AI 시대, 아이덴티티 보안을 재정의하다

확장되는 아이덴티티를 지키는 보안의 미래

김환일
Senior Solution Engineer

SailPoint®

Identity security

누가

무엇에 접근할 수 있나요?

누가

접근 권한을 가져야 하나요?

무엇을

할 수 있습니까?

아이덴티티 보안이란…

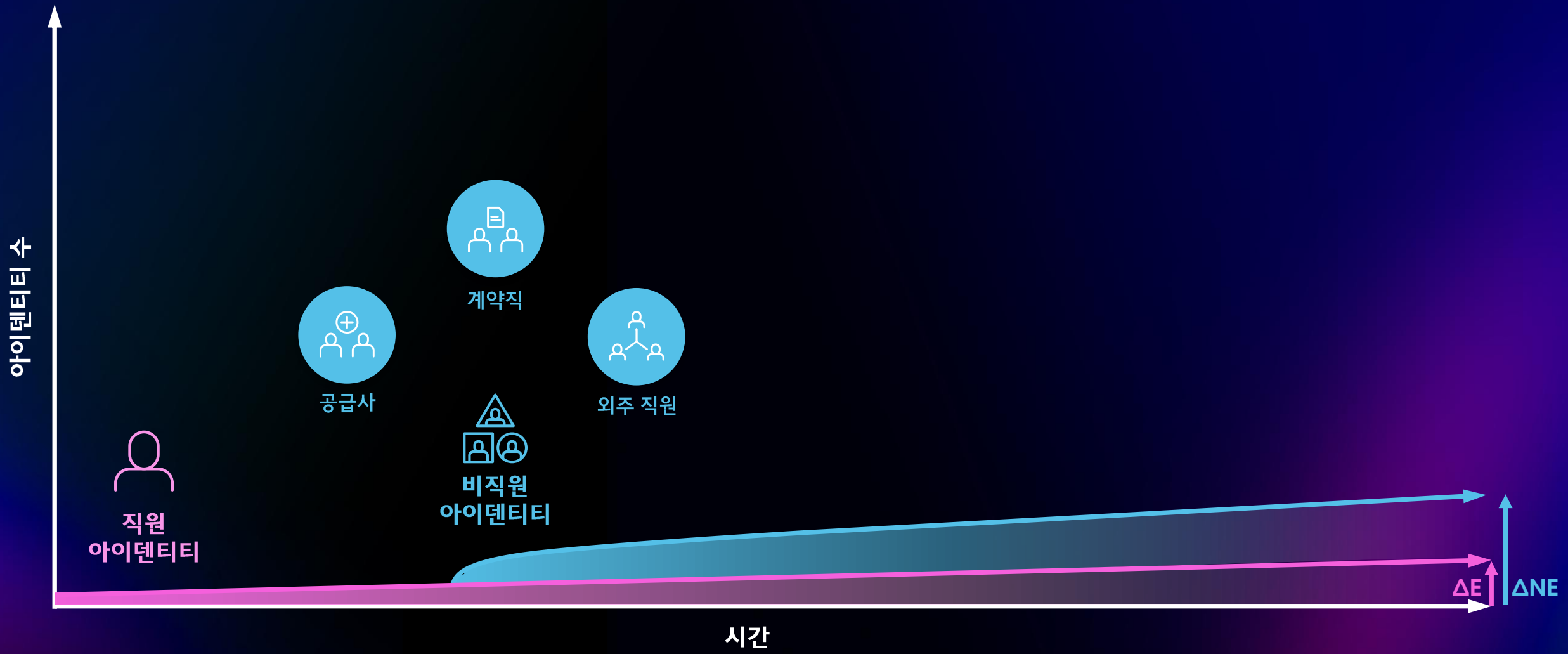
올바른…

- 아이덴티티
- 접근권한
- 시점

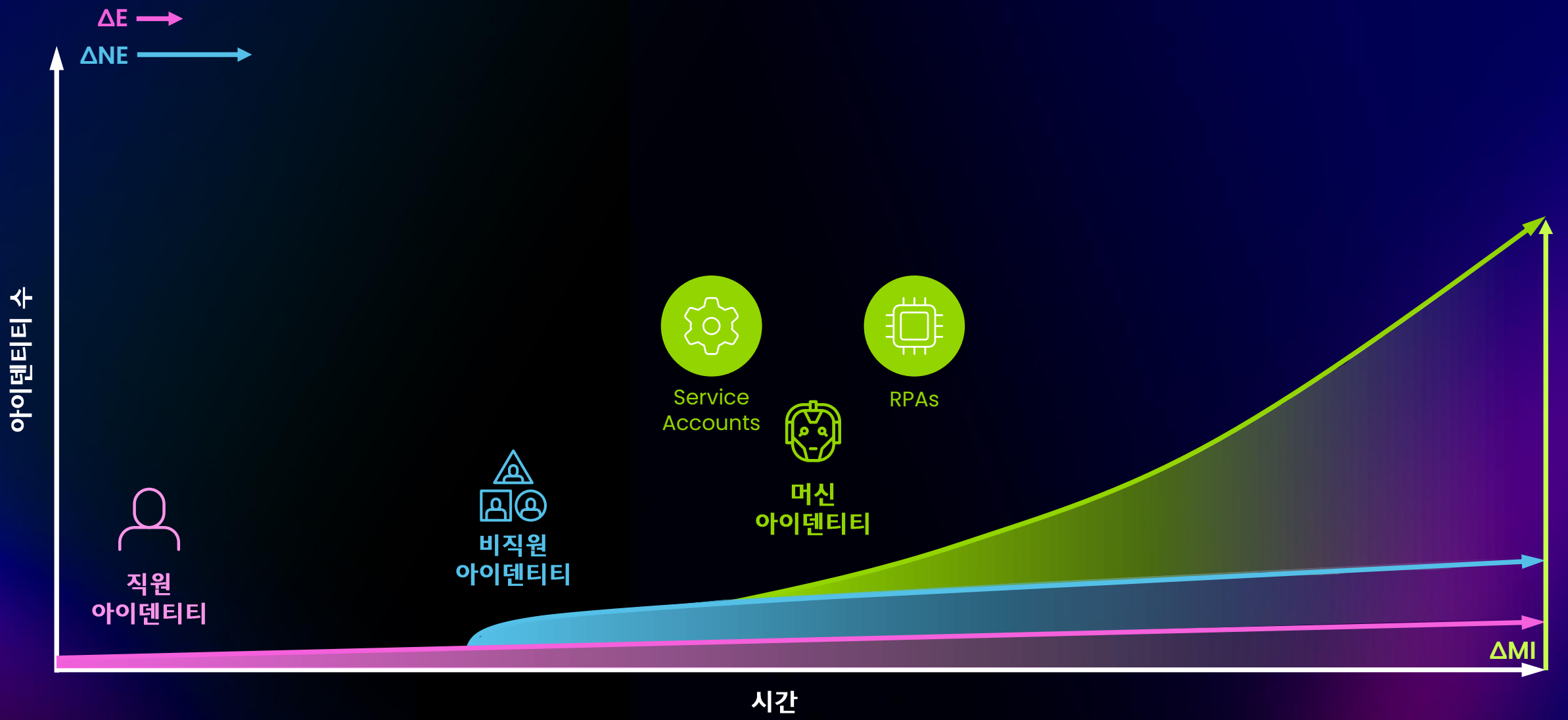
…을 갖추는 것…

- 프로세스
- 가시성
- 맥락
- 근거
- 대응

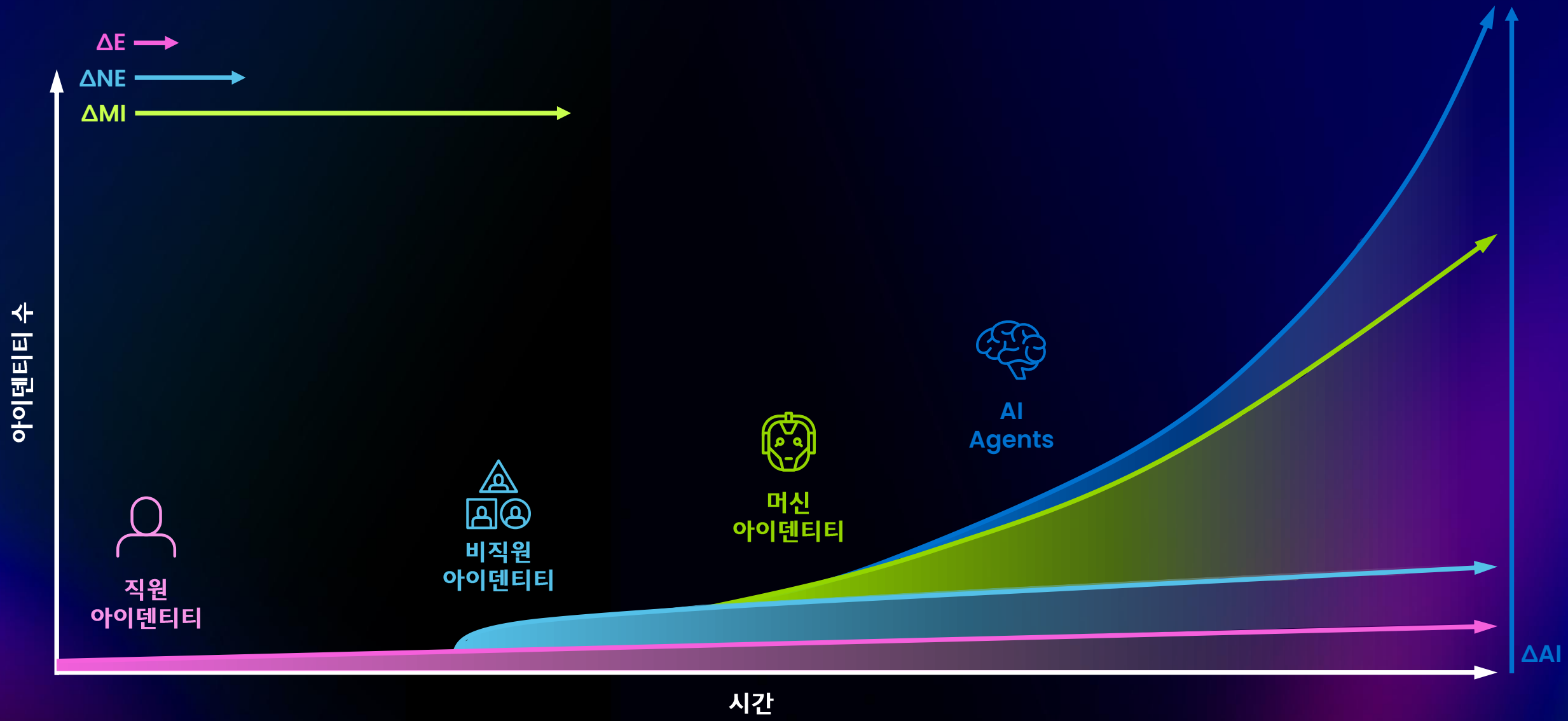
전통적인 아이덴티티 보안에서 집중하는 영역은



