 연방정부 제로트러스트 도입 전략

바이든 대통령 행정명령 (EO-14028, '21.05) - “Improving the Nation’s Cybersecurity”

"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."

— Executive Order on Improving the Nation’s Cybersecurity 12 May 2021

“점진적인 개선은 우리에게 필요한 보안을 제공하지 않습니다.
대신, 연방 정부는 미국인의 삶의 방식을 뒷받침하는 중요한 기관을
보호하기 위해 **대담한 변화와 상당한 투자**를 해야 합니다.”

02. 미 연방정부 제로트러스트 도입 전략

바이든 대통령 행정명령 (EO-14028, '21.05) - "Improving the Nation's Cybersecurity"

Sec. 3. *Modernizing Federal Government Cybersecurity.* (a) To keep pace with today's dynamic and increasingly sophisticated cyber threat environment, the Federal Government must take decisive steps to modernize its approach to cybersecurity, including by increasing the Federal Government's visibility into threats, while protecting privacy and civil liberties. The Federal Government must adopt security best practices; advance toward Zero Trust Architecture; accelerate movement to secure cloud services, including Software as a Service (SaaS), Infrastructure as a Service (IaaS), and Platform as a Service (PaaS); centralize and streamline access to cybersecurity data to drive analytics for identifying and managing cybersecurity risks; and invest in both technology and personnel to match these modernization goals.

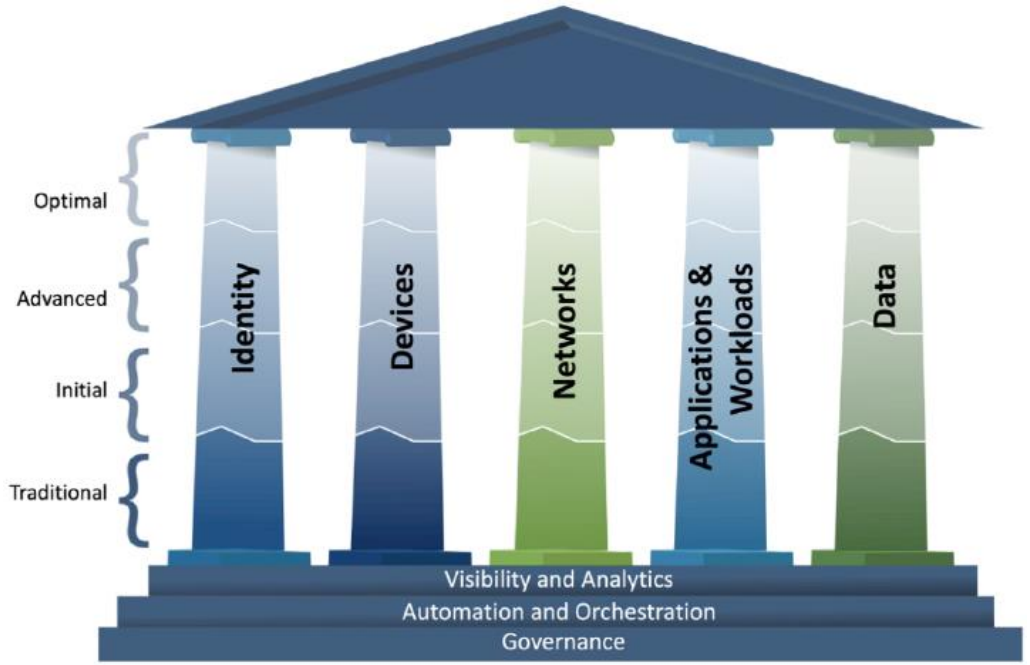
(b) Within 60 days of the date of this order, the head of each agency shall:

(ii) develop a plan to implement Zero Trust Architecture, which shall incorporate, as appropriate, the migration steps that the National Institute of Standards and Technology (NIST) within the Department of Commerce has outlined in standards and guidance, describe any such steps that

각 행정기관장은 **NIST의 표준, 지침**을 따르는 제로트러스트 아키텍처 도입 계획을 60일 이내에 개발해야 함

02. 미 연방정부 제로트러스트 도입 전략

CISA ZT Maturity Model ('21.06, '23.04)



	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

02. 미 연방정부 제로트러스트 도입 전략

예산관리실(OMB) 각서 (M-22-09, '22.01) - "제로트러스트 사이버보안 원칙을 향한 미 정부의 움직임"

