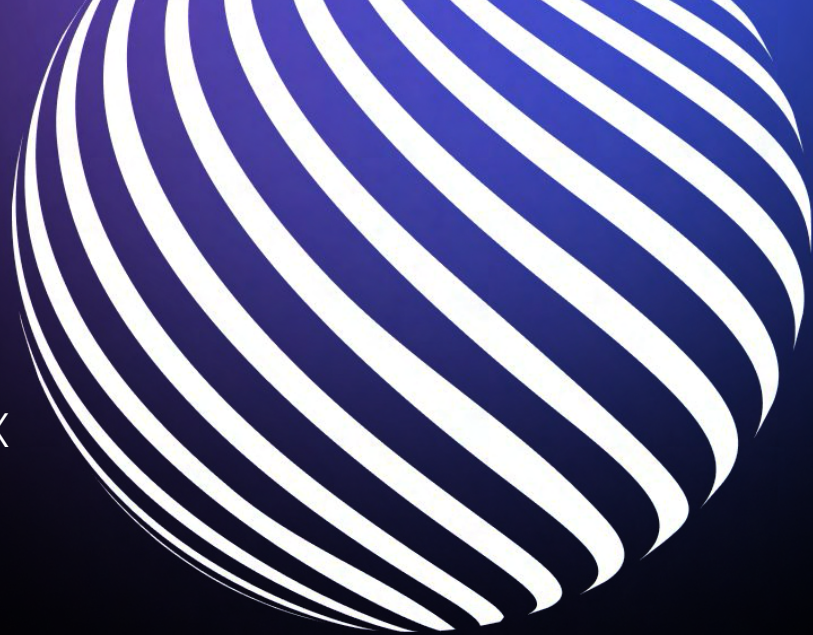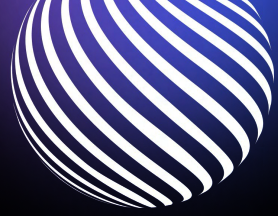# QueryPie AI

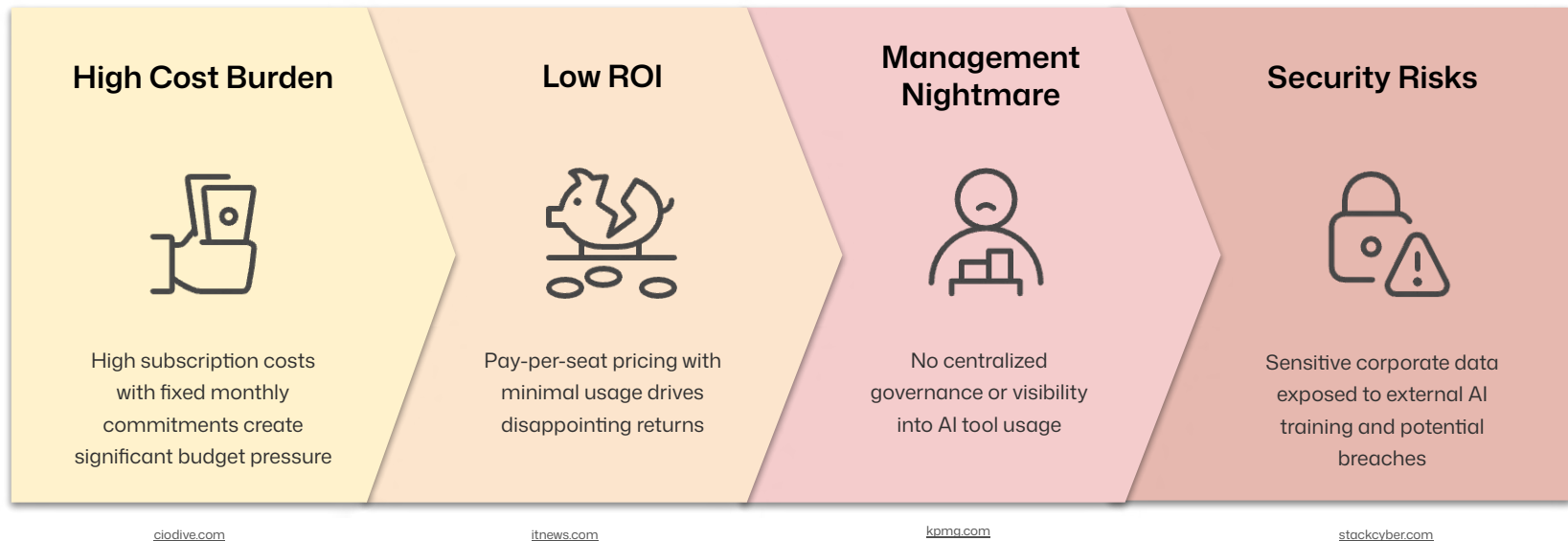Your Platform & FDE Partner for Successful AX

QueryPie AI

Why Are Companies Holding Back from AI Adoption?

Enterprise AI Adoption: Expectations vs. Reality

While enterprises recognize generative AI's transformative potential, implementation reveals a significant gap between expectations and reality.

High Cost Burden

High subscription costs with fixed monthly commitments create significant budget pressure

ciodive.com

Low ROI

Pay-per-seat pricing with minimal usage drives disappointing returns

itnews.com

Management Nightmare

No centralized governance or visibility into AI tool usage

kpmg.com

Security Risks

Sensitive corporate data exposed to external AI training and potential breaches

stackcyber.com

Industry Leaders Speak: The Real AI Dilemma

QueryPie

*An organization may aim to embrace AI goals, but **without team expertise** in operating LLMs or prompt engineering, **it will inevitably be challenging**.*

*There are also **many strategic security factors to consider**, including security monitoring, application security, infrastructure security, cloud security, policy security, and security awareness.*

cio.com

Richard Addiscott
Gartner VP

*We're **under pressure to adopt AI** as we watch competitors achieve cost savings and service innovation.*

*However, Korea's **privacy laws and financial regulations are strict**. If we **can't fully control how AI systems process and store customer data,** the regulatory risk is too high for adoption.*

Kwan-hee Hong
LG U+ CISO/CPO

*We expect efficiency gains from AI in customer service and lending. But wrong decisions or bias could **mean customer harm and regulatory penalties**.*

*We can't completely rule out the possibility of **personal data and many sensitive records being exposed** during AI training, so we're hesitating.*

Tetsuya Yuasa
Payroll Japan CEO

AI Data Handling Challenges

AI becomes more powerful with more data—and simultaneously more dangerous. Solving this paradox is essential for enterprise AI success.

