’25년 제로 트러스트 적용 전략 콘퍼런스

Zero Trust Architecture - Readiness & Implementation
(SGA ZTA 준비컨설팅과 구축사례 소개)

2025. 2. 20.

에스지에이솔루션즈㈜

목차

CONTENTS

I

Introduction

1. SGA 사업 영역

에스지에이솔루션즈는

시스템 보안, 응용 보안, 엔드포인트 보안 등 사업영역을 넘어
제로 트러스트/N²SF 보안, 클라우드 보안 등 차세대 IT 보안 시장을 선도하는 통합 IT 보안 기업입니다.

「보안 솔루션 소프트웨어 개발 및 공급사」

시스템 보안 솔루션 사업
System Security Solution Biz.

국내 점유율 1위의 서버보안(SecureOS) 솔루션 개발 및 공급

클라우드 보안 솔루션 사업
Cloud Security Solution Biz.

가상화, 컨테이너 등 최신 클라우드 환경에 대한
통합 보안 솔루션 개발 및 공급

엔드포인트 보안 솔루션 사업
Endpoint Security Solution Partner Biz.

Anti-Malware, 내PC지키미, 패치관리솔루션 등
통합 PC보안 솔루션 개발 및 공급

제로 트러스트 보안 / N²SF 컨설팅 / 솔루션 사업
Zero Trust Security Consulting/Solution Biz.

국내 제로 트러스트 보안 솔루션 개발 및 사업화 선두 업체

차세대 보안 솔루션 사업
Next Generation Security Solution Biz.

APT 등 최신 행위기반 위협 탐지 및 인텔리전스 보안 솔루션
개발 및 공급

응용 보안 솔루션 사업
Application Security Solution Biz.

출력물위변조 및 블록체인, FIDO 등 업무/대국민 서비스 등을
위한 응용보안 솔루션 개발 및 공급

2. SGA Solution Map

3. ZTA vs. ZTNA

- **Zero Trust Architecture** 의 구현방법에는 크게 **ZTA** 와 **ZTNA** 두 종류가 있음

Zero Trust Access

- **사용자 및 디바이스 접근**에 대한 보안에 중점을 둔 모델
- **모든 주체, 서비스, 데이터 등이 인증과 적절한 권한**을 부여 받아야 한다는 개념
- 네트워크, 애플리케이션, 데이터 등에 대한 **모든 권한을 재평가**하고, **접근 요청을 검증 및 승인**하는 프로세스

ZTNA
(Zero Trust Network Access)

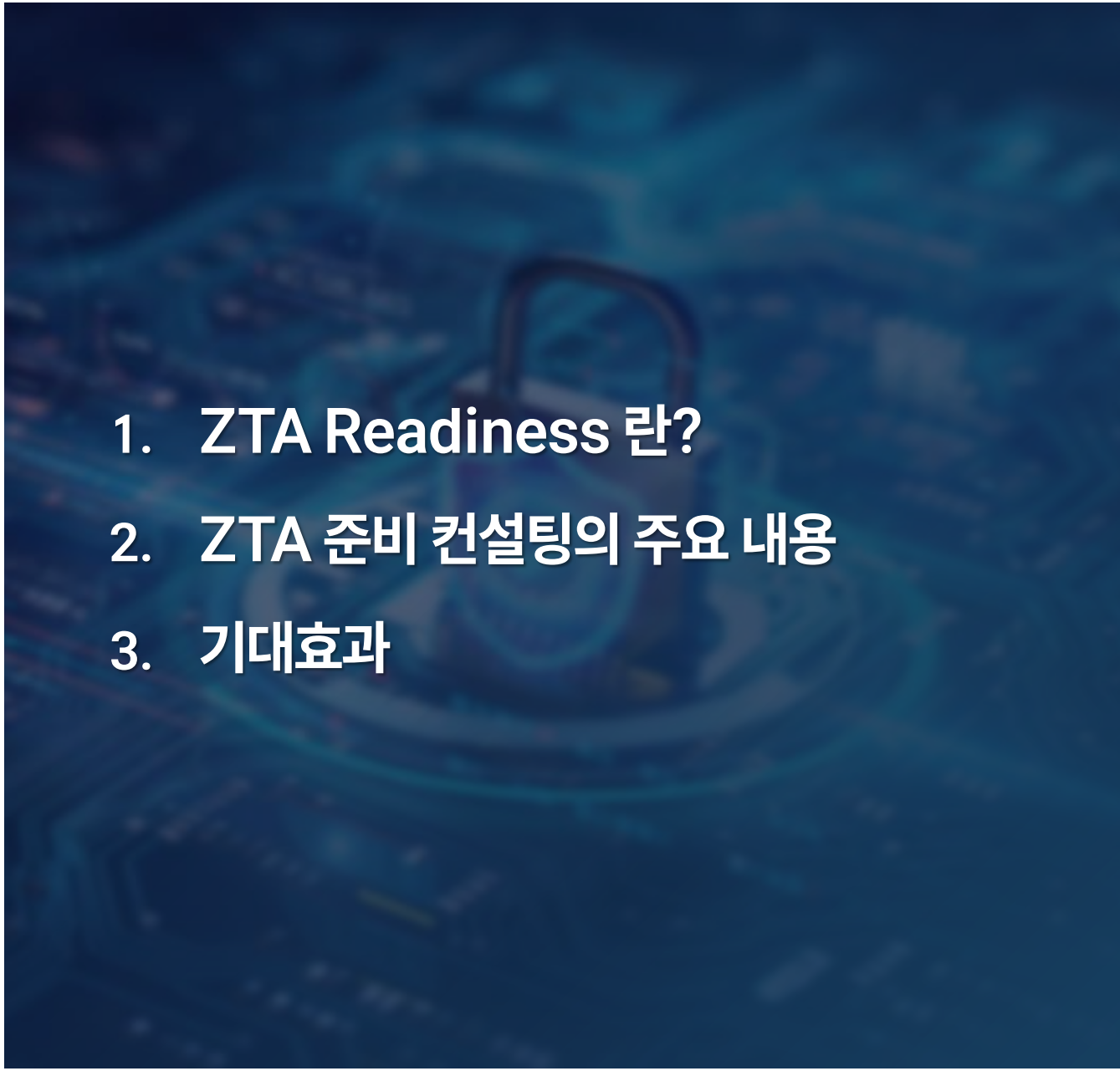
- **애플리케이션 및 데이터에 안전한 원격접근** 제공에 중점을 둔 **네트워크 보안 모델**
- 사용자가 필요한 애플리케이션에 직접 연결되는 것이 아니라 클라우드 기반 게이트웨이로 연결
- 리소스 요청에 따라 사용자의 신원과 권한을 확인하고, 데이터 및 애플리케이션에 대한 접근 제한

기업 내에서 사용되는 모든 시스템, 서비스, 애플리케이션 등

엔터프라이즈 리소스 보호를 위한 종합적인 제로 트러스트 적용 방법론

II

ZTA Readiness



1. ZTS Readiness 란?

컨설팅 필요성

제로 트러스트는 단순 제품이 아님

- 제로 트러스트는 단순 보안 제품을 의미하지 않음
- 제로 트러스트는 새로운 보안 프레임워크로 달성 가능하며, 그에 따른 접근방식이 필요함

제로 트러스트는 관점을 바꾸는 것

- 제로 트러스트는 전통적인 보안의 관점을 재 정립하도록 함
- 사전 분석을 통한 현황 대비 목표 모델링 및 그에 따른 제로 트러스트 관점의 결과를 도출함

정량적 달성지표의 분석 및 재정립 필요

- 비교 분석 및 목표 설정을 위한 정량적 지표 수집 및 분석, 정의
- 정량적 달성지표는 성숙도 관점에서 평가하고 결과에 따른 대응이 필요
- 성숙도 분석 및 평가결과는 제로 트러스트 달성 수준을 파악할 수 있게 해 줌

제로 트러스트를 새로운 보안 프레임 관점으로 해석

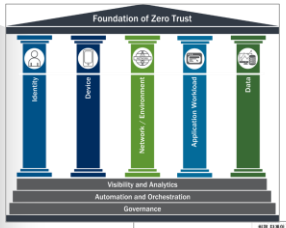
- 아키텍처 이해 및 준용
- 다양한 성숙도 참조모델 이해 및 활용
- 성숙도 기반 평가방안 도출 및 제시

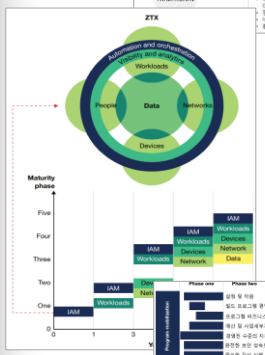
제로 트러스트는 기존 보안의 관점을 재정립

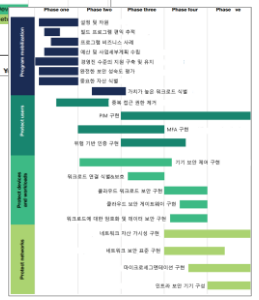
- 이론과 지식으로 달성 불가
- AS-IS / TO-BE 분석 및 모델링 필요
- 정량적 달성 지표 기반 현황분석 및 목표모델 정의
- 제로 트러스트 아키텍처 기반 보안 구성요소 매핑

주요 참조 모델

- DoD Zero Trust Capability Execution Roadmap(COA 1)
- CISA Zero Trust Maturity Model v2
- KISA Zero Trust Maturity Model
- Microsoft Zero Trust Maturity Model
- Forrester Roadmap Consideration







2. ZTA 준비 컨설팅의 주요 내용 (1/4)

컨설팅 대상 업무 시스템에 대한 단계적 제로 트러스트 적용 및 확대 방안 제시

환경 및 현황/분석 (AS-IS)

대상 업무 시스템 환경 및 현황분석

- 국내외 제로 트러스트 모범 사례 분석
- 대상 업무 및 시스템 선정
- 대상 업무 보안 시스템 환경/현황 조사
- 대상 업무 보안 시스템 제로 트러스트 요구사항 도출

GAP 도출/분석

대상 업무 시스템
제로 트러스트
GAP 도출 및 분석

- 제로 트러스트 성숙도 모델 중 6대 핵심요소 별(신원, 시스템 등) GAP 도출
- 제로 트러스트 성숙도 모델 단계별 해당 GAP 도출
- GAP 도출을 위한 제로 트러스트 성숙도 모델 활용

미래모델 수립 (TO-BE)

제로 트러스트 아키텍처 모델링

- GAP 분석 결과 반영
- 대상 업무 시스템 제로 트러스트 모델 도출
- 제로 트러스트 아키텍처 도출
- 단계별 제로 트러스트 확대 방안 도출
- 단계별 제로 트러스트 참조 모델 수립

피드백/개선/확대

단계적 제로 트러스트 체계 확대

- 프로젝트 종료 및 최종 산출물 검토/인도
- 'TO-BE' 모델 단계적 확대를 위한 피드백
- 제로 트러스트 아키텍처 지속적 전환/확대
- 반복/개선/모니터링/확대 등 사업 확대

단계적 제로 트러스트 체계로의 전환을 위한 파일럿 컨설팅

2. ZTA 준비 컨설팅의 주요 내용 (2/4)

[수행방안-1] 특정 업무 시스템 대상 제로 트러스트 전환 파일럿 컨설팅 사업 추진

- ✓ 협의를 통해 ZTA 적용 대상 업무 시스템 선정 후 관련 시스템에 대한 현황 분석
- ✓ 현행 시스템에 대한 제로 트러스트 관점에서의 요구사항 분석, GAP 분석 등 AS-IS, TO-BE 도출

