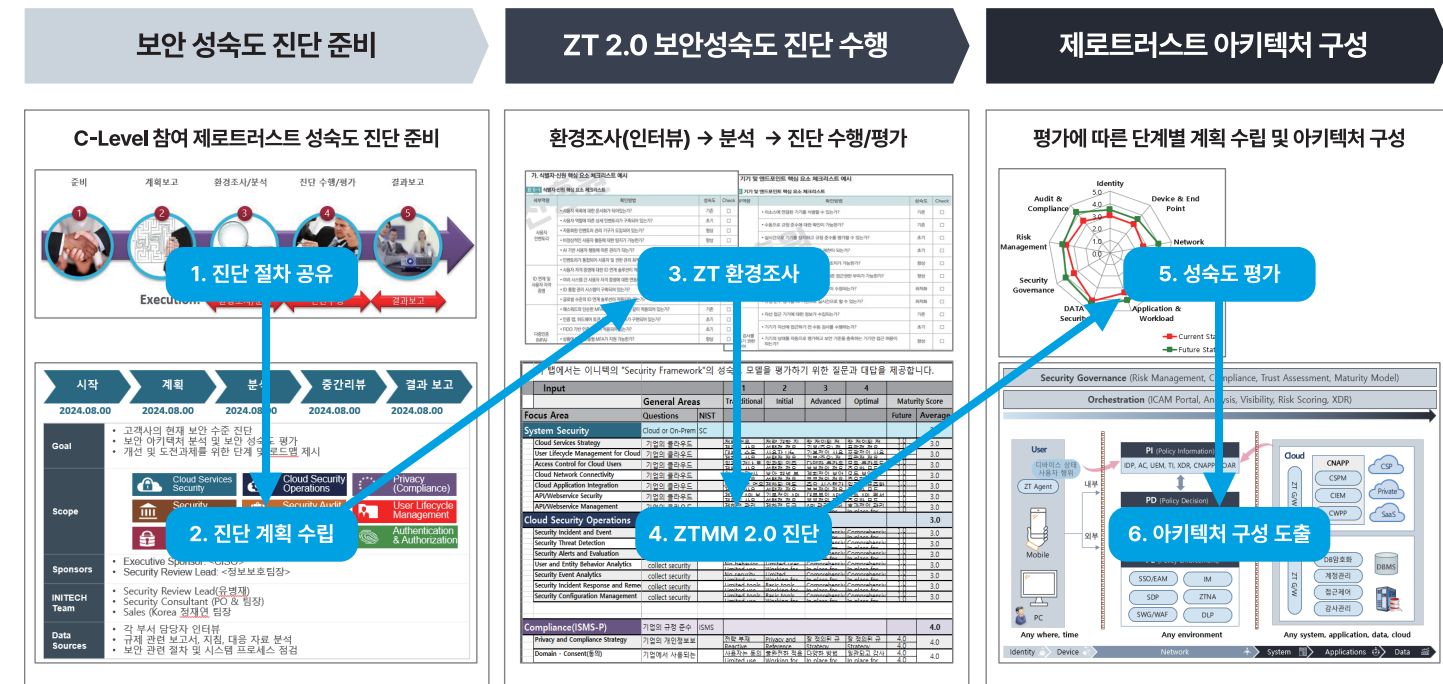


제로트러스트 진단

제로트러스트 성숙도 평가 방법론

제로트러스트 2.0 가이드 라인 기반 보안 성숙도 평가를 통한 아키텍처 구성안 도출



성숙도 평가(보안진단) 방법

1

ZTMM 2.0 기반 정밀 성숙도 진단

- ZT 가이드라인 2.0 및 Maturity Model 2.0을 기반으로 현재 보안 수준을 정량적으로 평가합니다.
- 기술, 정책, 운영 각 측면에서 정밀한 겹 분석을 통해 현실적인 개선 로드맵을 제공합니다.

2

ISMS-P, CSAP, N2SF 등 주요 규제 대응

- ISMS-P, CSAP, 국가망보안체계(N2SF) 등 국내외 Compliance에 최적화된 대응 전략을 수립합니다.
- 규제준수(Compliance)를 넘어 비즈니스 연속성과 신뢰도 확보까지 지원합니다.

