



Agentforce World Tour Korea



Forward looking statement

salesforce

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.

salesforce

AI 혁신과 데이터 보안의 균형을 확보하는 8가지 실행전략





이동승

Platform & Security 솔루션 엔지니어
Salesforce Korea





THANK
YOU



국내 기업의 침해사고 유형 및 위협 요인



국내 기업의 침해사고 경험 유형

랜섬웨어 감염



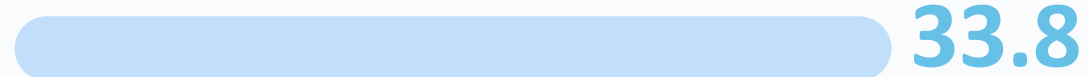
51.0

외부로부터 침투한 비인가 접근(해킹)



46.6

바이러스, 웜, 트로이잔, APT 공격



33.8

DoS, DDoS



11.3

1.4 인가받지 않은 인원의 불법적인 사내 침입 또는 침입 시도

0.8 기타

Base : 침해사고 경험한 기업체, 단위 %, 복수응답

우려하는 정보보호 위협 요인

고객 개인정보 유출 위험

인터넷을 통한
사내 전산 시스템 침해사고 위험

외부 공격에 의한 저장된
데이터 자산의 손·망실

인적 요인에 의한 정보유출 위험

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

증가하는 위협으로 인해 데이터와 신뢰가 위험에 노출

salesforce



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 미흡
은 막대한 손실을 초래함



200억원 (\$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 초래할것
이라고 생각하는 IT 리더 비율

Top Generative AI Statistics for 2025, Salesforce



증가하는 위협으로 인해 데이터와 신뢰가 위험에 노출

salesforce

AI 시대의 보안 위협

데이터 유출

악의적인 프롬프트 인젝션

AI 생성 콘텐츠의 조작/오남용/편향/유해성

자동화된 공격확대(예: AI기반 피싱, 딥페이크)

기업은 AI 도입 준비가 필요함



71%

생성형 AI가 새로운 보안 위험을 초래할것
이라고 생각하는 IT 리더 비율

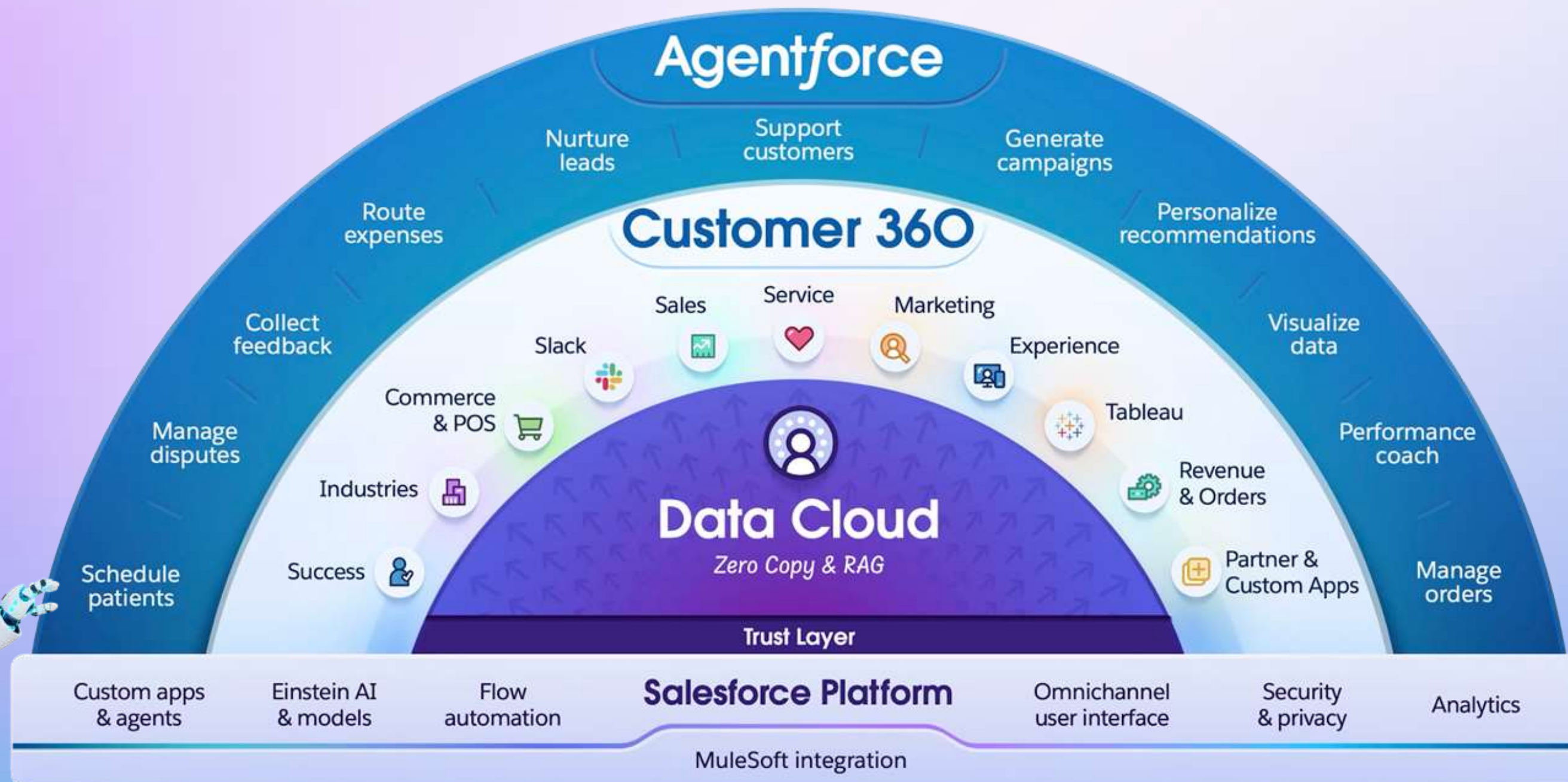
Top Generative AI Statistics for 2025, Salesforce

