Identity Security

The Foundation of Security

SailPoint®

SailPoint 회사소개

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

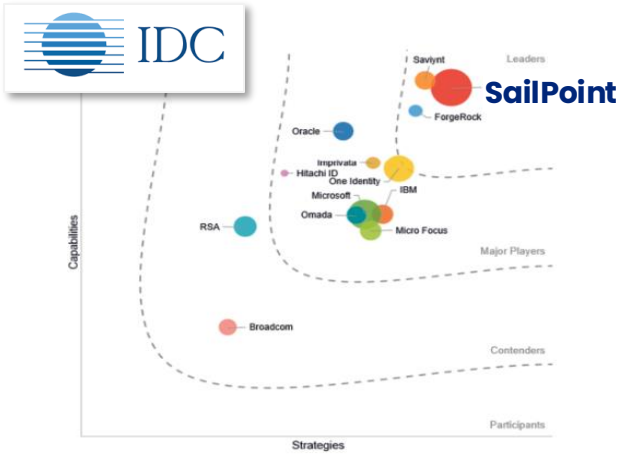
- 2005 — 회사설립 : 미국 Texas주 Austin
- 2007 — Identity 거버넌스 솔루션 시작
- 2010 — Provisioning을 Governance와 통합한 단일 솔루션 출시
- 2013 — SaaS 기반 Identity Provisioning 솔루션 출시
- 2015 — 비정형 데이터 거버넌스 솔루션 확장
- 2017 — AI/ML을 적용한 Identity 거버넌스 최적화 적용
- 2019 — RPA 관리 기능 추가
- 2020 — 클라우드 거버넌스 적용
- 2022 — SaaS identity 관리 SAP SoD 통합관리
- 2023 — SailPoint Atlas Platform 발표 비직원 리스크 관리 솔루션

46%
Fortune지 선정 500대 기업 사용

59%
Forbes 선정 Valuable Brands 기업 사용

3,000+
전세계 SailPoint 사용 고객 수

95%
고객 재구매 비율



Gartner
Gartner peerinsights customers' choice 2020
Gartner peerinsights customers' choice 2021
Gartner Peer Insights Customers' Choice 2023

SailPoint Global Reference

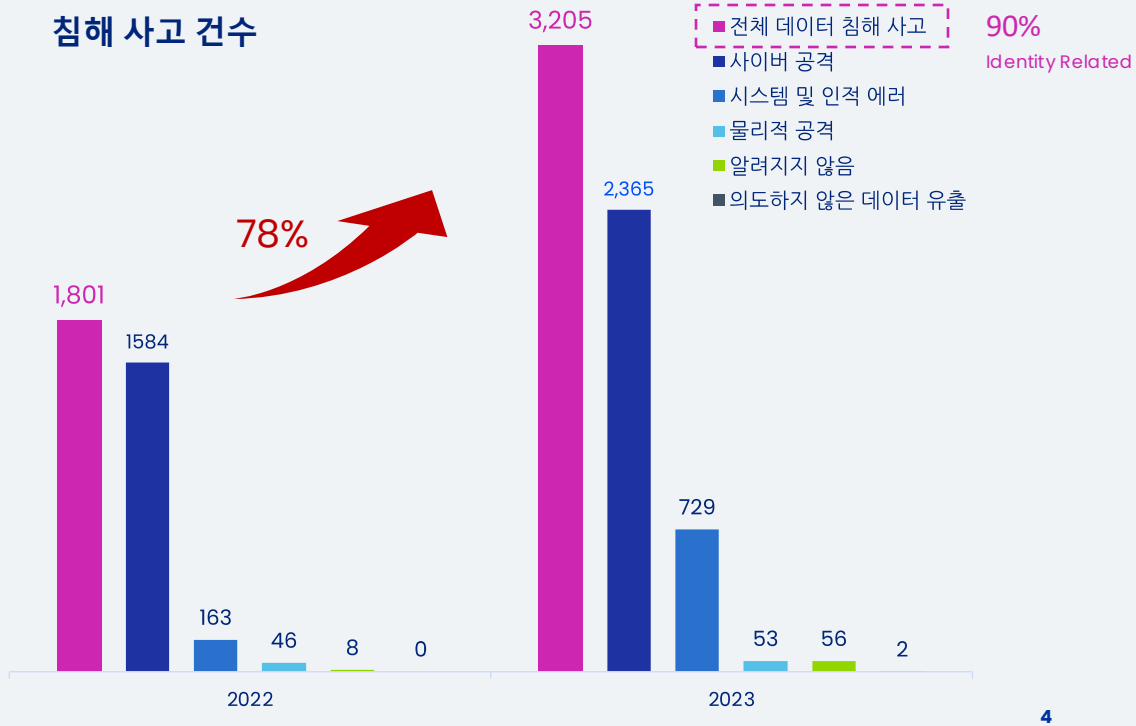
디지털 트랜스포메이션으로 증가하는 보안 위협

- 디지털 트랜스포메이션 가속화 도입 애플리케이션 급증
- 2023년 평균 **1,061**개의 애플리케이션 사용
- 보안 사고 78% 증가 2023년 한해 3,025건 발생
- 침해사고 중 90%가 아이덴티티 연관 보안 사고
- 확대되는 공격 요소, 증가하는 보안 위협