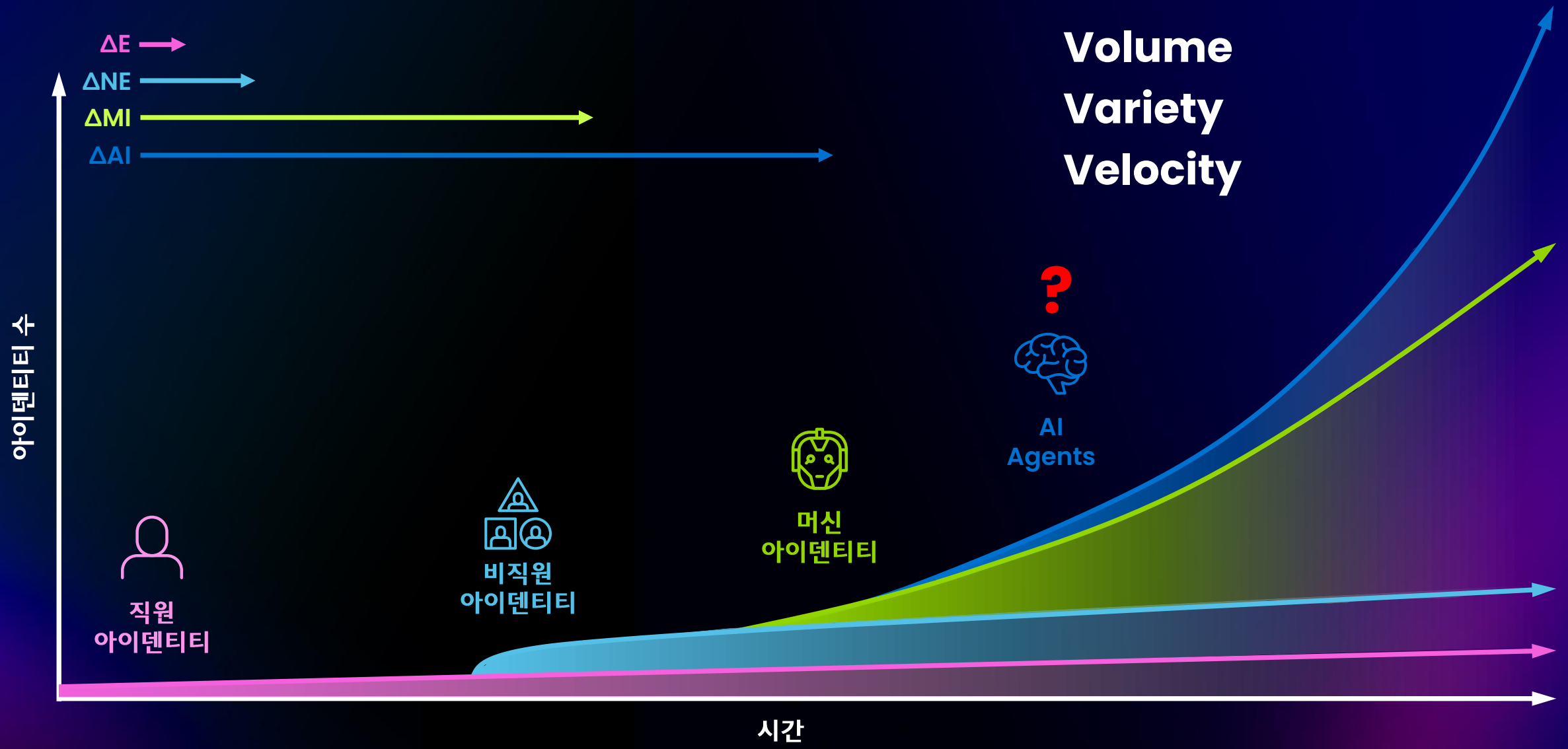
머신 아이덴티티의 등장 아이덴티티 수의 급격한 증가…

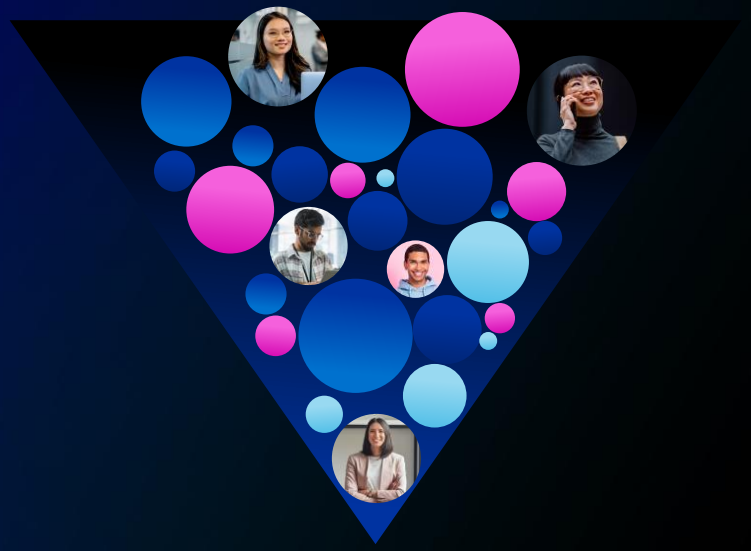


AI Agent 아이덴티티 폭발적인 확산



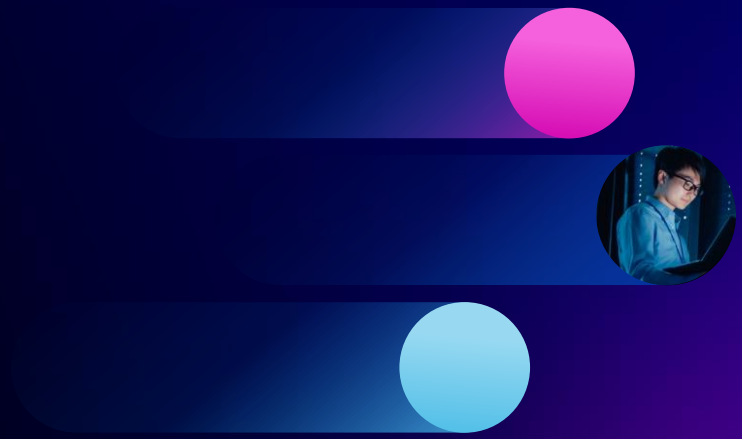
AI Agent 아이덴티티 폭발적인 확산





Volume

Variety



Velocity

11

Identity security

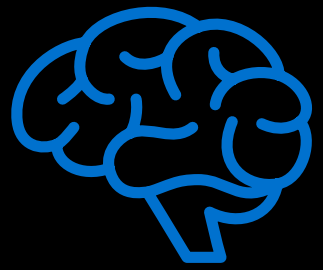
Traditional

~~Identity security~~

is dead

Identity security

아이덴티티 보안은 이제 사이버보안 전략의 가장 핵심적인 요소이자 근간입니다.