Agentforce

The digital labor platform

salesforce

Trusted
Easy to deploy
Humans in the loop
Zero hold time
Deeply unified
Open





Salesforce Shared Trust Model



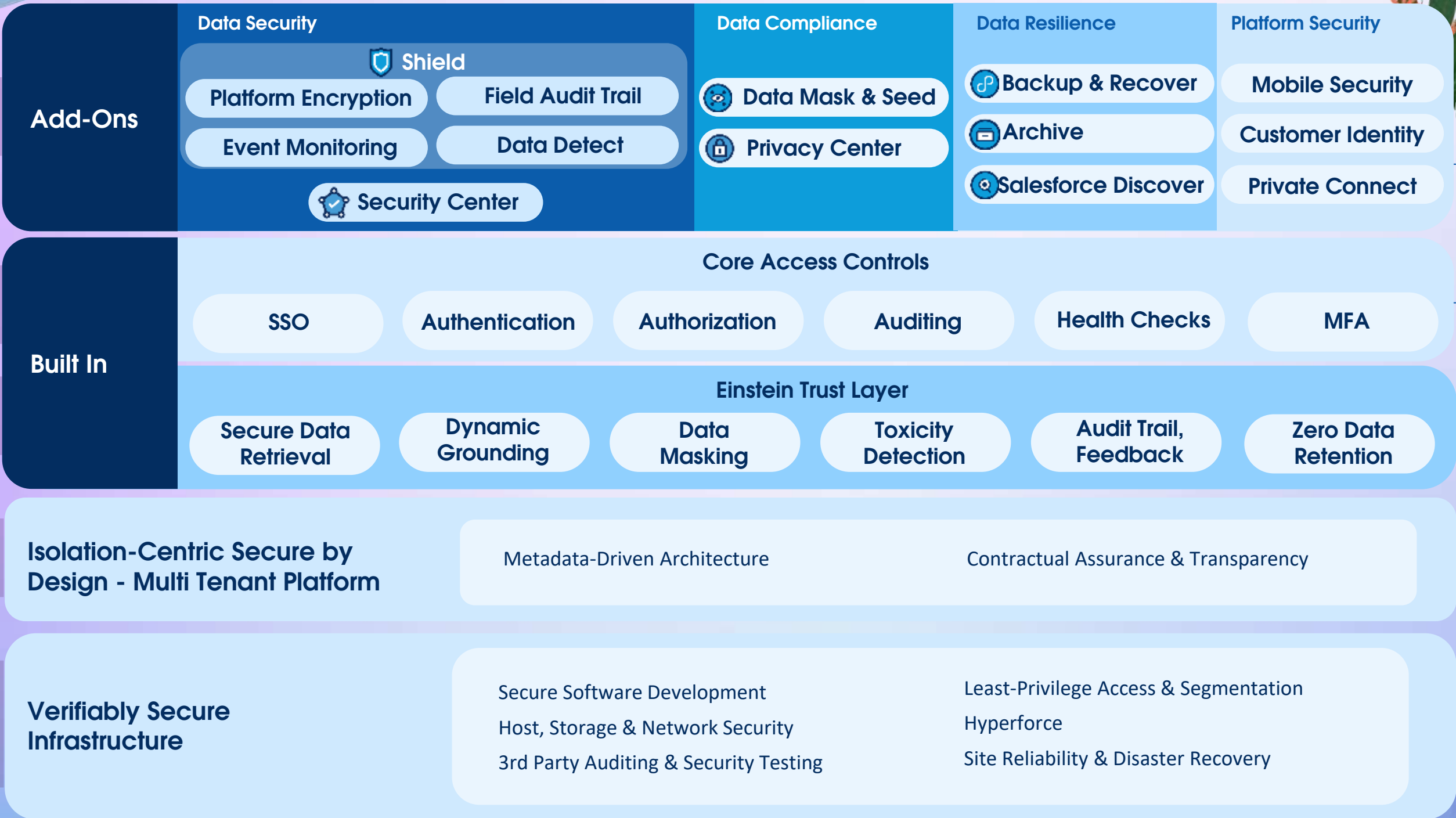
보안 강화 솔루션

보안 통제 기능

AI 보안을 위한 가드레일

메타 데이터 기반 아키텍처

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



Customer Controlled

Salesforce Controlled

AI 혁신과 함께하는 데이터 보안 8가지 실행 전략

salesforce

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

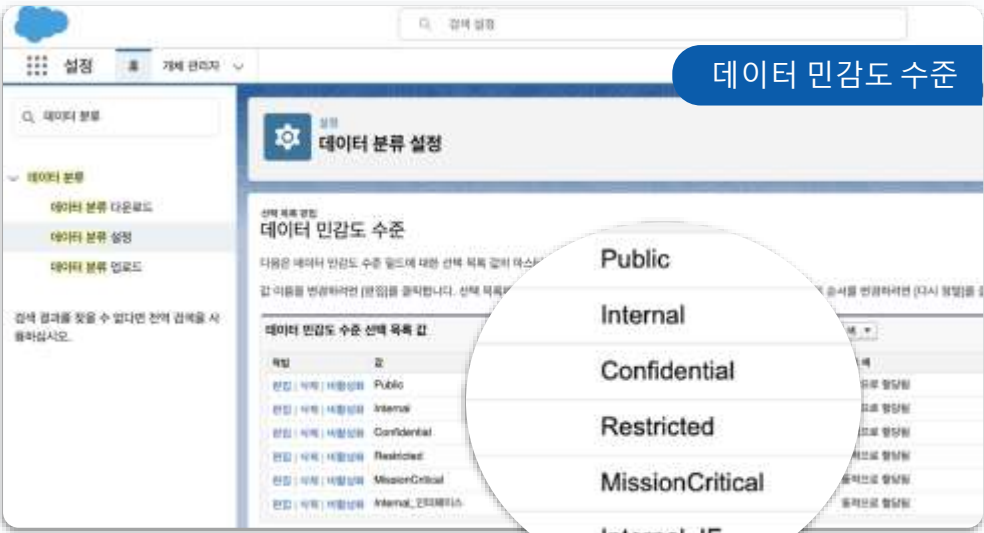


1 데이터 범위 파악 및 분류

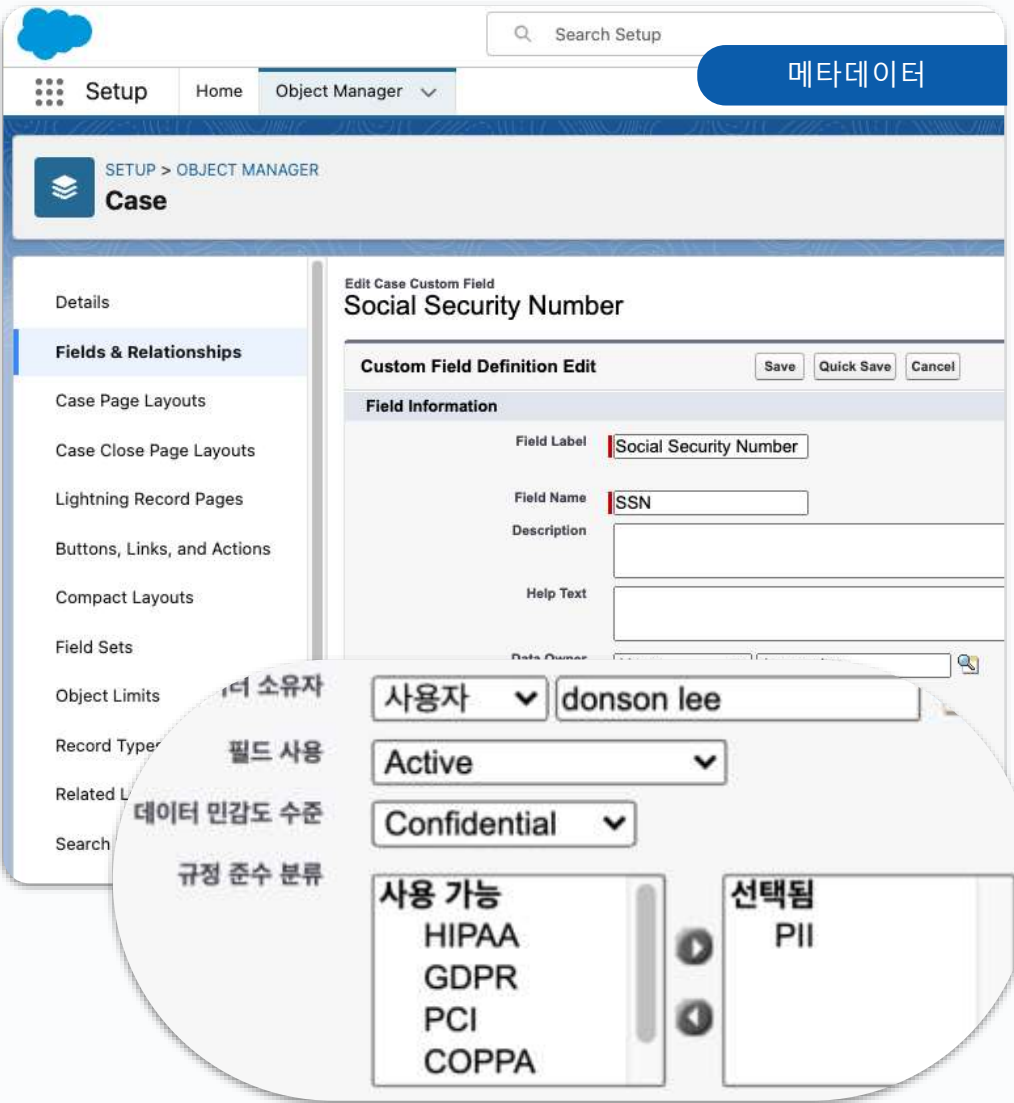
- 2
- 3
- 4
- 5
- 6
- 7
- 8

Salesforce 플랫폼의 메타데이터를 활용하여 중요 데이터 식별 및 분류 체계 확립

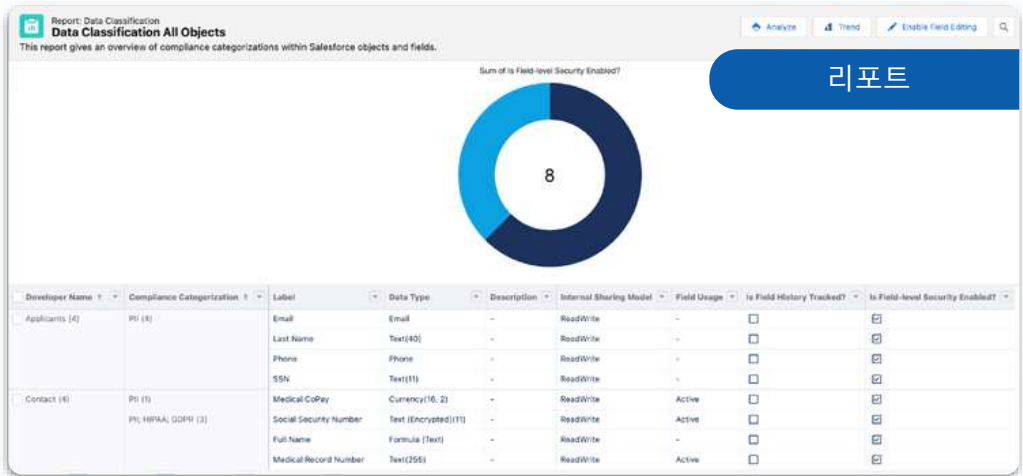
데이터 분류 설정



필드별 식별



모니터링



NAME	DEVELOPER NAME	DATA TYPE	COMPLIANCE	FILL RATE	SENSITIVITY
Email	Email	Email	High	95.83% (46/48)	High
Email Bounced Date	EmailBouncedDate	Date/Time	Low	0.00% (0/48)	Low
Email Bounced Reason	EmailBouncedReason	Text(255)	Low	0.00% (0/48)	Low
Mobile Opt Out	etAae5__HasOptedOu...	Checkbox	Low	100.00% (48/48)	Low
Mobile Country Code	etAae5__Mobile_Coun...	Picklist	Low	100.00% (48/48)	Low
Fax	Fax	Fax	High	29.17% (14/48)	High
Affiliations	FinServ__Affiliations_c	Text Area(255)	Low	0.00% (0/48)	Low
Age	FinServ__Age__c	Formula (Number)	High	89.58% (43/48)	High
Age As Text	FinServ__AgeAsText__c	Formula (Text)	High	89.58% (43/48)	High
Annual Income	FinServ__AnnualInco...	Currency(18, 0)	High	16.67% (8/48)	High
Billing Address	FinServ__BillingAddres...	Formula (Text)	High	85.42% (41/48)	High
Citizenship	FinServ__Citizenship__c	Text(50)	High	0.00% (0/48)	High

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

Security Center Extension

Security Insights

Data Classification

Who Sees What Explorer

Settings

Time Machine

Objects

contact

All Objects

Account Contact Relationship

Contact

Contact-Contact Relationship

Contact Employment

Contact Point Address

Contact Point Consent

Contact Point Email

Contact Point Phone

Contact Point Type Consent

Contact Quote Junction

Contact Regulatory Action

Contact Request

Contact Fields (146 of 14,286)

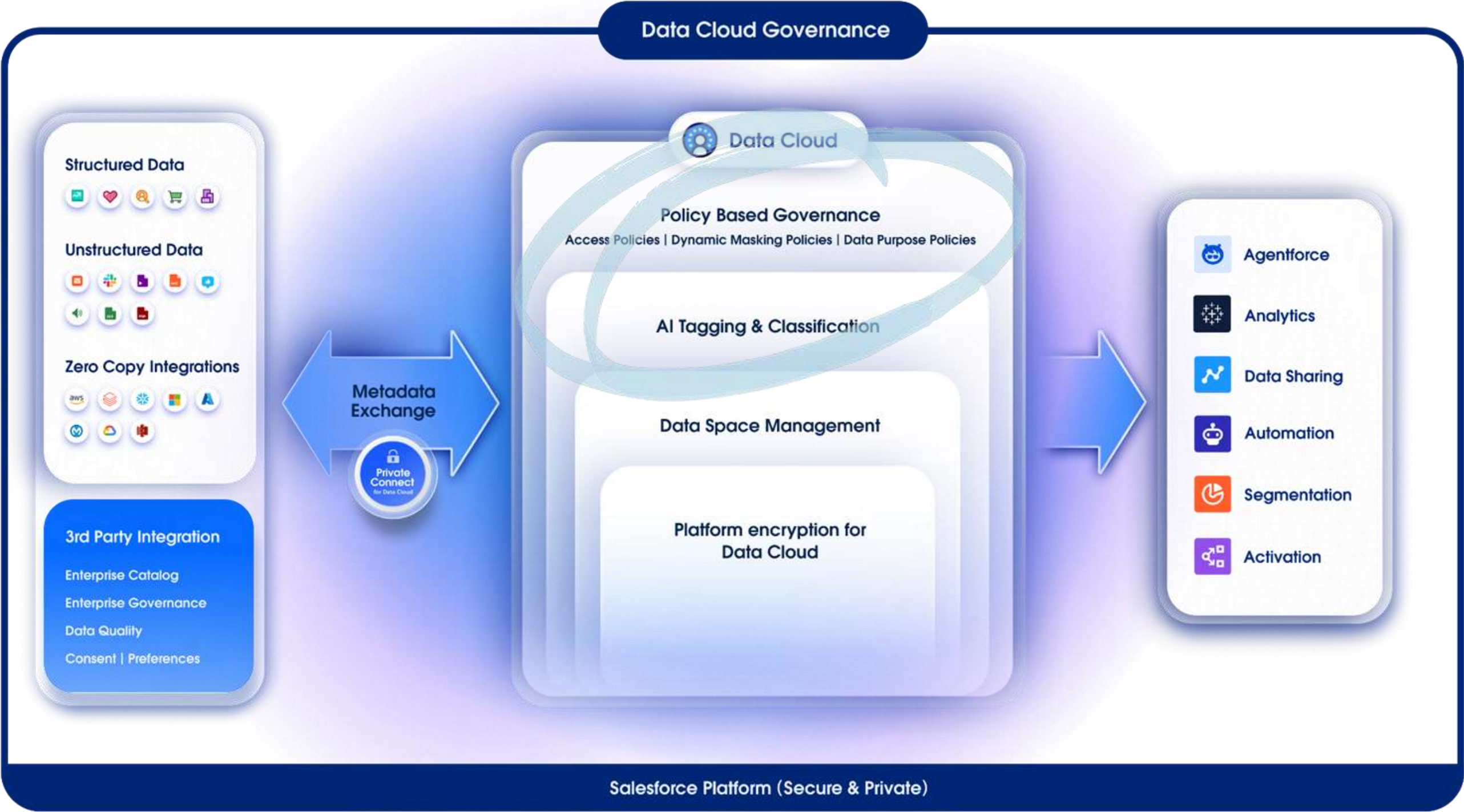
Selected Fields: 0

	NAME	DEVELOPER NAME	DATA TYPE	COMPLIANCE	FILL RATE	SENSITIVITY
	NAME	Developer Name	Text			
	Email	Email	Email	PII	95.83% (46/48)	High
	Email Bounced Date	EmailBouncedDate	Date/Time		0.00% (0/48)	Low
	Email Bounced Reason	EmailBouncedReason	Text(255)		0.00% (0/48)	Low
	Mobile Opt Out	et4ae5__HasOptedOu...	Checkbox		100.00% (48/48)	Low
	Mobile Country Code	et4ae5__Mobile_Coun...	Picklist		100.00% (48/48)	Low
	Fax	Fax	Fax	PII	29.17% (14/48)	High
	Affiliations	FinServ__Affiliations__c	Text Area(255)		0.00% (0/48)	Low
	Age	FinServ__Age__c	Formula (Number)	PII	89.58% (43/48)	High
	Age As Text	FinServ__AgeAsText__c	Formula (Text)	PII	89.58% (43/48)	High
	Annual Income	FinServ__AnnualInco...	Currency(18, 0)	PII	16.67% (8/48)	High
	Billing Address	FinServ__BillingAddres...	Formula (Text)	PII	85.42% (41/48)	High
	Citizenship	FinServ__Citizenship__c	Text(50)	PII	0.00% (0/48)	High

1 데이터 범위 파악 및 분류

- 2
- 3
- 4
- 5
- 6
- 7
- 8

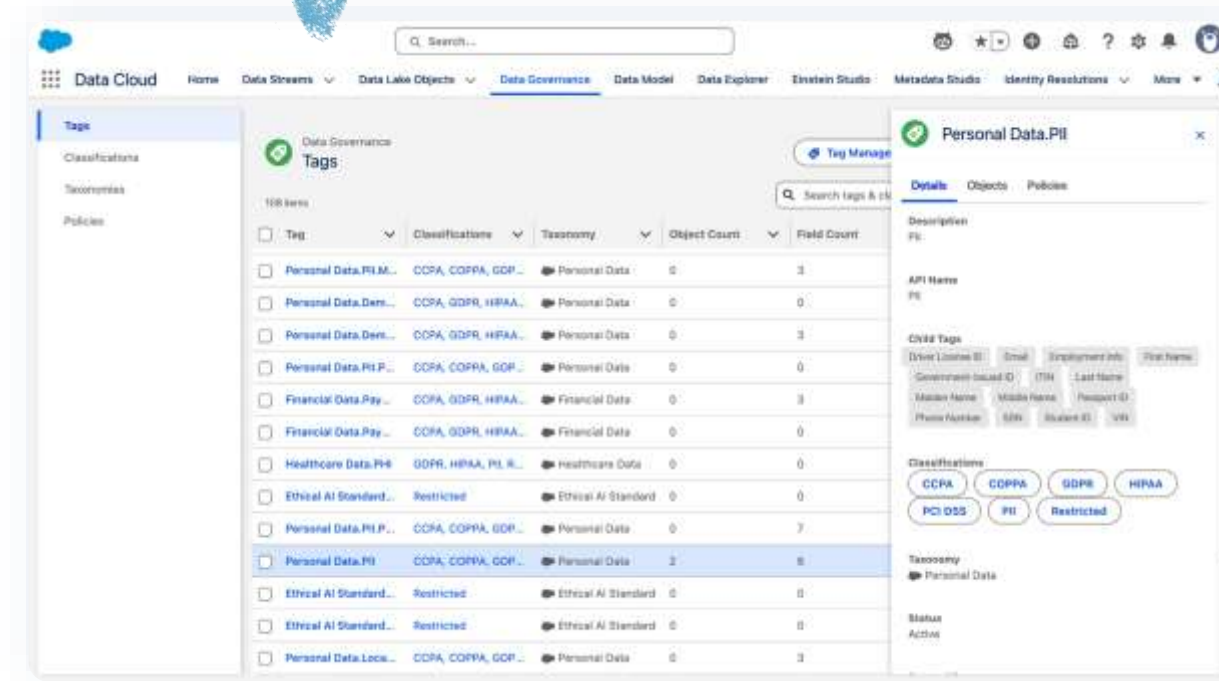
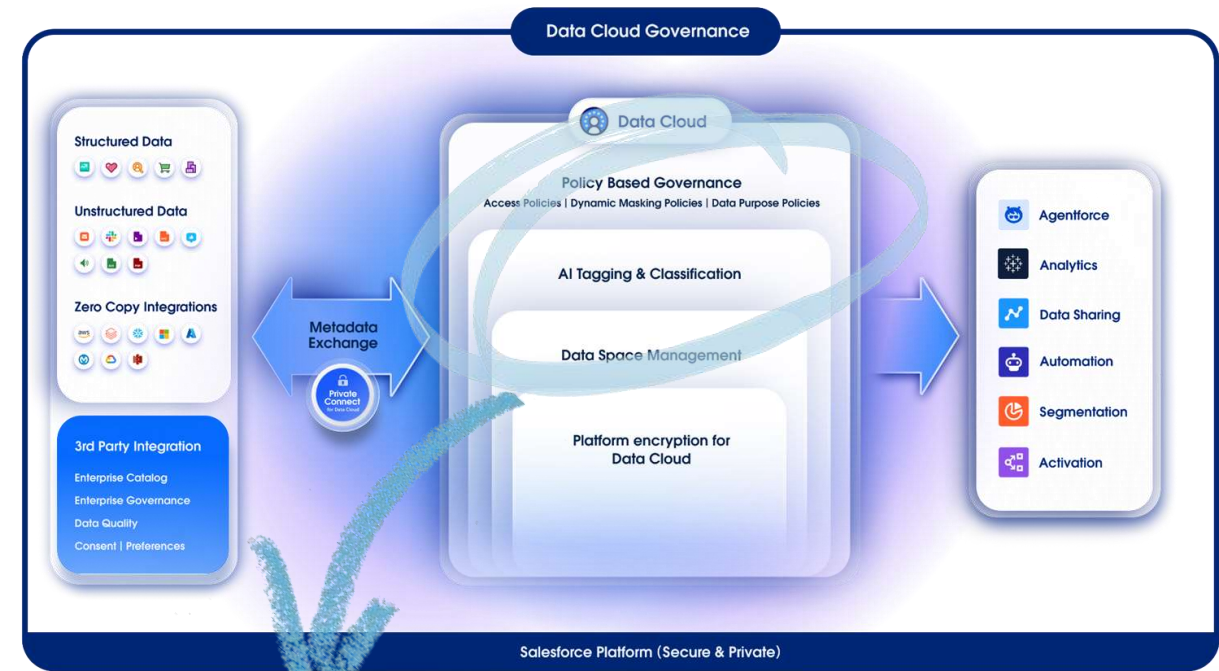
Agentforce 기반인 Data Cloud 경우, 태그 및 분류에 의한 데이터 거버넌스 확립