기업에서 도입한 APP 수

Source: Deloitte 2023 Connectivity Benchmark Report

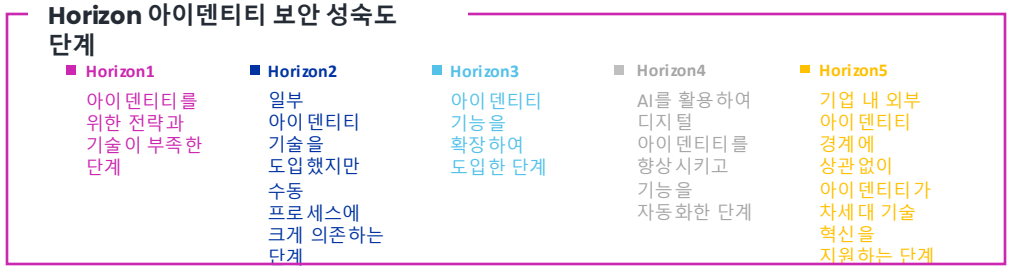
침해 사고 건수

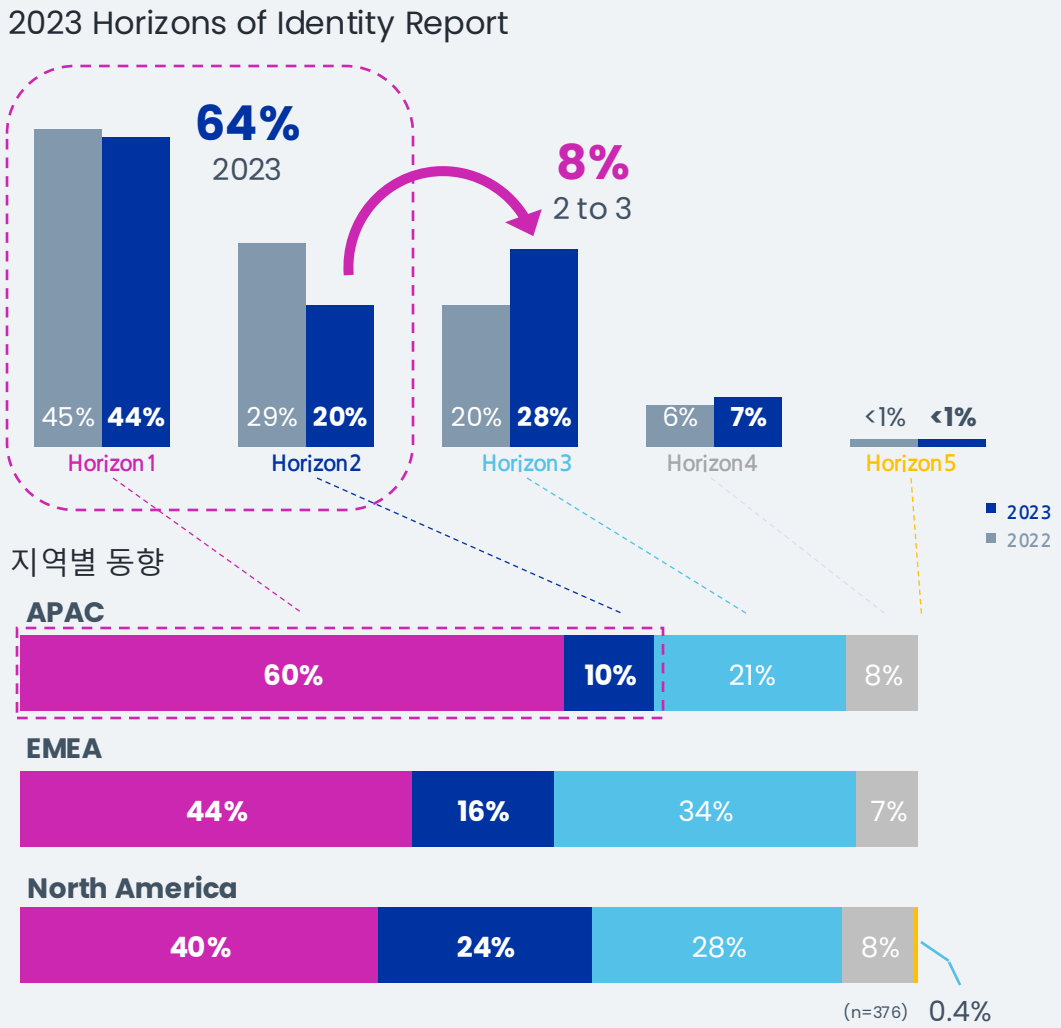


Source: ITRC 2023 Annual Data Breach Report

초기 단계에 머무른 아이덴티티 보안 현실

- 기업의 64% 기업은 초기 수준의 아이덴티티 보안
- 특히 APAC의 경우, 70%가 초기 수준으로 확인
- 아이덴티티에 대한 기본적인 거버넌스와 통합된 가시성 부족
- 자동화된 아이덴티티 보안이 적용된 기업은 7%뿐





Source: Customer survey (IAM/IGA decision maker survey conducted in August '23), total N=376 Note: Survey bias adjustment accounting for the share of the vended market not reached by the survey and accounts for respondents that were terminated for not having a formal IAM program or deploying IAM tools

아이덴티티란 무엇일까요?

Identity

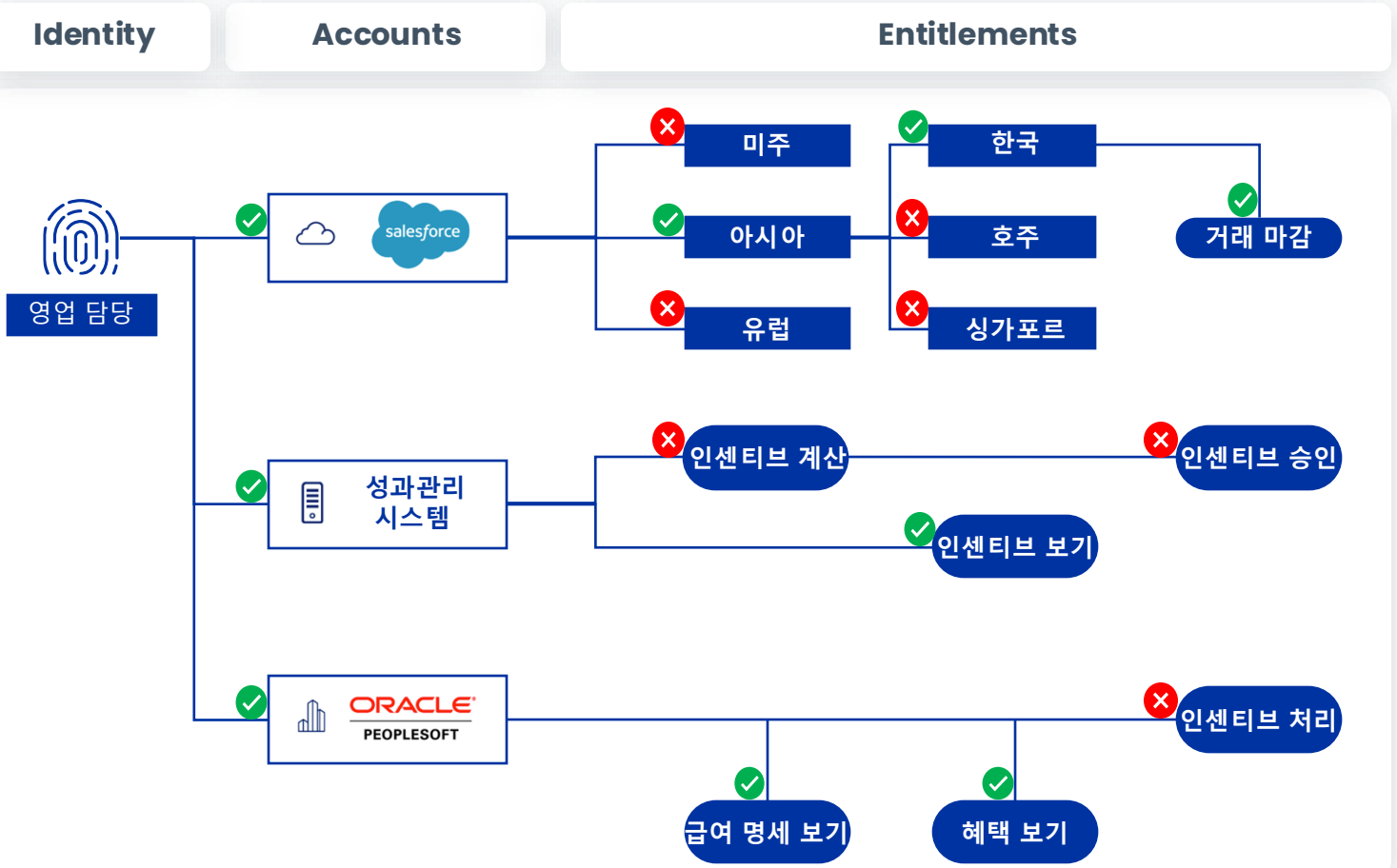
Attributes

- Name
- E-Mail
- Employee Number
- Job Title
- Type
- Department
- Location
- Phone Number

Employee

Non Employee

Non Human



아이덴티티 보안 솔루션 영역

IAM
(Identity Access Management)