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

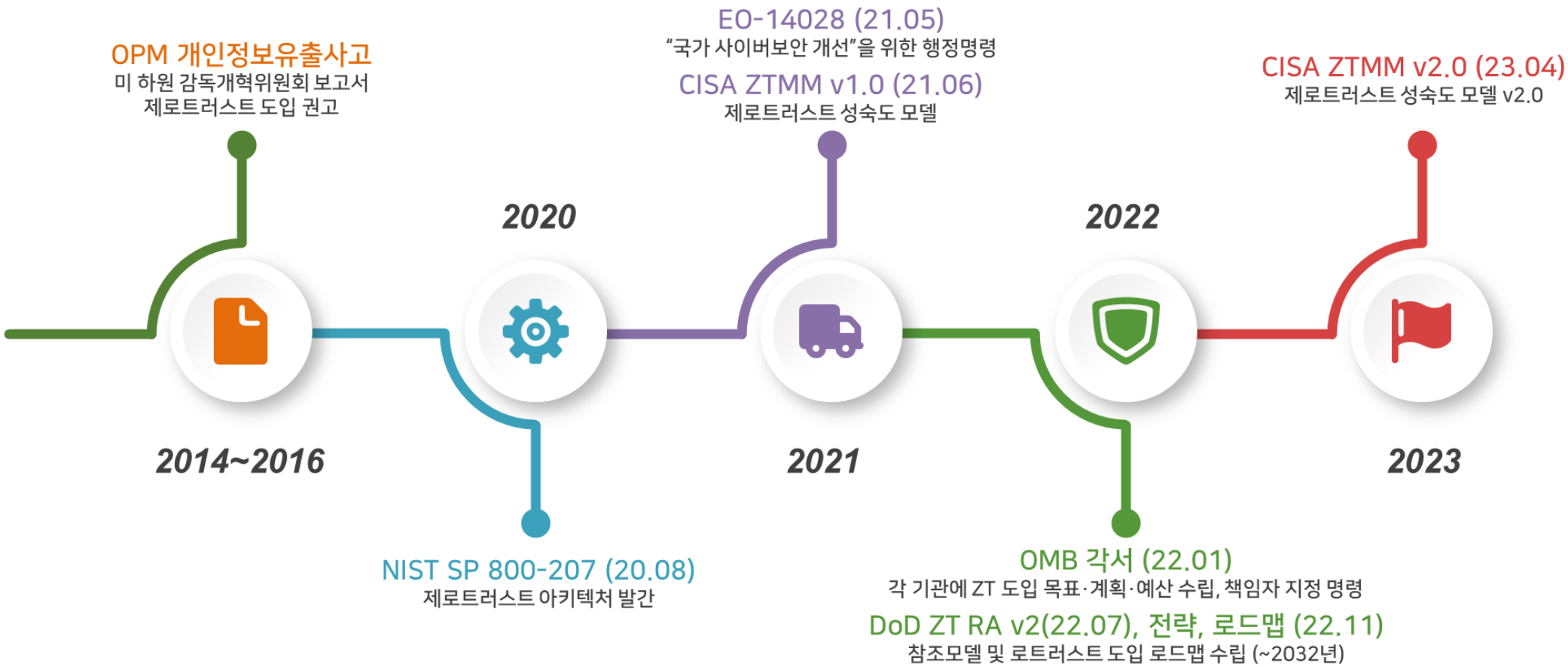
SUBJECT: Moving the U.S. Government Toward Zero Trust Cybersecurity Principles

각 행정기관에 대해 다음 사항을 요구

- FY 2024년말까지 제로트러스트 보안 목표를 수립할 것 (CISA 제로트러스트 성숙도 모델 5가지 핵심 요소와 일치)
- 각서 발표 60일 이내에 FY 2024년까지 도입 계획 및 예산 추정치를 OMB와 CISA에 제출할 것
- 각서 발표 30일 이내에 제로트러스트 전략 구현 책임자를 지정할 것