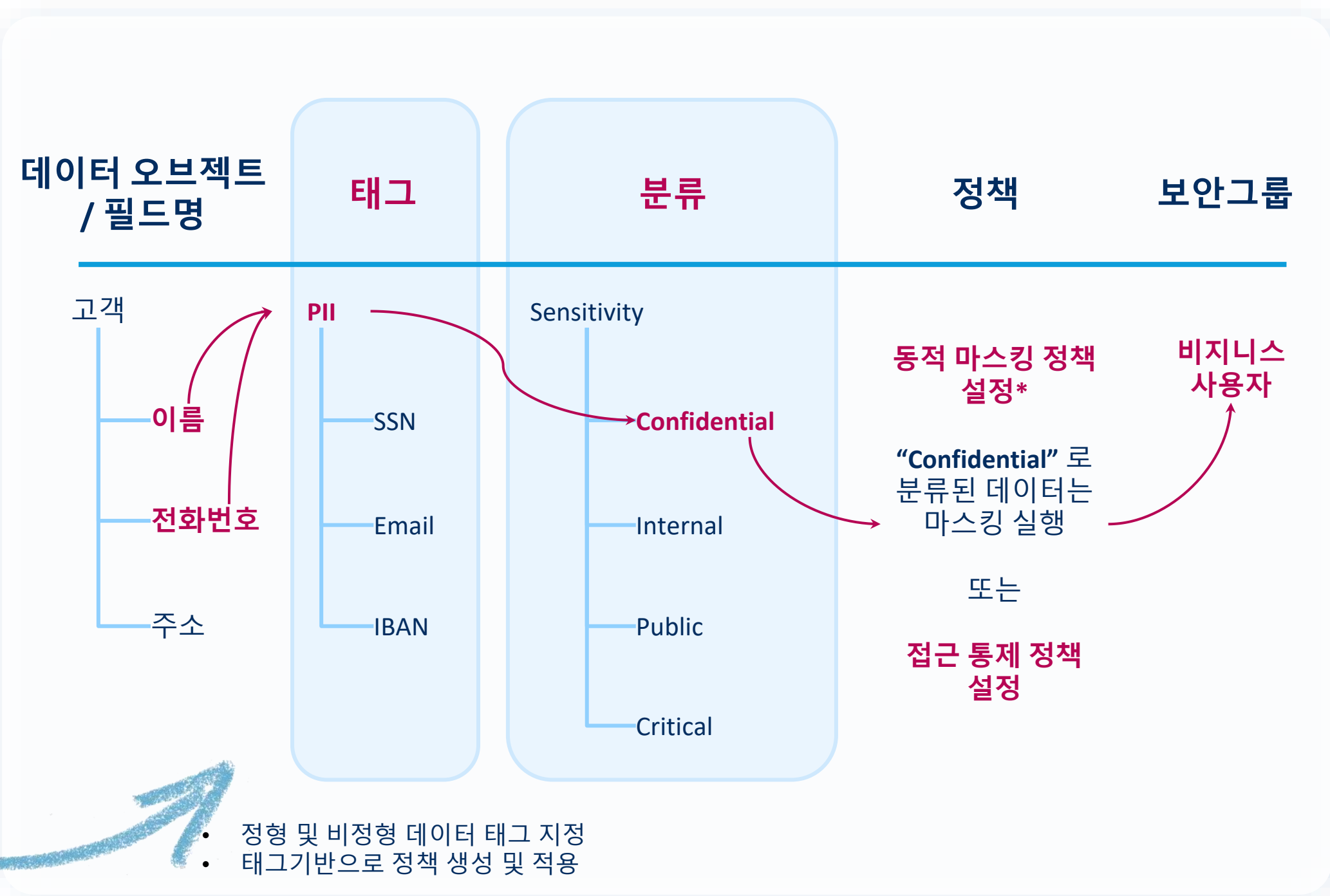
1 데이터 범위 파악 및 분류

- 2
- 3
- 4
- 5
- 6
- 7
- 8

Agentforce 기반인 Data Cloud 경우, 태그 및 분류에 의한 데이터 거버넌스 확립



AI Tagging & Classification



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



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
- 확장 필드
- 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

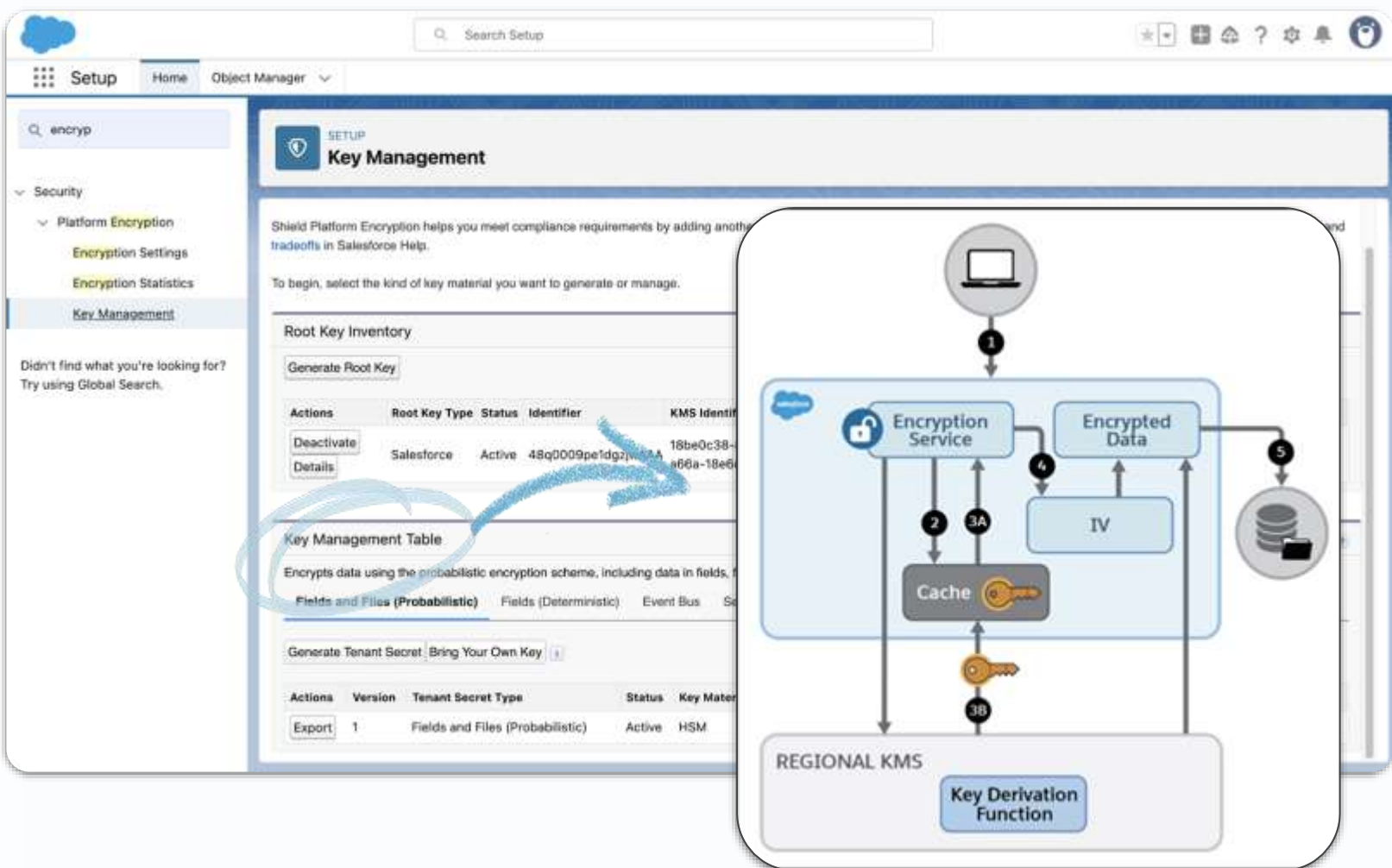
볼륨 암호화 또는 DB SAN 암호화

기본 적용됨

기본 적용됨

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

데이터 암호화 키 관리



The screenshot shows the Salesforce Setup page for Key Management. It includes sections for Root Key Inventory, Key Management Table, and Tenant Secret. A diagram on the right illustrates the key lifecycle: 1. Key generation/management, 2. Key storage in Cache, 3A. Key derivation from REGIONAL KMS, 4. Encryption of data using the key, 5. Encrypted data storage. The diagram also shows the flow from Encrypted Data back to the Cache and then to the REGIONAL KMS via a Key Derivation Function.

- 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

Shield Extension

Platform Encryption Analyzer

History Retention Policy Manager

Field History Explorer

Settings

Status

Complete

Execution #

8

Analyzed On

5/2/2025, 5:00:21 PM

Analyzed By

Admin User [Scheduled]

Analyze Again...

> Time Machine

All Clear

51

Encrypted by Shield

14

Blocked By Configuration

8

Blocked by Platform

617

Total Fields

9,932

Fields Excluded

1

Fields Selected

690

Objects

Search Objects

Fields (9,932)

