Agentforce World Tour *Korea*

Forward looking statement

This presentation contains forward-looking statements about, among other things, trend analyses and statements regarding future events, anticipated growth and industry prospects, and our strategies, expectation or plans regarding product releases and enhancements. The achievement or success of the matters covered by such forward-looking statements involves risks, uncertainties and assumptions. If any such risks or uncertainties materialise or if any of the assumptions prove incorrect, results or outcomes could differ materially from those expressed or implied by these forward-looking statements. The risks and uncertainties referred to above include those factors discussed in Salesforce's reports filed from time to time with the Securities and Exchange Commission, including, but not limited to: our ability to meet the expectations of our customers; uncertainties regarding AI technologies and its integration into our product offerings; the effect of evolving domestic and foreign government regulations; regulatory developments and regulatory investigations involving us or affecting our industry; our ability to successfully introduce new services and product features, including related to AI and Agentforce; our ability to execute our business plans; the pace of change and innovation in enterprise cloud computing services; and our ability to maintain and enhance our brands.

Last updated: September 10, 2024

AI 혁신과 데이터 보안의 균형을 확보하는 8가지 실행전략

이동승

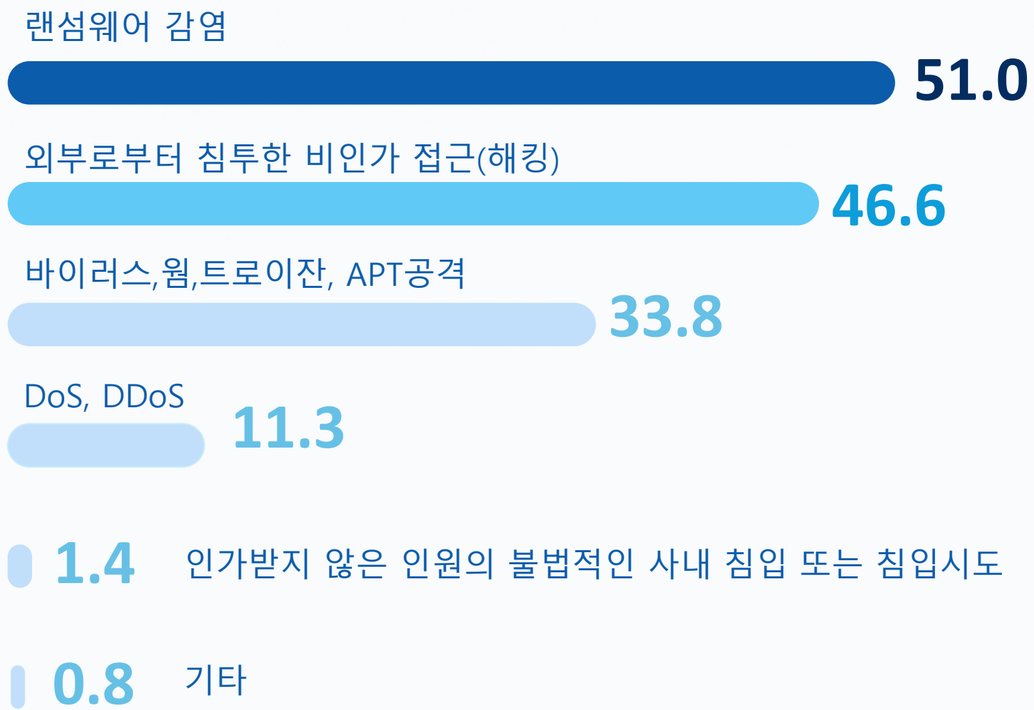
Platform & Security 솔루션 엔지니어

Salesforce Korea


THANK YOU
Korea
COEX

국내 기업의 침해사고 유형 및 위협 요인

국내 기업의 침해사고 경험 유형



Base : 침해사고 경험한 기업체, 단위 %, 복수응답

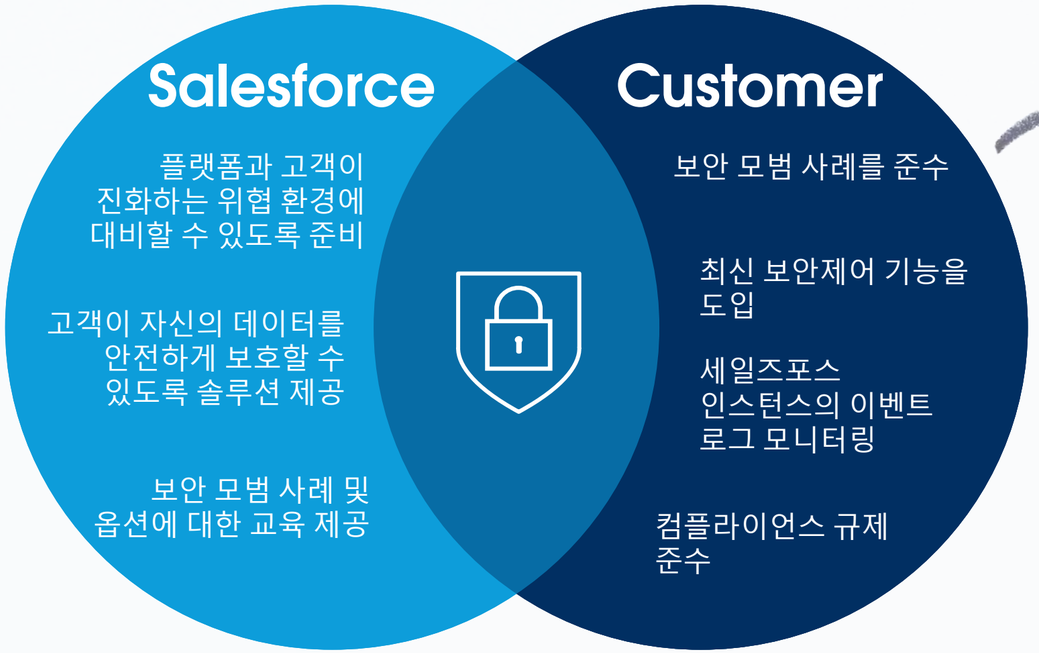
우려하는 정보보호 위협 요인

- 고객 개인정보 유출 위협
- 인터넷을 통한 사내 전산 시스템 침해사고 위협
- 외부 공격에 의한 저장된 데이터 자산의 손·망실
- 인적 요인에 의한 정보유출 위협

출처 : ”2024 정보보호 실태 조사”, 정보보호산업협회(KISIA), 2025년 4월

사회공학 위협으로부터 **Salesforce** 환경 보호

공유 책임 모델



Salesforce 권장 설정 및 보안 솔루션

1. **IP** 접근 통제
2. **MFA**
3. 최소 권한 통제
4. **Salesforce Shield**
5. 고객사의 보안 담당자 지정

출처 : “Protect Your Salesforce Environment from Social Engineering Threats”, Salesforce Blog(Link), 2025 March

증가하는 위협으로 인해 데이터와 신뢰가 위험에 노출

데이터 보안 공격은 더욱 정교해짐

258

데이터 유출을 식별하고 억제하는 데 걸리는 평균 일수

IBM Cost of a Data Breach Report 2024

규제/컴플라이언스 준수 미흡은 막대한 손실을 초래함

200억 원 ($14.8M)

HIPAA 및 GDPR과 같은 데이터 개인정보 보호 규정을 준수하지 못한 회사의 평균 비용

The True Cost of Compliance with Data Regulations

기업은 AI 도입 준비가 필요함

71%

생성형 AI가 새로운 보안 위험을 초래할것이라고 생각하는 IT 리더 비율

Top Generative AI Statistics for 2025, Salesforce

증가하는 위협으로 인해 데이터와 신뢰가 위험에 노출

AI 시대의 보안 위협

- 데이터 유출
- 악의적인 프롬프트 인젝션
- AI 생성 컨텐츠의 조작/오남용/편향/유해성
- 자동화된 공격확대(예: AI기반 피싱, 딥페이크)

기업은 AI 도입 준비가 필요함

71%

생성형 AI가 새로운 보안 위험을 초래할것이라고 생각하는 IT 리더 비율

Top Generative AI Statistics for 2025, Salesforce

Agentforce

The digital labor platform

Trusted

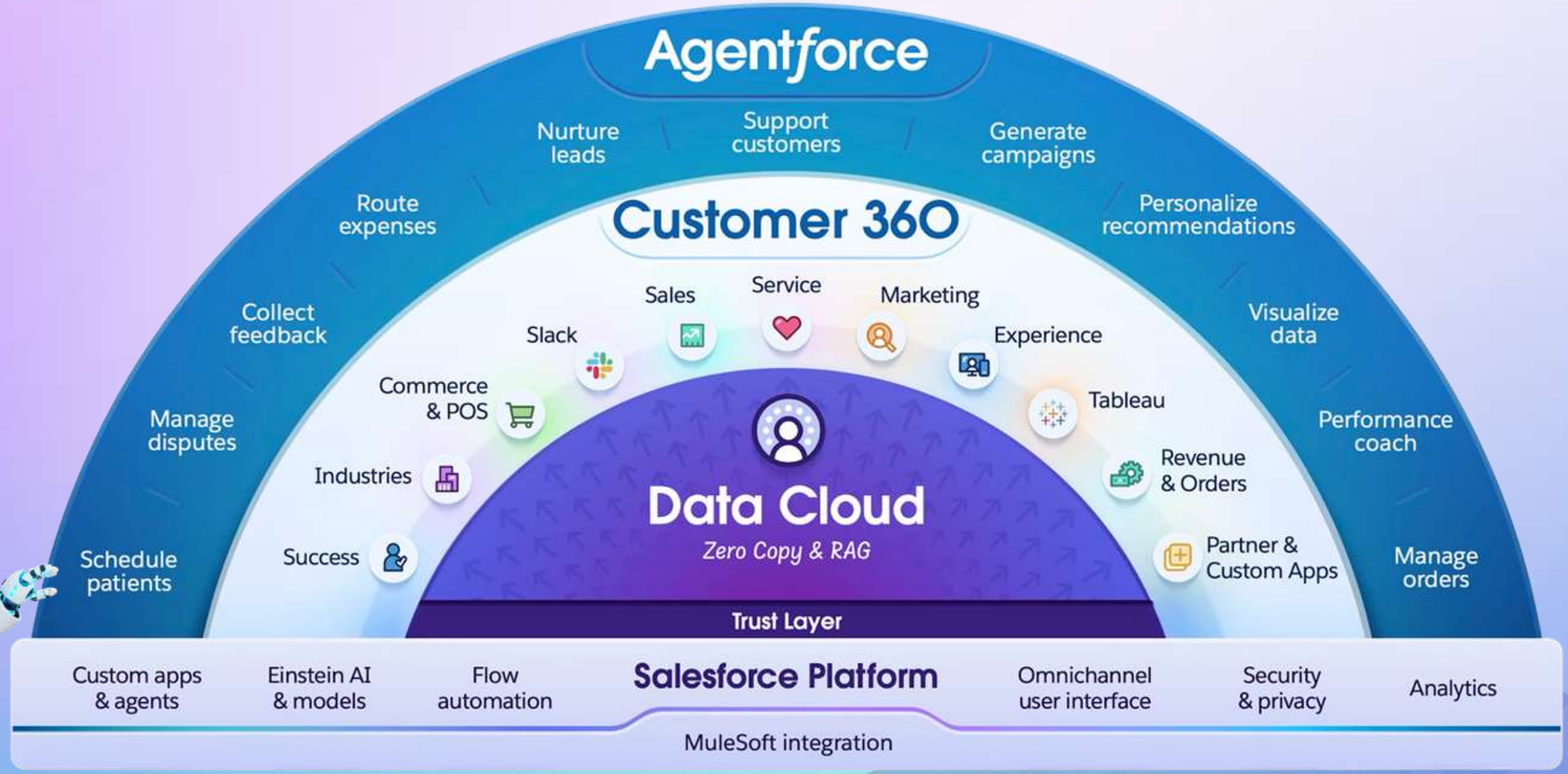
Easy to deploy

Humans in the loop

Zero hold time

Deeply unified

Open



Salesforce Shared Trust Model

보안 강화 솔루션

보안 통제 기능

AI 보안을 위한 가드레일

메타 데이터 기반 아키텍쳐

Zero Trust 전략
취약점 점검, 가용성 및 DR
24X7 보안관제
(방화벽, WAF, DDoS방어, SEIM 등)

Add-Ons

Data Security

Shield

- Platform Encryption
- Field Audit Trail
- Event Monitoring
- Data Detect

Security Center

Data Compliance

- Data Mask & Seed
- Privacy Center

Data Resilience

- Backup & Recover
- Archive
- Salesforce Discover

Platform Security

- Mobile Security
- Customer Identity
- Private Connect

Built In

Core Access Controls

SSO | Authentication | Authorization | Auditing | Health Checks | MFA

Einstein Trust Layer

Secure Data Retrieval | Dynamic Grounding | Data Masking | Toxicity Detection | Audit Trail, Feedback | Zero Data Retention

Isolation-Centric Secure by Design - Multi Tenant Platform

- Metadata-Driven Architecture
- Contractual Assurance & Transparency

Verifiably Secure Infrastructure

- Secure Software Development
- Host, Storage & Network Security
- 3rd Party Auditing & Security Testing
- Least-Privilege Access & Segmentation
- Hyperforce
- Site Reliability & Disaster Recovery