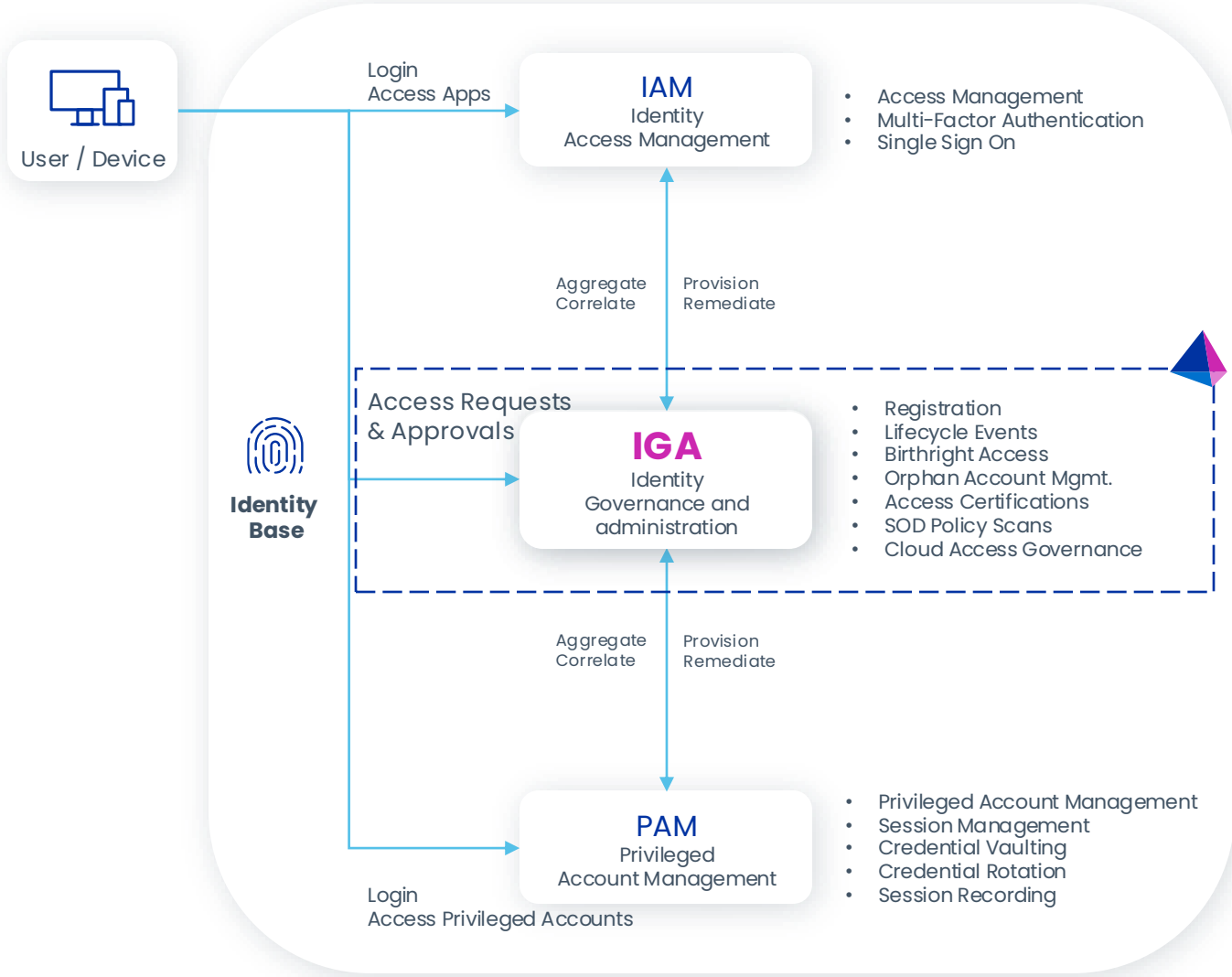
- 애플리케이션에 대한 접근
- SSO/MFA
- **아이덴티티의 신원 인증(Authentication) 영역**

IGA
(Identity Governance and administration)

- 아이덴티티 라이프사이클 관리
- 컴플라이언스 관리
- 역할 기반 접근 권한 관리
- 보유 권한 분석을 통한 역할 모델링
- 직무 분리 관리
- 주기적인 권한 리뷰
- 클라우드와 온프레미스 통합 관리
- **권한 부여(Authorization) 및 관리 영역**

PAM
(Privileged Account Management)

- 관리자 계정 및 고위험 권한 계정에 대한 집중 관리
- 세션 모니터링 및 기록
- 고위험 계정의 비밀번호 관리 및 변경
- **서버 네트워크 장비 등 주요 인프라에 대한 권한계정 접근 관리 및 모니터링 영역**



어느 영역의 보안에 집중하고 계십니까?

Identity 수동 개별 관리

수십 수백개의 시스템에 존재하는 Identity를 수동으로 개별 관리할 경우 적시 적소에 권한 부여 및 회수가 어려움

인증 강화

인증 방식만을 강화해서는 모든 보안 문제를 해결하기 어려움

접근 제어

접근 이후 권한 오남용 및 고아 계정 및 미사용 계정 사용 가능성이 존재

외부 침입 보안

관문단 혹은 단말의 보안을 강화하는 것으로는 내부자 또는 탈취당한 계정을 활용한 내부 공격 대응이 어려움

주요 자산

특정된 주요 자산 보안에 집중하여 대상 이외에서 보안 문제 발생 가능성 존재

아이덴티티 보안을 위협하는 요소들

아이덴티티 보안의 핵심 영역

Identity 통합 자동화 관리

중앙화된 Identity 통합 자동화 관리를 적용하여 적시 적소에 권한 부여 및 회수 프로세스 적용

라이프사이클 관리

사용자의 상황에 맞는 권한 부여와 회수 정책 실행
지속적인 역할별 접근 권한 개선

관리정책 적용

부적절한 접근 권한 탐지
주기적인 사용자 권한 검토

보안사고 예방 및 대응

사용자의 권한에 대한 가시성 확보
즉각적인 사고 발생 대응 프로세스 구축

일원화

온프레미스, 클라우드 시스템에 대한 통합 관리
직원 및 비직원의 Identity에 대한 통합 관리

Identity 일원화

Identity 관리 일원화

Employee와 Non-Employee, Non-Human의 Identity를 클라우드와 온프레미스를 **모두 일원화**하여 관리

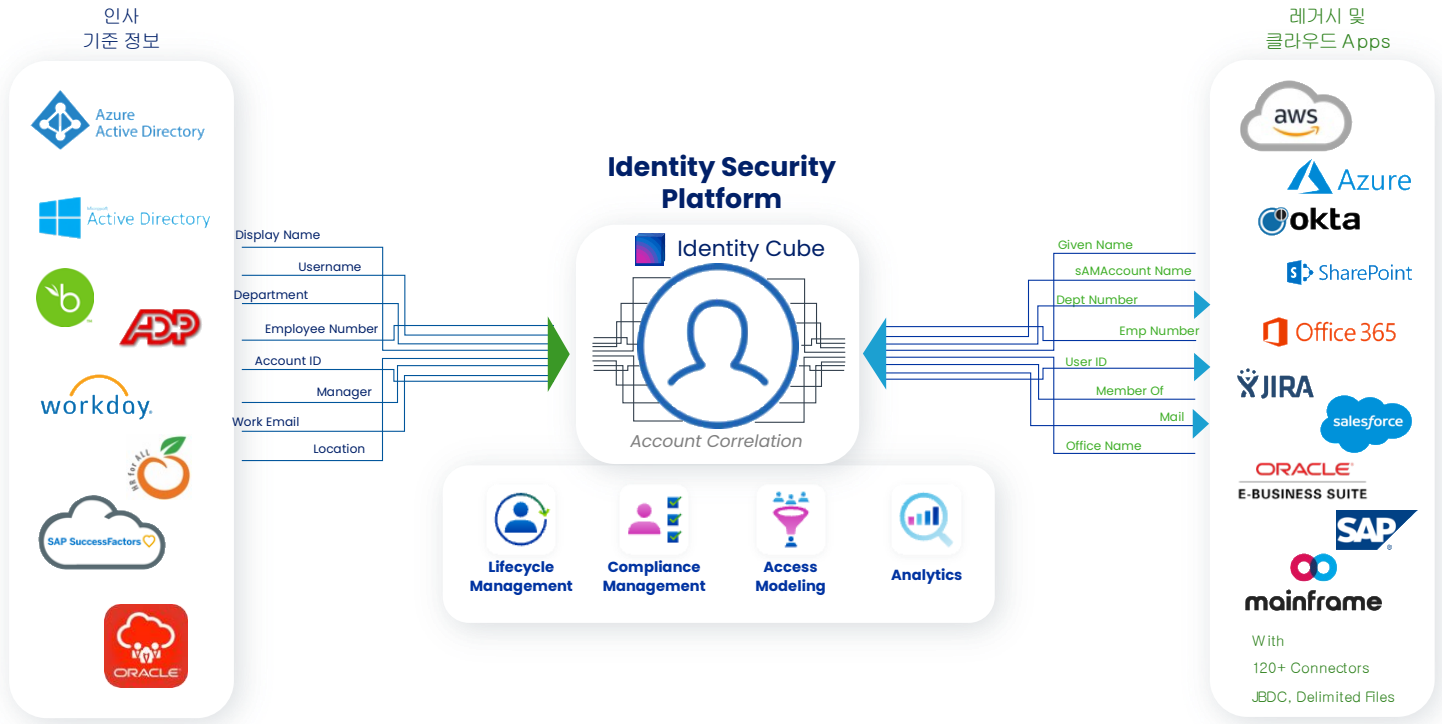
모든 Identity를 일원화하여 관리

관리 대상 Identity

- Employee(임직원)
- Non-Employee(협력사, 관계사, 외주업체 등)
- Non-Human(RPA, Bot, 서비스 등)