AS-IS

대상 업무 및 업무 시스템

- 사전 질문지 기반 Q&A
- 사전 인터뷰(현장 또는 원격)
- 업무 환경 분석 (본사, 지사, 재택, 대리점 등)
- 업무 시스템 분석 (PC, 모바일, 업무 서버, 업무 애플리케이션, 네트워크 구조 등)
- 제로 트러스트 체계 전환 요구사항 도출 등

제로 트러스트 핵심요소

제로 트러스트 성숙도 단계

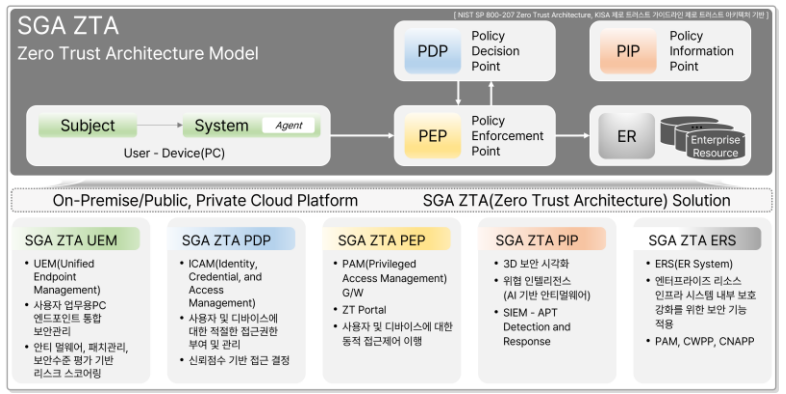
TO-BE

GAP 도출/분석

- 식별자·신원
- 기기 및 엔드포인트
- 네트워크
- 응용 및 워크로드
- 시스템
- 데이터

- 최적화(Optimal)
- 향상(Advanced)
- 기존(Traditional)

목표 제로 트러스트 아키텍처 도출



목표 제로 트러스트 보안 모델 도출

- 유스케이스
- 개선 우선순위
- 참조 모델
- 단계적 확대 방안

2. ZTA 준비 컨설팅의 주요 내용 (3/4)

[수행방안-1] 특정 업무 시스템 대상 제로 트러스트 전환 파일럿 컨설팅 사업 추진

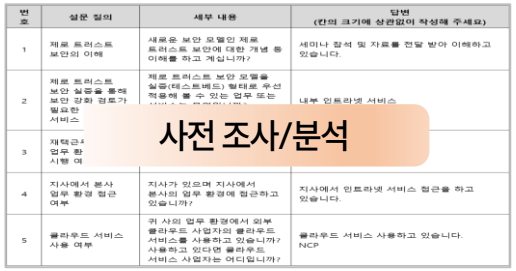
- ✓ 특정 대상 업무 시스템의 제로 트러스트 시스템 전환을 위한 분석, 도출, 모델 정립 등 추진
- ✓ 대상 업무 시스템의 사업환경 이해, 업무 프로세스 분석, 업무 시스템 분석 기반 미래모델 정립

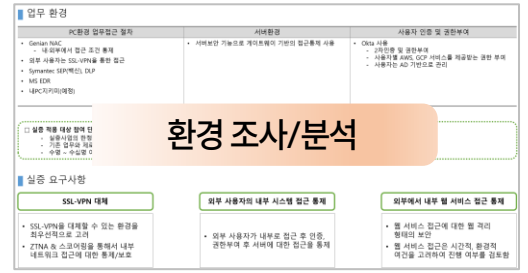
SGA 제로 트러스트 보안 수준 진단 컨설팅 방법론

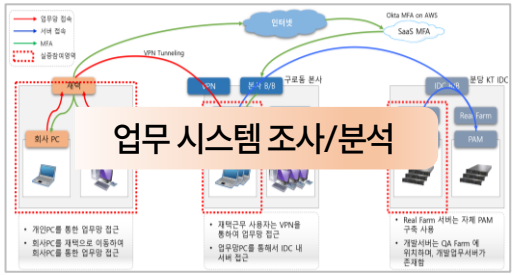
1	환경 및 현황분석 (AS-IS)	• 국내·외 제로 트러스트 선진 사례 분석 • 업무 시스템 선정 및 현황 분석 • 업무 시스템 요구사항 분석 및 GAP 분석
2	미래모델 수립 (TO-BE)	• 제로 트러스트 보안 아키텍처 도출 • 단계별 제로 트러스트 보안 확대 방안 도출 • 단계별 제로 트러스트 보안 참조 모델 수립
3	단계적 제로 트러스트 보안 체계 확대	• 프로젝트 종료 및 최종 산출물 검토/인도 • 'TO-BE' 모델 단계적 확대를 위한 피드백 • 제로 트러스트 보안 아키텍처 지속적 전환/확대

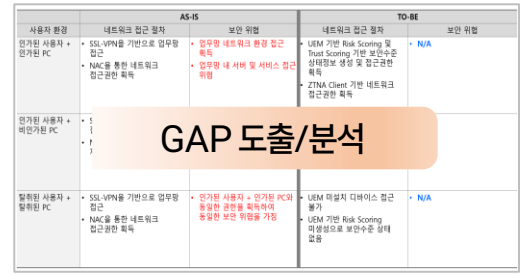
제로 트러스트 보안 특수성 이해 | 제로 트러스트 보안 아키텍처 설계 노하우 | 제로 트러스트 보안 사업 수행 경험 다수

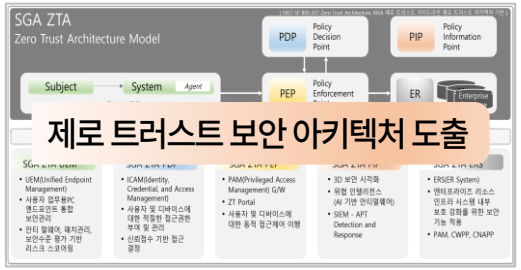
본 사업 제로 트러스트 수준 진단 컨설팅 방안 예시

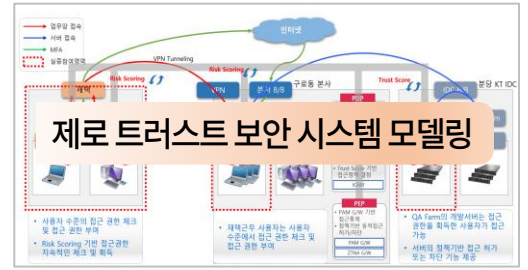












2. ZTA 준비 컨설팅의 주요 내용 (4/4)

[수행방안-2] 제로 트러스트 보안 원칙 및 아키텍처에 부합하는 대상 업무 시스템 미래 모델 도출

- ✓ 대상 업무 시스템의 제로 트러스트 전환에 대한 요구사항을 바탕으로 미래 모델 도출
- ✓ 대상 업무 시스템 제로 트러스트 참조 수립을 위한 성숙도 단계별 제로 트러스트 확대 방안 도출

통합 엔드포인트 관리 시스템

- 안티 멀웨어, 보안 패치관리, 보안 수준 진단 및 관리
- 엔드포인트 보안 수준 기반 리스크 스코어링

정책 통합관리 시스템

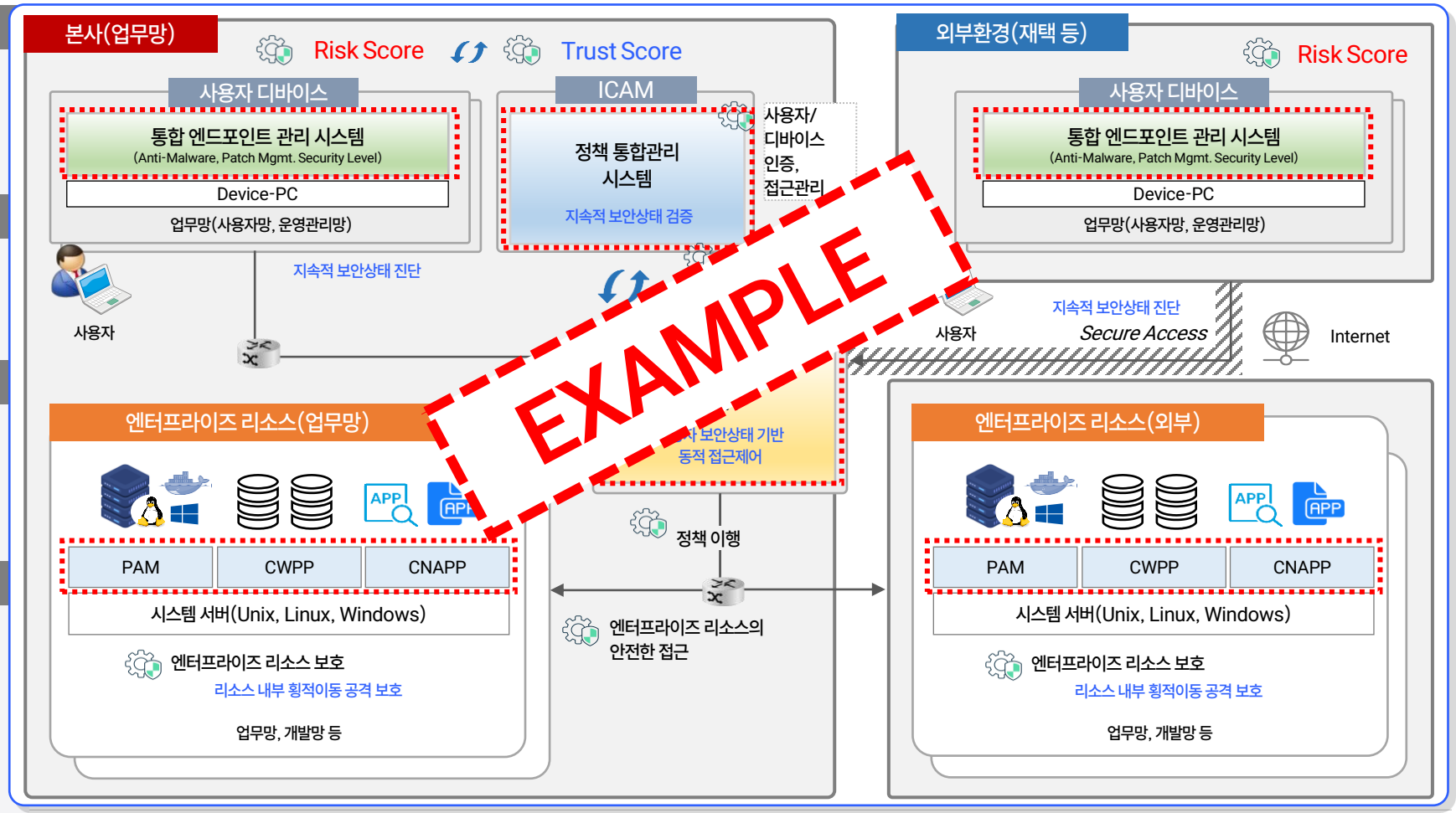
- 사용자, 디바이스 접근권한(계정, 크리덴셜, 접근) 관리
- 신뢰점수 기반 동적 접근제어 결정

시스템 접근제어 G/W

- 정책 기반 사용자, 디바이스 접근통제
- 사용자 디바이스 신뢰점수 기반 동적 접근제어(세션 차단, MFA)
- Secure Proxy G/W 기반 접근

엔터프라이즈 리소스 시스템 보호

- (PAM) 서버 접근통제(파일/디렉토리 접근통제, 명령어 통제, 경유통제 등)
- (CWPP) 서버 워크로드 보호(Host IPS/Firewall/Anti-Malware 등)
- (CNAPP) 컨테이너 보안, 애플리케이션 보호



3. 기대효과 (1/2)

ZTA 준비 컨설팅으로 기존 환경의 명확한 제로 트러스트 관점 취약점 분석이 가능합니다.