Search Fields

All Objects

* Prompt Search Term

AB Test

Account

Account-Account Relationship

Account Brand

Account Contact Relationship

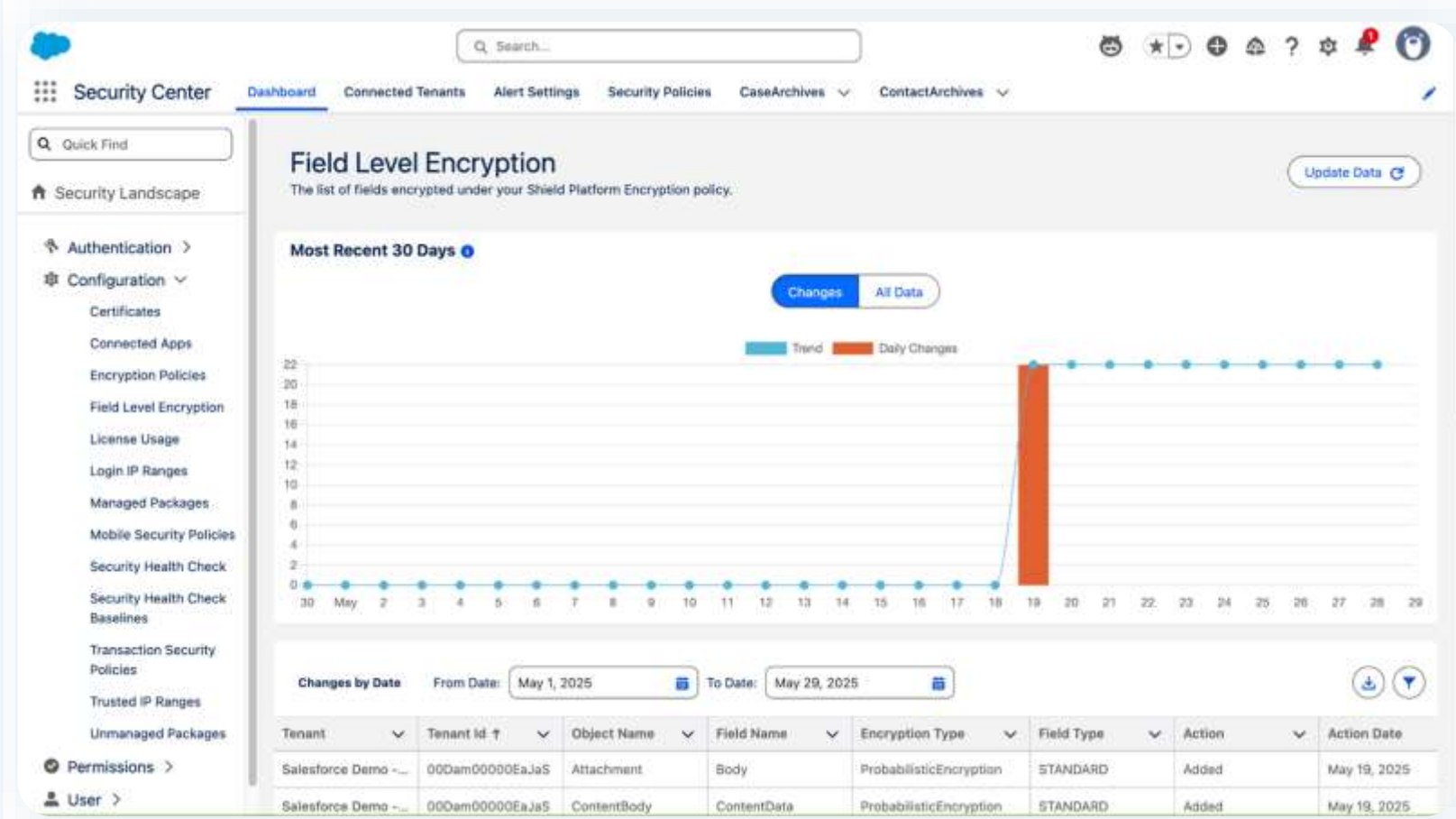
Account Pricing

Account Regulatory Action

	OBJECT NAME	NAME	DEVELOPER NAME	DATA TYPE	COMPLIANCE	FILL RATE	SENSITIVITY	RESULT
☐	Account	Account Name	Name	Name	PI	100.00% (53/53)	PI	-
☒	Account	Account Number	AccountNumber	Text(40)	PI	0.00% (0/53)	PI	×
☒	Account	Account Site	Site	Text(80)		0.00% (0/53)	PI	✓
☒	Account	Account Source	AccountSource	Picklist		0.00% (0/53)	PI	×
☒	Account	Active	vlocity_ins__Act...	Picklist		73.58% (39/53)	PI	×
☒	Account	Active	vlocity_ins__IsA...	Checkbox		100.00% (53/53)	PI	×
☐	Account	Affiliations	FinServ__Affiliati...	Text Area(255)		0.00% (0/53)	PI	-
☒	Account	Age	FinServ__Age_...	Formula (Number)	PI	75.47% (40/53)	PI	×

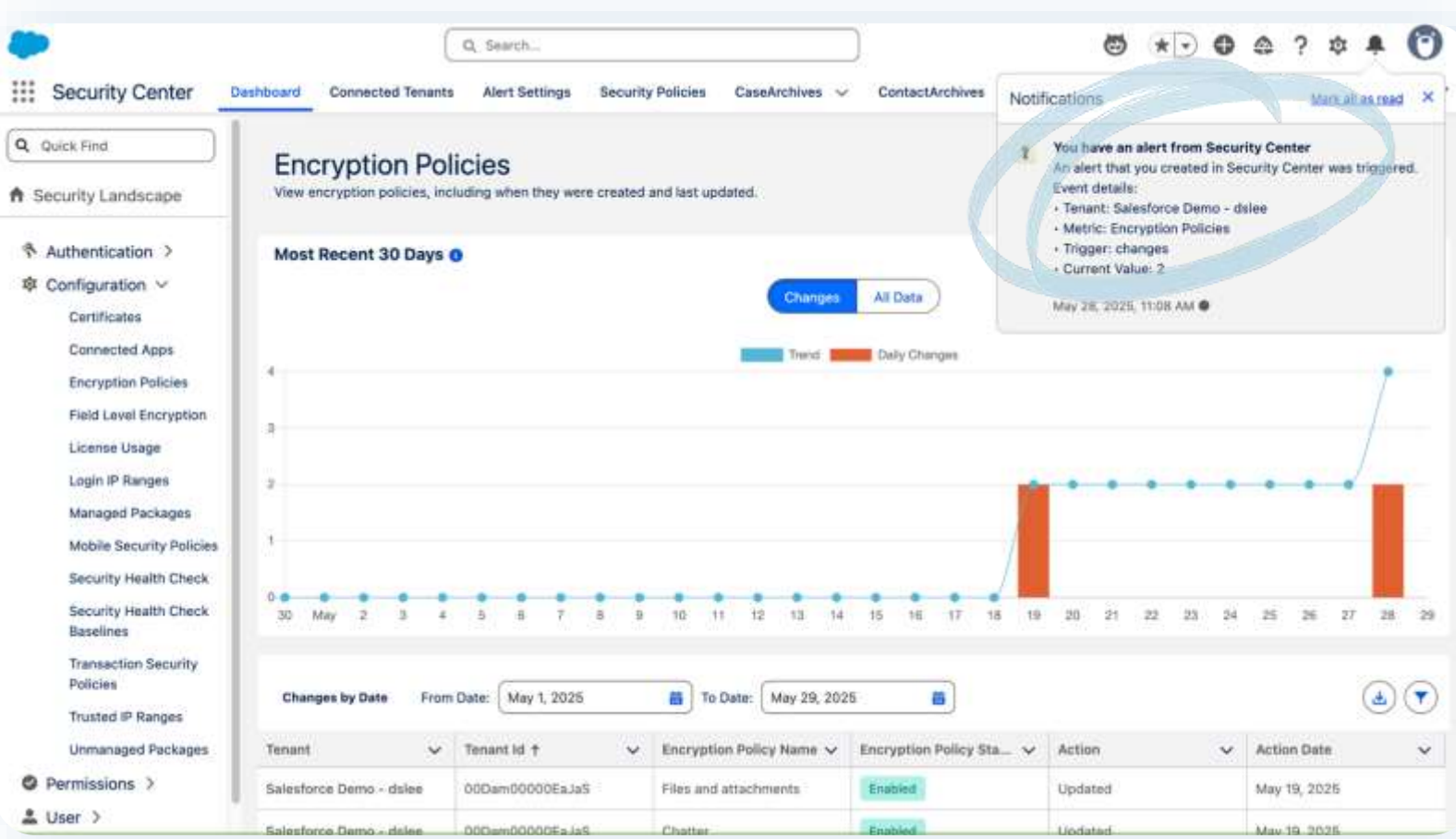
Security Center 솔루션으로 암호화 정책 및 암호화 필드 변경 추적 모니터링

데이터 필드 암호화 변경 추적



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

암호화 정책 변경 추적



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

1

2

3 역할 기반 접근 제어

4

5

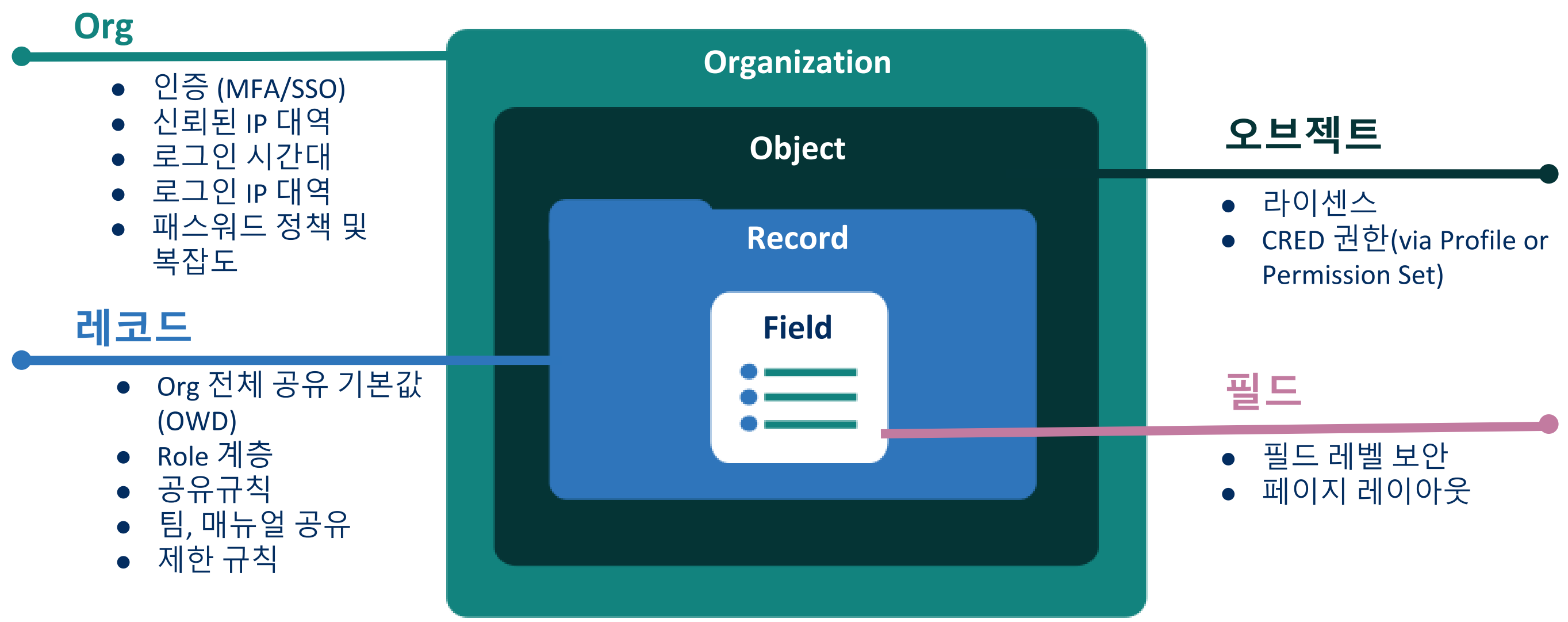
6

7

8



메뉴/데이터에 대한 세분화된 접근 권한기반 통제 실행 및 모니터링



1

2

3 역할 기반 접근 제어

4

5

6

7

8



AppExchange 앱, Salesforce Security Center 등으로 권한 모니터링

권한 모니터링

The screenshot shows the 'User Access & Permissions' tool in Salesforce. The top section, 'Users with Modify All Data permission', lists users with this permission. Below it, the 'User Access Summary' section provides a detailed view of permissions for a selected user, including a table of object permissions.

Full Name	Username	Alias	Profile	Active	Last Login
Dongseung Lee	dlee@dslee002.demo	DLee	System Administrator	✓	Aug 1, 2024
Elliot Executive	eeowc@dslee002.demo	Elliot	System Administrator	✓	Apr 21, 2020
Vance Channel	vchannel@dslee002.demo	Vance	*Channels	✓	Apr 6, 2020
Sunny Bot	sbot@dslee002.demo	SunnyBot	System Administrator	✓	
Chronos Bot	chronosbot@dslee002.d...	Chronos	System Administrator	✓	
Rider Bot	rbot@dslee002.demo	RiderBot	System Administrator	✓	
Tracker Bot	tbot@dslee002.demo	Tracker	System Administrator	✓	

Label	Object AP...	Read	Create	Edit	Delete	View All R...	Modify All...	View All FL...
AB Test	et4ae5_abTes...	✓	✓	✓	✓	✗	✗	✗
Account	Account	✓	✓	✓	✓	✗	✗	✗
Account Relat...	AccountRelat...	✓	✓	✓	✓	✗	✗	✗
Additional Doc...	SBQQ_Relate...	✓	✓	✓	✓	✗	✗	✗
Address	Address	✓	✓	✓	✗	✗	✗	✗
Aggregate Link...	et4ae5_Aggre...	✓	✓	✓	✓	✗	✗	✗

Security Center - 권한

The screenshot shows the 'Security Center' dashboard. The 'Permissions' section displays trends for various permissions. A callout box compares the number of users with 'Modify All Data' permission before and after implementation.

