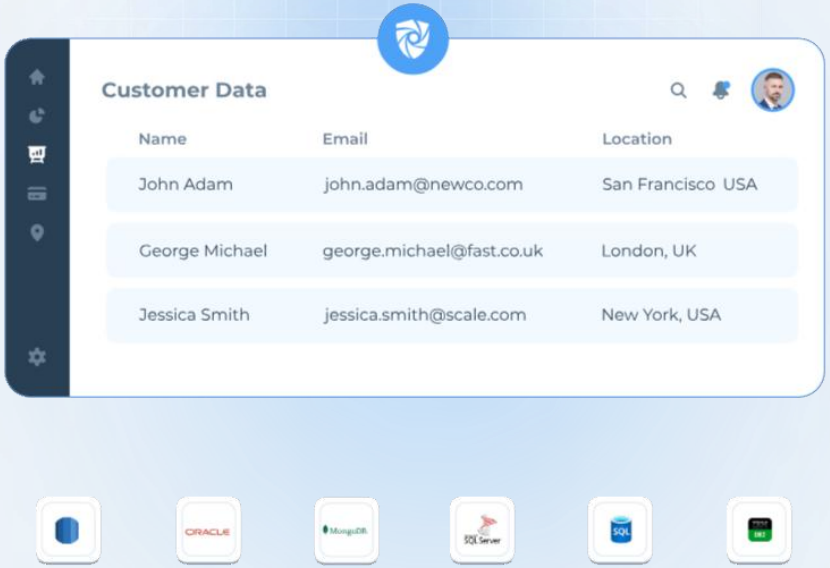
SecuPi

SecuPi
Data Security Platform

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

www.secupi.com



SecuPi Data Security Company

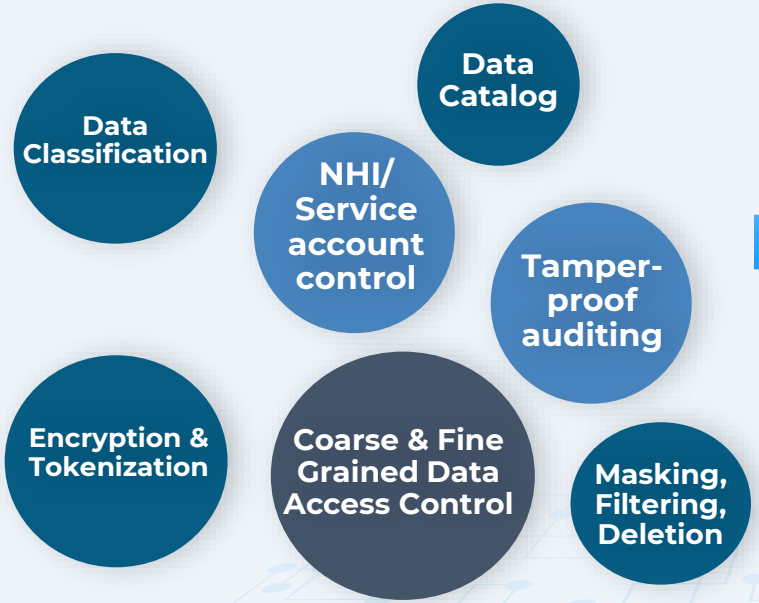
SecuPi, a pioneer in the Data Security Platform market, ensures fast, scalable, and compliant protection of sensitive data everywhere covering the entire data security lifecycle