3

기관 맞춤형 제로트러스트 아키텍처 모델링

- 보안 역량, IT 환경, 조직 특성을 고려한 맞춤형 통합 보안 아키텍처를 설계합니다.
- 단순 진단이 아닌, 장기적 운영을 고려한 실행 가능 모델을 제공합니다.

4

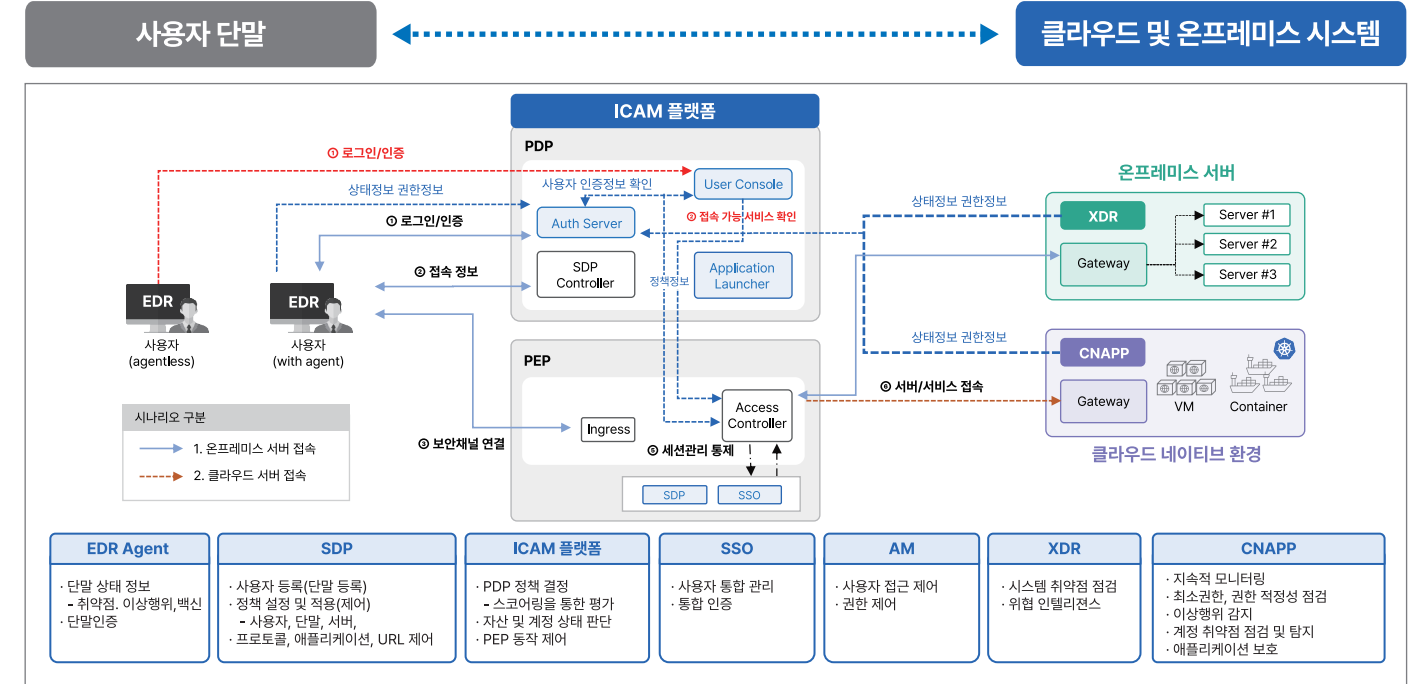
도입 범위 및 기간에 따라 무상 컨설팅 지원

- 프로젝트 범위 및 협의된 일정에 따라 무상 컨설팅을 유연하게 지원합니다.
- 초기 진단에서 실행 로드맵 수립까지, 도입 부담을 최소화하여 보안전략을 수립합니다.

제로트러스트 구성

아키텍처 구성

사용자 단말부터 온프레미스, 클라우드 환경까지 PDP/PEP를 통해 지속적인 신뢰도 검증을 하도록 구성



Why INITECH Consortium?

