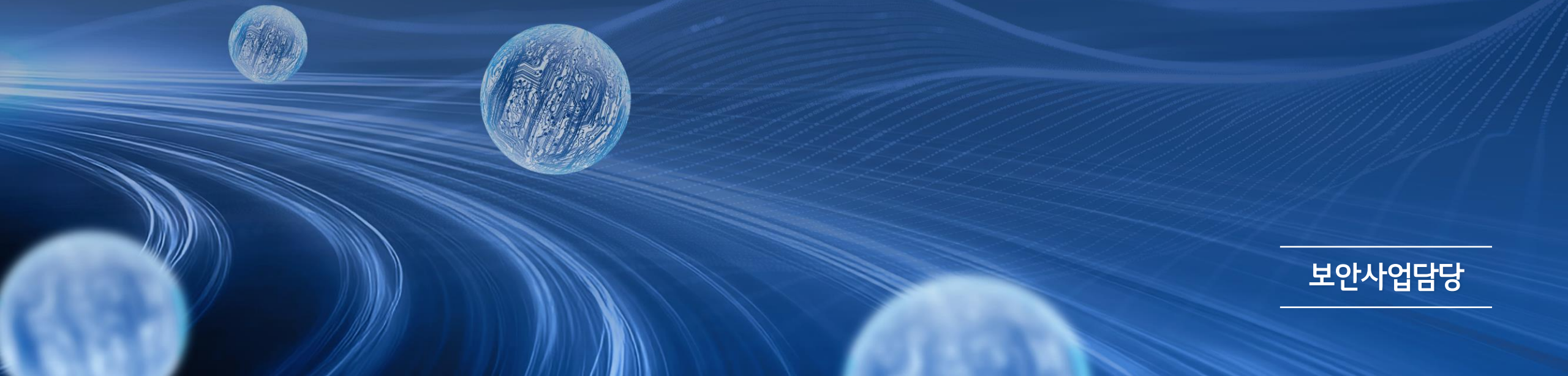
LG CNS

망분리 개선 로드맵과 제로트러스트 보안



보안사업담당

LG CNS

CONTENTS

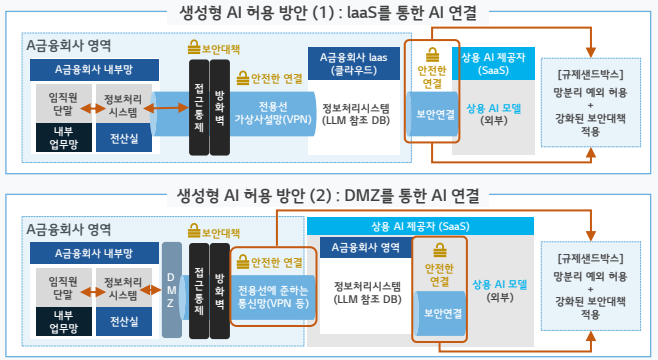
LG CNS

Ⅰ. 망분리 규제 개선 및 해외사례

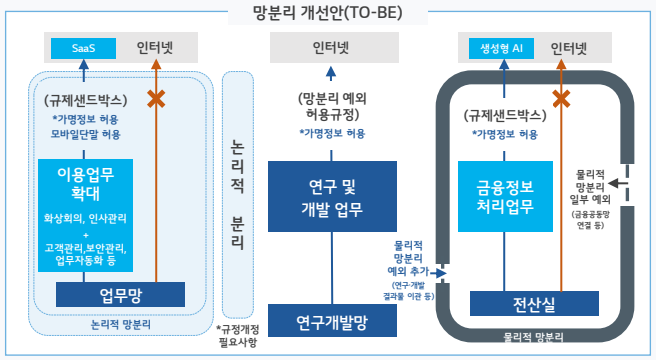
1. 변화의 배경

국내 망 분리 규제 개선 추진 「금융분야 망분리 개선 로드맵」 -2024. 8. 13.

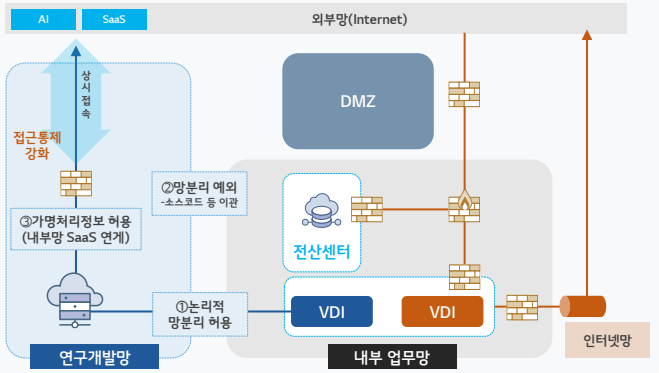
1.생성형 AI 활용 허용



2. SaaS형 응용 프로그램 활용도 제고



3. 연구 개발 분야 망분리 개선



국가 망 보안체계 보안 가이드라인 (N²SF) 금융망 로드맵과 유사, 현실적대안 ZT

<부록2, 모델 해설서 목차>

❶ 인터넷 단말의 **업무활용성** 제고
❷ 업무환경에서의 **생성형AI**활용
❸ **외부 클라우드** 활용 업무협업 재개
❹ **업무단말**의 인터넷 이용
❺ 공공 데이터의 **외부AI**융합
❻ **연구목적 단말**의 신기술 활용
❼ 개발 환경 **편의성 향상**
❽ **클라우드** 기반 통합문서체계