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

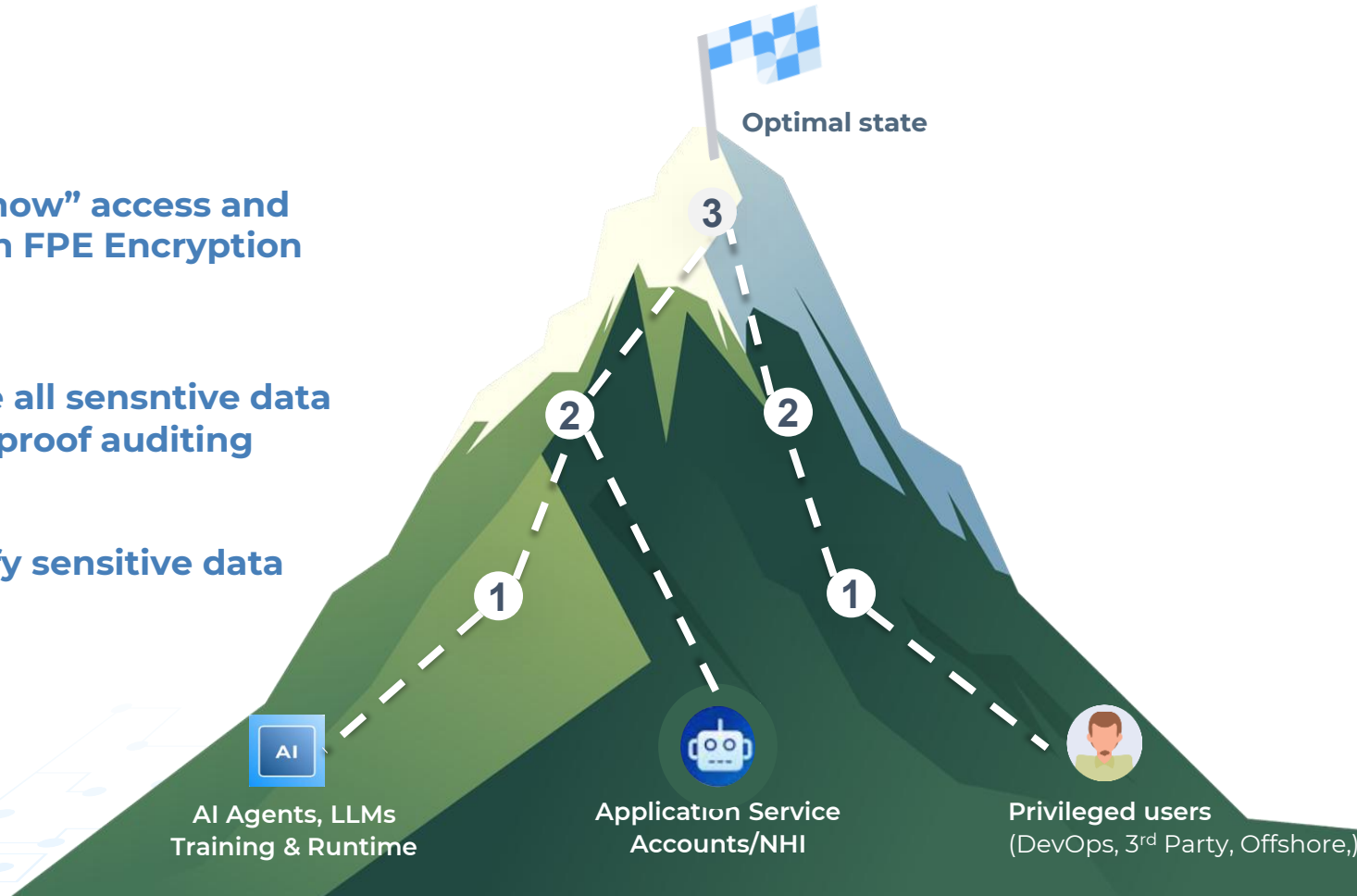
SecuPi unified platform, simple to maintain, cost savings, complete visibility & control

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 sensntive 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**

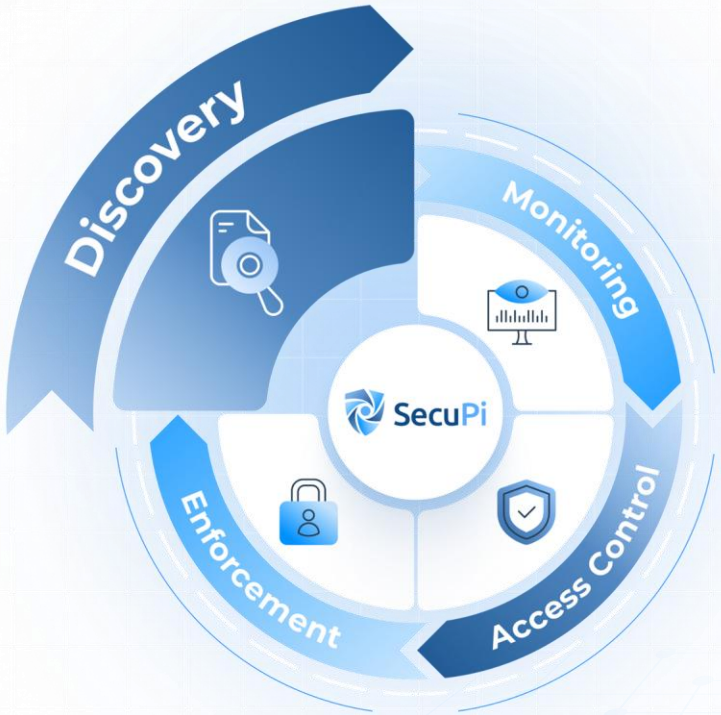
   EU AI Act, GDPR, SOC2, SOX, and data residency friction blocks AI adoption

