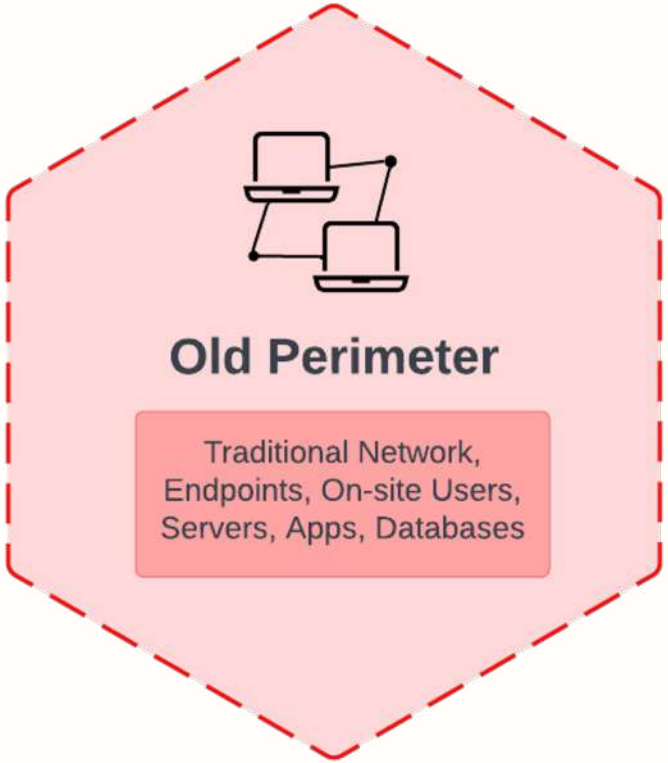
제로트러스트의 튼튼한 기반은 아이덴티티로부터

Heejae Chang
Principal Solutions Engineer, Okta

Zero Trust, 왜 합니까?

기존 기업 보안: 네트워크 경계 기반



- 외부 위협으로부터 네트워크와 시스템을 보호하는 데 중점을 둔 사이버 보안 접근 방식. 네트워크 경계가 가장 취약한 방어 지점이며, 경계를 보호하면 모든 내부 시스템과 데이터를 보호할 수 있다는 가정에 기반

CHALLENGES

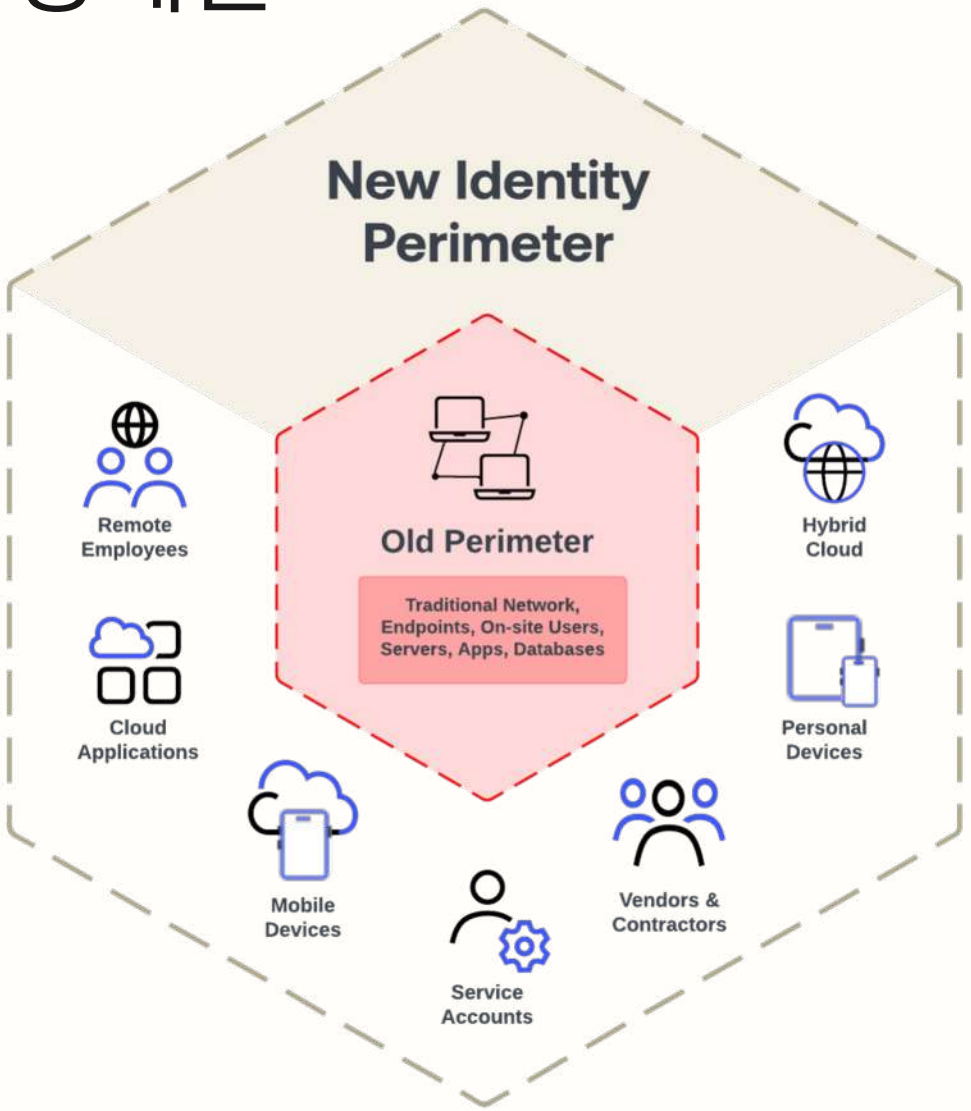
기존 경계 기반 보안의 주요 문제점 중 하나는 네트워크 경계가 명확하게 정의되어 있다는 가정에 기반한다는 것입니다. **하지만 오늘날에는 많은 사용자와 디바이스가 기존 경계 외부에서 네트워크에 액세스하는 등 네트워크 경계가 모호한 경우가 많습니다.**

기존의 경계 기반 보안의 또 다른 문제점은 **내부자 위협에 효과적이지 않다는 것입니다.** 내부자 위협은 네트워크와 시스템에 대한 합법적인 액세스 권한을 가진 개인이 수행하는 공격입니다. 기존의 경계 보안 조치로는 내부자 위협을 탐지하거나 예방할 수 없습니다.