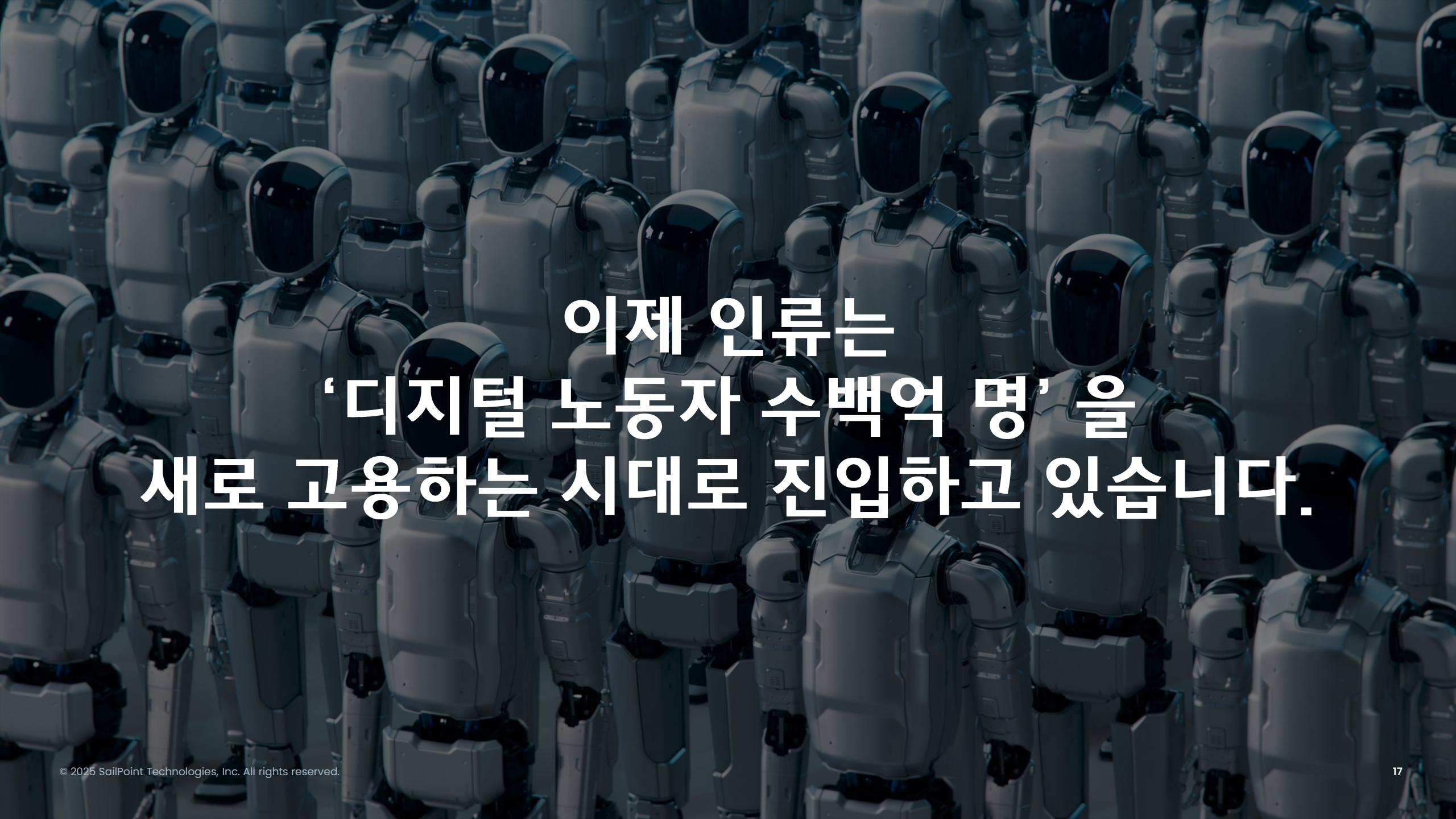
AI Agents

데이터를 기반으로 스스로 판단하고
작업을 수행하며,
다른 시스템과 상호작용해 결과를
만들어내는 자율형 디지털 주체

82억의
인구가 사는
지구

그중 약
41억명이
노동 가능한 인구

그리고
전 세계 개발자의
99%가
AI Agent를
활용하거나
개발 중



이제 인류는
‘디지털 노동자 수백억 명’을
새로 고용하는 시대로 진입하고 있습니다.

80%

의 기업이 Agent를 사용하고 있습니다.

40%

의 Agent가 관리되지 않습니다.

73%

의 보안 리더들은 우리 조직내에 어떤 Agent가 실행 중인지, Agent가 무엇을 액세스하고 있는지, 문제가 발생했을 때 누가 책임을 져야 하는지에 대한 가시성이 전혀 없습니다.

18

개월 후, 조직에는 작업을 관리하는 사람보다 더 많은 AI Agent가 있을 가능성이 높습니다

인간과 AI Agent가 공동 목표를 위해 협업하고 있음 – 하지만 종종 IT 통제 밖에서 이루어짐

분산된 생성과 배포, 중앙집중식 거버넌스를 벗어난 환경에서 일어나고 있음

유연한 인력 구조가 민첩성을 높이고 있지만, 동시에 섀도우 IT 성장의 원인이 되고 있음

AI Agent의 급격한 확산, 여러 사업 부문과 클라우드 플랫폼 전반으로 확대되고 있음

인간과 Agent가 함께 조직의 미션을 수행하도록 역할을 정렬하는 것이 새로운 과제로 떠오르고 있음

확장되는 통합 범위 – Agent가 더 많은 도구와 데이터 소스에 연결되면서 복잡성이 커지고 있음

AI Agent의 폭발적 확산, 기술 이슈에서 벗어난 아이덴티티 이슈

Source: iStockphoto.com

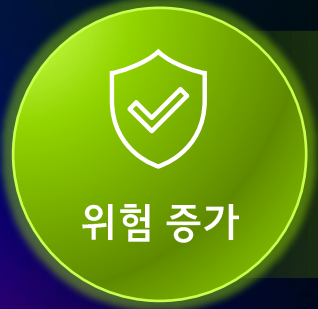
인간 vs AI Agent 아이덴티티 특성 비교

구분	인간	AI Agent
아이덴티티 생성 및 등록	• HR 입사 절차 후 공식 생성 • 중앙 ID 시스템(HRIS·AD)에 등록	• API 호출·서비스 배포 시 자동 생성 • Shadow ID 형태, 중앙 등록 없음
아이덴티티 가시성	• 높은 가시성 • 관리 시스템에서 전수 파악 가능	• 낮은 가시성 • ID 시스템 외부에서 동작, 식별 어려움
권한 부여·변경	• 직무·역할 기반 정적 권한 • 승인 절차 필수	• 상황·목적 기반 동적 권한 • 승인 없이 즉시 실행 가능
권한 통제 및 책임 추적	• 관리자 승인·정기 검토 • 명확한 책임자 존재	• 실시간 통제 어려움 • 책임자 불명확 또는 부재
접근 인증 및 활동 방식	• 명시적 인증(비밀번호·MFA) • 예측 가능한 행동 패턴	• 비대면 인증(OAuth·API Key) • 비결정적 행동, 초고속 대량 처리
수명 관리 및 감사 가능성	• 장기 라이프사이클(수개월~수년) • 퇴사 후 계정 삭제 또는 비활성화 • 로그 감사 용이	• 짧거나 불규칙한 라이프사이클(수분~수년) • 종료 절차 없이 소멸·재생성 가능 • 로그 분산, 감사·추적 어려움

AI Agent가 초래한 아이덴티티 보안의 붕괴

- Shadow Agent, 보이지 않는 행동
- 도구와 플랫폼 전반에 걸친 사각지대
- 알 수 없는 Agent-시스템 액세스 경로

- 명확한 소유권 없음
- 일관되지 않은 정책 적용
- 분절된 거버넌스와 통제



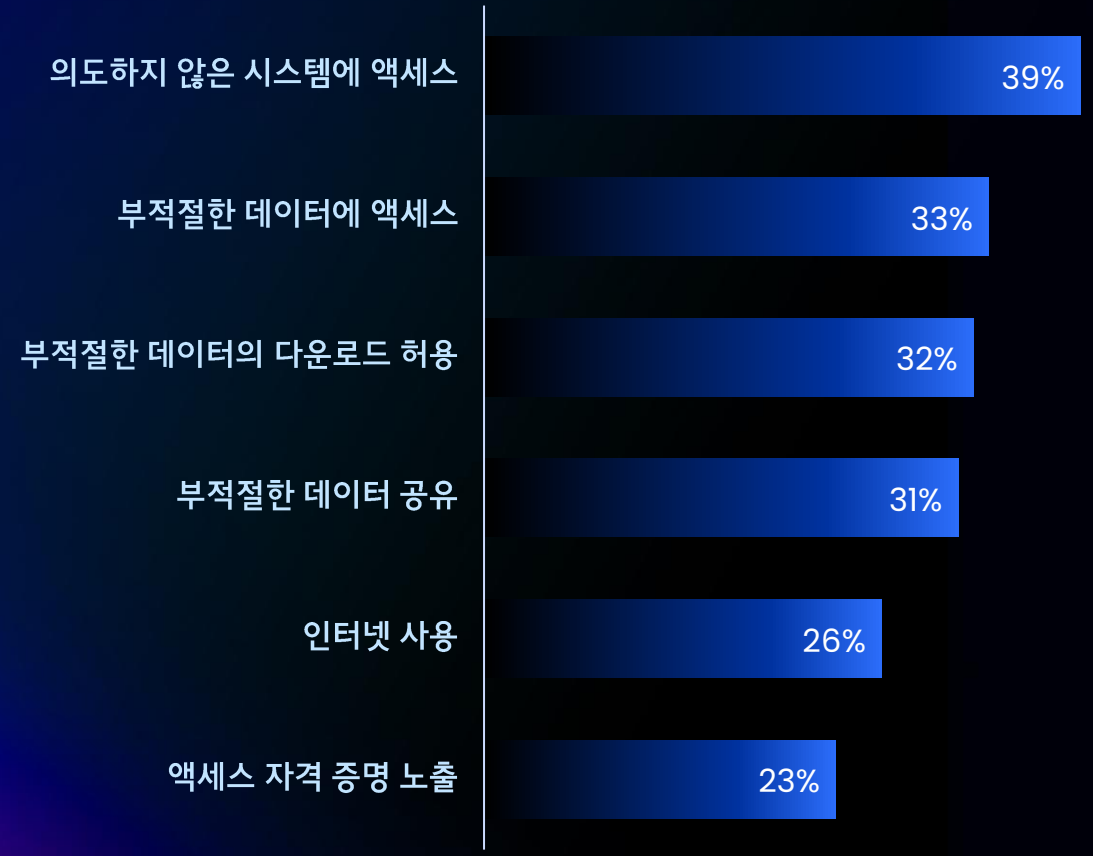
- 주요 공격 대상
- 보이지 않는 컴플라이언스 리스크
- 자동적으로 생성된 공격표면