Customer Controlled

Salesforce Controlled

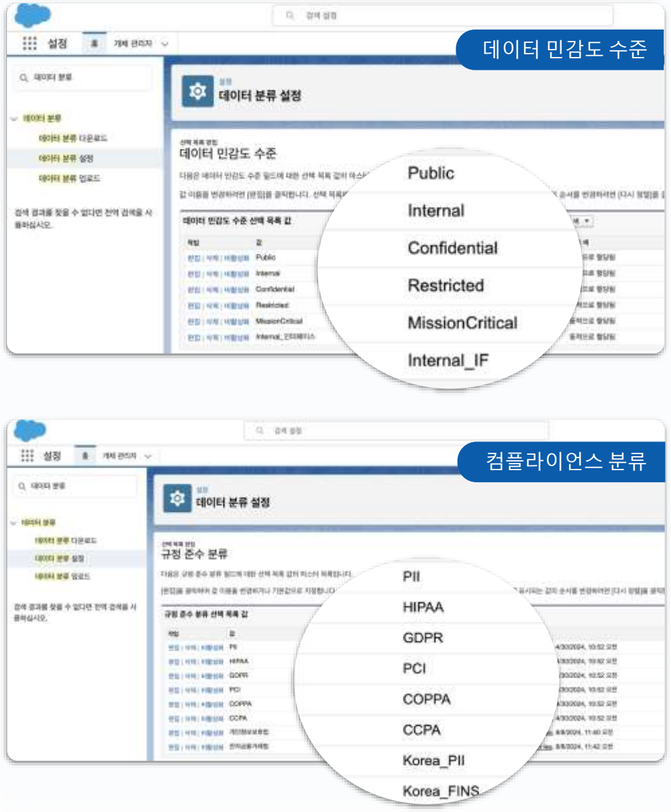
AI 혁신과 함께하는 데이터 보안 8가지 실행 전략

1. 데이터 범위 파악 및 분류
2. 데이터 암호화
3. 역할 기반 접근 제어
4. 이상 징후 모니터링
5. 데이터 마스킹 및 익명화
6. 데이터 변경 이력 추적 및 복구
7. 분리된 테스트 환경 사용
8. 정기적인 보안 테스트 수행

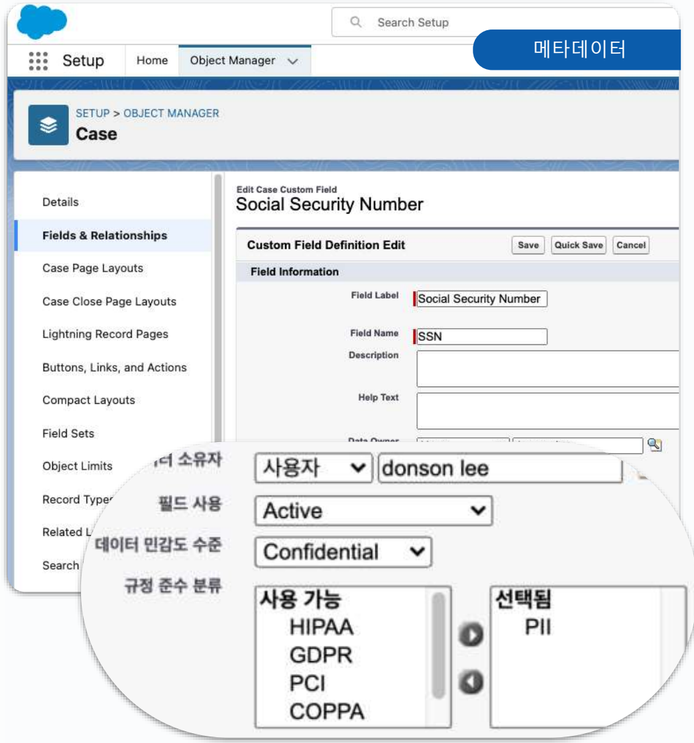
1 데이터 범위 파악 및 분류

Salesforce 플랫폼의 메타데이터를 활용하여 중요 데이터 식별 및 분류 체계 확립

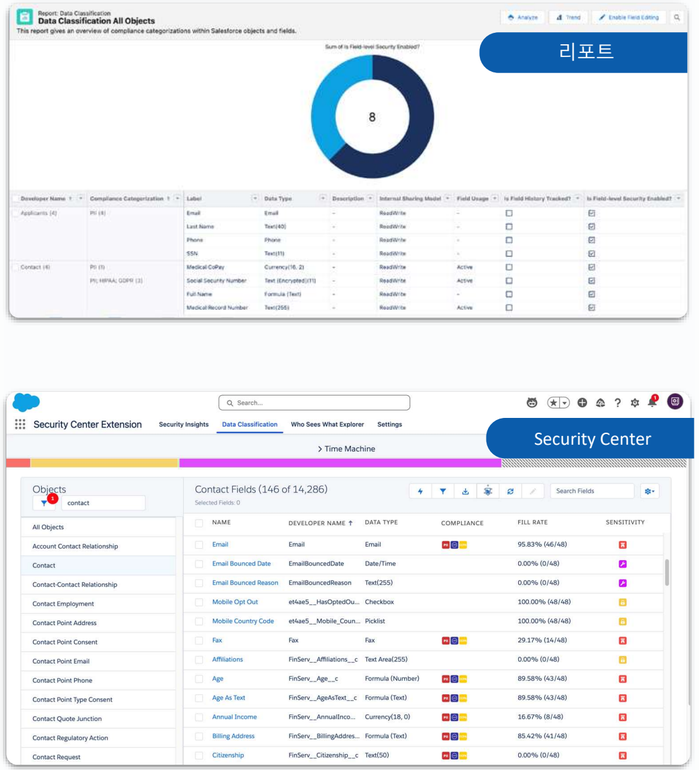
데이터 분류 설정



필드별 식별



모니터링



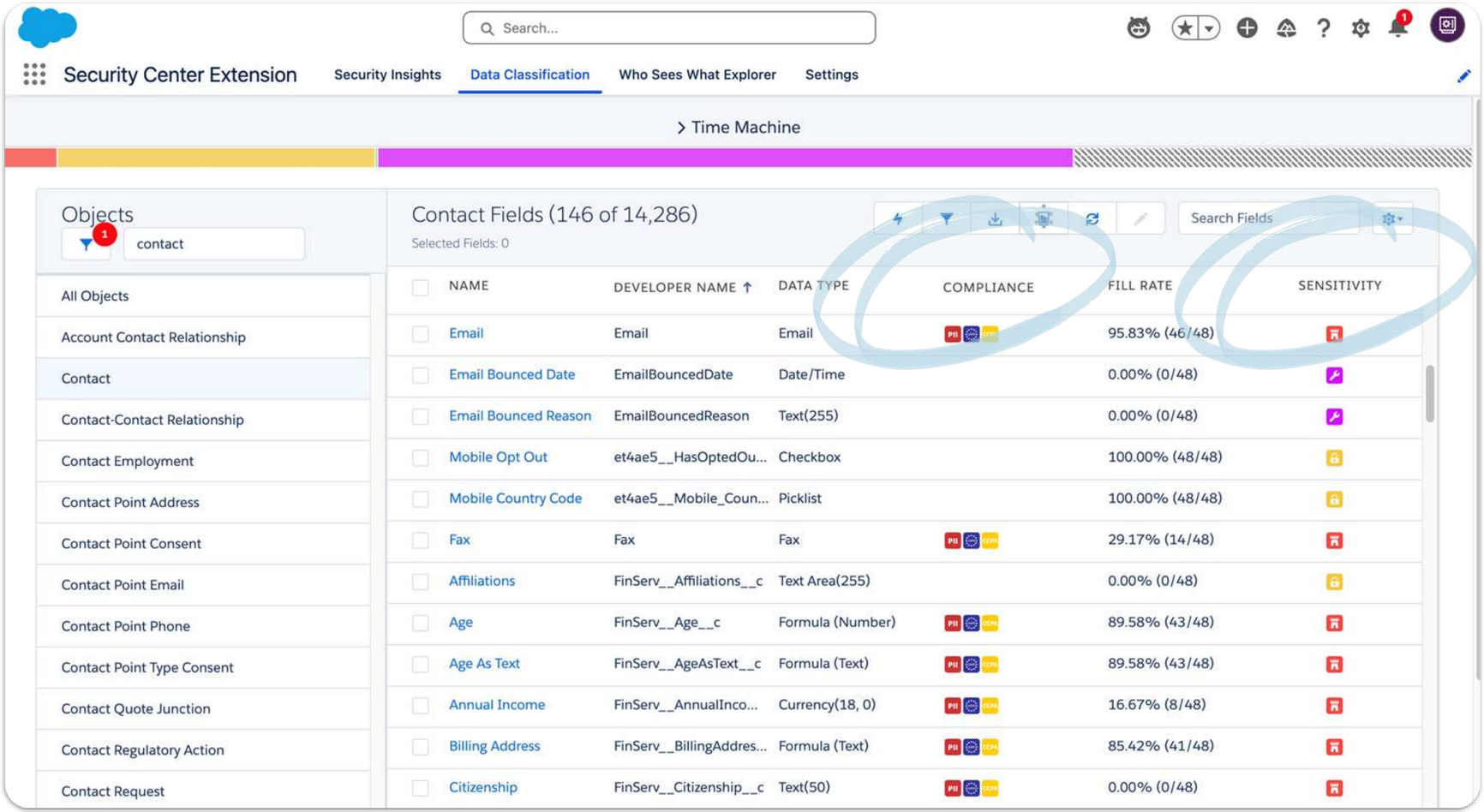
1 데이터 범위 파악 및 분류

Salesforce 플랫폼의 메타데이터를 활용하여 중요 데이터 식별 및 분류 체계 확립

Salesforce 보안 솔루션인 **Security Center** 확장 기능

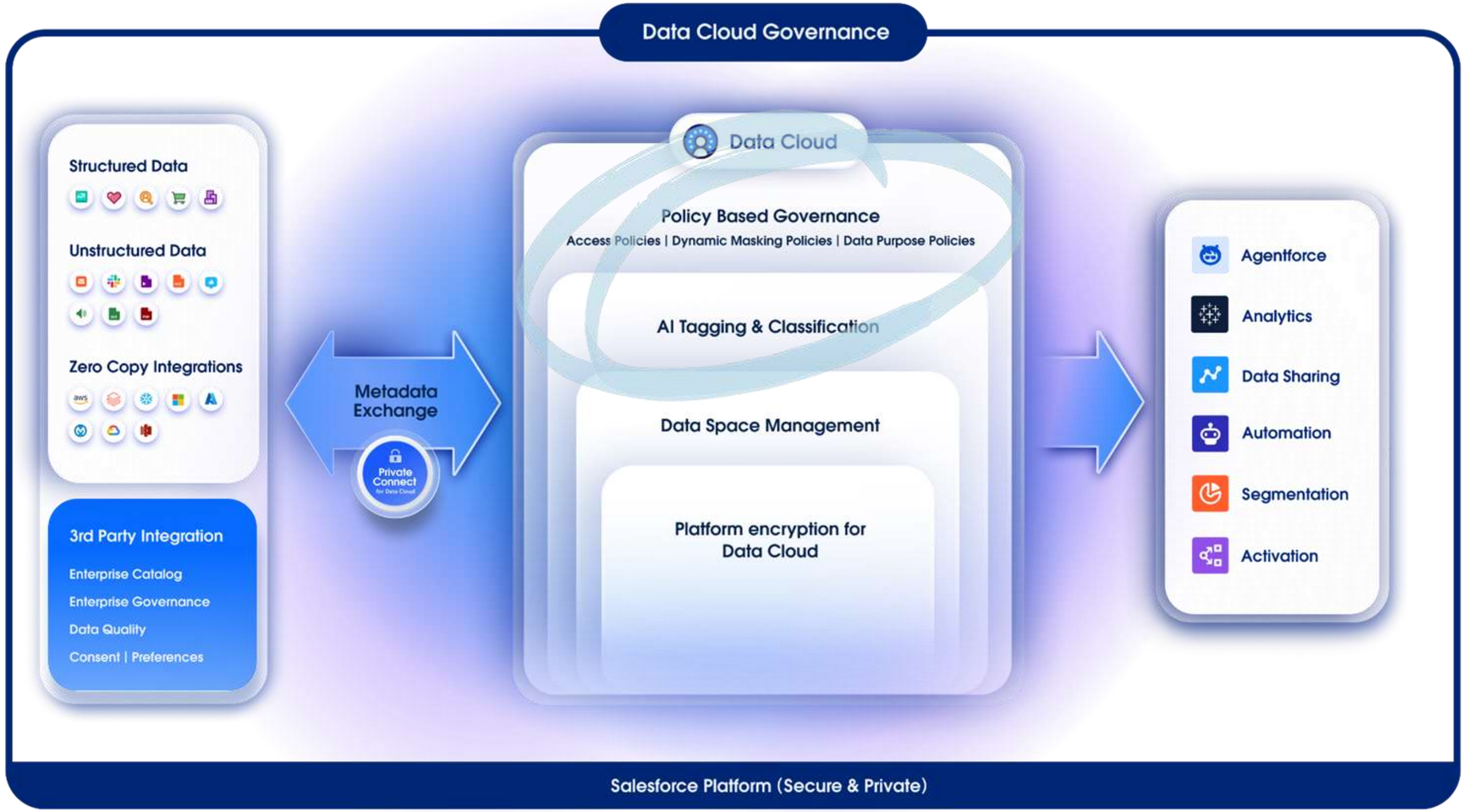
신속한 데이터 민감도 수준 및 분류 모니터링

민감한 정보의 보호 수준을 효율적으로 평가하고, Org 내 발생할 수 있는 고위험 상황을 완화



1 데이터 범위 파악 및 분류

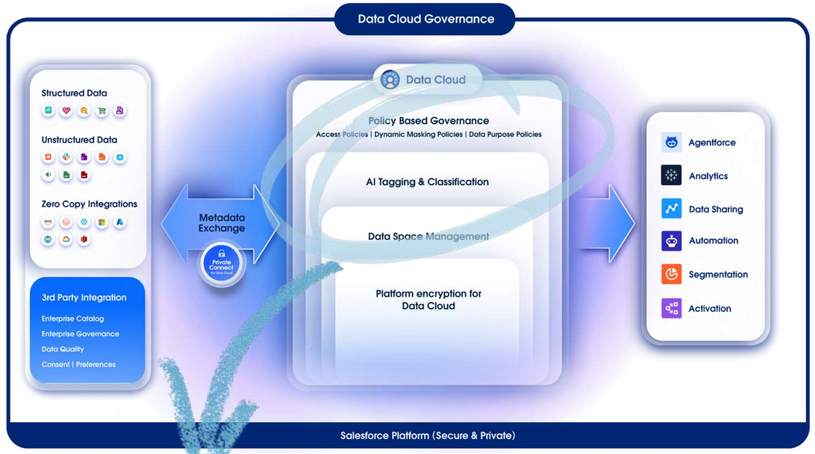
Agentforce 기반인 Data Cloud경우, 태그 및 분류에 의한 데이터 거버넌스 확립