02. 미 연방정부 제로트러스트 도입 전략

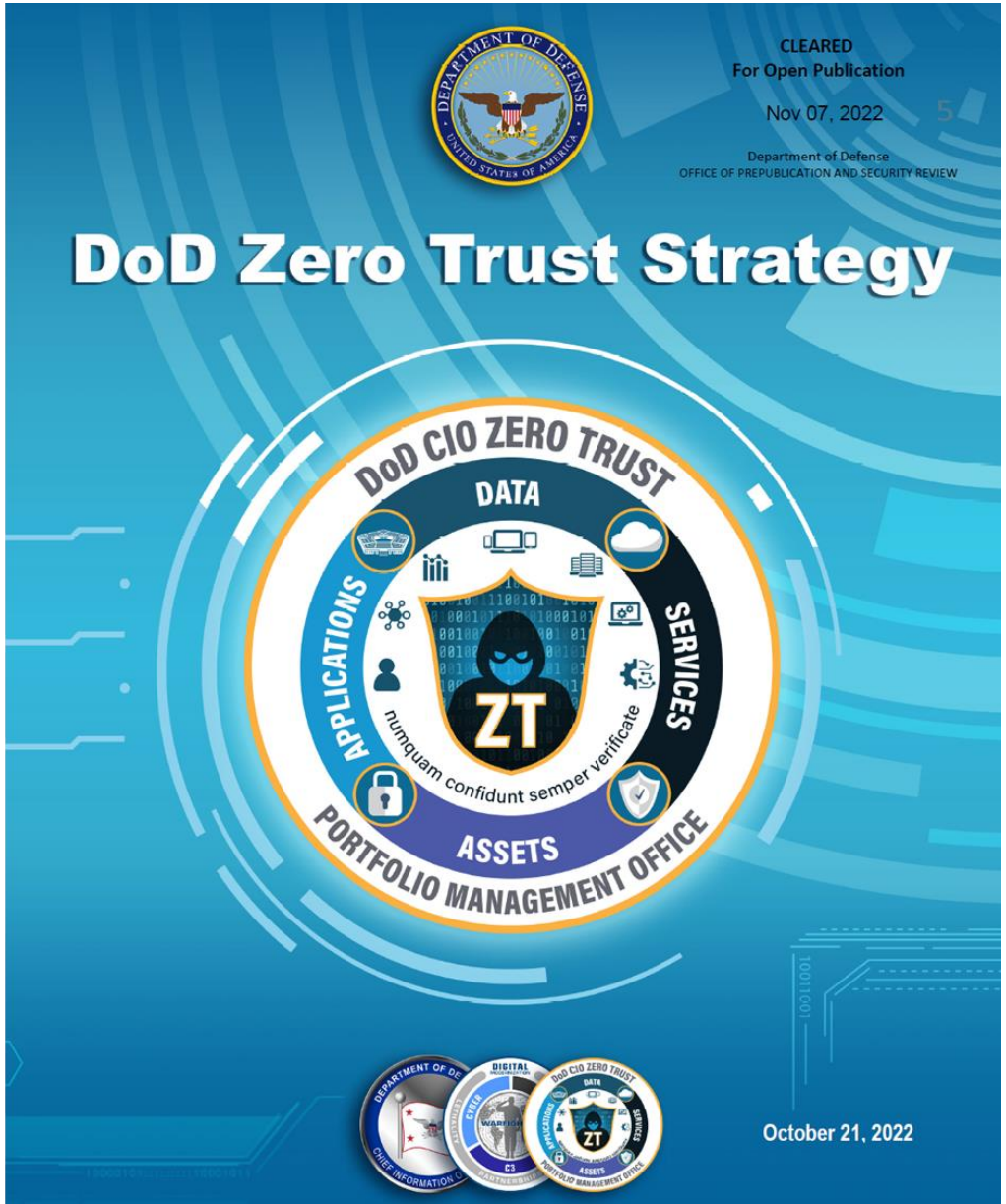
미 연방정부 제로트러스트 도입 움직임



02. 미 연방정부 제로트러스트 도입 전략

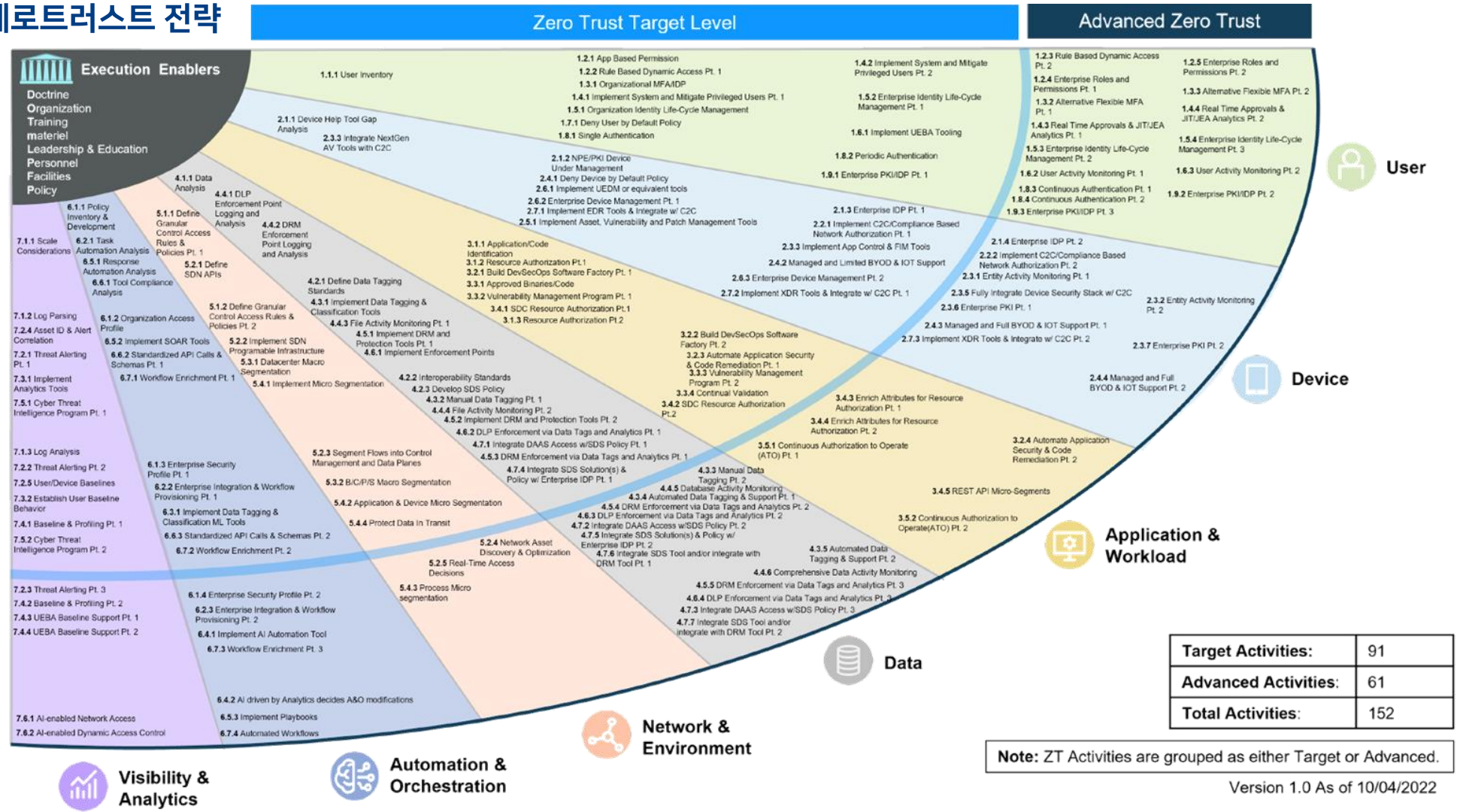
미 국방부 제로트러스트 전략

DoD 제로트러스트 관련 진행 사항
국방부 제로트러스트 참조 아키텍처 1.0 발표 (21.02)
NSA, 제로트러스트 보안 모델 수용 지침 (21.02)
The President, 국가 안보, 국방부 및 정보공동체 사이버 보안 개선을 위한 각서 발표 (22.01)
