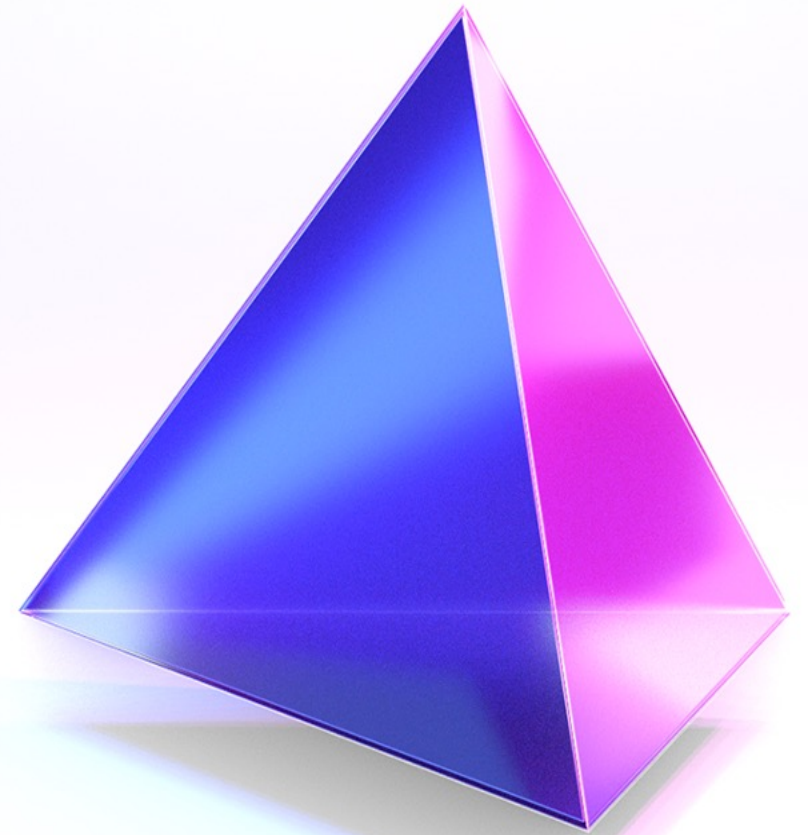


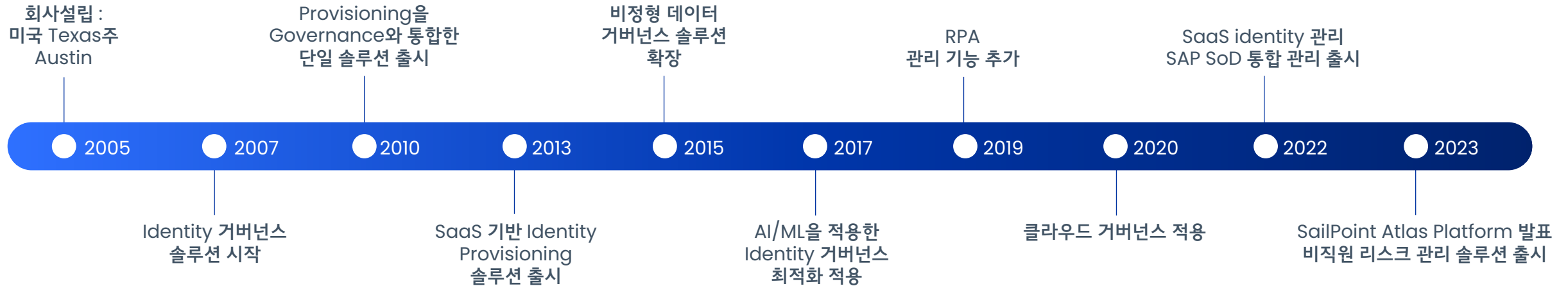
제로트러스트의 초석 :

AI 기반의 아이덴티티 보안



SailPoint 회사소개

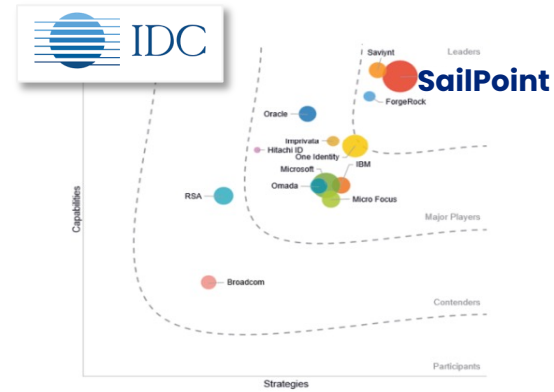
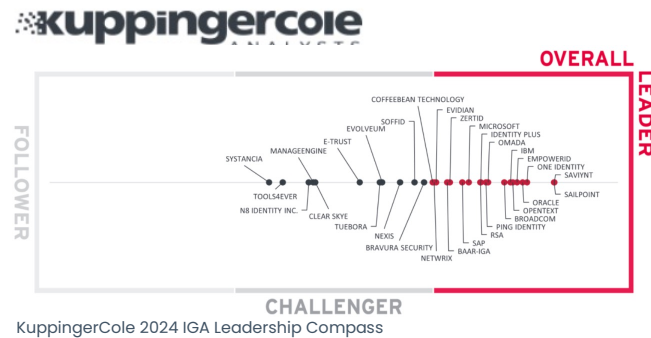
SailPoint는 2005년 미국 Texas주 Austin에서 시작되어 현재 아이덴티티 보안(Identity Security) 분야의 Global Leader로서, 전 세계 155개국에서 3,000개 이상 기업 고객에게 Unified Identity Security Platform을 통한 아이덴티티 보안 솔루션을 제공해 드리고 있습니다.