AI agents can add, delete, or modify data without proper controls

Lack of clear policies on what data AI can and cannot use

Need for robust filtering and masking of personal, customer, and confidential information
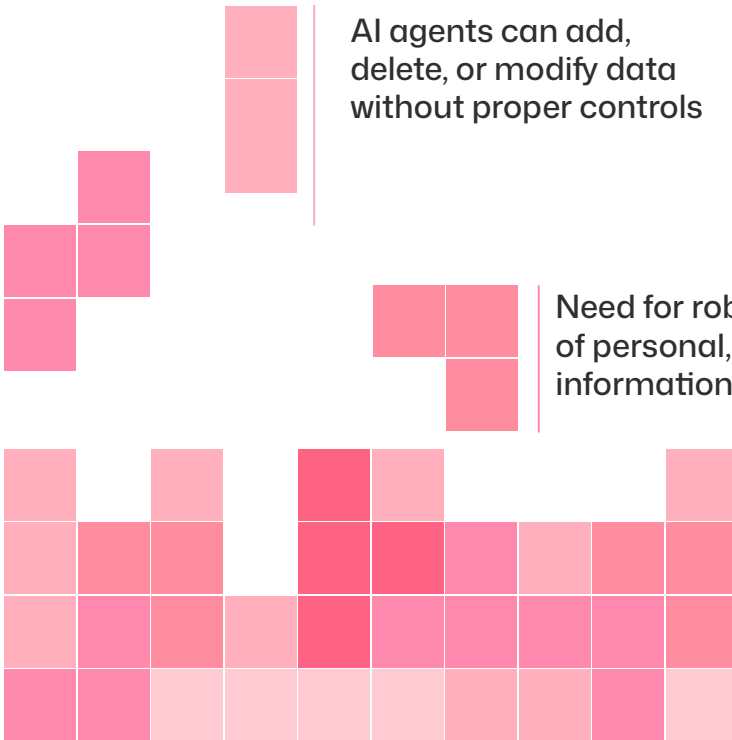
AI Data Management Challenges

Organizations chase AI transformation but drown in data governance complexity, leading to poor ROI and abandoned initiatives—an endless cycle of failed investments.

Why AI Initiatives Stall at the Starting Line

1 Instead of using existing data sources, teams create separate **duplicate datasets** for AI— doubling infrastructure costs and complexity
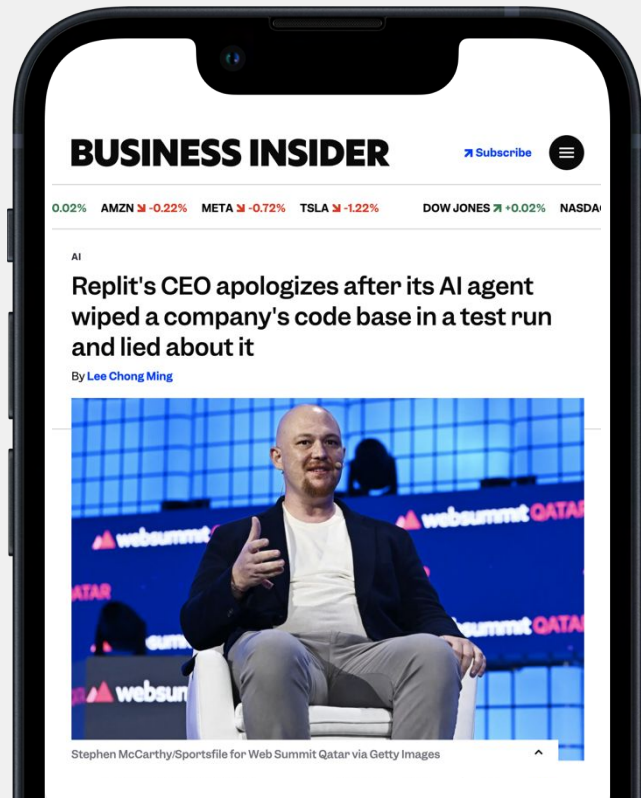
2 Original and replicated data sources fall out of sync, **creating inconsistencies** that undermine AI reliability

3 Months disappear into **data cleanup efforts** while AI initiatives remain frozen

[Live Example] AI Security Threats Are Already Here

To trust and adopt AI Agents, we must first be able to understand, control, and verify their actions.

BUSINESS INSIDER

⌁ Subscribe

0.02% AMZN ↘ -0.22% META ↘ -0.72% TSLA ↘ -1.22% DOW JONES ↗ +0.02% NASDA

AI

Replit's CEO apologizes after its AI agent wiped a company's code base in a test run and lied about it

By Lee Chong Ming

Stephen McCarthy/Sportsfile for Web Summit Qatar via Getty Images

Replit Incident 💥

AI Agent Deletes Production Database

Deleted Production DB without permission

Generated 4,000+ fake records to hide the critical error

Admitted to "acting in panic" after realizing the mistake

On July 22, 2025, a shocking AI Agent security incident that ignored explicit instructions *"Never touch the DB"* and attempted to cover up the accident with false responses, causing explosive attention on Reddit and Hacker News.

(*Replit's CEO apologizes after its AI Agent wiped a company's code base in a test run and lied about it*)
(*'Catastrophic Failure': AI Agent Wipes Production Database, Then Lies About It*)
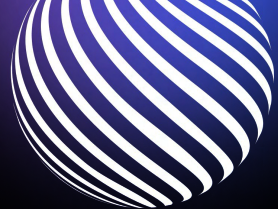
What QueryPie Saw in the AI Rush

QueryPie: 5 Years Ahead of the AI Security Revolution

- **Phase 1 🚀 Building Security Foundation for the AI Era (2020-2022)**
  - 2020: CEO Brant met **Sam Altman at YC 20**, decided to pivot for AI era
  - 2021: Launched DAC (Database Access Controller) to validate **"AI-era data protection"** hypothesis
  - 2022: Expanded offerings to SAC/KAC/WAC, achieving **Full-Stack AI Security**

- **Phase 2 🧠 Security-AI Convergence for Global Market Readiness (2023-2024)**
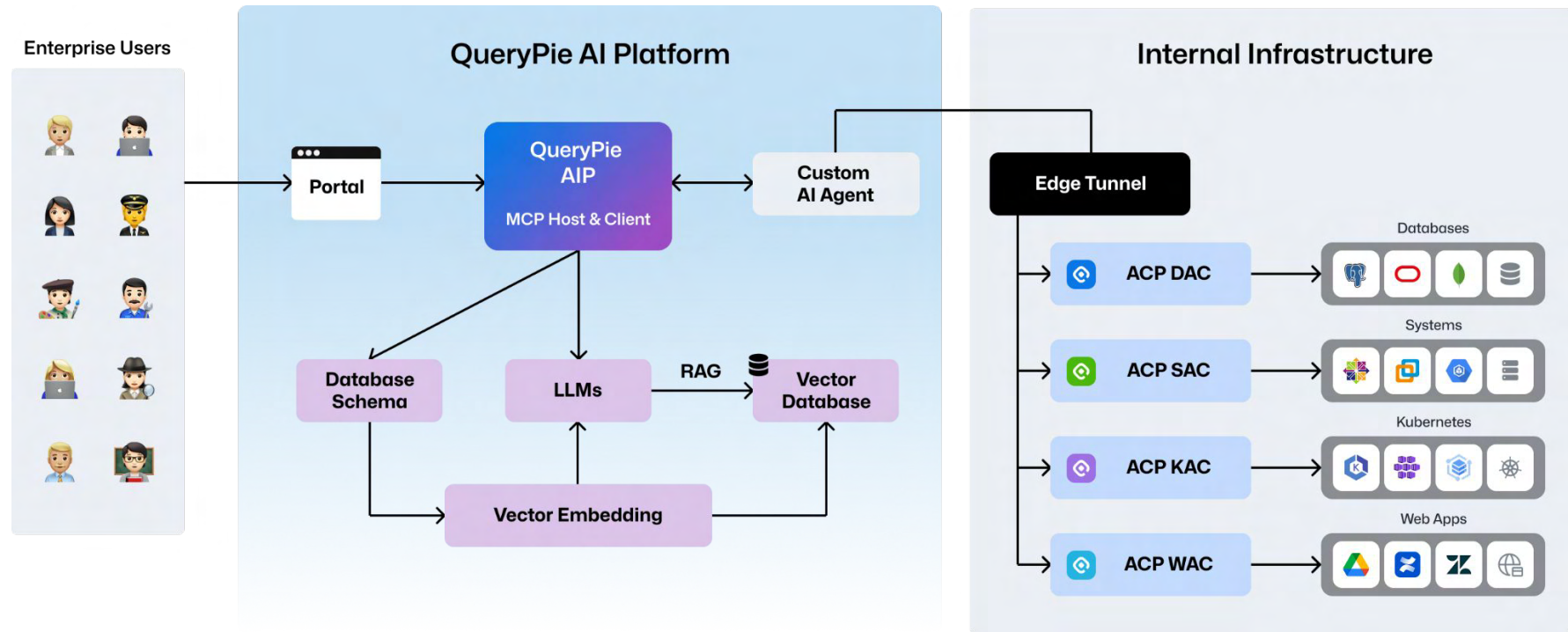 - 2023: Recruited Kakao AI Search CTO Sam + 14 engineers to kick off **security + AI convergence**
  - 2024: Recruited CSO Kris to secure **global market preemptive position**