다변화 되어 가는 업무환경 및 위협

- 하이브리드 워크플레이스 확대
- 지능형 보안 위협 지속적 증가

사용자, 디바이스 지속적 검증 미흡

- 리소스에 접근하는 사용자, 디바이스에 대한 지속적인 보안 수준 검증 없음
- 정적 인증, 정적 접근통제 정책 바탕

단계별 보안성 확대 기준 부재

- 기존 보안 정책, 보안 시스템과 관련된 단계별 보안 수준 확대 기준 없음
- 레거시 보안 시스템 지속적 의존

암묵적 신뢰기반 경계 보안 위협

- 네트워크 경계 보안 모델 암묵적 신뢰
- 네트워크 내부는 신뢰하는 영역으로 가정하고 설계된 태생적 한계성 내포

기존 보안 모델 대비 효과성 검증

- 모든 리소스 요청에 대한 타당성은 배제하고 지속적인 사용자 및 디바이스에 대한 검증 기준 적용
- 사용자, 디바이스의 보안 상태를 지속적으로 평가한 후, 안전하게 접근할 수 있도록 함

단계별 보안성 강화

- 제로 트러스트 성숙도 모델 단계(전통 → 향상 → 최적) 별 기반 보안성 달성 방안 제시
- 제로 트러스트 성숙도 모델에 적합한 보안성 확대 방안 적용

> “ 본 사업을 통해 제로 트러스트 보안 도입 및 적용을 검토하기 위한 미래 보안전략의 기초를 마련할 수 있음 ”

자산 중심 보호 전략

- 고정된 경계를 방어하는 것에서 사용자/자산 중심 방어로 보안 관점을 변경
- 자원(자산, 서비스, 워크플로우, 계정 등)을 보호하는 것에 초점을 맞춤

암묵적 신뢰 제거

- 암묵적 신뢰를 바탕으로 구성된 네트워크 경계형 모델 탈피
- 네트워크의 위치는 더 이상 자원의 보안 상태를 결정하는 주요 요소로 볼 수 없음

3. 기대효과 (2/2)

ZTA 준비 컨설팅으로 최적의 도입 계획을 수립하고 전략적으로 추진할 수 있습니다.

1 증권사 최초 수행

- 빠른 제로 트러스트 보안 체계 도입전략 수립 가능
- 전통적 레거시 보안 모델 대비 차별성 검증
- 미래 지향성 보안 모델 사전 확보

2 새로운 모델 기반 방향 제시

- 다년간의 사업 노하우, 분석 기반의 구체적인 모델의 도입
- 환경에 맞는 최적의 제로 트러스트 보안 모델 제시
- 업무환경 및 비즈니스 모델을 고려한 제로 트러스트 보안 TO-BE 모델 도출

3 제로 트러스트 효과성 확보

- 단계적인 제로 트러스트 방향성 수립
- 성숙도 기반 보안성 달성 방안 제시
- 통합 제로 트러스트 솔루션 기반의 비용 절감
- 보안 강화, 안정성 등 다양한 효과 검증/확보

4 미래 보안모델의 선도적 준비

- 업무 및 업무 서비스 관련 리소스 관리 및 보호 강화 방안 마련
- 중장기적으로 안전하고 신뢰할 수 있는 업무 및 대 고객 서비스 강화

sga 에스지에이솔루션즈(주) SGA Solutions Co., Ltd.

업무환경과 비즈니스 환경에 적합한 제로 트러스트 보안 모델 도출

III

ZTA Implementation (ZTA 의 적용)

1. 사업 개요
2. 사업 수행 내용
3. 솔루션의 구성
4. 효과성 분석
5. 기대효과

1. 사업 개요_ 컨소시엄 및 수요기관 구성

- ▢ 한국인터넷진흥원「2023년 제로 트러스트 보안 모델 실증 지원」사업 수행사 포함 컨소시엄 구성으로 기술적 연속성 부여
- ▢ 제로 트러스트 포럼 산업분과 참여 기업, 한국제로트러스트협의회(KOZETA) 회원사 참여 컨소시엄 구성으로 전문성 부여

[주관/참여기관]

에스지에이솔루션즈(주)

제로 트러스트, 시스템 보안 등 솔루션 전문 기업 — 주관기관

- ▢ '21년 과학기술정보통신부 제로 트러스트 연구개발과제사업 주관기관
- ▢ '23년 과학기술정보통신부 제로 트러스트 보안 모델 실증 지원사업 주관기관

에스지에이아이피에스(주)

제로 트러스트, 엔드포인트 보안 등 솔루션 전문 기업 — 참여기관

- ▢ 에스지에이솔루션즈㈜와 통합 보안영역 기술 공유 및 역량 보유
- ▢ 제로 트러스트 엔드포인트(PC) 영역 전문 사업 및 기술 역량 보유

SGN 에스지앤㈜

제로 트러스트, 시스템 접근제어 등 솔루션 전문 기업 — 참여기관

- ▢ '23년 과학기술정보통신부 제로 트러스트 보안 모델 실증 지원사업 참여
- ▢ 15년 노하우 기반 국내 시스템 접근제어, 계정관리 보안 솔루션 전문 기술 보유

KSIGN ㈜케이사인

데이터 보안 영역 솔루션 전문 기업 — 참여기관

- ▢ 국내 데이터 암호화 및 접근제어 등 데이터 보안 전문 기업
- ▢ 제로 트러스트 데이터 보안 영역 전문 사업 및 기술 역량 보유

ENKI ㈜엔키화이트햇

모의 침투 테스트 기반 보안 컨설팅 전문 기업 — 참여기관

- ▢ PTaaS(Penetration Testing as a Service) 기반 도입 모델의 완성도, 보안성 검증(취약점 진단, 모의해킹 등) 전문 기술 보유

[수요기관]

정부·공공

책임운영기관 행정안전부 국가정보자원관리원

세계 최초 정부 통합 데이터 센터, 디지털 서비스 전문기관

대한민국 공공기관 행정안전부 소속 책임운영기관
중앙행정기관, 지방자치단체 및 공공기관의 정보시스템 및
국가정보통신망 운영 관리

정부·공공

공무원연금공단

공무원 복지향상을 위한 종합 연금복지서비스 기관

안정적인 연금복지서비스로 전·현직 공무원의
복지향상과 지속가능한 사회발전에 기여

1. 사업 개요_수요기관 참여 내용

- ▢ 향후 확대/확장 적용 시 국가정보자원관리원 대구센터 내 On-Premise 형태로 제로 트러스트 보안 시스템 구축 고려
- ▢ 국가정보자원관리원 운영관리 대상 및 입주기관(이용기관)인 공무원연금공단, 삼성SDS 클라우드 환경 적용 고려

책임운영기관
행정안전부
국가정보자원관리원

운영관리 업무 영역

- □ 국가정보자원관리원 대구센터 **운영관리 영역** 대상
- □ 운영관리자, 운영관리 서버 대상
- □ 국가정보자원관리원 제로 트러스트 보안모델 도입 및 운영계획에 준하여 구축 및 적용 수행(세부 수행계획, 구축방안, 적용절차 등 추진)

공무원연금공단 업무 영역

- □ 국가정보자원관리원 대구센터 내 **입주기관(이용기관)**
- □ 국가정보자원관리원 대구센터 입주기관의 업무 대상 제로 트러스트 보안 모델 적용
- □ 대상업무: **"DID기반 신원인증 시스템"**

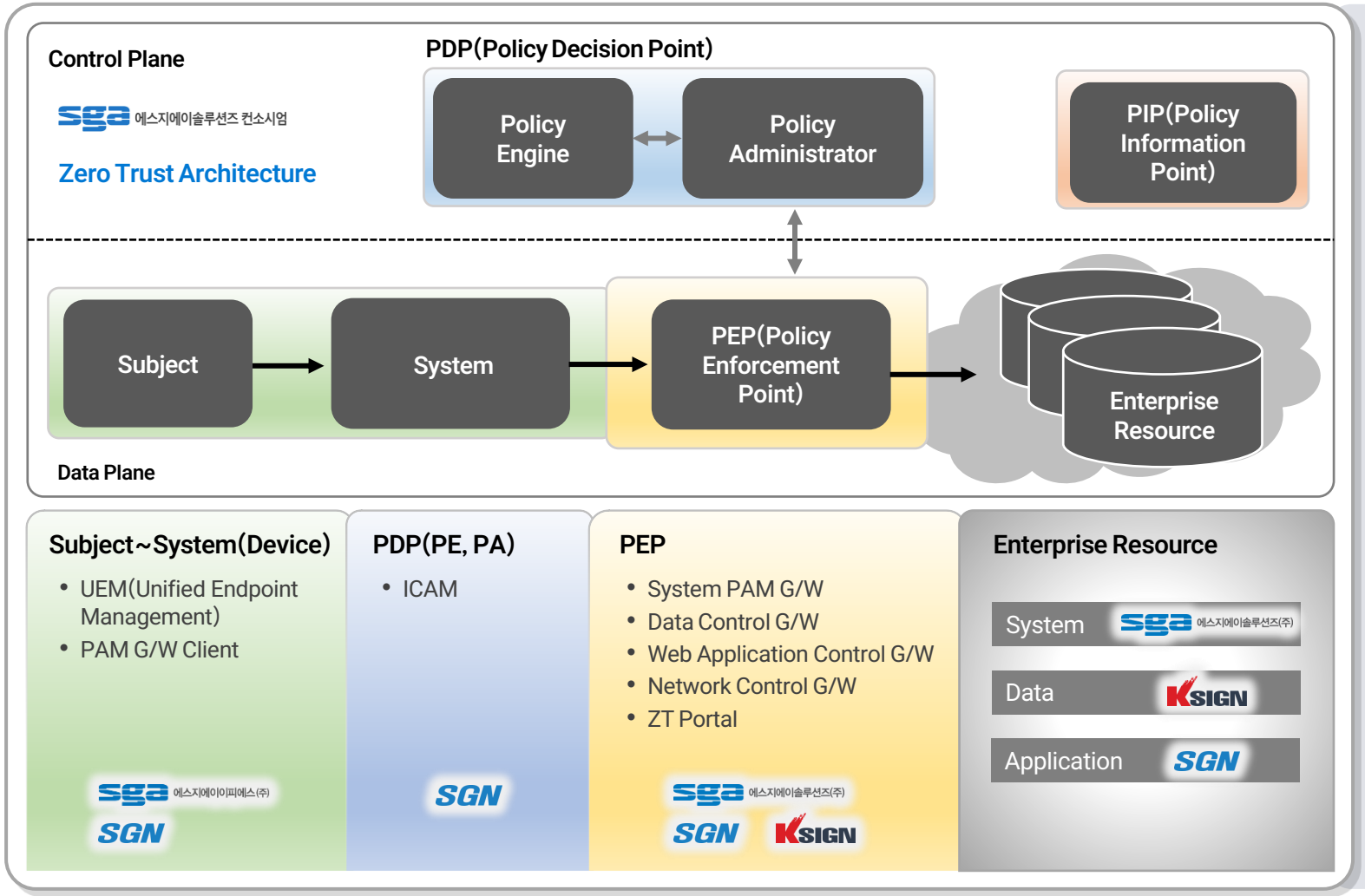
삼성SDS 클라우드

- □ 국가정보자원관리원 대구센터 내 클라우드 자원 제공 기관
- □ 삼성SDS 클라우드에 **SECaaS 형태로 구축 적용 검토**
- □ 테스트 환경 기반 제로 트러스트 보안 모델 적용 및 **향후 서비스 모델 추진 도모(협업 지원)**