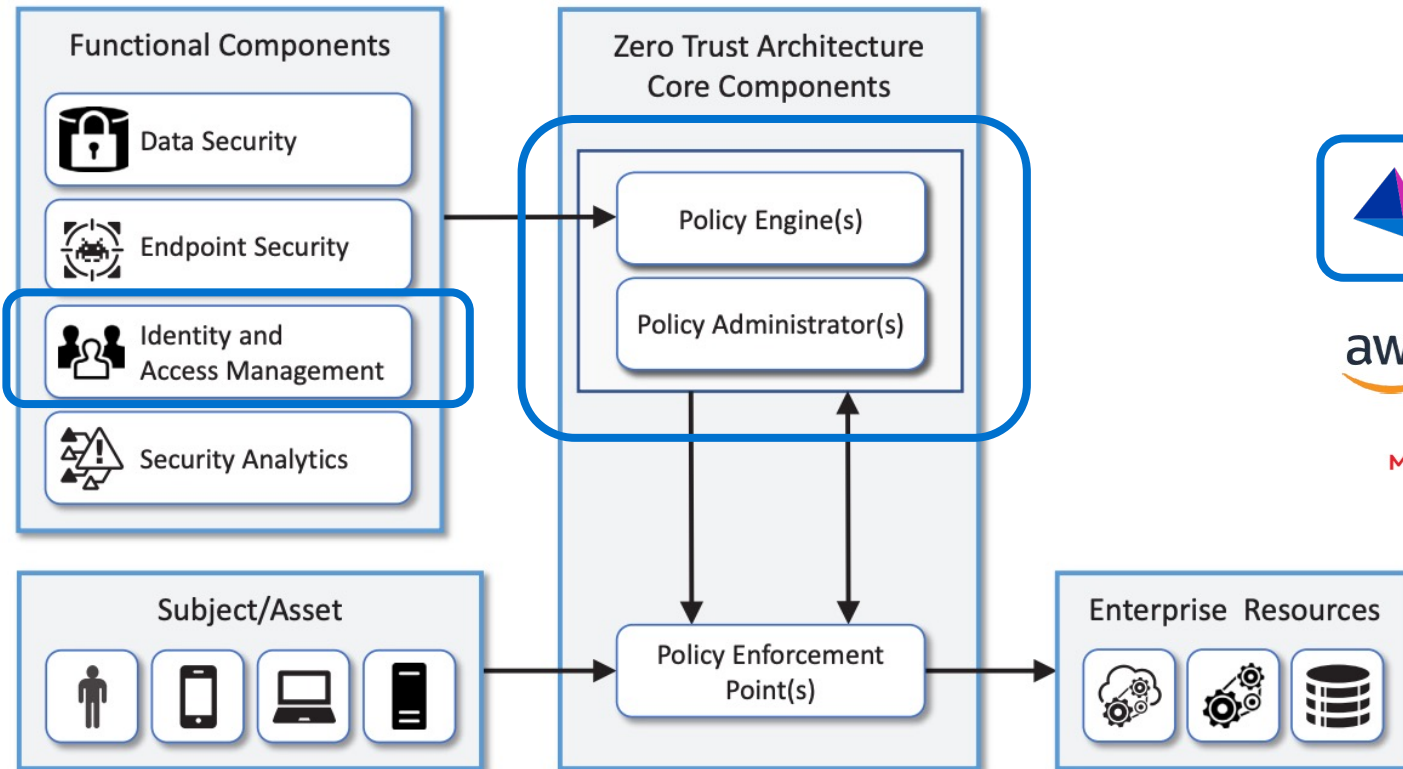
SailPoint

성장을 위한 지속적인 노력

- 전세계 직원 수: 2,500명 +
- 연간 연구 개발비: \$ 9천 8백만 +
- 연구 개발 투입 공수: 470M/M +



NIST NCCoE ZTA Project Partner SailPoint



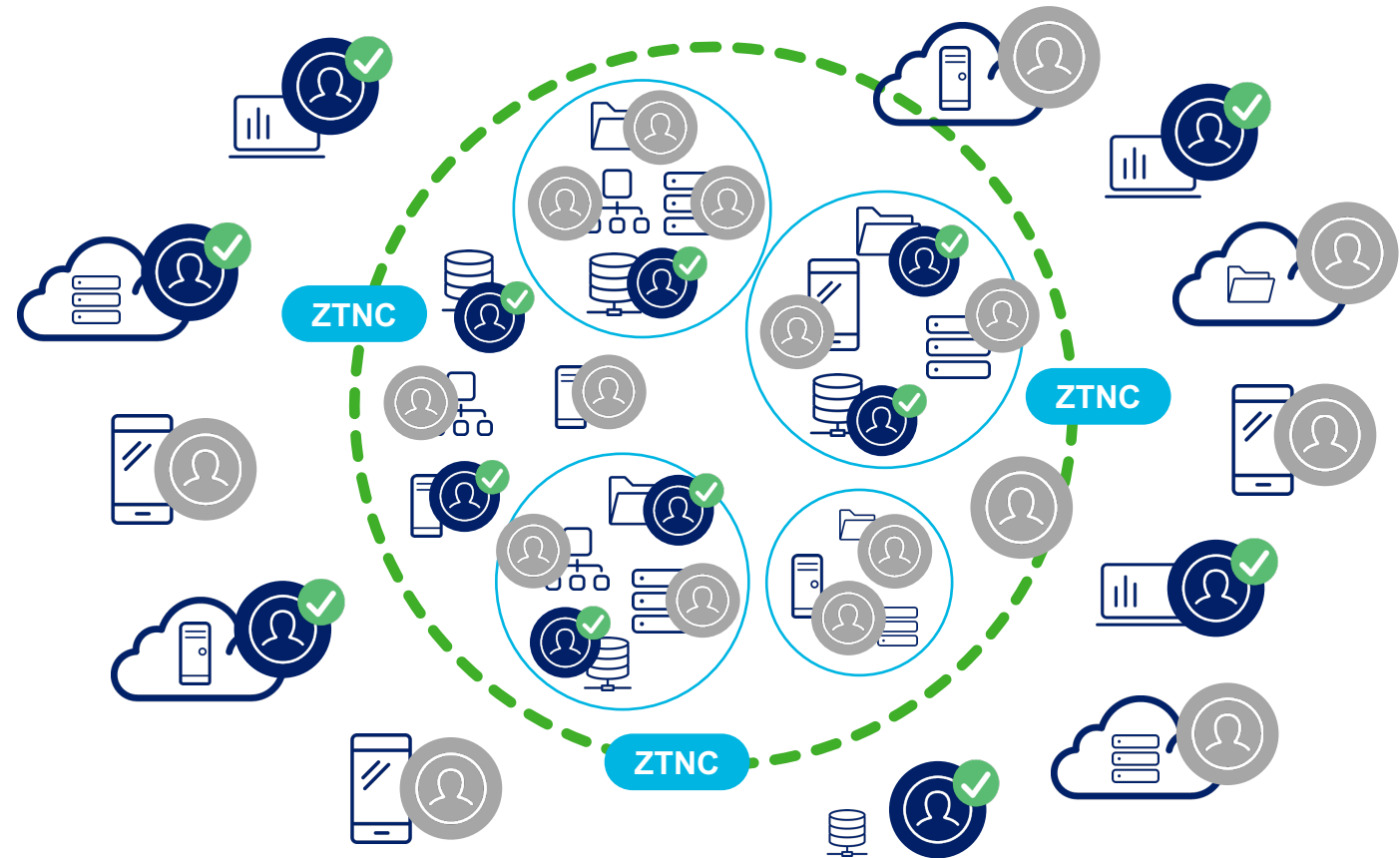
<https://www.nccoe.nist.gov/projects/building-blocks/zero-trust-architecture>

Zero Trust

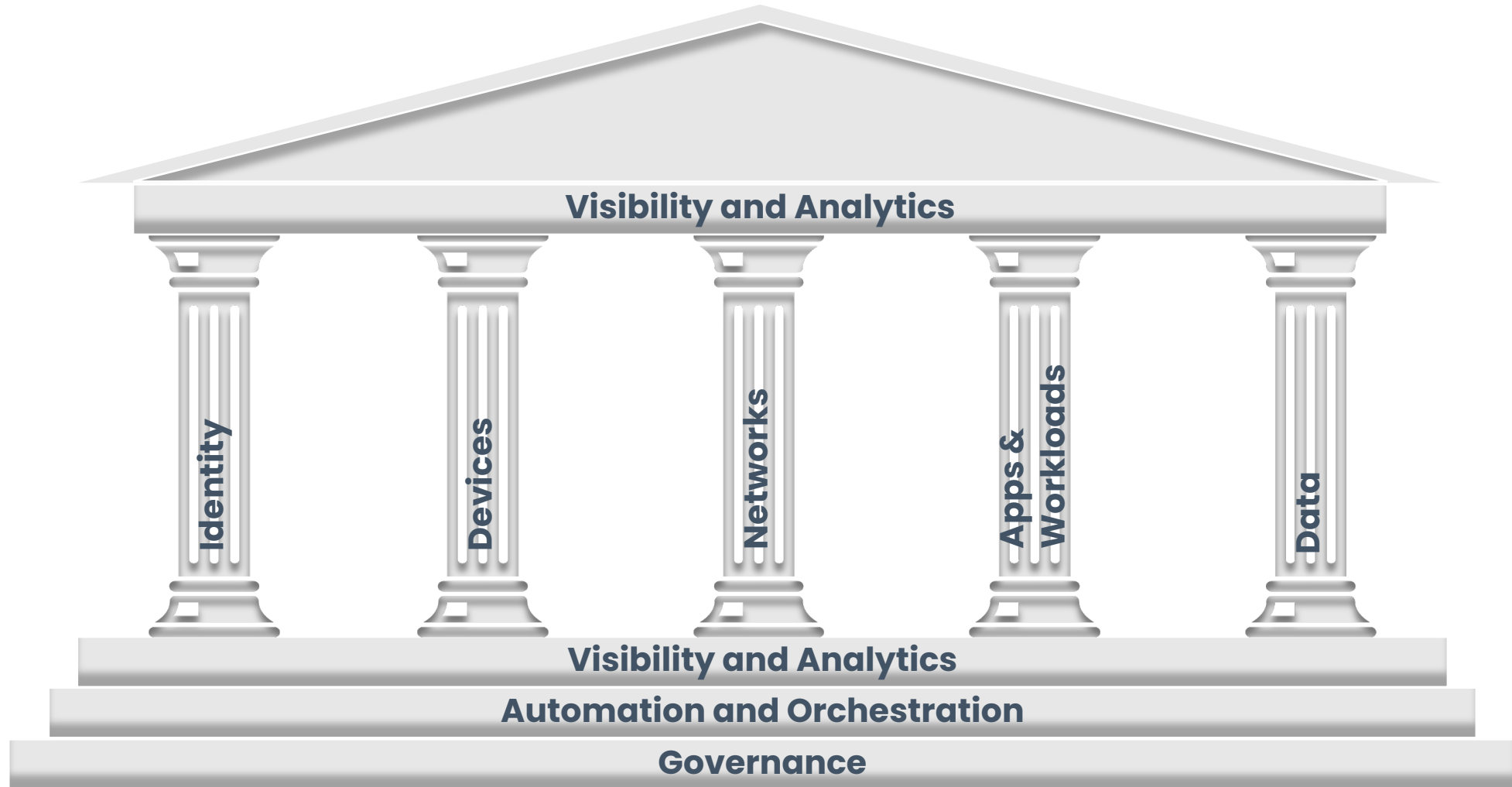
Never Trust, Always Verify

네트워크가 이미 침투당했다는 관점에서 정보 시스템 및 서비스에서 '정확한', '최소 권한의', '요청 단위 접근 결정'을 강제하여 불확실성을 최소화하기 위해 설계된 개념과 아이디어 모음

