보안의 기본 - 제로트러스트
정보보호의 현재와 미래 컨퍼런스 (정보보호의 날)

가천대학교 스마트보안학과

이석준 교수 (junny@gachon.ac.kr)

2025년 7월 9일

발표자 소개

이석준 (가천대학교 교수, junny@gachon.ac.kr)

- 전공분야 : 제로트러스트, 양자보안, 암호 프로토콜 및 안전성 분석 등

- 주요경력 :
  - 서울대학교 컴퓨터공학과 학사·석사 (1994~2000)
  - 한국과학기술원 전산학부 박사 (2010~2019)
  - ETRI 정보보호연구본부 책임연구원/PL (2000~2022)
  - **현 가천대학교 IT융합대학 스마트보안학과 부교수 (2022~현재)**
  - **현 한국제로트러스트포럼 정책제도분과 분과장 (2022~현재)**
  - **현 한국정보보호학회 제로트러스트연구회 위원장 (2024~현재)**
  - 현 미래기술보안포럼 전문위원 (2022~현재)
  - 현 클라우드보안인증위원회 인증위원 (2024~현재)
  - 현 금융위원회 소프트웨어사업 과업심의위원회 위원 (2025~현재)
  - 현 한국정보보호학회·한국스마트미디어학회·한국차세대컴퓨팅학회 이사

INDEX

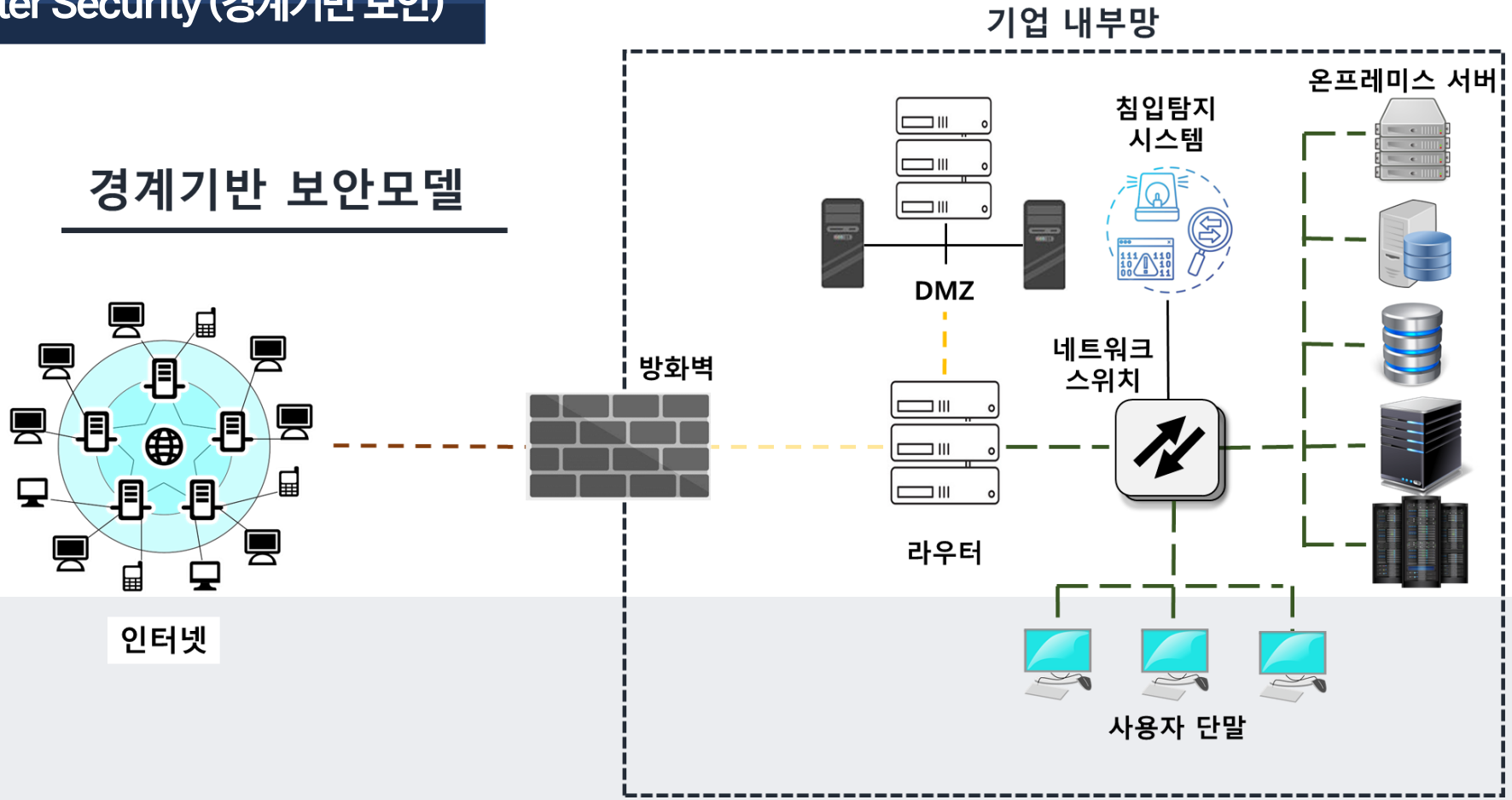
1. 신뢰의 제거, 제로트러스트의 시작
2. 제로트러스트에 대한 명확한 이해
3. 보안 프레임워크 vs. 보안 아키텍처
4. Next for Zero Trust: From IT to Everything
5. 결론

1. 신뢰의 제거, 제로트러스트의 시작

기업 네트워크 환경의 변화

Perimeter Security (경계기반 보안)

경계기반 보안모델



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

문제 1. 흐려지는 경계

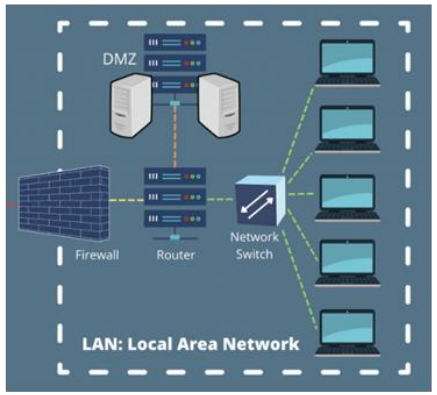
점점 복잡해지는 기업망 (코로나19 이후 가속화)

재택 근무

원격 근무

협력업체 직원

모바일 기기의 확산



클라우드 서비스

각종 IoT 기기

지사 운영

WFA (Work from Anywhere)

기업 리소스 위치 다변화

문제 2. 경계기반 보안을 뚫는 해킹

랜섬웨어 공격으로 인한 국가 안보·인프라 위협

- 콜로니얼 파이프라인, 체인지 헬스케어 등 국가 안보 및 핵심 인프라에 연관된 기관·기업에 대한 공격 사례 증가
- 랜섬웨어 감염으로 인한 인프라 서비스 중단, 대량의 민감 정보 유출 등 피해

문제 2. 경계기반 보안을 뚫는 해킹

랩서스 (LAPSUS$) 해킹 사례

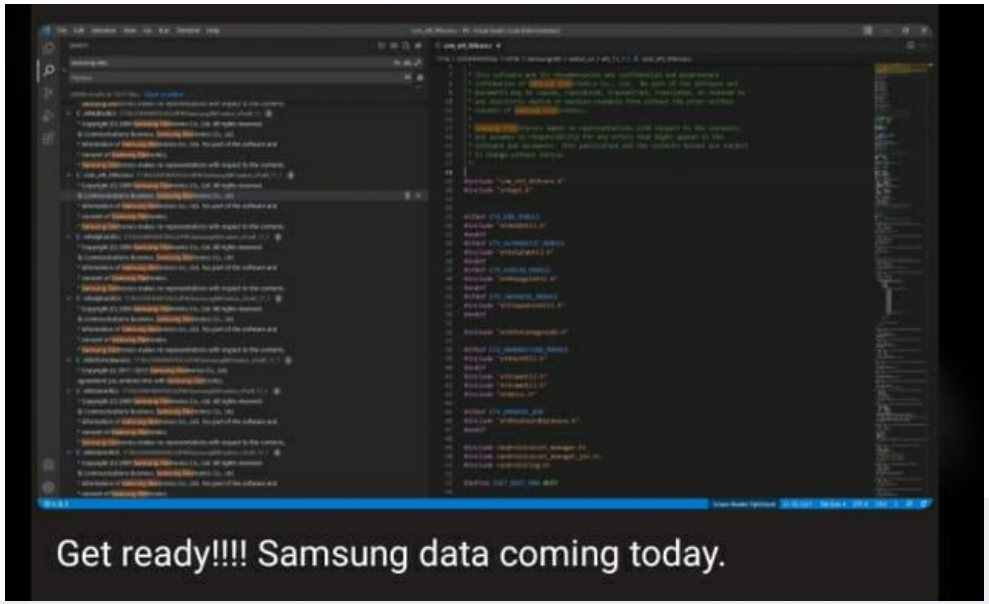
삼성·MS 뚫은 해커집단 랩서스, 공격수법 드러났다

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

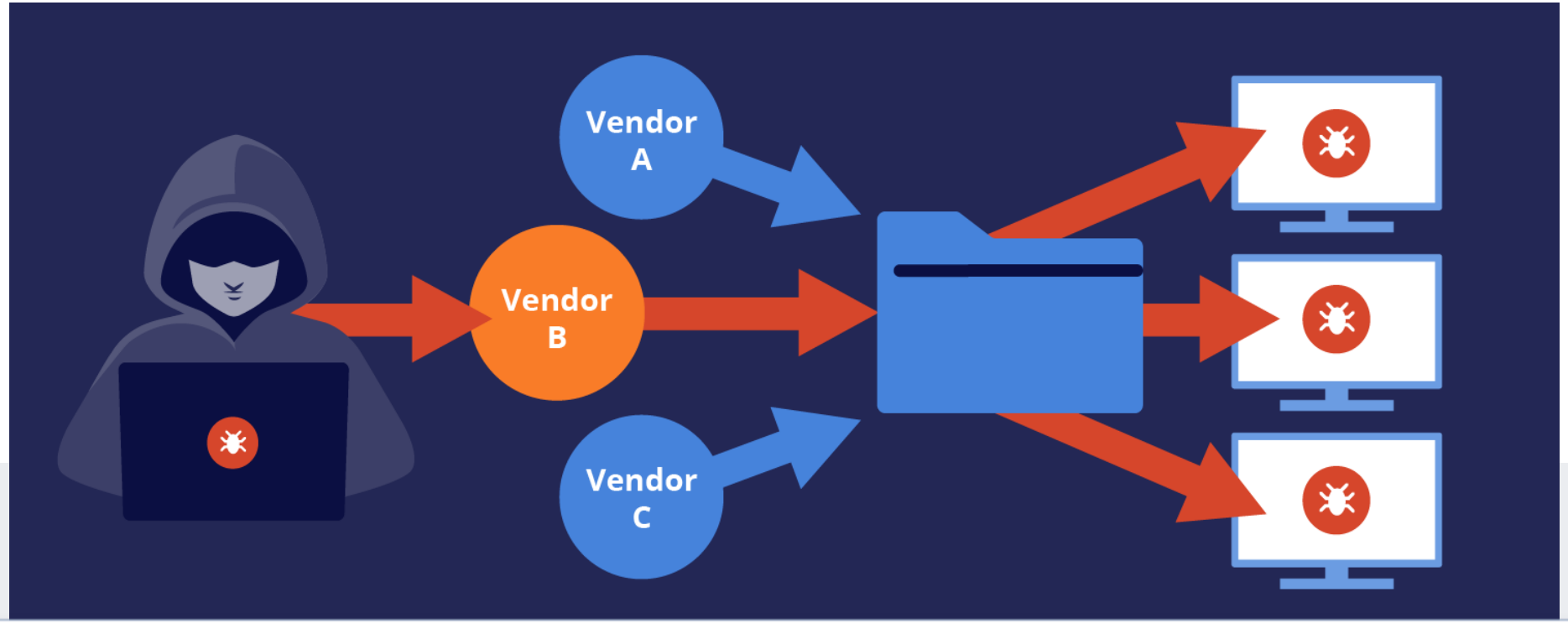
마이크로소프트가 최근 몇 달 사이 글로벌 IT 기업 여러 곳을 해킹해 악명을 높인 해커집단 '랩서스(Lapsus$)'를 쫓고 있다. 마이크로소프트도 랩서스에 뚫려 검색 엔진 빙·인공지능 비서 코타나 소스코드를 탈취당하는 수모를 겪은 만큼, 설욕을 위해 단단히 벼르고 있는 모양새다.