Application Connectivity

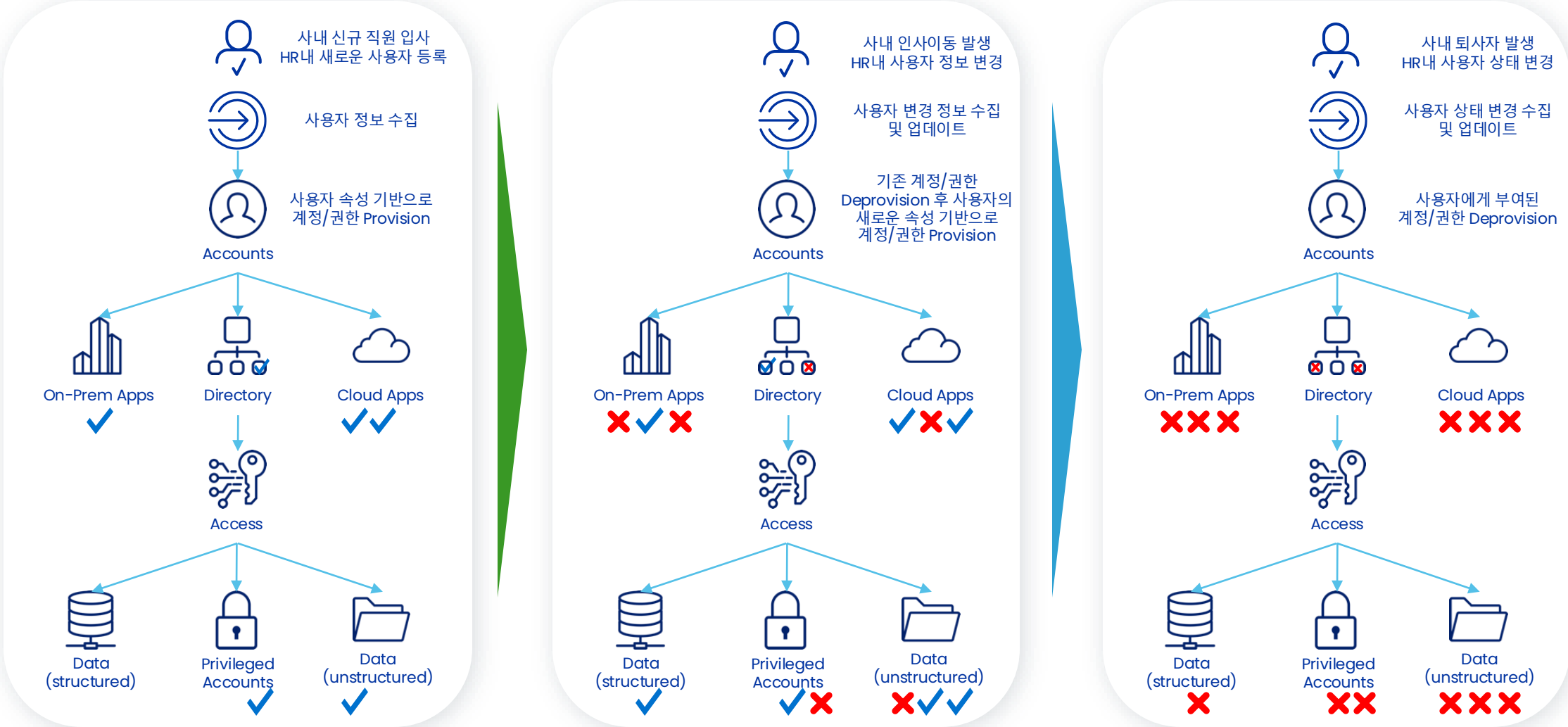
- 온프래미스, 클라우드 제한 없는 통합 관리
- **120+ OOTB 커넥터 제공**
- JDBC, Delimited File 활용으로 기존 레거시 시스템과 유연한 연결