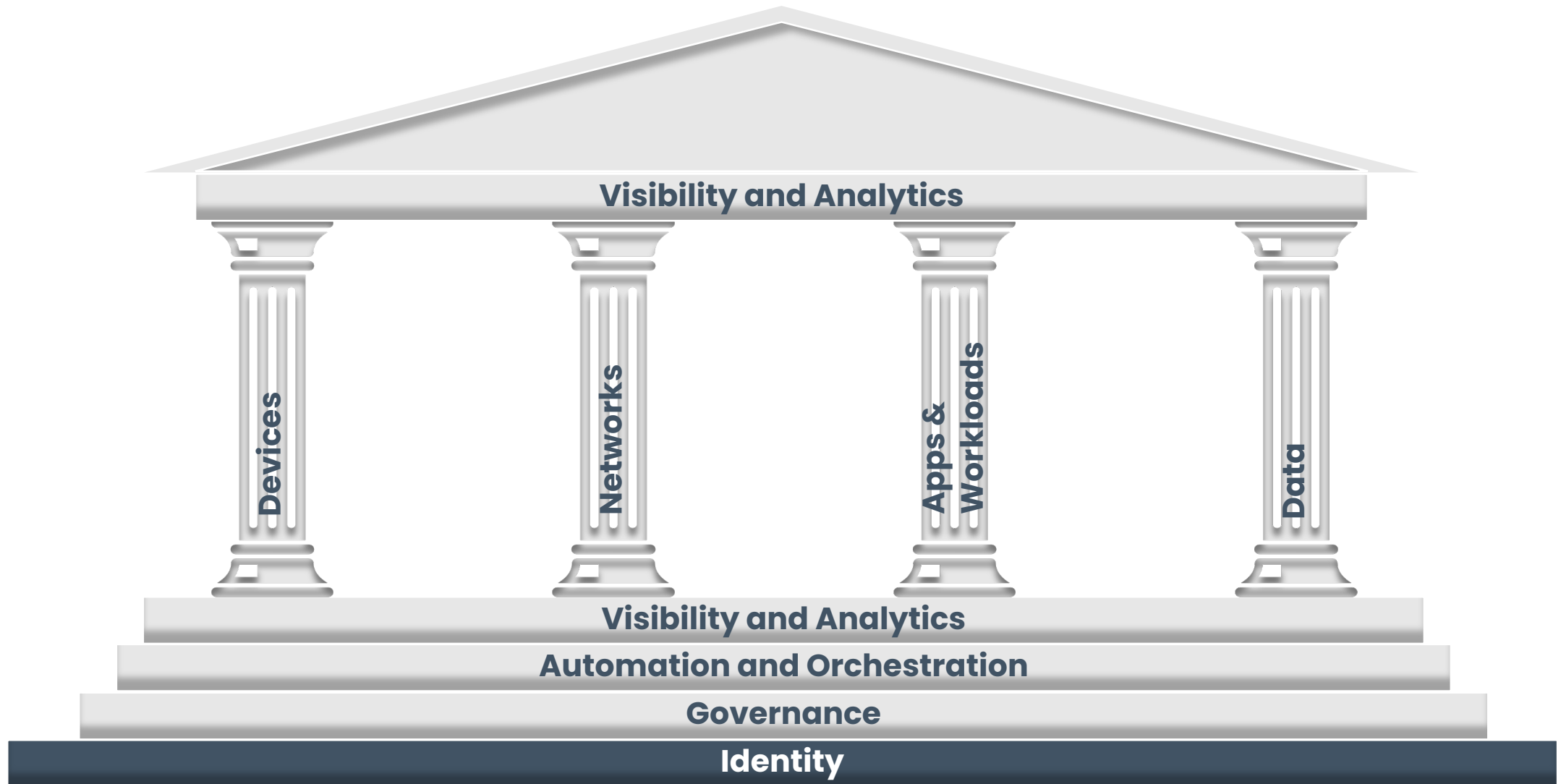
NIST SP 800-207, 'Zero Trust Architecture'



제로트러스트의 기둥



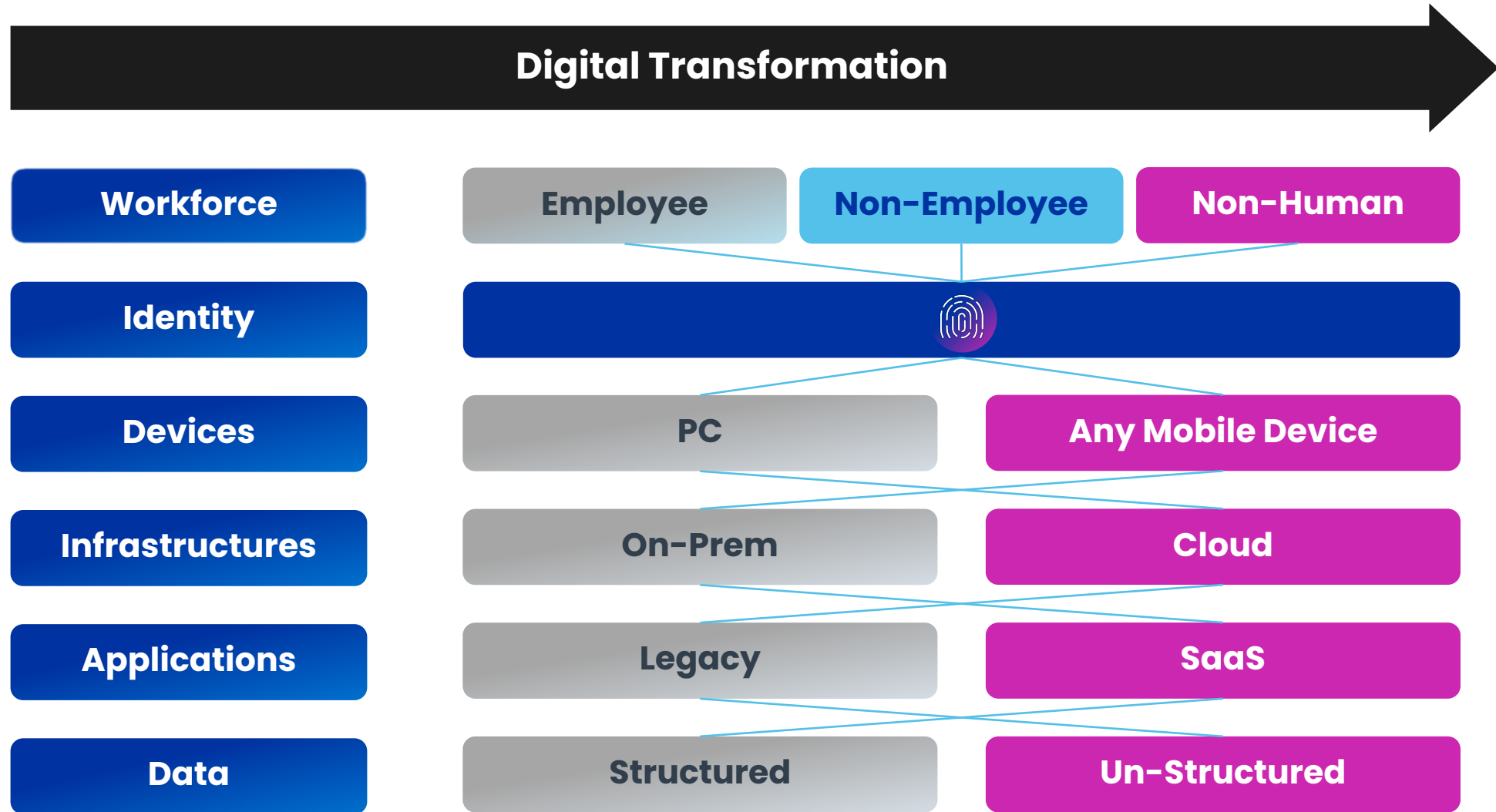
제로트러스트의 기둥



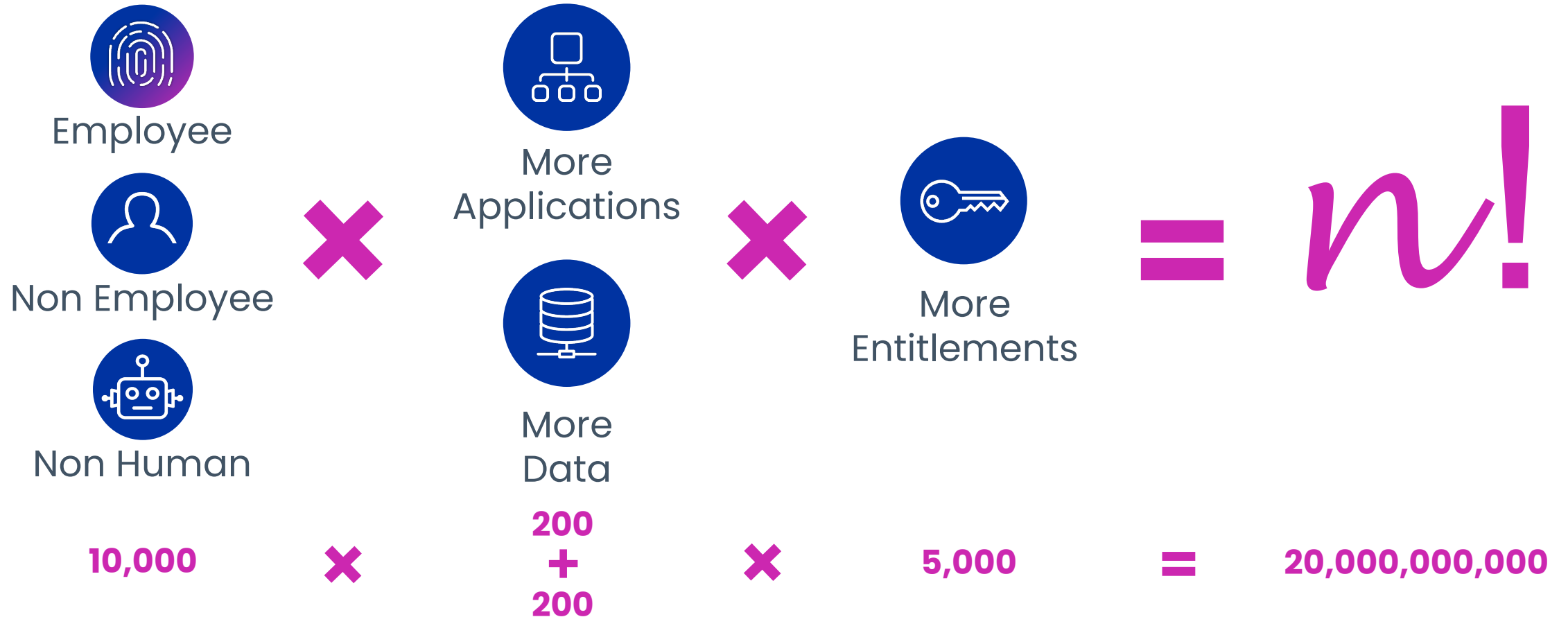
아이덴티티의 의미 그리고 아이덴티티 보안이란?