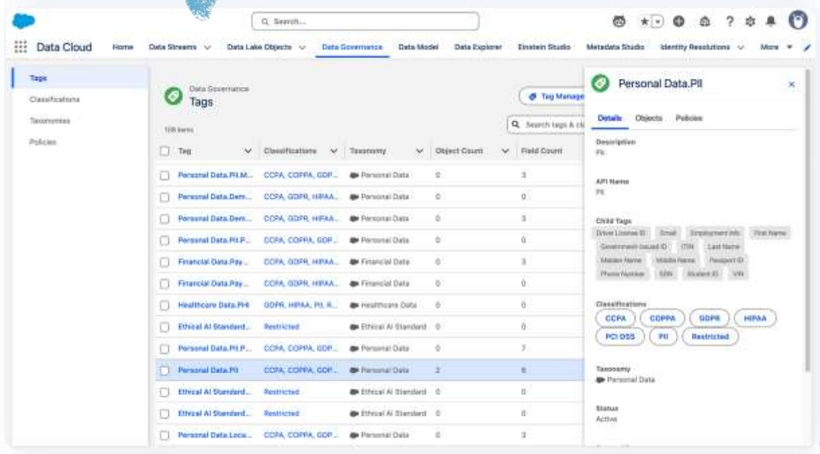


2025년 하반기 출시 예정

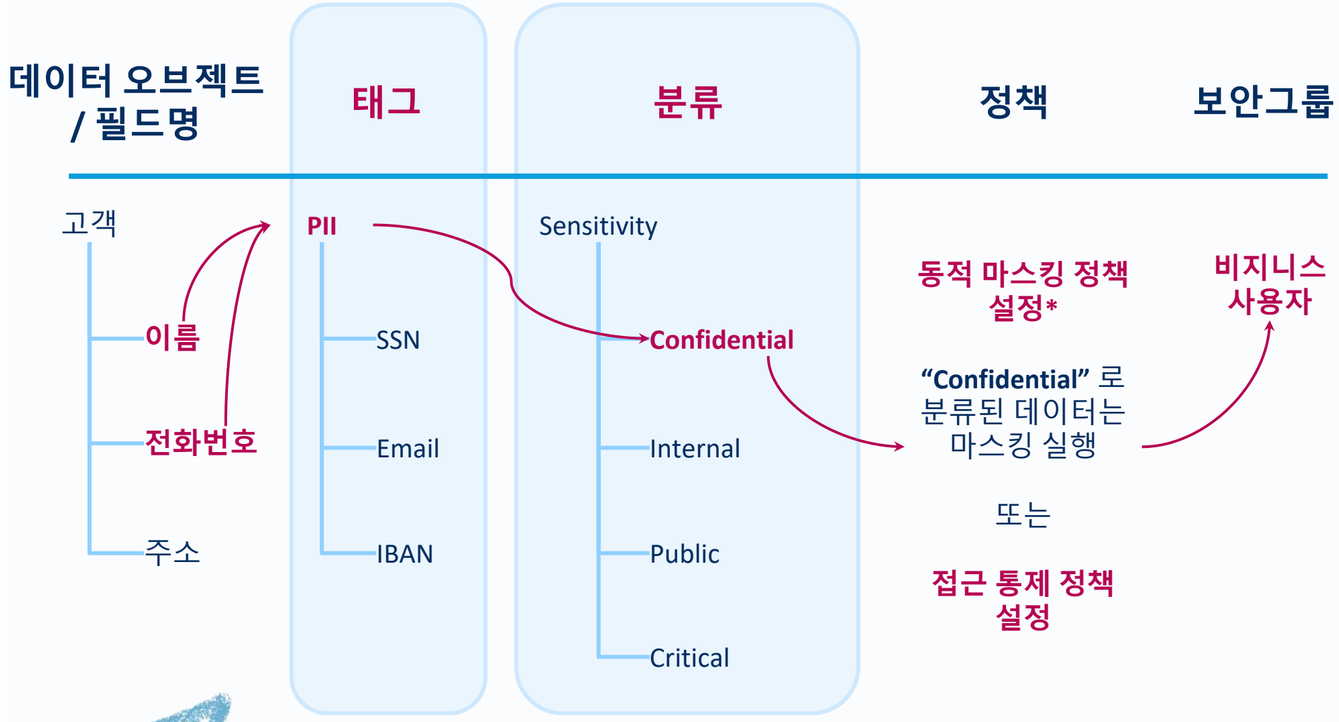
1 데이터 범위 파악 및 분류

Agentforce 기반인 Data Cloud경우, 태그 및 분류에 의한 데이터 거버넌스 확립





AI Tagging & Classification



- 정형 및 비정형 데이터 태그 지정
- 태그기반으로 정책 생성 및 적용


Data Cloud
Governance

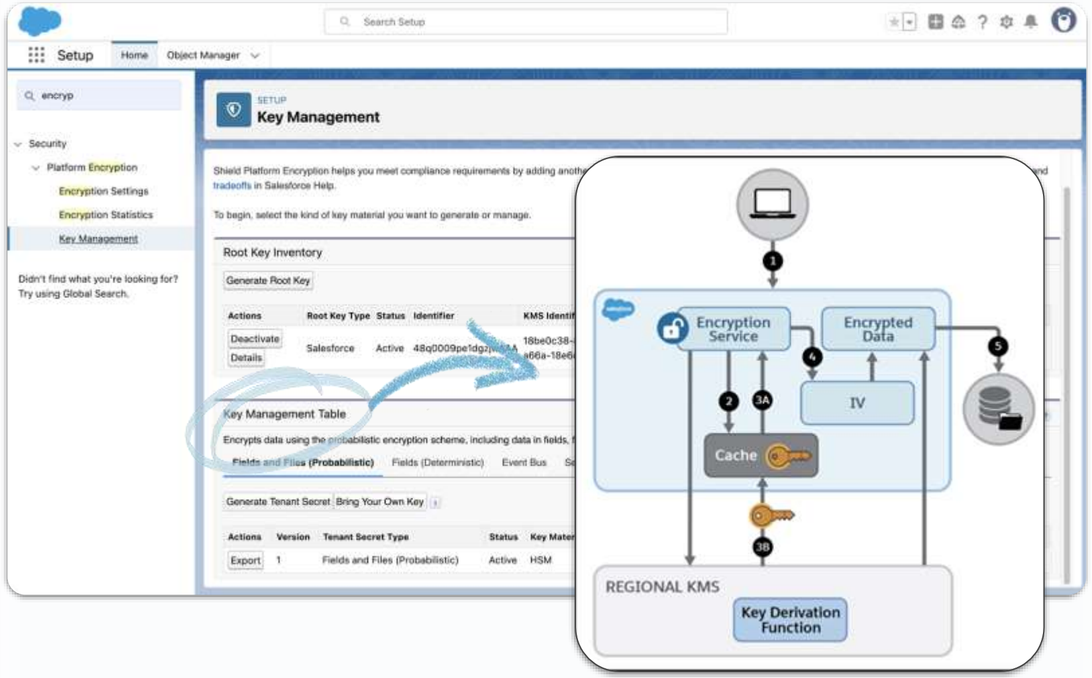
Shield - Platform Encryption 솔루션으로 데이터 암호화 및 키관리 강화

데이터 암호화

	무엇을 암호화 하는가?	1st Party	Hyperforce
App Tier Shield 필드 단위 암호화 256 bit AES CBC	• 일부 표준 필드 • 확장필드 • 첨부파일, 플랫폼이벤트, 채터, 검색인덱스, CRM Analytics	제공 (Shield)	제공 (Shield)
DB Tier Shield 데이터베이스 암호화 256 bit AES GCM	전체 트랜잭션 데이터베이스 • 모든 표준 필드값 • 모든 확장 필드값 • 커스텀 메타데이터 등	미적용	적용 예정 (2025년 하반기) 단, Shield 또는 Platform Encryption 구매고객에만 적용
Volume Encryption 256 bit AES	볼륨 암호화 또는 DB SAN 암호화	기본 적용됨	기본 적용됨

- 데이터 필드레벨 암호화
- DB 암호화(tenant level, 2025하반기 예정)
- 볼륨/스토리지 레벨 암호화

데이터 암호화 키 관리



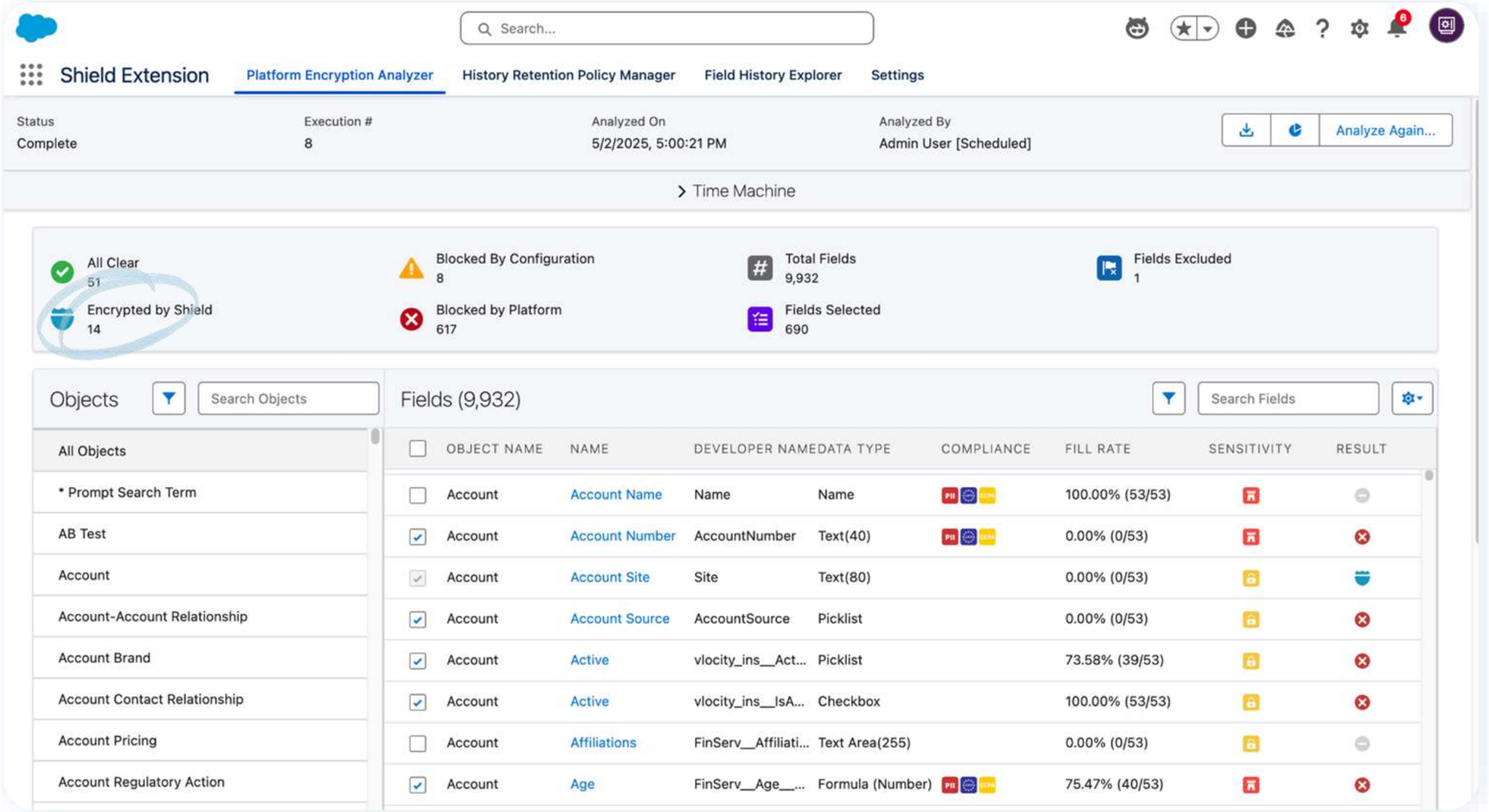
- 고객에의한 키 라이프사이클 : 데이터 암호화 키 생성/파기 등의 정기적인 관리 수행
- Salesforce HSM : FIPS 140-2 레벨 3 인증 **하드웨어 보안 모듈(HSM)** 장치를 사용하여 암호화 처리 및 키 관리