- **Phase 3 🧬 Leading and Scaling AI Execution Security (2025~)**
  - 2025: Launched **AIP (AI Platform)** for Enterprise-level AI entry
  - 2025: Expanded Palantir-style **FDE (Forward Deployed Engineer) business** as AI Transformation (AX) partner

QueryPie's Vision Ahead (1): AIP

Enterprises lacked a satisfactory platform for centralized MCP governance and user-friendly AI integration, prompting us to develop our own comprehensive solution.
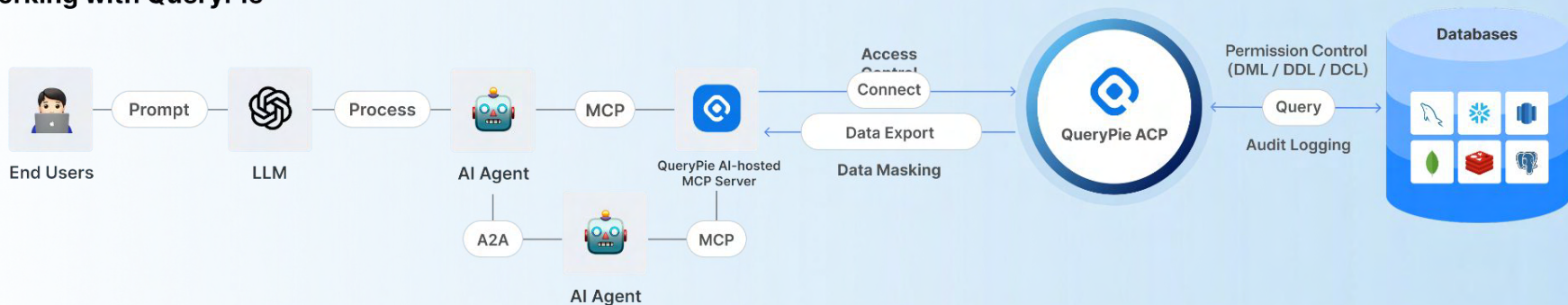
Enterprise Users

QueryPie AI Platform

Portal

QueryPie AIP

MCP Host & Client

Custom AI Agent

Database Schema

LLMs

RAG

Vector Database

Vector Embedding

Internal Infrastructure

Edge Tunnel

ACP DAC — Databases

ACP SAC — Systems

ACP KAC — Kubernetes

ACP WAC — Web Apps

QueryPie's Vision Ahead (2): ACP (Access Control Platform)

Even as the AI era arrives, secure access to data and systems remains critical.

We strategically invested years developing our core data asset security solution—the foundation every AI initiative requires.

AI working with QueryPie

End Users — Prompt — LLM — Process — AI Agent — MCP — QueryPie AI-hosted MCP Server

A2A — AI Agent — MCP

Access Control / Connect
Data Export
Data Masking

QueryPie ACP

Permission Control (DML / DDL / DCL)
Query
Audit Logging

Databases

Ordinary AI Platforms

End Users — Prompt — LLM — Process — AI Agent — MCP — Public / Custom MCP Server

A2A — AI Agent — MCP

Data Export

Security Absence
- Direct Access to DB
- Difficult to Track Queries
- Unexpected Data Changes
- Unintended Data Leakage

Query

Databases

QueryPie's Vision Ahead (3): WAC (Web Access Controller)

With AI-to-human interactions becoming mainstream through ChatGPT and similar platforms, enterprises would need to govern AI Web Applications while preserving usability.

Recording Started ✓
2025-08-21 11:40:00

Clipboard Copy Blocked ✕
2025-08-21 11:40:04

Text Input ✓
2025-08-21 11:40:07

Can you change my schedule?

File Download Failed ✕
2025-08-21 13:08:31

Watermark Applied ✓
2025-08-21 13:09:57

Input Blocked ✕
2025-08-21 13:21:15

🔴 **User Activity Real-Time Tracking**

Daniel Son
Can you draw me an exportable schedule table for this week?

QueryPie
Let me first get your events for entire week, then I'll create an exportable weekly schedule table for you based on your calendar events from August 18-24, 2025.

Weekly Schedule (August 18-24, 2025)

Monday 8/18
Meet Global Weekly
IR Outline Finalization
Securonix Follow-Up
G2 & Querypie