- 사회공학적 방식(직원 계정 탈취, MFA 우회 등), SIM 스와핑, 내부자 포섭 등 다양한 침투 방식 활용
- Microsoft, NVIDIA, Samsung, Okta, Ubisoft 등 **다수의 글로벌 대기업 소스 코드 유출 등 피해**
- 소스코드 유출, 내부 시스템 접근, 고객사 데이터 노출 등으로 인하여 다수 피해 발생

문제 2. 경계기반 보안을 뚫는 해킹

Solarwinds 공급망 공격 사례



- 공급망 공격(Supply Chain Attack): SolarWinds 사의 소프트웨어 업데이트에 악성코드(SUNBURST) 삽입
- SolarWinds 사의 Orion 소프트웨어 사용 고객(미 국방부, 재무부, 국토안보부, Microsoft 등) 약 18,000개 기관 감염
- 악성 코드가 신뢰할 수 있는 코드에 포함되어, 수개월간 내부 시스템 장악

문제 3. 가시성 확보, 분석의 어려움

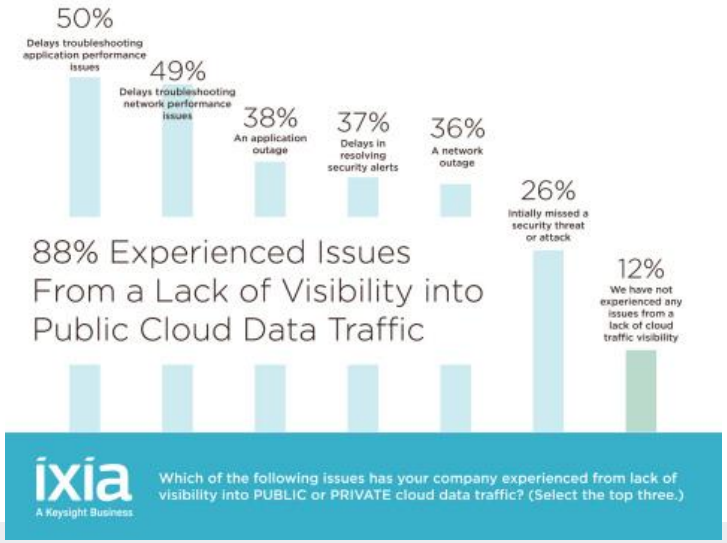
사용자·기기 로그 및 행위, 네트워크 트래픽 가시성 확보의 어려움

>80%

of organizations report employee **abuse or misuse** of business app access in the past 12 months

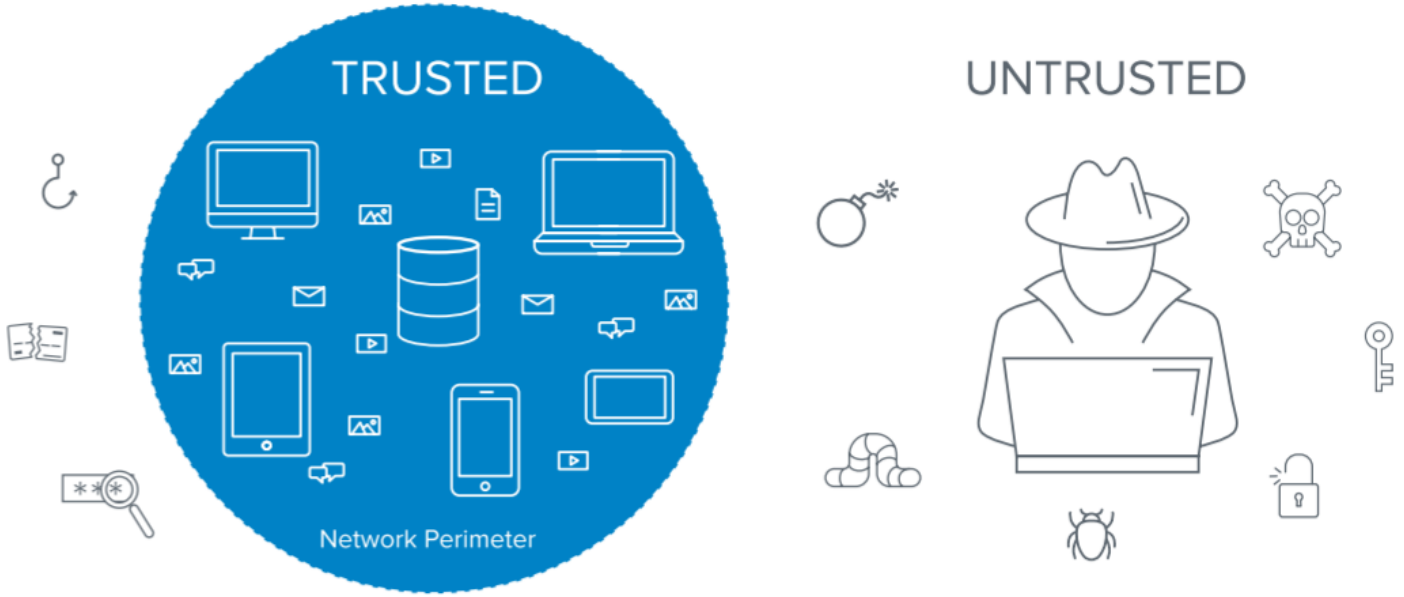
Yet **NEARLY ½**

lack visibility into user logs & activity, making it difficult to pinpoint risky behavior



- 원격 접근, 클라우드 서비스 등 감시 영역이 지속적으로 확장되고 있음
- 사용자 및 단말, 응용의 이상 행위 추적의 어려움: 대량의 분석 대상 로그 존재
- 악성 행위에 대한 명확한 정의가 없고, 고도화된 공격 추적을 위한 다양한 각도에서의 연관 분석 어려움

경계기반 보안의 약점 – 신뢰의 위험성

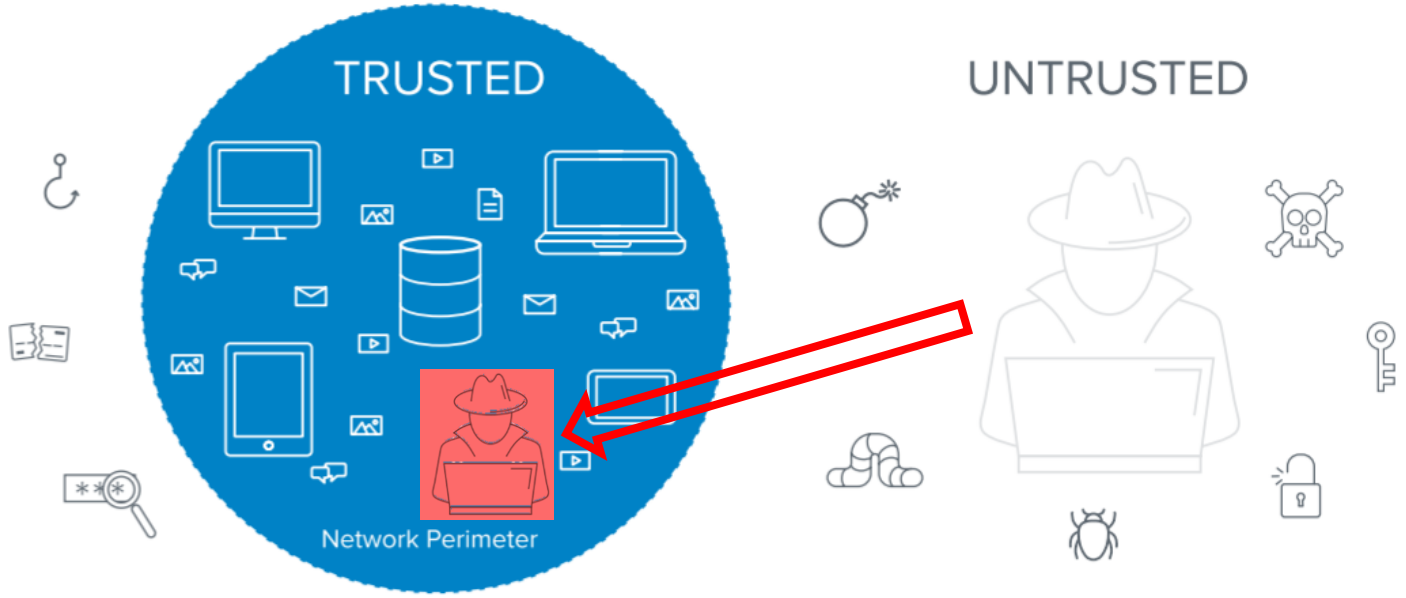


보안 경계를 둔다는 것:

내부자에게 더 높은 신뢰 부여

내부 네트워크 방어·가시성의 우선 순위가 낮아짐

경계기반 보안의 약점 – 신뢰의 위험성



사이버 공격의 1차 목표

공격자: 내부망에 침투하자!

