



SecuPi Data Security Platform

Sensitive Data Access Protection and
de-identification for cross-Cloud and on-prem

www.secupi.com

A screenshot of the SecuPi web interface showing a "Customer Data" table. The interface includes a dark sidebar with navigation icons, a search bar, and a user profile icon. The table lists customer information with columns for Name, Email, and Location.

Name	Email	Location
John Adam	john.adam@newco.com	San Francisco USA
George Michael	george.michael@fast.co.uk	London, UK
Jessica Smith	jessica.smith@scale.com	New York, USA



SecuPi Data Security Company



SecuPi, a pioneer in the Data Security Platform market, ensures fast, scalable, and compliant protection of sensitive data everywhere covering the entire data security lifecycle

Vanguard

Fidelity
INTERNATIONAL

NORTHERN
TRUST

KeyBank

vodafone

KEMPER

swisscom

DHL

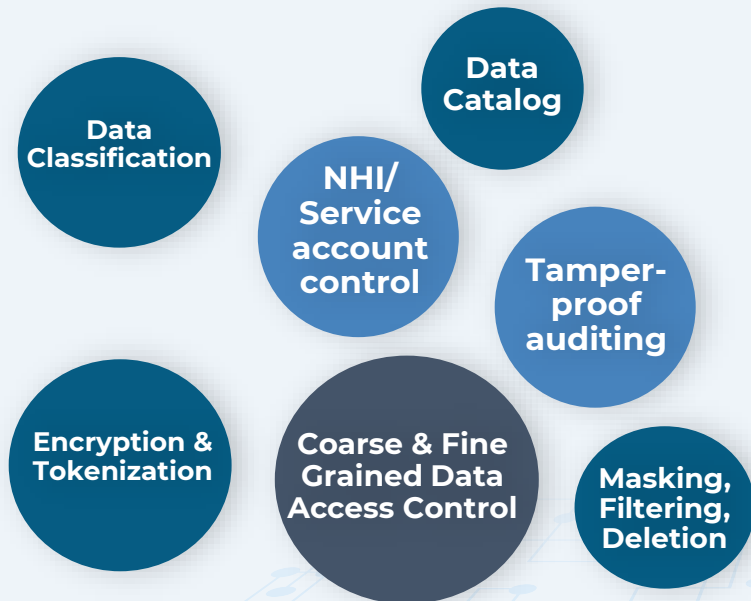
AXA

UBS

Moving from a Fragmented to a Unified AI Data Security Lifecycle Model

Before

Disconnected tool sprawl, draining budgets & resources, failed audits while leaving blind spots attackers exploit



After

SecuPi unified platform, simple to maintain, cost savings, complete visibility & control