Shield - Platform Encryption 솔루션의 Analyzer로 암호화 분석 및 실행

싱글 뷰를 통한 신속한
암호화 필드 모니터링

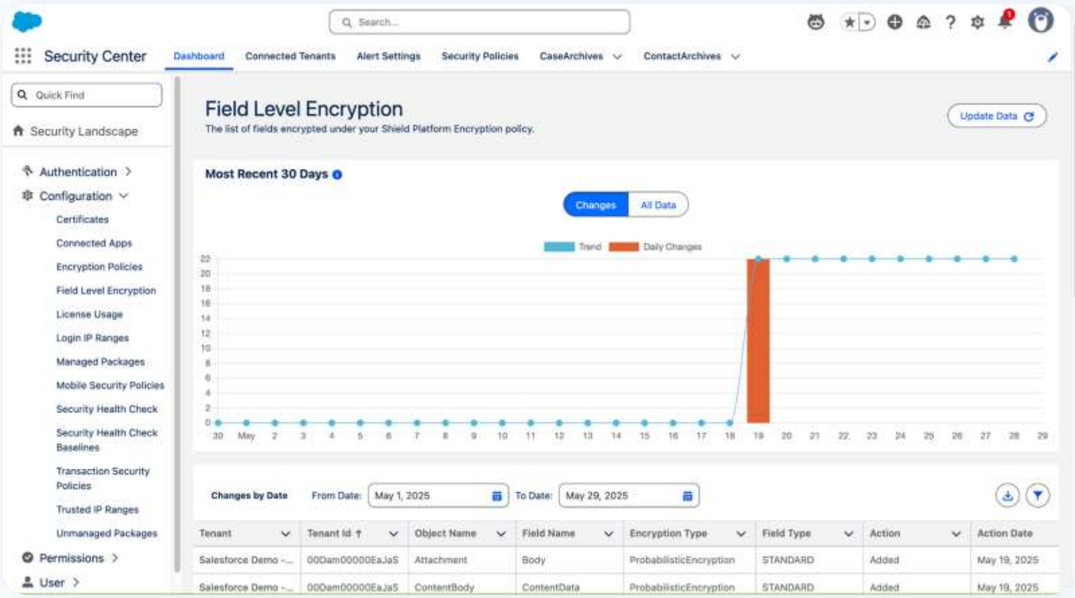
데이터 민감도 및
컴플라이언스 분류에 따른
암호화 여부 모니터링

필드 암호화 가능여부 분석
및 필요시 암호화 적용



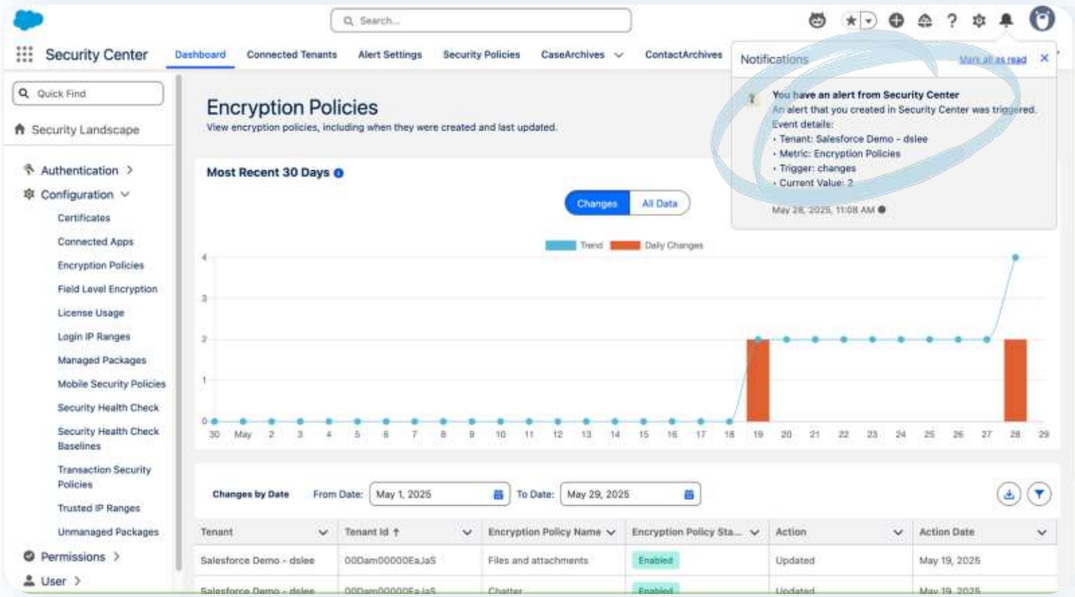
Security Center 솔루션으로 암호화 정책 및 암호화 필드 변경 추적 모니터링

데이터 필드 암호화 변경 추적



- **Salesforce Security Center**
  권한,인증,설정변경사항 등의 제어 현황을 모니터링하여,
  위험분석 및 평가를 통해서 위협 노출을 최소화

암호화 정책 변경 추적



- **Alert** 설정
  암호화 정책, 필드단위 암호화등의 변경사항이 발생할 경우에
  알람 실행

3 역할 기반 접근 제어

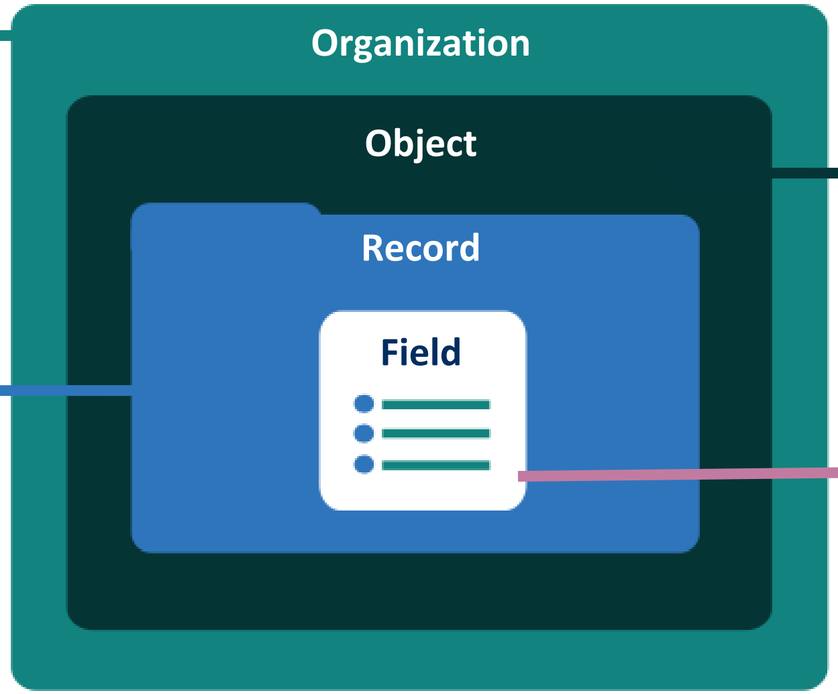
메뉴/데이터에 대한 세분화된 접근 권한기반 통제 실행 및 모니터링

Org

- 인증 (MFA/SSO)
- 신뢰된 IP 대역
- 로그인 시간대
- 로그인 IP 대역
- 패스워드 정책 및 복잡도

레코드

- Org 전체 공유 기본값 (OWD)
- Role 계층
- 공유규칙
- 팀, 매뉴얼 공유
- 제한 규칙



오브젝트

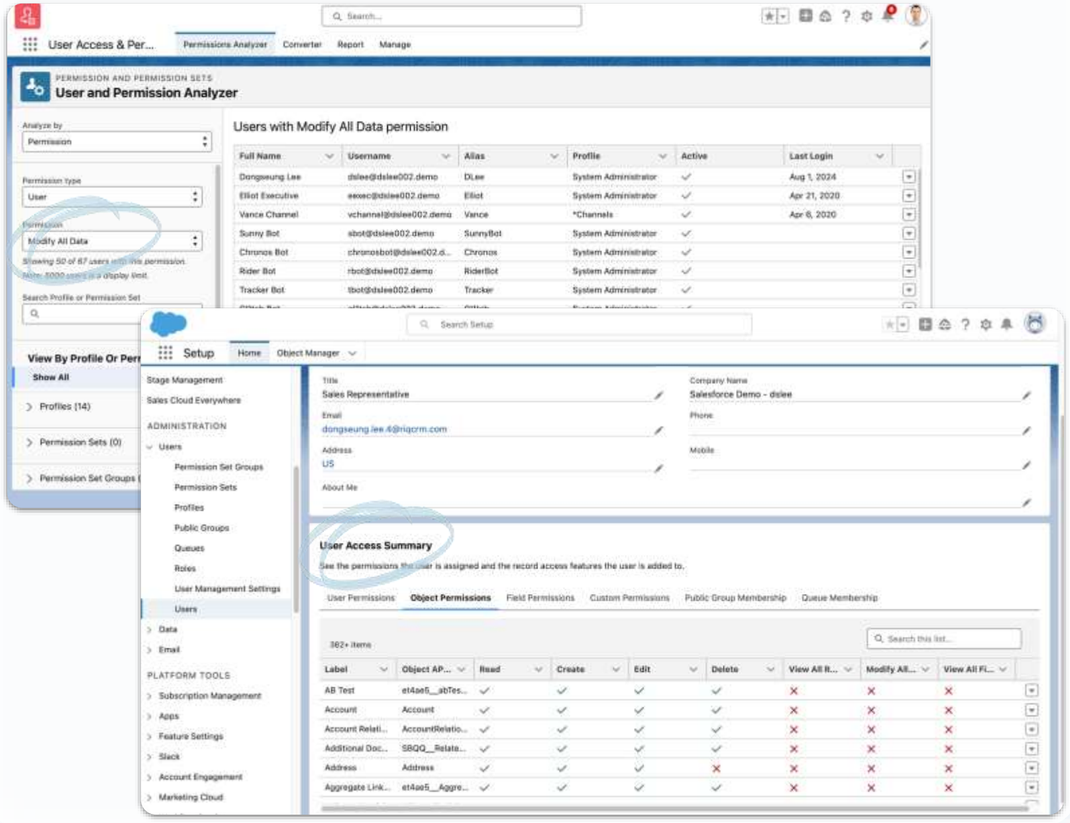
- 라이센스
- CRED 권한(via Profile or Permission Set)

필드

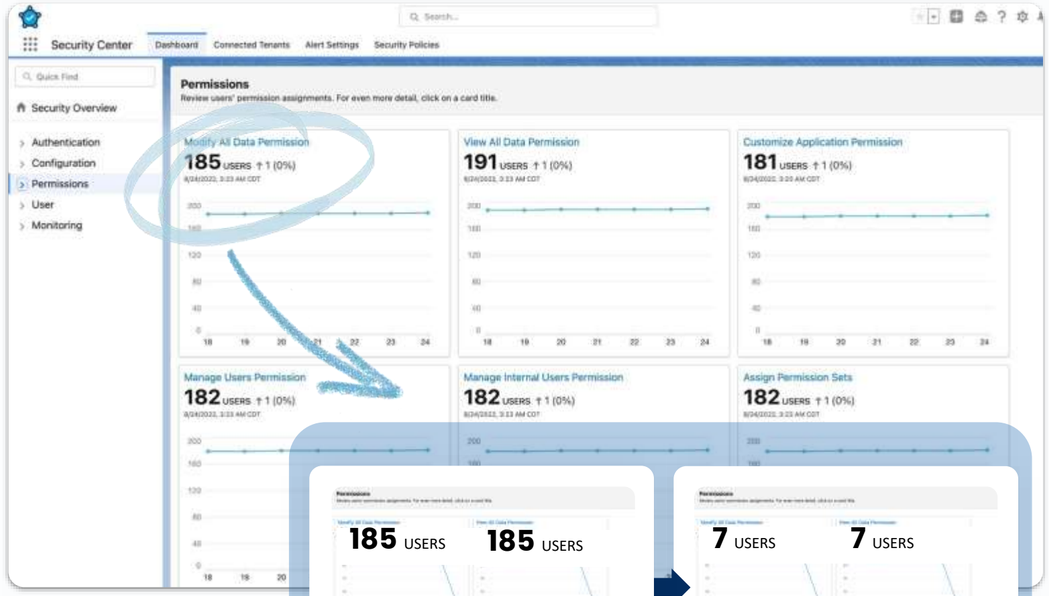
- 필드 레벨 보안
- 페이지 레이아웃

AppExchange 앱, Salesforce Security Center 등으로 권한 모니터링

권한 모니터링



Security Center - 권한



Modify All Data 권한 예시

Security Center 사용 이전
과다한 권한 사용자, 보안 정책 일관성 등 가시성 확보 부족

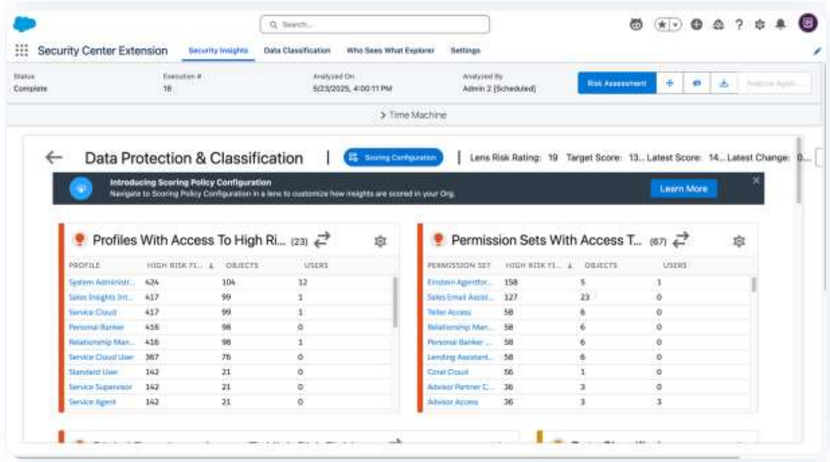
Security Center 사용후
싱글 뷰 가시성 확보

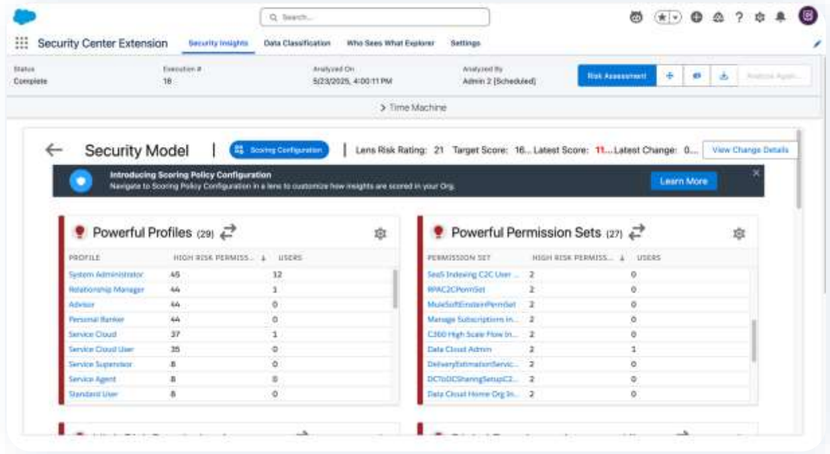
Security Center 데모 동영상 1

Security Center 데모 동영상 2

3 역할 기반 접근 제어

Security Center의 확장기능인 Security Insight로 리스크 관리





보안 인사이트

데이터 보호 및 분류

접근 제어 (인증)