이니텍은 단순한 통합보안을 넘어, 고객사의 미래 디지털 혁신을 위한 제로트러스트 기반의 최적화된 융합보안체계를 제시합니다. 아래 5가지 핵심 메시지를 통해 이니텍 컨소시엄만이 제공할 수 있는 차별화된 가치를 확인하십시오.

1

미래를 향한 선제적 보안: AI & 클라우드 분야 제로트러스트 리더십

이니텍 컨소시엄은 단순한 제로트러스트 도입을 넘어, 고객의 핵심 미래 전략인 AI 및 클라우드 환경에 특화된 제로트러스트 모델을 제시합니다. 다가오는 AI 시대의 보안 위협에 선제적으로 대응하고, 클라우드 기반 미래 사업의 안전한 성장을 견인할 수 있는 최적의 파트너입니다.

2

경계 없는 통합 보안: End-to-End 제로트러스트 솔루션

기존의 단편적인 보안 방식을 넘어, 엔드포인트부터 온프레미스, 클라우드 인프라까지 모든 IT 자산을 아우르는 End-to-End 제로트러스트 보안을 제공합니다. 전방위적인 보안 체계 구축으로, 고객의 모든 환경에서 잠재적인 위협을 빈틈없이 차단합니다.

3

혁신을 위한 확장성: 무한한 사업적 기회 포착을 통한 보안산업 기여

제로트러스트는 시작이 필요합니다. 이니텍 컨소시엄은 공공 클라우드 네이티브 전환, 금융 클라우드 사업, CSP 협력 모델 등 다양한 미래 사업으로의 확장을 제시합니다. 고객의 장기적인 성장 전략과 발맞춰, 새로운 보안산업 기회를 창출하는 핵심 동력이 될 것입니다.

4

성공을 향한 강력한 의지: 이니텍 컨소시엄 - 최고 파트너십

이니텍은 이미 오래전부터 IAM을 기반으로 제로트러스트 통합보안을 추진하고 있습니다. 제로트러스트 분야를 선도하는 이니텍의 만남은 단순한 협력을 넘어, 중장기적인 발전을 이룰 것입니다. 경영진의 전폭적인 지원과 고객사와의 협력은 사업의 성공을 보장하는 가장 확실한 밑거름입니다.