하이브리드 환경에서 기업 보안의 경계는 아이덴티티로 확대 중

새로운 하이브리드 환경에서는 기존의 네트워크 경계가 아닌 사용자 아이덴티티와 리소스에 대한 액세스를 보호하는 데 중점을 둔 보안 접근 방식이 필요합니다.

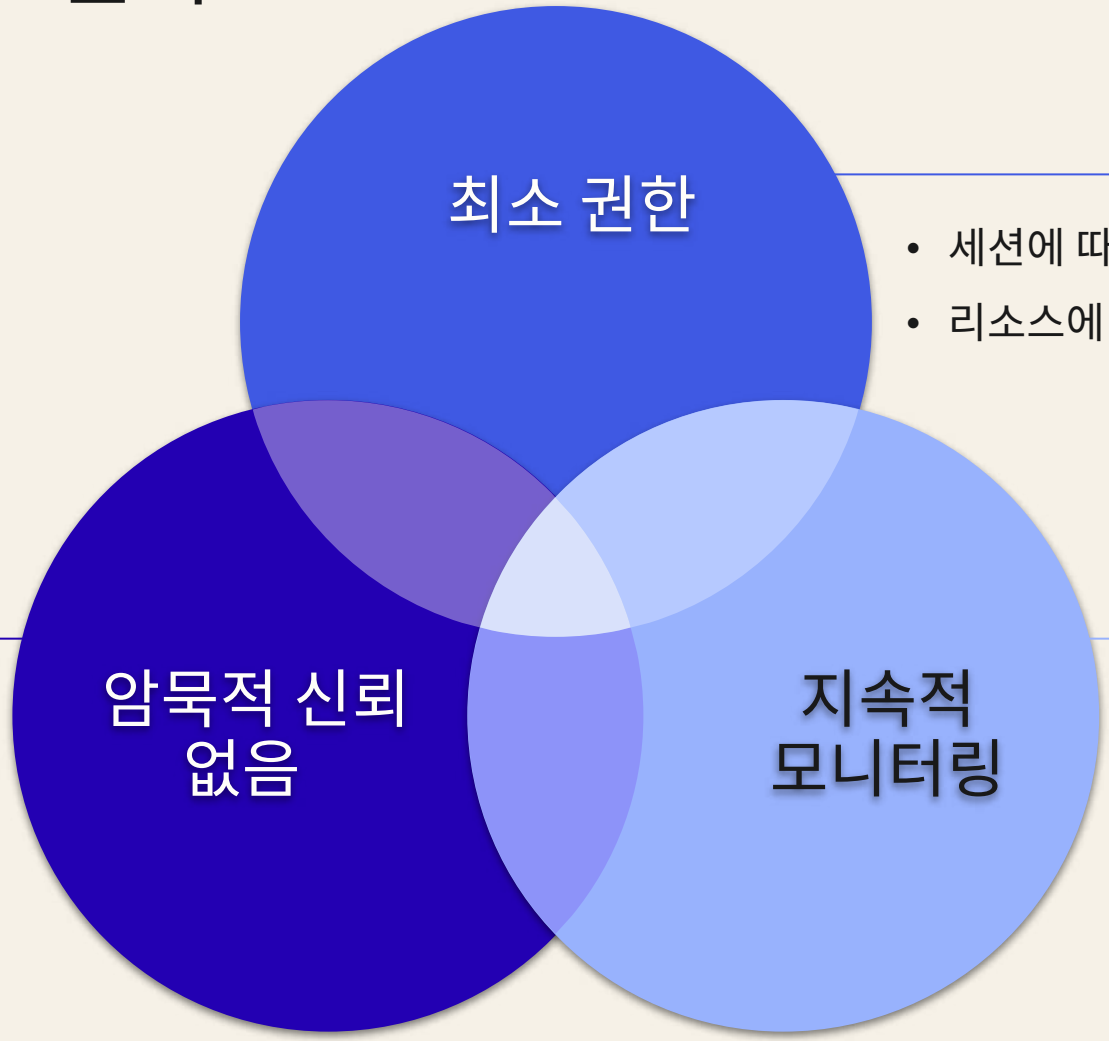
이 접근 방식은 기본적으로 어떤 사용자나 디바이스도 신뢰할 수 없으며, 리소스에 대한 모든 액세스는 검증 및 인가되어야 한다는 원칙에 기반합니다.



제로 트러스트의 궁극적인 지향점

사용자가 디바이스를 이용하여 네트워크를 통해 어플리케이션에 연결되어 데이터에 접근하는 과정을 검증

CISA: 제로 트러스트 원칙



- 세션에 따른 접근 허용
- 리소스에 따른 접근 허용

- 정책 기반 인증 및 인가
- 자산 자체의 정합성 및 보안성
- 안전한 통신

- 지속적 모니터링
- 동적 상태 관찰

okta

KISA: 제로트러스트 기본 철학

제로트러스트 기본철학

① 모든 종류의 접근에 대해 신뢰하지 않을 것(명시적인 신뢰 확인 후 리소스 접근 허용)
② 일관되고 중앙집중적인 정책 관리 및 접근제어 결정·실행 필요
③ 사용자, 기기에 대한 관리 및 강력한 인증
④ 자원 분류 및 관리를 통한 세밀한 접근제어(최소 권한 부여)
⑤ 논리 경계 생성 및 세션 단위 접근 허용, 통신 보호 기술 적용
⑥ 모든 상태에 대한 모니터링, 로그 기록 등을 통한 신뢰성 지속 검증·제어

제로 트러스트 아키텍처에서 아이덴티티의 역할

NIST: 아이덴티티는 제로 트러스트 아키텍처의 핵심

“행위자의 아이덴티티”

제로 트러스트 아키텍처 개발에 대한 강화된 아이덴티티 거버넌스 방식(Enhanced Identity Governance)은 **행위자의 아이덴티티를 정책 수립의 핵심 요소로 사용합니다**. 엔터프라이즈 리소스에 대한 액세스를 요청하는 주체가 없다면 액세스 정책 생성 자체의 필요성이 없습니다. 이 접근 방식에서 **엔터프라이즈 리소스 액세스 정책은 아이덴티티와 해당 아이덴티티에 할당된 속성값에 기반합니다. 해당 주체에 부여된 권한이 특정 리소스 접근을 위한 가장 기본적인 요건입니다.**

~*NIST Special Publication 800-207*

“대상자의 아이덴티티”

... 우리의 첫 번째 (제로 트러스트) 구현은 EIG (강화된 아이덴티티 거버넌스) 접근 방식을 기반으로 선택했는데, **그 이유는 EIG가 오늘날 하이브리드 환경에서 활용되는 배포 방식들의 기본 구성 요소로 간주되고 있기 때문입니다.** EIG 접근 방식은 **대상자의 아이덴티티**와 디바이스 상태를 정책 결정의 주요 결정 요인으로 사용합니다....