LG CNS

2. 시사점

개선된 규제를 적극 활용하기 위한 보안대책은 필수

IP기반에서 ID기반 통제로 변경, 인증강화 및 접근통제

생성형 AI 및 SaaS 이용 규제특례 보안대책 ('24.8) | 금융분야 망분리 개선 로드맵 ('24.8)

생성형 AI 활용 허용

- AI 서비스별 생성형 AI 사용 목적, 데이터 범위 등에 따라 보안 수준을 정의하기 위한 판단 기준 수립 필요
- 생성형 AI 활용을 위한 보안정책 수립, 금융보안원 실사 대응 및 이력 관리

SaaS형 응용 프로그램 활용도 제고

- SaaS 이용 목적, 활용 범위 등에 따라 보안 수준을 제시하기 위한 판단 기준 정의 필요
- 단말기 / SaaS 연계 / SaaS 관리 / SaaS 운영정책 보안대책 수립 필요
- 단말기권한관리, MDM, MFA, 전송구간암호화, 가명처리 등 솔루션 확대적용 및 정책 고도화

연구 개발 분야 망분리 개선

- 연구개발망의 VDI 허용에 따른 ID기반 보안정책 및 아키텍처 수립 필요
- VDI를 통한 별도망 접근 구성은 이미 활용 중, 하지만 정책 고도화 필요
- 사용자인증, 데이터 암호화, 접속 통제 등 구체적인 보안정책의 현실화 필요

지금까지는 규제대로 적용 및 심사, **지금부터는 자율보안 역량 강화 및 책임**

ZeroTrust 아키텍처로 전환 준비 필요

3. 해외 금융 기관 및 회사 사례

국내 당국의 규제 개선 방향과 유사

인증강화 및 접근통제 중심의 제로트러스트 아키텍처로 전환 중

공개 AI 사용 금지	• 미 금융기관은 ChatGPT와 같이 인터넷에 **공개된 AI 사용을 금지**하고 있음 • 전용 AI를 구성하여 **데이터**가 외부로 나가지 못하도록 **통제**하고 있음
SaaS 사용 허용	• M365 등 SaaS형의 다양한 기능을 가진 서비스, 솔루션 사용 가능. 단, **인터넷으로 정보가 공개되는 경우는 제외**. • SaaS 서비스 제공자가 미국(America)에 Region을 제공하지 않더라도, **미국의 규제를 준수** 필요 • 금융기관/감독기관은 규제준수관련 보고서 요청
Private Cloud 환경 구성 가 추세	• 미 정부는 상당 수 **Private Cloud 환경**을 구성한 것으로 파악됨 • **미 금융권은 약 30% 정도** 클라우드 환경 사용, 주요 시스템의 경우 On-premise 환경 유지 • AWS, GCP, Azure 등 Public Cloud 기반의 **금융기관용 Private cloud** 구성
제로 트러스트 보안 아키텍처 전환	• 미국 **정부기관은 ZT**를 도입하도록 강제화하고 있으며, 금융 등 민간 기업은 대상이 되지 않음 • 금융기관도 미 정부기관을 참고하여 **제로 트러스트 보안 아키텍처 전략 수립 및 전환 진행 중** • 사용자와 단말의 **강화된 인증**을 통한 네트워크 **접근통제**를 중심 • 모든 사용자는 **"외부"에서 접근한다는 개념**으로 단계별 전환을 진행하고 있음

3. 해외 금융 기관 및 회사 사례

A사례

제로 트러스트 아키텍처 전환 1단계 완료('21~)

- **사용자 계정 및 단말 관리**
  - On-prem에서 Cloud 기반 계정/단말 관리로 전환 진행 중
  - 로컬 PC의 데이터는 클라우드 백업
  - 단말 이상징후 발생 시 초기화
  - 생체인증 솔루션을 통한 OS 인증 강화
  - Risk 탐지 또는 관리자 등 특수권한 접속 시 추가 인증 필요
- **네트워크 접근통제**
  - On-prem과 Cloud 환경 구성 모두 논리적 망 분리 구성
  - SASE 기반 네트워크 접근통제
- **데이터 관리**
  - 문서단위의 데이터 등급분류
  - 문서 생성자가 등급선정을 위한 결제 진행
- **기타**
  - M365 기반 생산성 도구 및 보안 솔루션 사용