Digital Transformation 시대의 아이덴티티



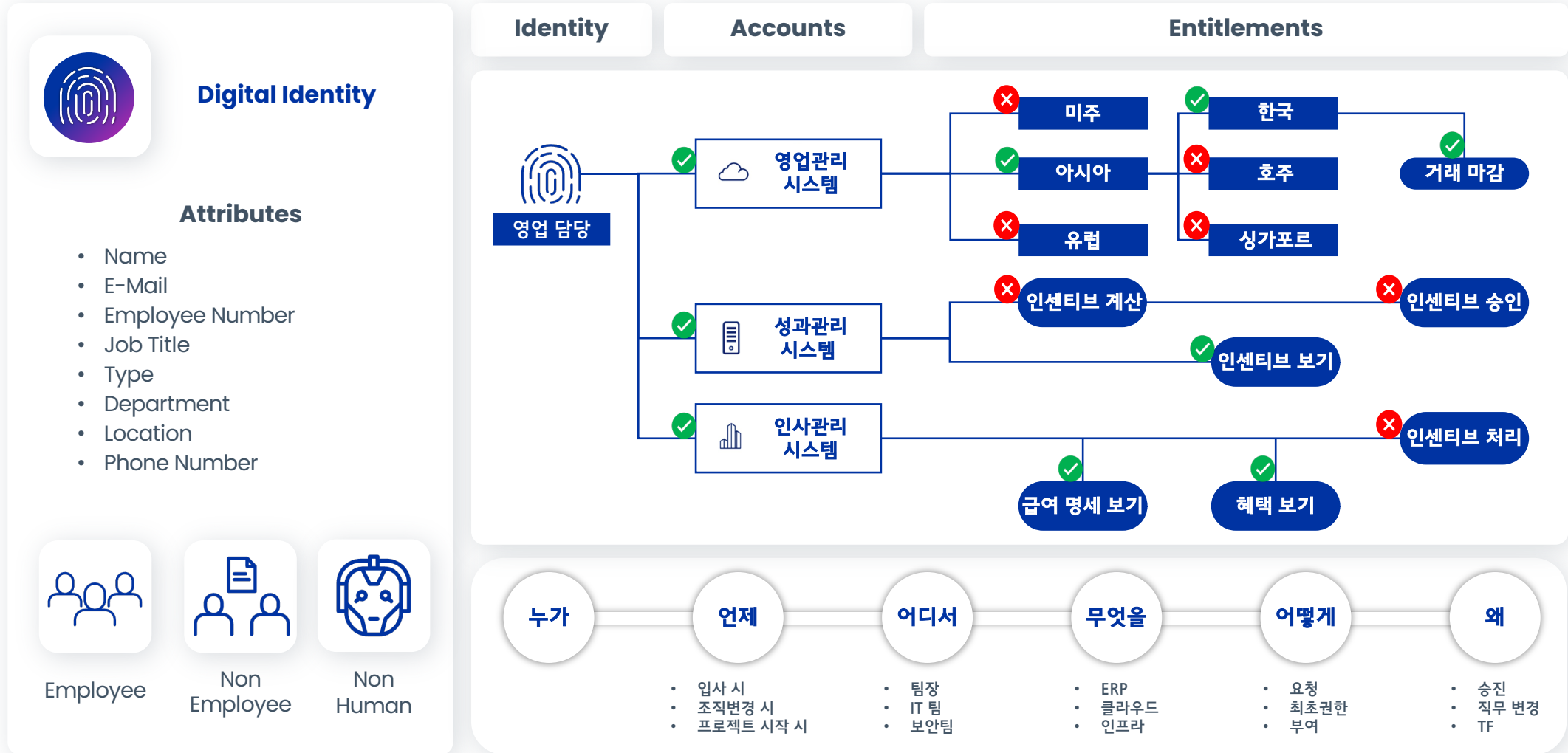
감당할 수 없는 복잡성 아이덴티티에 부여되는 경우의 수



아이덴티티 보안의 위협 요소



아이덴티티 및 아이덴티티 보안이란?



아이덴티티 보안이란?



Never Trust, Always Verify

SailPoint® 는 어떻게 아이덴티티 보안을 구현하나요?