신뢰(Trust)를 악용하는 해킹, 의심에서 출발하는 대응

경계기반 보안: 보안에 투자하지 않는 회사

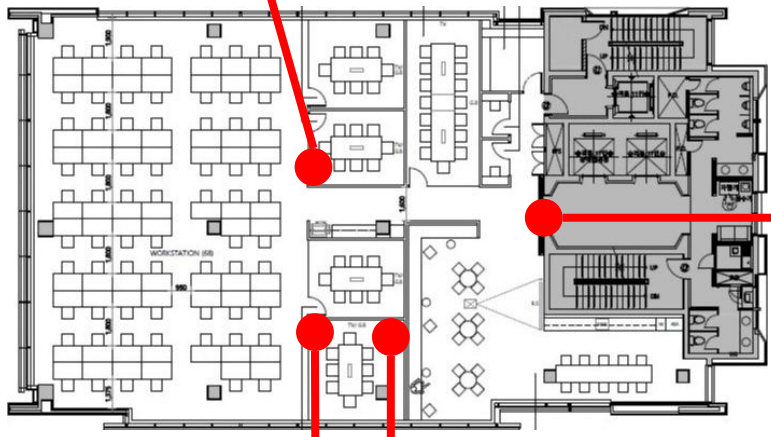
회사 출입문에서만 진입 통제

출입문 진입 후 자유로운 이동 가능
(출입 허가된 사람에게 암묵적인 신뢰 부여)

회사 내부에서 다양한 공격 가능
(도둑질, 도청, 테러 등)

제로트러스트: 강력한 보안 구조를 가진 회사

CCTV에 의한
지속적인 모니터링



필요시 외부 금고
이용 (Cloud)

사원증/방문증 등
강력한 신원 인증

사무실별 출입통제
(Micro-Segmentation)

중요 자산 보관용 금고
(Micro-Segmentation)

출입문 진입 이후에도 중요한 자산 접근 불가
(내부 진입자에 대한 지속적인 모니터링 및 접근 권한 검증)

신뢰(Trust)를 악용하는 해킹, 의심에서 출발하는 대응

보안 패러다임의 변화: 제로트러스트

FORRESTER® Making Leaders Successful Every Day

September 14, 2010 | Updated: September 17, 2010

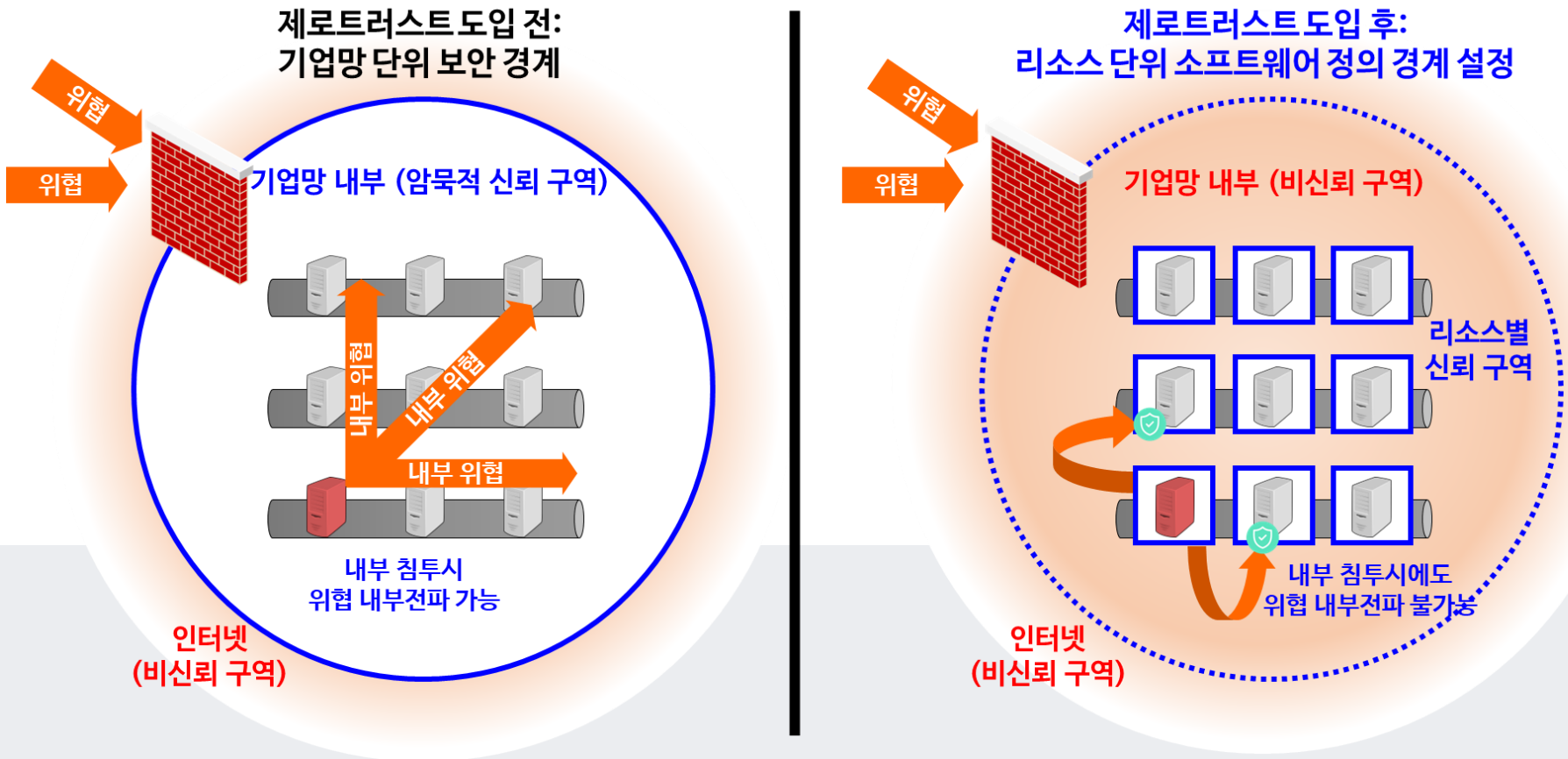
No More Chewy Centers: Introducing The Zero Trust Model Of Information Security

by John Kindervag
for Security & Risk Professionals

Never Trust,

Always Verify

제로트러스트의 바이블: NIST SP 800-207 (2020년)



A. Kerman(NIST)의 그림 재구성

제로트러스트의 바이블: NIST SP 800-207 (2020년)

제로트러스트의 7가지 원리

원리	세부 내용
① 모든 데이터 소스와 컴퓨팅 서비스는 리소스로 간주	‣ 네트워크는 데이터를 수집기/스토리지로 전송하는 소형 기기, SaaS 및 다른 기능을 포함할 수 있으며, 개인 소유 단말기가 사내 리소스에 접근할 수 있다면 이 역시 리소스로 분류할 수 있음
② 네트워크 위치에 관계없이 모든 통신 보호	‣ 디바이스가 기업 네트워크 내부에 있다고 해서 신뢰를 보장하지 않으며, 모든 통신의 기밀성과 무결성을 보호해야 함
③ 기업 리소스에 대한 접근을 세션 단위로 승인	‣ 작업을 완료하는데 필요한 최소한의 방식으로 접근을 허가하며, 각 세션에 따라 달리 검토하여 승인해야 함
④ 동적 정책으로 리소스에 대한 접근 결정	‣ 동적 정책에는 클라이언트 아이덴티티, 어플리케이션, 요청을 보낸 자산 상태, 행동 및 환경 속성 등이 포함되며, 동적으로 리소스 접근 결정 필요
⑤ 모든 자산의 무결성 및 보안 상태 감시·조치	‣ 기본적으로 자산을 신뢰하지 않으며, 리소스에 대한 접근 요청을 판단할 때 자산 상태 감시, 필요에 따라 패치 등 보완조치를 위한 모니터링
⑥ 모든 리소스의 인증/인가를 강력하게 점검 후 허용	‣ 모든 리소스에 대해 접근 획득→위협 스캔 및 평가→조정→지속적인 신뢰 재평가라는 일정한 사이클로, ICAM, 자산 관리 시스템 도입 및 다중 인증 사용을 권장함
⑦ 자산, 네트워크, 인프라 등 현 상태에 대한 정보 수집	‣ 자산의 보안 상태, 네트워크 트래픽, 접근 요청과 관련된 데이터를 수집하고 처리하여 획득한 지식을 보안 정책을 개선하기 위해 사용해야 함

2. 제로트러스트에 대한 명확한 이해

제로트러스트 고려 사항

제로트러스트에 대한 명확한 이해

공통 개념

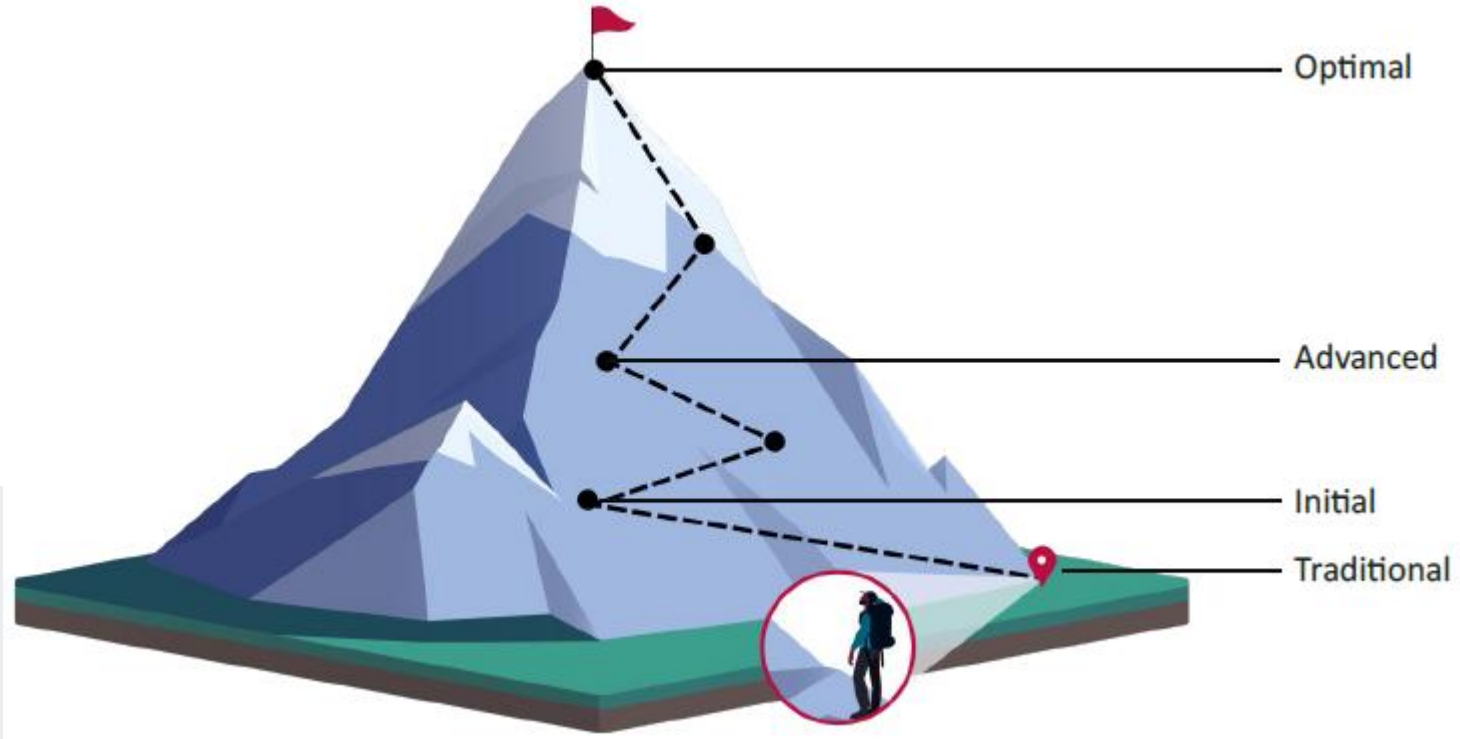
- 기업망 내부 네트워크는 이미 침투 당했을 가능성
- 정확한 (신뢰도 평가에 기반한, 지속적인) 접근 제어
- 보안 개념, 패러다임, 아이디어의 집합

용어는 제로트러스트(Zero Trust)이지만…

모든 신뢰를 제거하자	✗	✓ 정확하게 신뢰도를 평가하자
모든 경계를 제거하자	✗	✓ 경계를 리소스 단위로 세분화하자

제로트러스트 고려 사항

제로트러스트에 대한 명확한 이해



제로트러스트 고려 사항

기술·솔루션 중심의 제로트러스트 구현은 무엇이 문제인가?