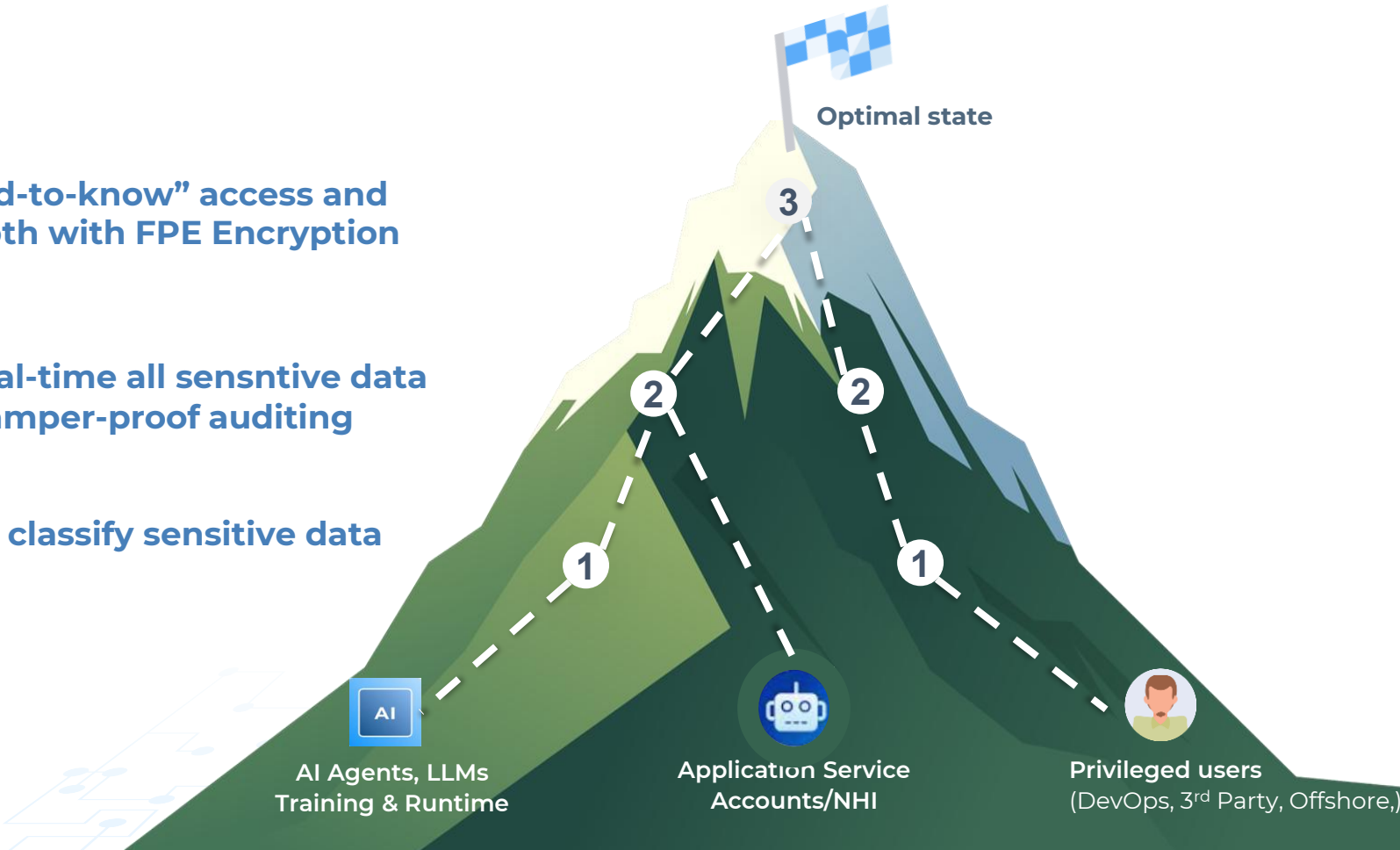


Zero Trust Maturity Model and NIST SP 800-207

> Enforce “need-to-know” access and defence in-depth with FPE Encryption

> Monitor in real-time all sensitive data activity with tamper-proof auditing

> Discover and classify sensitive data



AI exposes the enterprise to unprecedented regulatory and operational risk – focus on the EU AI Act

Governance	Root Cause	Business Risk
AI lacks access control	No reliable, fine-grained or deterministic access controls	Compliance Failure: Inability to enforce and prove "Least Privilege" under regulation such as the AI EU Act
Opaque Data Pipelines	Service account/non-human access (via MCP) create "backdoors" to sensitive data	Uncontrolled Exfiltration: Massive volumes of PII and IP ingested into LLMs with data loss risk
Auditability Deficit	Absence of tamper-proof, end-to-end audit trail for AI data interactions	Forensic Liability: Inability to provide verifiable audit trails during mandatory external audits or litigation

“Through 2029, over 50% of attacks will exploit access control issues.”

How to Secure Custom-Built AI Agents, Dionisio Zumerle, 11 June 2025

Gartner

AI Sensitive Data Challenges

1. Regulatory friction

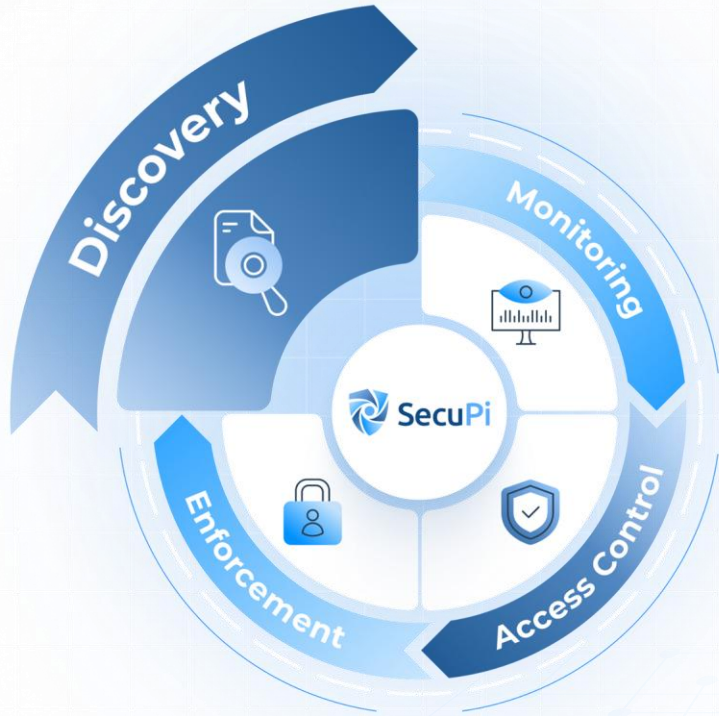
EU AI Act, GDPR, SOC2, SOX, and data residency friction blocks AI adoption

2. Sprawl of AI Agents and Workflows equipped with unbounded agent permissions

AI agents use NHI/service accounts inherited overly broad privileges creating new threat vectors