보안 모델 (권한)

연동

데이터 유출 방지

모니터링

Lens	Quantitative Risk Rating	Target Risk Mitigation Score	Latest Risk Mitigation Score	Change from Previous Analysis	Trend Last 365 Days
Data Protection & Classification	19	13.07	14.37	0.00	
Access Control (Authentication)	9	5.40	2.49	0.00	
Security Model (Authorization)	21	16.25	11.06	0.00	
Integration	15	11.94	11.95	0.00	
Data Loss Prevention	23	11.86	6.92	0.00	
Monitoring	14	11.27	11.36	0.00	

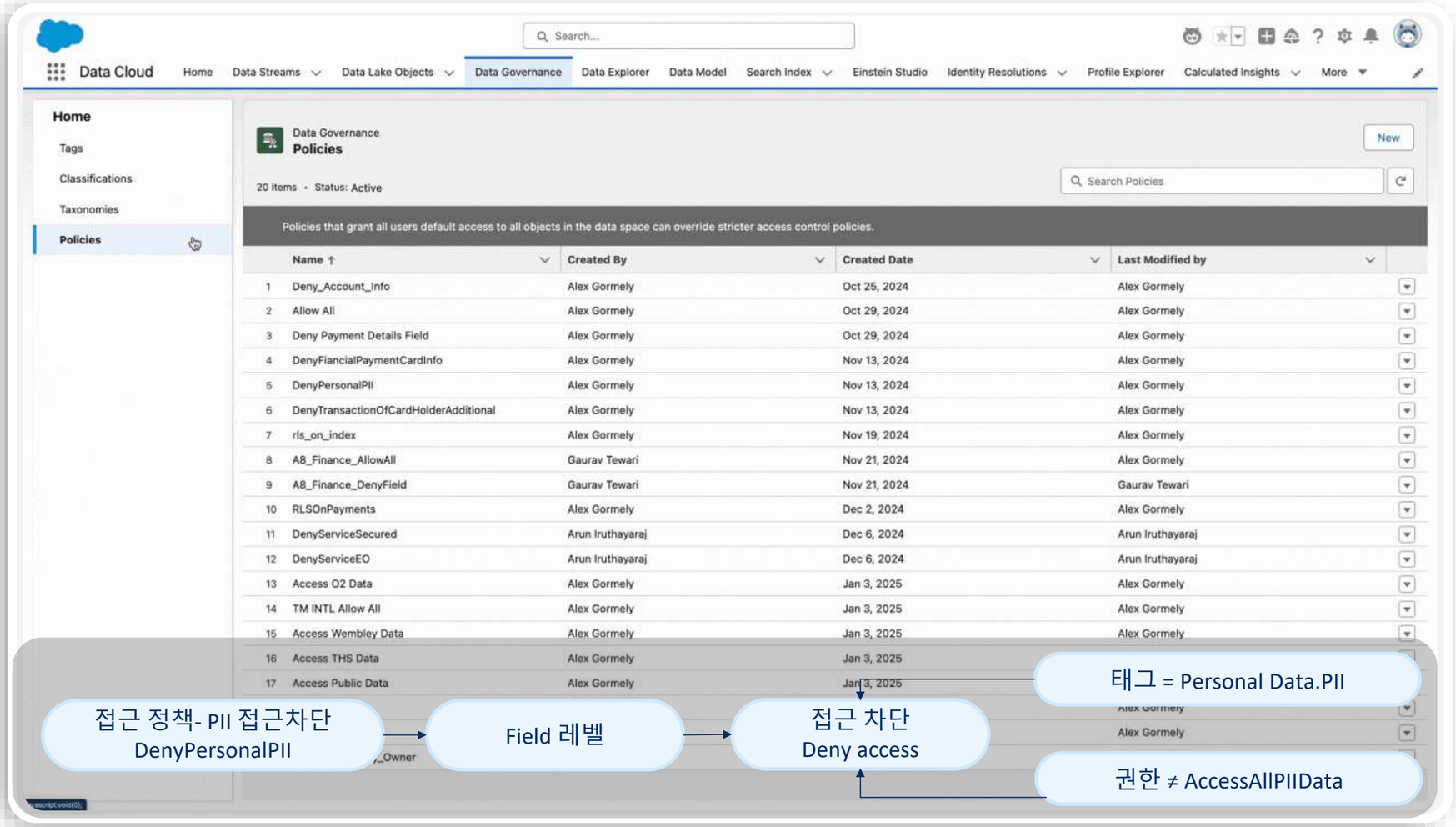
3 역할 기반 접근 제어

Agentforce기반인 Data Cloud에 대한 접근 정책 가버넌스 구현

속성/역할기반 접근통제
사용하여 정책 작성/실행/관리 (ABAC/RBAC)

오브젝트/필드/레코드
단위의 접근 통제 사용하여 정책을 일관되게 적용

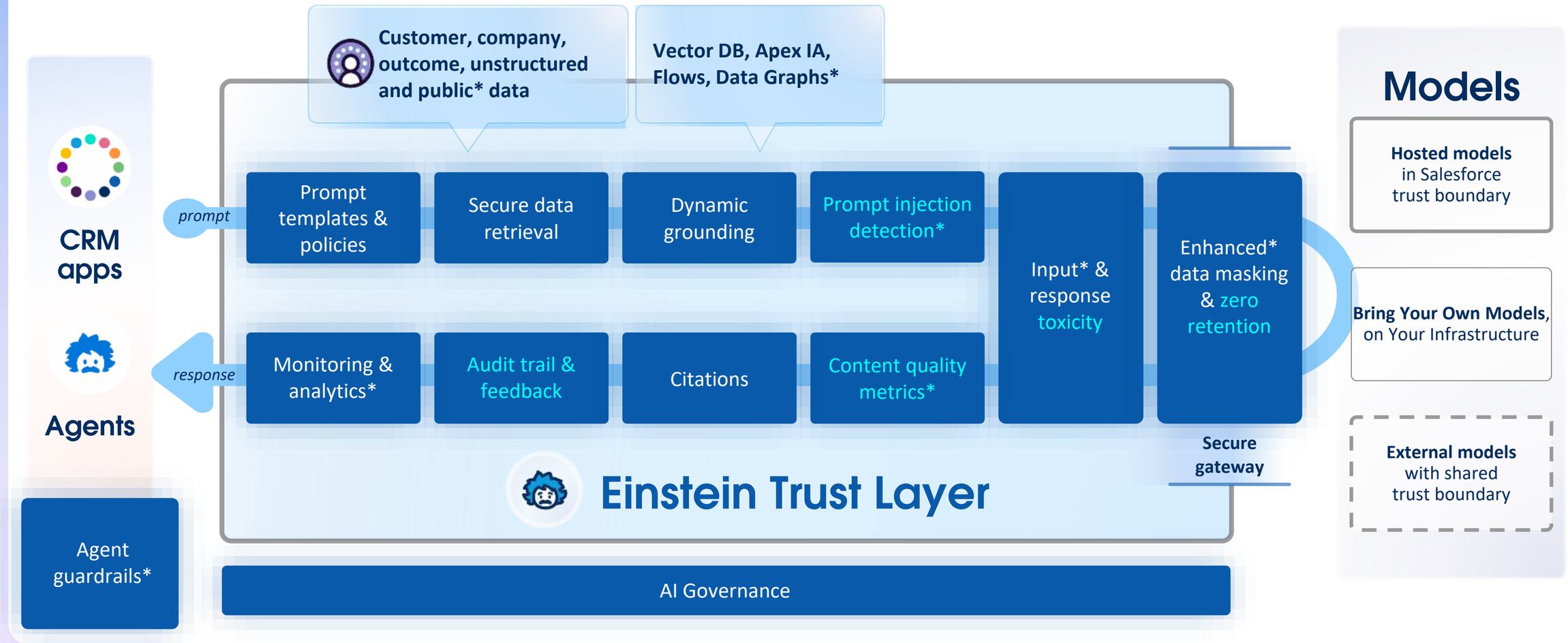
권한있는 사람 또는 Agent에게만 올바른 접근 제공



ABAC(Attribute Based Access Control)
RBAC(Role Based Access Control)

4 이상 징후 모니터링

Einstein Trust Layer로 안전한 AI 가드레일 제공하며, 유해성 등 이상 징후 모니터링



*일부 기능은 로드맵

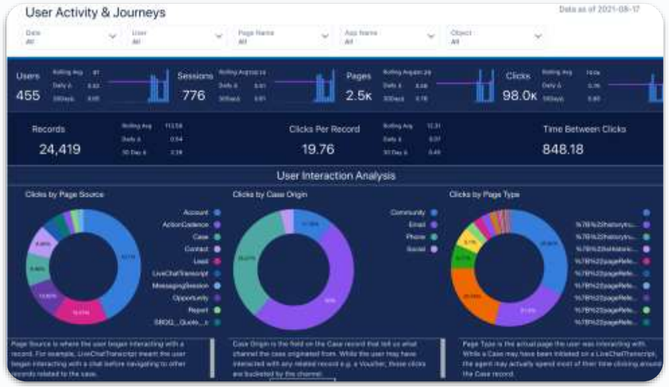
4 이상 징후 모니터링

Shield – Event Monitoring 솔루션으로 위협 탐지 및 데이터 유출 방지 수행

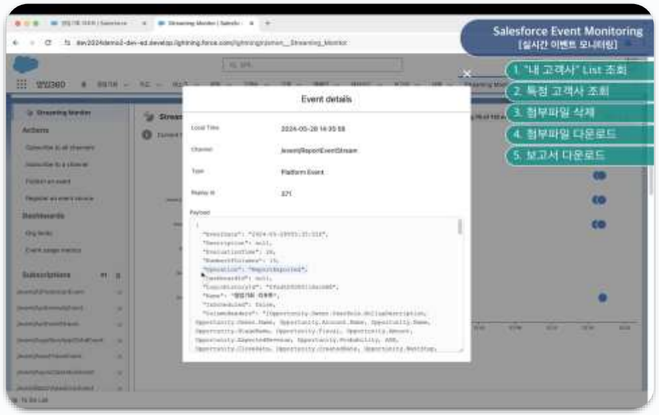
이벤트 로그 및 위협 탐지

이벤트 로그 모니터링
80여개의 이벤트 추적
(성능, 보안, 사용성)

분석대쉬보드
로그 시각화를 통한 모니터링



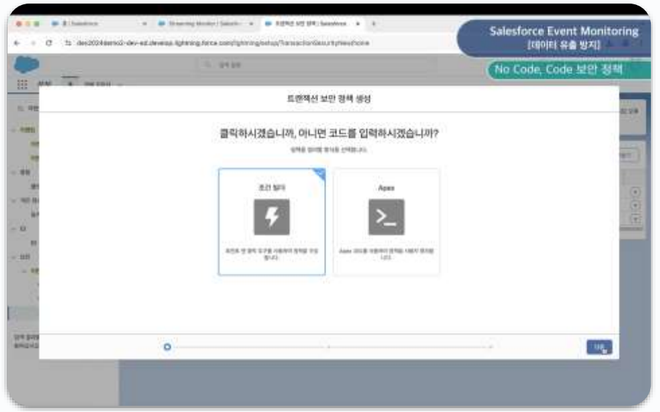
위협 탐지
통계 및 머신 러닝 기법 사용
Session Hijacking
Credential stuffing
Report Anomaly
API Anomaly
Guest User Anomaly



데이터 유출 방지

No Code/Code
보안정책 적용

차단 및 알람
(Block/Notification)