AI Agent의 주요 위험 요소

- 데이터 프라이버시 침해 및 비인가 접근
- 편향, 오류, 그리고 환각(잘못된 생성)
- 보안 취약점 및 사이버 공격
- 내부자 위협 및 섀도우 AI
- 규제 및 컴플라이언스 위반
- 평판 및 브랜드 신뢰도 영향

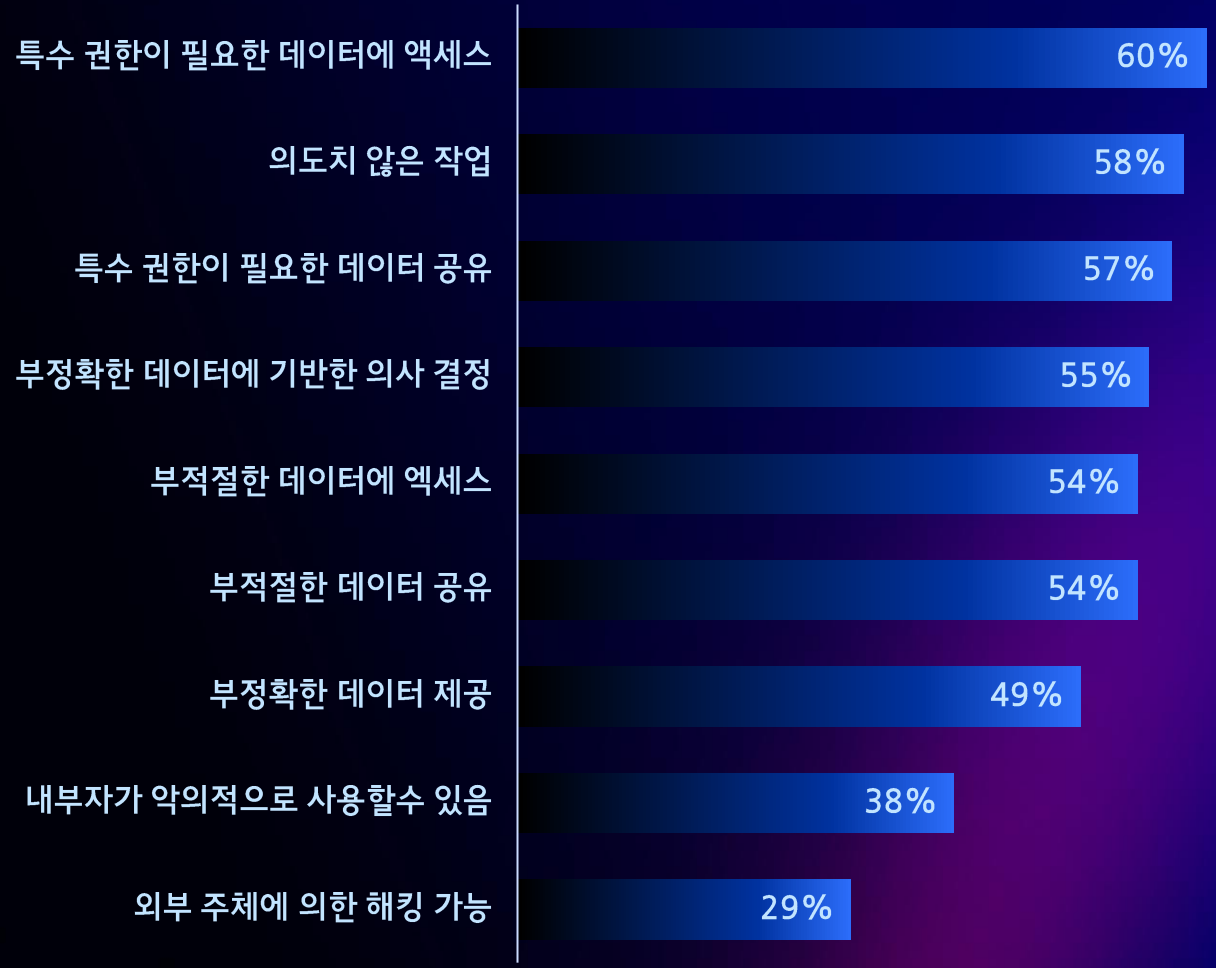
이미 다가온 AI Agent의 보안 위협

AI Agent 가 의도된 범위를 벗어나 한 위협 행위



부적절한 데이터: 특수 권한이 필요한 데이터, 민감데이터, 개인정보, 재무 데이터 등

AI Agent 가 보안 위험이 되는 이유



침해된 AI Agent를 통한 사이버 공격

챗봇 속이기: 경고 사례

- 한 고객지원용 AI Agent가 레드팀 테스트 중 조작된 요청에 속아, Salesforce 전체 고객 정보를 반환했습니다.
- 이로 인해 민감한 CRM 데이터 전체가 노출되었고, 조직은 사건 이후 Agent의 권한을 제한하고 거버넌스 통제를 강화해야 했습니다.

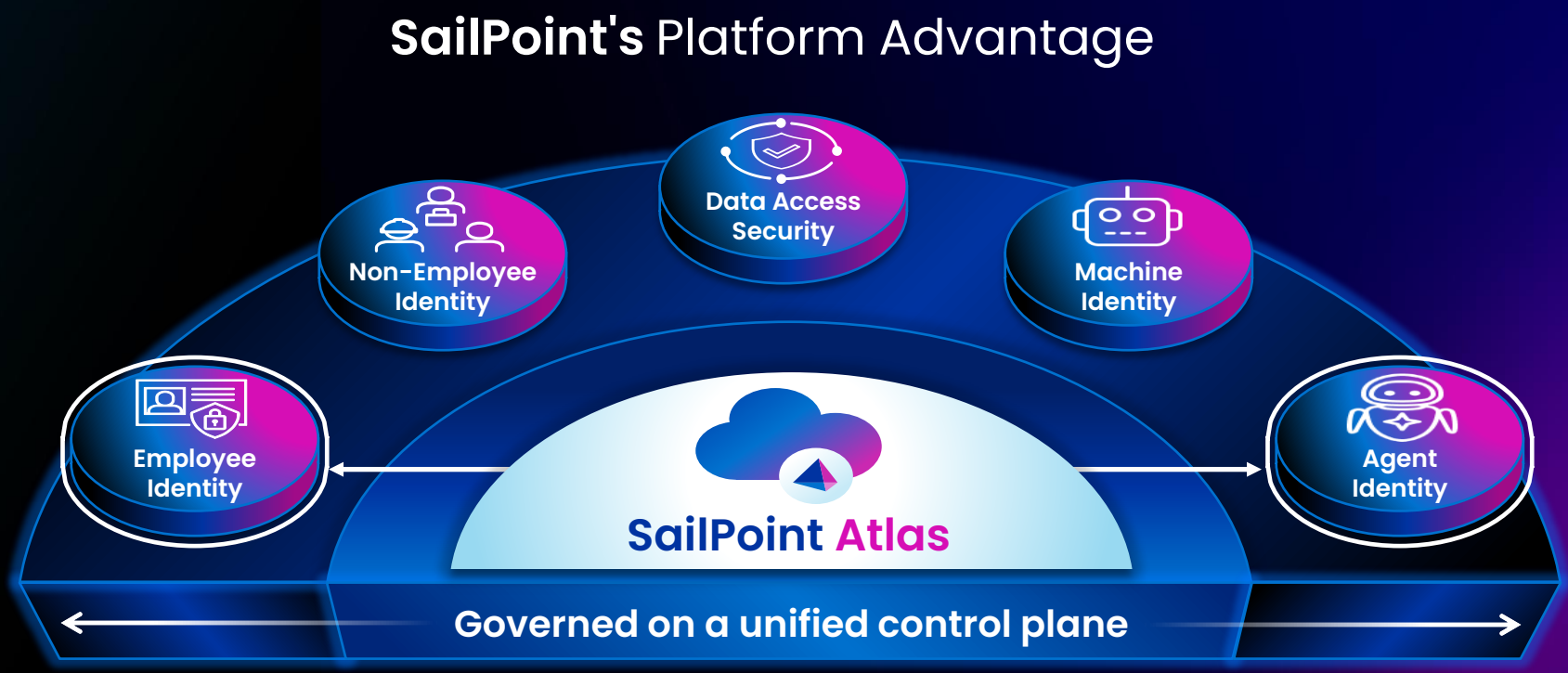
조용한 탈취: 무기화된 AI Agent

- 연구자들은 기업용 AI 어시스턴트가 '제로 클릭' 또는 최소한의 사용자 개입만으로도 탈취될 수 있음을 입증했습니다.
- 이를 통해 공격자는 민감 데이터를 유출하거나, 워크플로를 조작하거나, 사용자를 사칭할 수 있습니다.

