Dymium

Governed Data Access for the AI Era

Control what AI, Apps, and Analytics can see — securely and at scale

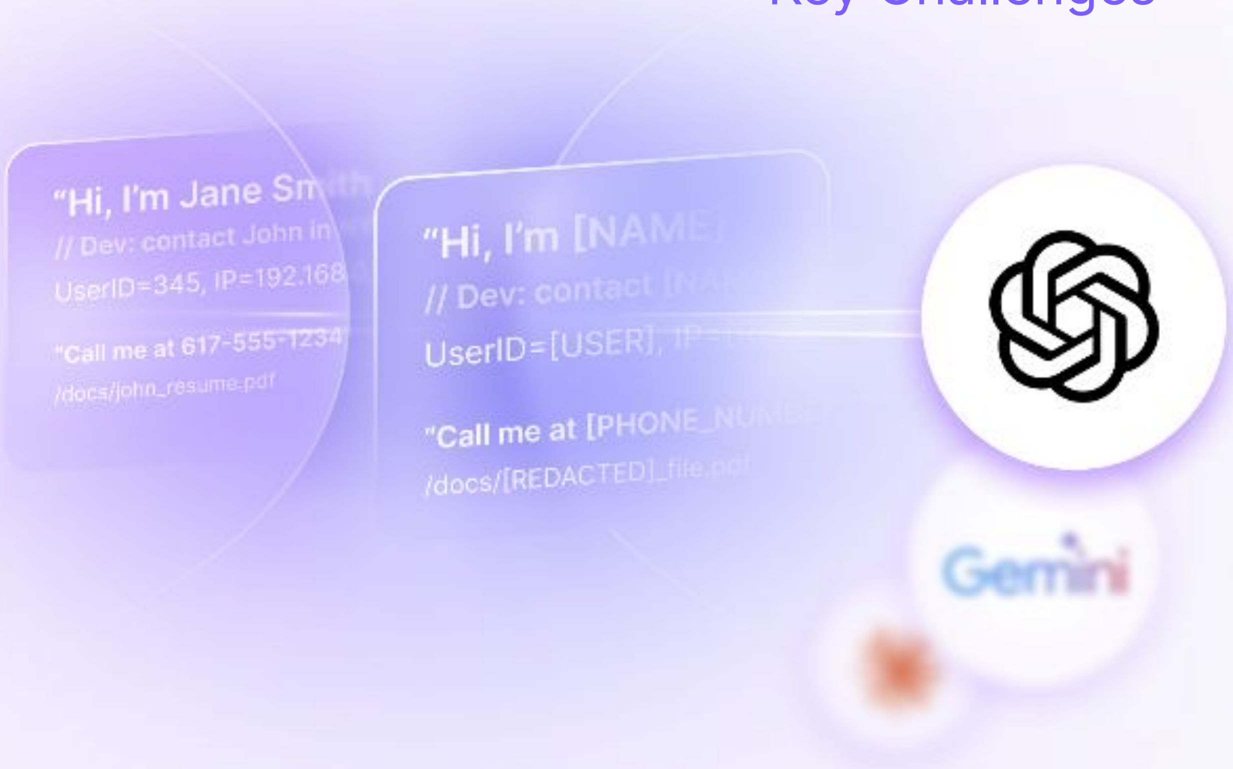
Denzil Wessels
Founder & CEO, Dymium

DATA IN (Reque
customer_id: 12345
customer_name: John Smith
customer_email: john.smith@
customer_phone: +1-555-12
product_name: Widget A
region: North America
sales_volume: 2500
purchase_date: 05/14/2

DATA OUT (Afte
customer_id: 12345
customer_email: xxxxx@
customer_phone: +1-xxx-xxx-
product_name: Widget A
region: North America
sales_volume: 2500
purchase_date: 2025-05-14

AI Is Scaling Faster Than Security Can Keep Up

But your existing controls are restraining your AI innovation...