Permission	Before	After
Modify All Data Permission	185 USERS	7 USERS

Modify All Data 권한 예시

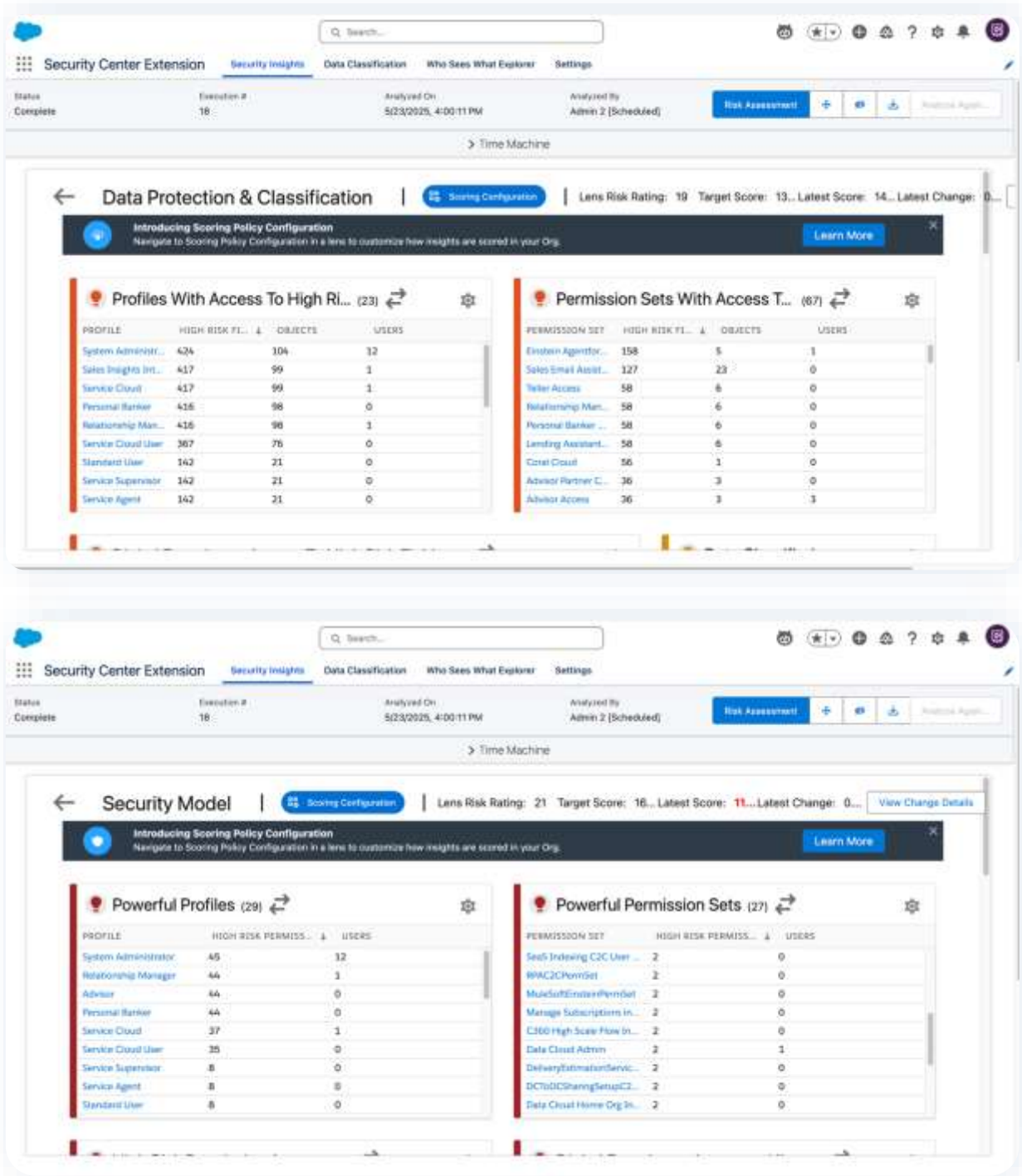
Security Center 사용 이전
과다한 권한 사용자, 보안 정책
일관성 등 가시성 확보 부족

Security Center 사용후
싱글 뷰 가시성 확보

▶ Security Center 데모 동영상 1

▶ Security Center 데모 동영상 2

Security Center의 확장기능인 Security Insight로 리스크 관리



보안 인사이트

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	

데이터 보호 및
분류

접근 제어
(인증)

보안 모델
(권한)

연동

데이터 유출
방지

모니터링

역할 기반 접근 제어

Agentforce 기반인 Data Cloud에 대한 접근 정책 가버넌스 구현

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

오브젝트/필드/레코드
단위의 접근 통제 사용하
여 정책을 일관되게 적용

권한있는 사람 또는 Agent
에게만 올바른 접근 제공

Home

Tags

Classifications

Taxonomies

Policies

Search...

Data Cloud

Home

Data Streams

Data Lake Objects

Data Governance

Data Explorer

Data Model

Search Index

Einstein Studio

Identity Resolutions

Profile Explorer

Calculated Insights

More

Data Governance Policies

20 items • Status: Active

Search Policies

New

Policies that grant all users default access to all objects in the data space can override stricter access control policies.

	Name ↑	Created By	Created Date	Last Modified by	
1	Deny_Account_Info	Alex Gormely	Oct 25, 2024	Alex Gormely	
2	Allow All	Alex Gormely	Oct 29, 2024	Alex Gormely	
3	Deny Payment Details Field	Alex Gormely	Oct 29, 2024	Alex Gormely	
4	DenyFiancialPaymentCardInfo	Alex Gormely	Nov 13, 2024	Alex Gormely	
5	DenyPersonalPII	Alex Gormely	Nov 13, 2024	Alex Gormely	
6	DenyTransactionOfCardHolderAdditional	Alex Gormely	Nov 13, 2024	Alex Gormely	
7	rls_on_index	Alex Gormely	Nov 19, 2024	Alex Gormely	
8	A8_Finance_AllowAll	Gaurav Tewari	Nov 21, 2024	Alex Gormely	
9	A8_Finance_DenyField	Gaurav Tewari	Nov 21, 2024	Gaurav Tewari	
10	RLSONPayments	Alex Gormely	Dec 2, 2024	Alex Gormely	
11	DenyServiceSecured	Arun Iruthayaraj	Dec 6, 2024	Arun Iruthayaraj	
12	DenyServiceEO	Arun Iruthayaraj	Dec 6, 2024	Arun Iruthayaraj	
13	Access O2 Data	Alex Gormely	Jan 3, 2025	Alex Gormely	
14	TM INTL Allow All	Alex Gormely	Jan 3, 2025	Alex Gormely	
15	Access Wembley Data	Alex Gormely	Jan 3, 2025	Alex Gormely	
16	Access THS Data	Alex Gormely	Jan 3, 2025	Alex Gormely	
17	Access Public Data	Alex Gormely	Jan 3, 2025	Alex Gormely	

접근 정책- PII 접근차단
DenyPersonalPII

Field 레벨

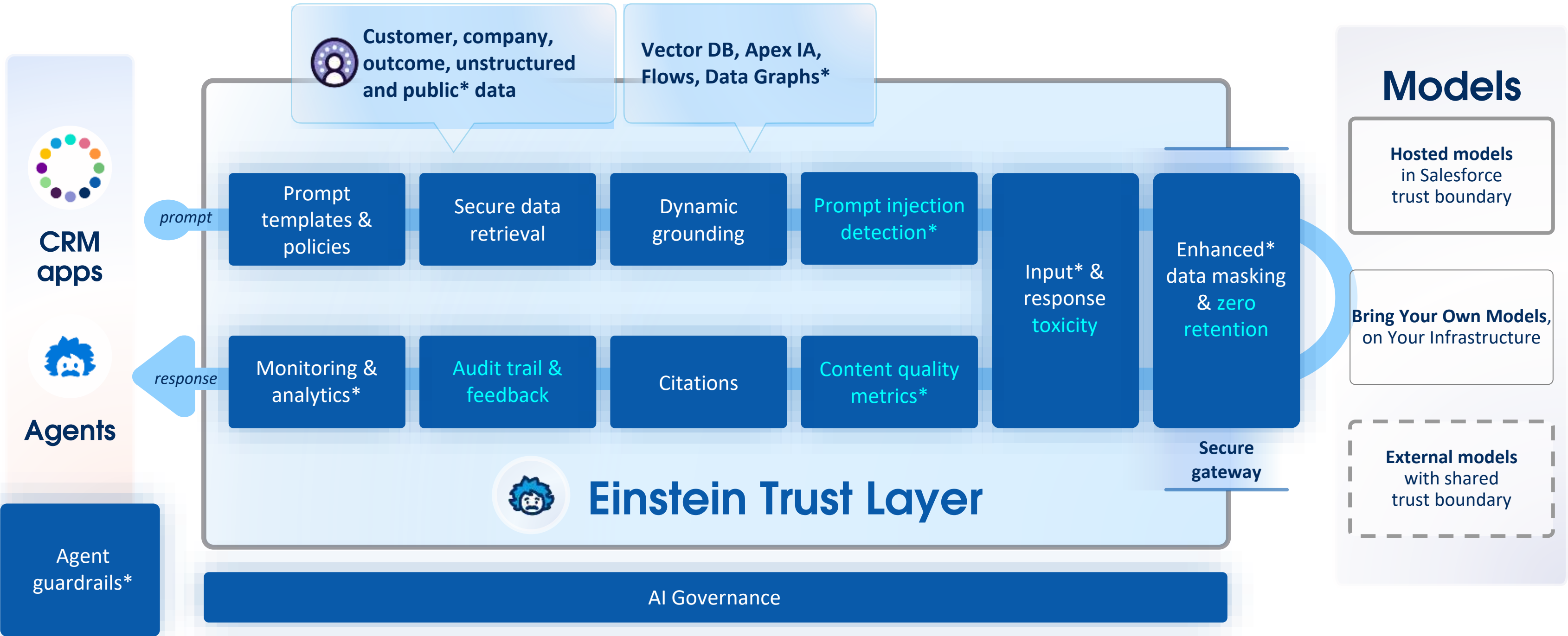
접근 차단
Deny access

태그 = Personal Data.PII

권한 ≠ AccessAllPIIData

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

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



*일부 기능은 로드맵

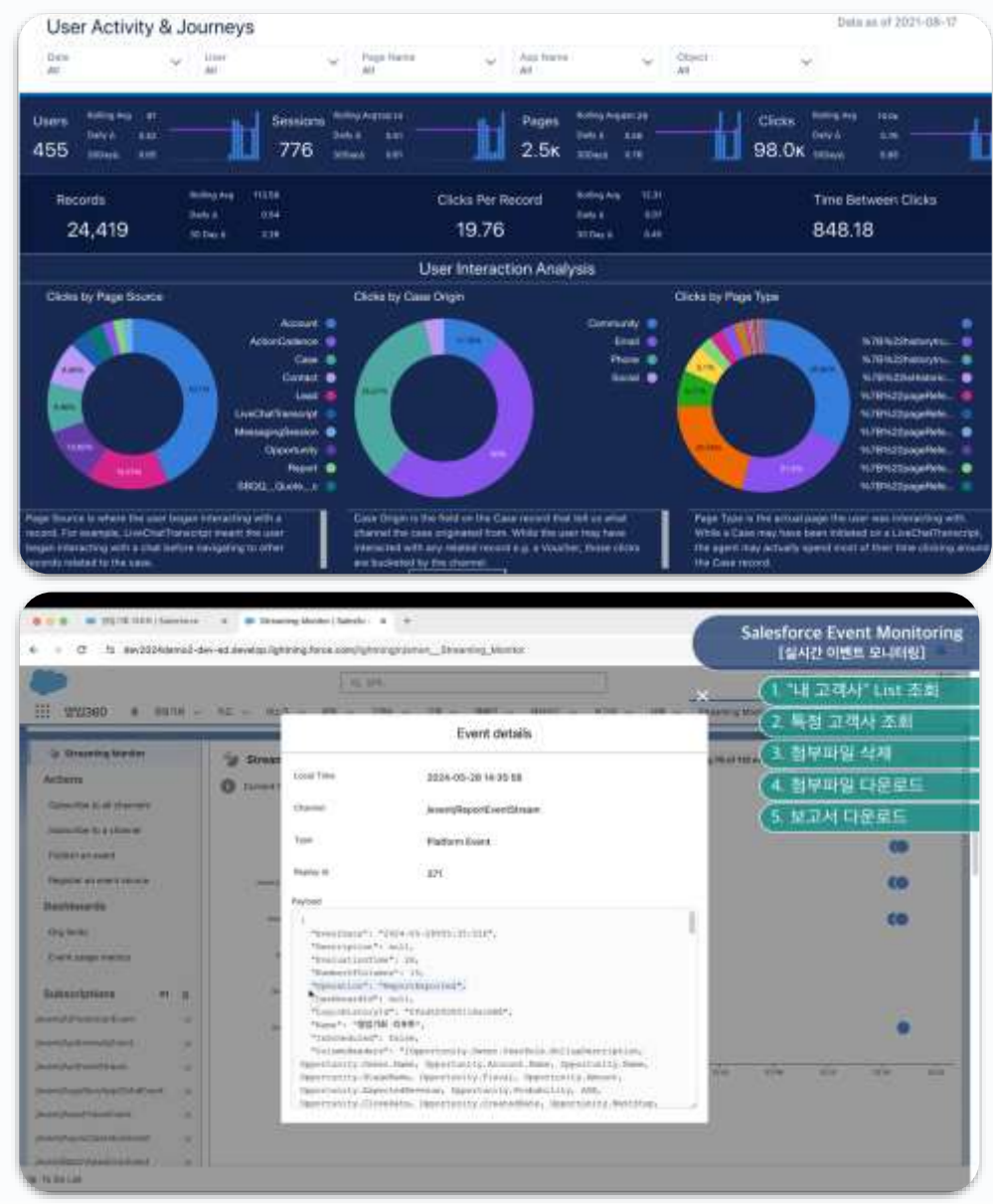
Shield - Event Monitoring 솔루션으로 위협 탐지 및 데이터 유출 방지 수행