" 정부·공공·민간기관 모두 포함하는 구축 및 적용 대상의 서비스형 제로 트러스트 표준 보안 모델로 확대 고려 "

2. 사업 수행 내용_목표 보안모델 및 역할 분담

- 국내 제로 트러스트 가이드라인 1.0, 제로 트러스트 아키텍처에 기반한 목표 제로 트러스트 보안 모델
- Subject~System, PDP,PEP, Enterprise Resource(System, Data, Application) ZTA 기준 솔루션 모델



Subject~System
- UEM(Unified Endpoint Management) Agent
- PAM G/W Client

PDP(Policy Decision Point)
- ICAM(Identity Credential, and Access Management)

PEP(Policy Enforcement Point)
- System PAM(Privileged Access Management) G/W
- Data Control G/W
- Web Application Control G/W
- Network Control G/W
- ZT(Zero Trust) Portal

Enterprise Resource
- System : PAM(Privileged Access Management) , ZTS(Zero Trust Segmentation)
- Data : Data Control
- Application : Web Application Control

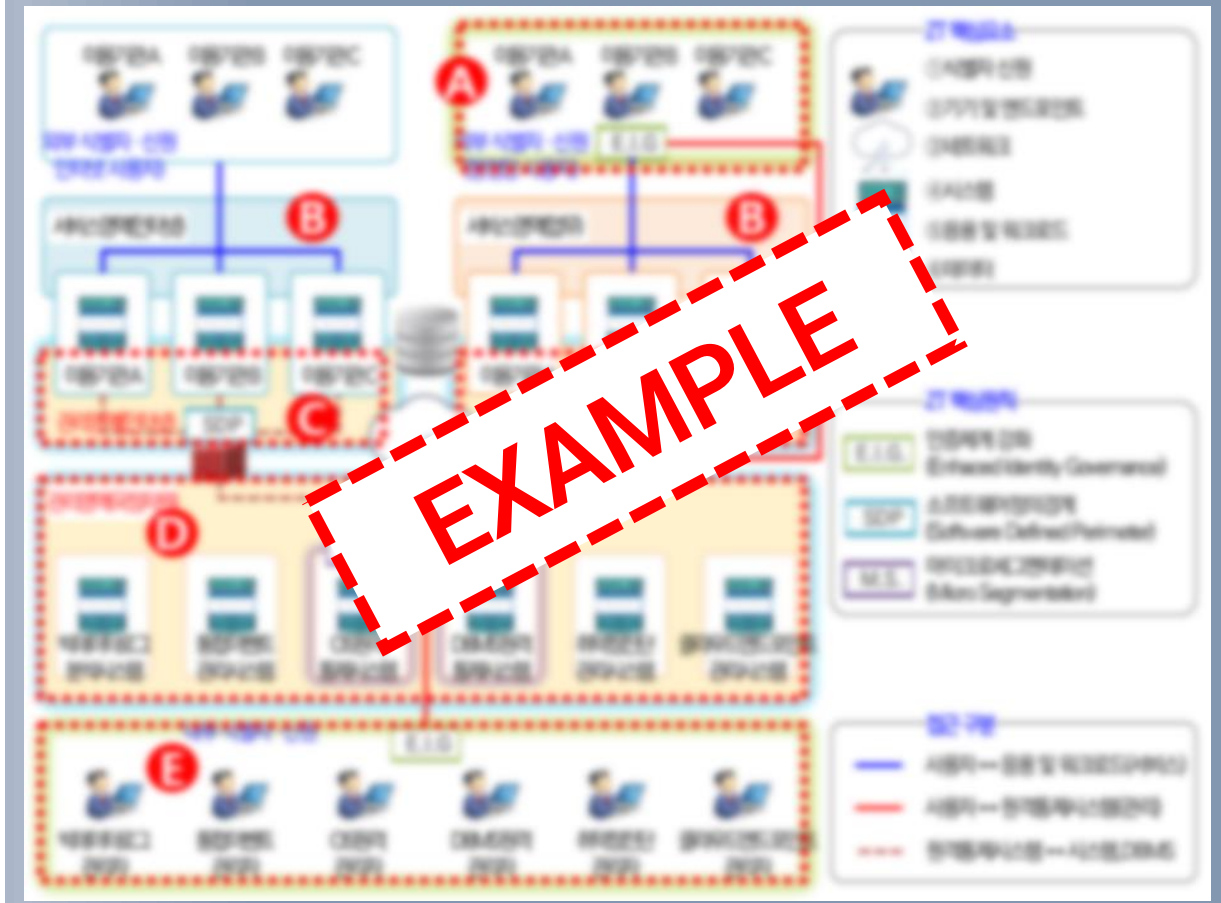
2. 사업 수행 내용_적용범위 및 대상 식별(AS-IS)

사업 착수 단계

❖ 본 사업의 최종 목표를 고려한 대상 및 범위에 대한 현황 파악 및 정의
❖ 시범사업 관점에서 실 적용 대상은 수요기관과 협의하여 진행

※ 기관의 세부정보는 표기하지 않음

[국가정보자원관리원]

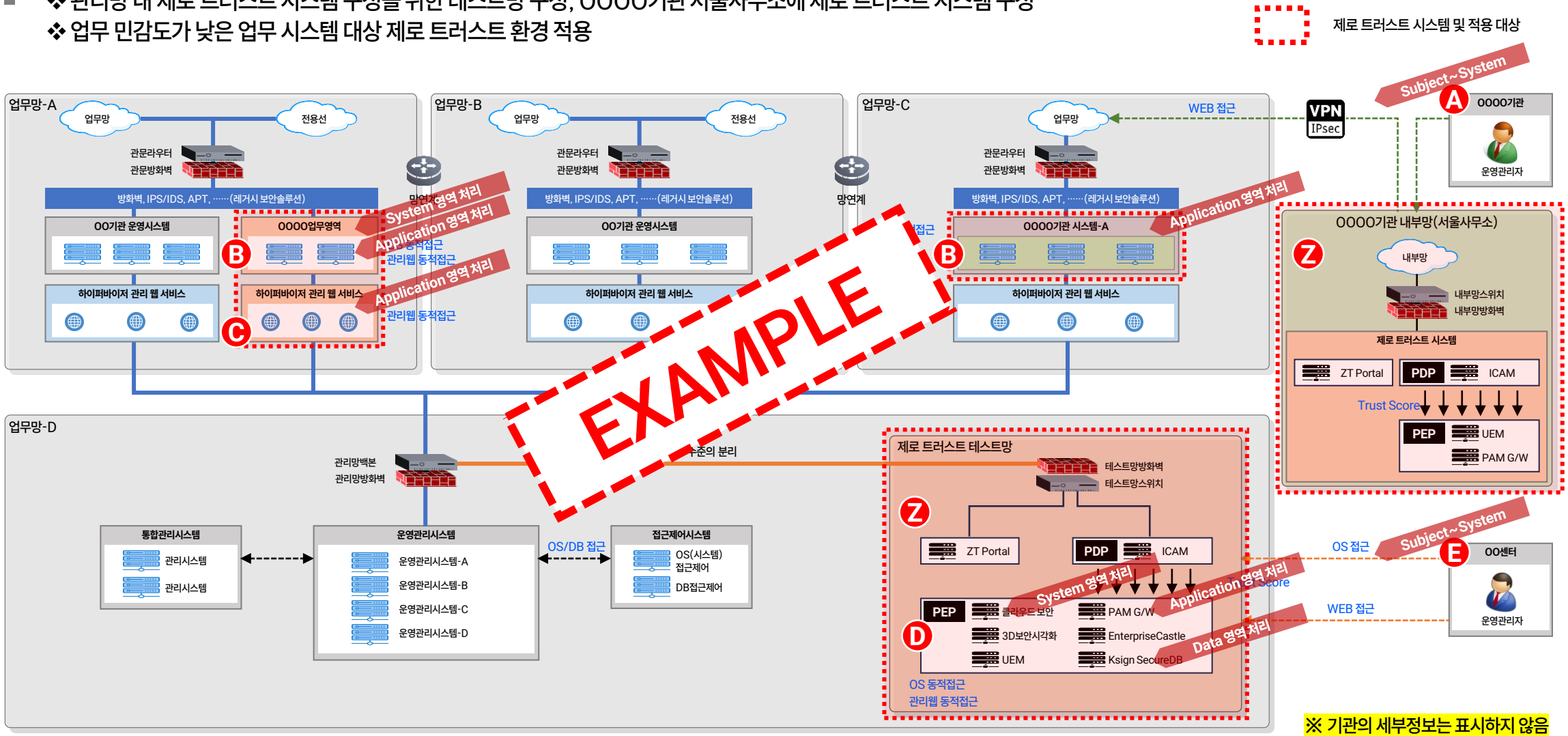


대상 영역	사용자 및 대상 서버	전체 수량	비고
A	• OO망 사용자	000명	OOOO기관
	• OO기관 운영관리자	000명	포함
B	• OO기관 가상서버	000대	OOOO기관 제로 트러스트 적용 일부 업무에 따라 대상 서버는 줄어듦
C	• OO센터 관리서버 (하이퍼바이저)	000대	
D	• OO센터 관리서버	000대	
E	• OO센터 운영관리자	000명	

2. 사업 수행 내용_시스템 구성 및 적용(TO-BE)

보안성 검토 결과에 따른 구성 및 대상의 변경

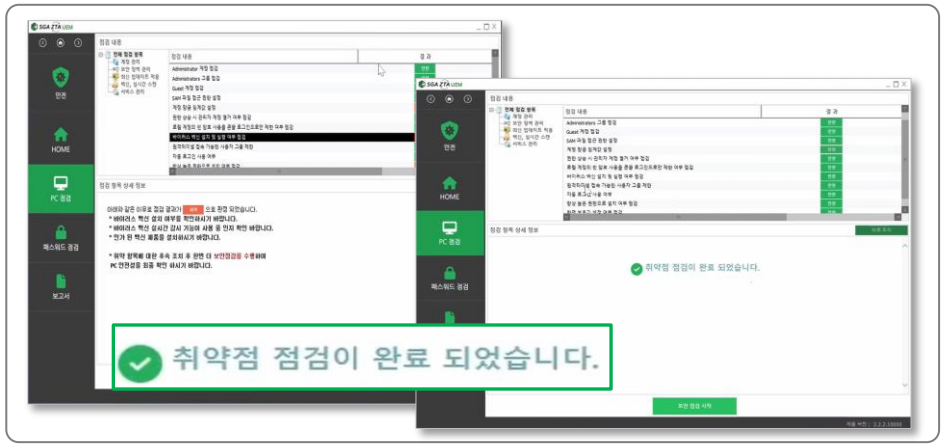
❖ 관리망 내 제로 트러스트 시스템 구성을 위한 테스트망 구성, OOOO기관 서울사무소에 제로 트러스트 시스템 구성
❖ 업무 민감도가 낮은 업무 시스템 대상 제로 트러스트 환경 적용