Key Challenges

Complexity

Legacy architectures delay AI deployment by months — or even years

Flexibility

Most systems aren't built for dynamic retrieval and real-time inference

Fragmented

Others leave data vulnerable to context leakage, prompt injection, and agent overreach

Protecting Your Sensitive Data is a Top Priority

AI Is Outpacing Security

- Only 24% of GenAI projects are secure[1]
- 100% of Fortune 1000 IT leaders express concern about AI risks[2]

AI Is Out of Control

- Enterprises use 300+ unsanctioned AI apps[3]
- Most orgs lack visibility into model use and AI app behavior

AI Breaches Are Here

- 73% of enterprises had an AI-related breach in 2024[4]
- +218% increase in AI-driven attacks from nation-states[4]

Sources: [1] IBM Institute for Business Value · [2] PagerDuty · [3] Metomic · [4] J.P. Morgan AI Security Report

Common Gaps in Data Access & Governance

Category	What They Do	How Dymium Closes Gaps
AI Control Tools	Filter GenAI prompts after exposure	Prevents exposure before prompts hit sensitive data
Data Integration/ETL	Move or replicate data	Leaves data in place — governs access in real time
Semantic Layer	Proxy queries for BI tools	Enforces policies instantly across AI, BI, and apps
DSP (Data Security Platforms)	Apply static masking at the warehouse	Dynamic enforcement per request across hybrid environments
DSPM (Posture Mgmt)	Discover/tag data and alert on risk	Blocks access live — not just alerts after exposure

What We Do

The Ghost Layer: A New Way to Govern Data Access

Sits between users/agents and data sources (warehouses, lakes, databases)

Intercepts and evaluates every downstream access request

Leaves no data at rest, no logs, no shadow copies

Logs access externally for auditability and transparency

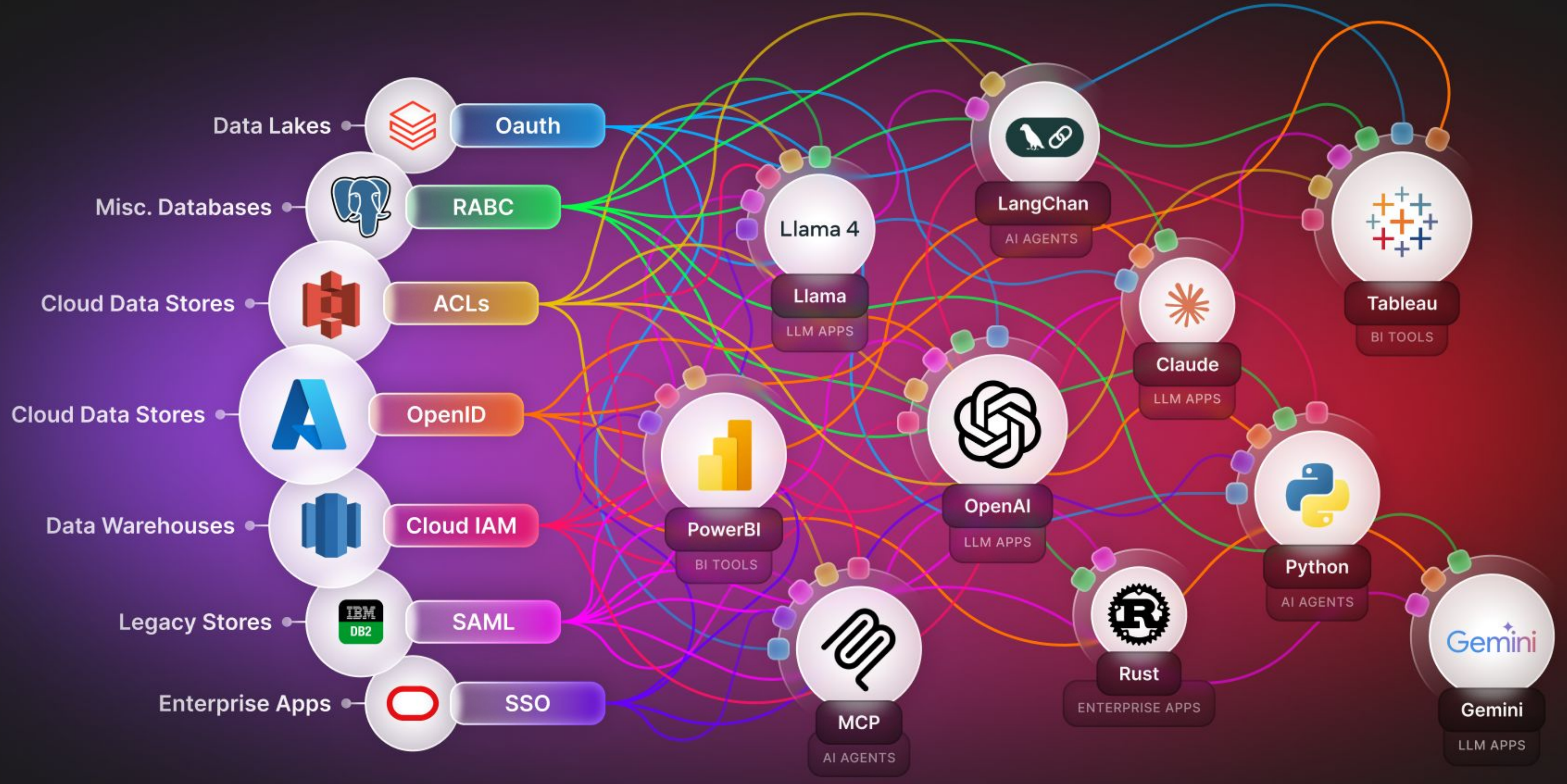
Applies policies on access — not after exposure