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

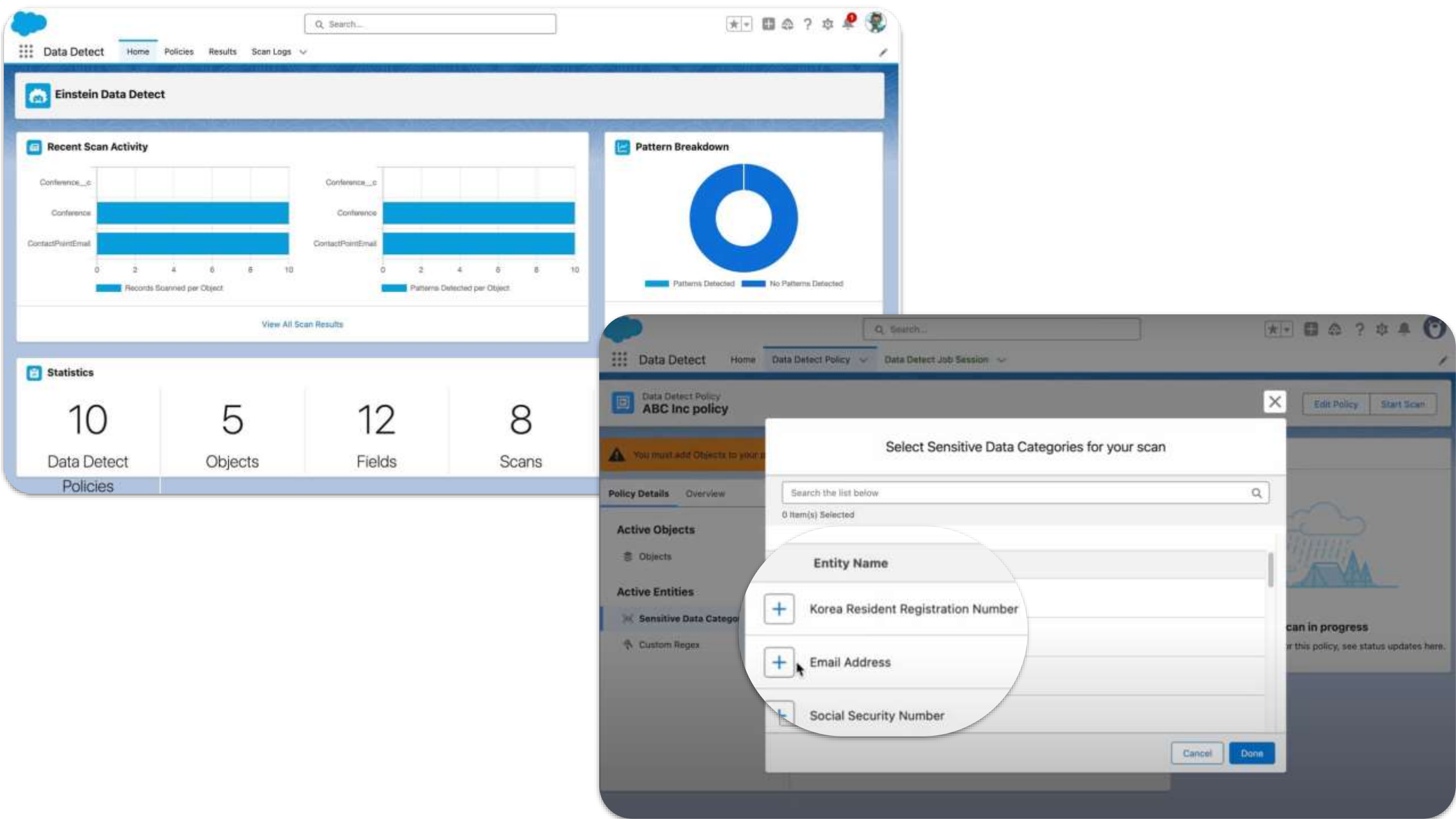


Shield - Data Detect 솔루션으로 패턴 매칭에 의한 민감 데이터 식별

민감한 데이터를 빠르게
찾고 분류

신용카드 번호,
이메일주소와 같은
패턴기반의 민감정보 식별

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



Agentforce를 활용하여, 보안솔루션과 연계하여 위협탐지 및 이상현상 모니터링

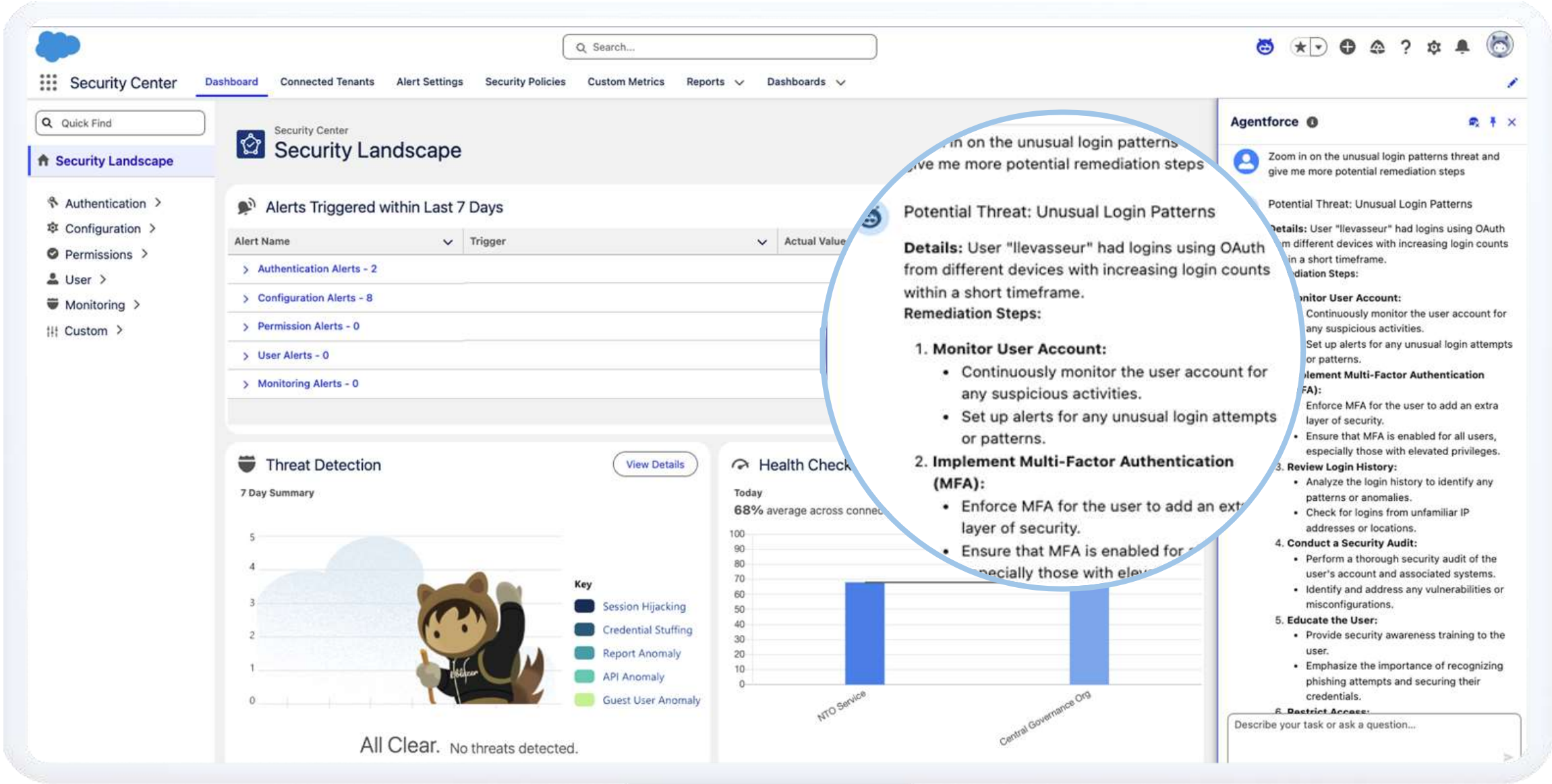
여러 Org의 보안 태세에 대한 강력하고 빠른 인사이트

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 ▼

API Anom

Quarterly Performance

As of Today 4:20 PM



CLOSED \$0 OPEN (>70%) \$0 GOAL --

500k

400k

300k

200k

100k

0

Feb

Mar

Apr

Add the opportunities you're working on, then come back here to view your performance.

Closed

Goal

Closed + Open (>70%)