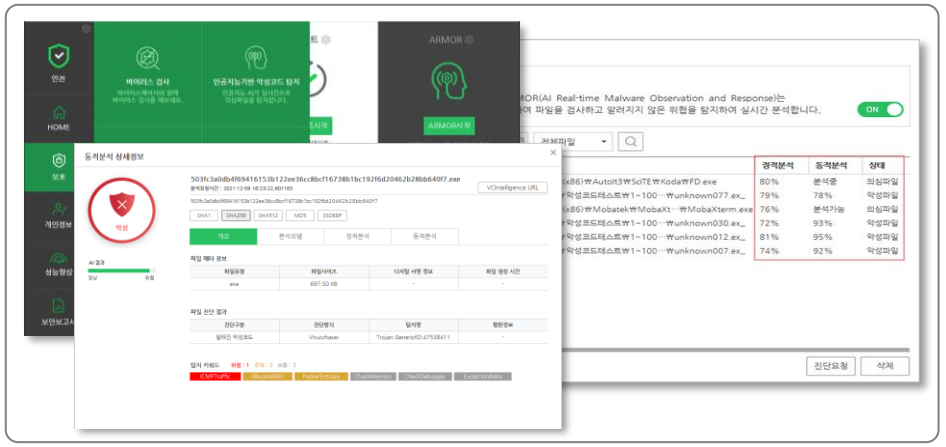
3. 솔루션의 구성 _ 사용자/UEM

- 엔터프라이즈 리소스로 접근하는 사용자 디바이스 통합 보안관리 및 보안성 검증
- 사용자와 기기의 통합 관리, 지속적인 보안 상태 관리를 통해 승인되지 않은 접근을 차단하여 보안을 강화

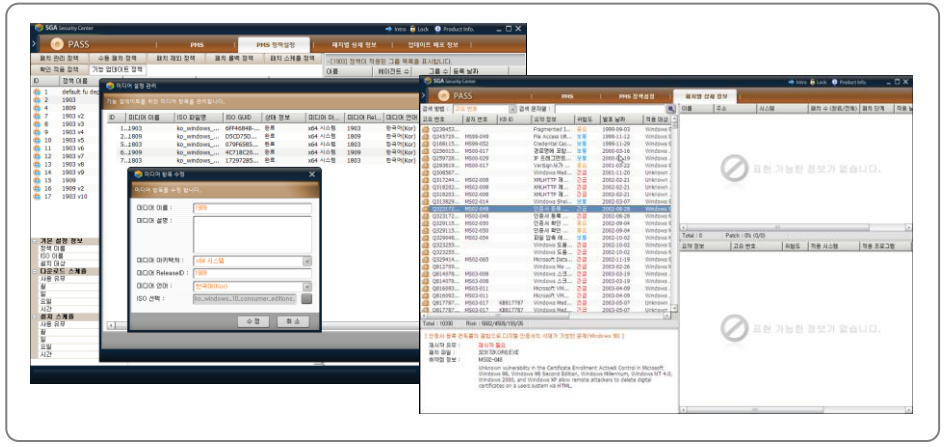
디바이스 위험도 평가



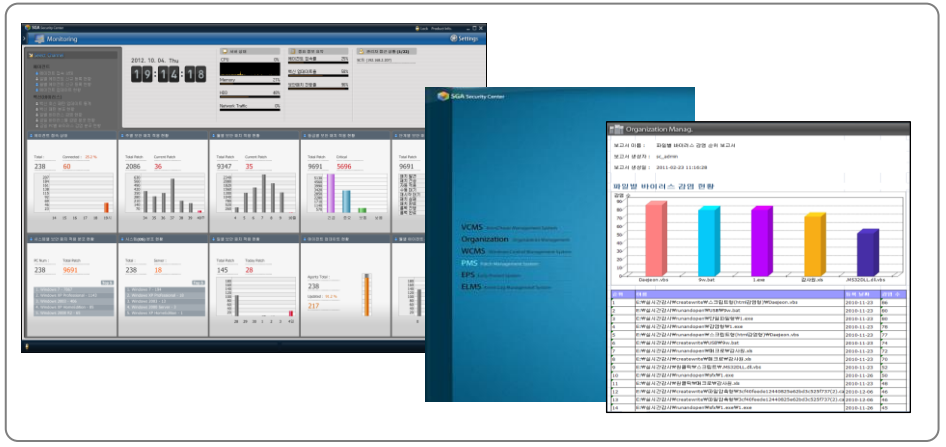
Anti-Malware



패치관리



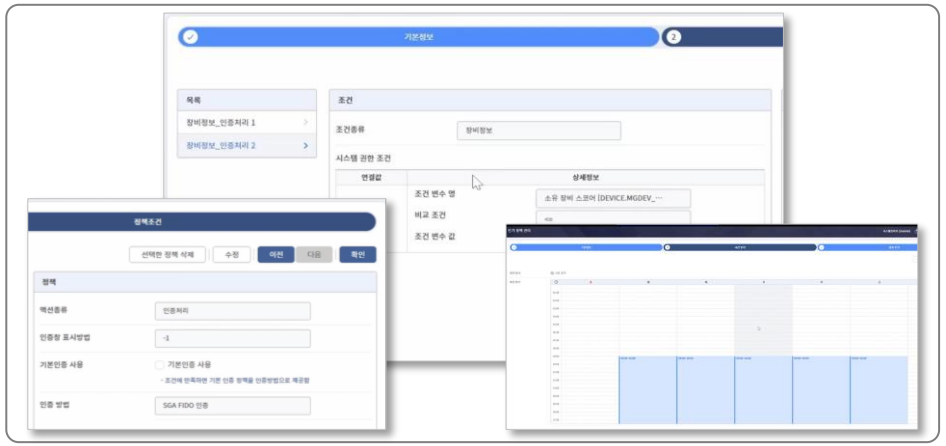
통합 모니터링/보고서



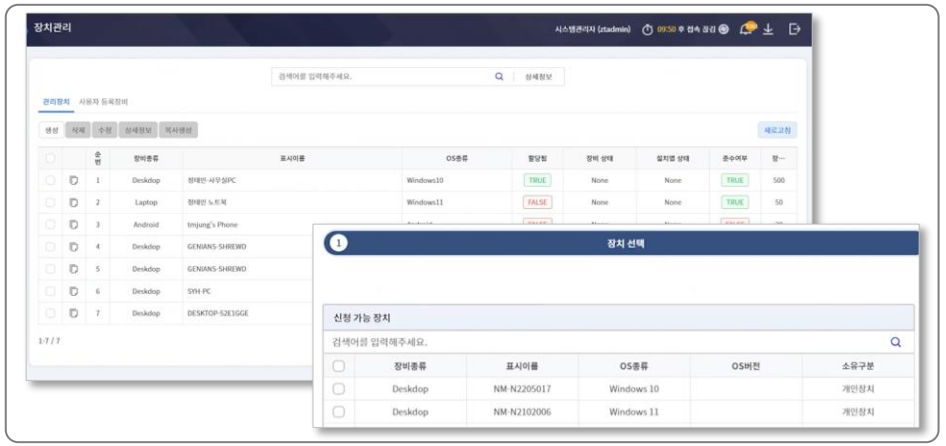
3. 솔루션의 구성 _ PDP/ICAM

- 엔터프라이즈 리소스로 접근하는 사용자/사용자 디바이스 인증, 정책 및 접근관리
- 신뢰할 수 있는 디지털 신원 확립과 체계적인 접근 통제를 통해 정보 보안을 강화하고 운영 효율성 향상

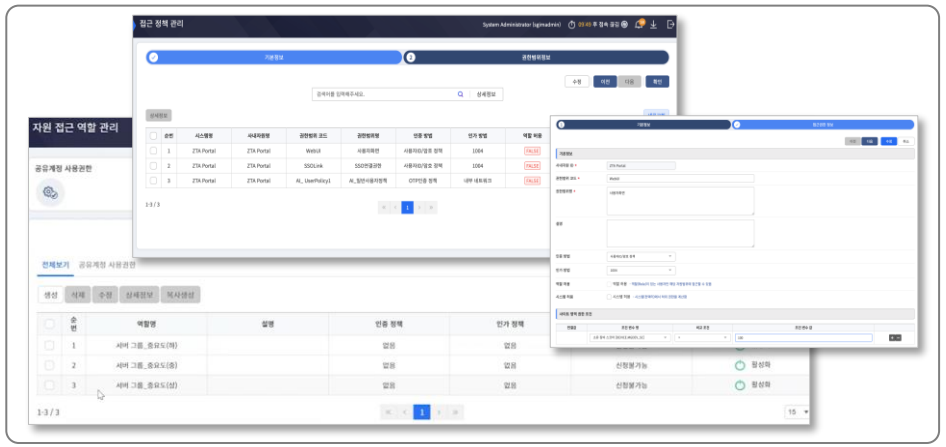
실시간 인증/인가, 지속적 유효성 검증



사용자 디바이스 보안성 실시간 확인



접근 대상 리소스 별 접근 정책 수립

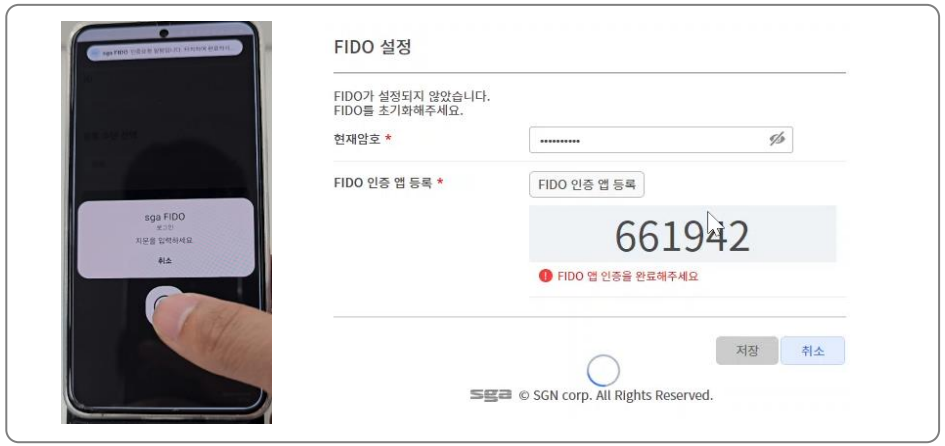


정책 수립 및 배포

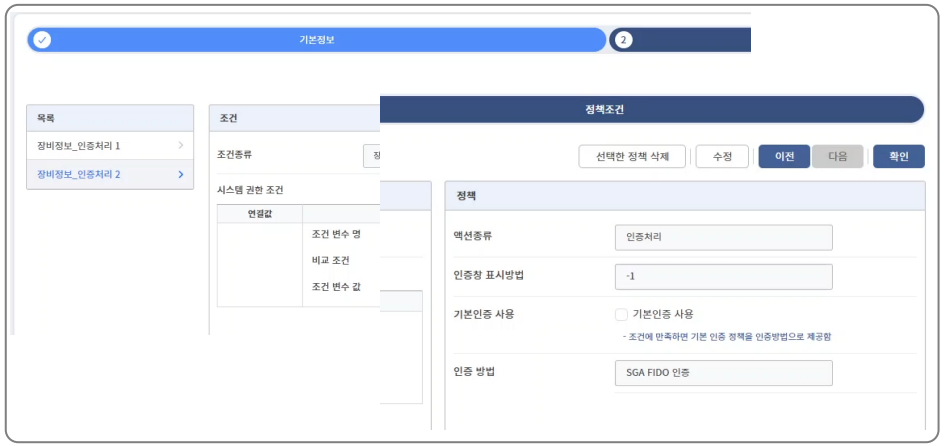
3. 솔루션의 구성 _ PEP/ICAM-MFA

- 제로 트러스트 시스템을 통한 보호 대상 리소스 접근 시 강화된 인증 체계 기반의 접근 제공
- FIDO, mOTP 등 다양한 인증 방식을 제공함으로써 신뢰 점수에 따른 동적 인증 시 강화된 인증 체계로 사용