라이프사이클 관리

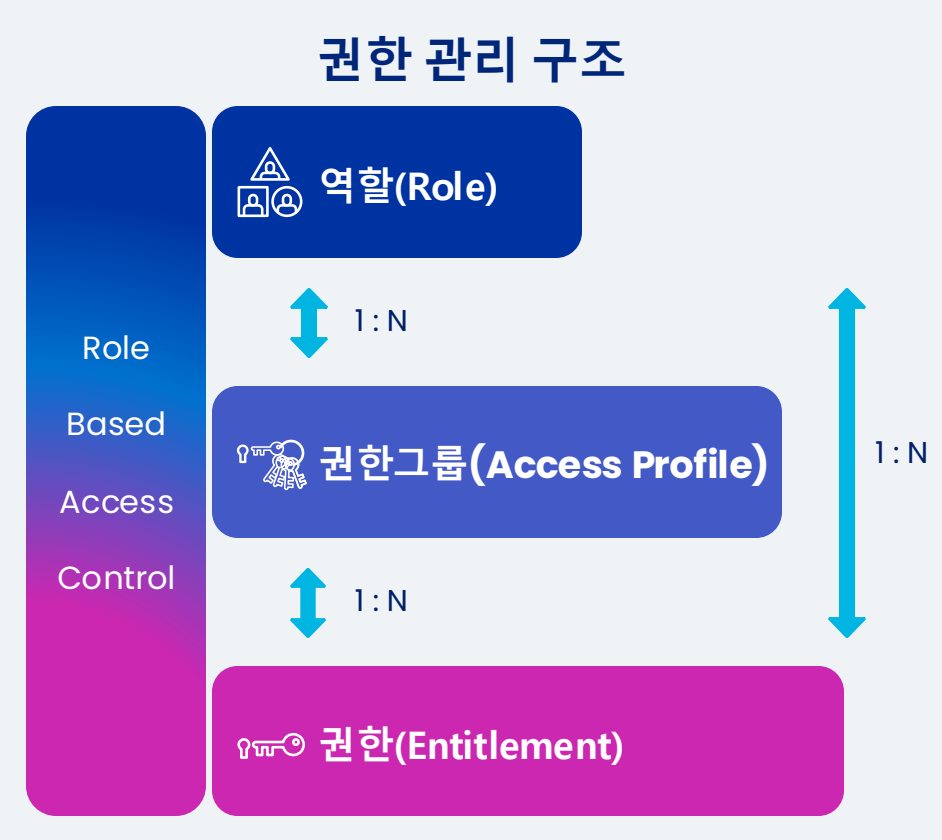
사용자 상태 기반의 계정 권한 처리 자동화

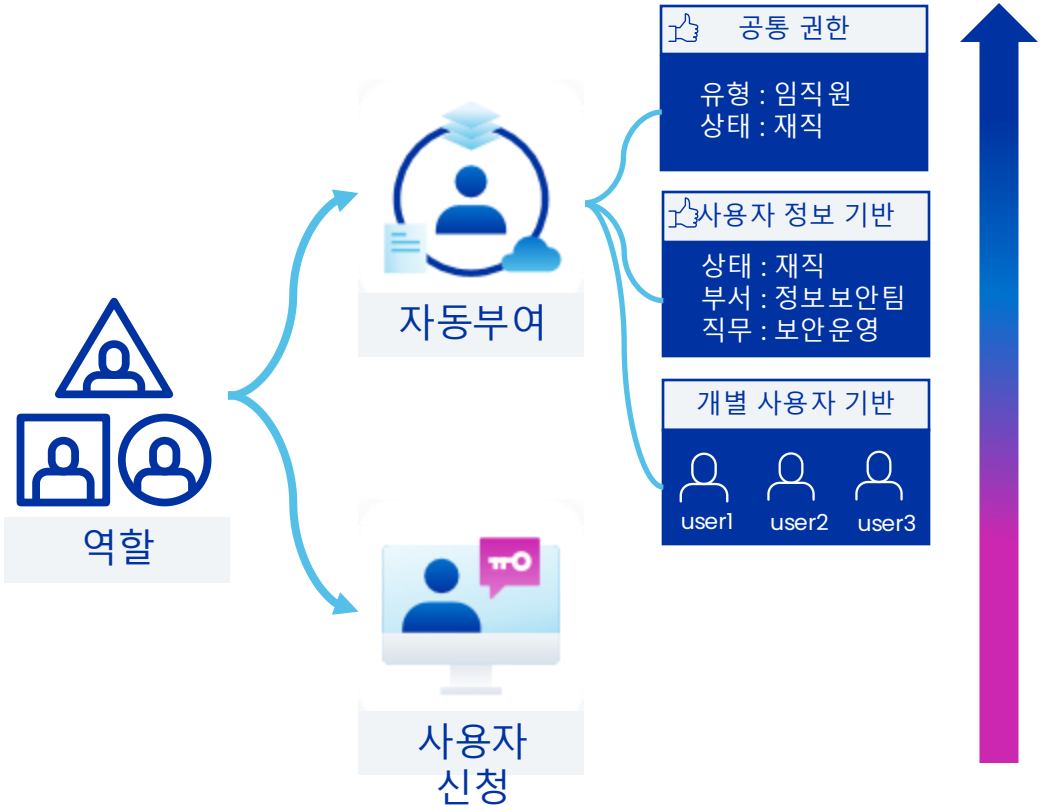
사용자의 입사 및 퇴사, 인사 이동 등의 부서 또는 직무 변경에 따라 **계정/권한 부여와 회수를 자동화**



역할 기반 접근 제어 적용

역할 기반 접근 제어(RBAC)은 임직원의 담당업무에 따라 부여할 권한을 정의하여 사용자의 역할에 따른 역할 모델 자동 부여/회수 자동화를 구성





사용자가 필요한 권한을 직접 신청

사용자는 역할을 통해 부여된 권한 외 **업무 상 추가로 필요**한 권한/권한그룹/역할을 직접 신청

신청 권한 제공 기준

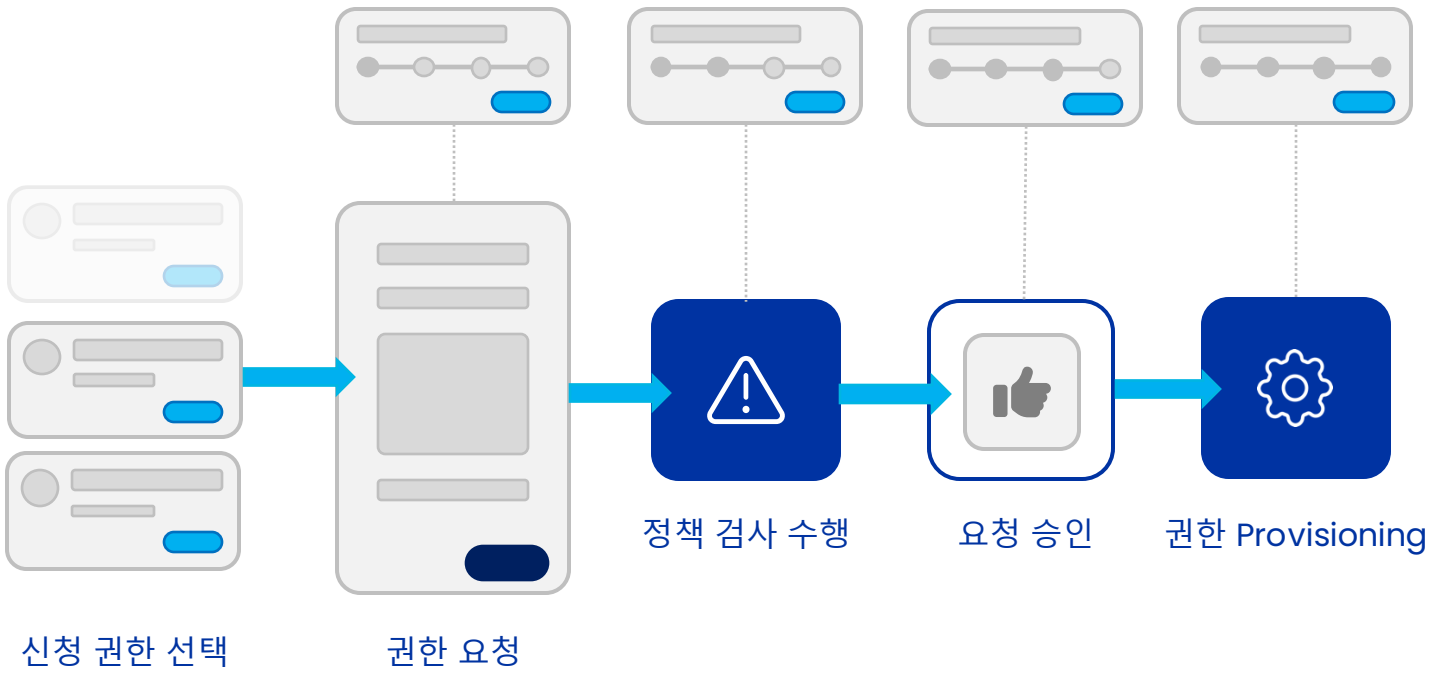
Access Request Recommendations

- 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**



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

관리정책 적용

권한관리 정책 적용 및 확인(계속)

권한관리 정책을 정의 및 적용하여 **정책 위반 사용자를 확인** 및 **권한 신청 시 위반 여부를 확인**

정책 설정을 이용한 사용자 권한관리

SoD 정책

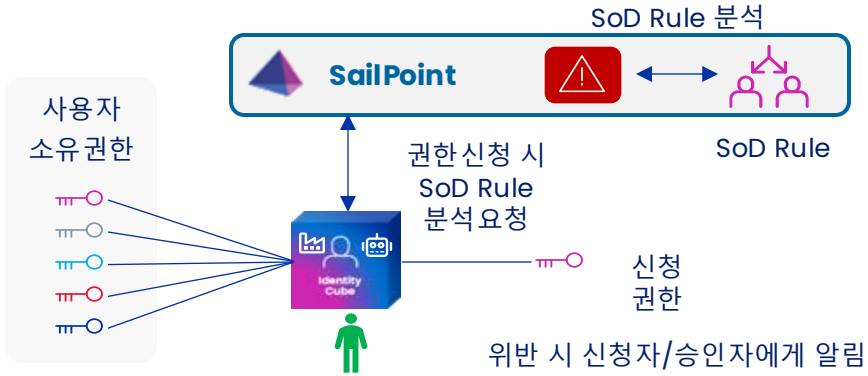
- 권한 기준의 정책으로 **함께 보유하면 안되는 권한을 정의**하여 정책 위반 사용자 확인
- SoD 정책은 사용자의 **개별 권한 신청 시 정책 위반 검사를 수행**하여 정책 위반 권한 신청에 대한 승인 및 부여를 사전에 방지