B 사례

제로 트러스트 아키텍처 전환 진행 중(3년 계획)

- **사용자 계정 및 단말 관리**
  - 계정 이외 추가 인증은 Hardware 인증서 사용
  - 모든 Endpoint (단말기, 서버, Backbone 등)에 EDR을 설치
  - 특정 시스템 접근시 Secure Enterprise Browser 이용 강제화
  - 위험 등급이 높은 업무시 Special Laptop으로만 접근강제화
- **네트워크 접근통제**
  - Lateral movement 방지를 위해 Proxy 기반 네트워크 마이크로 세그멘테이션 설계
  - NDR 을 이용한 트래픽 탐지
  - 단말별 접근이 가능한 서비스와 시스템을 지정해 접근통제
  - 지정 서비스 외 접근 시도 시 즉시 차단 및 조사 진행
  - SASE 도입 예정
- **데이터 관리**
  - 클라우드 데이터는 모두 암호화하고 Key는 On-prem에 보관

LG CNS

II. 망분리 규제 개선 대응사례

LG CNS

II. 망분리 규제 개선 대응사례

1. 생성형 AI 활용 허용

1. 생성형 AI 활용 관련 대응사례

금융 망분리 및 생성형 AI 관련 컴플라이언스 기반 AI 서비스 개발 단계 및 구성요소 별 보안통제 요건을 식별 및 관련 보안 솔루션, 서비스 조사

금융 컴플라이언스 분석

금융분야 AI 개발 활용 안내서 ('22.8)

- 「금융분야 AI 가이드라인」을 구체화한 세부 안내서
- 실제 AI 서비스를 개발·운영 시 체크리스트

금융분야 AI 보안 가이드라인 ('23.4)

- 금융권에서 사용하는 A) 서비스의 안전한 활용에 필요한 사항을 안내
- 금융회사 AI 활용 시 안전성 향상

금융분야 망분리 규제 로드맵 ('24.8)

- 금융회사 등의 생성형 AI 활용 허용 및 클라우드(SaaS) 이용 범위 대폭 확대
- 자율보안-결과책임 원칙으로의 규제 선진화 방향 제시

생성형 AI 및 SaaS 이용 규제특례 보안대책 ('24.8)

- 규제 샌드박스 신청기관의 자체 보안대책 수립 및 이행 지원을 위한 참조사항 제공

보안통제 요건 식별

AI 서비스 개발단계

AI 모델 개발	• AI 모델 도입 또는 개발 시 보안통제 • 학습데이터/참조데이터 및 생성형 AI 모델 보안관리 등
AI 서비스 구축	• AI 서비스 구축 시 보안통제 요건 • 클라우드, AI 관련 컴플라이언스 및 전자금융감독규정 보안요건 포함
AI 서비스 운영	• AI 서비스 운영 시의 보안통제 요건 • 정기적 AI 모델 취약점 점검, 사용자 프롬프트 로그 분석 등

AI 서비스 구성요소

데이터	• 학습데이터 및 참조데이터 관련 형상관리, 개인정보 보호 등
AI 모델	• AI 모델에 대한 적대적 공격 방지, 모델 강건성 확보 등 보안요건
AI 서비스	• AI 서비스 개발 시 입출력 데이터, API, 오픈소스 SW 등 보안요건
인프라	• AI 서비스를 운영하기 위한 서버, DB, 네트워크 인프라 보안요건