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**

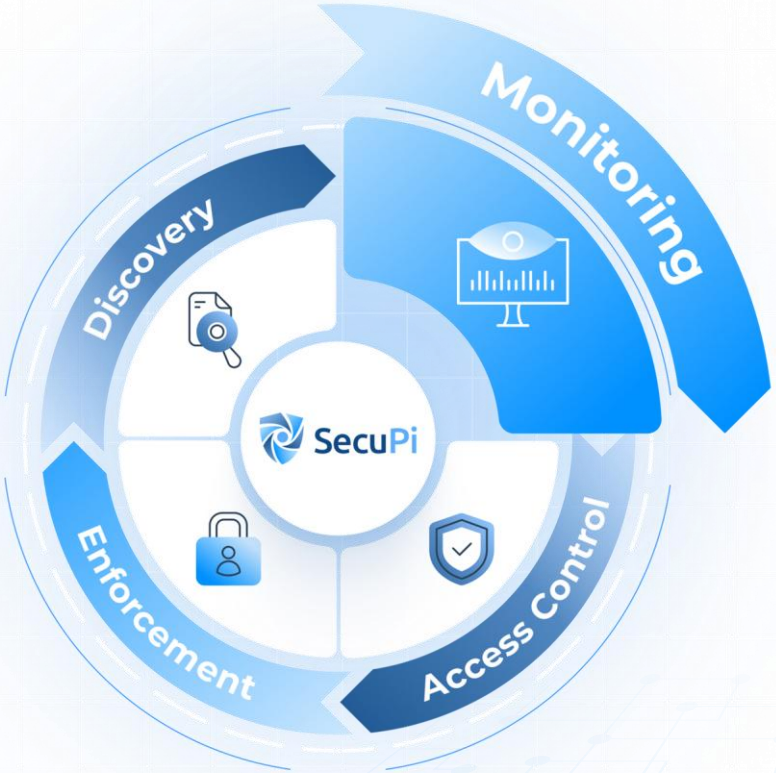
Data Security Platform for AI



Discovery & Classification

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

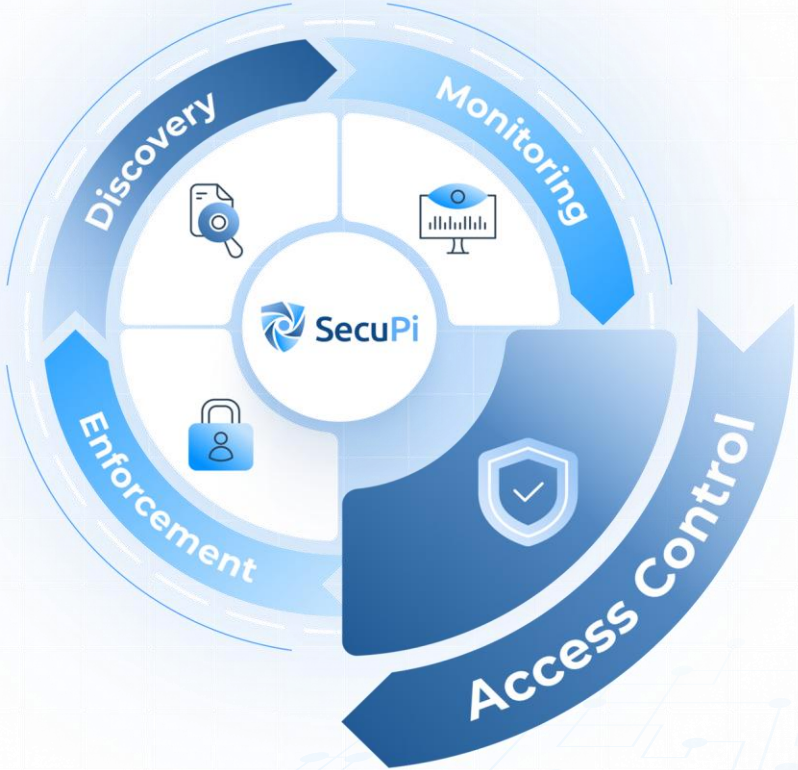