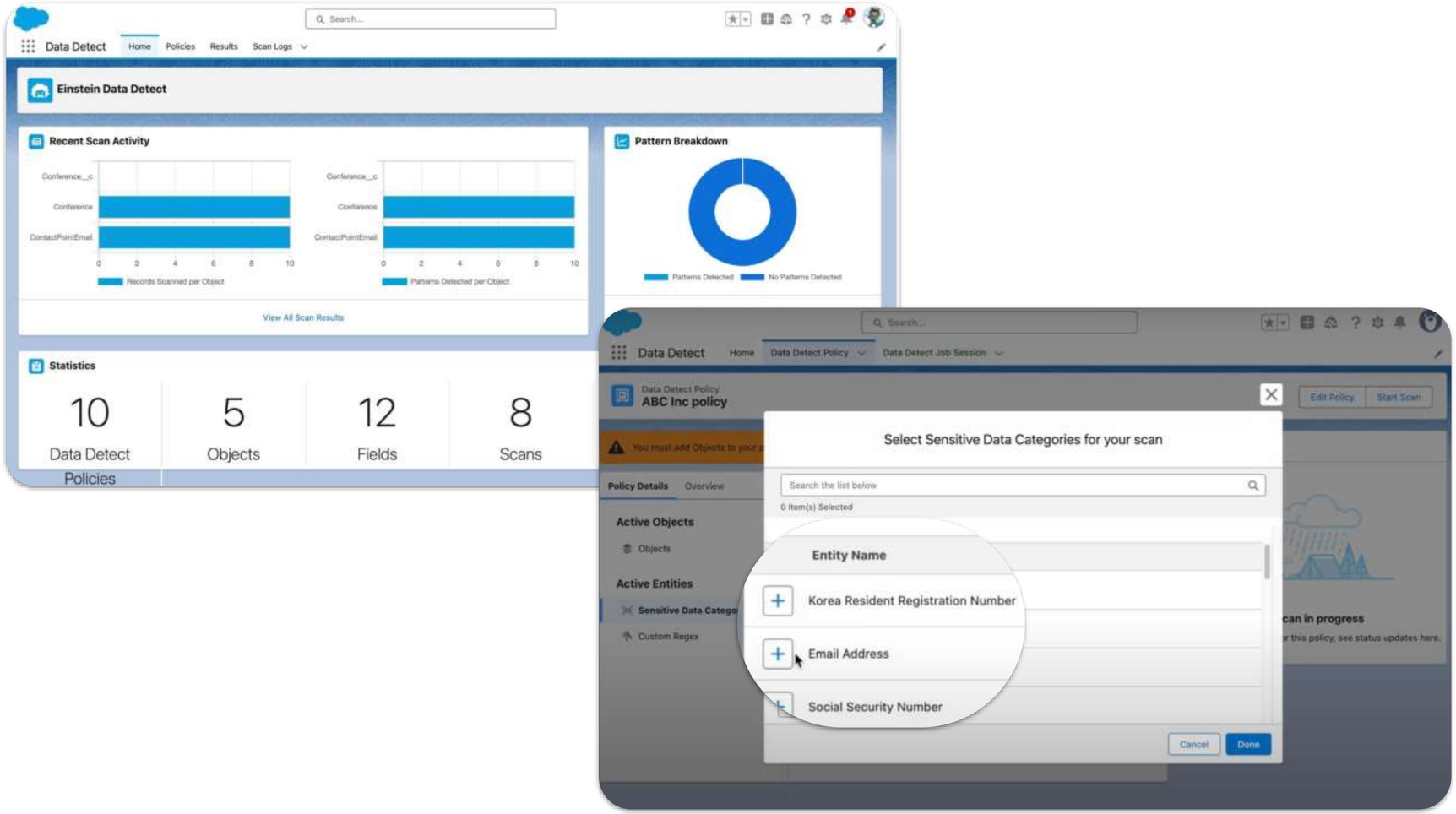
실시간 이벤트 모니터링 및 제어
ApiEvent
FileEvent
ListViewEvent
LoginEvent
ReportEvent
PermissionSetEvent
BulkApiResultEvent

Shield – Data Detect 솔루션으로 패턴 매칭에 의한 민감 데이터 식별

민감한 데이터를 빠르게
찾고 분류

신용카드번호,
이메일주소와 같은
패턴기반의 민감정보 식별

한국 주민번호 포함 21개
민감정보 식별 및 사용자
지정 패턴정의 (Beta)



4 이상 징후 모니터링

Agentforce를 활용하여, 보안솔루션과 연계하여 위협탐지 및 이상현상 모니터링

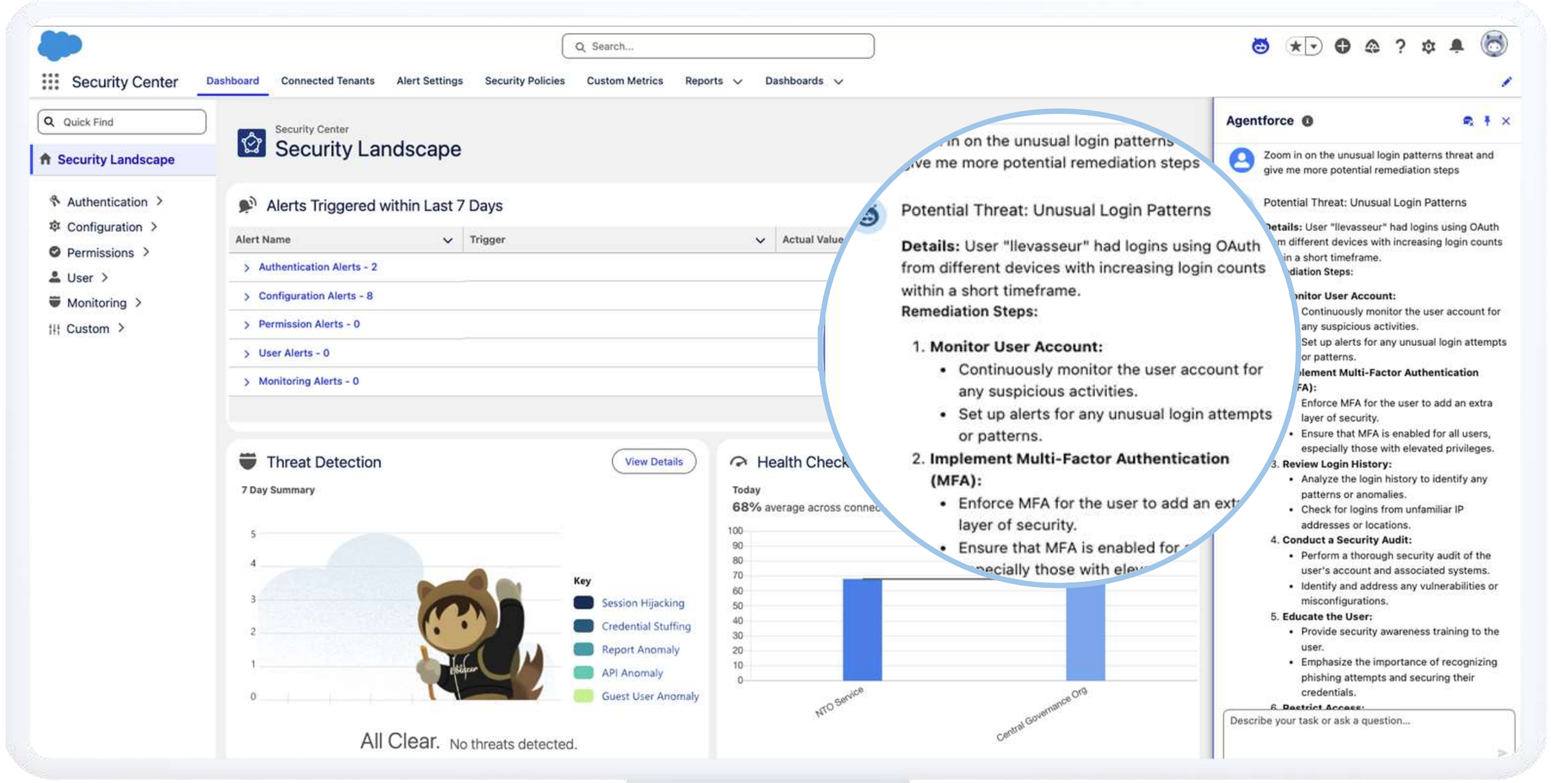
여러 Org의 보안 태세에 대한 강력하고 빠른 인사이트

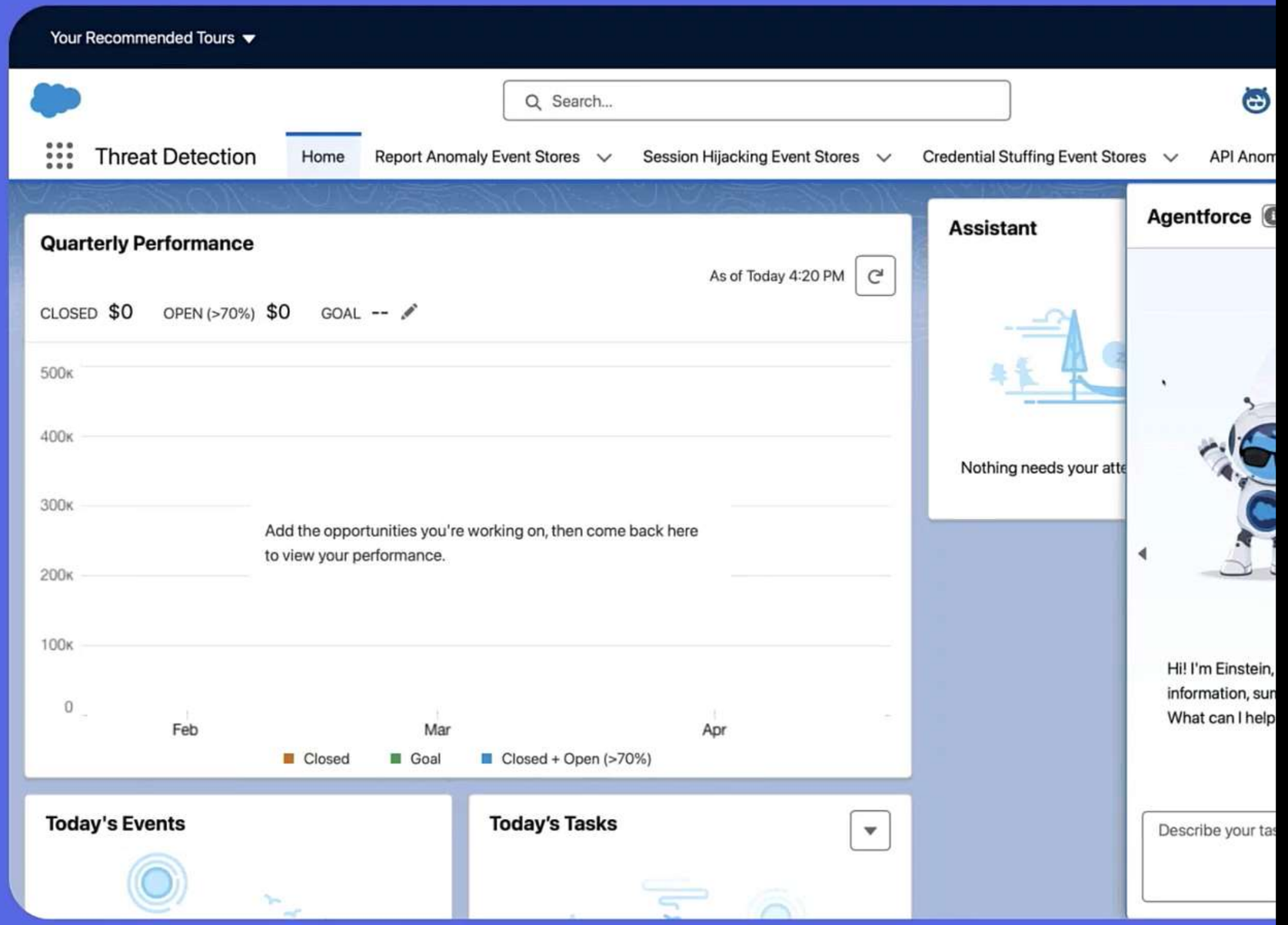
보안 취약점을 평가하고 신속하게 조치

선제적 보안을 통해 비정상적인 사용자 활동이나 동작을 탐지

Security Center

Shield: Event Monitoring

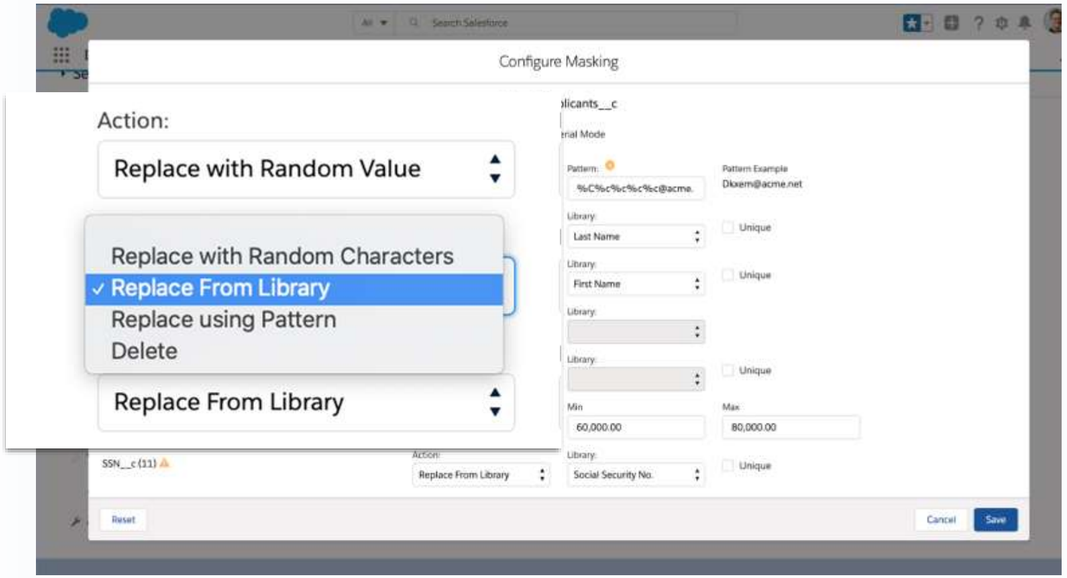



Your Recommended Tours
Search...
Threat Detection
Home
Report Anomaly Event Stores
Session Hijacking Event Stores
Credential Stuffing Event Stores
Quarterly Performance
As of Today 4:20 PM
CLOSED $0
OPEN (>70%) $0
GOAL --
500K
400K
300K
200K
100K
0
Add the opportunities you're working on, then come back here to view your performance.
Feb
Mar
Apr
Closed
Goal
Closed + Open (>70%)
Assistant
Nothing needs your atte
Agentforce
Hi! I'm Einstein,
information, sur
What can I help
Describe your ta
Today's Events
Today's Tasks