일반 정책

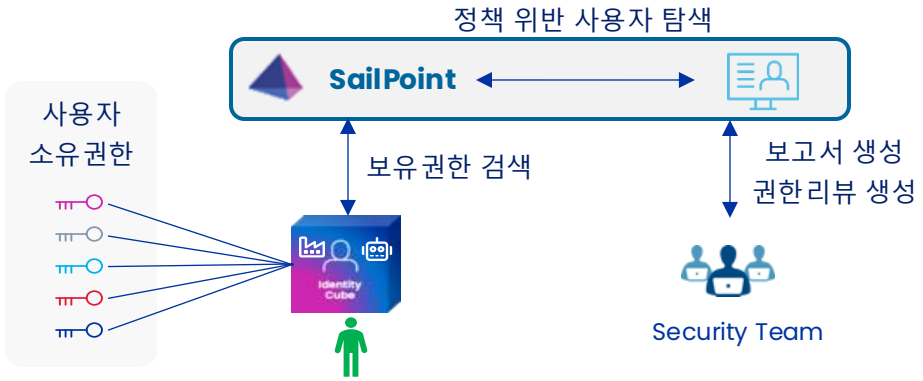
- 사용자 및 역할, 권한그룹, 권한 기준의 **쿼리 기반 검색 기능**을 통해 내부 권한관리 정책 위반 사용자 확인

  (예 : IT 유관 부서가 아닌 사용자 중 관리자 권한을 보유)

SoD 정책



일반 정책



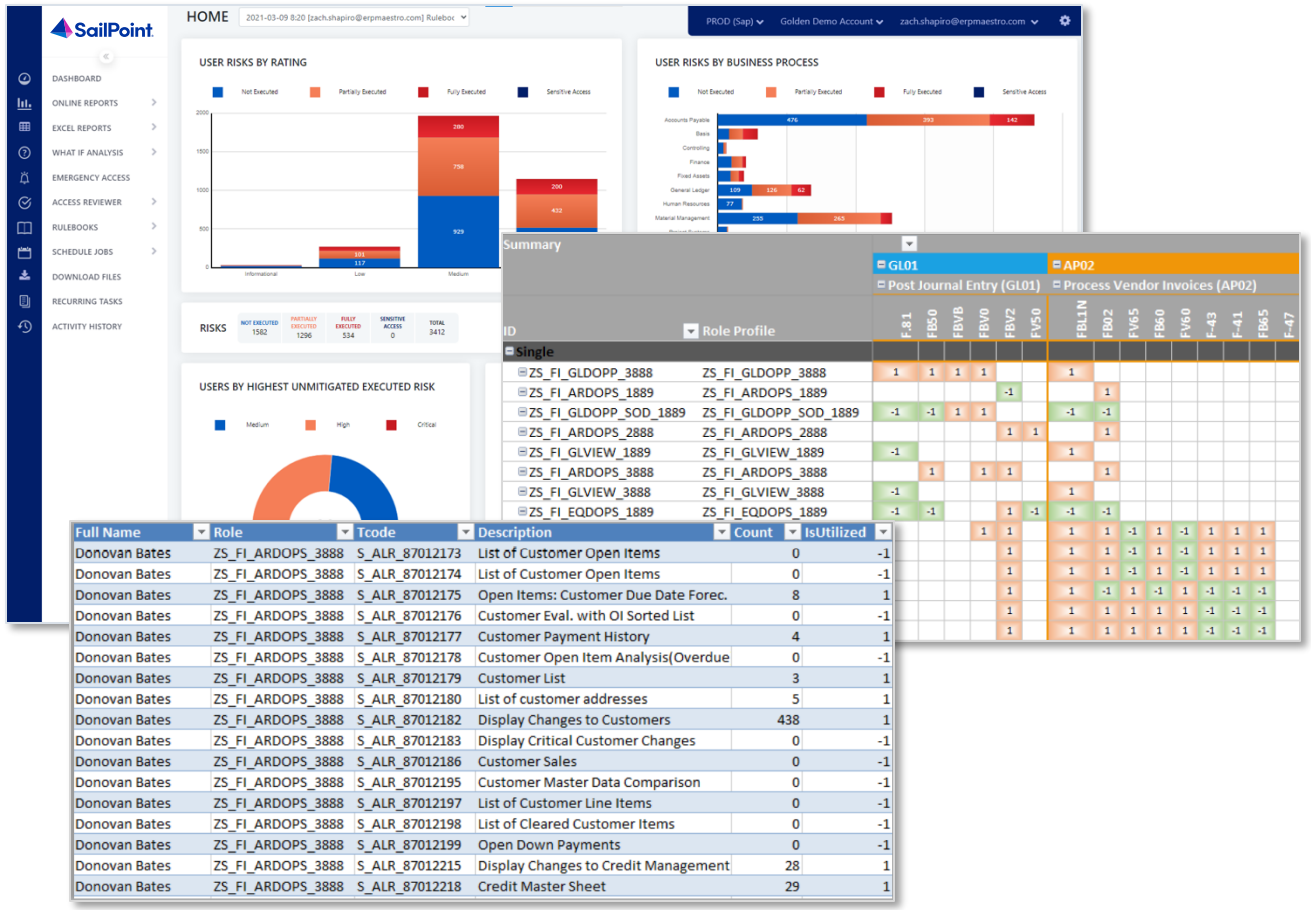
권한관리 정책 적용 및 확인

SAP ERP에 대한 효과적인 권한관리를 위한 **Rule book을 제공**하며 T-code 사용현황 및 Role에 대한 **위험을 관리**

권한오브젝트 단위의 SAP 위험 관리

SAP ERP 위험 관리

- SAP ERP에 대해 SoD 위험도를 사전에 정의된 **Rule book에 의해 측정**하고 **조치방안**을 제시
- 권한이 할당되기 이전에 대상 어플리케이션 전반에 걸쳐 **위험을 시뮬레이션**하고 SoD 정책 정의를 통해 정책 위반 발생에 사전에 대응
- SAP Role에 대해 SoD 위반에 해당하는 **T-code 보유 현황과 사용 현황을 제공**하여, SoD 위반에 따른 위험을 감소시킬 수 있도록 **Role 개선**
- 사용하지 않는 T-code를 제거할 수 있도록 근거자료 제공



주기적인 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

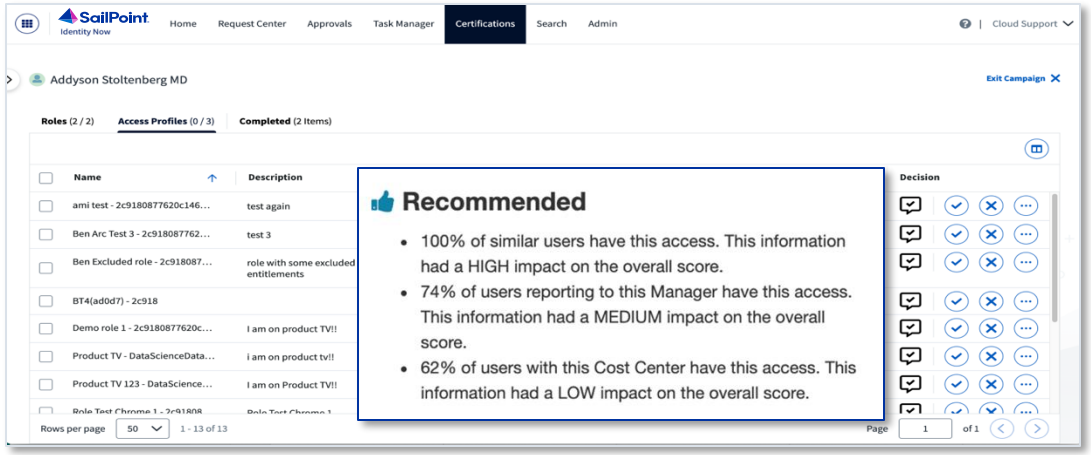
- 사용자의 부적절한 권한에 대해 의사결정자는 **즉시 회수 명령**하여 권한을 적절성을 유지