Data Security Platform for AI



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

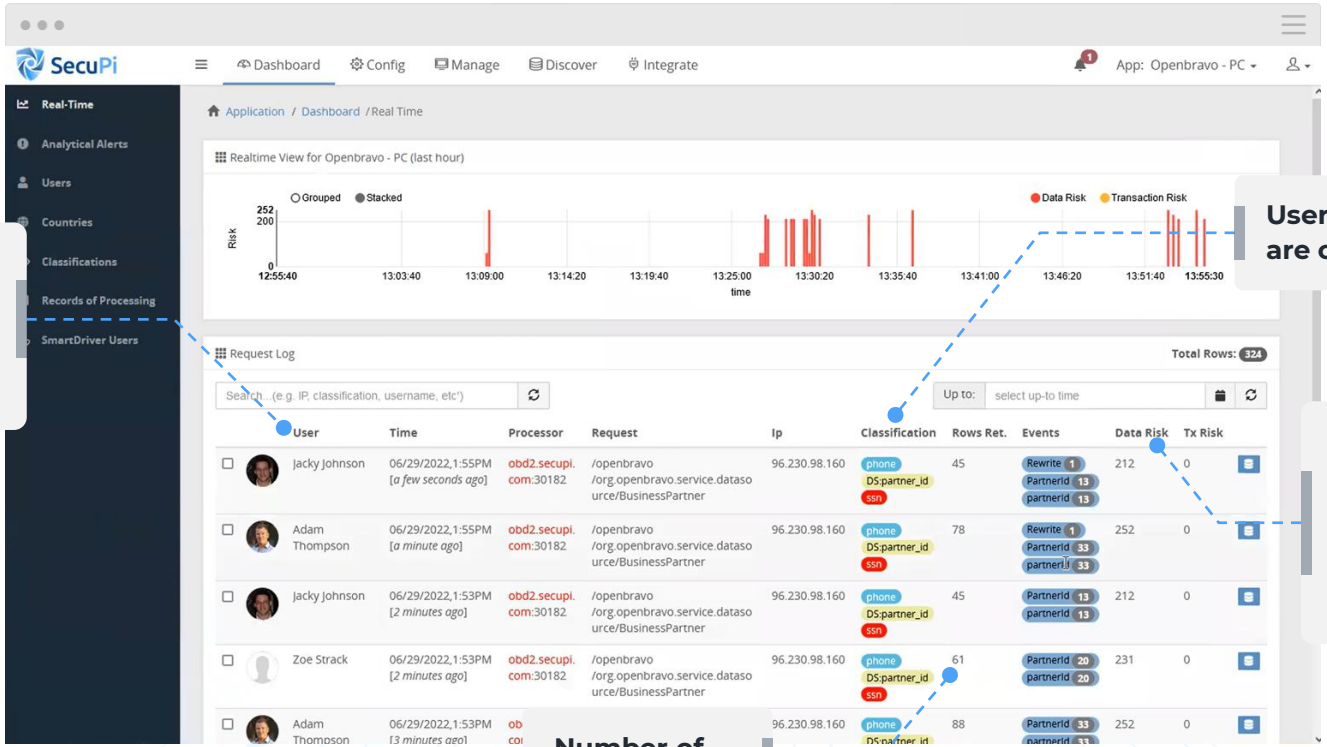
- Attribute based access control (location, intent, time, context)
- Centralized managed policies , applied in real time