3. AI agents pulls data from a source by ignoring its native access controls

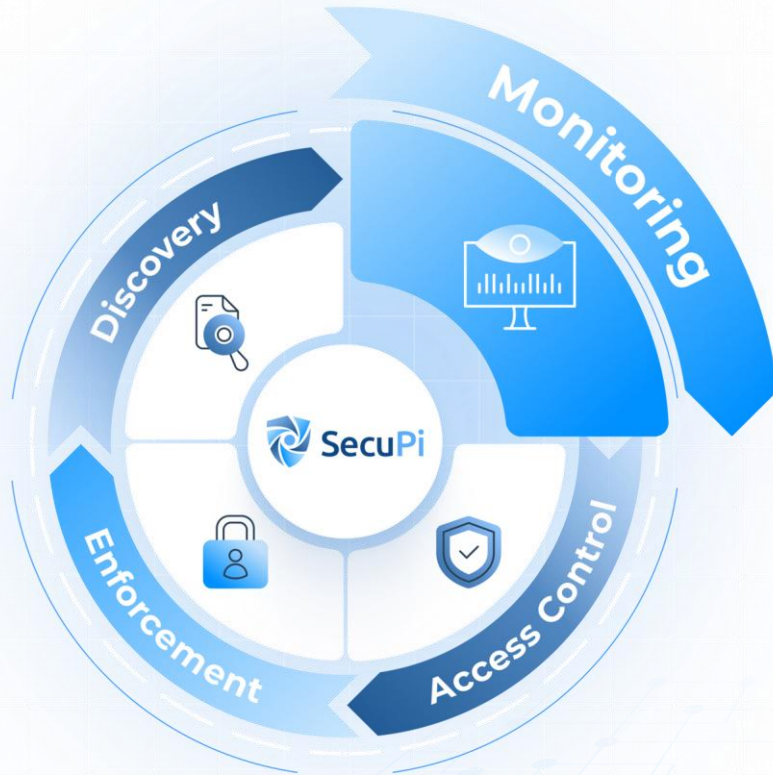
Data Security Platform for AI



Discovery & Classification

- Discover your data wherever it lives
- Classify data based on context and location

Data Security Platform for AI



Monitoring

- Seamless monitoring of all data repositories across hybrid network (Cloud & On-premise)
- Multiple deployment options (Agent, Agentless, proxy etc.)
- User Behavior Analytics for detecting hackers and malicious insiders
- SOC integration

Data Security Platform for AI



Access Control

- Attribute based access control (location, intent, time, context)
- Centralized managed policies , applied in real time

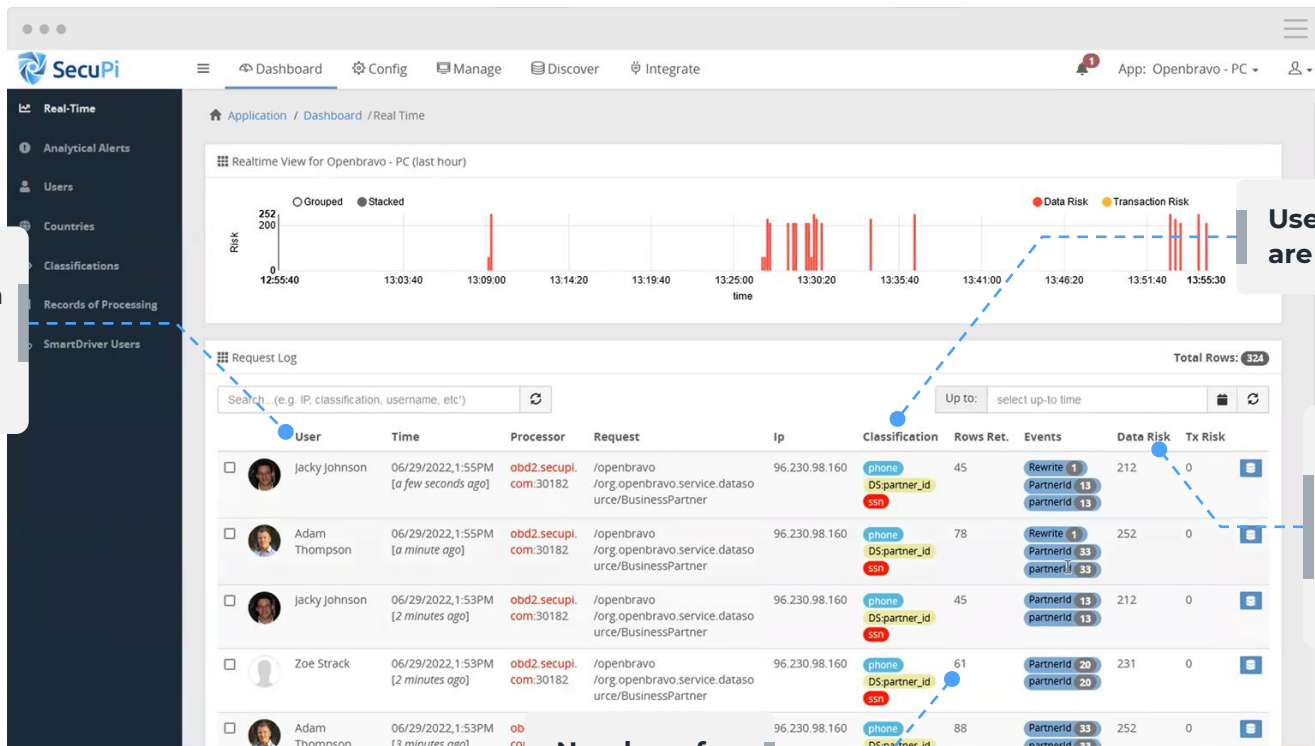
Data Security Platform for AI



Enforcement

- **Protect the data at-rest and in-use**
- **De-identify with NIST Standard Quantum-resilient encryption**
- **Mask, redact or block unauthorized data-products exposed to AI**