FIDO 등록 및 인증

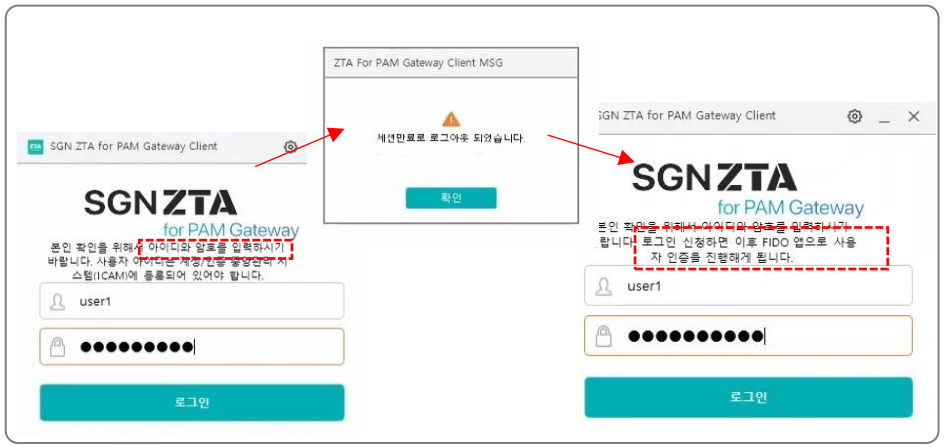


신뢰 점수에 따른 인증 정책 설정



mOTP 등록 및 인증

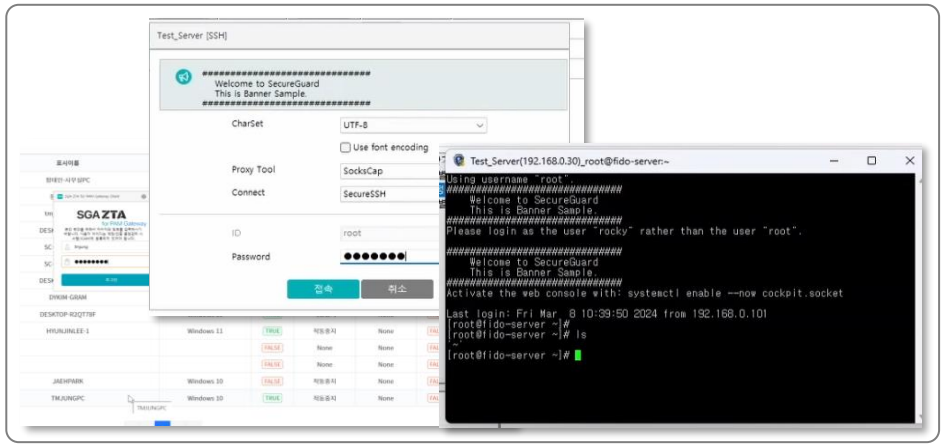
PEP 접근 동적 인증 절차



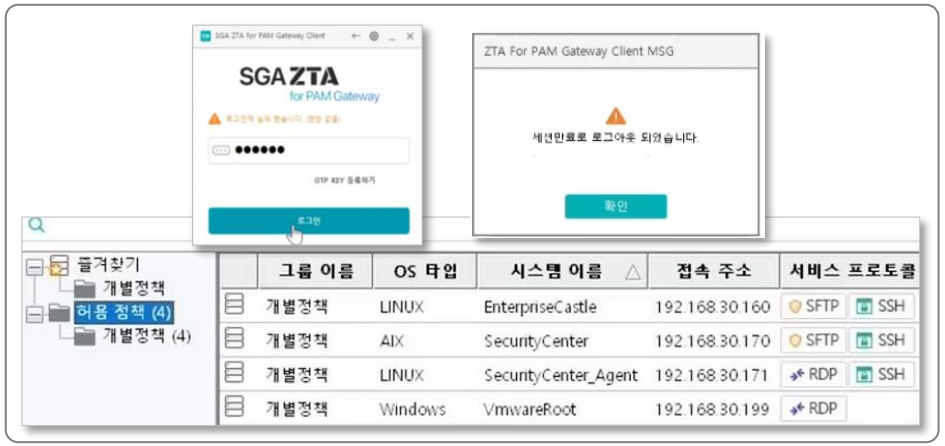
3. 솔루션의 구성 _ PEP/시스템, 어플리케이션

- 엔터프라이즈 리소스(시스템)로 접근하는 사용자/사용자 디바이스 보안 상태 지속적 검증 및 접근제어
- 강화된 인증, 접근통제, 감사기능을 통해 주요 시스템에 대한 안전한 접속과 행위통제를 수행하여 보안을 강화

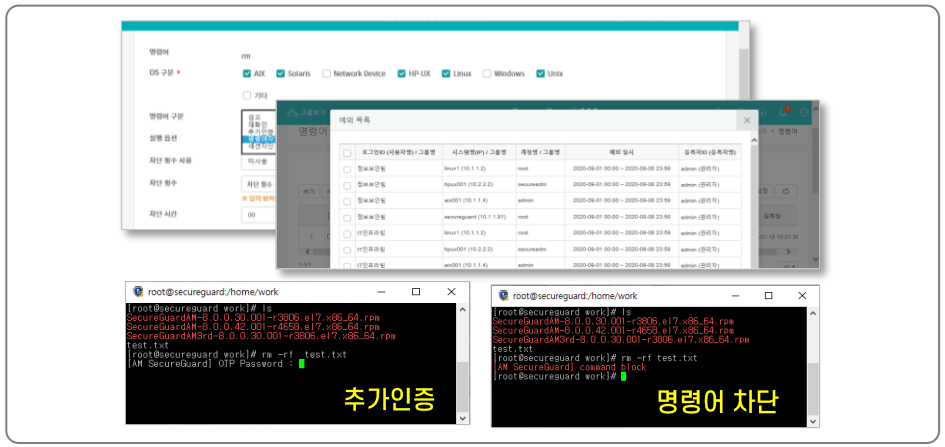
시스템 접근제어 G/W, 특권 접근 관리(PAM)



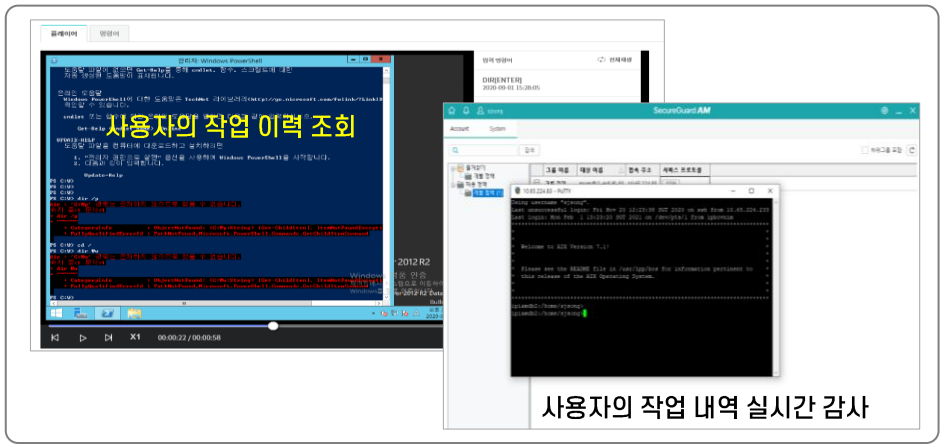
시스템 동적 및 세분화 접근제어



명령어 실행 통제



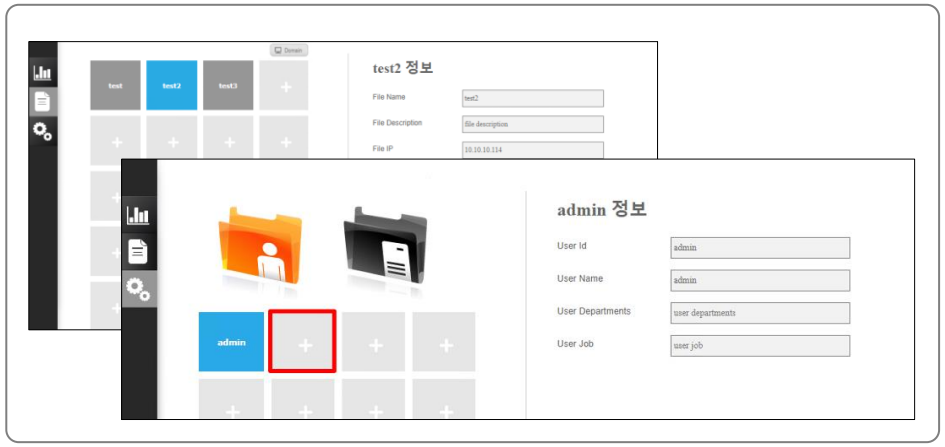
원격작업 로그/실시간 모니터링



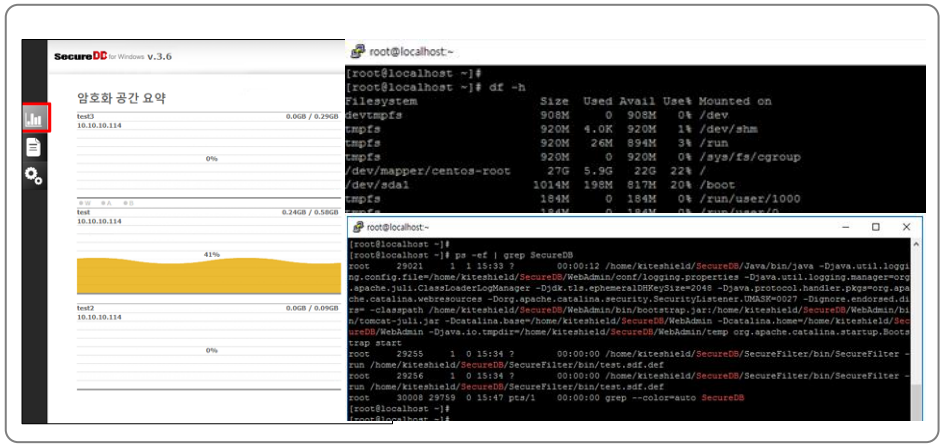
3. 솔루션의 구성 _ PEP/데이터

- 데이터 암호화 기반 데이터 영역에 대한 안전한 접근 등 보안 강화 제공
- 제로 트러스트 기업망 6대 핵심요소 중 하나로서 본 사업 수행에 충족