Customer Value Proposition

1. Accelerate innovation with sensitive data
2. Eliminate governance constraints
3. Improves data access & security processes
4. Simplify AI risk & compliance

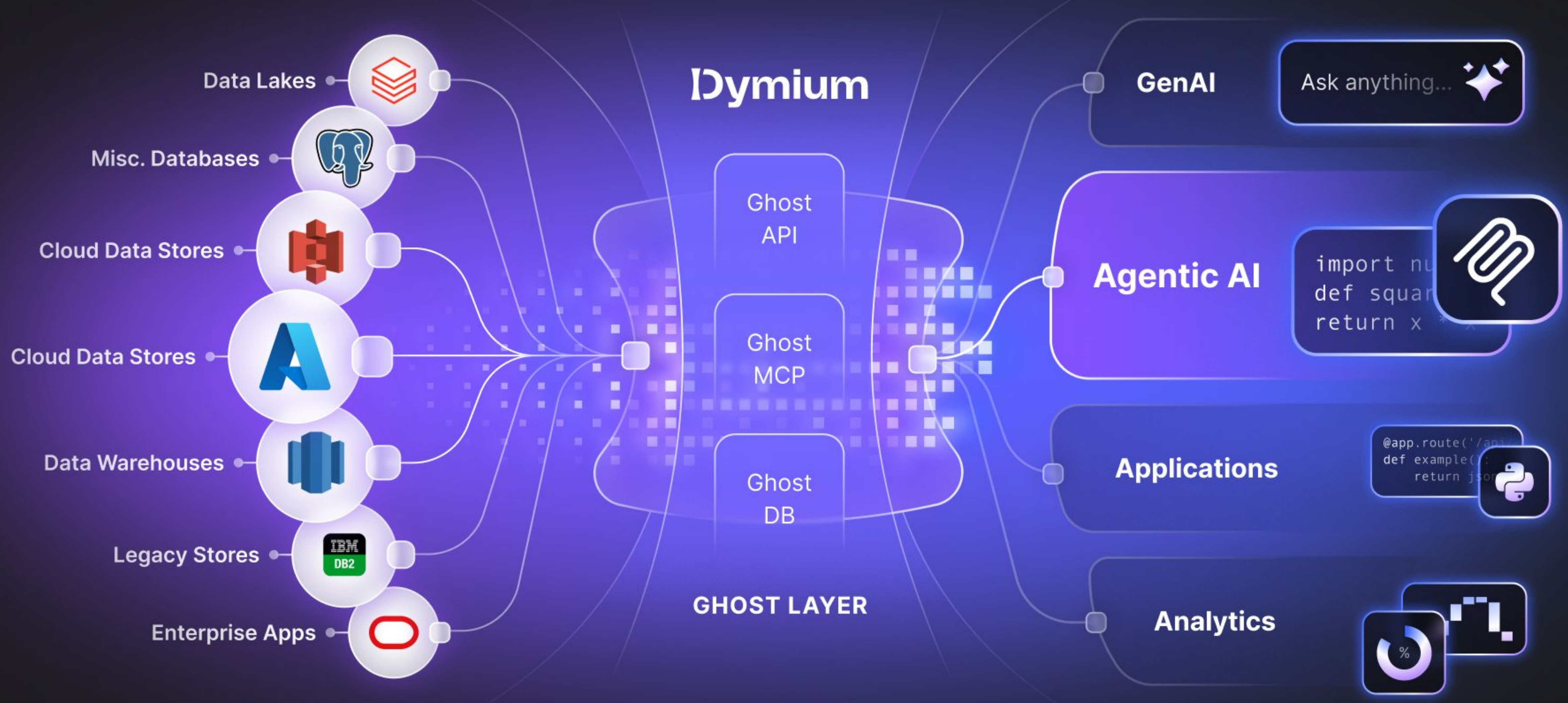
Complexity of Today's Landscape

Complex, fragmented, and hard to control.

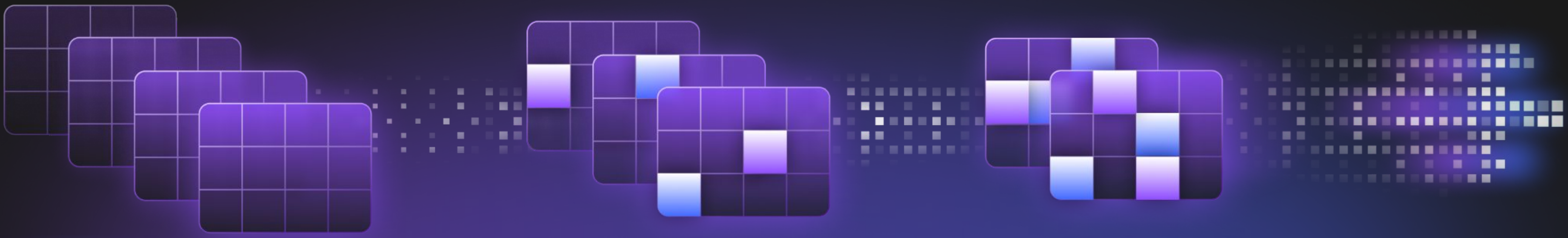


The Ghost Layer:

A New Way to Govern Data Access



One Layer. Three Ghosts.