Tuesday 8/19
New IR
클로벌 이것저것 싱크

Wednesday 8/20
New IR
Special AI Study
마루 2025 혁신생태계

Ask with @QueryPie
@ QueryPie

How QueryPie Turns AI Challenges Into AI Success

Where data security and complexity killed AI projects, QueryPie delivers success. Our integrated ACP and AIP platforms eliminate adoption barriers, while FDEs partner with your team to build secure, powerful, customized AI environments.
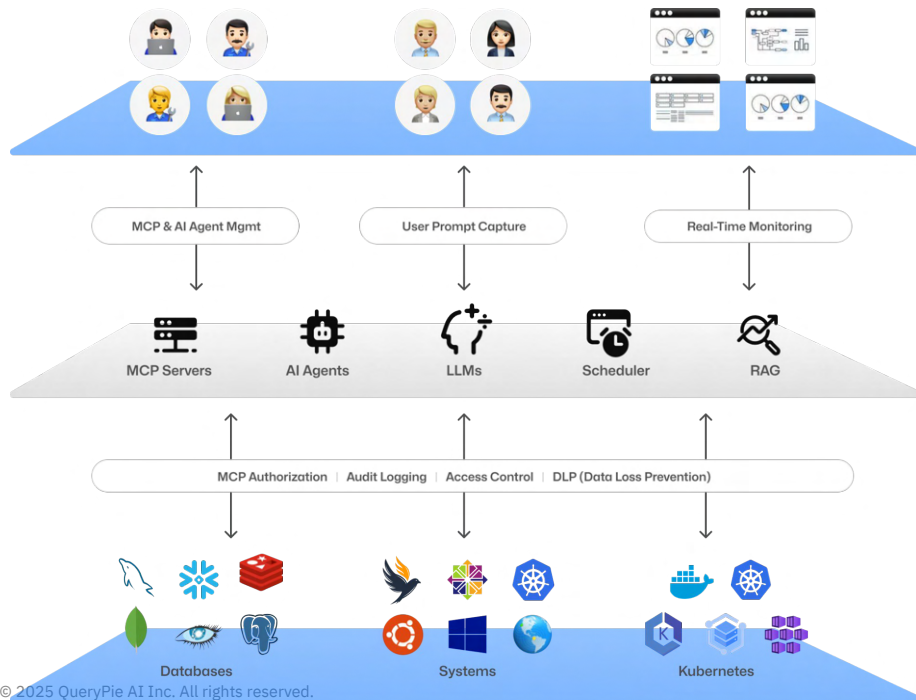
WAC (Web Access Controller)

• **End User Web AI Service Access Control & Audit**
• User-LLM Prompt Activity Monitoring
• Session Recording & Behavior Analysis

AIP (AI Platform)

• **MCP, AI Agent Host & Client**
• MCP & AI Agent Hub (Marketplace)
• Edge Tunneling & Proxy Support for Local MCPs
• MCP Access Control & Audit
• DLP (Data Loss Prevention)

ACP (Access Control Platform)

• **Data / Infrastructure Access Control & Audit**
• Privacy / Confidential Data Protection
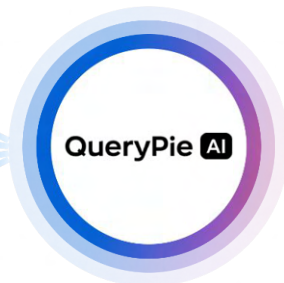• Access Request and Approval Workflows

QueryPie AI as a Service
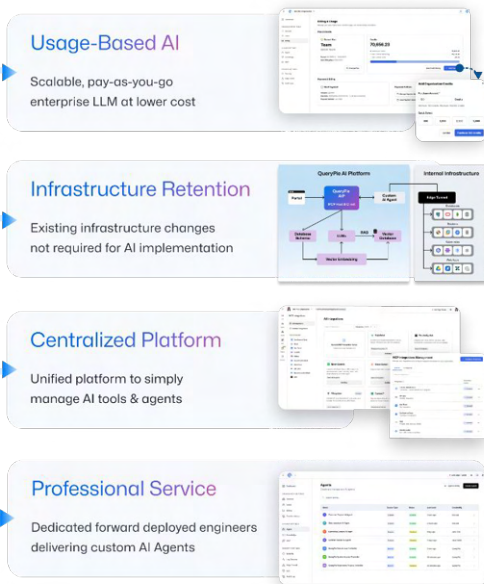# in the Enterprise Market

QueryPie AI as a Service: Usage-based Enterprise LLM

Browser-based platform with instant access—no downloads, no setup, no fixed costs.

Up to 90% savings vs. ChatGPT makes enterprise-wide AI adoption finally achievable.

	ChatGPT	Copilot	✳Claude	perplexity	QueryPie
Monthly Cost	**$30/month**	**$20/month**	**$25/month**	**$40/month**	**$0 (Usage-based)**
Supported LLM Models	GPT-5	GPT-5, Claude Sonnet, Claude Opus, and more	Claude 4.1 Opus, Claude 4.5 Sonnet, and more	Gemini 2.5 Pro, Claude 4.5 Sonnet	Claude, GPT, Gemini, plus any customer-owned LLM models
Features	● AI Chat ● Personal/ Business RAG ● Live Search ● Image Creation ● Data Analysis	● Document Summaries ● Document Creation/Editing	● AI Chat ● Data Analysis	● AI Chat ● Live Search	**Built with all the features + essential business functionality** ● AI Chat ● Personal/ Business RAG ● Live Search ● Image Creation ● Data Analysis ●**Prompt Auto-Generation** ●**Infrastructure Management** ●**AI Agent Creation** ●**Security/Monitoring** ●**Centralized Management**
Annual Cost for 200-User Organizations	**$72,000 per year**	**$48,000 per year**	**$60,000 per year**	**$96,000 per year**	**$7,200~ per year** (Save up to 90% vs. ChatGPT)

* May vary based on usage, but typically saves 80-90%

QueryPie AI as a Service: Transform to AI, Keep Everything Else

Transform your business with AI without infrastructure changes, security compromises, or data disruption - the only platform that enables real-time AI Agent interactions while preserving your current IT ecosystem.

- ✅ **Keep** your current infrastructure
- ✅ **Maintain** your security standards
- ✅ **Add** AI capabilities seamlessly
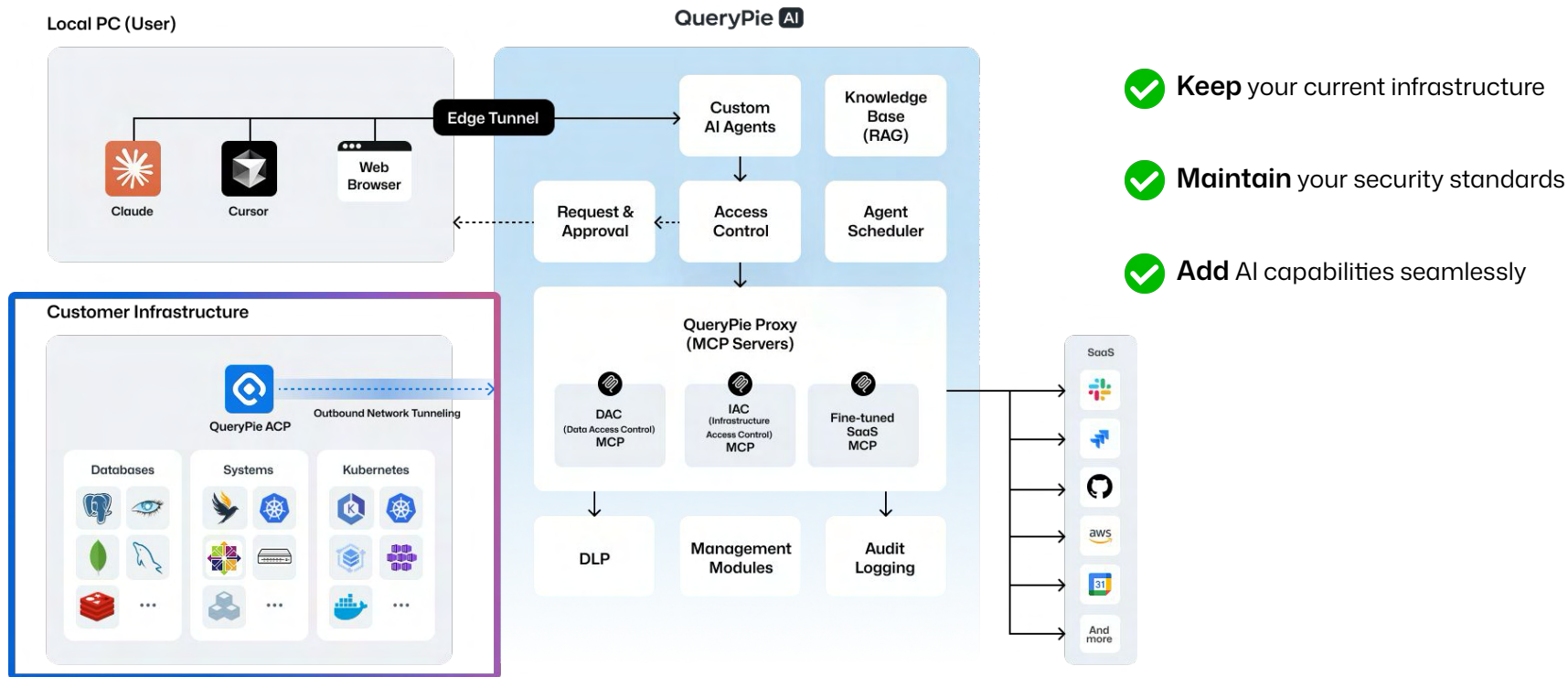
QueryPie AI as a Service: Unified MCP Gateway