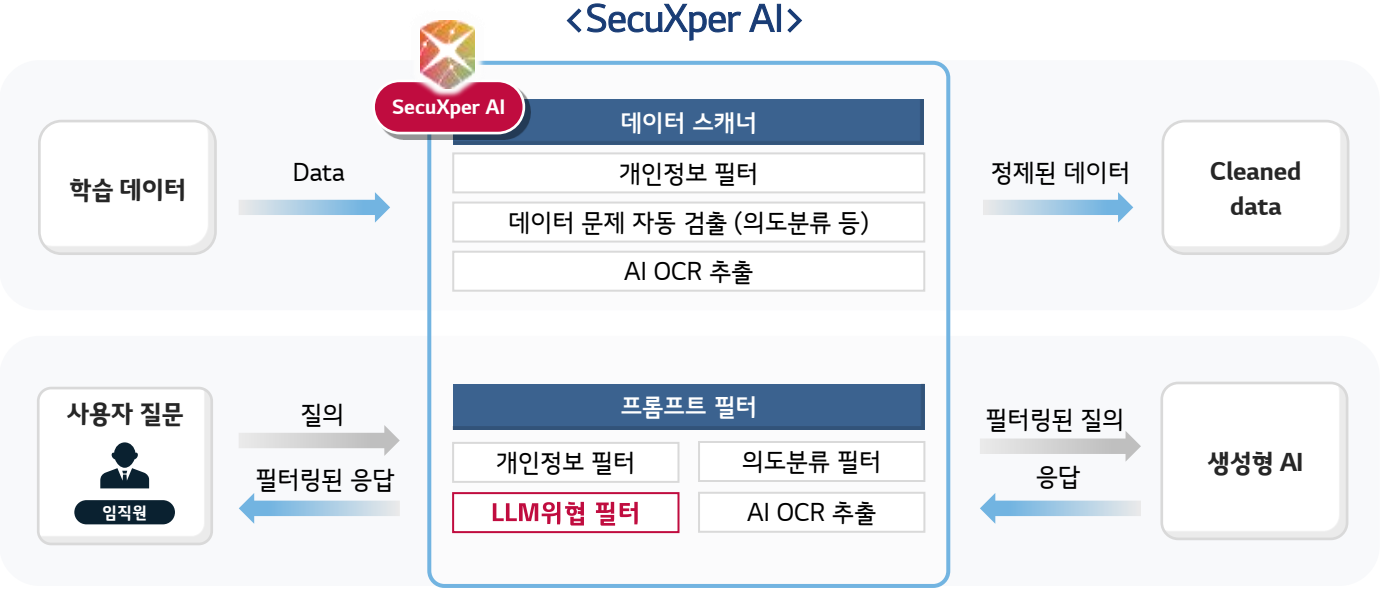
보안 솔루션/서비스 조사

보안통제요건	CSP Native
사용자 접근권한	AWS / Azure / GCP
이용 내역 로깅	
저장 내역 암호화	
개인정보 비식별화	
Prompt Filter	
중요정보 유출 방지	
계정 관리	
접근통제	
네트워크 보안	
보안 로그 수집	
클라우드 연계	
암호화 / 키 관리	
보안 모니터링	

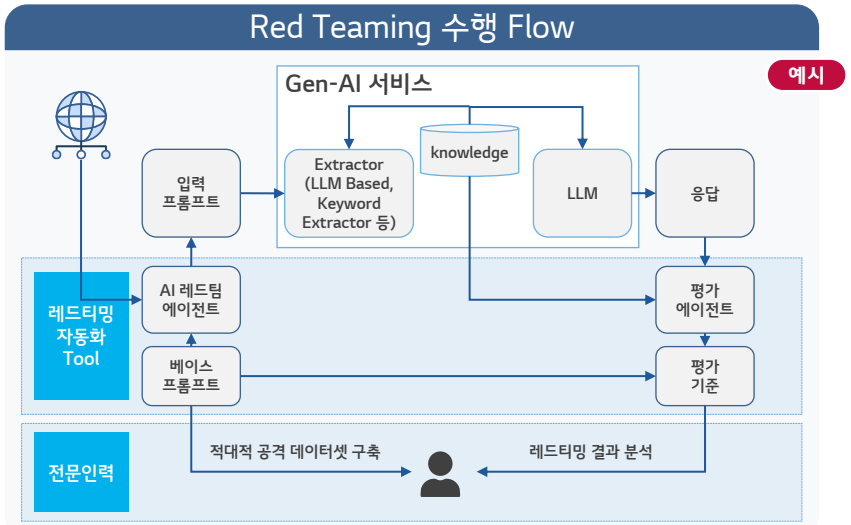
2. 생성형 AI 활용 규제샌드박스 대응 사례

다수 금융사 대상 생성형 AI 및 SaaS 이용 규제특례 관련 보안대책 대응 중
프롬프터필터, 개인정보비식별화 등 대응용 SecuXper AI 솔루션 적용 및 금융보안원 대응중

<SecuXper AI>



<Red Teaming>



규제샌드박스 점검항목

<AI 모델 보안성 검증 주요내용>

대분류	주요내용
❶ 데이터 오염 공격 대응	데이터의 무결성, 안전한 수집, 오염에 대한 대응 관련 사항
❷ 모델 오염 공격 대응	모델의 무결성, 안전한 모델 수집, 특수 모델 대상 공격 대응에 관한 사항
❸ 데이터 · 모델 추출 공격 대응	모델의 입·출력 관리, 민감정보의 관리, 데이터 및 모델의 추출 공격 대응에 관한 사항
❹ 회피 공격 대응	판단형, 생성형 AI에 대한 정상 동작을 방해하는 유형의 공격 대응에 관한 사항
❺ 적대적 공격 관리	적대적 공격에 대한 대응에 관한 사항