Data Security Platform for AI

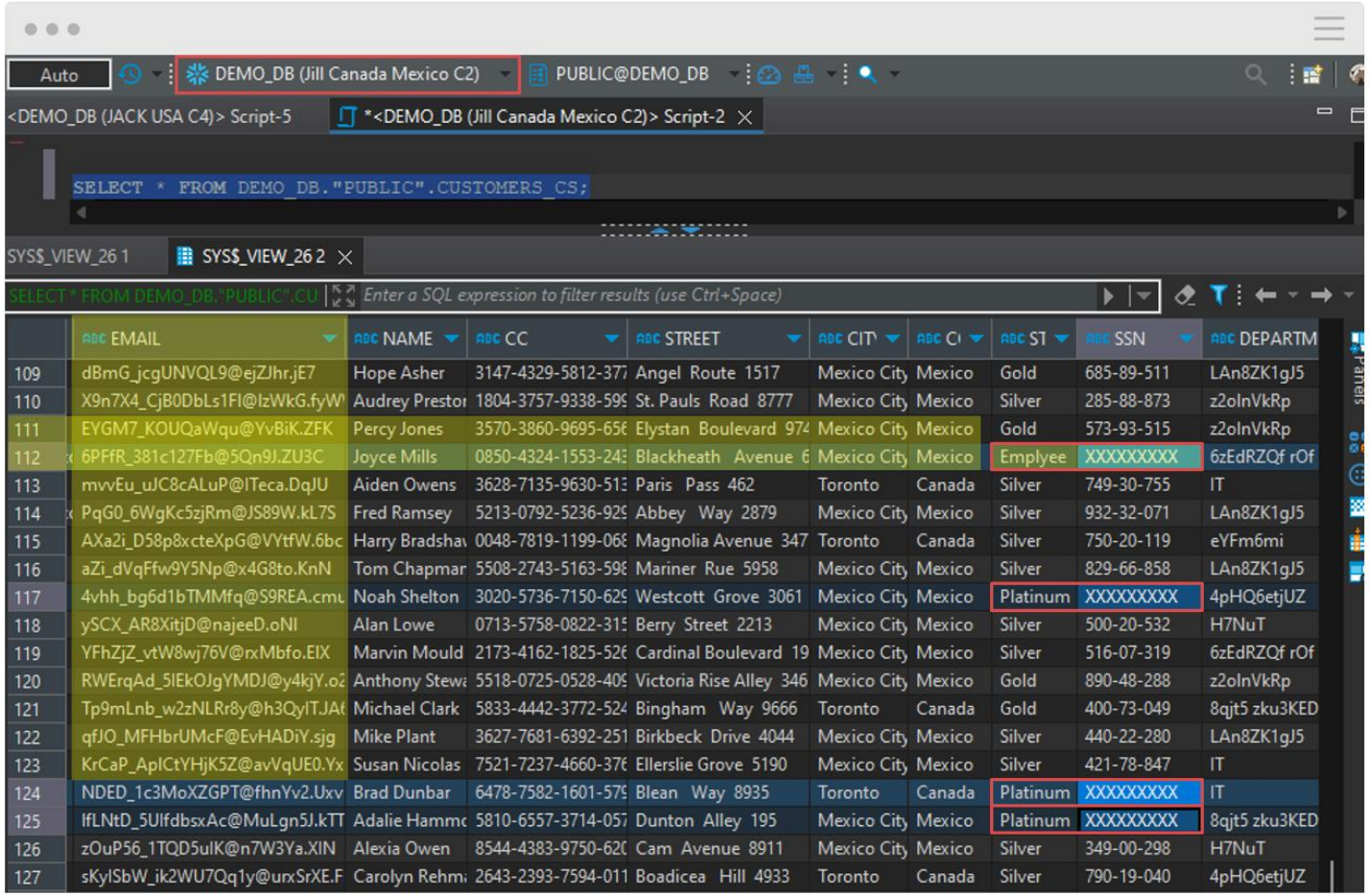
Enforcement

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

SecuPi real-time user context observability



Column, row and cell Level Access Control



Object level

Column level

Row level

Cell level

SecuPi classification and encryption example

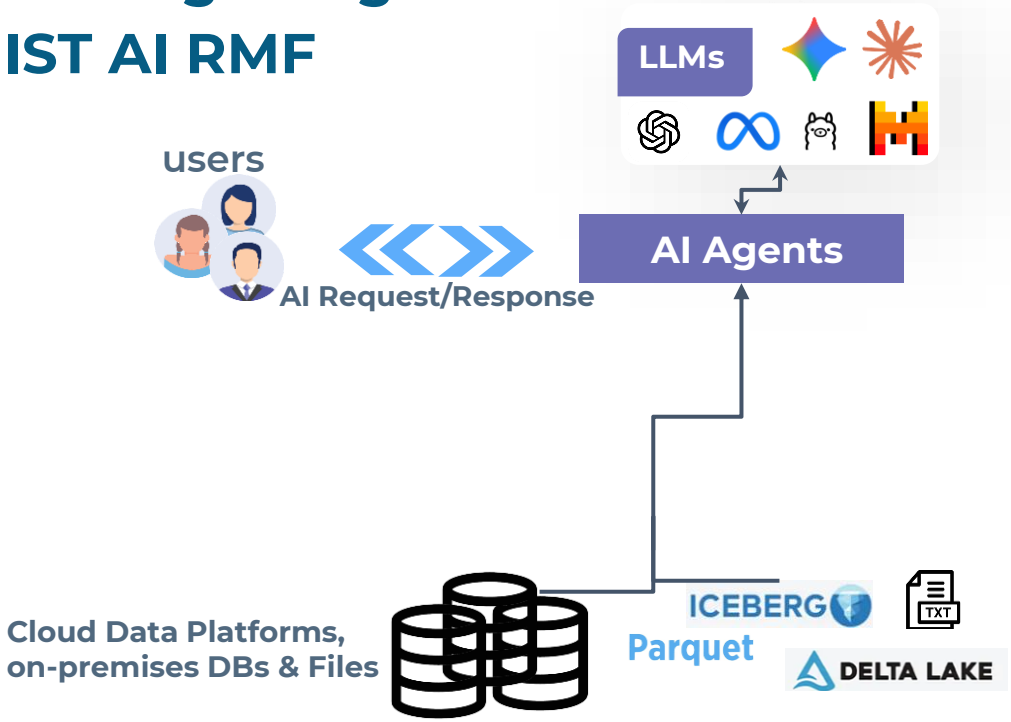
Source text

```
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?
```