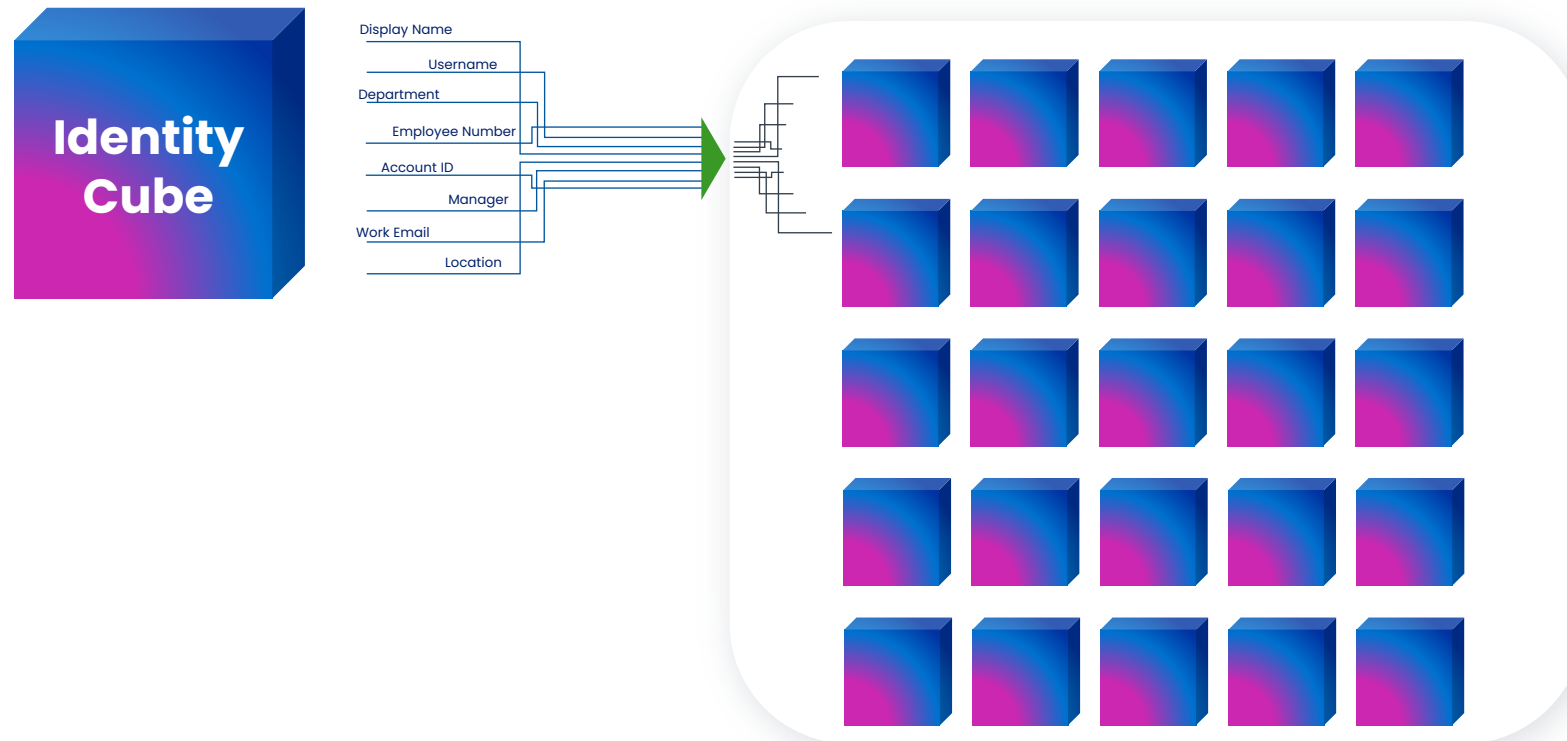
Identity Cube

기존 정보 시스템 및 타겟 시스템으로부터 모든 필요한 정보를 수집하여 Cube 형태로 사용자 기준의 계정 권한 정보 수집



Identity Warehouse

수집된 아이덴티티 기반 정보를 아이덴티티 웨어하우스에 통합 저장 관리

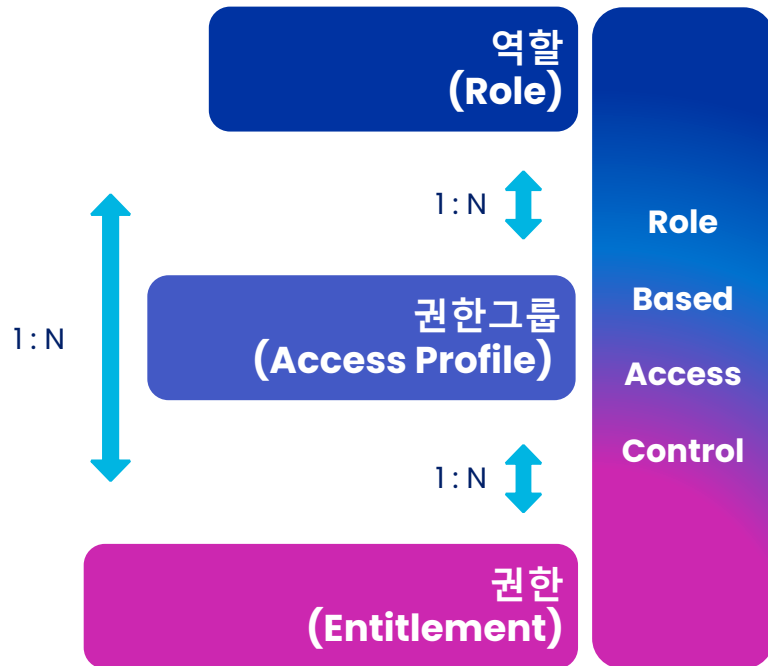


Identity Security Platform
Identity Warehouse

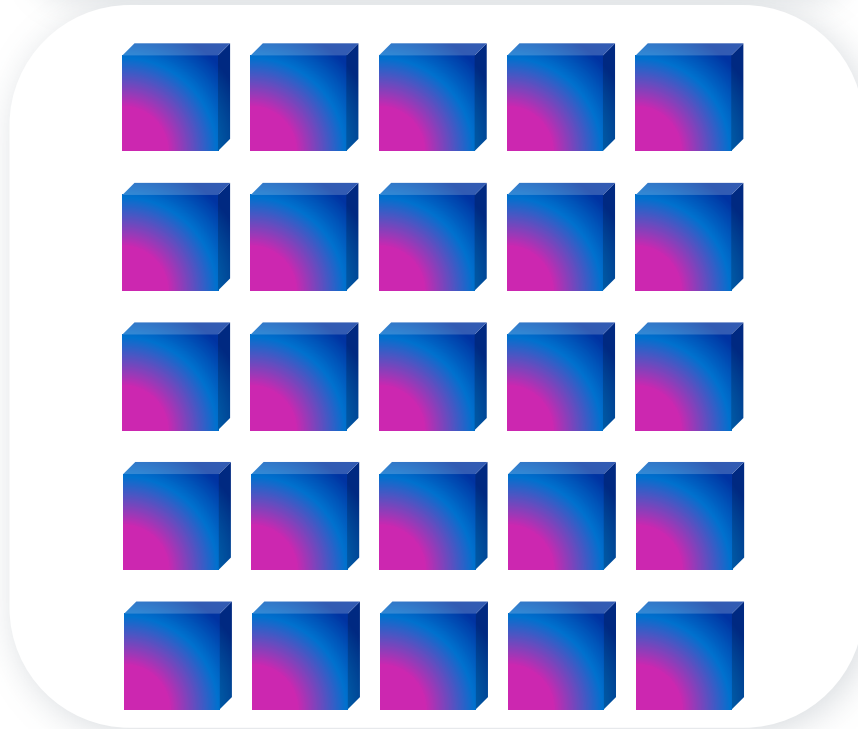
아이덴티티 정보 기반 권한 및 정책 설정

전사 차원에서 통합된 아이덴티티 정보를 토대로 조직 부서에 맞는 역할별 권한 설정 및 사내 정책 설정 관리

권한 관리

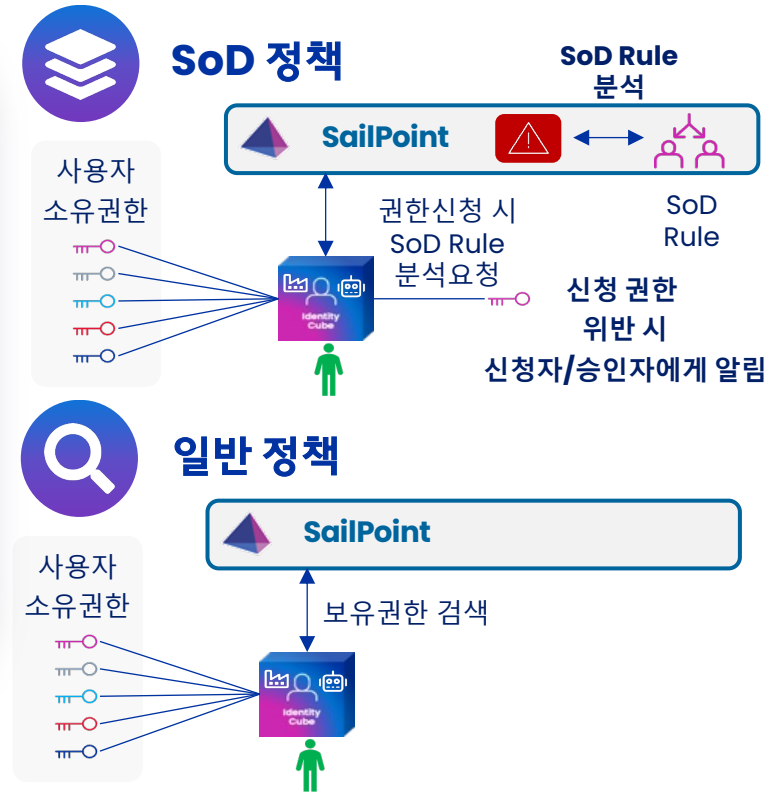


- Lifecycle Management
- Compliance Management
- Access Modeling
- Analytics



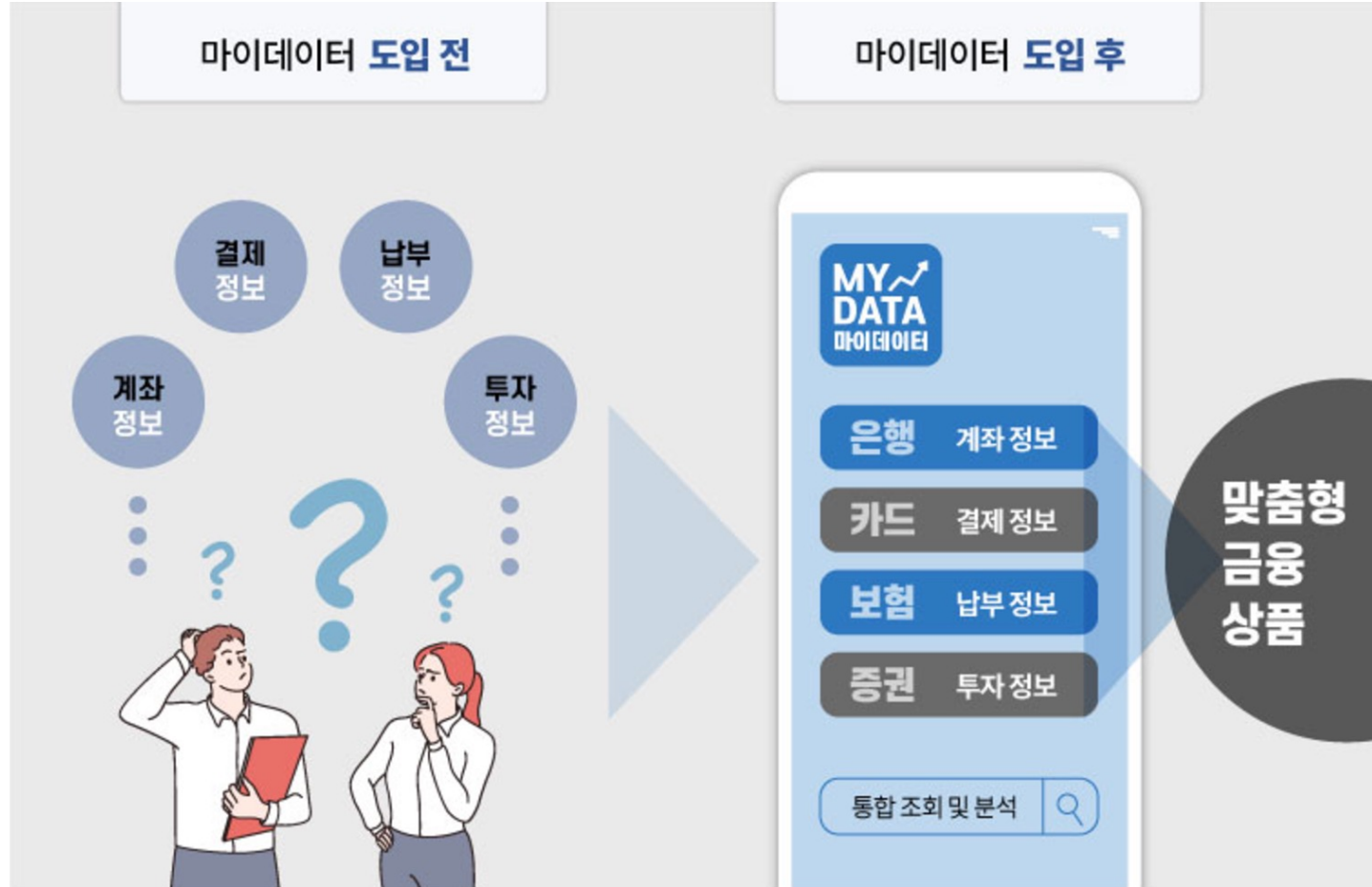
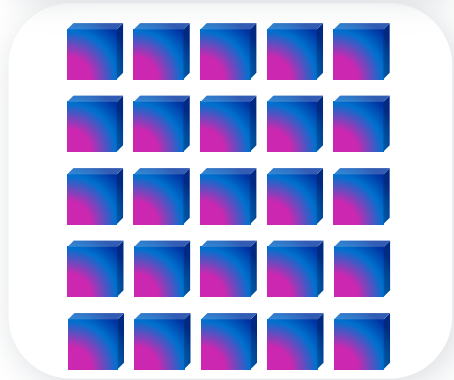
Identity Security Platform
Identity Warehouse