<혁신금융서비스 보안대책 평가 주요내용>

대분류	주요내용
1. 생성형 AI 운영 · 관리 보안 대책 (거버너스 포함)	생성형 AI 서비스의 운영과 관리에 관한 사항
2. 생성형 AI 모델 보안대책	생성형 AI 모델의 보안조치에 대한 이행 여부 관련 사항
3. 내부 단말기 보안대책 (모바일 단말 및 관리자 단말기 포함)	생성형 AI 서비스 관리에 사용하는 단말기에 대한 보안조치 이행에 대한 사항
4. 내부망↔외부 AI 모델 연계 네트워크 보안 대책 (암호화 등)	판단형, 생성형 AI에 대한 정상 동작을 방해하는 유형의 공격 대응에 관한 사항

LG CNS

II. 망분리 규제 개선 대응사례

2. SaaS형 응용프로그램 활용도 제고

1. SaaS 이용 규제특례 관련 보안대책 적용 사례

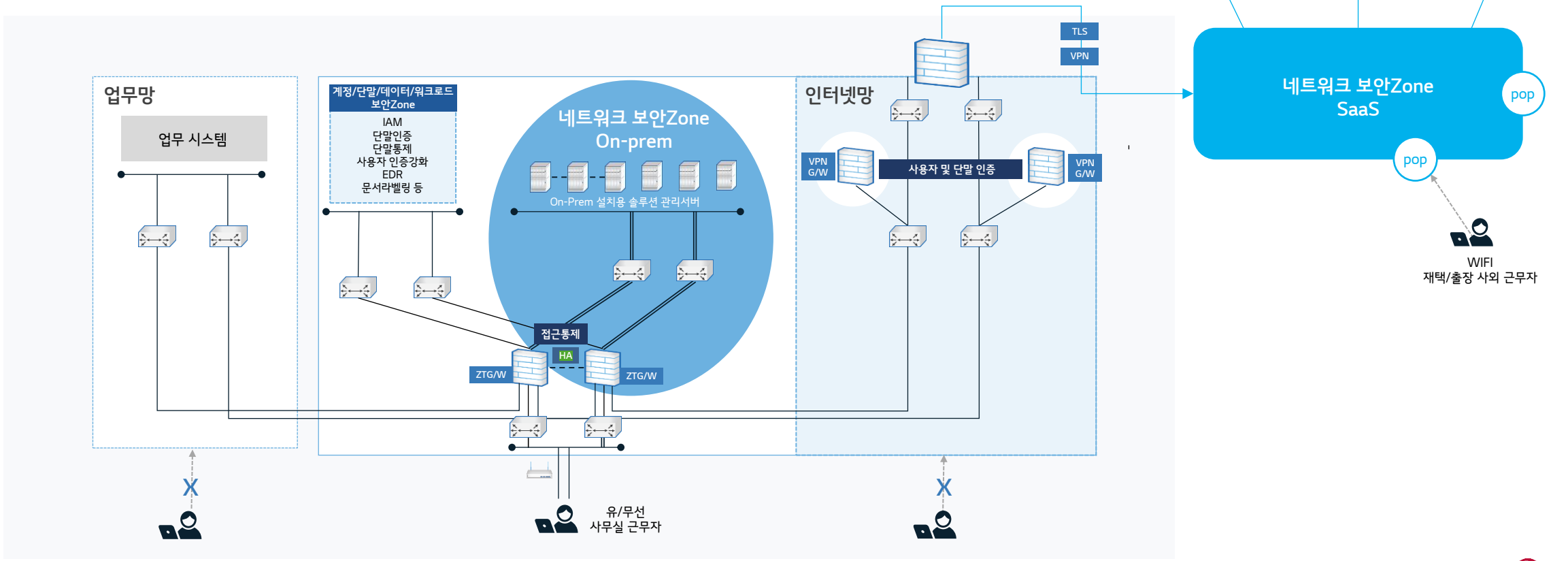
업무망에 SaaS 서비스활용을 위한 보안환경 구성 및 정책 검증 완료
단말기 / SaaS 연계 / SaaS 관리 / SaaS 운영정책 보안대책 수립

단말기 보안대책	통합인증	단말인증	AD계정 기반 계정관리, 단말 등록 및 인증
		단말통제	노트북, 모바일 이동형, 외장형 장치 통제, 소프트웨어 중앙배포, 원격초기화 등 단말 일관된 보안정책 적용 방안
		권한 상승	관리자 권한없는 단말에 대해 필요 시 권한상승 후 설정 변경 방안
		사용자 인증강화	사용자 인증 시 MFA 적용
	단말 이상징후탐지	EDR	단말에 랜섬웨어 등 다양한 침해행위에 대해 탐지 및 대응 방안
SaaS 연계 보안대책	네트워크	접근경로	네트워크 암호화 통신 및 단말 인증
		접근통제 및 탐지	사용자 인증을 통한 제로트러스트 기반 네트워크 접근통제
		웹격리	사용자가 웹브라우저를 통해 인터넷 사용시, 악성코드 다운로드 제한 등을 통한 사용자 기기 악성코드 감염 대응 방안
		SWG	사용자가 웹브라우저를 통해 인터넷 사용시, 유해, 비업무사이트 접근 대응 방안
SaaS 관리 보안대책	데이터보안	NDLP	개인정보 등 데이터유출 통제 방안
		EDLP	단말의 외장장치, 설치형 프로그램을 통한 데이터 유출 통제 방안
		문서라벨링	문서 보안등급에 따라 보안정책 차등 적용 방안
		문서암호화	문서 암호화 시 암호화 키 이중화 사용 방안
		포렌식	네트워크 트래픽 원본 저장을 통한 가시성 및 추적 감사 방안
		클라우드 데이터백업	클라우드 데이터 백업 방안
	통합보안	SIEM/SOAR	통합보안관제 및 자동화 대응