Sources: CX Today & Cybersecurity Dive

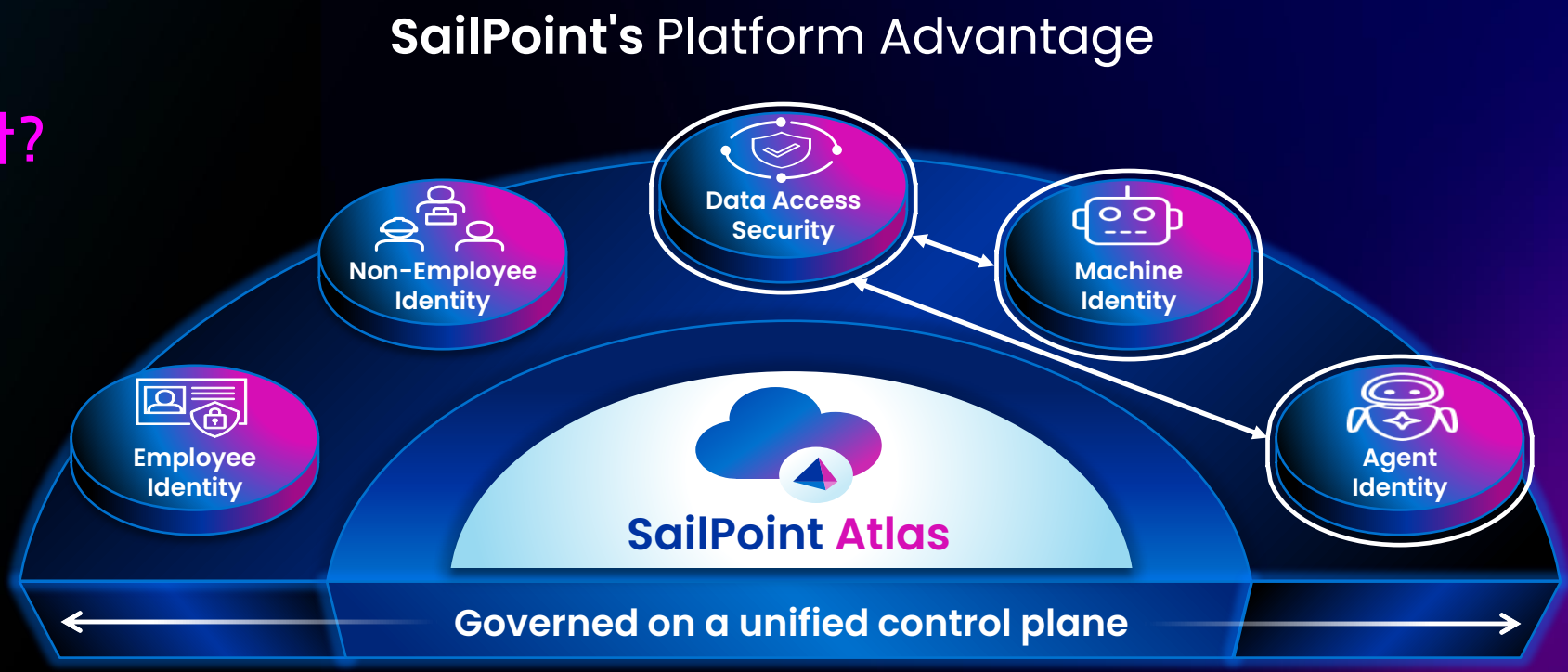
어떻게 해야 하나요?

… 직원이
액세스할 수 있는
AI Agent를
알고 계십니까?



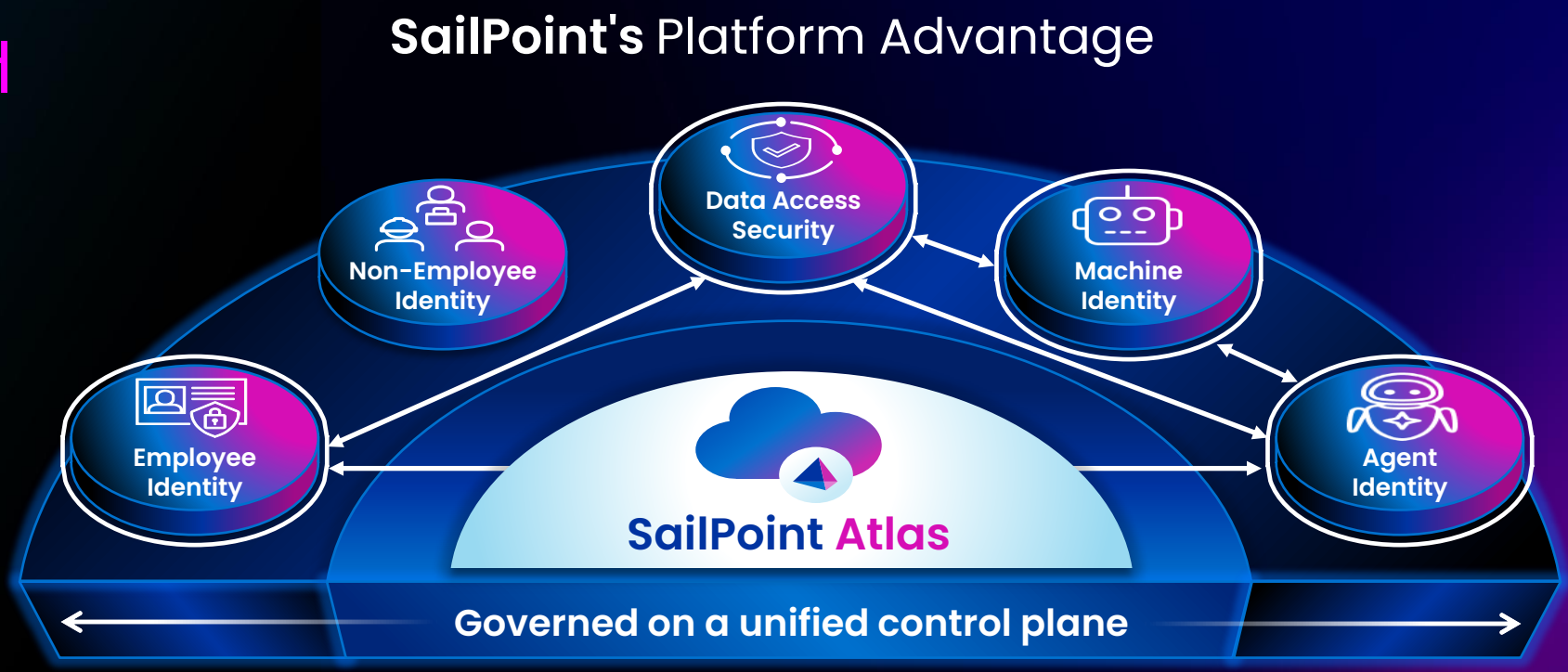
어떻게 해야 하나요?

... AI Agent가 어떤 도구에 액세스할 수 있는지 알고 계십니까?



어떻게 해야 하나요?

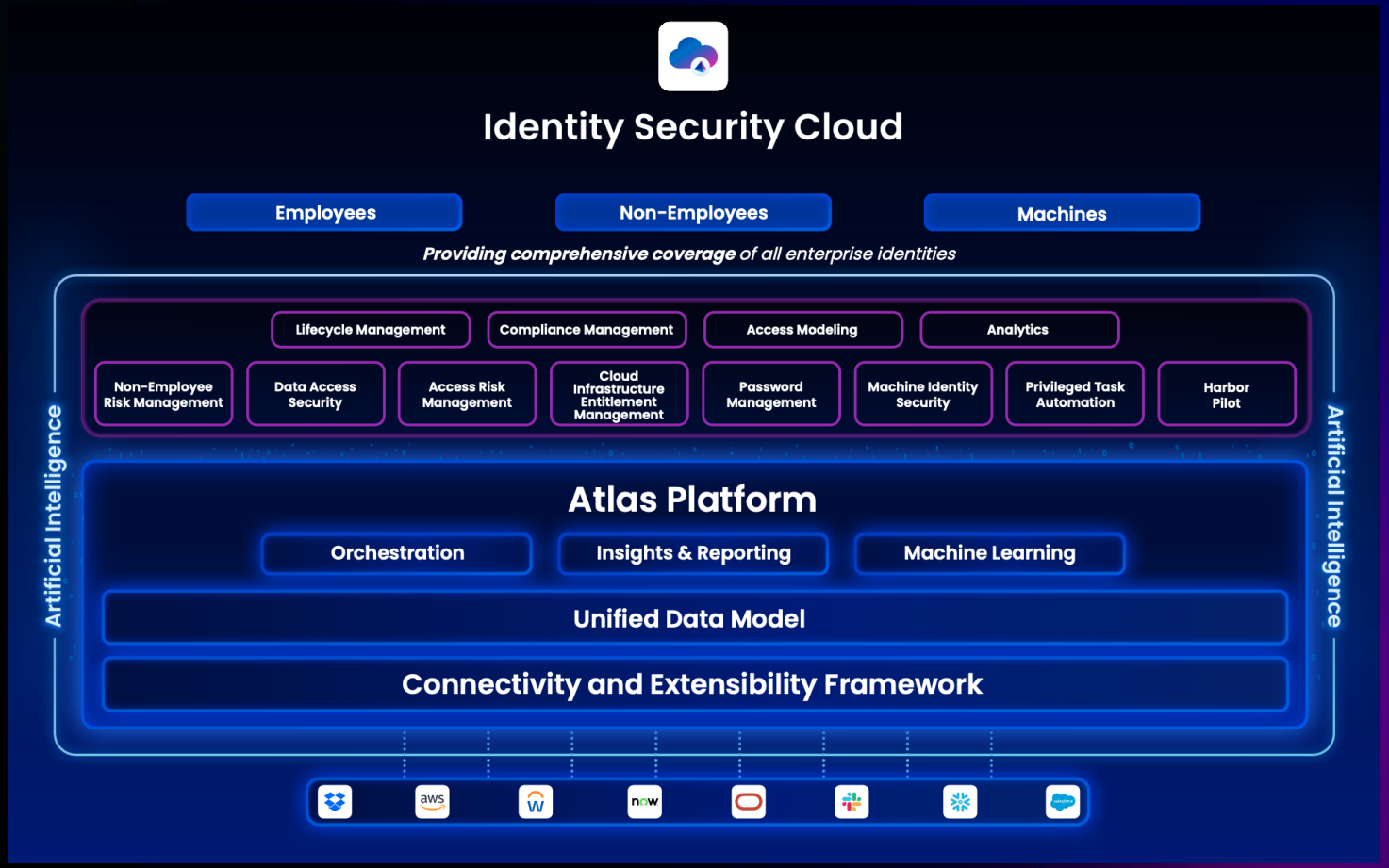
... AI Agent가
직원에게 무단 데이터
액세스 권한을
부여하지 않도록
합니까?