SecuPi real-time user context observability



End-user context (even when using service accounts)

User requests are classified

User requests are assigned Data Risk Score (for Threat Detection)

Number of rows returned

Column, row and cell Level Access Control



Auto | DEMO_DB (Jill Canada Mexico C2) | PUBLIC@DEMO_DB

<DEMO_DB (JACK USA C4)> Script-5 | *<DEMO_DB (Jill Canada Mexico C2)> Script-2

```
SELECT * FROM DEMO_DB."PUBLIC".CUSTOMERS_CS;
```

SYSS_VIEW_26 1 | SYSS_VIEW_26 2

SELECT * FROM DEMO_DB."PUBLIC".CU | Enter a SQL expression to filter results (use Ctrl+Space)

	ABC EMAIL	ABC NAME	ABC CC	ABC STREET	ABC CITY	ABC CI	ABC ST	ABC SSN	ABC DEPARTM
109	dBmG_jcgUNVQL9@ejZJhr.jE7	Hope Asher	3147-4329-5812-37	Angel Route 1517	Mexico City	Mexico	Gold	685-89-511	LAN8ZK1gJ5
110	X9n7X4_CjB0DbLs1FI@lzWkG.fyW	Audrey Prestoi	1804-3757-9338-59	St. Pauls Road 8777	Mexico City	Mexico	Silver	285-88-873	z2olnVkrP
111	EYGM7_KOUQaWqu@YvBiK.ZFK	Percy Jones	3570-3860-9695-65	Elystan Boulevard 974	Mexico City	Mexico	Gold	573-93-515	z2olnVkrP
112	6PFfR_381c127Fb@5Qn9J.ZU3C	Joyce Mills	0850-4324-1553-24	Blackheath Avenue 6	Mexico City	Mexico	Employee	XXXXXXXXXX	6zEdRZQf rOf
113	mvvEu_wJC8cALuP@ITeca.DqJU	Aiden Owens	3628-7135-9630-51	Paris Pass 462	Toronto	Canada	Silver	749-30-755	IT
114	PqG0_6WgKc5zjRm@JS89W.kL75	Fred Ramsey	5213-0792-5236-92	Abbey Way 2879	Mexico City	Mexico	Silver	932-32-071	LAN8ZK1gJ5
115	AXa2i_D58p8xcteXpG@VYtfW.6bc	Harry Bradshav	0048-7819-1199-06	Magnolia Avenue 347	Toronto	Canada	Silver	750-20-119	eYFm6mi
116	aZi_dVqFfw9Y5Np@x4G8to.KnN	Tom Chapmar	5508-2743-5163-59	Mariner Rue 5958	Mexico City	Mexico	Silver	829-66-858	LAN8ZK1gJ5
117	4vvh_bg6d1bTMMfq@S9REA.cmu	Noah Shelton	3020-5736-7150-62	Westcott Grove 3061	Mexico City	Mexico	Platinum	XXXXXXXXXX	4pHQ6etjUZ
118	ySCX_AR8XitjD@najeeD.oNI	Alan Lowe	0713-5758-0822-31	Berry Street 2213	Mexico City	Mexico	Silver	500-20-532	H7NuT
119	YFhZJZ_vtW8wj76V@rxMbfo.EIX	Marvin Mould	2173-4162-1825-52	Carrindale Boulevard 19	Mexico City	Mexico	Silver	516-07-319	6zEdRZQf rOf
120	RWErqAd_5IEkOJgYMDJ@y4kjY.o2	Anthony Stew	5518-0725-0528-40	Victoria Rise Alley 346	Mexico City	Mexico	Gold	890-48-288	z2olnVkrP
121	Tp9mLnb_w2zNLrR8y@h3QyIT.JA6	Michael Clark	5833-4442-3772-52	Bingham Way 9666	Toronto	Canada	Gold	400-73-049	8qjt5 zku3KED
122	qfJO_MFHbrUMcF@EvHADY.sjg	Mike Plant	3627-7681-6392-25	Birkbeck Drive 4044	Mexico City	Mexico	Silver	440-22-280	LAN8ZK1gJ5
123	KrCaP_AplCtYHjk5Z@avVqUE0.Yx	Susan Nicolas	7521-7237-4660-37	Ellerslie Grove 5190	Mexico City	Mexico	Silver	421-78-847	IT
124	NDED_1c3MoXZGPT@fhnYv2.Uxv	Brad Dunbar	6478-7582-1601-57	Blean Way 8935	Toronto	Canada	Platinum	XXXXXXXXXX	IT
125	lFlNtD_5UlfdbsxAc@MuLgn5J.kTT	Adalie Hammc	5810-6557-3714-05	Dunton Alley 195	Mexico City	Mexico	Platinum	XXXXXXXXXX	8qjt5 zku3KED
126	zOuP56_1TQD5ulK@n7W3Ya.XIN	Alexia Owen	8544-4383-9750-62	Cam Avenue 8911	Mexico City	Mexico	Silver	349-00-298	H7NuT
127	sKylSbW_ik2WU7Qq1y@urxSrXE.F	Carolyn Rehm	2643-2393-7594-01	Boadicea Hill 4933	Toronto	Canada	Silver	790-19-040	4pHQ6etjUZ