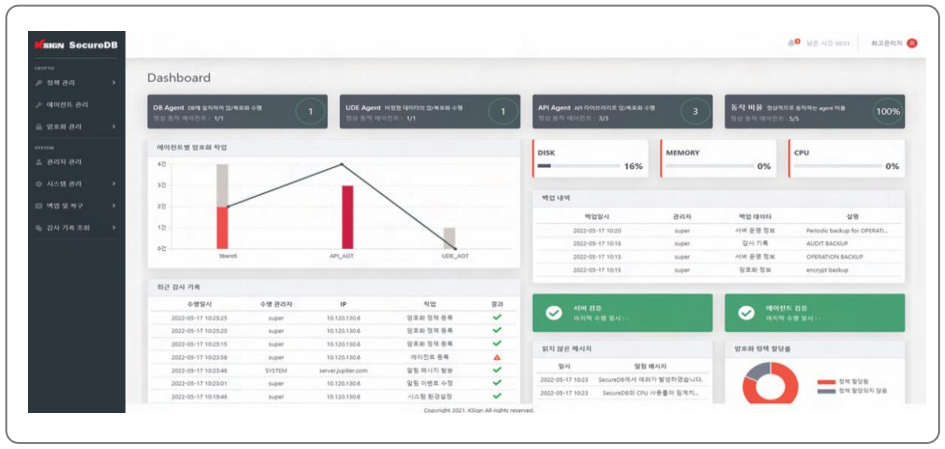
파일 및 접근 사용자 등 암호화 통합 관리



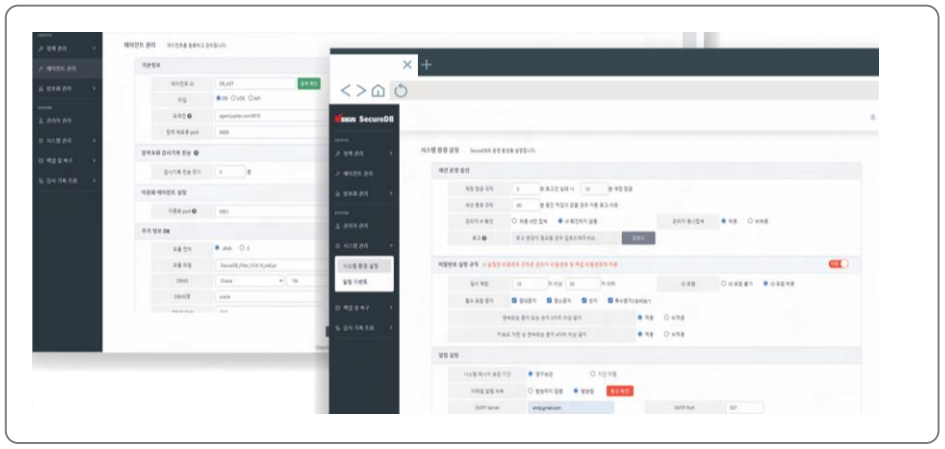
자원 점유율, 시스템 등 가용성 모니터링



DB 암호화 통합 모니터링



DB 암호화 정책 설정 및 관리

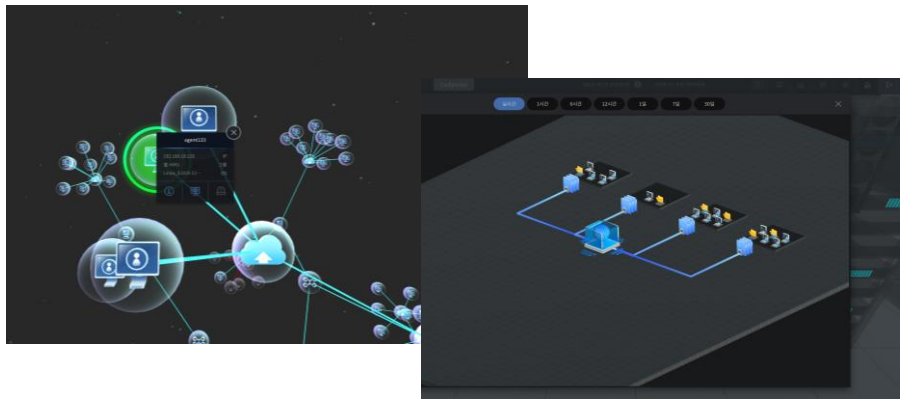


3. 솔루션의 구성 _ PIP/가시성 & 시각화

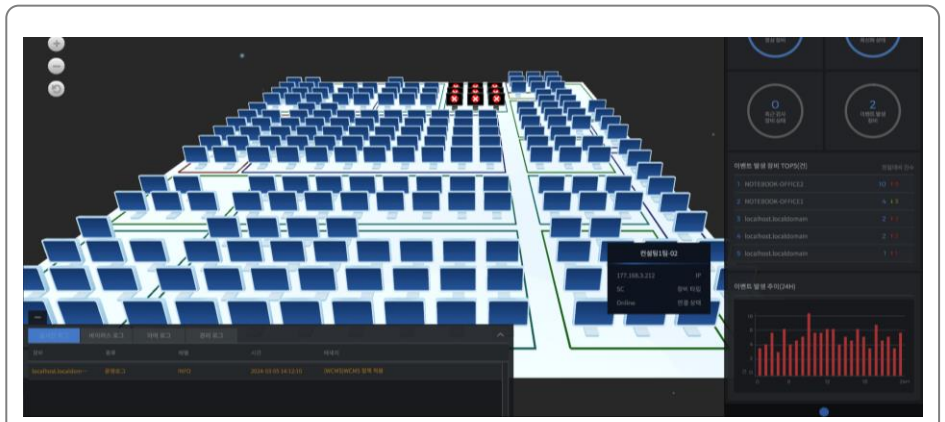
- PEP/PDP 로그를 수집하고 2D 및 3D 대시보드를 통해 보안 이벤트의 가시성을 제공
- 보안 로그를 수집/저장하고 시각화 대시보드를 통해 보안에 대한 가시성과 인사이트 강화 제공

통합 서버 환경 모니터링

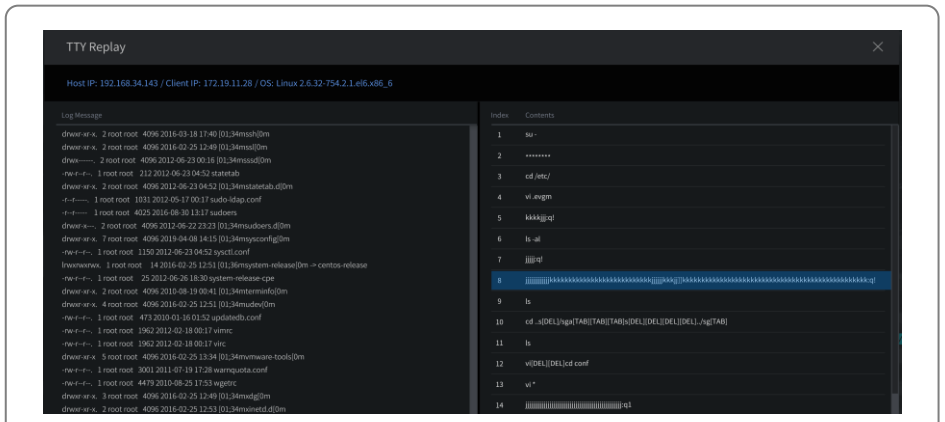
접속 네트워크/경로 추적 및 분석



엔드포인트 통합 모니터링



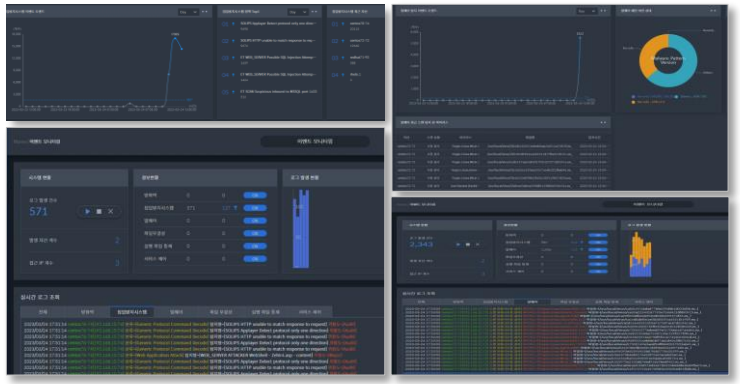
행위 재연



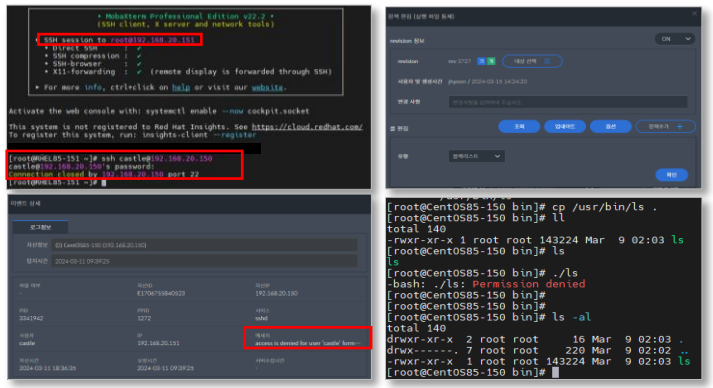
3. 솔루션의 구성 _ 마이크로 세그멘테이션

- 호스트 기반 IPS/Anti-Malware, 컨테이너 플랫폼 승인제어 등 제로 트러스트 환경의 리소스 보호 적용
- 클라우드 워크로드, 컨테이너, 서버, 애플리케이션 등에 대해 일관된 보안 정책과 접근/실행 통제 제공

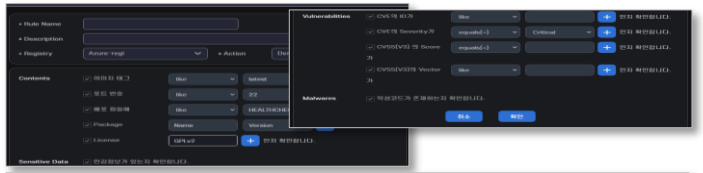
호스트 기반 IPS, 안티멀웨어



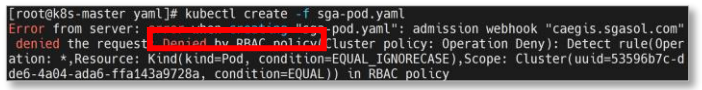
호스트 서비스 제어, 애플리케이션 통제



이미지 보증, 컨테이너 플랫폼 승인제어

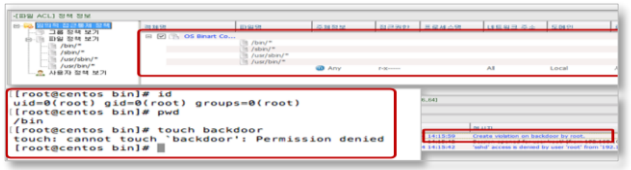


미보증 컨테이너 이미지 배포 제어

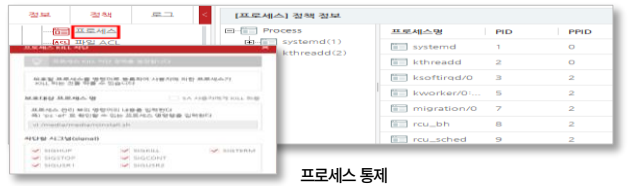


컨테이너 워크로드 실행 제어 - Operation(create)

(Agent based) PAM



파일/디렉터리 접근 통제



프로세스 통제

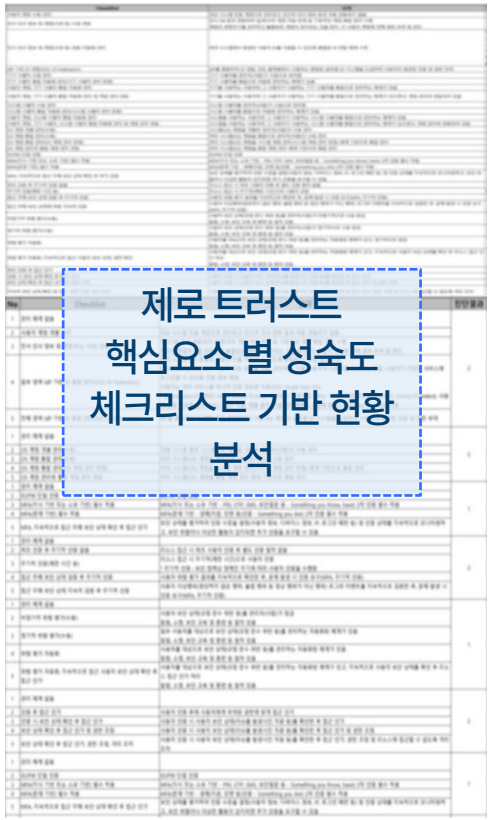
4. 효과성 분석 (1/2)

- ▢ 수요기관 대상 업무 서비스(또는 시스템)의 제로 트러스트 성숙도 현황을 파악하기 위해 성숙도 웹 다이어그램 모델 적용
- ▢ 컨소시엄 제로 트러스트 보안 솔루션 적용 시 대상 서비스(또는 시스템)의 목표 제로 트러스트 성숙도 도달 검증