Today's Events



Today's Tasks



Assistant



Nothing needs your atte

Agentforce



Hi! I'm Einstein,
information, sur
What can I help

Describe your tas

- 1
- 2
- 3
- 4

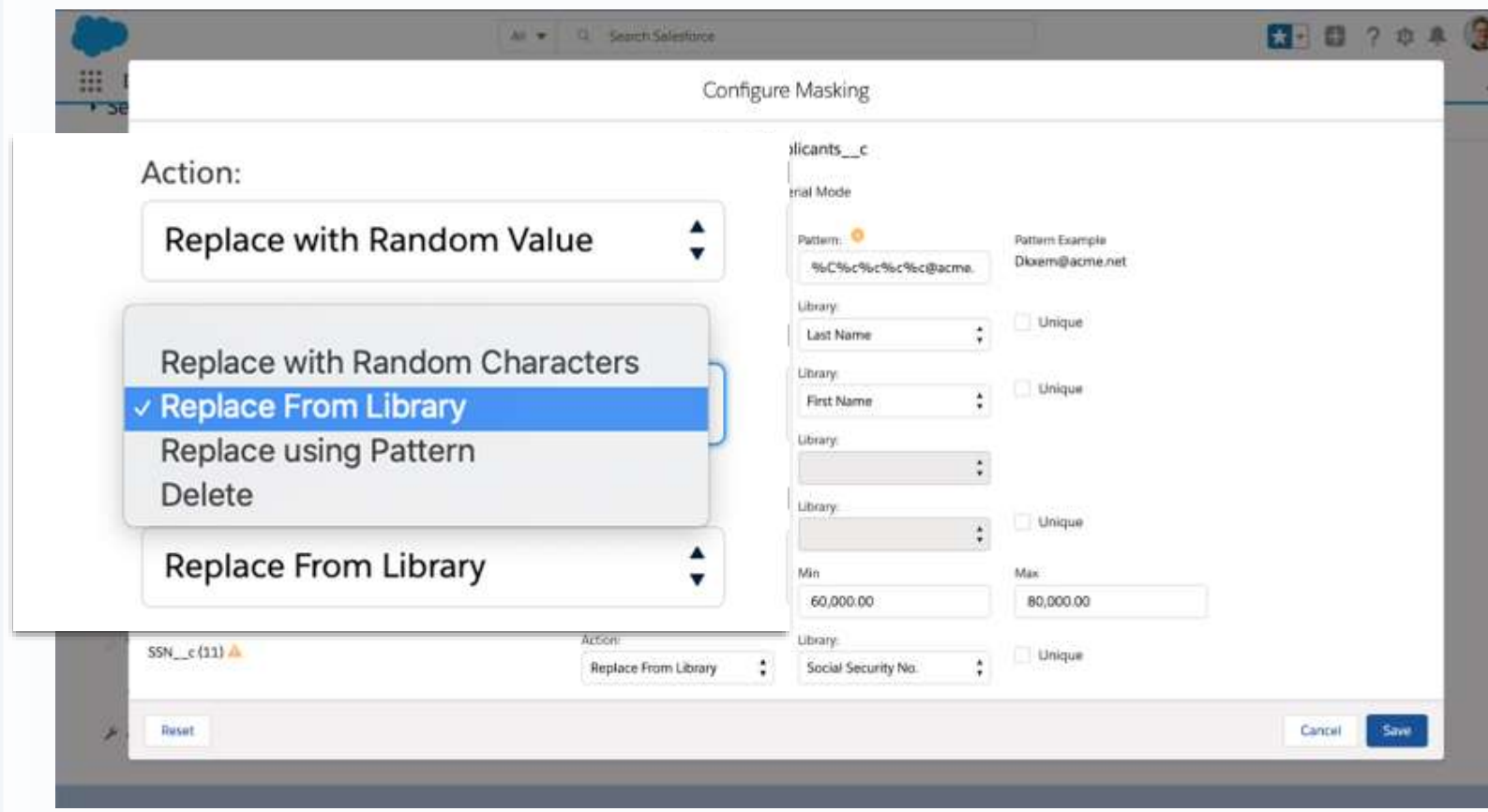
5 데이터 마스킹 및 익명화

- 6
- 7
- 8



Data Mask & Seed 솔루션으로 운영데이터를 Sandbox환경으로 복제시 데이터 마스킹

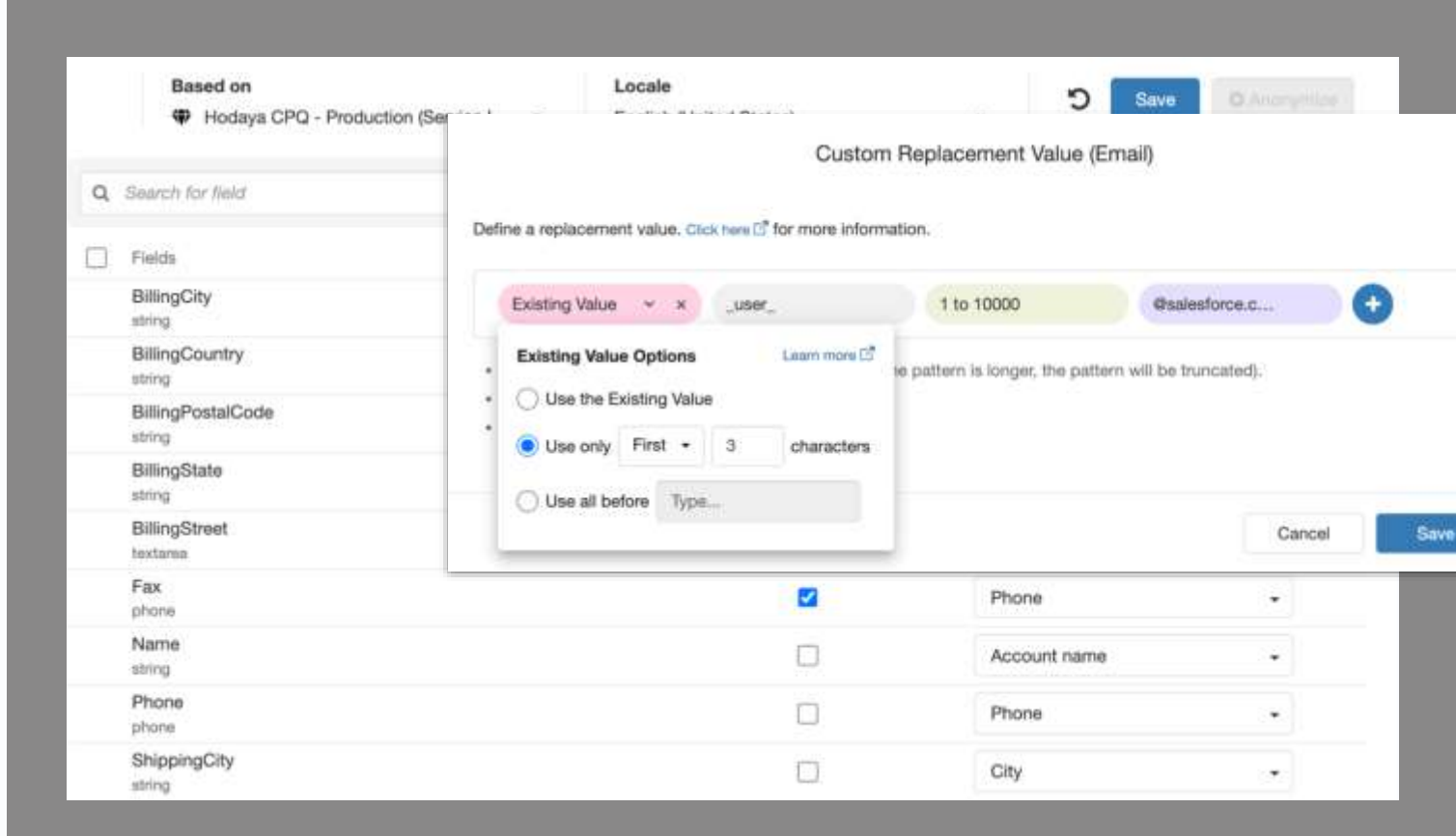
데이터 마스크



라이브러리에서 대체
Balke → Kelsey

패턴 매칭
999-99-9999 → XXX-XX-9999

익명화



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

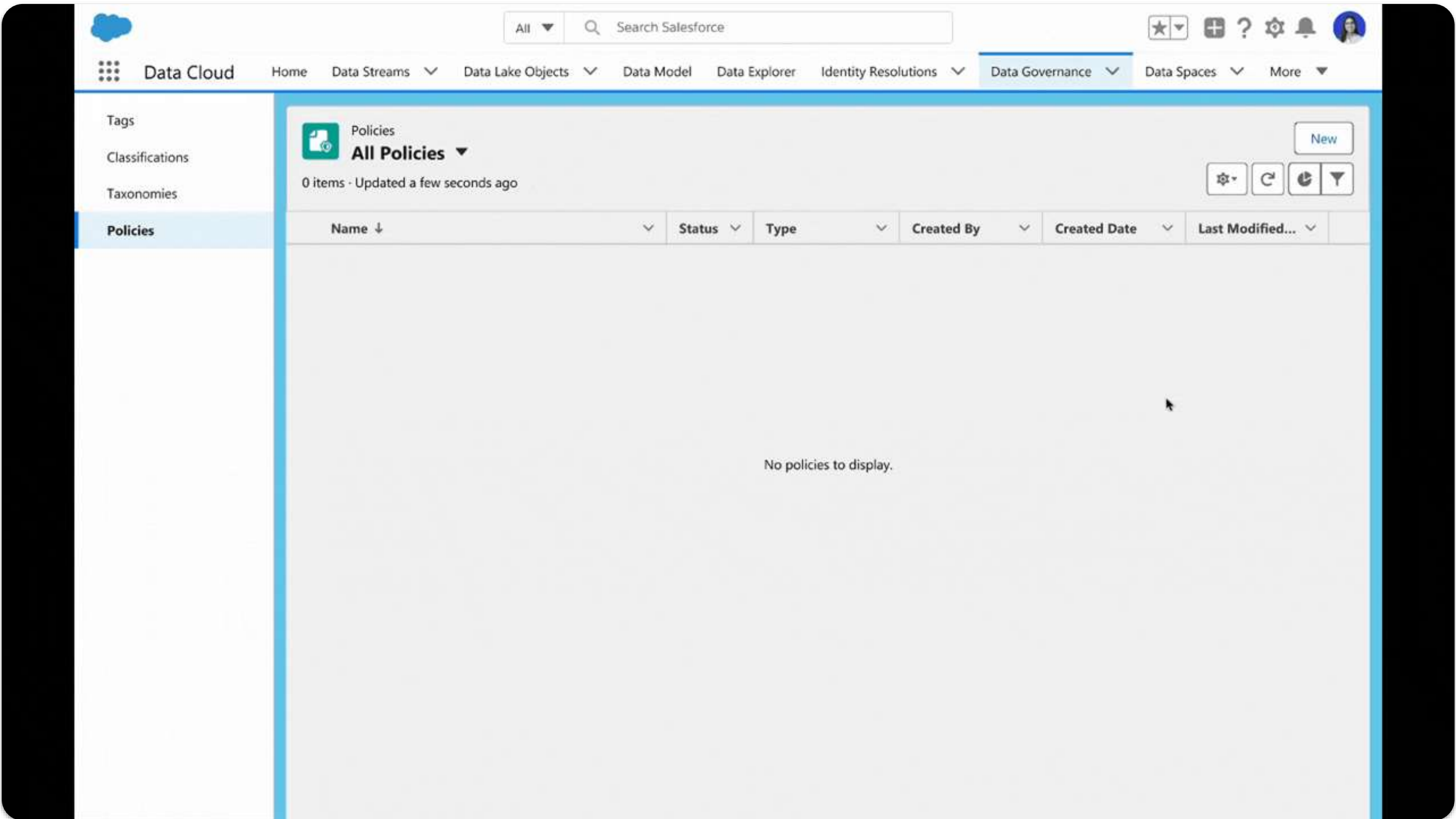
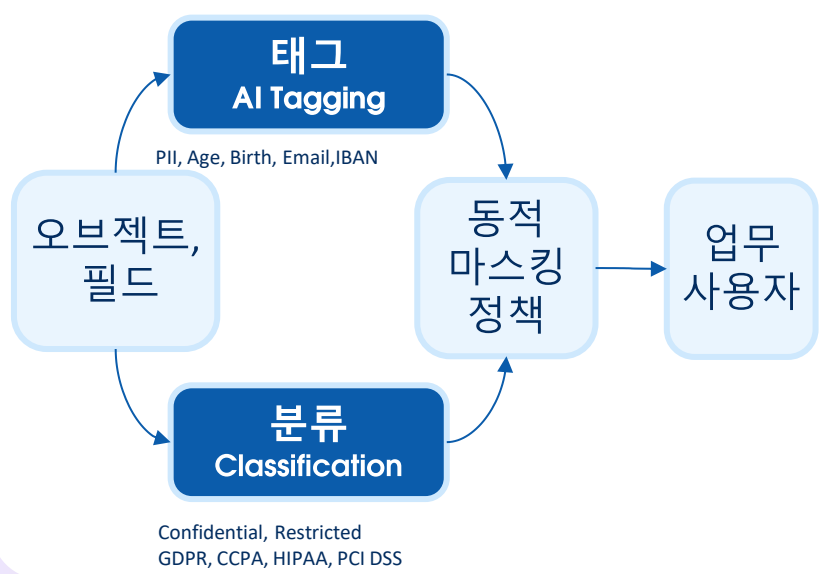
빈값 채우기
_____ → Blake

Dynamic Data Masking Policies

(2025년 하반기 출시, Data Cloud)