Object level



Column level



Row level



Cell level



SecuPi classification and encryption example

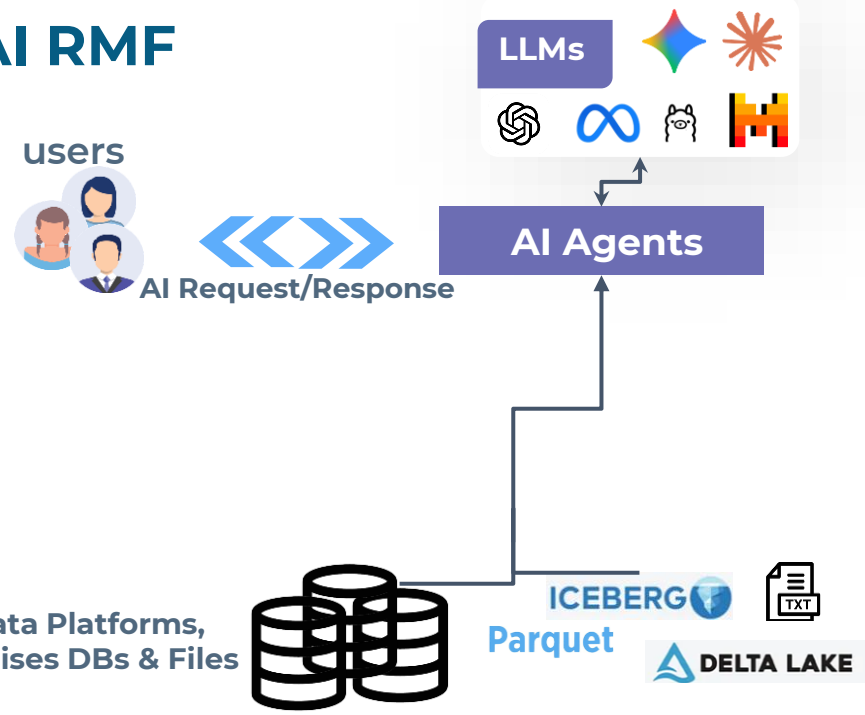
Source text

```
1 # Can you confirm your full name?
2 # My name is Tammy Alvarez.
3   What is your spouse's name?
4 # Their name is Sarah Alvarez.
5   What is your date of birth?
6 # It is 1976-06-16.
7 # Can you share your Social Security Number?
8 # It is 260-56-5225.
9   What is your Taxpayer ID Number?
10 # It is 260-56-5225.
11 # Do you have your State ID Number?
12 # Yes, It is D6605307.
13   Please confirm your Driver License ID Number.
14 # It is D6605307.
15   What is your Passport Number?
16 # It is 364931974
17   Can you provide your current address?
18   Sure, It is 771 Alvarez Underpass Apt. 175
19 # San Jose, CA 95152.
20   What is your mailing address?
21 # It is 771 Alvarez Underpass Apt. 175
22 # San Jose, CA 95152.
23   What is your primary telephone number?
24 # It is 541-483-2605x205.
25   What is your email address?
26 # It is wheelercourtney@example.com.
27   Do you have an alternate phone number?
28 # Yes, 541-483-2605x205.
29   What is your preferred communication method?
30   Text.
31   Can you confirm your work phone number?
32 # Yes, 541-483-2605x205.
```