~*NIST/NCCOE Special Publication 1800-35B Preliminary Draft*

okta

KISA: 제로트러스트 구현 핵심원칙

● **(핵심원칙)** 제로트러스트 아키텍처를 구현하기 위한 **접근방법**으로 **네트워크 환경**에 따라 일부 상이할 수 있으나, 완전한 제로트러스트 솔루션은 **3가지 핵심원칙**을 모두 포함

* 기존 경계 기반 보안과 달리 내부자조차도 더 이상 신뢰하지 않으므로, 강력한 관리, 인증, 접근제어 및 상태 감시를 통한 통제 필요

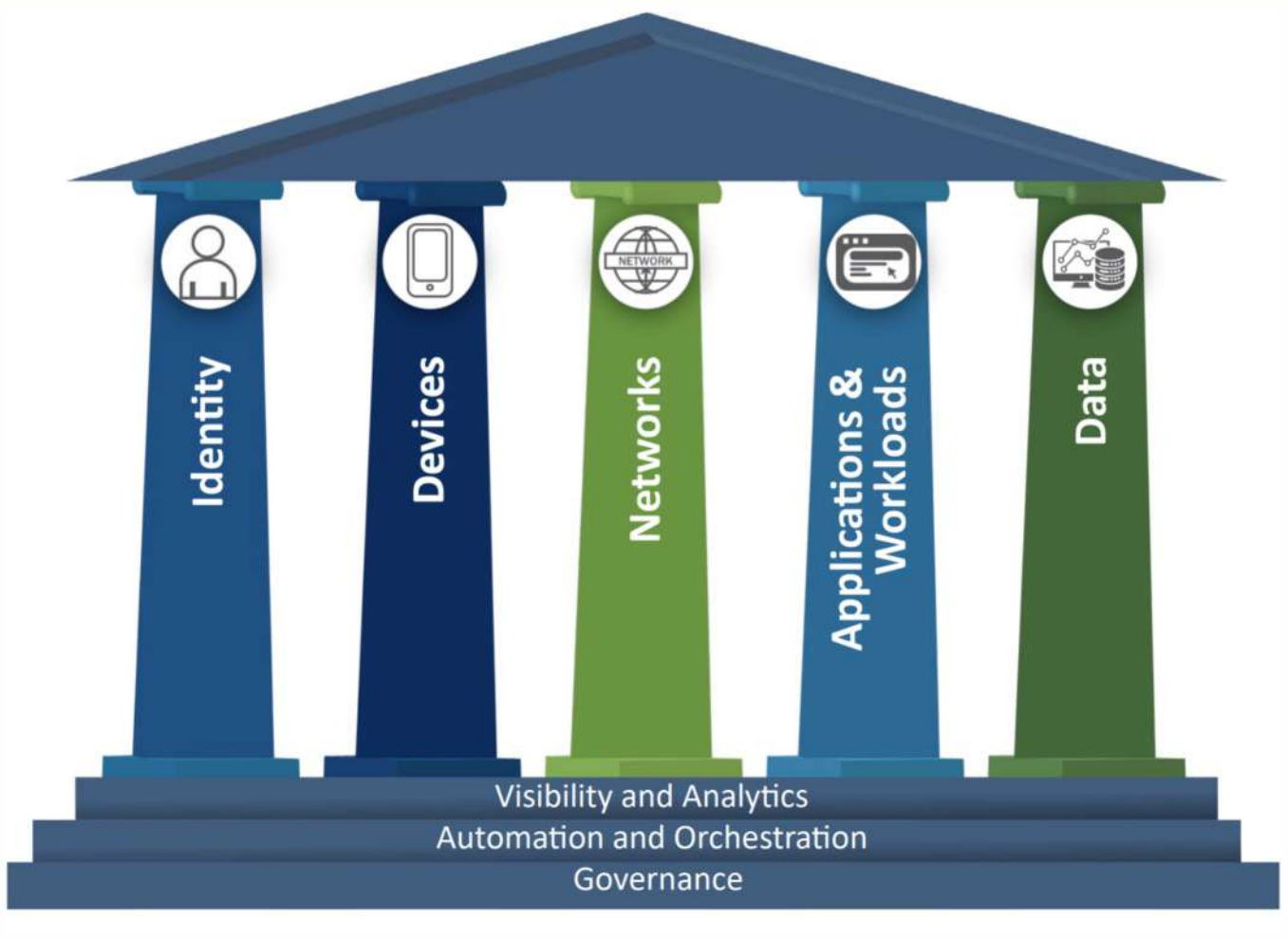
〈제로트러스트 구현 핵심원칙〉

핵심 원칙	세부 내용
인증 체계 강화 (기본철학 중 ①②③⑥)	▲ 각종 리소스 접근 주체에 대한 신뢰도(사용하는 단말, 자산 상태, 환경 요소, 접근 위치 등을 판단)를 핵심요소로 설정하여 인증 정책 수립 ※ 기업내 사용자에 대한 여러 아이디를 허용하여 일관된 정책을 적용하지 않거나, 신뢰도 판단없이 단일 인증 방식만으로 접속을 허용할 경우 **크리덴셜 스터핑**에 취약
마이크로 세그멘테이션 (기본철학 중 ②④⑤)	▲ 보안 게이트웨이를 통해 보호되는 단독 네트워크 구역(segment)에 개별 자원(자원그룹)을 배치하고, 각종 접근 요청에 대한 지속적인 신뢰 검증 수행 ※ 개별 자원별 구역 설정이 없으면, 기업망 내부에 침투한 공격자가 중요 리소스로 이동하기 쉬워 **횡적이동 공격 성공 가능성**이 높아짐
소프트웨어 정의 경계 (기본철학 중 ①②⑤)	▲ 소프트웨어 정의 경계 기법을 활용하여 정책 엔진 결정에 따르는 네트워크 동적 구성, 사용자·단말 신뢰 확보 후 자원 접근을 위한 데이터 채널 형성 ※ 클라우드·온프레미스로 구성된 기업 네트워크 내부에서 단말이 임의 데이터를 전송할 수 있다면, **네트워크 및 호스트 취약성에 따르는 피해 가능성**이 커짐