국방부 제로트러스트 참조 아키텍처 2.0 발표 (22.07)
국방부 제로트러스트 전략 발표 (22.11) - 목표 수준 (Target Level ZT, ~2027년) - 고급 (Advanced ZT, ~2032년)
국방부 제로트러스트 역량 실행 로드맵 발표 (22.11)
NSA, 사용자 핵심요소를 통한 제로트러스트 성숙도 개선 (23.04)



02. 미 연방정부 제로트러스트 도입 전략

미 국방부 제로트러스트 전략



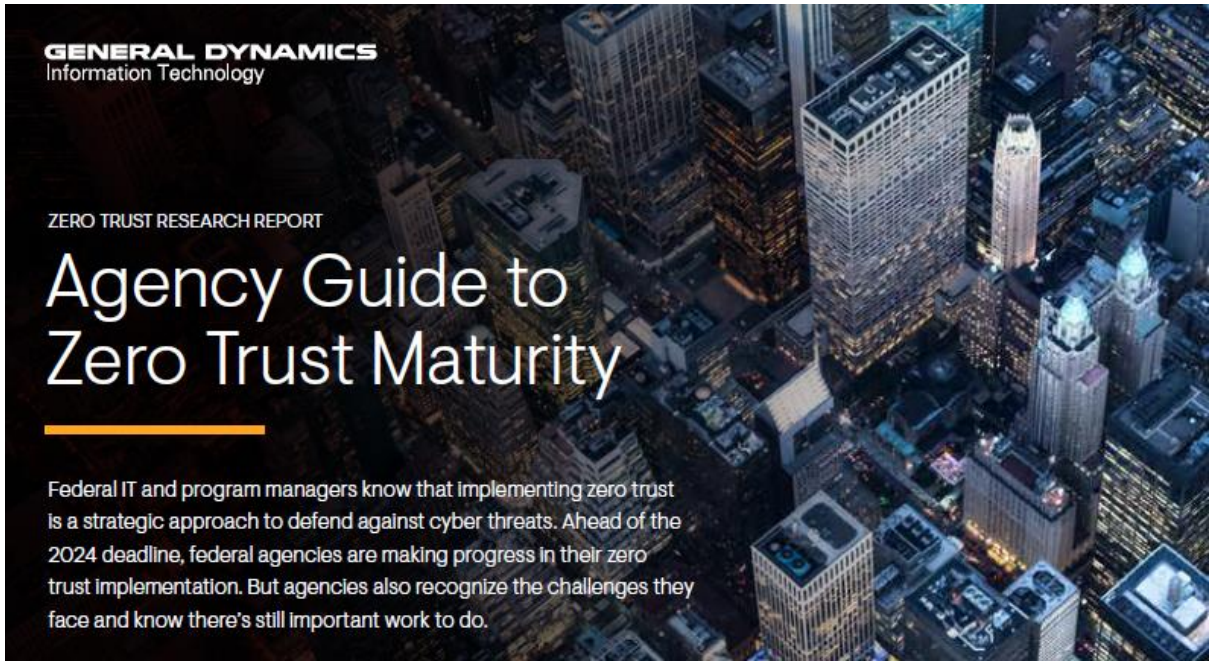
Target Activities:	91
Advanced Activities:	61
Total Activities:	152