권고사항 제시

- 사용자의 속성과 유사한 그룹을 분석하여 의사결정을 위한 **권고사항 정보를 제공**

권한 리뷰 기준

- 사용자
- 권한
- 역할
- 비상관 계정
- SoD 정책
- 일반 정책



보안사고 예방 및 대응

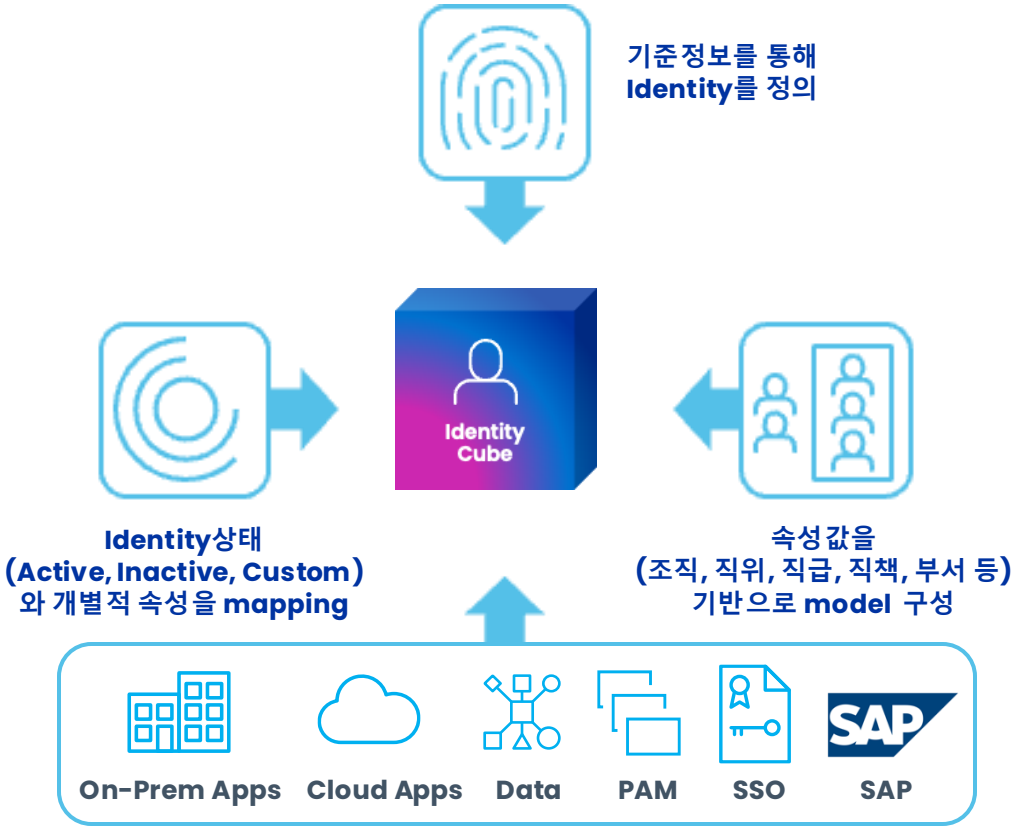
사용자 기준의 계정 권한 보유 현황 확인

사용자 기준으로 **계정 현황을 확인**하고 **보유 계정의 권한 및 속성 정보**를 한 눈에 검토

사용자 권한 가시성 확보

Identity Cube

- 인사정보로부터 사용자가 수집될 시 사용자가 가지는 모든 정보(인사정보 출처, 사용자 상태, 속성, 보유 계정, 보유 권한 및 역할 등)을 **Cube 형태로 저장**하여 관리
- 사용자 대상의 모든 이벤트(인증, 활성화, 계정 생성/변경/제거 등)의 정보를 함께 저장하여 **감사 추적** 용이
- 직접 혹은 관리자를 통해 사용자의 부재 기간 동안 **업무 대리인 지정** 가능



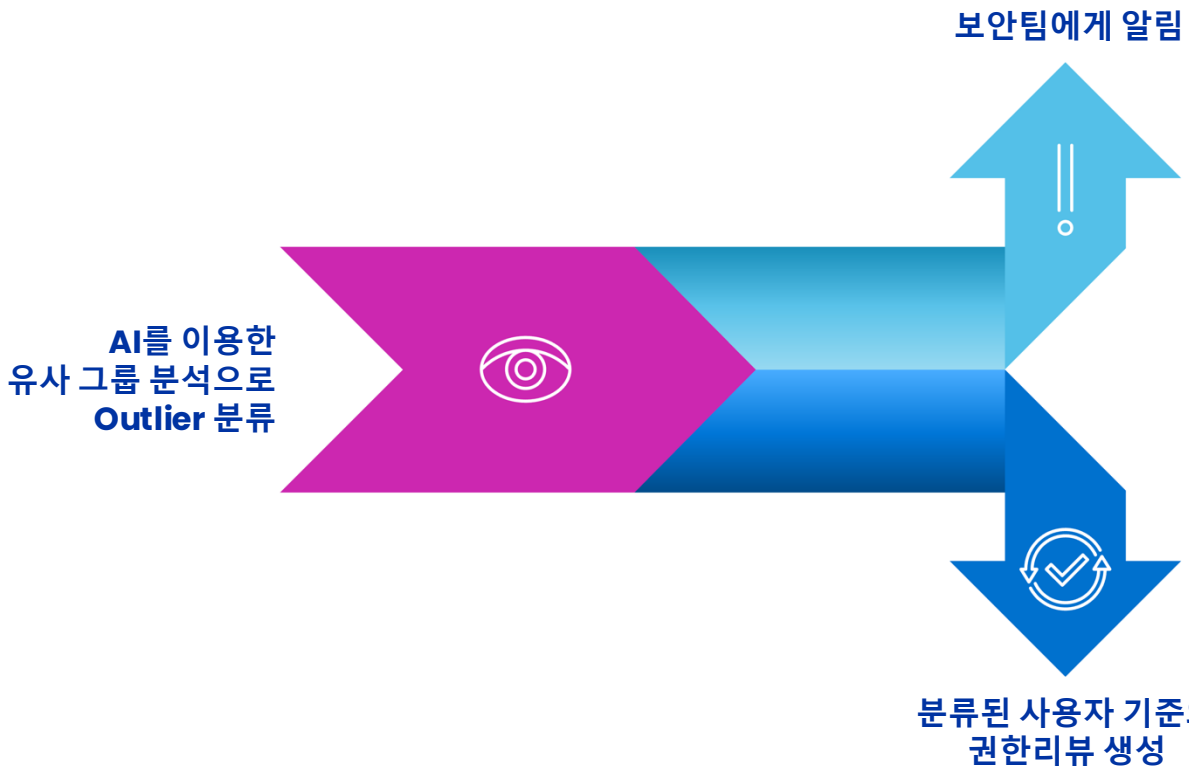
주의 필요 사용자 분류

AI를 이용하여 **분류 기준에 따른 점수 산정**으로 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