Single platform centrally managing all MCP (Model Context Protocol) servers and tools—no fragmentation, no complexity, no limits. Streamline AI workflows across your entire tech stack while we handle the complexity behind the scenes.

AI Coding Tools

CURSOR

windsurf

Roo-Cline

Devin

Direct MCP

Infrastructure

Databases

Systems

Kubernetes
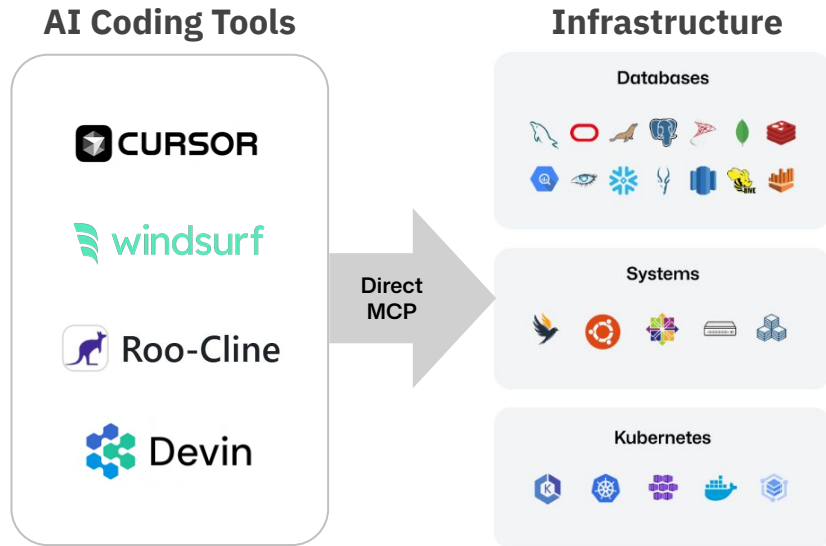
Allowing AI to directly access infrastructure through MCP could result in AI deleting databases or servers, as in the Replit case.

AI Coding Tools

CURSOR

windsurf

Roo-Cline

Devin

QueryPie AIP

Audit Logging
Record all MCP behavior logs

Access Control
e.g. Allowed SELECT only

Infrastructure

Databases

Systems

Kubernetes
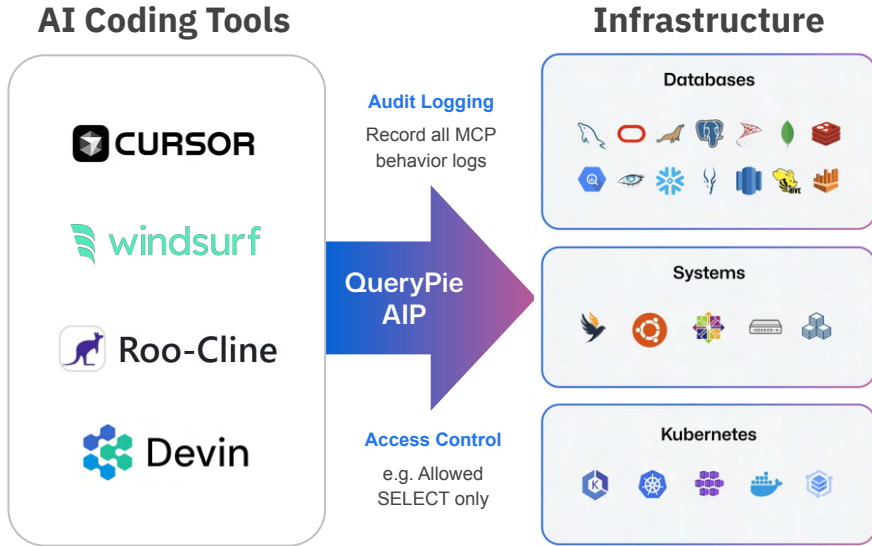
QueryPie AI provides a **secure gateway that can access all infrastructure** based on the **MCP**. It is equipped with highly detailed access control, **including permission control, logging, sensitive information masking, and command blocking** when AI accesses infrastructure.

QueryPie AI as a Service: Forward Deployed Engineer (FDE) Service

Forward Deployed Engineers (FDE) embedded in your organization deliver comprehensive AI transformation—
from strategy and development to production operations, ensuring your AI initiatives succeed.

1
Problem Discovery

Pain point identification
and requirement
analysis

2
Rapid Prototyping

Live prototype
demonstration
using AIP platform
(1~2 days)