Note: ZT Activities are grouped as either Target or Advanced.

Version 1.0 As of 10/04/2022

02. 미 연방정부 제로트러스트 도입 전략

제로트러스트 성숙도에 대한 기관 가이드



연방정부에 근무중인 IT 의사결정권자 300명에 대한 설문조사

DEFENSE AGENCIES

40%

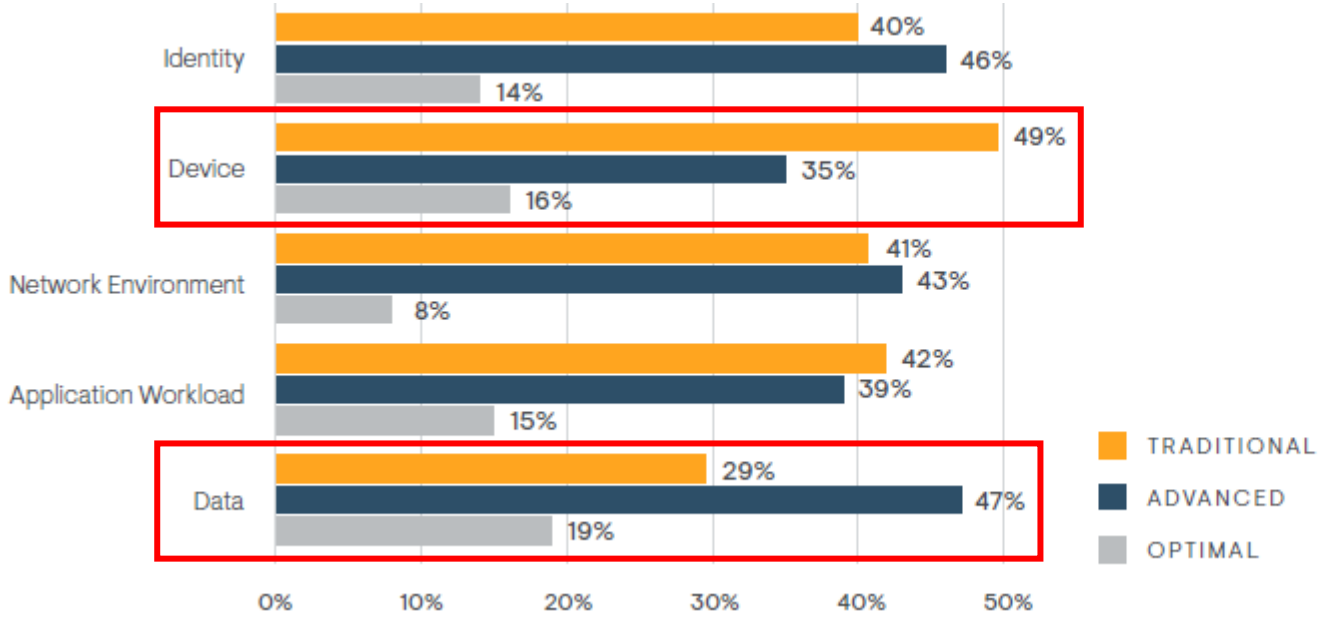
FEDERAL CIVILIAN AGENCIES

60%

02. 미 연방정부 제로트러스트 도입 전략

제로트러스트 성숙도에 대한 기관 가이드

CISA 제로트러스트 성숙도 모델의 5개 핵심 요소



DATA PILLAR

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

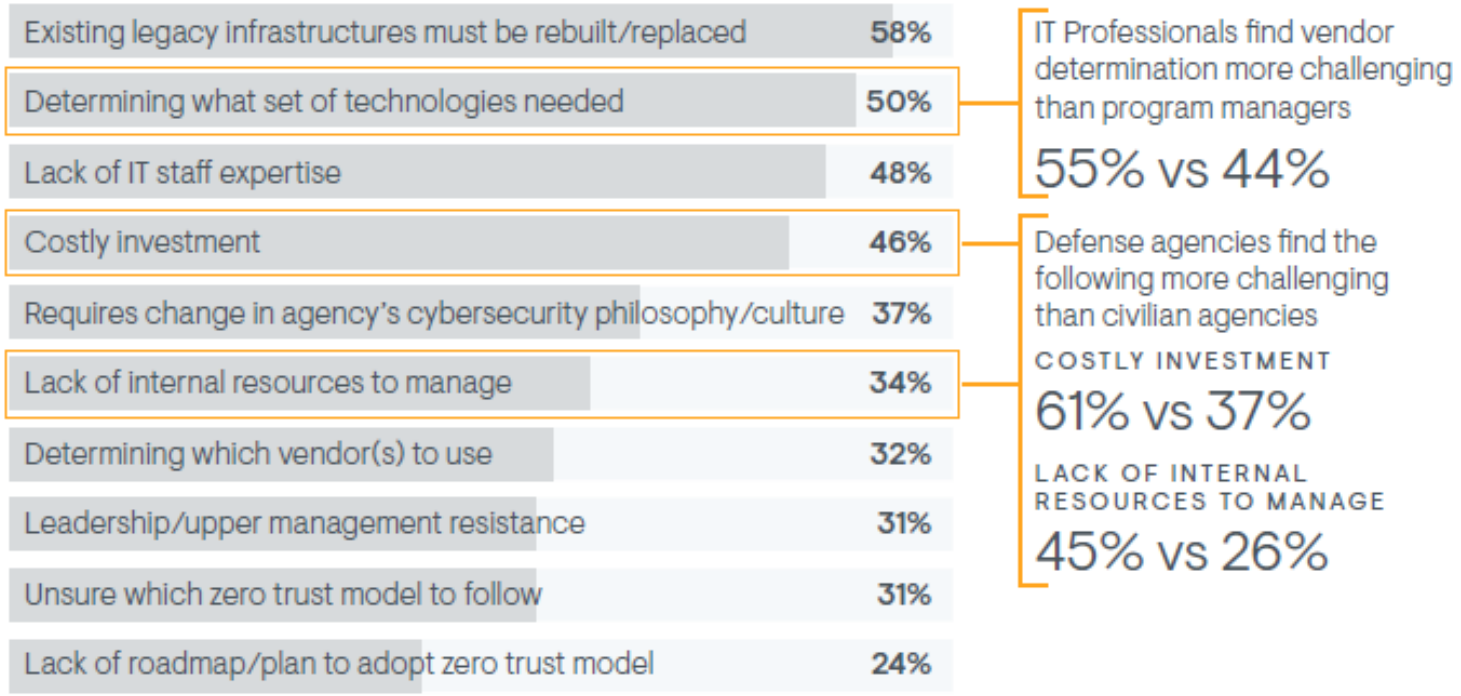
34% vs 23%

미 연방정부 IT의사결정권자들은 제로트러스트 관점에서 가장 성숙도가 낮은 핵심요소로 "단말"을 언급