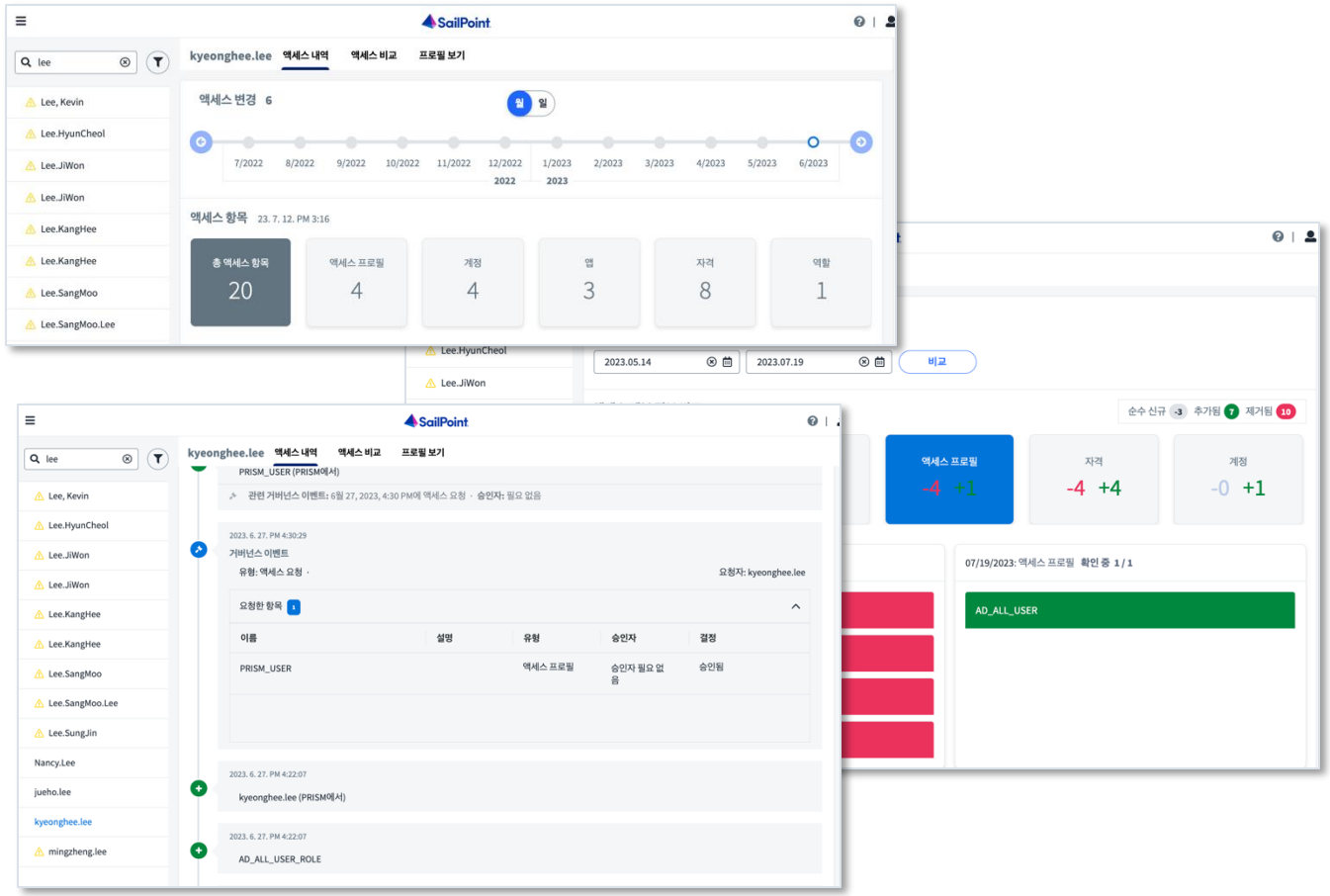
사용자 계정 권한 이벤트 이력 관리

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

사용자 권한 이력관리

Access History

- 사용자의 입사부터 속성 정보 변경, 퇴사까지 아울러 모든 계정/권한 부여 및 회수에 대한 **이력**과 사용자 속성 **변경을 기록**
- 사용자의 개별 권한 신청 및 관리자에 의한 권한 제거 이벤트는 이력에 거버넌스 이벤트로 기록하여 **권한 부여 및 회수에 대한 증적**을 관리
- 모든 이벤트는 **타임라인**을 함께 기록
- 현재의 계정/권한 보유 통계와 **특정 시점 간의 보유 내역 차이를 가시화**



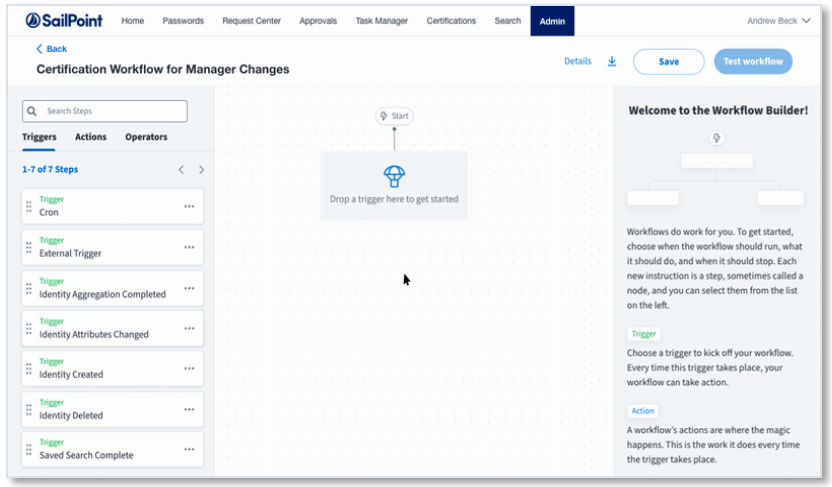
계정 권한 관련 업무 프로세스를 구현

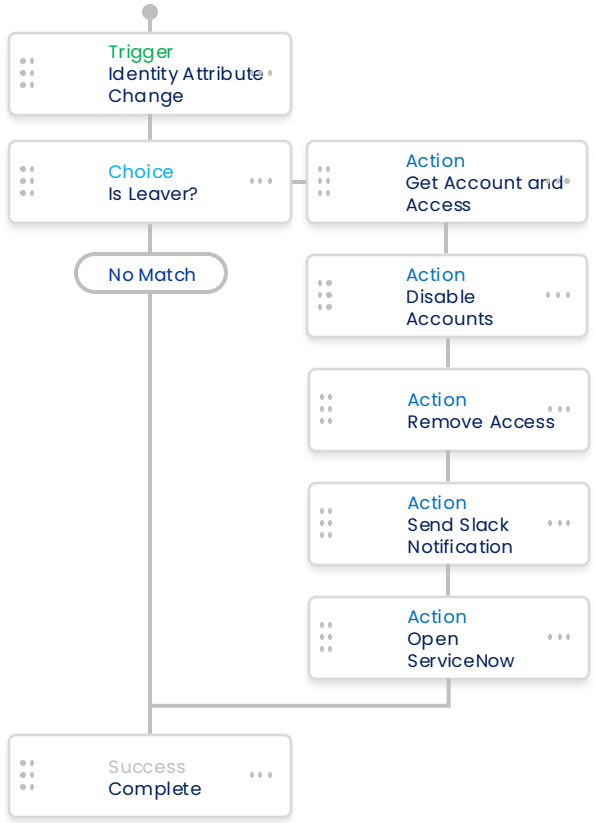
워크플로우 적용을 통해 내부 업무 프로세스를 구현하여 업무 자동화 구성

이벤트 기반 프로세스 자동화

Workflow

- 조직에 새로운 부서생성 및 새로운 App이 도입되는 경우, **기존 프로세스 변경 또는 신규 프로세스 생성**을 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





대시보드를 통한 Identity 현황 파악

Identity 관련 모든 항목에 대한 데이터 및 추이 정보를 통한 모니터링

이벤트 기반 프로세스 자동화

Access Intelligence Center

- SailPoint에서 제공하는 사용자/권한 데이터 시각화 도구로 Out-of-the-box 형태의 **개인화 대시보드**로 제공
- 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 여부**를 간편하게 확인 가능