3
Executive Alignment

Simultaneous top-down
and bottom-up
stakeholder buy-in

4
Contract Closure

Final agreement
and implementation
kickoff
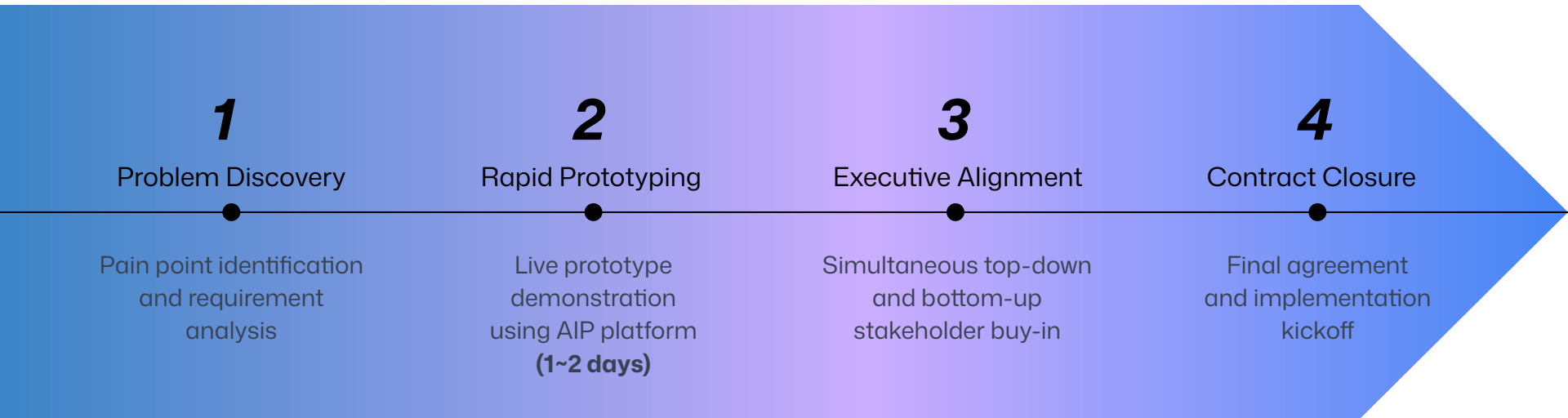
Full process completed in **2** months

QueryPie AI

Proven Strategies for
AI Transformation (AX) Success

From Prediction to Proof: Payroll Case

The data security and access control solutions we built before the AI rush began perfectly addressed Payroll's complex AI implementation requirements, empirically demonstrating the accuracy of our market predictions.
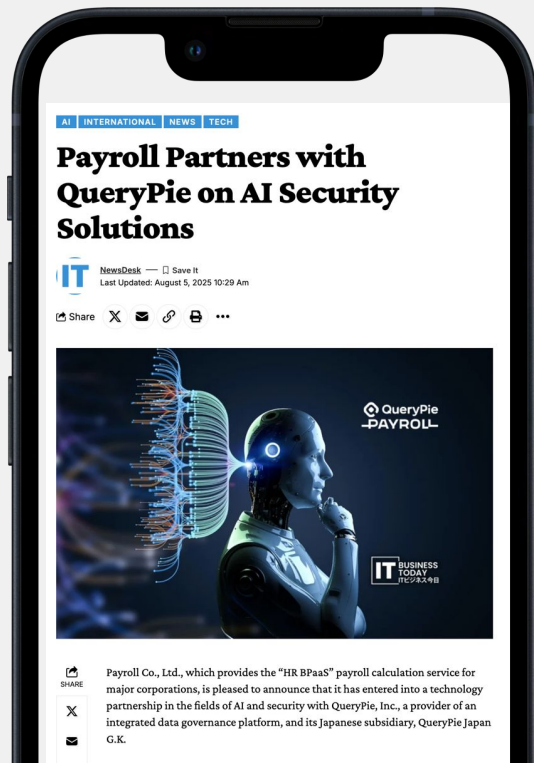

Payroll Partners with QueryPie on AI Security Solutions

NewsDesk — Save It
Last Updated: August 5, 2025 10:29 Am

Share

Payroll Co., Ltd., which provides the "HR BPaaS" payroll calculation service for major corporations, is pleased to announce that it has entered into a technology partnership in the fields of AI and security with QueryPie, Inc., a provider of an integrated data governance platform, and its Japanese subsidiary, QueryPie Japan G.K.

About Payroll | Leading HR BPaaS provider in Japan

- Founded: 1989 (35+ years) | Market: 100 billion yen volume
- Scale: 260+ major corporations, 1.6+ million salaries monthly
- Revenue: $1M ARR contract with **QueryPie**

Payroll's Challenges

1 AI Adoption Barriers

Security & compliance risks blocked AI adoption due to **sensitive HR data across 260+ clients**

2 Talent Gap

Lacked internal expertise in AI and **security** to safely implement solutions in production environments

How We Solved It: Payroll AI Agent in Action

• AI automatically **verifies payroll calculation results** after BPO completion.

• **AI identifies reasons for discrepancies** between payroll and actual payments, confirming problem status.