02. 미 연방정부 제로트러스트 도입 전략

제로트러스트 성숙도에 대한 기관 가이드

제로트러스트 구현에서의 도전 사항

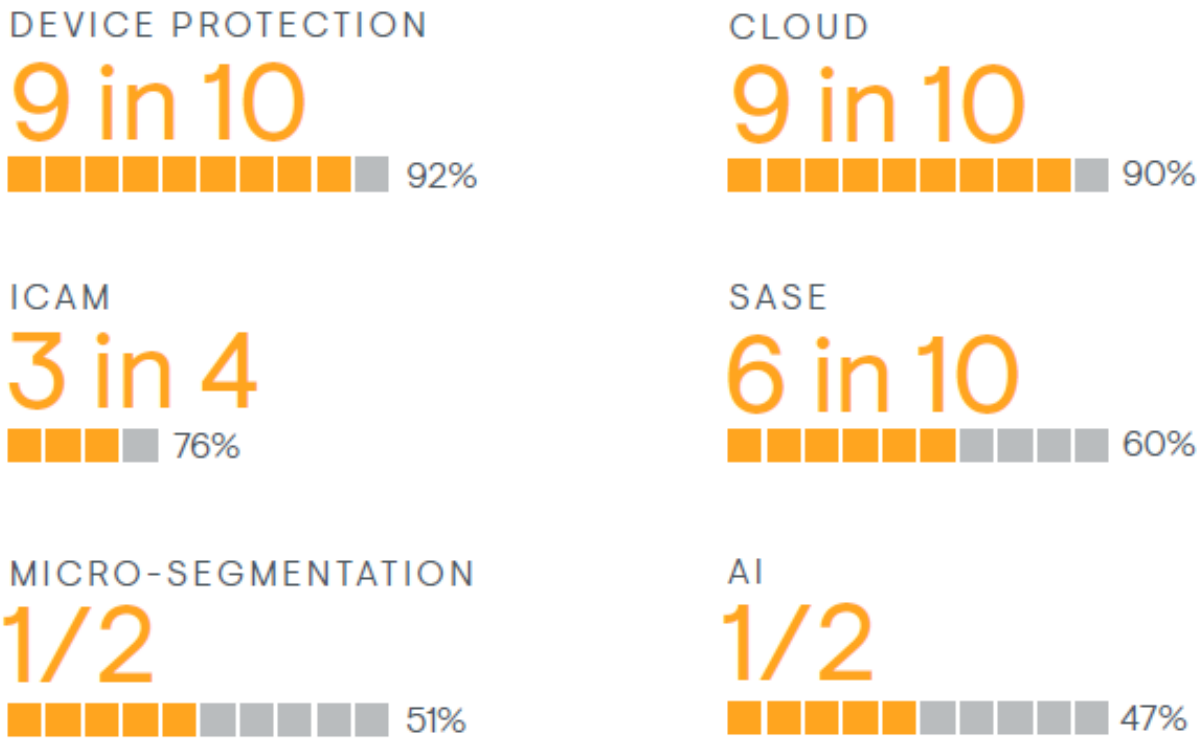


1. 현재의 레거시 인프라 재구현/교체 필요
2. 어떤 기술 집합이 필요한지 결정
3. IT 스태프 전문성 부족
4. 투자 비용
5. 기관 사이버 철학/문화에 대한 변화 요구
6. 내부 리소스 관리 부재
7. 어떤 기업 제품을 사용할지 결정
8. 상위 관리자의 저항
9. 어떤 제로트러스트 모델을 따를지 불확실
10. 제로트러스트 모델 채택을 위한 로드맵/계획 부재

02. 미 연방정부 제로트러스트 도입 전략

제로트러스트 성숙도에 대한 기관 가이드

제로트러스트 투자 우선 순위



02. 미 연방정부 제로트러스트 도입 전략

제로트러스트 성숙도에 대한 기관 가이드

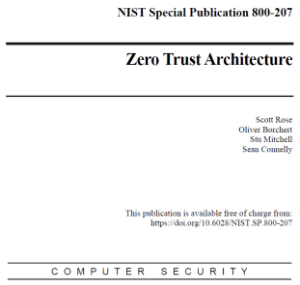
☑ 개념 정립	제로트러스트는 도대체 무엇인가요?