1. SaaS 이용 규제특례 관련 보안대책 적용 사례

업무망에 SaaS용 보안솔루션 적용 및 정책 테스트 구성도

- 인터넷과 3호 단말 통합, 인증 후 업무망과 인터넷망을 1대 PC로 이용하는 구성 검증 완료
- 통합된 1대로 업무망 접속 및 실업무 수행, 해당 단말대상 SaaS 서비스 이용을 위한 정책 적용 및 검증
- SaaS 이용 규제특례 가이드의 단말기 / SaaS 연계 / SaaS 관리 / SaaS 운영정책 보안대책 검증 수행



LG CNS

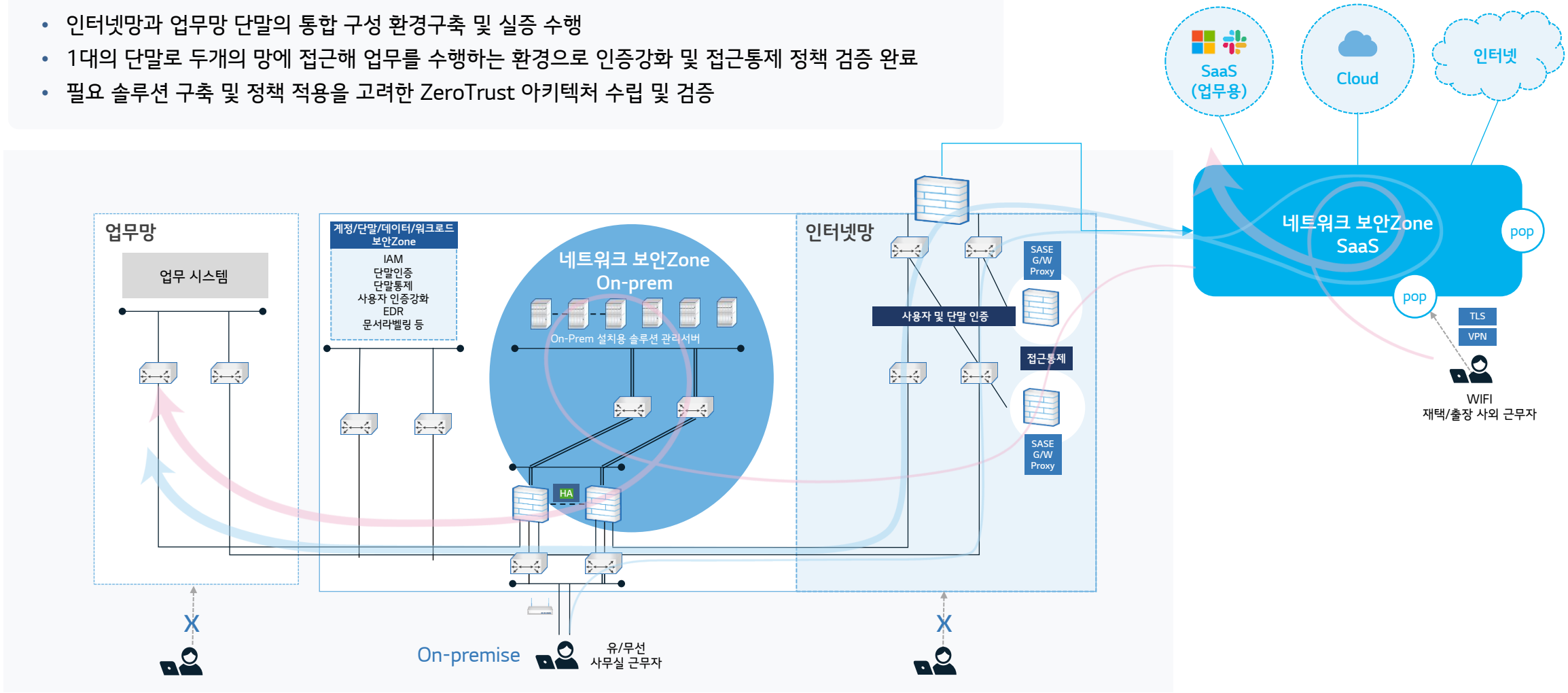
II. 망분리 규제 개선 대응사례

3. 연구 개발 분야 망분리 개선

1. 연구개발망 개선 관련 사례

On-Prem, SaaS, Hydrid 기반 ZeroTrust 아키텍처 검증

- 인터넷망과 업무망 단말의 통합 구성 환경구축 및 실증 수행
- 1대의 단말로 두개의 망에 접근해 업무를 수행하는 환경으로 인증강화 및 접근통제 정책 검증 완료
- 필요 솔루션 구축 및 정책 적용을 고려한 ZeroTrust 아키텍처 수립 및 검증