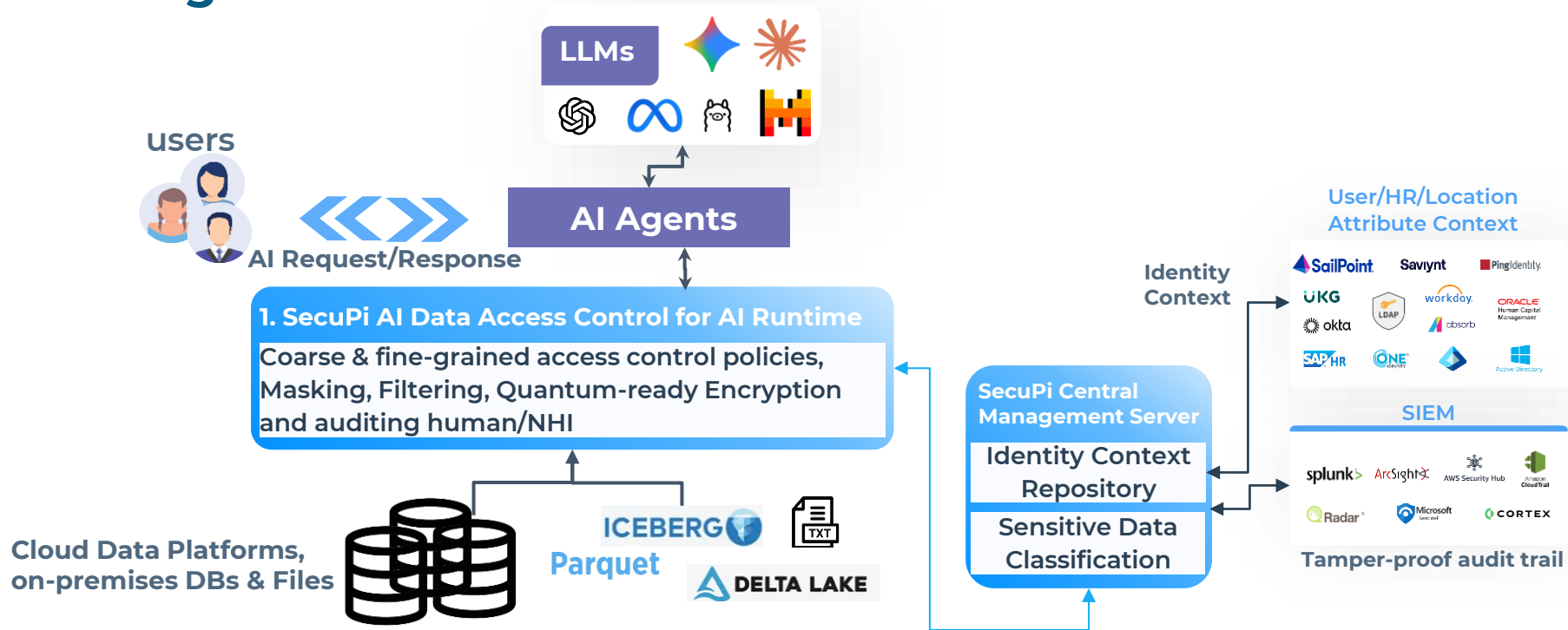
Tagged and encrypted with SecuPi

```
1 # [XYZ::Can you Co]nfirm your full name?
2 # My name is [PERSON::wduyQ me2WbJy].
3   What is your spouse's name?
4 # Their name is [PERSON::f3zKe wPLvLQL].
5   What is your date of birth?
6 # It is [DATE_TIME::5eCJ-Cv-ft].
7 # Can you share your [ORGANIZATION::Social Security] Number?
8 # It is [US_SSN::888-96-0600].
9   What is your Taxpayer ID Number?
10 # It is [US_SSN::888-96-0600].
11 # Do you have your [ORGANIZATION::State] ID Number?
12 # Yes, It is 53 586 032.
13   Please confirm your Driver License ID Number.
14 # It is 53 586 032.
15   What is your Passport Number?
16 # It is [US_PASSPORT::583485217]
17   Can you provide your current address?
18   Sure, It is [ADDRESS::584 Edsfvgf Ptrdfqwed Rdf. 584
19 # East Patriciafort, FM 96552].
20   What is your mailing address?
21 # It is [ADDRESS::584 Edsfvgf Ptrdfqwed Rdf. 584
22   East Patriciafort, FM 96552]
23   What is your primary telephone number?
24 # It is [PHONE_NUMBER::709-589-6580x893].
25   What is your email address?
26 # It is [EMAIL_ADDRESS::BggXyI2B7sXGxo3@example.com].
27   Do you have an alternate phone number?
28 # Yes, [PHONE_NUMBER::709-589-6580x893].
29   What is your preferred communication method?
30   Text.
31   Can you confirm your work phone number?
32 # Yes, [PHONE_NUMBER::709-589-6580x893].
```