Ghost DB

A governed SQL interface backed by live transformations and policy

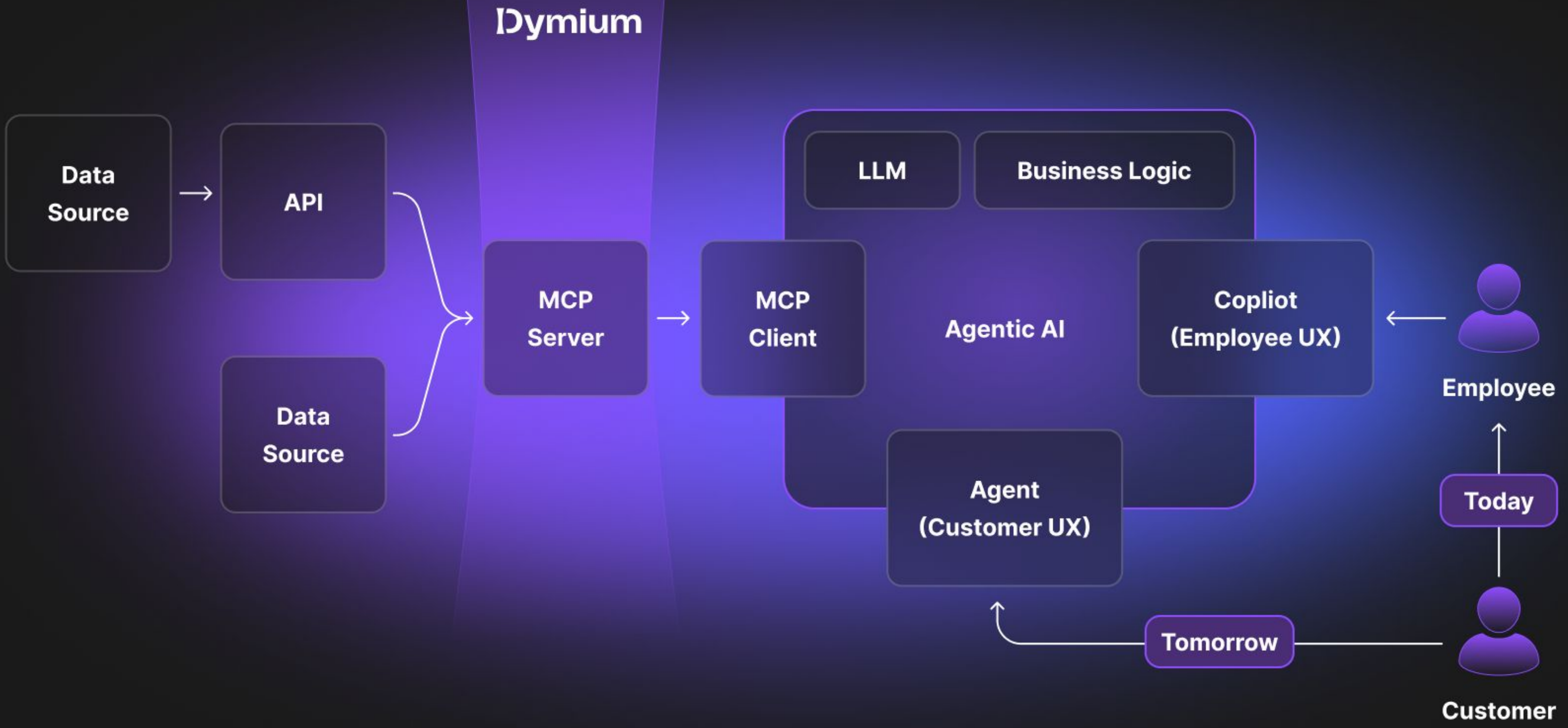
Ghost API

A RESTful endpoint for partner systems, apps, and integrations

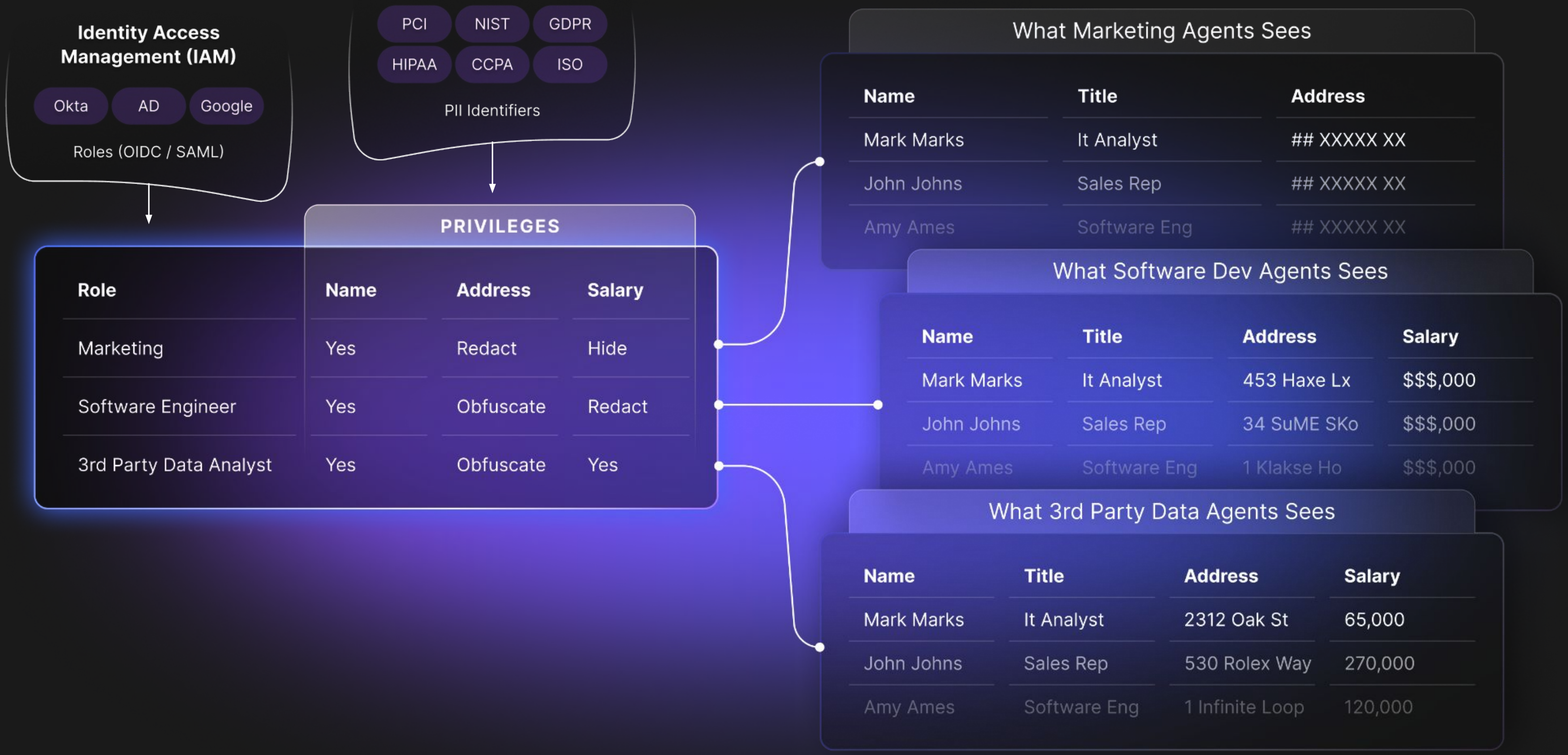
Ghost MCP

A secure stream for AI agents and copilots — real-time policy per request

Ghost MCP: Real-Time Interference Governance



Roles & Policies for Confidential AI



Identity Access Management (IAM)

Okta · AD · Google

Roles (OIDC / SAML)

PCI · NIST · GDPR · HIPAA · CCPA · ISO

PII Identifiers

PRIVILEGES

Role	Name	Address	Salary
Marketing	Yes	Redact	Hide
Software Engineer	Yes	Obfuscate	Redact
3rd Party Data Analyst	Yes	Obfuscate	Yes

What Marketing Agents Sees

Name	Title	Address
Mark Marks	It Analyst	## XXXXX XX
John Johns	Sales Rep	## XXXXX XX
Amy Ames	Software Eng	## XXXXX XX