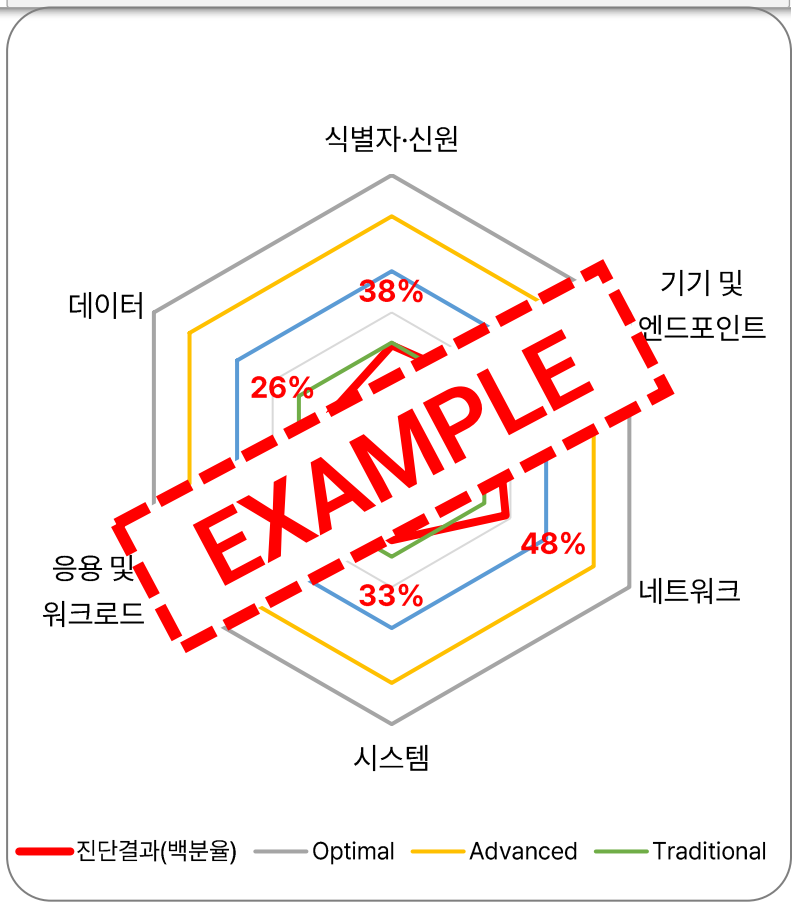
핵심요소	기능	세부기능
식별자·신원	식별자 관리 (Identity Management)	사용자 계정 관리 (User Account Management)
기기 및 엔드포인트	데이터 접근제어 (Data Access Control)	기기 접근 인가 (Device Access Authorization)
네트워크	암호화 (Encryption)	네트워크 트래픽 암호화 (Network Traffic Encryption)
시스템	접근 통제 (Access Control)	시스템 계정(OS) 인증 (System(OS) Account Authentication)
응용 및 워크로드	애플리케이션 보안 (Application Security)	애플리케이션 테스트 (Application Test)
데이터	가시성 및 분석 (Visibility and Analytics)	데이터 백업 (Data Backup)

~~~~~후략~~~~~

체크리스트



제로 트러스트 성숙도 현황 예시

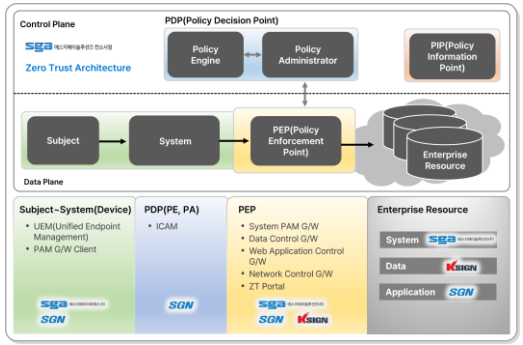

~~~~~

4. 효과성 분석 (2/2)

전문기관을 통한 모의해킹

❖ 전문인력 현장 투입을 통한 정확한 검증 수행
❖ 구현된 목표 보안 모델에 침투 테스트 수행으로 제로 트러스트의 성숙도 향상 현황 및 평가

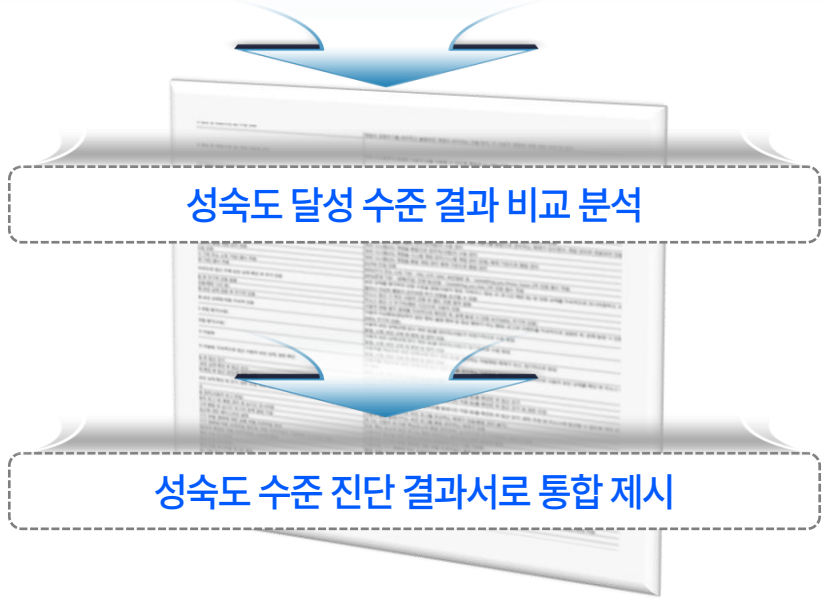
[국가정보자원관리원 제로 트러스트 시스템]



도입 모델 검증 및 결과 제시

유스케이스 도출 목록 기반 검증 테스트 분석

AS-IS	평가 결과 조치	TO-BE
• 달성하고자 하는 제로 트러스트 성숙도 목표 설정 • 제로 트러스트 6개 필러 영역에 대하여 성숙도 평가 진단 • 실제 효과를 검증하기 위한 모의 침투 테스트 수행 및 평가 결과 반영		• 제로 트러스트 성숙도 목표 달성 여부 확인 • 제로 트러스트 6개 필러 영역에 대하여 성숙도 재 평가 • 모의 침투 테스트 수행 결과에 대한 이행 점검



5. 기대효과 (1/2)

- ▢ 수요기관인 국가정보자원관리원 특성을 반영한 제로 트러스트 보안모델 도입 – “서비스형 제로 트러스트 보안모델” 기반 마련
- ▢ 제로 트러스트 6대 핵심 구성요소 최상위 단계 구현 목표 - 정부·공공분야 제로 트러스트 모델 도입의 모범 사례 도출

디지털플랫폼정부 도입 사례 확보

디지털플랫폼정부의 선제적 ZT 보안 체계 기반 마련

디지털플랫폼정부에 적합한 보안 모델 도입

- 전통적 보안체계(폐쇄형, 경계형)에서 **개방·공유환경에 적합한** 新 **보안체계(제로 트러스트)로 전환** 기반 조성
- **국가 핵심 인프라에 대한 사이버 복원력 강화**를 실현하는 제로 트러스트 보안전략 구현 방안 마련

전문 보안 기술 역량 총결집 목표 모델 구현

- 주관/참여기관의 국내 IT 보안 전문사업 및 기술 역량을 총결집한 **목표 제로 트러스트 보안 모델 구현 및 적용**
- 컨소시엄 전문기술이 적용된 솔루션으로 제로 트러스트 가이드라인의 **6대 핵심 구성요소 최상위 단계 구현 목표** 달성 가이드 제시

수요기관 특성을 반영한 보안 모델

정부 데이터센터 역할로서 ZT 도입 입주기관으로 ZT 모델 확장 용이

‘서비스형 제로 트러스트 보안모델’ 기반 마련

- 국가정보자원관리원 및 입주기관인 **공무원연금공단 대상** 제로 트러스트 모델 적용
- 민·관협력형 클라우드 사업자**(삼성SDS) 클라우드 플랫폼 대상** 제로 트러스트 모델 도입을 고려한 SECaaS 서비스 실증 방안 및 사례 기반 기술 지원

유연하고 안전한 제로 트러스트 모델 구현

- 국가정보자원관리원 및 입주기관 **모두가 활용할 수 있는 제로 트러스트 참조모델** 마련

모든 핵심요소를 포함하는 모델

구성요소, 핵심요소, 접근법, 성숙도 수준을 모두 준용한 모델

제로 트러스트 가이드라인 완벽 준용 모델

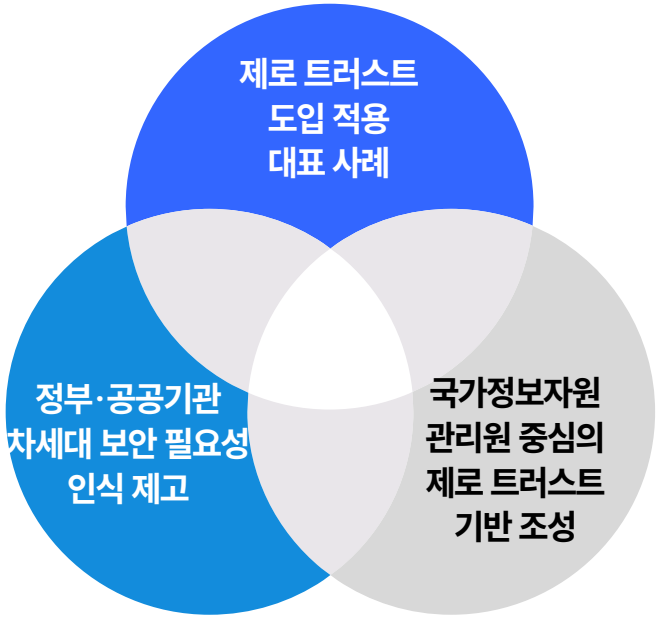
- 접근주체 Subject 부터 Enterprise Resource까지 **제로 트러스트 아키텍처의 모든 구성요소를 포함**한 구현
- 국내 제로 트러스트 가이드라인 1.0의 **6대 기본 원리, 6대 핵심요소, 3대 접근법을 모두 준용**한 모델의 구현

제로 트러스트 성숙도 GAP 분석 및 확대 체계

- 성숙도 모델 및 체크리스트 기반으로 컨소시엄 솔루션 적용 전·후를 비교할 수 있는 **ASIS-TOBE 분석 및 도입효과 도출**
- 현행 성숙도와 컨소시엄 솔루션 적용 성숙도 수준을 파악할 수 있는 **비교 분석 및 방향성 제시**

5. 기대효과 (2/2)

1 정부·공공기관 대표기관의 참여



2 IT 보안 산업의 활성화

- **산업 활성화** — 침체된 IT 보안 산업의 신규시장 형성 기여
- **수요 창출** — 패러다임 전환에 따른 수준진단 등 컨설팅 사업 수요 창출 효과
- **제도 개선** — 간담회, 포럼 등을 통한 제도 개선 활성화 기대

3 제로 트러스트 저변 확대

- **선도 기업** — 제로 트러스트 전문 기업의 역할 증대
- **연동 공조** — 관련 기업 간 연동/연계 기반의 공조체계 확립
- **사업 실효성** — 실증 기반의 사업 수행으로 실효성 있는 결과 획득

"제로 트러스트 보안모델 시범사업 결과를 토대로
정부·공공기관 **패러다임 전환 보안 생태계 조성** 기반 마련"

감사합니다!

SGA 에스지에이솔루션즈(주)