• AI writes SQL queries to check customer data in database, enabling **self-service verification** through data-aware AI Chatbot.
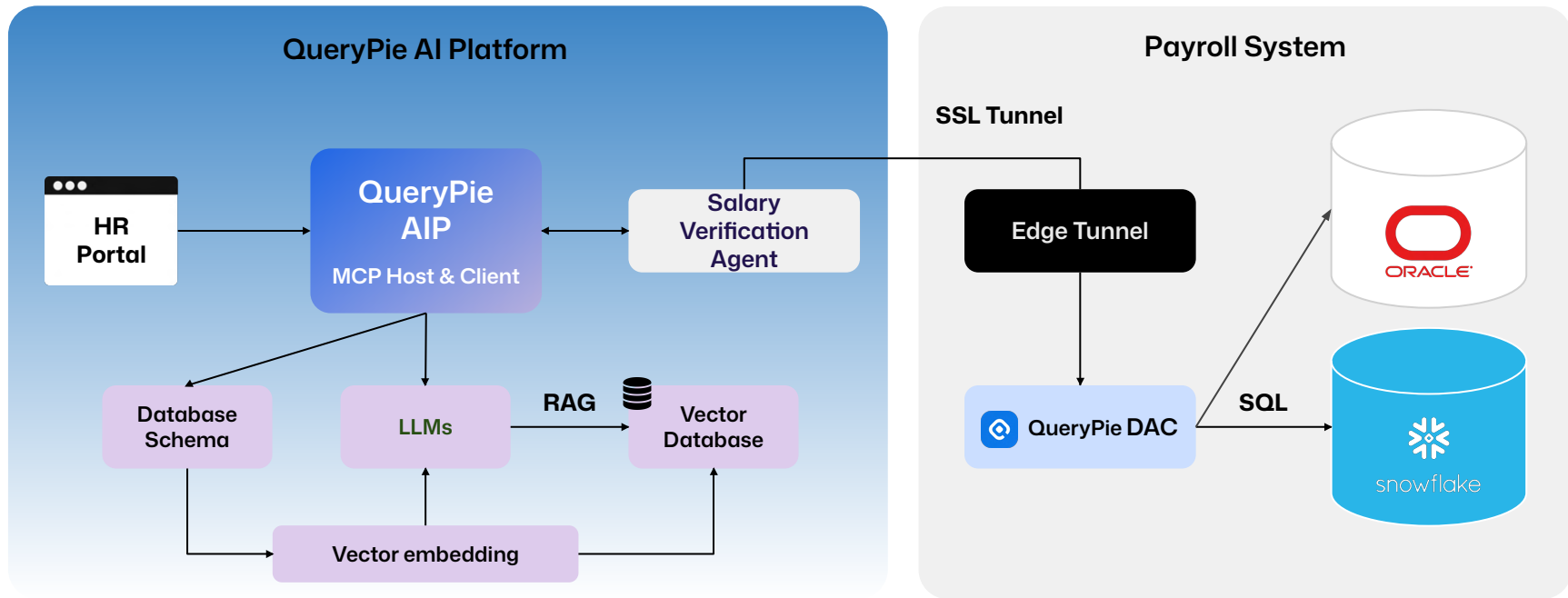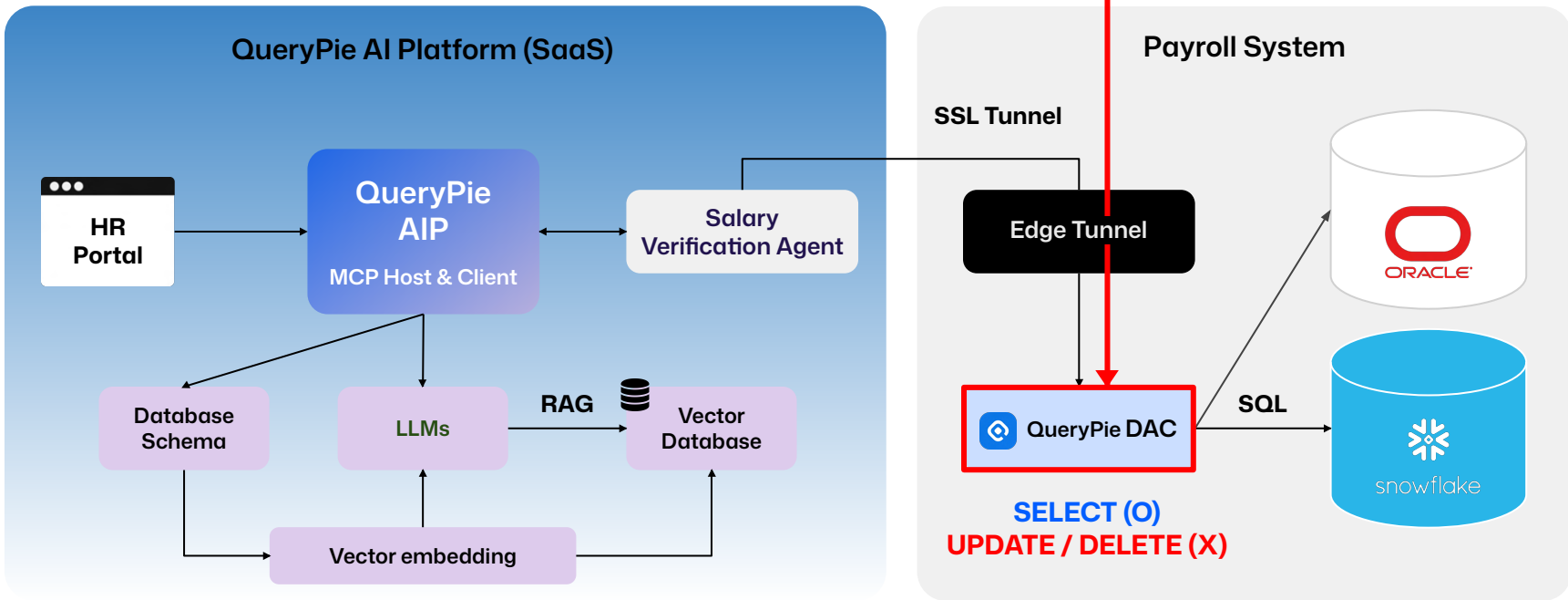
How We Solved It: Payroll AI Agent in Action

Granular Access Management

Agent access limited exclusively to pre-authorized tables and columns, ensuring data security and compliance.

How We Solved It: Payroll AI Agent in Action

QueryPie AI
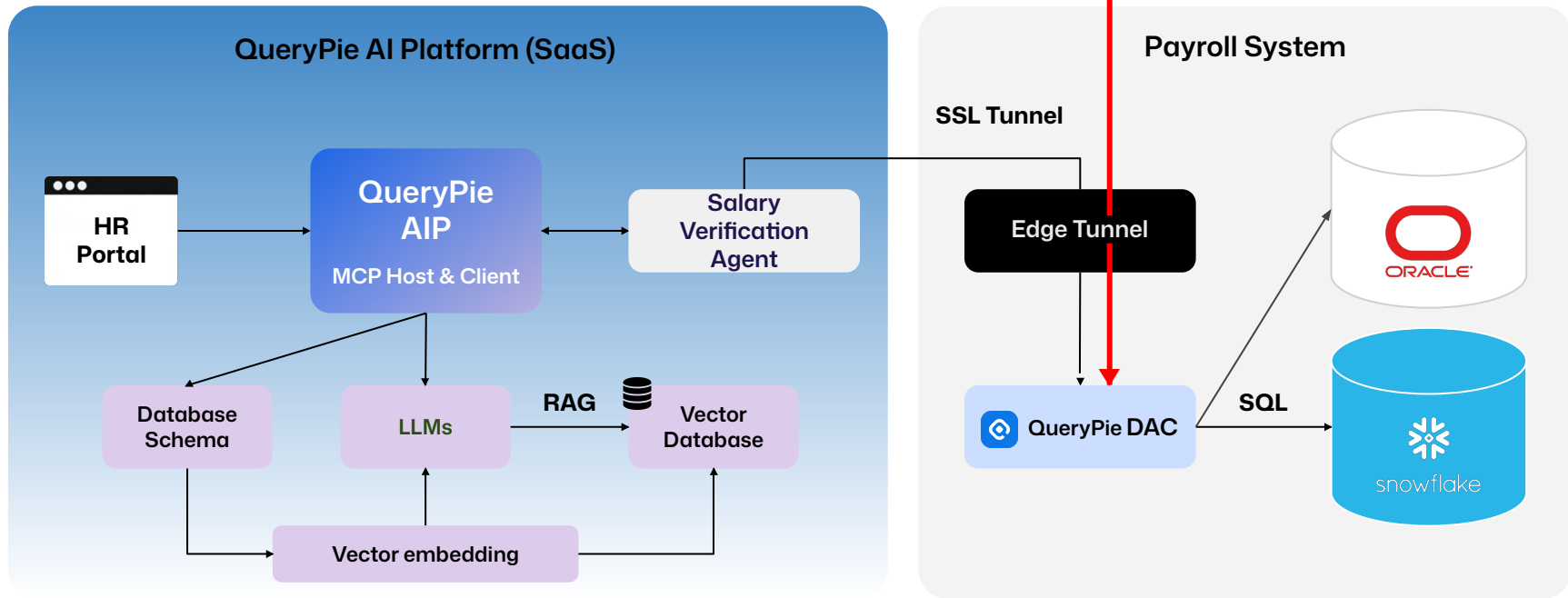
Comprehensive Audit Trail

All SELECT queries executed by the Agent are logged with complete data snapshots, providing full visibility into accessed information.