정책 관리



금융 마이데이터와의 공통점

Sailpoint Identity Security Platform Warehouse



은행(계좌정보), 카드회사(결제정보), 보험회사(납부정보) 등에 흩어져 있는 정보를 한눈에 파악하기 어려움

마이데이터 서비스를 통해 흩어져 있는 개인신용정보를 한번에 확인하고 통합 분석이 가능

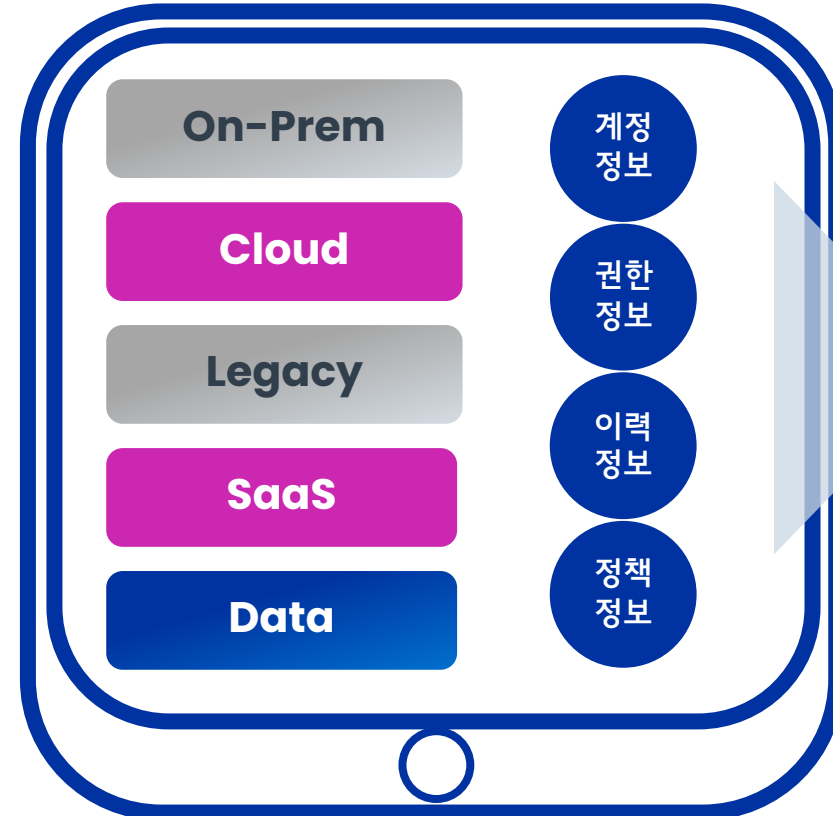
아이덴티티 보안을 위한 전방위적 가시성 확보

세일포인트 도입 전



인프라(온프레미스, 클라우드), 애플리케이션(레거시, 클라우드), 데이터(정형, 비정형) 등에 흩어져 있는 정보를 한눈에 파악하기 어려움

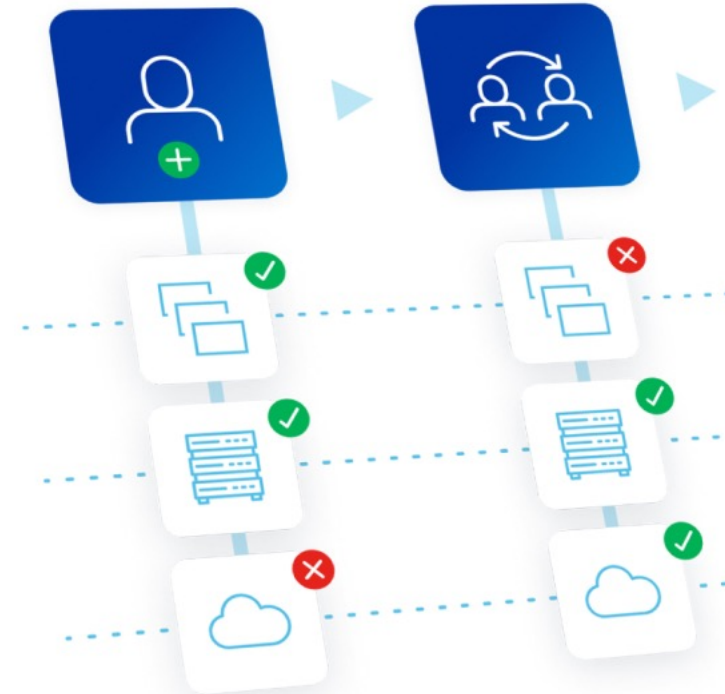
세일포인트 도입 후



세일포인트 아이덴티티 시큐리티 클라우드를 통해 흩어져 있는 정보를 한번에 확인하고 통합 분석이 가능

맞춤형
계정
권한
관리

 **SailPoint**® 를
도입하면 어떤 이점을
얻을 수 있나요?



이점 1. 사용자 상태 기반의 계정 권한 처리 자동화

사용자의 입사 및 퇴사, 인사 이동 등의 부서 또는 직무 변경에 따라 계정/권한 부여와 회수를 자동화



이점 2. 권한 신청, 승인 프로세스의 인사이트 확보

사용자는 역할을 통해 부여된 권한 외 업무 상 추가로 필요한 권한/권한그룹/역할을 직접 신청

신청 권한 제공 기준

Access Request Recommendations

- 사용자의 속성과 유사한 그룹을 분석하여 신청 권한에 대한 권장사항을 제공

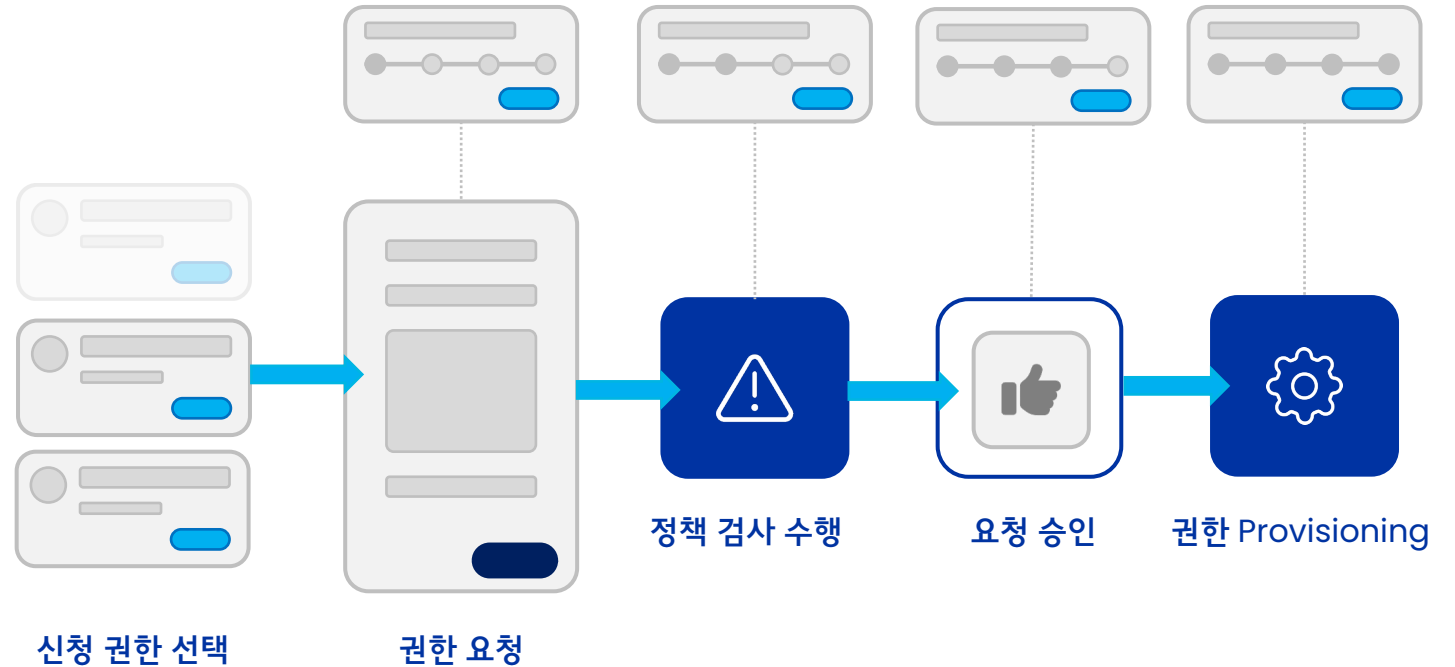
Application

- 가상 권한그룹 형태로 시스템 혹은 시스템 내 상세 업무 기준과 같이 구분하며 Access Profile로 구성

Role

Access Profile

Entitlement



이점 3. 지속적인 역할 모델 적용

기존 정의된 역할 모델에 사용자의 보유 권한을 분석하여 새로운 권한을 추가 혹은 신규 역할을 생성하여 **지속적인 역할 기반 접근 제어 모델**을 적용