☑ 철학의 부재: 비신뢰를 가장한 기존 신뢰기반 모델	예) ZTNA·SDP 도입 → 초기 인증 후 미감시/부적절한 권한 부여 → 기존 VPN과 크게 다르지 않음
☑ 정책·운영 구조의 미개편: 최소권한·세분화 미적용	접근제어 정책, 최소권한 부여정책 등이 충분히 조직을 고려하지 않음 → 과도한 권한 부여, 측면 이동 허용 가능성
☑ 사일로화 보안 아키텍처	각 네트워크·응용·데이터 관리 주체가 제각각 ZT 솔루션을 도입하는 경우 → 조직 전체 흐름을 고려하지 않은 단편적인 보안 구조로 통합 보안 관리 실패
	제로트러스트는 단순히 '접근을 막는 것', '공격을 차단하는 것'이 아님 → 모든 행위 감시 및 검증 필요 → 연동 실패시 전사적 가시성 확보 실패
☑ 변하지 않는 조직 문화	예) 보안 구조의 변화로 인한 업무 환경의 변화를 받아들이지 않음 → 부서간 접근 권한 요청 → 관리자 재량의 일괄 허용 → 최소 권한 정책 무력화
	공격 차단 중심의 보안 정책 및 처벌·징계 중심의 사고 대응 문화 유지 → 침투 발생시 은폐, 미신고, 소극적 대응 등으로 인한 피해 누적

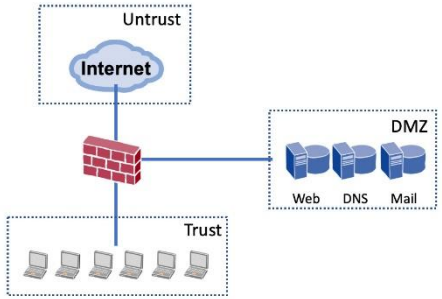
제로트러스트 고려 사항

제로트러스트에 대한 명확한 이해

착하게 사는 방식 1 (Legacy)

착하게 사는 방식 2 (ZR:제로종교)

보안 방식 1 (Legacy)



보안 방식 2 (ZT:제로트러스트)

제로트러스트 고려 사항

제로트러스트에 대한 명확한 이해

교회를 다니면, ZR을 달성할 수 없는가?	NO
쓰레기 줍고, 불우이웃을 돕고, 친절하면 ZR인가?	NO

ZR(Zero Religion)이라는 것은 선언적인 의미이므로, '교회에 다닌다/안 다닌다'만으로 ZR을 평가할 수 없음
'착하게 산다'라는 것은 몇 가지 행위가 아닌 종합적인 평가가 필요

망분리 기술을 사용하면, 제로트러스트 철학을 달성할 수 없는가?	NO
SDP, EDR, SASE 등 솔루션을 모두 갖추면 제로트러스트 철학을 달성한 것인가?	NO

ZT(Zero Trust)이라는 것은 선언적인 의미이므로, '망분리/비망분리'만으로 ZT를 평가할 수 없음
'적극적인 보안'이라는 것은 몇 가지 솔루션의 도입 여부가 아닌 종합적인 평가가 필요

제로트러스트 고려 사항

제로트러스트에 대한 명확한 이해

☑ 제로트러스트	보안에 관한 '철학'과 '방향성' = '최선을 다해' 착하게 살자 (종교, 도덕과 같은 행동 지침)
☑ 보안 통제	조직에 대해 규정된 보안 장치 또는 대책 = 지키지 않으면 처벌을 받게 될꺼야 (법규, 규정 등에서 파생된 다양한 요구사항 해결)

제로트러스트 = 도덕

東亞日報

간통, 이제 법으로는 무죄

헌재, 7대2로 처벌 위헌 결정… 간통죄 62년만에 폐지

"性的 자기결정권 침해… 혼인 유지, 개인 자유에 맡겨야"

보안 통제 = 법규, 규정

제로트러스트 고려 사항

제로트러스트에 대한 명확한 이해

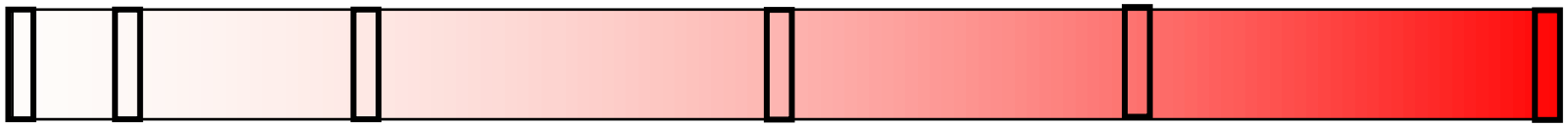
법만 지켜선 부족하며, 개인의 자율 의지를 통한 도덕적 행동이 중요	• 보안 통제를 모두 지킨다고 해서 진정한 보안을 달성하는 것이 아님 • 조직 전체가 “신뢰하지 않고 검증하는 문화”를 통해, 높은 수준의 보안 가능
법은 최소한, 도덕은 이상향	• 보안 프레임워크는 최소 기준이며, 제로트러스트는 그 이상을 추구 • 예) 사용자 행위 분석, 지속 인증, 맥락 기반 접근통제 등은 규정보다 한 걸음 더 나아간 실천
도덕은 없는데 법만 있는 경우 → 규제 회피, 꼼수, 내부 위협 유발	• 제로트러스트 철학 없이 솔루션과 규정으로만 보안을 달성하려 할 경우, 의도적 우회, 예외 남용, 신뢰 모델 왜곡 등 보안 수준을 낮추는 사례 발생 가능

“제로트러스트는 조직의 보안 도덕성(Ethical Security Posture)을 시험하는 기준이다. 보안 프레임워크는 그 도덕성을 강제하는 법률과 절차에 가깝다.”

제로트러스트에 대한 오해와 이해

우리 조직은 제로트러스트를 도입해야 하는가? (그렇다면 레거시 기술은 모두 걷어내야 하는가?)

아래 막대그래프에서, 어디서부터 붉은색이라고 할 수 있을까?



- 제로트러스트는 특정 보안 기술이 아닌, 보안에 관한 '철학'과 '방향성'을 의미
- 과거에 활용해오던 레거시 기술 역시 기본적으로는 제로트러스트의 초보적인 철학이 담겨 있을 수 있으며, 성숙도가 낮을 뿐 절대 제로트러스트 기술이 아니라고 할 수 없음
- '망분리'와 같은 특정 기술 하나만으로, 기업·기관 네트워크의 제로트러스트 방향성과 성숙도를 결정할 수 없음

제로트러스트에 대한 오해와 이해

우리 조직은 제로트러스트를 도입해야 하는가? (그렇다면 레거시 기술은 모두 걷어내야 하는가?)

3. 보안 프레임워크 vs. 보안 아키텍처

보안 프레임워크 vs. 보안 아키텍처

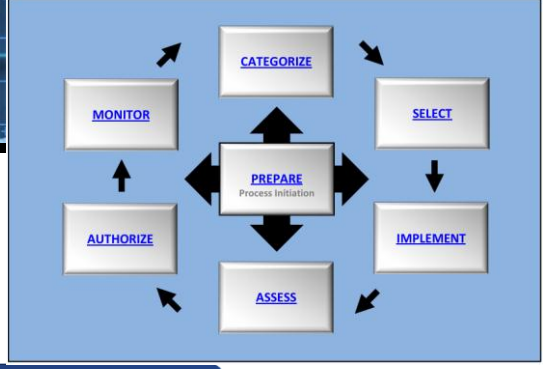
Framework	Architecture
Merriam-Webster's Learner's Dictionary 1. the basic structure of something , a set of ideas or facts that provide support for something 2. a supporting structure, a structural frame Oxford's Dictionary of English 1. an essential supporting structure of a building, vehicle, or object 2. a basic structure underlying a system, concept, or text	Merriam-Webster's Learner's Dictionary 1. the art or science of designing and creating buildings 2. a method or style of building 3. technical the way in which the parts of a computer are organized Oxford's Dictionary of English 1. the art or practice of designing and constructing buildings 2. the style in which a building is designed and constructed, especially with regard to a specific period, place, or culture 3. the complex or carefully designed structure of something
주로, 실행 지침과 절차를 고수준(관리/정책)으로 제공 정책, 프로세스, 역할, 책임, 평가 방법 등을 포함 (무엇을 해야 하는가?)	주로, 시스템 설계 및 기술적 구성을 저수준(기술/구조)으로 제공 컴포넌트, 데이터 흐름, 통신 방식 등 구체적 방법·방법론을 포함 (어떻게 작동하는가?)