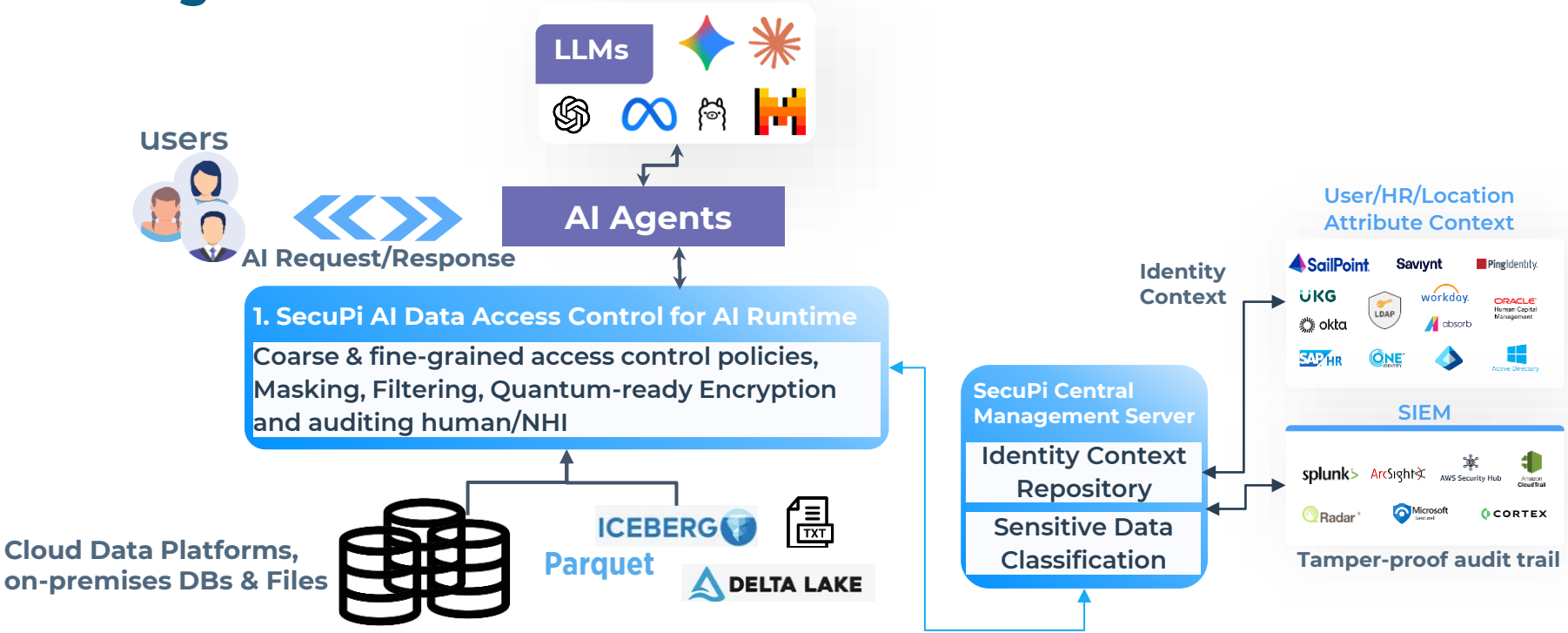
Tagged and encrypted with SecuPi

```
1  [XYZ::Can you co]nfirm your full name?
2  My name is [PERSON::wdyuQ 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?
```