RBAC 유지 및 개선을 위한 단계

1단계 - 권한 가시성 확보

- 사용자에게 할당된 역할과 개별 신청하여 획득한 권한을 확인

2단계 - 역할 및 권한 사용분포 분석

- 사용자의 속성(부서,직무,위치 등)을 비교하여 유사 그룹 간의 역할 및 권한 분포 분석

3단계 - 역할 모델 개선 및 생성

- 분석된 정보를 기준으로 기존의 역할에 권한을 추가 혹은 신규 역할 생성을 제시



이점 4. 주의 필요 사용자 자동 분류

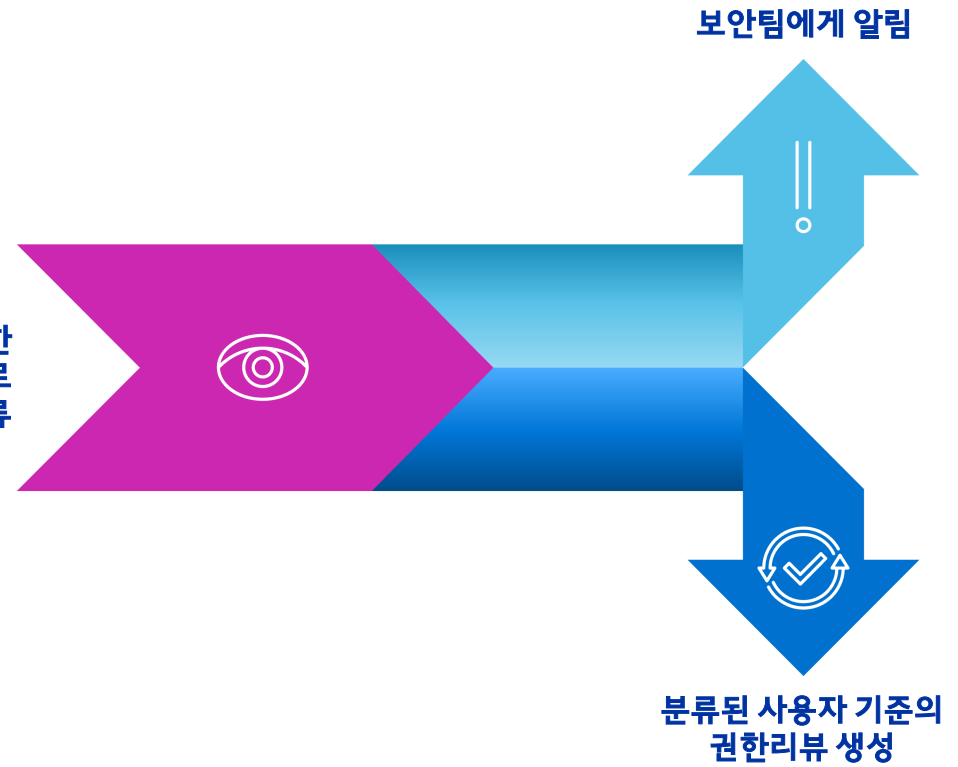
AI를 이용하여 분류 기준에 따른 점수 산정으로 주의가 필요한 사용자를 분류

요주의 사용자 분류

Outlier 분류 기준

- 사용자의 속성과 유사한 그룹을 분석하여 유사성이 낮은 경우
- 전체 권한 분포를 분석하여 대부분이 보유하고 있지 않은 권한을 보유
- 보유하고 있는 권한의 수량이 과도한 경우
- 다른 권한그룹(Access Profile) 및 역할(Role)의 고유성이 높은 경우
- 역할(Role)에 단일 권한만 포함된 경우

AI/ML를 이용한
유사 그룹 분석으로
Outlier 분류



이점 5. 지속적인 권한 리뷰 프로세스 적용

승인권자 및 의사결정권자, 시스템 담당자를 대상으로 계정 및 권한에 대한 리뷰 프로세스 적용으로 사용자 보유 권한의 적절성을 검토

권한리뷰를 통한 최소 권한 유지

권한리뷰 캠페인

- 권한리뷰 캠페인 생성으로 주기적인 권한 리뷰 수행

권한 조정

- 사용자의 부적절한 권한에 대해 의사결정자는 즉시 회수 명령하여 권한을 적절성을 유지

권고사항 제시

- 사용자의 속성과 유사한 그룹을 분석하여 의사결정을 위한 권고사항 정보를 제공

권한 리뷰 기준



사용자



권한



역할



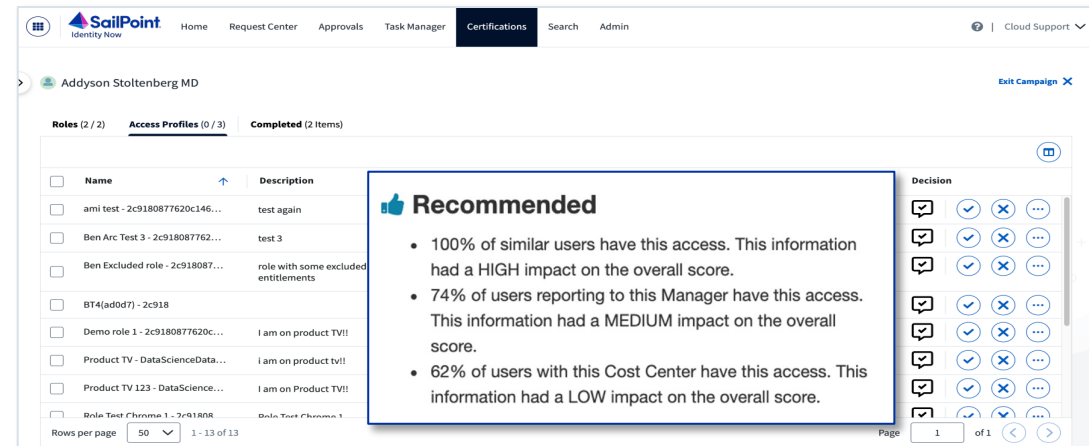
비상관 계정



SoD 정책



일반 정책



이점 6. 사용자 계정 권한 이벤트 이력 관리 및 가시성 확보

사용자의 입사부터 퇴사까지 계정 및 권한에 대한 부여/회수 이벤트를 확인하여 감사 대응

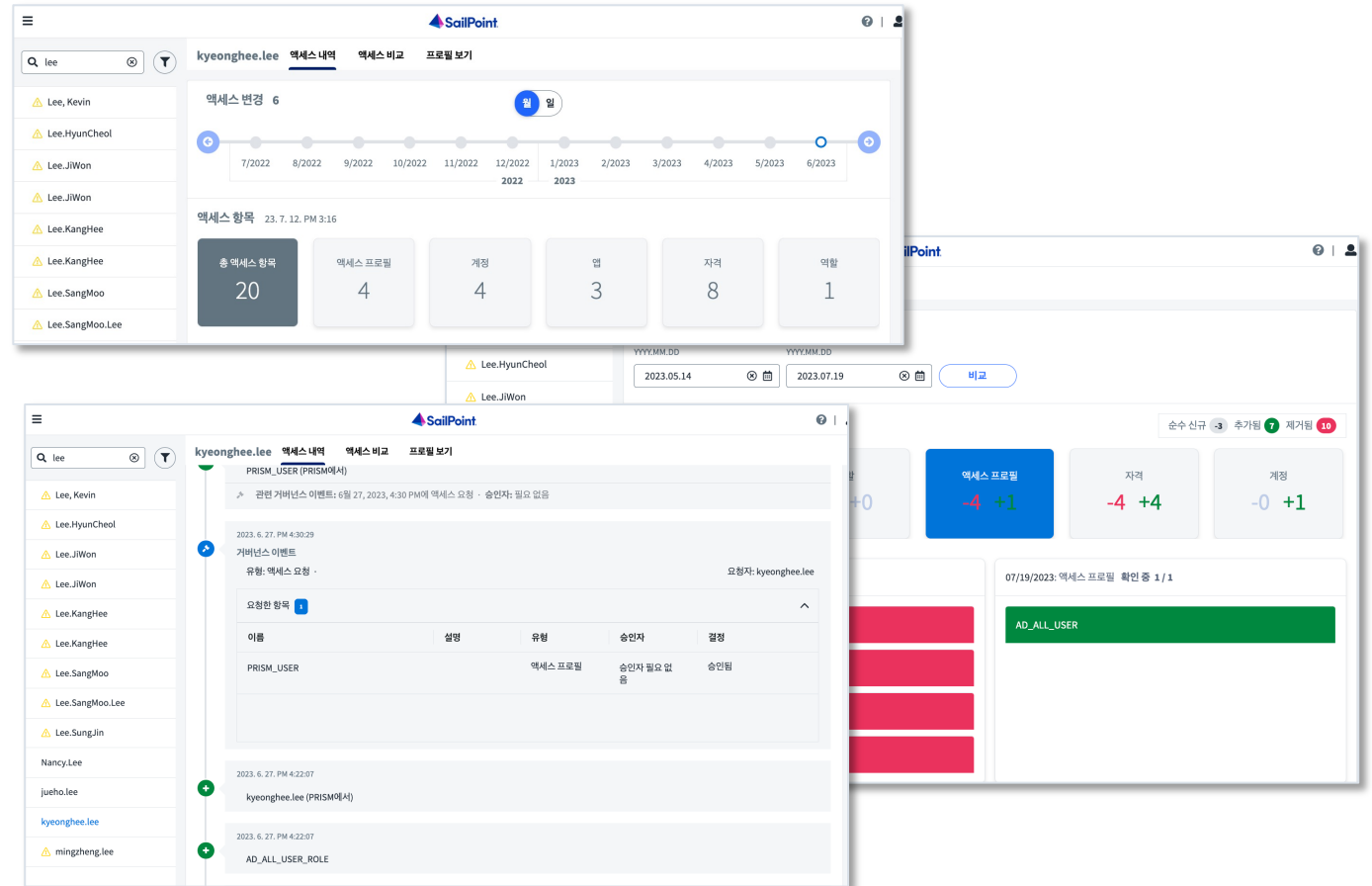
사용자 권한 이력관리 및 대시보드

Access History

- 사용자의 입사부터 속성 정보 변경, 퇴사까지 아울러 모든 계정/권한 부여 및 회수에 대한 **이력**과 사용자 속성 변경을 타임라인과 함께 기록
- 현재의 계정/권한 보유 통계와 특정 시점 간의 보유 내역 차이를 가시화