5

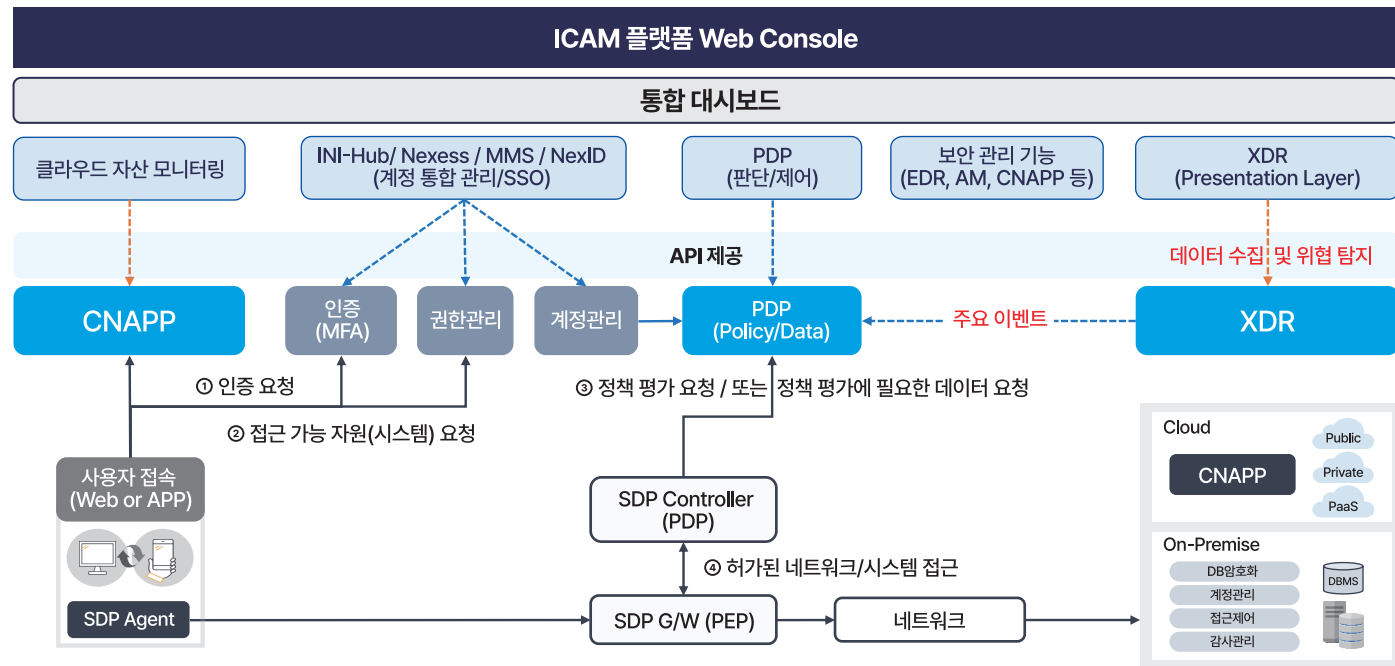
검증된 전문성과 혁신 기술력

이니텍 컨소시엄은 제로트러스트의 부분 보안기능을 구축하지 않고, ZT 2.0 및 글로벌 표준에 대하여 과감한 기술혁신과 투자를 통해 전문성을 확보하고 있습니다. 오랜 성공 사례와 축적된 노하우를 바탕으로, 고객사의 제로트러스트 여정을 성공적으로 이끌어갈 것입니다.

ICAM 플랫폼 구성

● ICAM 플랫폼 개발 및 상용화

이니텍 ICAM 플랫폼은 차별화된 PDP, PEP 기능을 기반으로 계정과 권한 관점의 위협 감시 및 대응이 가능



ICAM 플랫폼 Dashboard



영업문의

주소 : (08389) 서울특별시 구로구 디지털로26길 61 에이스하이엔드타워2차 11층

전화 : (대표) 02-6445-7000

(보안 & 제로트러스트 문의) 02-6445-7210

www.initech.com

※ 컨설팅, 솔루션 소개 등 상담을 언제든지 환영합니다

이니텍 제로트러스트 솔루션 소개

제로트러스트 개요

"Never Trust, Always Verify"

- 1 인증체계 강화 (Strong Authn & Least Privilege)**
각종 리소스 접근 주체에 대한 신뢰도(사용하는 단말, 자산 상태, 환경 요소, 접근위치 등을 판단)를 핵심요소로 설정하여 인증 정책 수립
 - 2 마이크로 세분화 (Micro-segmentation)**
기관 내부의 모든 리소스에 접근하는 사용자와 기기에 세분화된 접근제어 정책을 적용함으로써 공격자의 횡적 이동을 어렵게 하는 보안 기법 혹은 기술
 - 3 소프트웨어 정의 경계 (Software Define Perimeter)**
안전하지 않은 네트워크로부터 서비스를 보호하고 네트워크 공격을 막기 위해 애플리케이션 소유자에게 동적 네트워크 Provisioning과 같은 경계 기능을 제공
- +**
- α 지속/지능/자동 + 통합/가시성 (Orchestration & Visibility & XDR)**
민첩한 비즈니스 환경, 지능화된 위협 대응, 통합보안 관리, 가시성 확보

"통합보안(Zero Trust)"으로 안전하고, 신뢰할 수 있는 비즈니스 환경 구축

● ZeroTrust Journey

제로트러스트 2.0 가이드라인 기반의 성숙도 진단을 통해, 조직의 현재 보안 수준을 점검하고 단계별 ZT 보안 전환 실현

- 1 현황 분석, 방향 설정**
- 2 성숙도 평가, 보안전략 수립**
- 3 아키텍처 수립, 시스템 적용**



<기준 프레임워크>

ZTMM 2.0 (Zero Trust Maturity Model 2.0)을 활용하여, 조직의 제로트러스트 보안 모델 성숙도를 평가합니다.

각 성숙도 수준에 맞는 전략적 목표를 설정하고, 우선순위를 정해 ZT 보안 구현이 가능하게 합니다.

각 단계에서 요구되는 기술적 요소(예: MFA, Micro Segmentation, ZTNA 등)와 개선 과제를 도출하여 단계적 실행 전략을 구체화합니다.