[NIST SP 800-207, 제로트러스트 아키텍처에 대한 다양한 접근법(3.1절)을 기반으로 작성]

okta

CISA Zero Trust Maturity Model Pillars

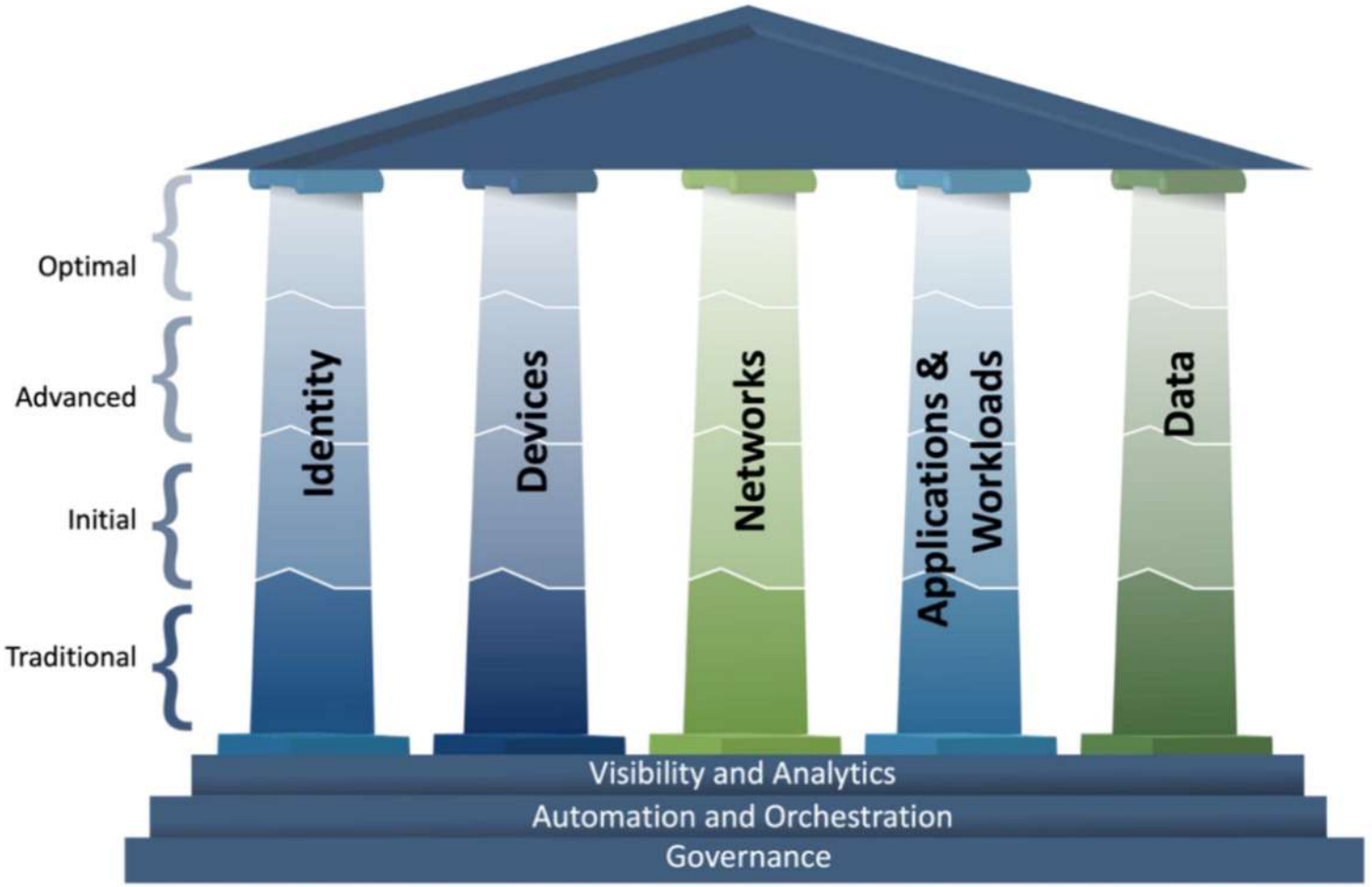


주요 원칙

- 최소 권한
- 암묵적 신뢰 없음
- 지속적 모니터링

okta

CISA Zero Trust Maturity Evolution

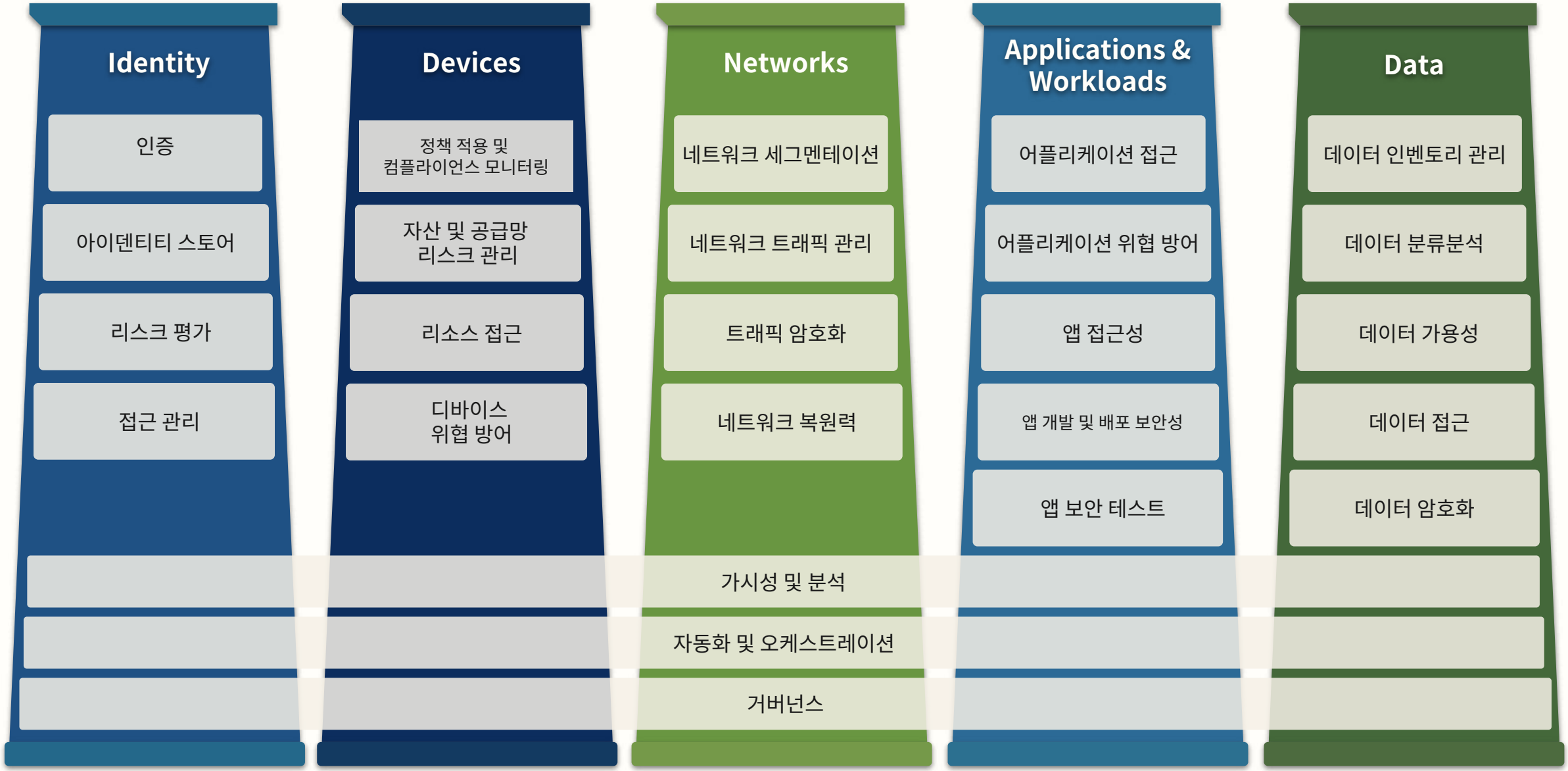


주요 원칙

- 최소 권한
- 암묵적 신뢰 없음
- 지속적 모니터링

okta

CISA Zero Trust Maturity Model Functions

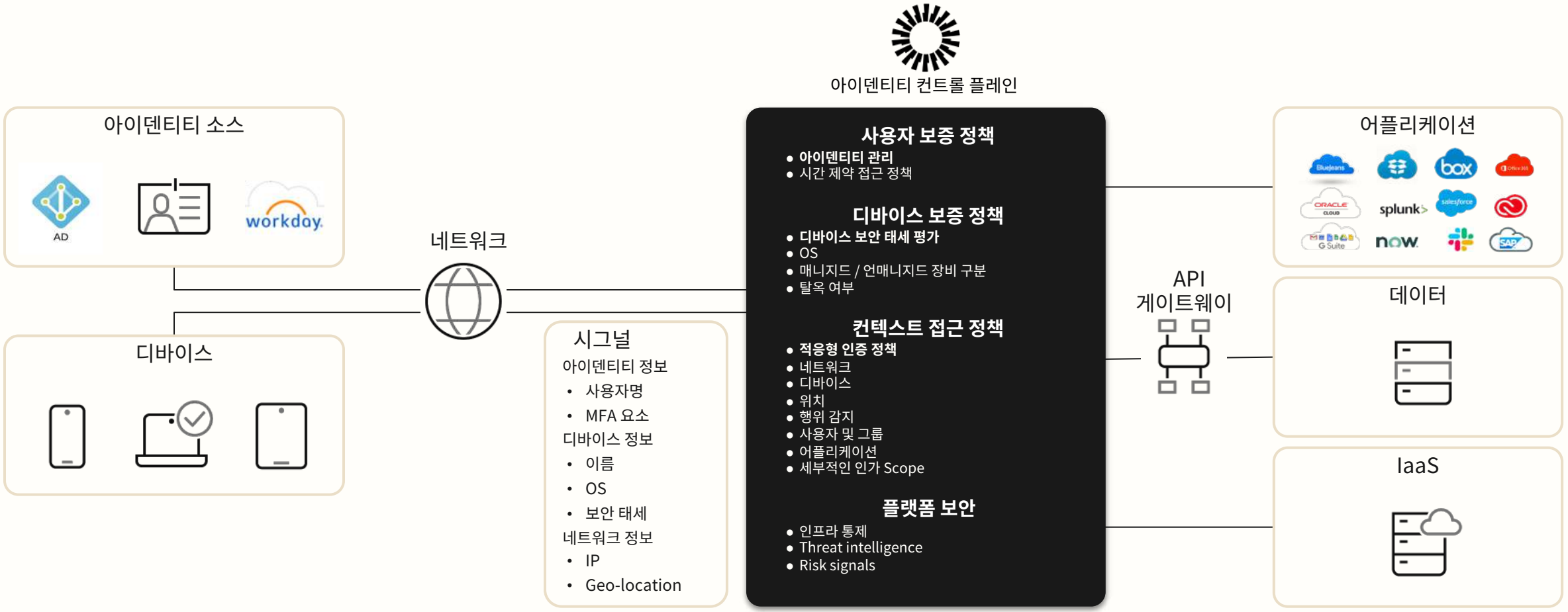


아이덴티티 보안 제어를 위한 제로 트러스트 성숙도

IDENTITY

	Traditional	Initial	Advanced	Optimal
인증	PW+MFA 정적 접근	PW+AMFA 동적 접근	패스워드리스 + 피싱 방어 MFA	패스워드리스 + 피싱 방어 MFA + 지속적 검증
아이덴티티 스토어	자체 관리 온프렘 ID 스토어	자체 관리 + 클라우드 스토어	ID 스토어 통합	완전히 통합된 ID 스토어
리스크 평가	제한적 ID 리스크 평가	정적 룰을 통한 ID 리스크 관리	자동화 / 동적 룰을 이용한 ID 리스크 관리	지속적 분석 및 동적 룰을 이용한 리스크 관리