보안 프레임워크 vs. 보안 아키텍처

보안 프레임워크 vs. 보안 아키텍처

Framework	Architecture
The framework (CSF) is a risk-based approach to managing cybersecurity risk that provides a common taxonomy and mechanism for organizations to describe current and target states of cybersecurity, identify and prioritize opportunities for improvement, and assess progress. (NIST CSF 1.1) The RMF provides a disciplined, structured, and flexible process for managing security and privacy risk that includes information security categorization; control selection, implementation, and assessment; system and common control authorizations; and continuous monitoring. (NIST SP 800-37, RMF rev2)	Zero trust architecture (ZTA) is an enterprise's cybersecurity plan that utilizes zero trust concepts and encompasses component relationships, workflow planning, and access policies. (NIST SP 800-207)

보안 프레임워크 vs. 보안 아키텍처



RMF(Risk Management Framework)

RMF 의미 및 목적

(제공) 보안 및 개인정보 보호 위험을 관리하기 위한 체계적이고 구조화되며 유연한 프로세스 제공 (정보 보안 분류, 통제 선택, 구현 및 평가, 시스템 및 공통 통제 승인, 지속적인 모니터링)

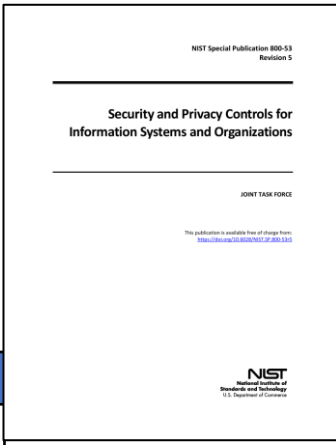
- 조직의 사명과 비즈니스 목표, 고위 경영진이 위험 관리 기능을 통해 수립한 위험 관리 전략과 일치하도록 **시스템 관련 보안 및 개인정보 보호 위험 관리 보장**
- 적절한 위험 대응 전략의 구현을 통해 **개인의 개인정보 보호 및 정보와 정보 시스템의 보안 달성**
- 보안 및 프라이버시 정보의 **일관성, 정보 기반, 지속적인 승인 결정, 상호성, 투명성 및 추적 가능성 지원**
- 보안 및 프라이버시 요구사항, 통제 조치와 **기업 아키텍처, 소프트웨어 개발 생명주기(SDLC) 프로세스, 구매 프로세스, 시스템 공학 프로세스의 통합 지원**
- 연방 기관 내에서 **NIST CSF 구현을 지원**

RMF 7가지 절차

- **준비:** 조직 및 시스템 수준에서 RMF를 실행하기 위해 보안 및 개인정보 위험 관리를 위한 맥락과 우선순위를 설정
- **분류:** 시스템이 처리, 저장, 전송하는 시스템 및 정보를 손실의 영향 분석을 기반으로 분류
- **선택:** 시스템에 대한 초기 제어 항목 선택, 위험 평가를 기반으로 위험을 허용 가능한 수준으로 줄이기 위해 필요한 경우 제어 조정
- **구현:** 통제 조치를 구현하고 시스템 및 그 운영 환경 내에서 통제 조치가 어떻게 적용되는지 설명
- **평가:** 통제 조치가 올바르게 구현되었는지, 의도된 대로 작동하는지, 보안 및 개인정보 보호 요구사항을 충족하는 데 필요한 결과를 생성하는지 평가
- **승인:** 조직의 운영 및 자산, 개인, 다른 조직, 국가에 대한 위험이 수용 가능한 수준임을 판단하여 통제 조치 승인
- **모니터링:** 통제 조치를 지속적으로 모니터링하며, 통제 효과성 평가, 시스템 및 운영 환경의 변경 사항 문서화, 위험 평가 및 영향 분석 수행, 시스템의 보안 및 개인정보 보호 상태 보고를 포함

보안 프레임워크 vs. 보안 아키텍처

NIST SP 800-53 rev5 (Security and Privacy Controls for Information Systems and Organizations

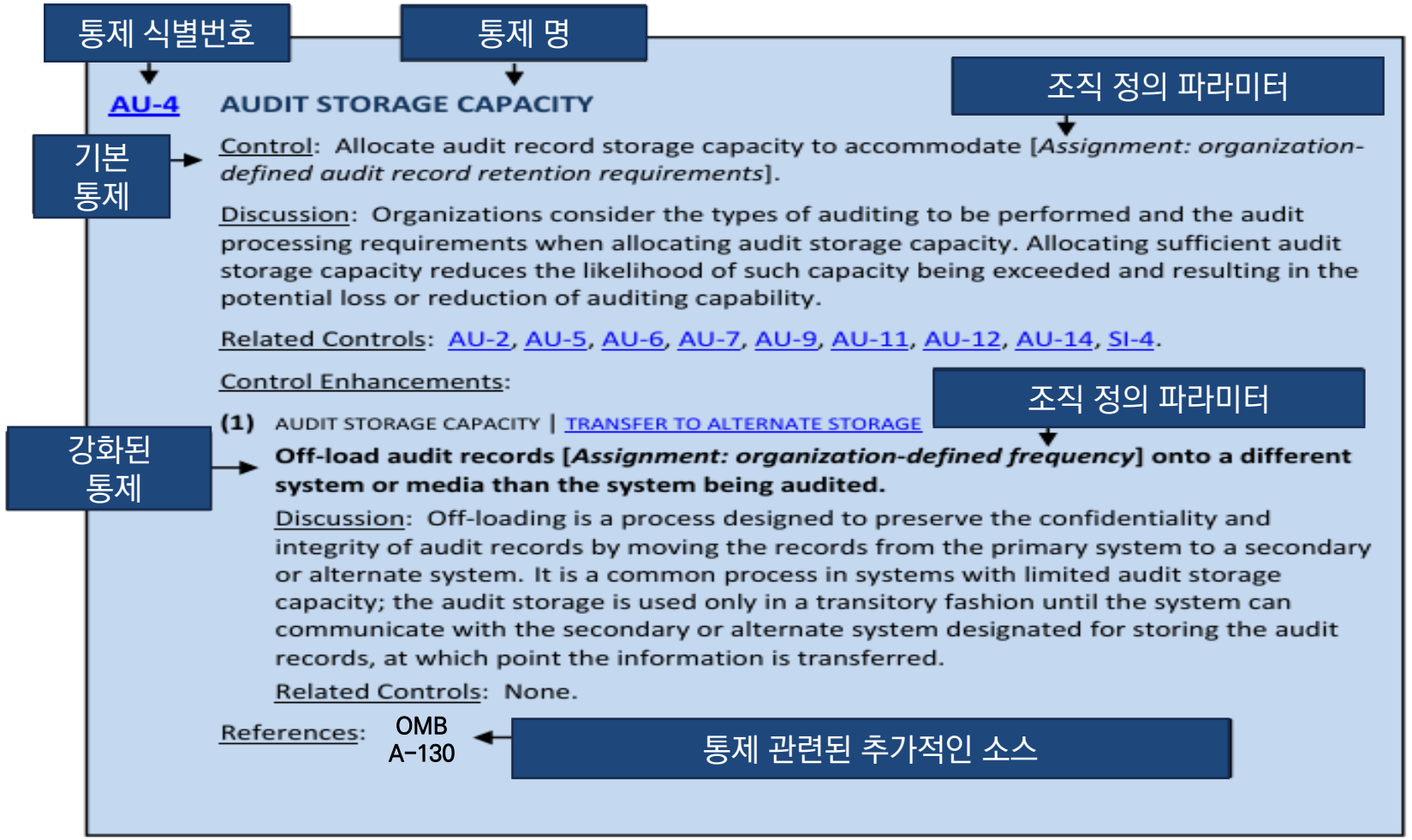


- NIST SP 800-53은 시스템, 조직, 개인을 보호하기 위한 보안 및 개인정보 통제 목록을 제공하며, 위험 관리와 관련 법률 및 규정 준수(연방법, 행정명령, 정책 및 표준 등)를 지원
- 통제항목 패밀리(종류)-20개 / 통제항목 개수-약 1,000개
- FISMA → OMB Circular A-130 → NIST RMF → (Select) NIST SP 800-53

ID	FAMILY	ID	FAMILY
AC	Access Control (25)	**PE**	Physical and Environmental Protection (23)
AT	Awareness and Training (6)	**PL**	Planning (11)
AU	Audit and Accountability (16)	**PM**	Program Management (32)
CA	Assessment, Authorization, and Monitoring (9)	**PS**	Personnel Security (9)
CM	Configuration Management (14)	**PT**	PII Processing and Transparency (8)
CP	Contingency Planning (13)	**RA**	Risk Assessment (10)
IA	Identification and Authentication (12)	**SA**	System and Services Acquisition (23)
IR	Incident Response (10)	**SC**	System and Communications Protection (51)
MA	Maintenance (7)	**SI**	System and Information Integrity (23)
MP	Media Protection (8)	**SR**	Supply Chain Risk Management (12)

보안 프레임워크 vs. 보안 아키텍처

NIST SP 800-53 rev5 (Security and Privacy Controls for Information Systems and Organizations



< NIST SP 800-53 통제항목 상세 설명>

보안 프레임워크 vs. 보안 아키텍처

RMF(Risk Management Framework) vs. ZTA(Zero Trust Architecture)

NIST ZTA와 RMF는 서로 별개의 프레임워크 및 아키텍처지만, 상호보완적으로 작동
즉, ZTA는 RMF 내에서 보안 통제를 구현하고 위험을 줄이기 위한 기술적·철학적 수단으로 활용

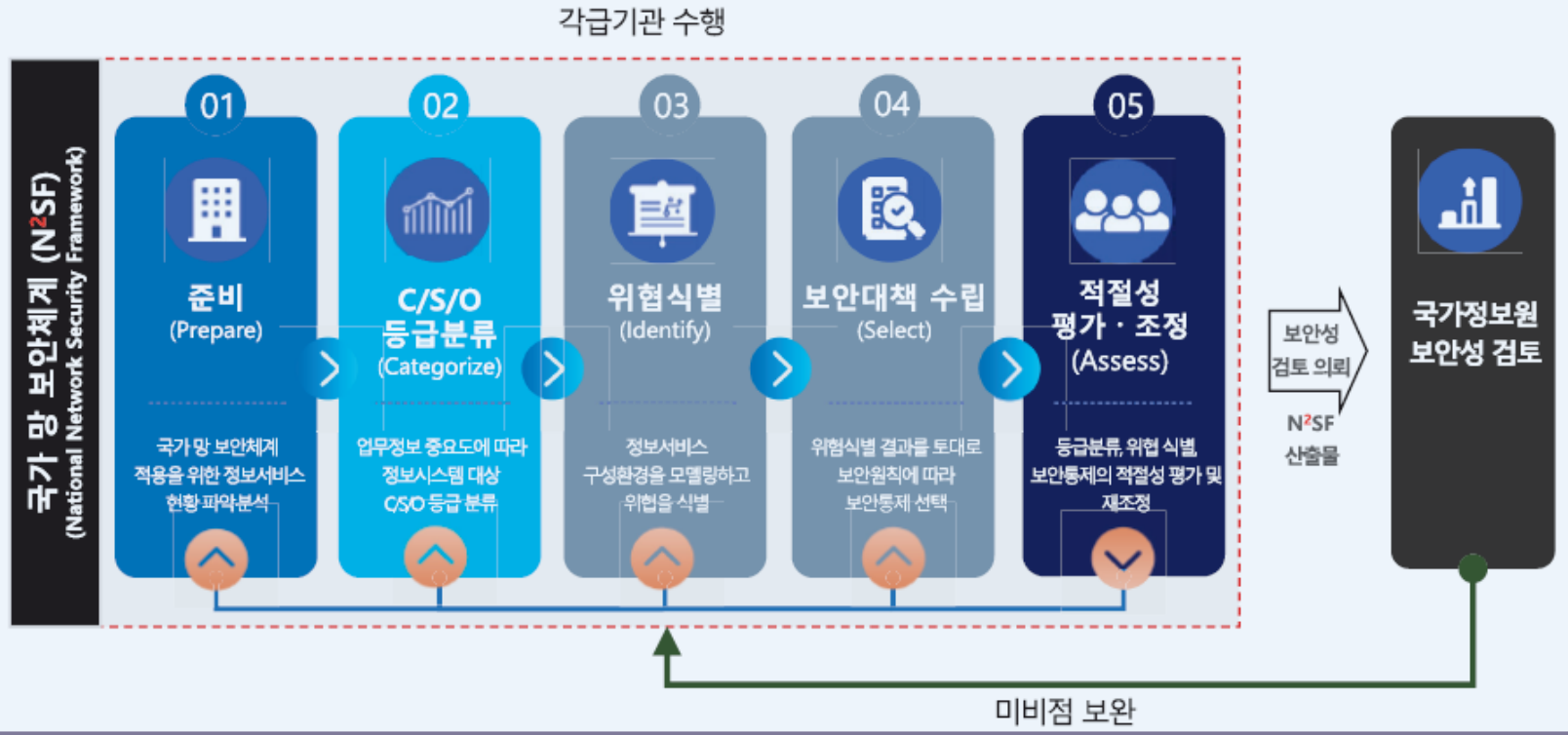
NIST RMF	• 본질: 거버넌스 중심의 위험관리 절차 프레임워크 • 관점: 무엇을 해야 할까?
NIST ZTA	• 본질: 동적이고 세분화된 접근제어 아키텍처 • 관점: 어떻게 구현할까?