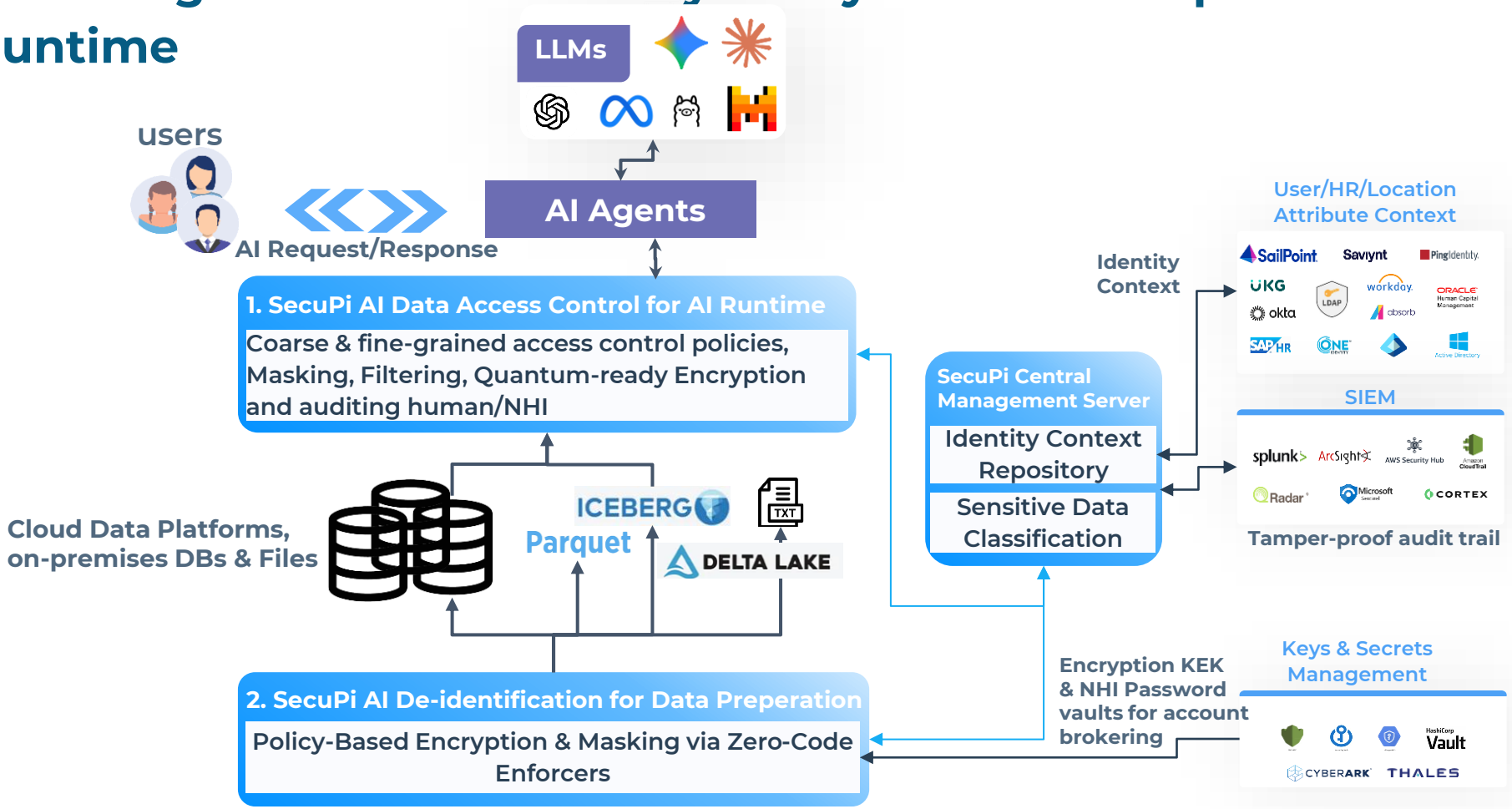
Securing AI Agent Access to Sensitive Data Under EU AI Act & NIST AI RMF