접근 관리	정적 접근에 대한 주기적 리뷰	정적 접근에 대한 자동화된 리뷰	최소 권한에 따른 접근 권한 부여	최소 권한 및 JIT를 이용한 권한 부여
가시성 및 분석	수동 로그 분석	로그 상관관계 및 자동화 분석	자동화 분석 + 강화된 로그 수집	행위 탐지를 포함한 포괄적 로그 분석 자동화
자동화 및 오케스트레이션	파편화된 ID 스토어에 대한 전체 수동 JML 작업 수행	파편환된 ID 스토어에 대한 일부 자동화 JML 작업 수행	통합된 ID 스토어에 대한 일부 자동화 JML 작업 수행	통합된 ID 스토어에 대한 완전한 자동화 JML
거버넌스	정적 ID 정책 적용 및 수동 리뷰	정적 ID 정책 적용 및 최소한의 자동화	정책 자동화 및 주기적 리뷰	정책 자동화 및 동적 / 지속적 업데이트

아이덴티티 기반 보안을 통한 제로 트러스트 구현



자동화 / 오케스트레이션	**LCM** ● JIT 프로비저닝 ● 롤 할당	**Governance** ● Access Requests ● Access Certifications
가시성 및 분석	**지속적 모니터링 및 정책 적용** ● Workflows ● Event hooks	

okta

아이덴티티 콘트롤 플레인을 통한 제로 트러스트 성숙도 향상

아이덴티티

강력한 인증을 포함한 아이덴티티 자격 증명이 권한이 부여된 사용자에 대해 시행, 관리, 확인, 해지 및 감사됩니다.