☑ 도입 효과	제로트러스트는 왜 도입해야 하나요?
☑ 도입 방법	도입 기업·기관은 무엇을, 어떻게 도입해야 하나요?

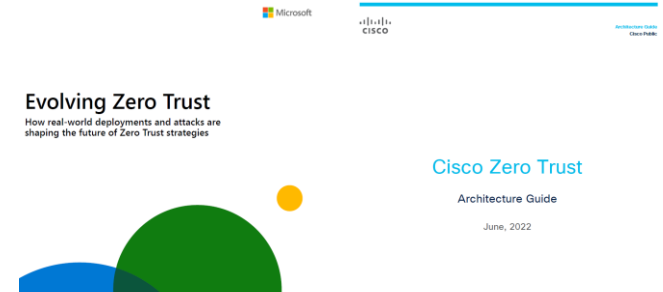
제로트러스트에 대한 공통된 이해 필요

02. 미 연방정부 제로트러스트 도입 전략

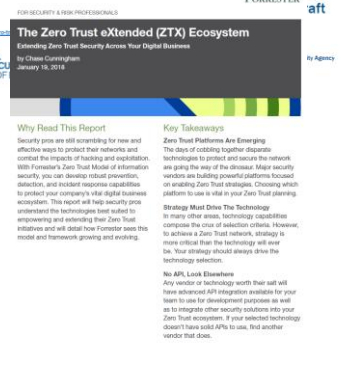
제로트러스트 도입에 대한 어려움

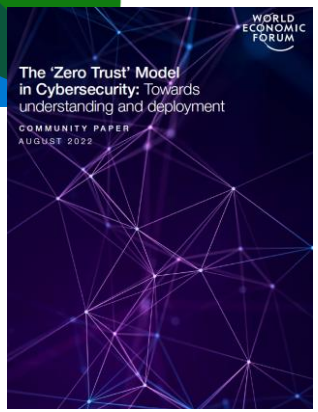
수많은 제로트러스트 가이드라인, 참조 아키텍처, 전략 관련 문서들





Zero Trust Cybersecurity
Current Trends
April 18, 2019





03. 제로트러스트 가이드라인 1.0

제로트러스트 국내 도입을 위한 노력 - 한국제로트러스트포럼 출범 ('22.10.26)

03. 제로트러스트 가이드라인 1.0

제로트러스트 국내 도입을 위한 노력 - 한국제로트러스트포럼 출범 ('22.10.26)