5 데이터 마스킹 및 익명화

Data Mask & Seed 솔루션으로 운영데이터를 Sandbox환경으로 복제시 데이터 마스킹

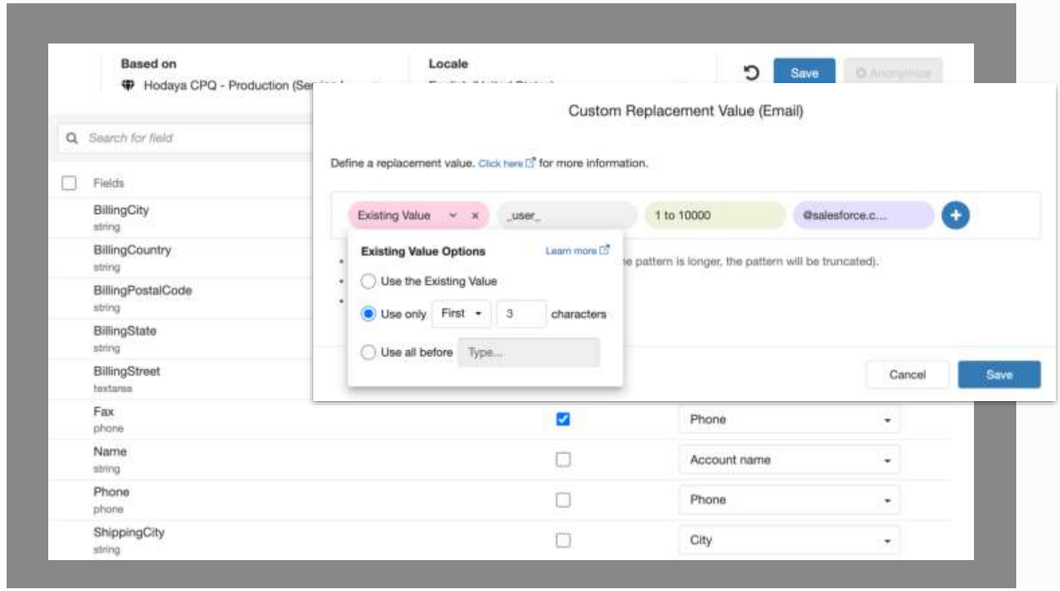
데이터 마스크



라이브러리에서 대체
Balke→ Kelsey

패턴 매칭
999-99-9999 → XXX-XX-9999

익명화



임의 값
Blake@gmail.com→
Bla_user_5@sample.com

빈값 채우기
_____ → Blake

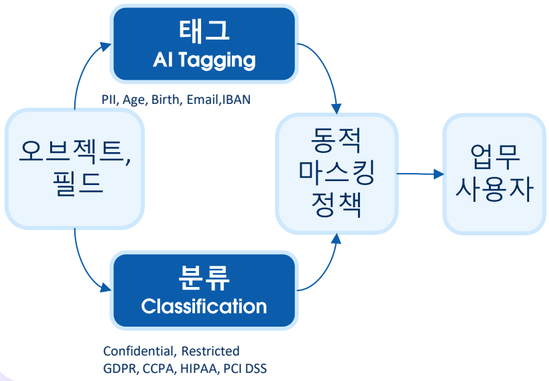
5 데이터 마스킹 및 익명화

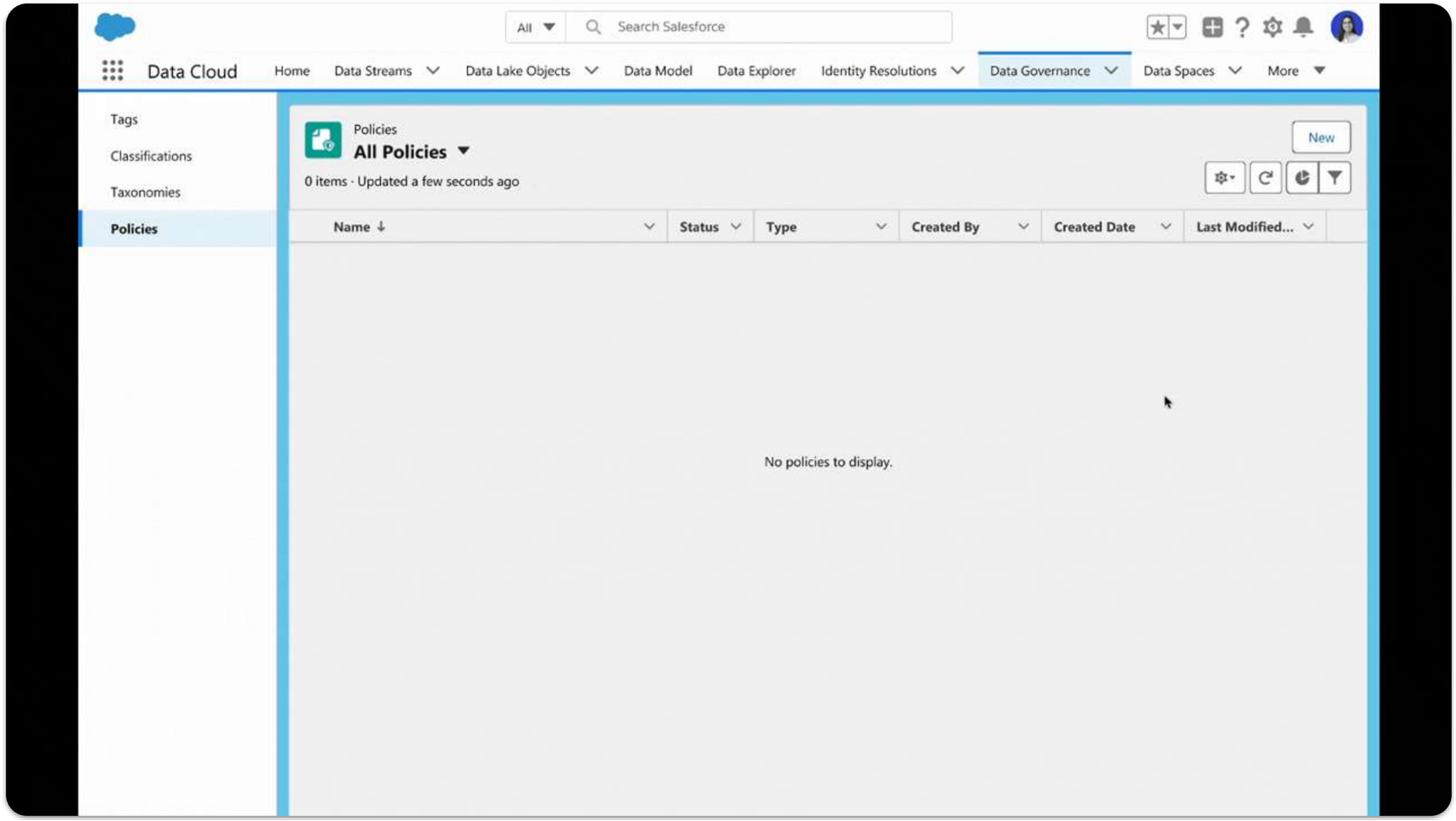
Dynamic Data Masking Policies

(2025년 하반기 출시, Data Cloud)