Identities: 파편화 → 통합 아이덴티티
Passwords: 패스워드 필요 → 패스워드리스
MFA: 레거시 -> 피싱 방지
Risk assessment: 정적 평가 → 지속적 평가
Access: 정적 접근 -> JIT

디바이스

디바이스 보안 태세 점수를 포함한 디바이스 보안 체크가 시행되고 감사됩니다.

Device status: 알려진 디바이스 → 등록된 디바이스 → 관리되는 디바이스 → 보안성 높은 디바이스
Device security: 인증서 체크 → 보안 태세 체크
Device policy: MDM → 로컬 디바이스 보증

네트워크

네트워크 IP 및 인라인 트래픽 검사가 수행됩니다.

Network IPs: 정적 -> 동적 정책 기반
Internet threats: 파편화된 정적 검사 → ThreatInsights를 통해 서비스 레이어 에코시스템 활용

어플리케이션

트래픽 검사와 함께 애플리케이션 액세스 권한이 평가되고 필요 시 사용자가 격리됩니다.

Application Policy: SSO 세션 → 앱별 인증 정책 평가
Application Access : 정적 접근 -> JIT
Application Controls : 개괄적 권한 → 세부 권한 Scope, 세션 관리, SLO
Application Threats : 모니터링 없음 → Workflows 이용한 실시간 대응

데이터

데이터 접근에 대한 인가 요건이 적용됩니다.

Data Compliance: API 엔드포인트에 대한 접근 정책 중앙 관리

Visibility & Analytics

모든 인증 및 아이덴티티 관리에 대한 로그

Automation & Orchestration

에코시스템의 이벤트에 대한 대응 및 요청에 대한 자동화된 대응 구성
(Okta Workflows, Okta Identity Governance)

Governance

거버넌스 정책에 따른 리소스별 접근 정책 관리

okta

아이덴티티 기반의 보안

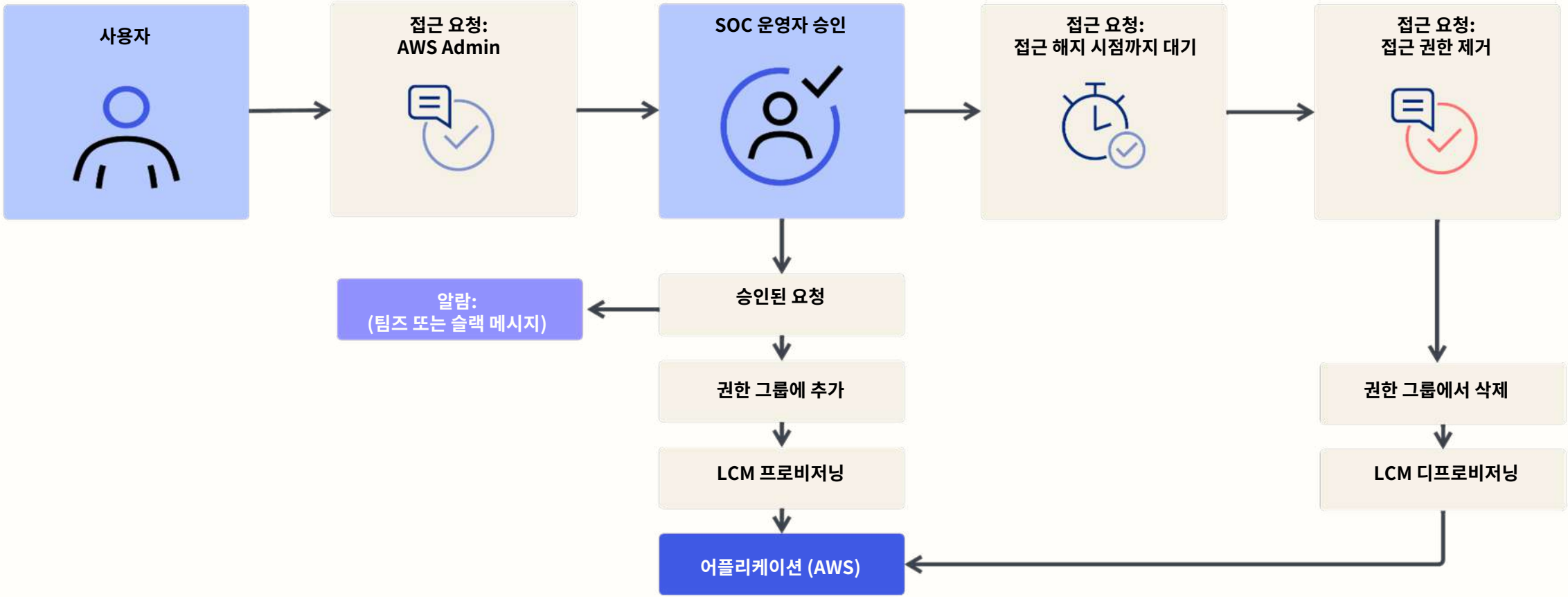
- 아이덴티티: 컨트롤 플레인 역할
- ZTA 첫번째 단계 – 아이덴티티 검증
- 최소 권한 원칙 적용을 위한 핵심 요소
- 아이덴티티는 네트워크, 데이터, 앱, 디바이스 등 다른 Zero Trust Pillar가 기능하기 위한 기반 요소