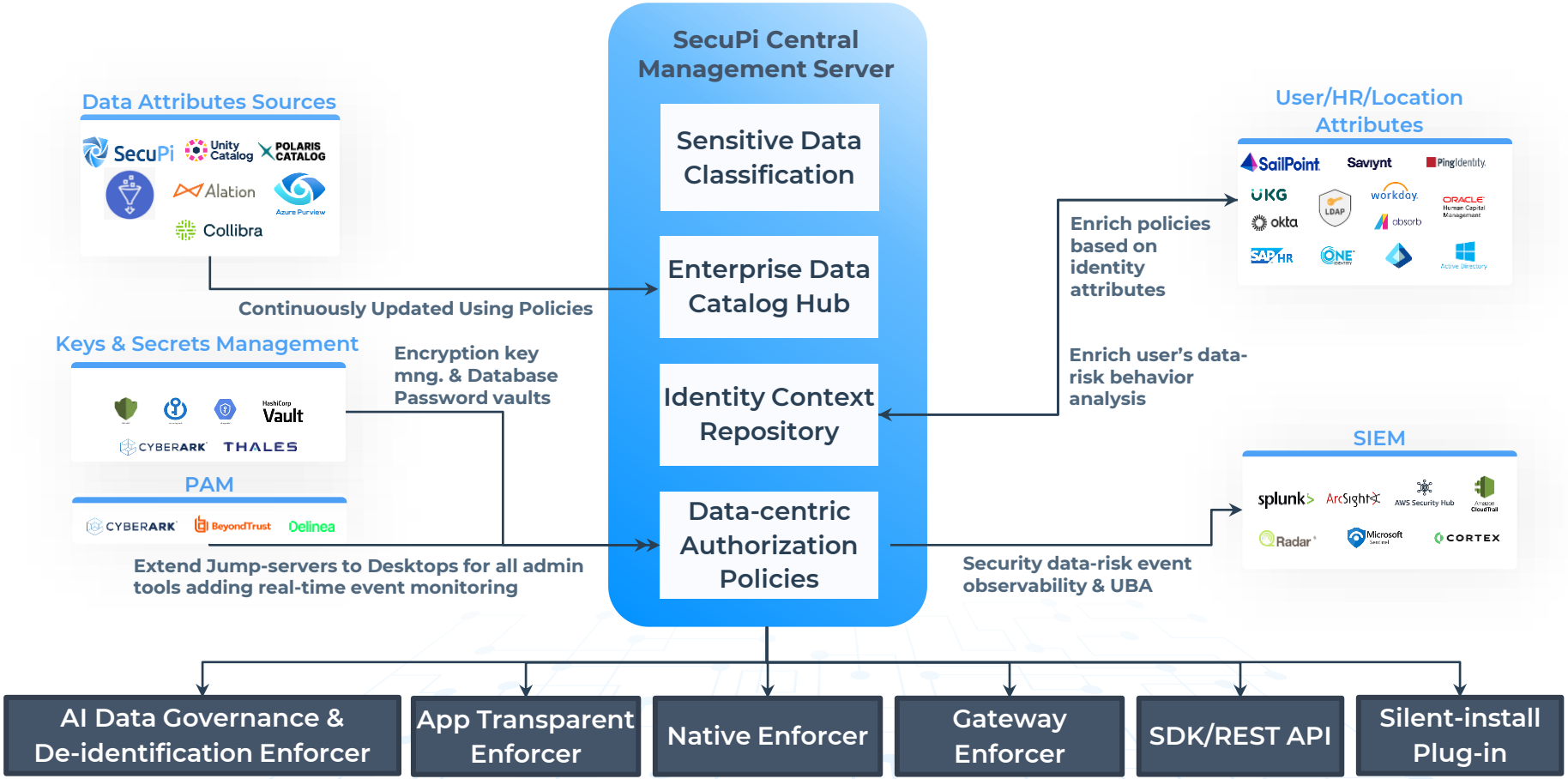
Enforcing Data Access Control at AI Runtime



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 FF1)
- **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

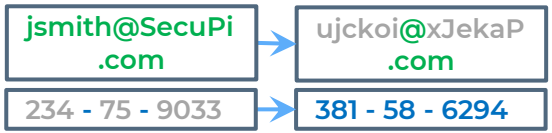
YXNkIGdmc2RmZbmJhc3NkIA==

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



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

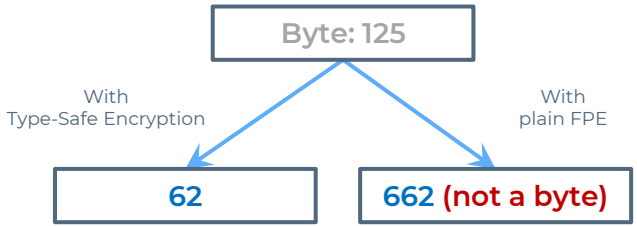
- Like AES with Authentication (storing Key Name + Version as part of the value)
- Ciphertext result is longer than AES
- Fast, Reversible
- Non-Format Preserving, hard to use with Database Schemas

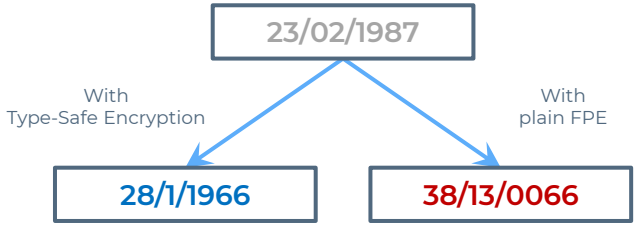
SecuPi Data Protection Methods

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