AI 시대를 위한 통합 아이덴티티 플랫폼 SailPoint Atlas

SailPoint의 SaaS제품군을 하나로 통합하고 확장하는 플랫폼

- 미션 크리티컬 수준의 연결성과 확장성
- 통합 데이터 모델
- 강력한 인사이트와 오케스트레이션 기능
- 더 적은 노력으로 더 많은 성과를 고객이 달성하도록 지원
- 모든 엔터프라이즈 아이덴티티를 위해 설계 됨



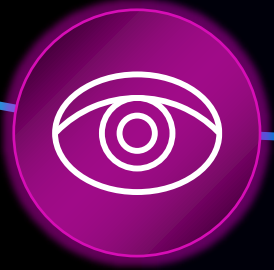
SailPoint Agent Identity Security (AIS)

SailPoint

Agent Identity Security (AIS)

SailPoint Agent Identity Security (AIS) 는 AI Agent의 아이덴티티 생애주기를 관리하고 통제하여 이들이 기업 업무 환경에 안전하게 통합될 수 있도록 지원합니다.

보안과 신뢰를 기반으로 AI의 잠재력을 안전하게 활용

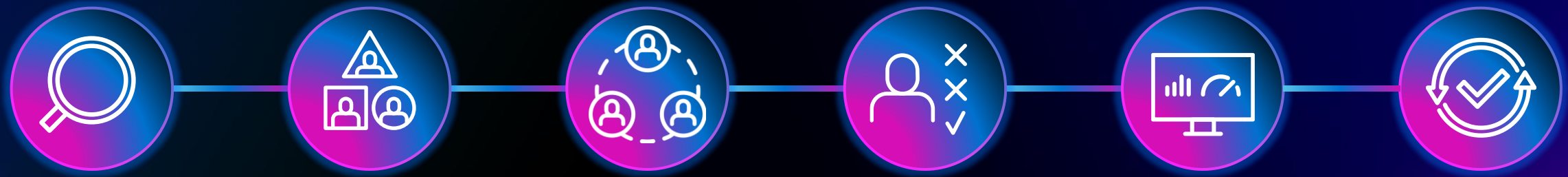


AI Agent와 그 사용자의 활동에 대한 완전한 가시성 확보

규제 대응을 위한 완전한 감사 추적(Audit Trail) 제공

AI Agent의 과도한 권한(Over-Permission) 부여 방지

AI Agent 통합 아이덴티티 거버넌스



AI Agent 식별 및 가시성 확보

책임 주체 지정

Agent·도구·사용자 거버넌스 강화

과도한 권한 부여 방지

데이터 접근 인사이트 확보

지속적인 리스크 감소 실현

가시성확보	책임 주체	거버넌스	데이터 관리 및 모니터링	보안강화
모든 AI Agent와 관련 리소스를 통합 수집하고 식별합니다.	각 Agent와 데이터, 툴의 소유자와 관리 책임을 명확히 정의합니다.	AI Agent와 사용자의 상호작용 및 권한을 정책 기반으로 관리합니다.	AI Agent가 불필요하거나 과도한 접근 권한을 갖지 않도록 통제합니다.	AI Agent의 데이터 접근 경로와 사용 행위를 가시화하고 분석합니다.	자동화된 통제와 지속적 모니터링을 통해 보안 리스크를 장기적으로 완화합니다.

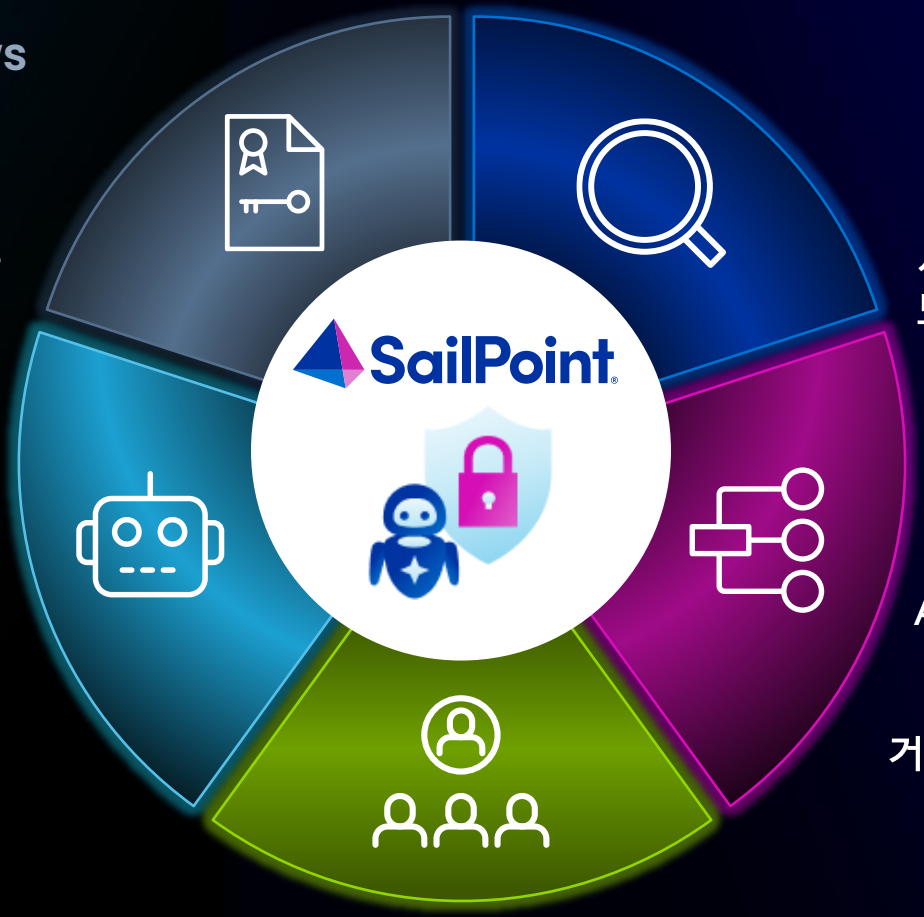
AIS 주요 활용 사례

AI agent reviews

AI Agent의 접근 권한을 주기적으로 검토하고 필요 시 접근 권한을 해제합니다.

Agent inventory

모든 AI Agent를 통합 관리합니다. 집계(Aggregation), 사용자 인터페이스(UI), 또는 엔드포인트를 통해 관리할 수 있습니다.



User authorization

인간 사용자의 AI Agent 활용을 통제하고, 과도한 권한을 탐지하여 방지합니다.

Tool governance

AI Agent의 서비스 계정을 생성부터 폐기(retirement)까지 거버넌스 정책으로 관리합니다.

Ownership & succession planning

모든 AI Agent의 소유권을 명확히 유지하고, 담당자 변경(퇴사자 발생 등) 시에도 책임이 지속되도록 관리합니다.