민감한 정보를 동적으로 마스킹 하기 위한 정책 생성

기본 데이터 세트를 수정하지 않고 데이터마스킹

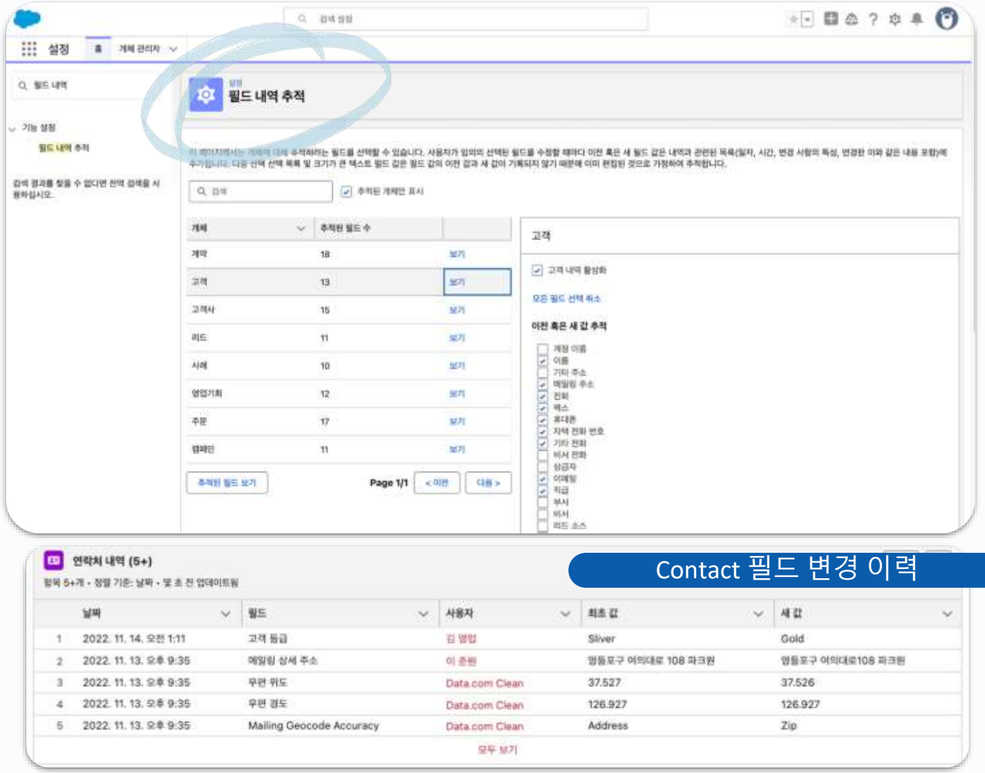




6 데이터 변경 이력 추적 및 복구

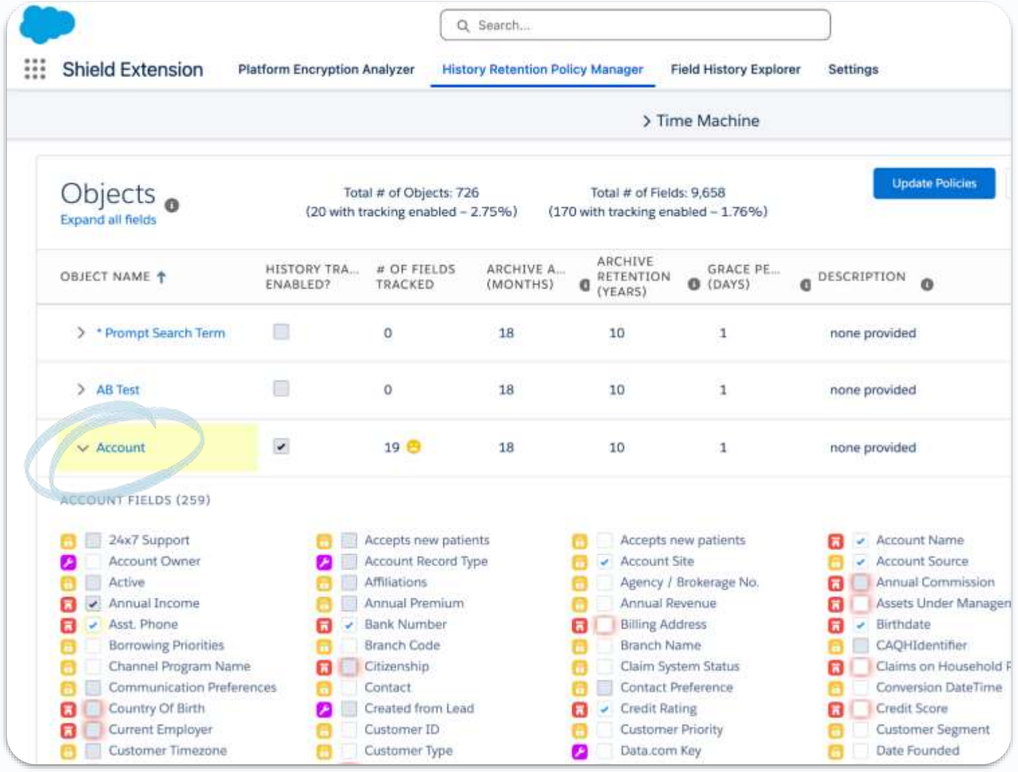
데이터 변경 이력에 대한 추적성 유지 및 이력 보관 정책 수립

Field History Tracking



Object당 20개필드, 6개월 이력 보관, CSV/API 연계

Shield - Field Audit Trail



Object당 60개필드, 무제한 이력 보관

6 데이터 변경 이력 추적 및 복구

Salesforce Backup & Recover

실수로 변경된 내용을 복구하기 위한 복구 계획 구현 필요

자동 백업

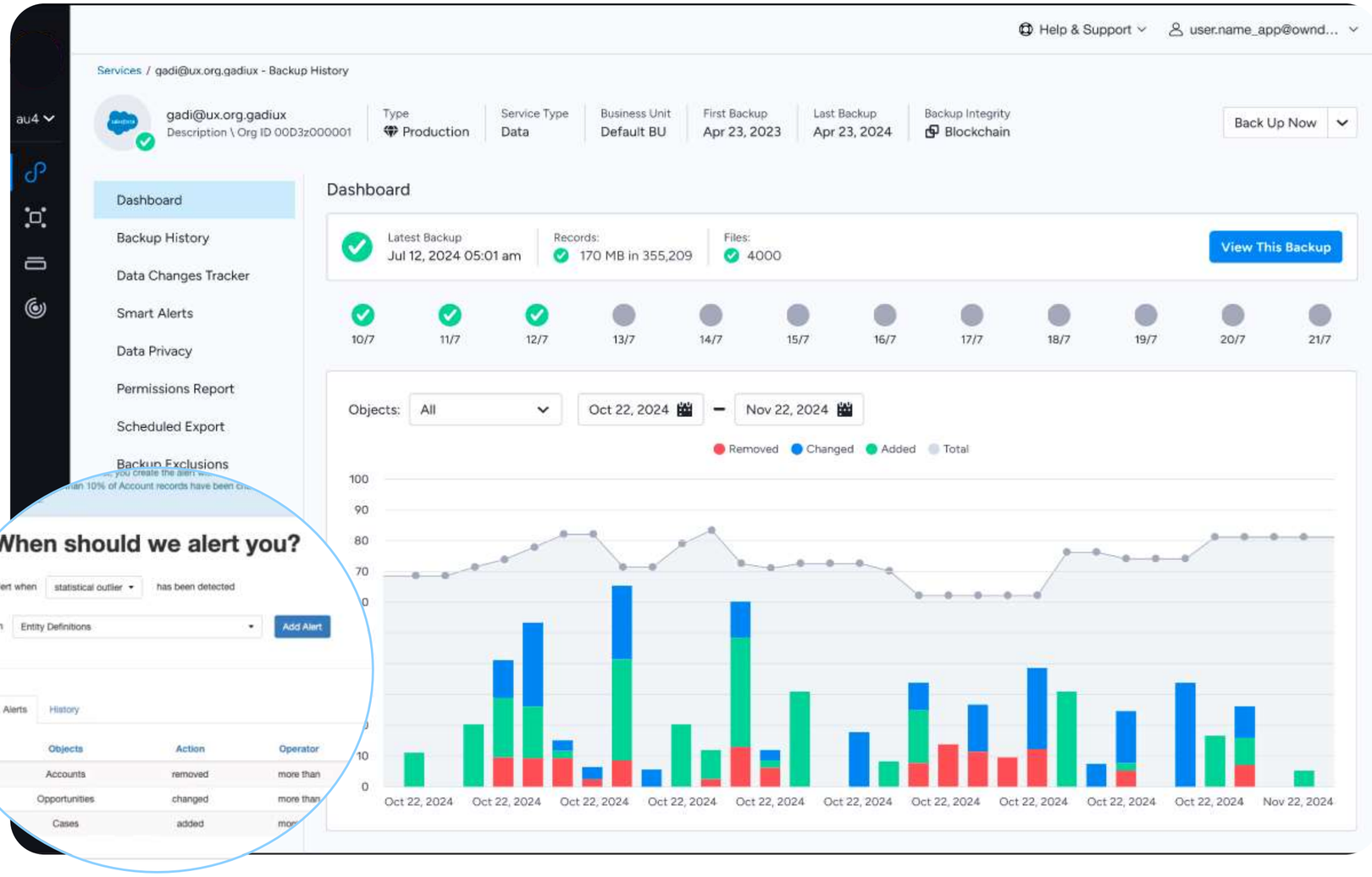
중요한 데이터, 메타데이터, 샌드박스 등을 매일 자동으로 백업하여 데이터를 쉽게 보호

정확하고 신속하게 복원

손실 영향을 받은 객체, 필드 및 레코드를 정확하게 복원하여 복구 가속

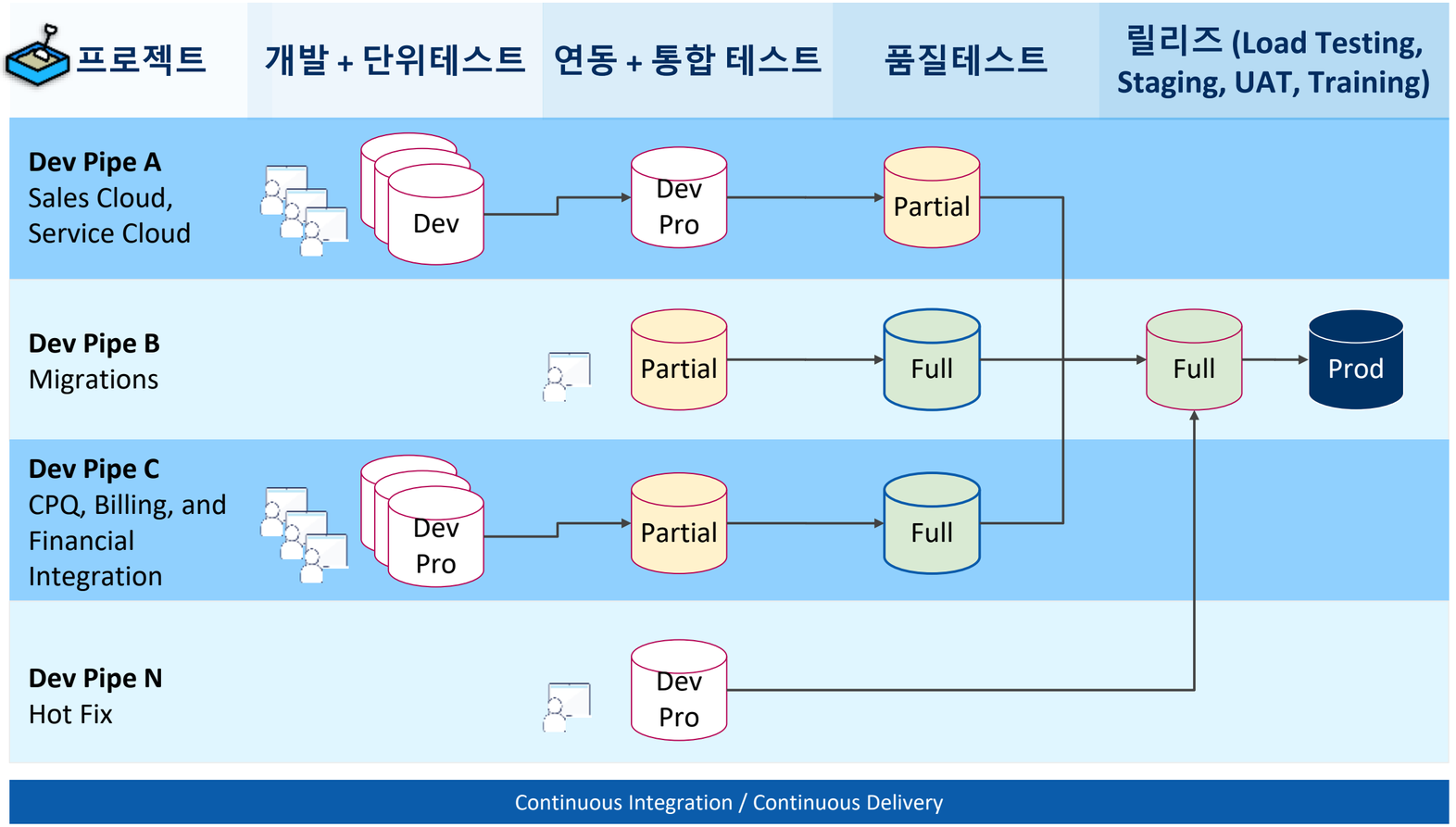
사전 예방적인 데이터 모니터링

이메일로 직접 알림을 보내 비정상적인 데이터 활동을 감지



7 분리된 테스트 환경 사용

Sandbox환경으로 운영환경과 분리하여, 우발적인 데이터 유출 및 무단 접근 방지



샌드박스 관리 및 안전한 테스트를 위한 4가지 실행전략

1. Agentforce Agent를 전용 환경에서 테스트하세요
2. 전체 데이터 세트를 사용하여 UAT를 수행하세요
3. 직원들에게 AI 기반 도구에 대한 교육을 제공하세요.
4. 샌드박스 환경에 대한 구조화된 전략을 도입하세요

정기적인 보안 테스트 수행

공유책임모델 관점에서 취약점 점검 및 위협 탐지를 정기적으로 수행

Salesforce 자체 취약점 점검

내부 점검
Salesforce 내부 Red 팀에 의한 수시/정기적 스캔 수행
OWASP top10 등 보안가이드 반영된 보안개발 Lifecycle 적용

외부 점검
Third Party에 의한 취약점/침투테스트 매년 수행
애플리케이션 1년 3번, 네트워크 1년 4번

버그포상 프로그램
보안 연구자(화이트 해커)에게 취약점 발견시 포상 (Bug Bounty)
2023년 40억원($3M) 포상하는등 예방적 보안 노력 강화

외부 보안 정보 조사
3rd party 취약성 인텔리젼스 피드 및 벤더 보안 통지 등 수집 리뷰
보고된 잠재적 취약점은 리스크 및 심각도 수준에 따른 대응

고객사 직접 취약점 점검

고객사 직접 점검
Salesforce 승인없이 고객사 자체적으로 취약점 테스트 수행
검증된 취약점 발견사항은 Security@salesforce.com로 제출

Salesforce 보안 솔루션

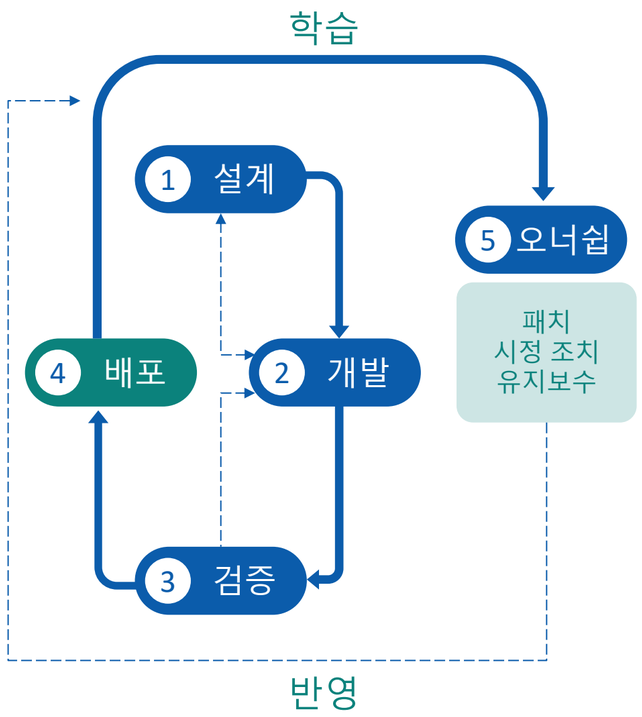
Salesforce Shield Event Monitoring :
사용자 수행 업무 등 80여개 이벤트 추적성 및 분석 보고서 활용하고, 데이터유출방지 및 위협탐지 수행

Salesforce Security Center :
인스턴스별 사용자 권한, 인증 등을 추적하고, 자동화된 위험 평가 수행

8 정기적인 보안 테스트 수행

Salesforce 자체적으로는 보안 개발 라이프사이클 프로세스를 운영하고 있음

Salesforce Secure Development Lifecycle



설계/개발

위협 모델링 → OWASP 보안 코딩 → SAST (정적 애플리케이션 보안 테스트) → Fuzz 테스트

STRIDE Model

White Box testing (Automatic)

배포후

제3자에 의한 취약성・침투테스트 (자동+수동)

세일즈포스의 취약성진단 비정기 침투테스트 및 레드팀 연습/대응 상황 확인

DAST (동적 애플리케이션 보안 테스트)

Black Box testing

- 벤더 배포 모니터링
- 버그 바운티
- 고객사에서 직접 침투테스트

발견된 취약점 등록

취약점 발견 직후의 조치

시스템 설정 및 수정을 통한 제한 및 모니터링 강화 등의 조치 시행

취약점 수정(패치)

심각도에 따른 패치 적용 및 변경 관리

취약점 분석 및 조치 판단

버그 추적 시스템

외부 기관 어드바이스

AI 혁신과 함께하는 데이터 보안 8가지 실행 전략

1 데이터 범위 파악 및 분류	데이터 감사 수행, 중요/민감 정보 식별, 분류 기준 설정
2 데이터 암호화	전송 및 저장중 데이터 암호화, 키 라이프사이클 수행 및 접근 제한
3 역할 기반 접근 제어	AI Agent포함해서 사용자별 접근 권한 설정, 정기적인 접근 감사 로그 검토
4 이상 징후 모니터링	AI 프로세스에 대한 실시간 모니터링, 이상 행동 조기 감지
5 데이터 마스킹 및 익명화	테스트 및 운영 환경에서 중요/민감 데이터 마스킹
6 데이터 변경 이력 추적 및 복구	데이터 변경 이력 보관 및 추적, 필요시 신속한 데이터 복구
7 분리된 테스트 환경 사용	운영과 분리된 Sandbox 환경에서 테스트 수행
8 정기적인 보안 테스트 수행	주기적인 취약점 및 모의 테스트 점검, 모델 무결성 위한 안전성과 윤리적 검증

AI 혁신과 함께하는 데이터 보안 8가지 실행 전략

1 데이터 범위 파악 및 분류	데이터 감사 수행, 중요/민감 정보 식별, 분류 기준 설정
2 데이터 암호화	전송 및 저장중 데이터 암호화, 키 라이프사이클 수행 및 접근 제한
3 역할 기반 접근 제어	AI Agent포함해서 사용자별 접근 권한 설정, 정기적인 접근 감사 로그 검토
4 이상 징후 모니터링	AI 프로세스에 대한 실시간 모니터링, 이상 행동 조기 감지
5 데이터 마스킹 및 익명화	테스트 및 운영 환경에서 중요/민감 데이터 마스킹
6 데이터 변경 이력 추적 및 복구	데이터 변경 이력 보관 및 추적, 필요시 신속한 데이터 복구
7 분리된 테스트 환경 사용	운영과 분리된 Sandbox 환경에서 테스트 수행
8 정기적인 보안 테스트 수행	주기적인 취약점 및 모의 테스트 점검, 모델 무결성 위한 안전성과 윤리적 검증

Salesforce 보안 기능 및 솔루션

- Platform - Data Classification
- Data Cloud - Governance (beta)
- Agentforce Einstein Trust Layer
- Shield - Event Monitoring
- Shield - Platform Encryption
- Shield - Field Audit Trail
- Shield - Data Detect
- Security Center
- Data Mask & Seeding
- Backup & Recover
- Sandbox

보안 백서

Contents

http://sfdc.co/datasecurityBP

Thank you