정책·제도 분과 미션

- 국내 디지털 전환 관점에서

  1) 공공·민간 제로트러스트 도입 전략 수립 지원 및
  2) 국내 기업 경쟁력 강화를 위한

  제로트러스트 아키텍처 **가이드라인·정책 개발 및 표준화**

01 제로트러스트 가이드라인 개발 (~'23년 초)

- **제로트러스트 가이드라인** (전체본, 요약본) **발간 ('23.07)**

03. 제로트러스트 가이드라인 1.0

제로트러스트 국내 도입을 위한 노력 - 한국제로트러스트포럼 출범 ('22.10.26)

02 제로트러스트 도입·확산을 위한 구체적인 지침서 추가 개발 ('23년~)

- 공공·민간을 위한 제로트러스트 성숙도 수준 평가(Assessment) 모델 및 방법 개발
- 디지털 정부 제로트러스트 도입을 위한 보안요구사항 및 전환 가이드라인 연구
- 특정 분야별 제로트러스트 도입 전략·로드맵 구성

03 산업·기술 분과 협력을 통한 추가 정책·제도 발굴

- 제로트러스트 정책, 기술 및 산업 동향 공유
- 제로트러스트 유스케이스 구체화 및 정책·실증 과제 발굴, 구현 지침 검토 등 역할 분담

04 제로트러스트 표준화 아이템 발굴

- 제로트러스트 전환 가속화, 산업 활성화 등을 위한 가이드라인 등 표준화
- ISO/ITU-T 등 국제 표준화 단체의 관련 표준화 동향 검토 및 제로트러스트 표준화시 적극 참여

03. 제로트러스트 가이드라인 1.0

제로트러스트 가이드라인 1.0

03. 제로트러스트 가이드라인 1.0

제로트러스트 가이드라인 1.0

발간목적

국내 정부·공공, 기업 관계자 등이 제로트러스트 아키텍처의 개념을 빠르고 쉽게 이해하여

향후 국내 정보통신 환경에 적합한 제로트러스트 보안체계를 도입할 수 있도록 지원하기 위함

요약본

- 일반인들부터 전문가들까지 폭넓은 대상층
- 의사 결정 과정에 포함된 정책 결정자, 기업의 경영진 및 임직원, 일반인의 제로트러스트 이해와 인식

전체본

- 보안 전략수립 책임자 및 실무자
- 조직내 사이버보안 계획 수립, 운영 등을 담당하는 보안 담당자의 제로트러스트 전략 수립에 도움

03. 제로트러스트 가이드라인 1.0

제로트러스트 가이드라인 1.0

발간원칙

① 미국을 중심으로 논의되어 온 제로트러스트의 배경·기본 원리 등은 국가별로 다르지 않으므로 NIST 문서 등을 최대한 참고하였으며, 기본 철학을 유지

② 국내 환경을 고려하여 핵심 요소(시스템) 및 도입 참조모델(원격근무 및 망분리) 추가

③ 도입하고자 하는 기업 및 정부, 공공기관에 따라 네트워크 구조, 조직내 정책, 규정이 모두 다르므로, 이들을 모두 아우를 수 있도록 상위 수준에서 기술

④ 의사 결정 과정에 참여하는 비전문가, 제로트러스트의 철학과 개념 이해를 필요로 하는 조직내 모든 구성원들을 배려하여 상세한 기술보다는 더 쉽게 개념을 이해할 수 있도록 문서 작성

03. 제로트러스트 가이드라인 1.0

제로트러스트 가이드라인 1.0 (전체본)

03. 제로트러스트 가이드라인 1.0

제로트러스트 가이드라인 1.0 - 제로트러스트 핵심 요소 및 교차 기능

결론

제로트러스트 도입 고려 사항

- 제로트러스트는 신뢰를 배제하고, 강력한 인증, 최소 권한, 컨텍스트에 따르는 동적 접근 제어 등을 통한 **위험 최소화 및 높은 보안성**을 확보하려는 **보안 철학**
- **고수준의 제로트러스트 철학**을 기술적으로 도입·구현하는 것은 **(10년 이상의) 오랜 시간**이 걸릴 수 있으며, **기업 상황과 성숙도 수준에 따르는 전략 및 중간·최종 목표 설정 필요**
- ZT는 **전사적으로 도입되어야 할 보안 철학**이며, 일부 원칙만을 강조하거나 특정 보안 기술·솔루션 도입을 통해 달성하는 것이 불가능

제로트러스트 가이드라인 1.0 공개

- “제로트러스트”라는 새로운 보안 개념을 **국내에 도입하기 위한 첫 삽을 뜨는 과정**
- **가이드라인 V1.0에 대한 의견 수렴, 실증사업 결과 반영** 등을 통하여 지속적으로 업데이트 계획
- 특정 분야별 제로트러스트 도입 전략·로드맵·구현 참조 모델 등 구체화 예정

감사합니다.

이석준 교수, 가천대학교
junny@gachon.ac.kr