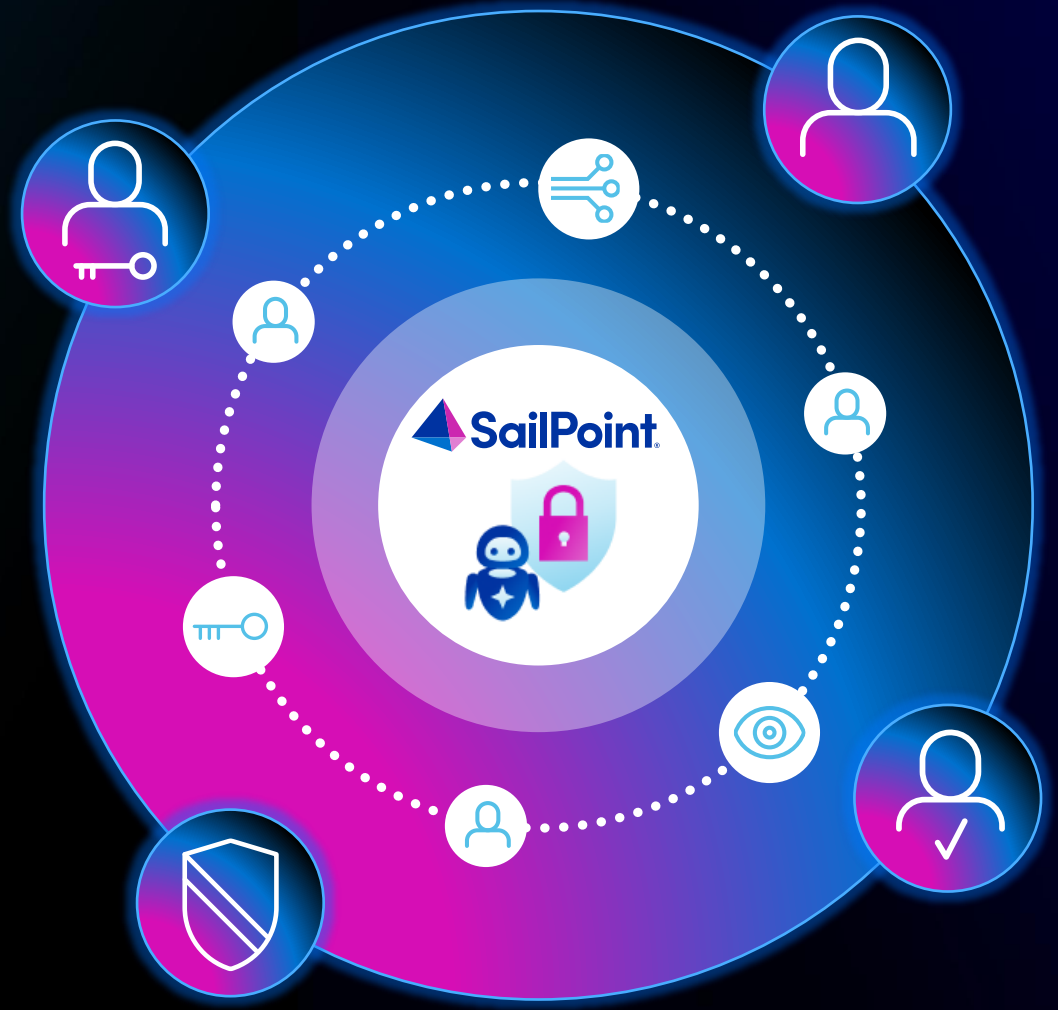
SailPoint Agent Identity Security가 조직에 제공하는 가치

CISO

AI가 통제 범위를 넘어서는 일이 없도록 보장합니다.

IGA teams

AI, 클라우드 운영(Cloud Ops), 보안팀과 함께 정책을 일관되게 적용하고 준수하도록 지원합니다.



Security teams

AI Agent와 사용자 전반의 위험한 접근 권한을 탐지하고 노출시킵니다.

CDO

AI Agent의 데이터 접근과 활용을 거버넌스 체계로 관리합니다.

3단계 AI Agent 아이덴티티 보안 전환 로드맵

가시성 확보

단기 (0 ~ 3 개월)

- AI Agent 아이덴티티 식별
- Owner 식별
- 접근 관계 가시화
- 위험 레벨 분류
- Shadow AI 탐지

거버넌스 정립

중기 (3 ~ 9 개월)

- AI Agent 라이프사이클 정책
- 권한 부여 표준화 및 승인 프로세스
- 액세스 검토 정책 적용
- 데이터 접근정책 연동
- IGA 플랫폼 통합

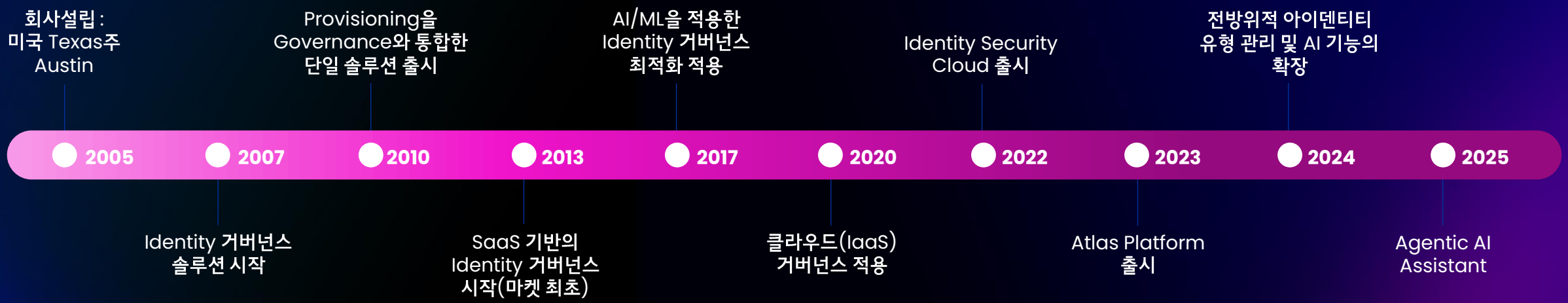
지속적인 관리

장기 (9 ~ 18 개월)

- AI 이상행동 탐지
- AI 기반 정책 엔진
- 자동화된 조치
- AI 거버넌스 분석 리포트
- Zero-Trust AI운영

SailPoint 회사소개

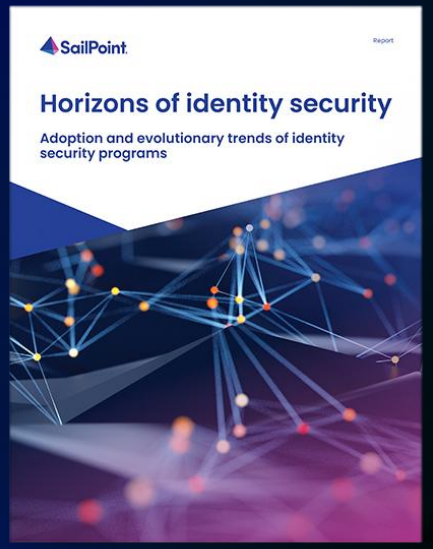
SailPoint는 2005년 미국 Texas주 Austin에서 시작되어 현재 아이덴티티 보안(Identity Security) 분야의 Global Leader로서, 전 세계 155개국에서 3,000개 이상 기업 고객에게 Unified Identity Security Platform을 통한 아이덴티티 보안 솔루션을 제공해 드리고 있습니다.



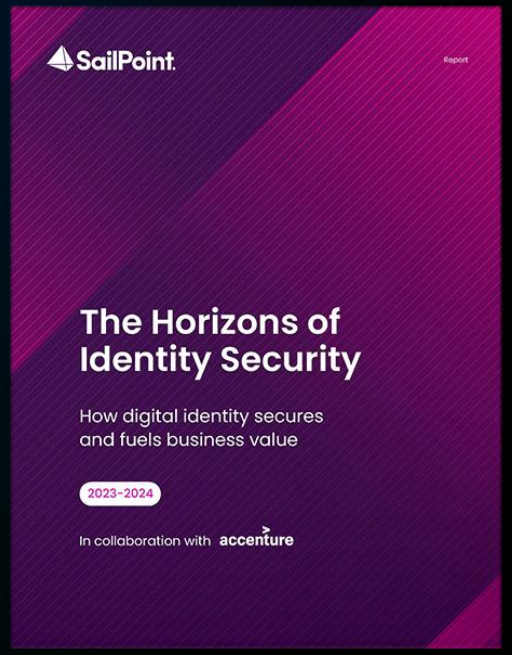
Certifications

SOC 1, 2, 3 | ISO 27001:2022, 27017, 27018, 27701 | FedRAMP | CSA STAR Level 1 | C5 | IRAP | Common Criteria