1. 연구개발망 개선 관련 사례

내부 정보 유출을 목적으로 C2, 내부자 관점의 다양한 시나리오의 모의해킹 점검

<취약점 점검 내역>

점검 방법	상세	예상 피해 시나리오
외부 비인가 단말 우회시도	VPN 기능을 통한 내부망 침투	• 유출 계정을 통한 한국은행 내부망 접근
DC서버 권한 획득	SMB 포트를 통한 원격 명령어 실행	• 주요 PC/서버의 쉘 획득 후 시스템 명령어 실행 • 악성프로그램(백도어) 설치 • 임직원 인증정보 획득 (NTLM Hash, 평문 패스워드 등)
c2 framework	악성코드를 이용한 임직원 PC권한 획득	• 내부 시스템을 장악하고 제어하여 조작 및 파괴 • 외부자에 의한 기밀 정보유출 • 악성코드나 랜섬웨어를 실행시켜 내부망에 확산 공격
정보 유출	외부로 내부 기밀 파일 유출	• 내부 임직원에 의한 정보유출 • 인증서 및 파일이 노출되어 추가적인 공격 가능

LG CNS

Ⅲ. LG CNS 망분리 규제 개선 대응 오퍼링

1. LG CNS의 규제 개선 대응 보안 아키텍처 수립 컨설팅

국내 망 분리 규제 개선 대응 컨설팅

- **규제개선 대응을 위한 보안 아키텍처 수립 컨설팅**
  - 현재 사용중인 솔루션 및 정책 기반의 제로트러스트 성숙도 평가
  - 단계별 고도화 방안제시 및 향후 필요 과제도출
- **새로운 보안 거버넌스 수립을 위한 전략과제 제시**

생성형 AI 활용 허용

- 생성형 AI 활용 서비스 대상 취약점 점검 및 증적관리
- 원본데이터 검증 및 프롬프터 입출력 값 필터링
- AI-Red Teaming 서비스
- 규제샌드박스 대응 지원