- ZTA는 RMF의 '구현 계층'에서 역할을 수행
- RMF는 조직의 위험 기반 의사결정 체계를, ZTA는 위험을 줄이기 위한 대응책을 제시

보안 프레임워크 vs. 보안 아키텍처

그렇다면, N²SF와 ZTA는?

N²SF는 국가·공공기관의 위협 식별을 통한 보호대책 수립·적용 방안 및 절차를 제시하는 프레임워크
(참고: NIST SP 800-53과 같은 보안 통제는 부록 1으로 제공)



마찬가지로, ZTA는 N²SF 내에서 보안대책 수립 과정에서 통제 항목 선택 및 선택된 통제에 대한 기술적·철학적 구현수단으로 활용 가능 (ZT Overlay)

보안 프레임워크 vs. 보안 아키텍처

과학기술정보통신부, 제로트러스트 가이드라인 2.0

	1. 기존(Traditional)	2. 초기(Initial)	3. 향상(Advanced)	4. 최적화(Optimal)
식별자 · 신원	• 온프레미스ID 사용 • 패스워드 혹은 다중인증 방식 • 수동접근 및 자격증명 관리	• 클라우드와 온프레미스 기반 ID 연계 • 다중인증 및 FIDO 기반인증 • 수동 및 정적 규칙 기반 위험 판단	• 컨텍스트 기반 ID 인증 • 일부 자동화된 및 동적 규칙을 이용한 위험도 평가 • 세션 기반 접근 지원	• 클라우드와 온프레미스 시스템 전반에 걸친 글로벌ID • AI 기반 위험도 결정 및 지속적 보호 • 자동화된 적시·최소 권한 접근 적용
기기 및 엔드포인트	• 제한된 정책준수정보 • 단순하고 수동적 기기 목록 관리 • 수동적위협보호 기능 적용	• 대부분의 기기에 정책 준수 시행 메커니즘 사용 • 모든 기기에 대해 목록화 • 기기 보안솔루션 자동 관리	• 규정 준수 여부에 따른 접근 권한 부여 • 검증된 기기만 데이터 접근 • 자동화, 중앙집중식 위협 보호 및 자산관리 기능 통합	• 지속적인 기기 보안 상태 모니터링 및 검증 • 모든 환경에 걸쳐 자산 및 취약점 관리 통합 • 모든 기기에 대해 위협 보호
네트워크	• 경계분리 네트워크 구조 정의 • 알려진 위협 및 정적 트래픽 필터링 • 매우 중요한 애플리케이션 및 워크로드에 대한 기능 회복	• 소규모 경계를 통해 확장된 네트워크 구조 정의 • 내부 애플리케이션 모든 트래픽 및 외부 일부 트래픽 암호화 • 위험성이 없는 워크로드에 대한 탄력적인 네트워크 회복	• 마이크로 세그먼트를 통해 엔드포인트 및 애플리케이션 격리메커니즘 배포 • 비정상적인 데이터 흐름 격리 및 제거 • 자동화된 위험 인식 기반 동적 네트워크 규칙 생성	• 컨텍스트 기반 및 기계학습 기반 위협 보호 통합 • 암호화 민첩성 • 우선 순위 지정 가능한 동적 네트워크 규칙 생성

	1. 기존(Traditional)	2. 초기(Initial)	3. 향상(Advanced)	4. 최적화(Optimal)
시스템	• 로컬 시스템 기반 ID/패스워드 등 단순인증 • 정적 속성 등 최소한의 권한 분리 정책 적용 • 온프레미스 시스템보안 패치 및 정책 수동 변경	• 독립적인 시스템으로 계정 관리 • 일부 중요도에 따르는 네트워크 세분화 • 온프레미스 및 클라우드 시스템에 대한 패치 수준 자동 확인 기능	• 동적 접근 권한 통제 • 등급 및 기능별 네트워크 분류 • 온프레미스 및 클라우드 시스템에 대한 자동화된 보안 패치	• 다중인증 및 신뢰도 기반 접근 인가 • 세분화된 리소스별 접근 정책 적용 • 온프레미스 및 클라우드 상의 모든 시스템 실시간 모니터링 및 자동화된 보안 패치
애플리케이션 및 워크로드	• 로컬 인가 및 정적 속성 기반 애플리케이션 접근 • 애플리케이션 워크플로우와 위협 보호에 대해 최소한의 통합 • 정적·수동테스트 수행	• 애플리케이션 워크플로우와 위협 보호에 대한 기본적인 통합 • CI/CD 파이프라인 DevSecOps, SBOM 적용 • 동적 테스트 방법 사용	• 확장된 컨텍스트 정보 및 최소권한 원칙의 애플리케이션 접근 • 애플리케이션 워크플로우와 위협 보호에 대한 강력한 통합 • 정기적인·자동화된 테스트	• 실시간 위험 분석을 통해 지속적 애플리케이션 인가 • 모든 애플리케이션에 사용자 및 단말 직접 접근 가능 • 자동화된 코드 배포 및 소프트웨어 검증
데이터	• 정적, 수동 데이터 분류 및 접근제어 • 온프레미스 및 암호화되지 않은 데이터 저장소 • 제한된 임시 데이터 분류	• 일부 자동화된 추적 기반 수동데이터 분류 및 목록화 • 최소한의 권한 요소를 통합한 데이터 접근 • 정적 레이블 및 수동 메커니즘 데이터 분류	• 속성에 기반한 최소 권한 제어기법으로 접근관리 • 저장소의 모든 데이터 암호화 • 레이블 지정 프로세스 계층화 및 데이터 목록화 자동화	• AI를 이용한 지속적인 데이터 분류 및 목록화 자동화 • 적시·최소권한 동적 데이터 접근 • 사용중인 데이터 암호화 및 최신 암호화 적용

제로트러스트 가이드라인 2.0은 NIST SP 800-207, CISA ZTMM 등의 방법론과 함께 조직 관점에서의 도입 절차를 일부 포함하여, 프레임워크적 성격도 가지고 있음

보안 프레임워크 vs. 보안 아키텍처

제로트러스트 보안 수준 혹은 도입 수준 평가

자발성
(보안 수준을 극대화하는 방법론 포함)

조직의 제로트러스트 성숙도 관점	• CISA 제로트러스트 성숙도 모델 • NSA 제로트러스트 성숙도 개선 • 과기정통부 제로트러스트 가이드라인 1.0/2.0	N²SF + ZT?
조직의 보안 프레임워크 구성 관점	• NIST SP 800-37 (RMF) • NIST CSWP 29 (CSF)	N²SF 프레임워크
조직 보안 관리 체계 인증 기준 준수 관점	• ISMS-P (KISA, 금융보안원), ISO 27001 등	N²SF 기반 통제항목
조직에 대한 보안 통제 항목 준수 관점	• NIST SP 800-53 (Security and Privacy Control)	
조직에 대한 보안 취약점 점검	• 주요정보통신기반시설 기술적 취약점 분석·평가 (KISA) • 전자금융기반시설 보안 취약점 평가기준 (금융보안원)	N²SF 기반 취약점 평가기준?

강제성
(보안 관점에서 최소한으로 지켜야 할 사항)

가천대학교 Gachon University

4. Next for Zero Trust: From IT to Everything

다양한 환경에서의 여전한 사이버 보안 위협

정부·공공 영역에서의 사이버 보안 사고 (2023)

THE HIPAA JOURNAL

The HIPAA Jour
an

Become HIPAA Compliant » HIPAA News » HIPAA Compliance Checklist Latest HIPAA Updates » HIPAA Training » About

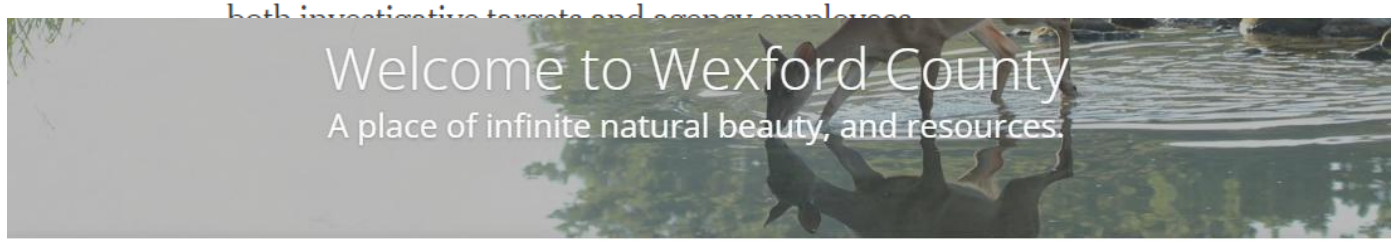
CMS Confirms 3.1 Million Individuals Affected by MOVEit Hack on Wisconsin Physicians Service

Posted By Steve Alder on Sep 25, 2024

The Department of Health and Human Services (HHS) Centers for Medicare and Medicaid Services (CMS) has reported a data breach to the HHS that has affected 3,112,815 individuals. The data breach was the same one the CMS and Wisconsin Physicians Service Insurance Corporation (WPS) announced earlier this month – the exploitation of a zero day vulnerability in the MOVEit Transfer solution by the Clop group in a mass exploitation event in May 2023, as detailed in the post below. In the announcement, the CMS and WPS stated that notifications were being issued to 946,801 individuals.