SailPoint Horizon Report



2023

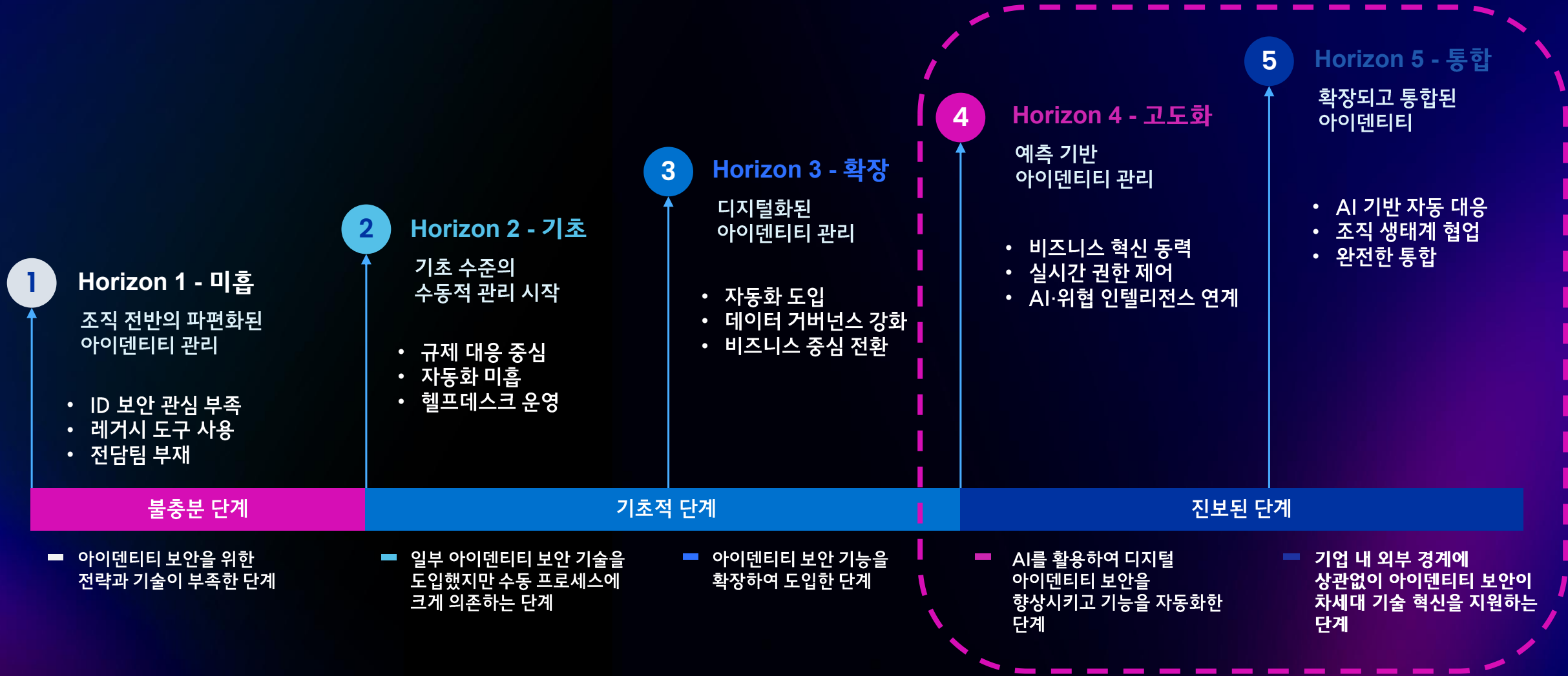


2023-2024

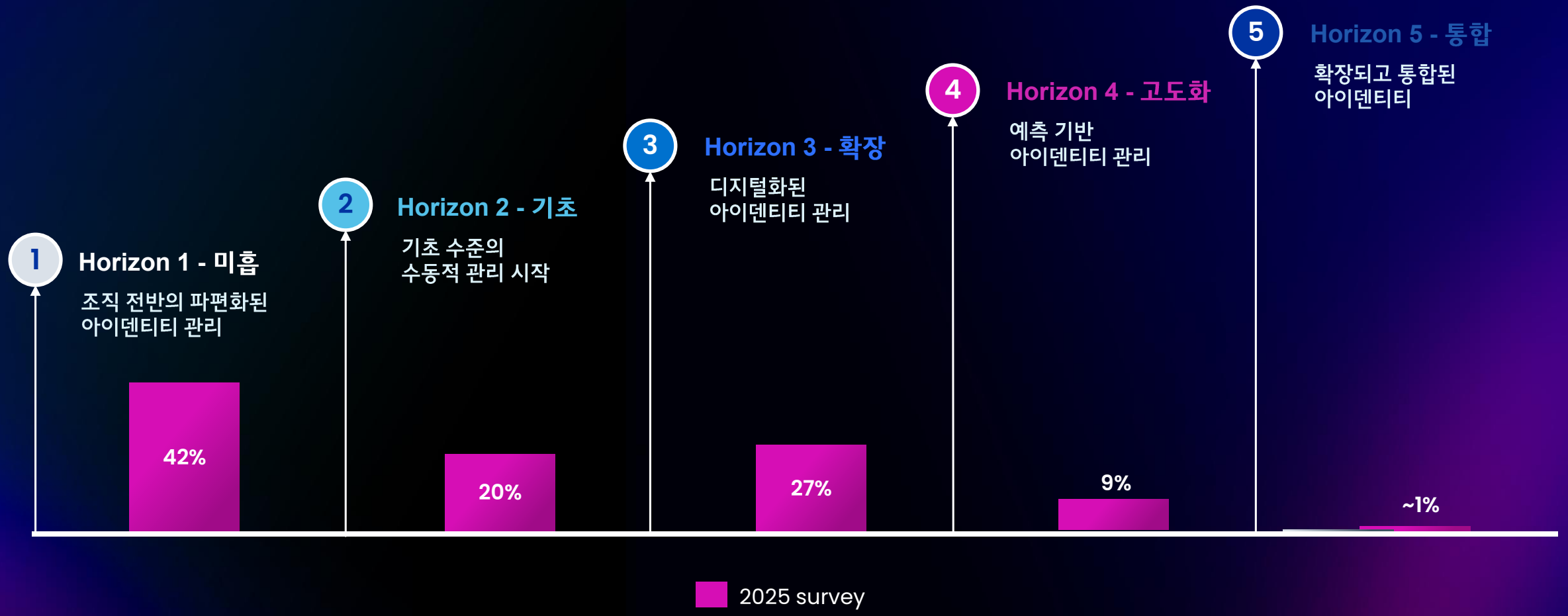
2024-2025

2025-2026

Horizon 아이덴티티 보안 성숙도 5단계 모델



많은 조직이 아직 시작 단계에 머무르고 있습니다



고객 성공 사례 1. Horizon 1 → 2

Specsavers

파편화에서 표준화로

2,600개 매장, 11개국 직원들의 권한 관리를 하나로 통합하다.

조직 개요

- Specsavers는 11개국에 2,600개 매장을 운영하는 글로벌 리테일 기업으로, 급격한 성장에 따라 확장 가능한 아이덴티티 보안 체계를 구축하고 전 세계 직원들의 접근을 일원화(Unify)하는 것이 목표였습니다.

과제 (Challenges)

- 국가별 HR 및 급여 시스템이 분산, 통합 거버넌스 부재
- 아이덴티티 소유권 및 전략이 명확하지 않음
- 수천 개의 중복 또는 고아 계정 존재, 관리 불가

조치 (Actions Taken)

- 아이덴티티 성숙도 평가를 통한 구조적 로드맵 수립
- 중복 계정 식별 및 제거로 신뢰할 수 있는 단일 원천 (HR) 구축
- 전담 IAM 팀 구성, 경영진 후원 및 명확한 책임체계 확립
- Joiner / Mover / Leaver 자동화 프로세스 구현

성과 (Outcomes)

- 10배 이상 더 많은 계정 통합 관리
- 2,000개 비활성 계정 제거
- 전사 직원 42,000명 접근 자동화 관리
- 온보딩/오프보딩 프로세스 일관성 확보
- IT 운영 비용 절감 및 감사 대응 시간 단축

고객 성공 사례 2. Horizon 2 → 3

Temple Health

자동화와 효율성 중심의 전환

20,000명의 직원을 위한 접근 관리, 수작업의 한계를 넘어서다.

조직 개요

- Temple Health는 미국의 대형 의료기관으로 20,000명 이상의 의료진과 직원이 다양한 헬스케어 시스템을 사용합니다.
  그러나 기존의 온보딩과 권한 부여 과정이 대부분 수작업으로 운영되어 보안·운영·시간 효율성 측면에서 심각한 부담이 있었습니다.

과제 (Challenges)

- 20,000명 이상 사용자 계정의 수작업 프로비저닝
- 역할 기반 접근 자동화 부족
- 헬스케어 시스템 간 중앙 가시성 부재

조치 (Actions Taken)

역할 템플릿 기반의 자동 프로비저닝 규칙 설계
RBAC 시스템 구현으로 접근 자동화
온프레미스와 클라우드 시스템을 연결하는 통합 커넥터 구축
접근 승인·변경 프로세스의 표준화 및 자동 트리거화

성과 (Outcomes)

- 온보딩 소요시간 99% 감소 (120시간 -> 1.5시간)
- 패스워드 초기화 시간 93% 감소 (30분 -> 2분)
- IAM 운영 인력 60% 절감 (10명 -> 4명)

고객 성공 사례 3. Horizon 3 → 4+

AI 기반 아이덴티티 자동화의 선도자

AI를 활용해, 23만 명의 글로벌 워크포스를 자동화된 보안 체계로 운영하다.

조직 개요

- Wipro는 전 세계 66개국에 230,000명 이상의 직원을 보유한 글로벌 IT 서비스 기업으로, 빠르게 성장하는 인력 규모와 하이브리드 클라우드 환경에서 아이덴티티 생애주기 관리(Identity Lifecycle Management) 의 자동화와 통합이 핵심 과제였습니다.

과제 (Challenges)

- 보안 기술 격차 – 인력의 역량 불균형
- 사람과 기계의 이원화된 아이덴티티 시스템
- 하이브리드 환경에서의 동적 규제 대응 어려움

조치 (Actions Taken)

- AI 기반 보안 도구 및 적응형 통제 교육 및 내재화
- 온보딩·권한관리·비활성화 등 모든 ID 라이프사이클 업무 자동화
- 실시간 리스크 분석 및 권한 검토에 AI 도입
- 전사 정책과 DevSecOps 체계 내에 AI 기반 거버넌스 연계 구축

성과 (Outcomes)

- 95%+ 사용자 만족도
- 50%+ 아이덴티티 관련 작업의 AI 자동화
- 100% 신규 사용자(직원) 1일차 자동 온보딩 달성





"AI가 혁신의 속도를 이끈다면,
아이덴티티 보안은 그 혁신의 방향을 바로잡습니다."





Thank you!