okta

Okta 기반 Zero Trust 시나리오 예시

OKTA DEMONSTRATION

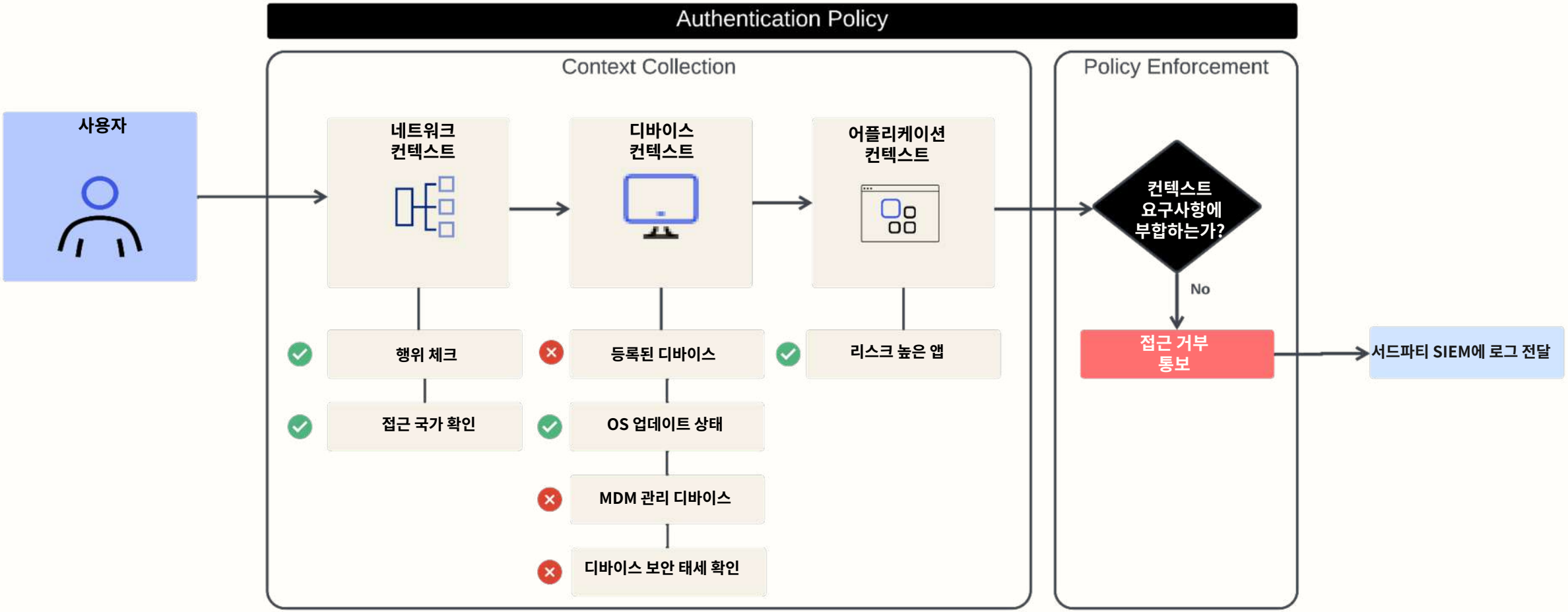
최소 권한 USE CASE: 한시적 접근 권한 부여



okta

OKTA DEMONSTRATION

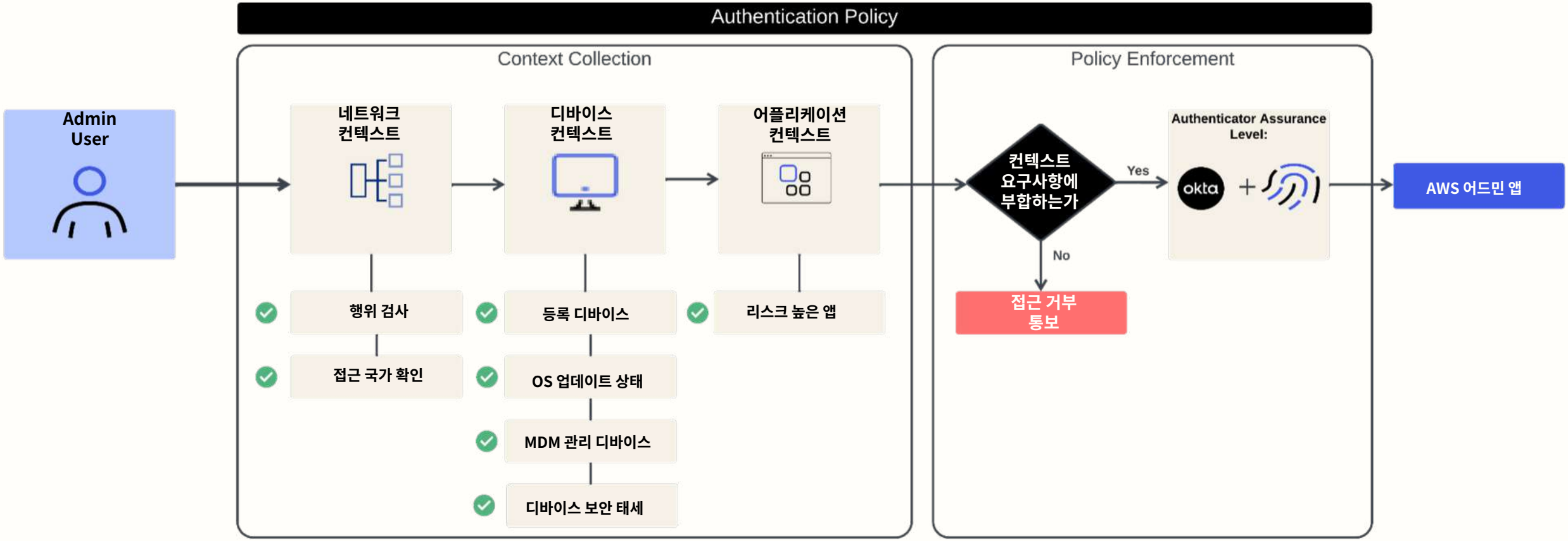
암묵적 신뢰 없음 USE CASE: Assurance Level로 인한 접근 실패