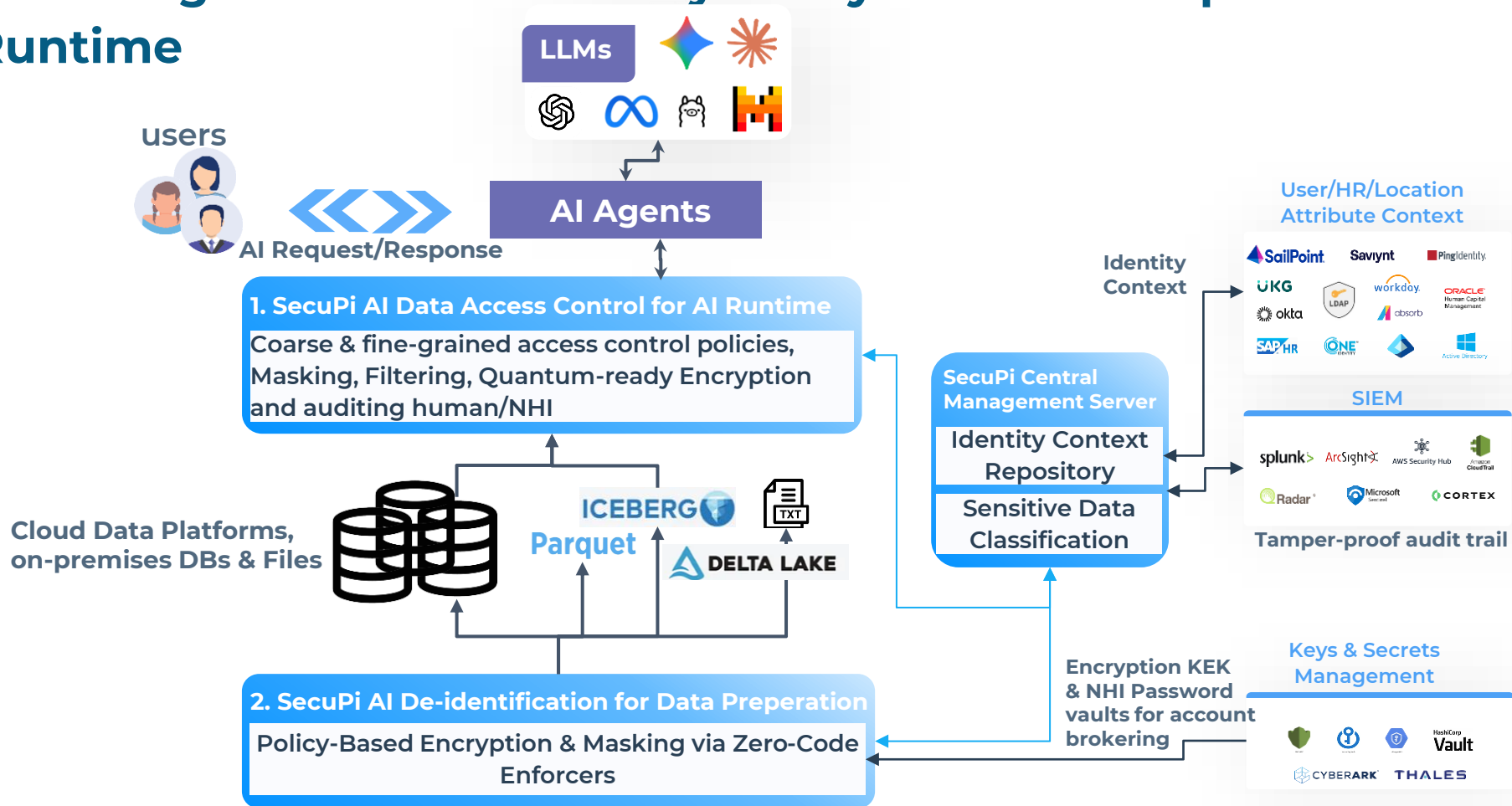
Securing AI Agent Access to Sensitive Data Under EU AI Act & NIST AI RMF



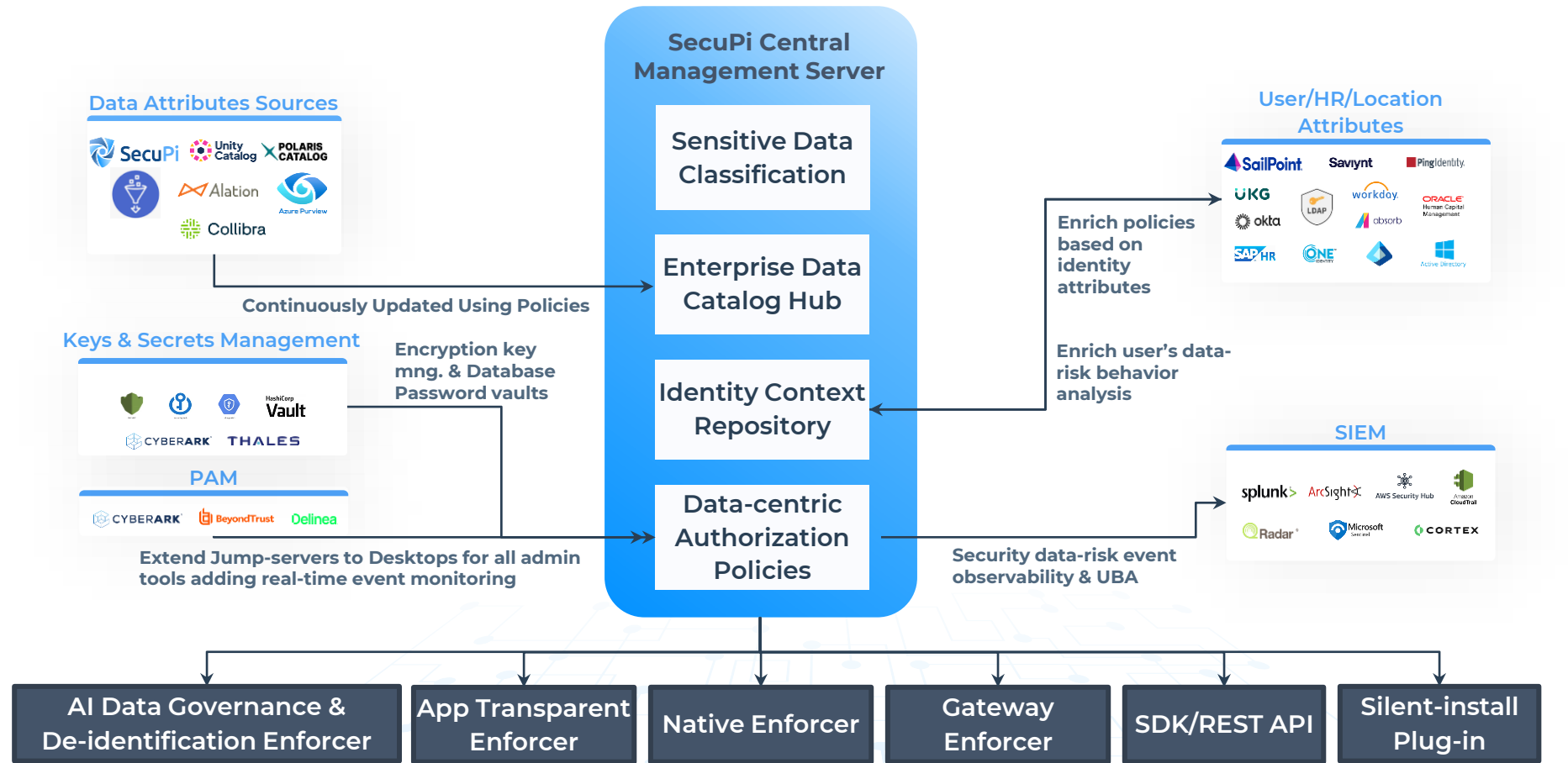
Enforcing Data Access Control at AI Runtime