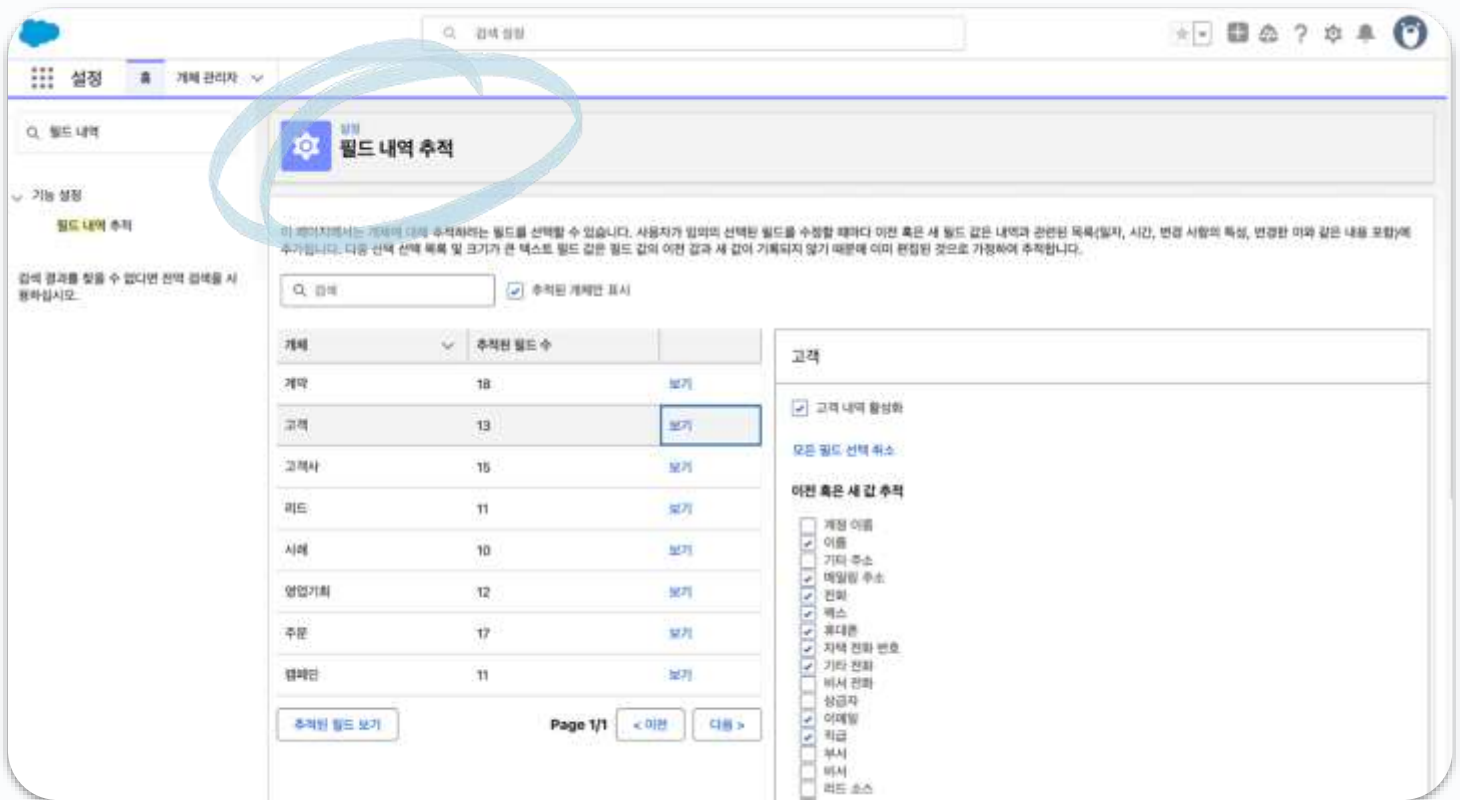
민감한 정보를 동적으로 마스킹하기 위한 정책 생성

기본 데이터 세트를 수정하지 않고 데이터마스킹



데이터 변경 이력에 대한 추적성 유지 및 이력 보관 정책 수립

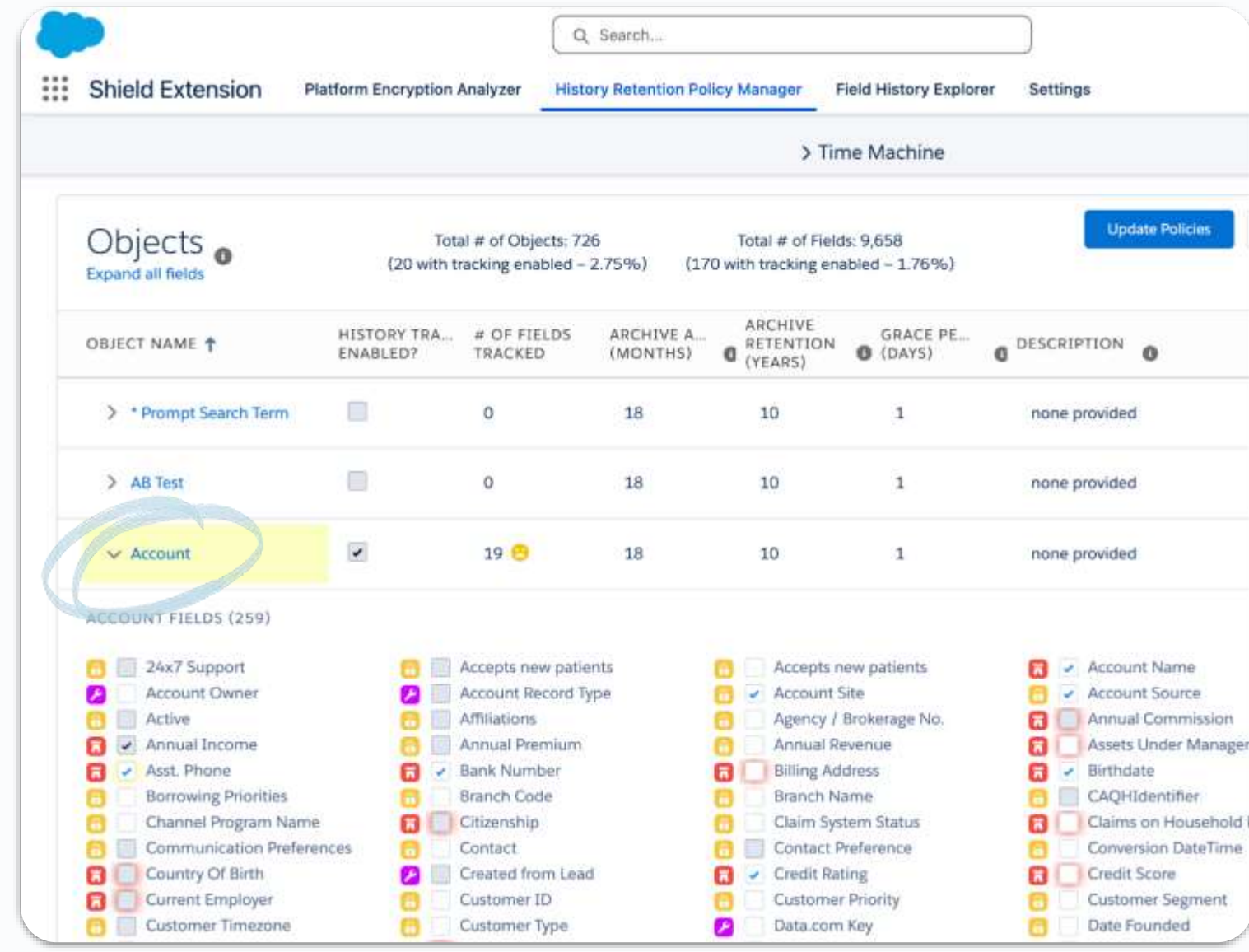
Field History Tracking



Contact 필드 변경 이력

Object당 20개 필드, 6개월 이력 보관, CSV/API 연계

Shield - Field Audit Trail



Object당 60개 필드, 무제한 이력 보관

Salesforce Backup & Recover

실수로 변경된 내용을 복구하기 위한 복구 계획 구현 필요

자동 백업

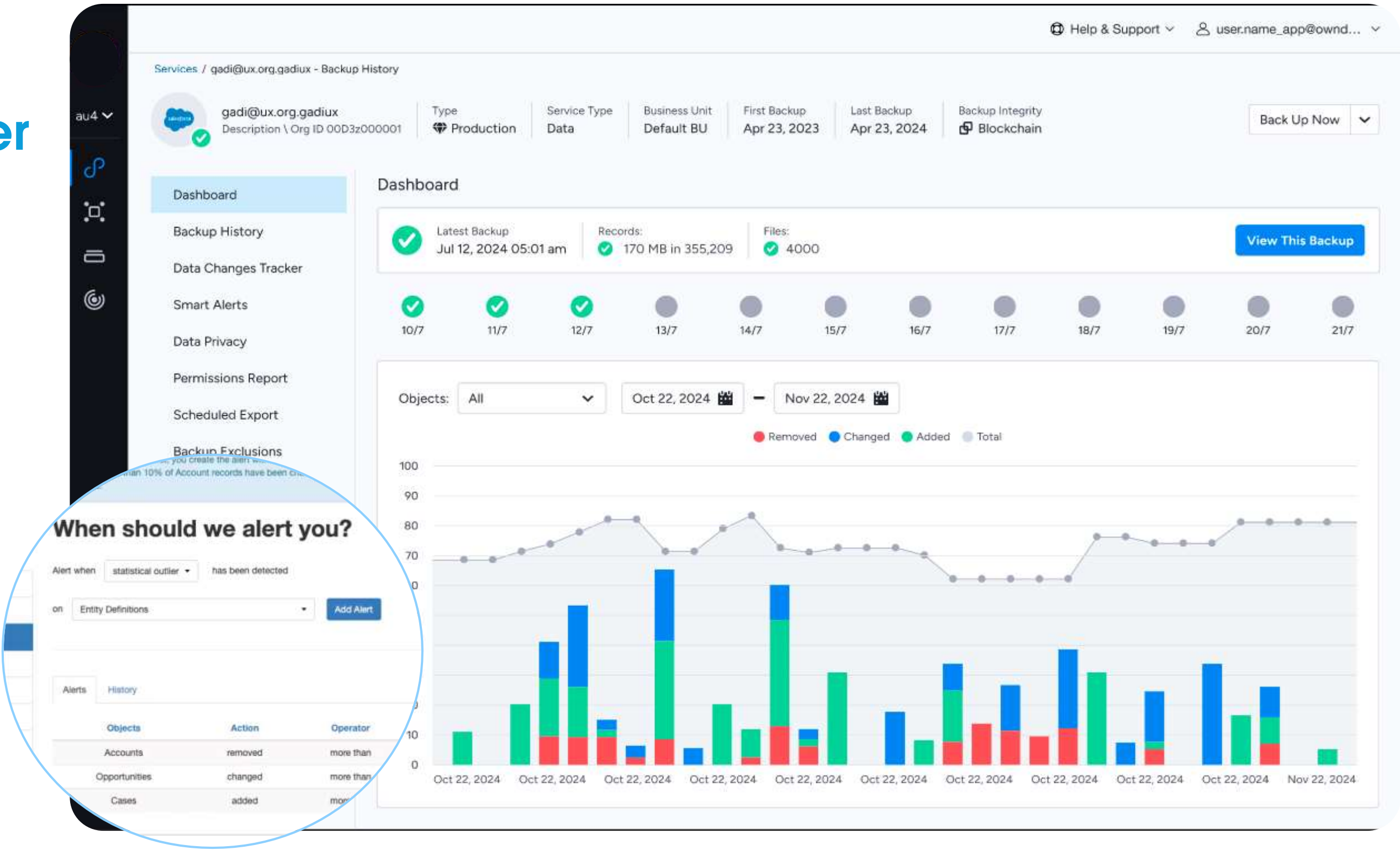
중요한 데이터, 메타데이터, 샌드박스 등을 매일 자동으로 백업하여 데이터를 쉽게 보호

정확하고 신속하게 복원

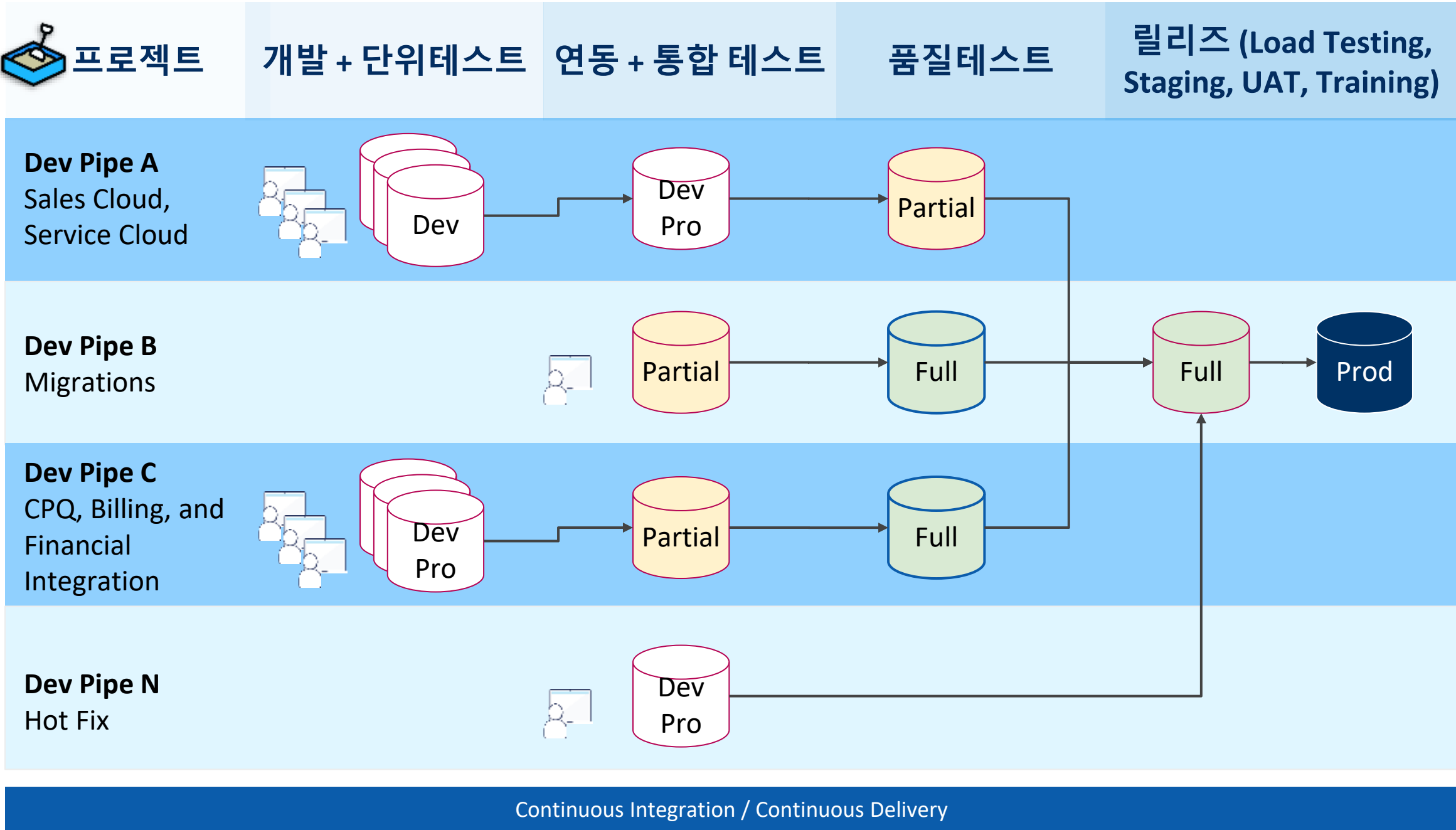
손실 영향을 받은 객체, 필드 및 레코드를 정확하게 복원하여 복구 가속

사전 예방적인 데이터 모니터링

이메일로 직접 알림을 보내 비정상적인 데이터 활동을 감지



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



- 1
- 2
- 3
- 4
- 5
- 6
- 7

8

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 인텔리전스 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



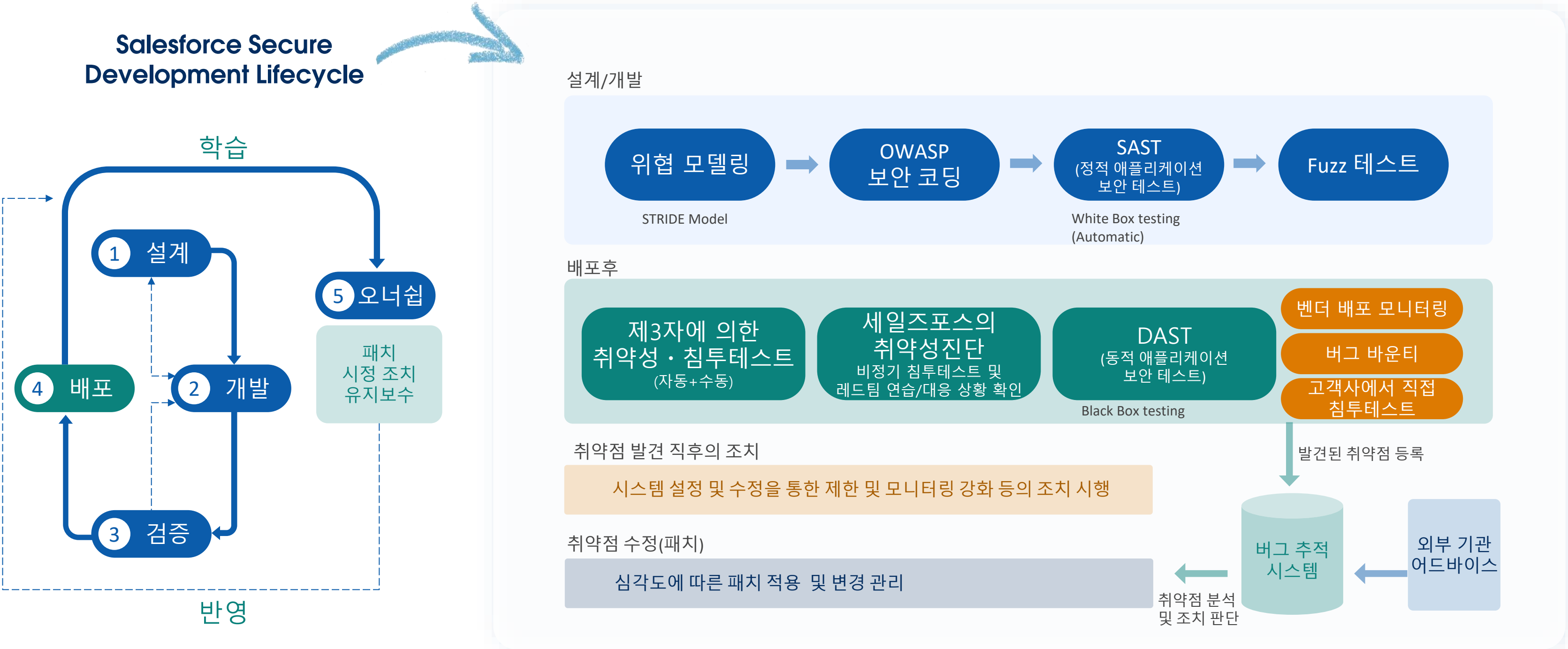
Salesforce Security Center :
인스턴스별 사용자 권한, 인증 등을 추적하고, 자동화된 위
험 평가 수행



- 1
- 2
- 3
- 4
- 5
- 6
- 7

8 정기적인 보안 테스트 수행

Salesforce 자체적으로는 보안 개발 라이프사이클 프로세스를 운영하고 있음



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 Agent 포함해서 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

salesforce

Salesforce 보안 기능 및 솔루션

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 Agent 포함해서 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



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

salesforce

salesforce

Data Security Best Practices in the Age of AI



Contents

Introduction

The critical inflection point of AI and data security

3

Research and statistics

A portrait of the modern threat landscape

4

Best practices

Strike the balance between AI innovation and data security

6

Solutions for success

Salesforce security and privacy

11

Conclusion

Employ AI quickly and securely with Salesforce

21



<http://sfdc.co/datasecurityBP>



Thank you