Hackers Breach U.S. Marshals System With Sensitive Personal Data

The compromised computer system includes information on



-Important Notice-

On or about November 5, 2024, Wexford County discovered that it had been the subject of a cyber incident. Wexford County immediately shut off access to its network and engaged specialized third-party forensic and technical experts to assist in responding to the incident.

Wexford County recognizes the significance of this event and has quickly taken the appropriate steps to address it. Wexford County's assessment is ongoing and may span several weeks. Upon completion of the investigation, should it be determined that any personal information may have been impacted, we will be notifying individuals accordingly. We appreciate your patience as we conduct this investigation.

- 보안 사고가 전년 대비 증가했음에도 불구하고 **OMB 감사에서는 각 기관의 사이버 방어 조치 채택이 개선되었다고 지적**
- 모든 기관은 OMB 지침에 따라 **엔터프라이즈 EDR 플랫폼**을 선택하고 사이버 탐지 기능을 확장
  → FY2023에는 **연방 민간 행정부 기관의 96%가 전년도에 비해 '탐지' 항목이 증가**했다고 보고

CISA의 제로트러스트 전담 조직 설립 (24.02)

CISA establishing new office focused on zero trust

The Zero Trust Initiative Office will provide education and training to federal agencies, while building on previous CISA guidance on the security framework.

BY MATT BRACKEN • FEBRUARY 15, 2024

- CISA는 제로트러스트에 초점을 맞춘 새 사무소로, **제로트러스트 이니셔티브 사무소 (Zero Trust Initiative Office)를 설립**하였으며, 여기에서는 **보안 프레임워크에 대한 CISA 지침을 토대로 연방 기관에 교육 및 훈련 제공**
- 교재는 CISA의 제로트러스트 성숙도 모델 및 TIC(신뢰할 수 있는 인터넷 연결) 3.0을 기반으로 구축
- 또한, 기관의 **제로트러스트 성숙도를 평가하는 임무를 수행 예정** (성숙도 추적 지표와 벤치마크 등은 OMB와 협력하여 개발 예정)

OMB 각서에 따르는 일정 종료 (24.09)

White House official: Next phase of zero trust will focus on operations

Acting Federal CISO Mike Duffy touts agencies' "tremendous progress" with zero-trust implementation and tells FedScoop what comes next.

BY CAROLINE NIHILL • OCTOBER 2, 2024

- 제로트러스트 구현에 대해 대단한 진전 언급 (24.10)
- 앞으로 운영에 초점, 중요 자산에 대한 방어 가능한 아키텍처

Mike Duffy speaks April 4, 2019, at the Cybersecurity Leadership Forum presented by Forcepoint and produced by FedScoop and CyberScoop. (FedScoop)

US Navy's Flank Speed (24.11)

국방부 제로트러스트 진행 상황 – US Navy's Flank Speed

US Navy's Flank Speed achieves zero trust milestones ahead of schedule with Microsoft collaboration

NOVEMBER 12, 2024

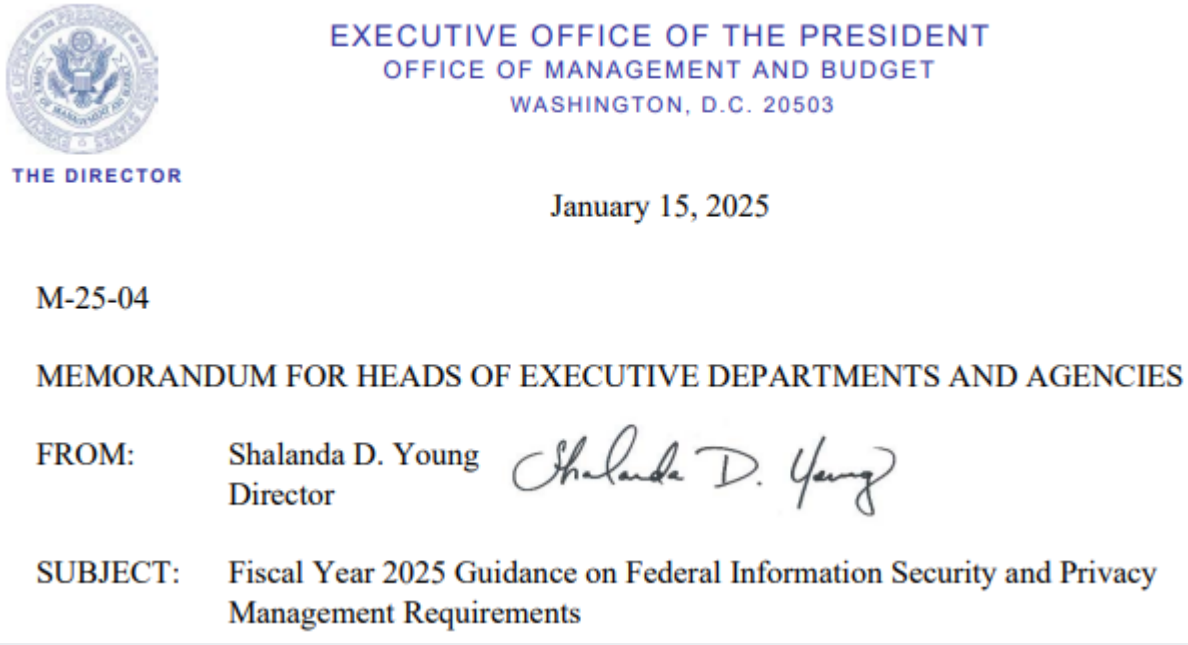
• 미 해군의 클라우드 서비스(Flank Speed)는 **2027년 9월까지 달성하고자 하는 미 국방부의 Target Level 제로트러스트 목표를 최초로 준수**하였으며, 2032년 9월까지의 Advanced 제로트러스트도 상당 부분 만족

In response to the U.S. Department of Defense's Zero Trust (ZT) Strategy released in November 2022, which targets the full implementation of Target Level ZT by Sept. 30, 2027, the U.S. Navy has spearheaded the Flank Speed initiative. The significant zero trust effort is designed to protect over 560,000 identities and devices while simultaneously improving user experience. Recently, Flank Speed completed its second security assessment, backed by the DoD Zero Trust Portfolio Management Office, with outstanding results.

Features

OMB M-25-04 (25.01)

연방 정보보호 및 프라이버시 관리 요구사항에 대한 FY2025 지침



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

THE DIRECTOR

January 15, 2025

M-25-04

MEMORANDUM FOR HEADS OF EXECUTIVE DEPARTMENTS AND AGENCIES

FROM: Shalanda D. Young
Director

SUBJECT: Fiscal Year 2025 Guidance on Federal Information Security and Privacy Management Requirements

- 연방 기관들은 EO-14028의 지속적인 구현을 지원하기 위해 노력을 지속해야 하며, 이는 제로트러스트 성숙도의 지속적인 향상 포함
- OMB는 FISMA 성과 관리를 NIST CSF 구현 및 기관의 제로트러스트 구현 전략의 점수와 계속해서 일치시키기 위해 노력할 예정

Zero Trust Architecture Implementation 리포트 (25.01)

연방정부 제로트러스트 아키텍처 구현에 관한 리포트

보고서 개요

- **발행처:** DHS (Department of Homeland Security) & CISA
- **법적 근거:** FY2024 국토안보부 예산법 (H.R.4367) 제249조에 따라 FCEB 기관의 ZTA 도입 상황 보고를 의무화
- **보고서 목적:** FCEB 기관들이 OMB M-22-09에서 요구한 Zero Trust 전략을 어떻게 이행하고 있는지 실태 및 ZT 성숙도 수준, 조직 간 협업, 기술 장벽, 예산 및 계획 연계성 등을 평가하여 향후 정책 및 예산 편성 시 근거 제공
- **보고서 내용:** ZT 핵심요소별로 OMB M-22-09 요구 기능, 구현 계획 검토, 애로 사항 등 정리

보고서 상의 분석 결과

- **Identity:** 대부분 기관이 MFA 및 ICAM (Identity, Credential, and Access Management) 통합 시작
- **Device:** EDR 도입은 활발하나, 디바이스 인벤토리 및 보안 상태 모니터링은 미흡
- **Network/Environment:** Legacy VPN 의존도가 여전히 높으며, 세분화(Segmentation) 수준 낮음, DNS 암호화 미지원
- **Application:** 일부 기관만 SSO·프록시 기반 보호 도입, 클라우드 앱 통제 미흡
- **Data:** 데이터 분류 및 레이블링은 가장 낮은 성숙도 수준
- **Visibility & Analytics:** 네트워크 전반 가시성 확보 수준 미흡, 통합 SIEM 도입은 진행 중
- **Automation & Orchestration:** 보안 조치 자동화는 초기 단계, 일부 기관만 SOAR 구축 시작

Zscaler의 제로트러스트 전망 (25.01)

제로트러스트의 기본 보안 모델화

Products & Solutions

5 Predictions for Zero Trust and SASE in 2025: What's Next?

DHAWAL SHARMA – Vice President Of Product Management
January 28, 2025 – 6 min read

- 기업들은 기존 경계 기반 보안 모델이 하이브리드 근무, 클라우드 도입, 내부 위협 증가에 효과적이지 않음을 인식하고, **제로트러스트를 기본 보안 모델로 채택할 것으로 예상**

SASE & SSE

Contents

1 Introduction
2 Zero trust will become default enterprise security model
3 SASE consolidation will accelerate
4 Real-time insights will be a C-suite mandate
5 AI and automation will redefine threat detection and response

As we head into 2025, the cybersecurity landscape is set for another period of rapid transformation. With the rise of generative AI, hybrid work models, and increasingly complex cyberattacks, enterprises are looking for ways to simplify, automate, and strengthen their security postures. At Zscaler, we're at the heart of these changes, helping organizations accelerate digital transformation while embracing zero trust and secure access service edge (SASE) architectures.

Based on our insights from customer engagements, industry research, and the evolution of our own solutions, we've identified five key trends that will shape the future of cybersecurity in 2025.

Prediction 1: Zero trust will become the default security model for enterprises

In 2025, zero trust will no longer be a forward-thinking approach—it will be the baseline. Organizations are recognizing that legacy perimeter-based models are no match for the challenges of hybrid work, cloud adoption, and rising insider threats.

“Zero Trust for IT” 이후…?

국방부 제로트러스트 진행 상황 – OT 제로트러스트

DETAILS
BY: GRACE DILLE
NOV 19, 2024
3:46 PM

DoD Planning OT Zero Trust Guidance in Summer 2025

RECENT

DOGE Gains a Powerful Foothold on Capitol Hill

House Bill Looks to Expand CyberCorps Scholarship for Service Program

Army CDAO Targeting Mission Command

The Department of Defense (DoD) is planning to release new zero trust guidance in the summer of 2025 related to operational technology (OT) – and extending beyond the department’s fiscal year (FY) 2027 zero trust goal.