Enforcing the AI Data Security Lifecycle: From Preparation to Runtime



SecuPi architecture: harmonizing identity & data context



Summary: AI Data Access Control

- **Safely expose sensitive data to AI**

Secure training and runtime access to data across cloud and on-prem with Quantum-resilient FPE Encryption (NIST FFI)

- **Runtime protection + tamper-proof auditing**

Control exactly what data AI agents receive across Snowflake, Databricks, Oracle, mainframes, and data lakes

- **Fine and coarse-grained enforcement**

Row/column-level security with masking, FPE, tokenization, and deletion Enforce policies by user identity, role, geography, data sensitivity, purpose, and session context

- **Eliminate NHI risk**

Map AI/service accounts to real user identity—no blind over-privileged access

- **Zero-code deployment**

No changes to AI apps, schemas, or pipelines—operational in days



Sensitive data de-identification

SecuPi Data Protection Methods

Deterministic & Reversible Methods

Original Data

4472-8302-9115-3562

4472-9665-3456-2362

YXNklGdmc2RmZbmJhc3NkIA==

NTY5MGprbGZzZHM7YTA5MzQ
9MGdmbGtkO2phMDkzMg==

Tokenization and FPE

- × Based on NIST standard, using 128, 192 or 256bit enc keys
- × Fast, Reversible.
- × Preserves Form & Length based on the Data Format
- × Can include checksum and validation bits

Original Data

jsmith@SecuPi.com

ujckoi@xJekaP.com

234 - 75 - 9033

381 - 58 - 6294

AES Encryption

- × Data is converted to binary ciphertext using mathematical algorithm and encryption key.
- × Fast, Reversible.
- × Non-Format Preserving , hard to use with Database Schemas

AEAD Encryption

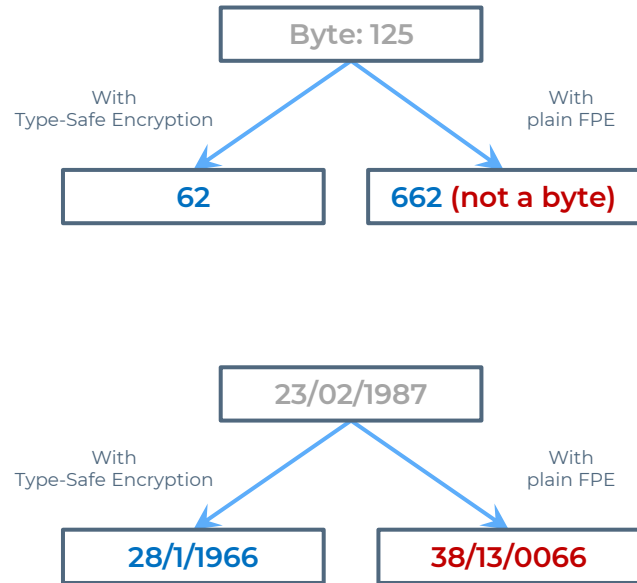
- × Like AES with Authentication (storing Key Name + Version as part of the value)
- × Ciphertext result is longer than AES
- × Fast, Reversible
- × Non-Format Preserving, hard to use with Database Schemas

SecuPi Data Protection Methods

Deterministic & Reversible Methods

Type-Safe Encryption

- × Transform values into a different value in the same Type
- × Type of data preserved (Integer, Long, Dates, Floats, Doubles)
- × Reversible
- × Good for Database Types, ETL processes, making sure encryption does not break applications
- × Plain FPE may fail in those cases



SecuPi Data Protection Methods

Deterministic & Irreversible Methods

Bucketing/Rounding

- × Group values into buckets (configurable)
- × Irreversible
- × Good for Low-Environments

Dynamic Masking

- × Transform values into non-readable form
- × Irreversible
- × Good for Low-Environments / Application Data Minimization

Replacing/Zeroing/Nullifying

- × Mask/Hide parts of the result with X, Zero or Random value.
- × Irreversible.

Obfuscation

- × Data is consistently randomized into a set of values
- × Irreversible
- × Good for Low-Environment / Testing purposes