okta

OKTA DEMONSTRATION

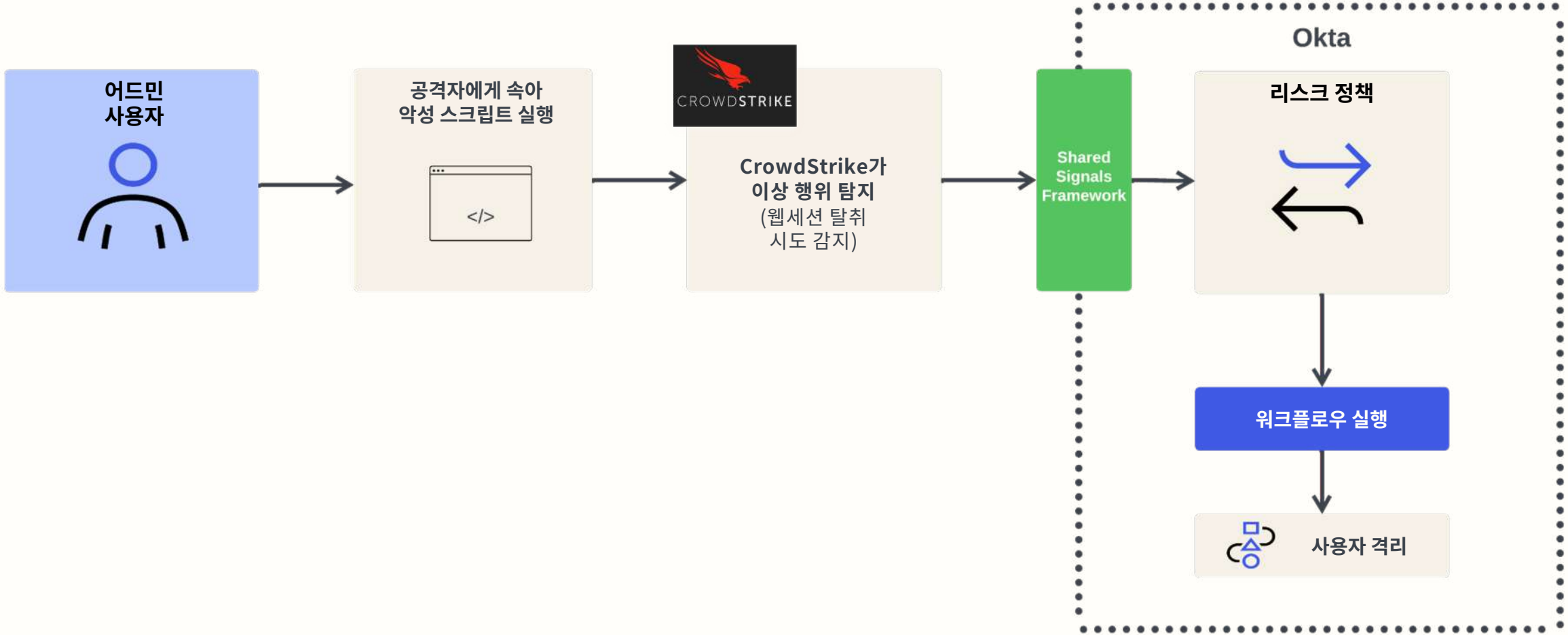
암묵적 신뢰 없음 USE CASE: Assurance Level 검사 후 접근 허용



okta

OKTA DEMONSTRATION

지속적 모니터링 USE CASE: ITP



okta

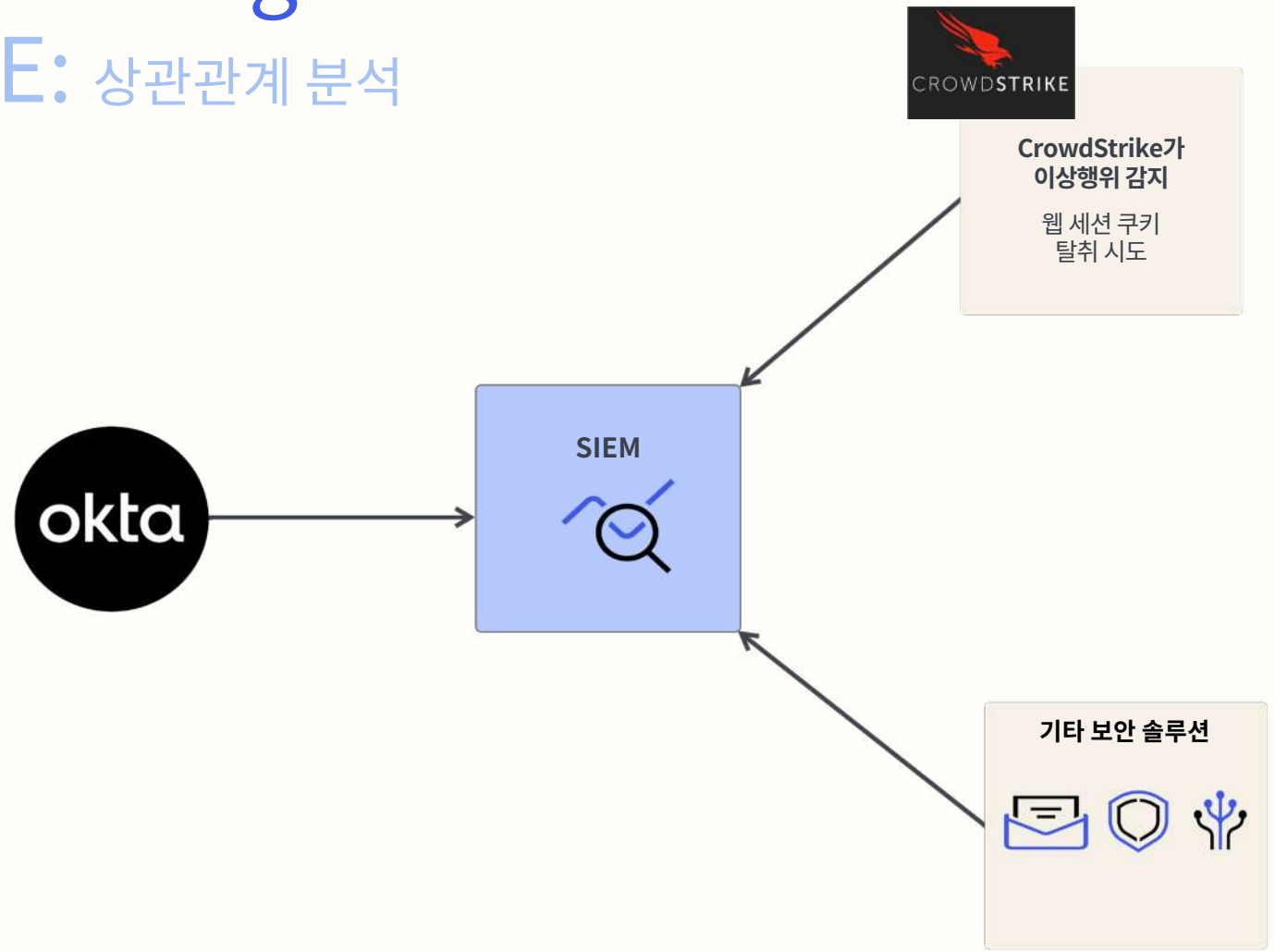
OKTA DEMONSTRATION

Continuous Monitoring

USE CASE: 상관관계 분석

Okta는 다른 보안 솔루션과 상관관계를 파악할 수 있도록 조직의 SIEM에 로그를 제공하여 SOC가 다음과 같은 질문에 대한 실시간 분석을 수행할 수 있음:

- Okta가 기기를 일시 중지하기 직전에 관리자가 액세스한 애플리케이션은 무엇인가?
- Okta가 외부 시스템에서 실패한 피싱 시도를 감지했는가?



okta

Thank you!

okta