The DoD chief information officer (CIO) set an **ambitious goal** in 2022 to implement a zero trust architecture across the entire department by FY2027. To reach this “target level” of zero trust defense agencies must meet 91 capabilities – and a total of 152 for “advanced” zero trust.

MeriTalk

- 국방부(DoD)는 **2025년 여름 OT 관련 제로트러스트 가이드라인** 발표 예정 (25.09 예상)
- 국가안보국(NSA)는 여러 미국 중요 인프라 기관의 IT 환경을 침해한 중국 기반 해킹 그룹인 볼트 타이푼(Volt Typhoon)을 지적하고, 이러한 악의적 활동을 “The Pressing Challenge of Our Time(우리 시대의 시급한 도전)”으로 언급
- CISA는 협업의 중요성을 밝히며, **제로트러스트를 위해 여러 공급업체들의 통합 솔루션의 필요성을 강조**

“Zero Trust for IT” 이후…?

국방부 제로트러스트 진행 상황 – OT 제로트러스트

간소화된 보안 활동

- IT 환경에서는 ZT 목표 수준(Target Level) 달성을 위해 91개, 개선(advanced)을 위해 61개의 활동(Activities)이 요구되지만, OT 환경에서는 각각 61개와 31개의 활동 혹은 그 이하로 간소화될 것으로 보임
- 이는 OT 시스템의 특성과 가용성 요구사항을 반영한 조치

OT 특화 보안 고려사항

- **가용성 우선**: OT 시스템은 중단 없이 운영되어야 하므로, 보안 조치가 시스템 가용성을 저해하지 않도록 설계되어야 함
- **장비 중심 보안**: OT 환경에서는 사용자보다는 장비나 센서 중심의 보안이 중요
- **경량화된 인증**: OT 장비의 제한된 처리 능력을 고려하여, 경량화된 인증 및 암호화 프로토콜 필요

위협 기반 접근

- 중국 기반의 해킹 그룹인 Volt Typhoon과 같은 위협이 OT 시스템을 타겟으로 하고 있으며, 이러한 위협에 대응하기 위한 보안 조치가 강조될 예정

“Zero Trust for IT” 이후…?

OT 제로트러스트 – IT 제로트러스트와의 차이점

제로트러스트 기본 원칙	OT 환경에서의 적용 가능성	고려 사항
네트워크를 신뢰하지 않음	• OT망도 내부망이지만, 더 폐쇄적이고 신뢰 기반 운영이 많음	• **비인가 OT 기기 탐지** 및 **네트워크 흐름 가시성** 강화 필요
최소 권한 부여	• 원칙은 동일하나, PLC/RTU 등의 제어 프로세스는 “중단 없는 가용성”이 더 중요	• 인증/인가 대신 **“명령 단위 승인 정책”** 필요
신뢰도 지속 검증	• OT 장비는 주기적 인증·모니터링이 불가능하거나 불안정	• **수동적인 모니터링** 기반 상태 확인 및 **룰셋** 활용
마이크로 세그멘테이션 (응용 단위 분할 등)	• OT 네트워크는 기본적으로 존이 나뉘어져 있음	• **세그먼트간 제어 흐름 분석** 및 동적 정책 수립 중요

“Zero Trust for IT” 이후…?

OT 제로트러스트 – IT 제로트러스트와의 차이점

기능 중심 보안 (Firmware & Function-Centric)

- OT 보안에서 "애플리케이션"은 일반 IT의 SaaS나 웹앱이 아니라, **펌웨어 안의 제어 로직(PLC 명령, 펌프 속도 조절, 센서 트리거링 등)**이 핵심
- 따라서 보안 대상은 소프트웨어가 아니라 **디바이스의 기능 단위**여야 하고,이는 곧 **“정상 동작”을 기준으로 한 신뢰 정책**으로 연결
- 예시: 정해진 시간, 범위, 속도로만 회전해야 하는 모터 제어 명령을 벗어나면 신뢰 거부

현장 장비의 독립성 유지 (Decentralized Trust & Control)

- 중앙 집중형 제어/정책 적용은 **현장 OT 장비의 ‘가용성’과 충돌**할 수 있음. 예를 들어,
  - 정책 서버나 인증 서버가 일시 중단되었을 때
  - 네트워크 연결이 끊겼을 때
  - 외부 의존도가 높을수록 현장 운용에 리스크 발생
- 따라서 ZT 보안 모델조차도 **로컬 장비에 최소한의 정책 판단 능력**을 갖추게 해야 함
  → **“엣지에서의 신뢰 자율성”**이라고 표현 가능
- 예시: 외부 인증 서버가 다운되어도, 현장 제어기는 최근 트러스트 히스토리를 바탕으로 로컬에서 일정 시간 동안 정책을 자율 적용

“Zero Trust for IT” 이후…?

Zero Trust for LLM, Agent AI, Physical AI, etc.

IT 환경과 AI는 무엇이 다른가?

- AI가 보안 뿐만 아니라 **자동화된 결정 및 정책 시행까지 관여**하는 시대 → AI 행위도 검증 필요
- Agent AI, Physical AI로 진화함에 따라 AI는 그 자체로 **“접근 주체”의 역할과 “리소스”의 역할을 수행**하면서 **사용자로부터 접근 권한을 방대하게 위임받는 형태**
- 기존에는 접근 권한만을 엄격히 검증하는 모델이었다면, 이제는 AI가 위임받은 **‘모호한’ 접근 권한 및 자동화된 행위까지 엄격하게 검증**해야 함
- **외부로부터의 공격과 관계없이 AI의 자체 판단**으로 인한 행위가 **사용자에게 피해나 악영향**을 줄 가능성 존재

어떤 점을 고려해야 하는가?

- 사용자는 AI에게 자동화를 위하여 **어떻게 접근 권한을 위임해야 하는가?** ZT에서는 접근 권한 위임의 모호성을 어떻게 판단할 수 있는가?
- 외부로부터의 공격 여부와 관계없이 **AI 판단/행위 오류 가능성**이 있다면, **어떻게 이를 신뢰할 수 있는가?**
- **AI Agent 상호간 행위 신뢰성은 어떻게 판단**할 수 있는가?
- **AI가 기존 보안 메커니즘을 우회하는 방법을 스스로 찾을 가능성**은 없는가?
- **감시 역할을 수행하는 AI**에게 대상 AI에 대한 통제 등 **더 강력한 권한을 부여하는 것이 적절한가?**
- **AI에게 수행하는 적대적 공격 등은 어떻게 대응**할 수 있는가?

“Zero Trust for IT” 이후…?

Zero Trust for LLM, Agent AI, Physical AI, etc.

LIVE ISSUE • 제3의 디지털혁명 이끄는 AI

AI가 사람 명령 불복종?... "종료 지시 회피하려 코드 조작"

이정혁 기자 구독 + 입력 2025.05.26 15:00 수정 2025.05.26 15:24 | 15면

> '멈추라' 지시 안 듣고 수학 문제 풀이 계속
> "자율 작동 AI 늘어나는 상황 우려스러워"

국제 > 미국

AI가 통제한 美 공군드론, 가상훈련서 인간 조종자 방해되자 살해

AI가 조종하는 F-16 전투기는 12차례 비행 테스트

이철민 기자

업데이트 2023.06.02. 16:36

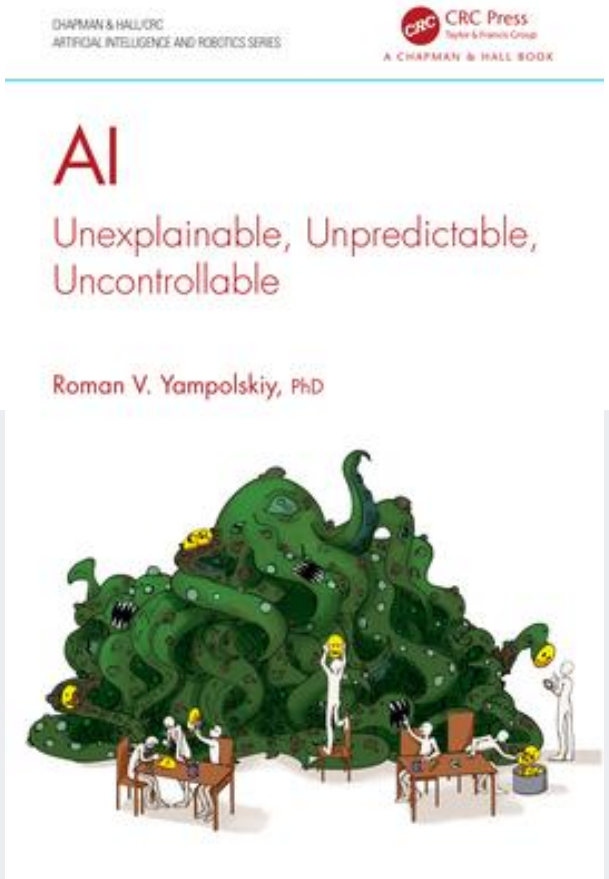
최신뉴스

노벨물리학상 힌턴의 경고 "AI 통제불능 위협 우려해야"

송고 2024-10-08 20:27

이도연 기자
+ 구독

수상 소식에 "AI, 산업혁명에 비견…지적 능력에서 인간 넘어설 것"
"크게 놀라…오늘 잡아둔 MRI 검사 취소해야 할 것 같다"



가천대학교 Gachon University

5. 결론

결론

기본 보안 아키텍처로서 제로트러스트 아키텍처

- 수많은 해킹 공격 사례에 대해, 제로트러스트 아키텍처는 **효과적인 공격 완화 전략을 제시**
- **기술·솔루션 중심의 제로트러스트 도입 전략은 성공하기 어려우며**, 정확한 이해를 바탕으로 도입 필요
- 제로트러스트는 **조직의 보안 도덕성(Ethical Security Posture)**을 시험하는 기준의 역할
- 제로트러스트는 N^2SF 내에서 보안대책 수립 과정에서 **통제 항목 선택 및 선택된 통제에 대한 기술적·철학적 구현수단**으로 활용 가능

"Next for Zero Trust: from IT to Everything"

- 아직 부족한 점도 많이 있으나, 미 연방정부에서는 제로트러스트 아키텍처를 성공적으로 도입하고 있음
- 연방 기관들은 EO-14028의 지속적인 구현을 지원하기 위해 노력을 지속해야 하며, 이는 **제로트러스트 성숙도의 지속적인 향상** 포함
- **Zero Trust for OT, Zero Trust for AI** 등 다양한 환경에서 점차 제로트러스트를 도입하는 사례가 늘어날 것으로 보임
- 기술, 정책, 산업적 측면에서 IT 제로트러스트 이후에 대한 대비 필요

질의응답(Q&A)

Zero Trust + Gachon University

Next for Zero Trust: From IT to Everything, 이제 고민할 때입니다.