SaaS형 응용 프로그램 활용도 제고

- 업무망에서 SaaS 사용시 보안정책 수립
- 보안솔루션 및 아키텍처 검증
- 규제 및 가이드 기반 고도화 방안 제안

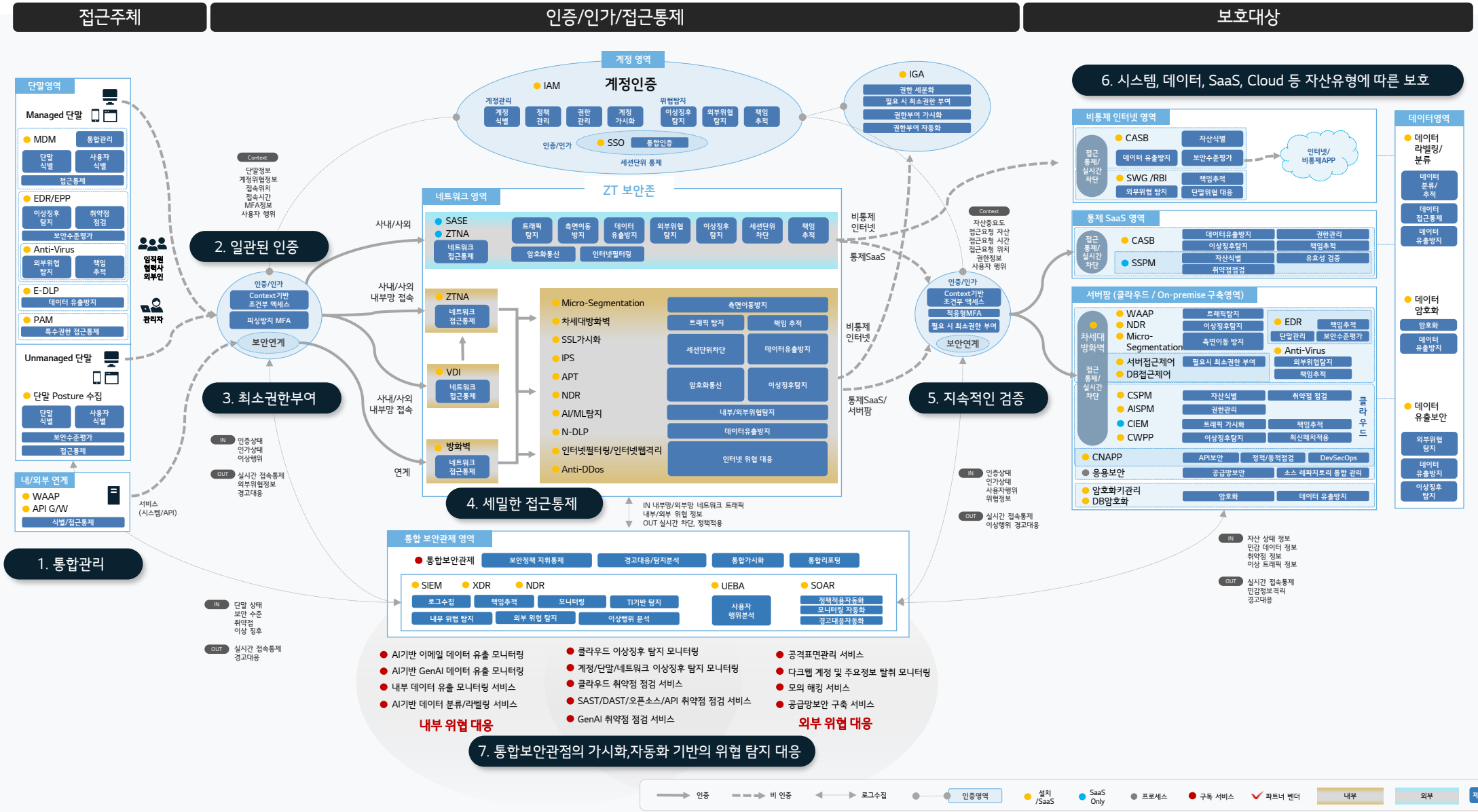
연구 개발 분야 망분리 개선

- VDI를 통해 연구개발망 접근시
- 데이터의 등급에 따른 차별 정책 적용 사례 확보, 정책안 제시
- 거시적 관점의 방향성 제시
- 정보 중요도 평가 사례 제시

2. LG CNS의 ZeroTrust 성숙도 평가모델

영역	항목수	항목	상세 내용	평가항목(예시)
❶ 계정	14	식별관리 접근통제 위험관리	계정 저장소, 인증 및 권한관리, 위험 평가	**사내 자원에 접속하는 계정을 식별하고 있는가?** 1)사용자계정 : 임직원, 협력사, 임시계정, 공용계정, 관리자 등 2)서비스계정 : API 등 시스템이나 서비스 및 솔루션에서 사용하는 계정
❷ 단말-접근주체	11		자산 관리, 접근통제, 규정준수 모니터링	**기기보안상태에 대한 Context 기반의 조건부 액세스가 적용되어 있는가?** - 기기 ID 상태 : 사용가능, 불가 (예 : 퇴사한 임직원에게 할당된 기기 접속 불가) - OS Version - 최신 보안패치 적용 여부 - 필수 SW 설치 여부 - 보안설정 활성화 여부 (윈도우 방화벽, 화면 보호기, 공유폴더 제거 등) - 악성코드 감염 여부 등 확인
❸ 단말-Infrastructure	11		자산 관리, 데이터 액세스, 규정준수 모니터링	**인프라 자산의 규정준수 측면에서 주기적인 취약점 점검을 하고 있는가?**
❹ 네트워크	12		네트웍 세분화, 위협 보호, 암호화	**네트워크별 신뢰영역으로 간주되는 영역 없이 접근통제 정책이 관리되고 되있는가?**
❺ 응용워크로드	14		접근 권한, 위협 보호, 접근성, 응용 보안	**SaaS, 사내 앱, 서비스, API 등 보호 대상 모든 응용 워크로드가 식별 되는가?**
❻ 데이터	7		목록 관리, 액세스 결정, 암호화	**데이터 분류정책이 마련되어 있는가?**
❼ 가시화 자동화 거버넌스관리	27	거버넌스, 가시화, 자동화	공통, 계정, 단말-접근주체, 단말-Infra, 네트워크, 응용워크로드, 데이터 ,계정, 단말_접근주체, 단말_infra, 네트워크, 응용워크로드, 데이터	**전사 접근통제 정책이 계정/단말/네트워크/응용워크로드/데이터 영역에 일관되게 적용되도록 지휘통제가 가능한가?** -각 항목별 보안정책과 통합되어 지휘통제가 가능하며, PaC로 정책을 관리하는 수준 ※ PaC(Policy as a Code) : 정책을 코드화하여 정책 표준을 만들고, 중앙 집중식 관리. CI/CD와 통합가능하고, 자동화 및 버전 관리, 불필요한 정책 생성 불가, Code의 신속한 대응 및 확장성 이점 활용 가능
	96			

3. LG CNS의 ZeroTrust 구성도



감사합니다