Access Intelligence Center

- 사용자 / 역할(Role) / 권한 / 계정 / 권한리뷰에 대한 현황 정보 제공과 동적 대시보드 기능으로 특정 정보에 대한 **Raw data** 확인 및 보고서 생성 가능
- 감사자가 규정 준수 여부를 간편하게 확인 가능



이점 7. 계정 권한 관련 업무 자동화 프로세스를 구현

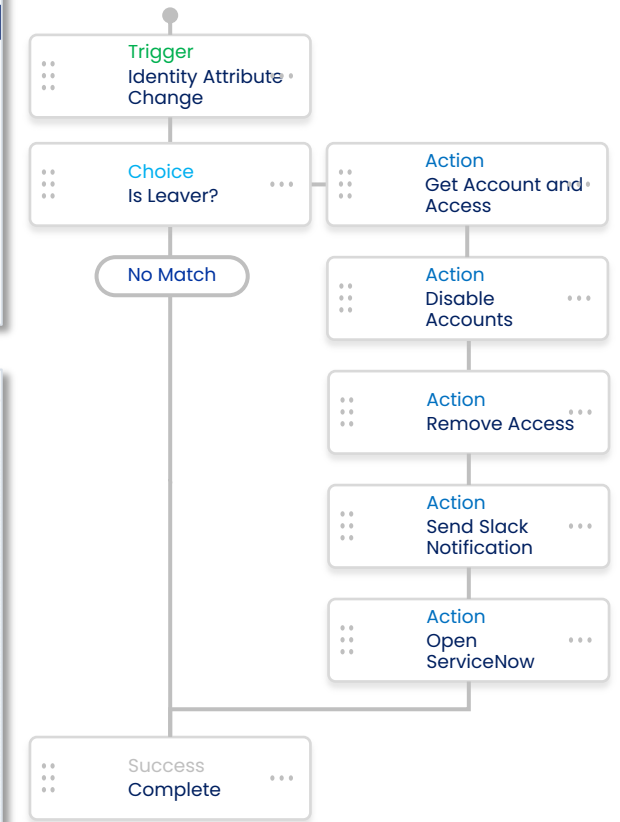
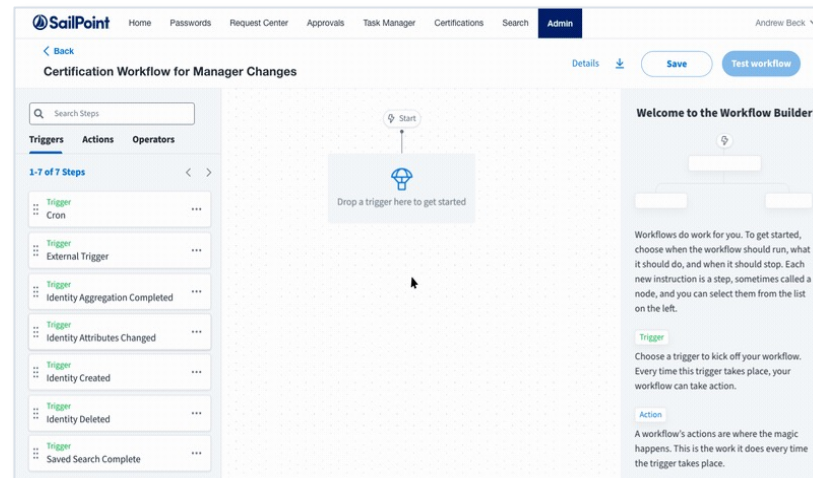
워크플로우 적용을 통해 내부 업무 프로세스를 구현하여 업무 자동화 구성

이벤트 기반 프로세스 자동화

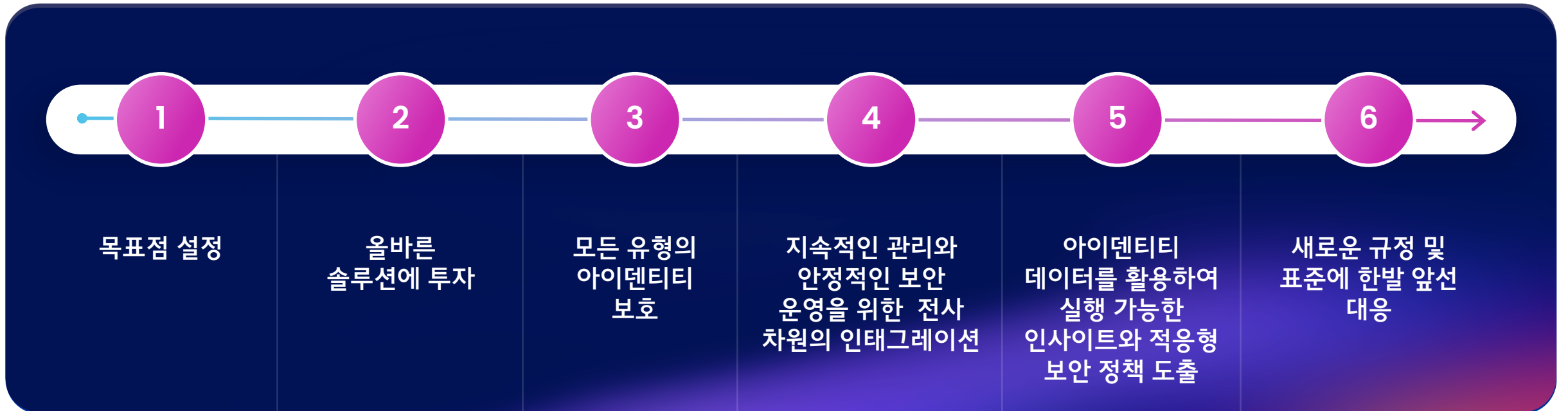
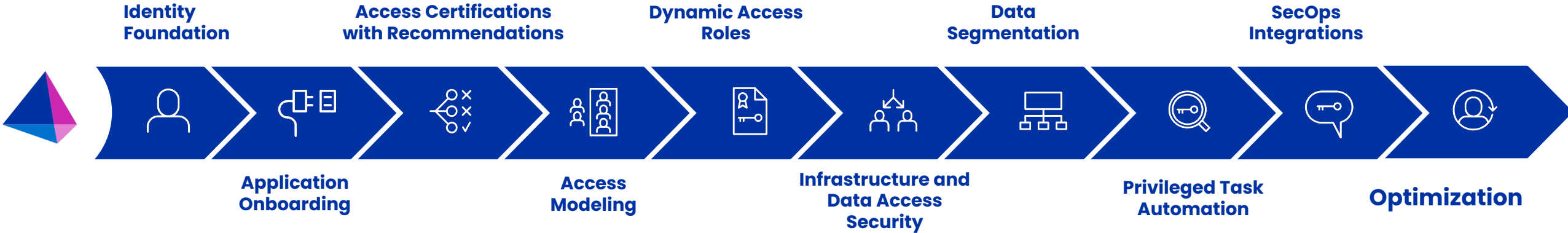
Workflow


- 조직에 새로운 부서생성 및 새로운 App이 도입되는 경우, 기존 프로세스 변경 또는 신규 프로세스 생성을 적용
- 워크플로우는 ID 프로세스에 대해 사전에 필요한 동작을 정의해 놓고, 필요 시 **drag & drop** 만으로 프로세스를 생성
- 외부 호출용 Workflow를 생성하여 보안 조치 자동화 구현
- 이벤트 발생 시 WebHook 방식의 알림으로 실시간 연동

이름	수정일	생성일	소유자	성공적인...	오류 비율	작업	상태
Ahead	2023. 4. 8.	2023. 4. 8.	Jerry.Bennett	0	0.00%	🗑️ 📄 🔄	비활성화됨 🔴
Windows Adm...	2023. 4. 6.	2023. 4. 6.	Jerry.Bennett	0	0.00%	🗑️ 📄 🔄	비활성화됨 🔴
Tag Recomm...	2023. 4. 6.	2023. 2. 25.	Jerry.Bennett	2	0.00%	🗑️ 📄 🔄	비활성화됨 🔴
Alex Test	2023. 4. 1.	2023. 4. 1.	Jerry.Bennett	0	0.00%	🗑️ 📄 🔄	비활성화됨 🔴
JobTitle Mover ...	2023. 4. 1.	2022. 8. 27.	Jerry.Bennett	116	0.85%	🗑️ 📄 🔄	활성화됨 🔵



아이덴티티 보안은 프로젝트가 아닌 프로그램



An overhead view of an office with eight people working at desks. A central dark blue and purple gradient banner contains white Korean text. The office desks are white and equipped with computers, keyboards, mice, and various office supplies. The floor is grey tile. The text is centered and reads:

아이덴티티 보안은
Zero trust 시대의 새로운 Firewall