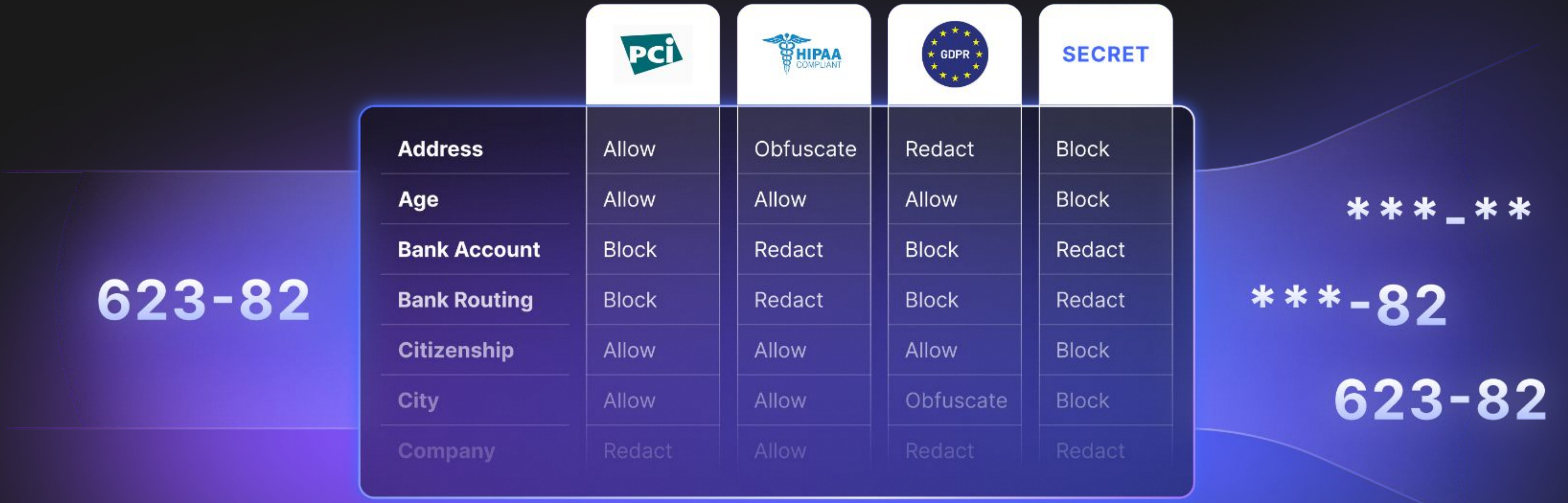
What Software Dev Agents Sees

Name	Title	Address	Salary
Mark Marks	It Analyst	453 Haxe Lx	$$$,000
John Johns	Sales Rep	34 SuME SKo	$$$,000
Amy Ames	Software Eng	1 Klakse Ho	$$$,000

What 3rd Party Data Agents Sees

Name	Title	Address	Salary
Mark Marks	It Analyst	2312 Oak St	65,000
John Johns	Sales Rep	530 Rolex Way	270,000
Amy Ames	Software Eng	1 Infinite Loop	120,000

Data Access & Governance via Neural Layer



	PCi	HIPAA COMPLIANT	GDPR	SECRET
Address	Allow	Obfuscate	Redact	Block
Age	Allow	Allow	Allow	Block
Bank Account	Block	Redact	Block	Redact
Bank Routing	Block	Redact	Block	Redact
Citizenship	Allow	Allow	Allow	Block
City	Allow	Allow	Obfuscate	Block
Company	Redact	Allow	Redact	Redact

Automatically discovers sensitive data

Applies policies per role, field, and purpose

Enforces access in real time

Broad Use Case Coverage

AI

- ✓ Prevents over-permissioned AI data access
- ✓ Blocks AI agents from seeing sensitive fields
- ✓ Audits all autonomous data interactions

Applications

- ✓ Protects data shared via apps and APIs
- ✓ Masks sensitive fields before external use
- ✓ Tracks and audits all data sharing activities

Analytics

- ✓ Limits reporting tools to only approved data
- ✓ Redacts private fields for compliance
- ✓ Eliminates risky data copies for BI access

Dymium

Let's Connect!

AI moves fast.
Make Security Your AI accelerator.

For more information, contact:

Denzil Wessels
CEO & Founder

✉ Denzil@dymium.io