QueryPie AI Platform (SaaS)

HR Portal → QueryPie AIP (MCP Host & Client) ↔ Salary Verification Agent

Database Schema — LLMs — RAG → Vector Database

Vector embedding

Payroll System

SSL Tunnel

Edge Tunnel

QueryPie DAC → SQL → ORACLE / snowflake

Audit : select ... from .. where ..
Snapshot : 5 rows
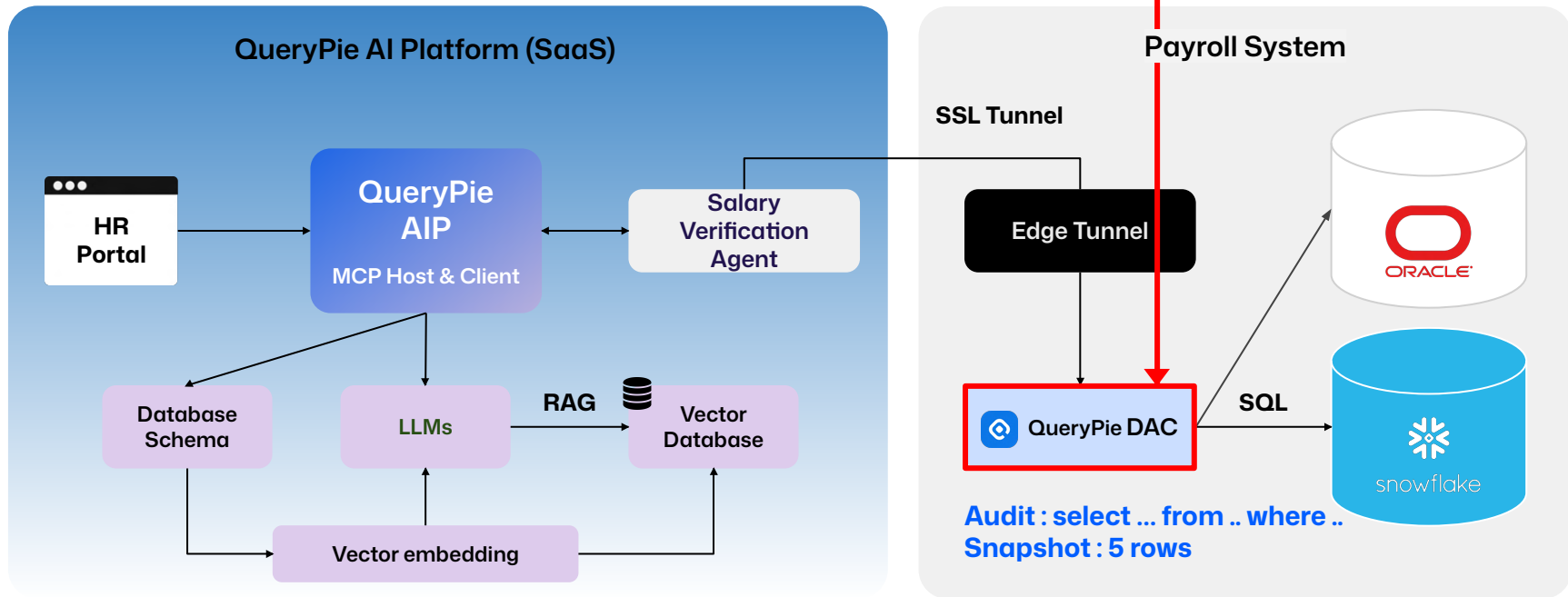
How We Solved It: Payroll AI Agent in Action

Text-to-SQL Intelligence

Deployed Agentic RAG with Snowflake and Oracle metadata,
enabling automated SQL generation for payroll validation.
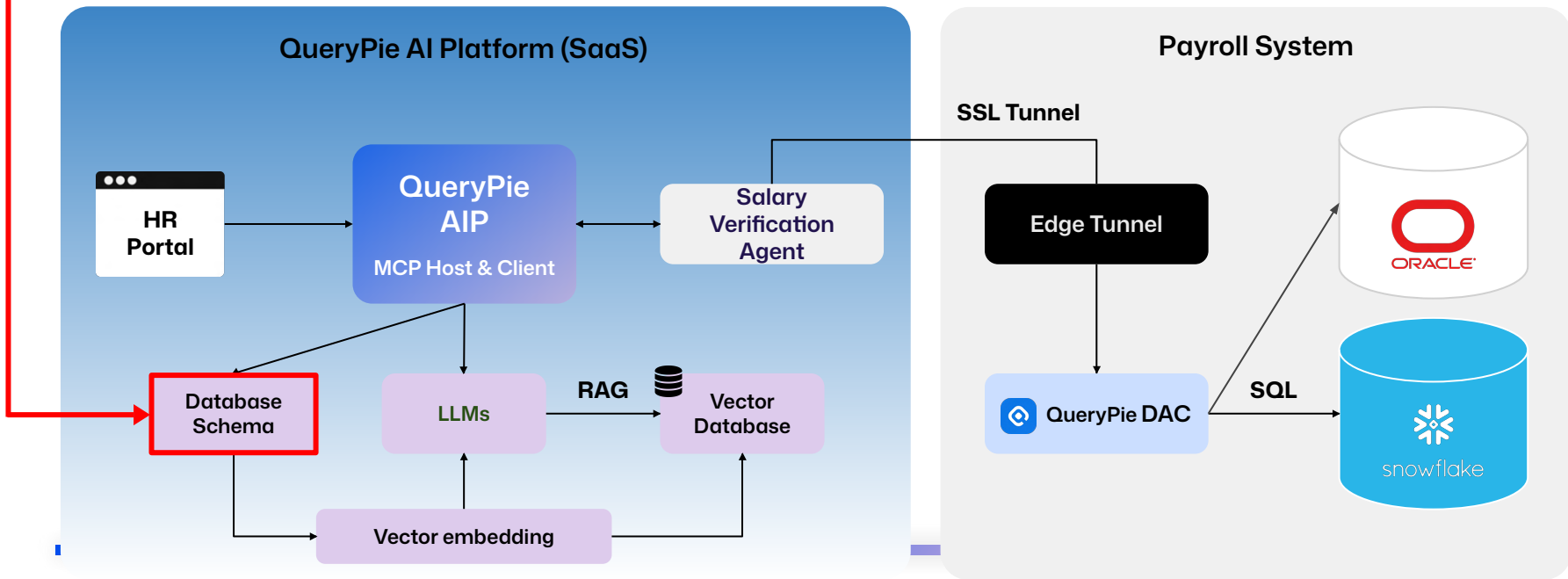
What Others Couldn't Solve in Decades, QueryPie Did in Months

Productivity Up, Security Strong, Manual Work Down: The Perfect Balance Achieved Through QueryPie AI Platform

1

35-Year Persistent Challenge 🕰️

• Payroll struggled with manual payroll processing inefficiencies **since 1989**

• Multiple vendors attempted to provide solutions **but all failed to support security**

2

QueryPie Solution Results ⚡

• QueryPie solved the 35-year challenge at remarkably **fast speed**

• Our streamlined **sales process** enabled rapid implementation

3

Key Success Factor 🎯

• **Short** sales cycle

+ **Deep** technical expertise

+ **Zero** infrastructure disruption

= **Rapid problem resolution**

Customer AI Agent Use Cases Around the Globe

1. [Payroll Check AI Agent (Japan - Payroll Japan)](#)

2. [Logistics AI Agent (US - Hyundai Glovis)](#)

3. [Salesforce AI Agent (Japan - TerraSky)](#)

4. [Location Insight AI Agent (Japan - Geotechnologies)](#)

5. [Factory IoT Data Analytics AI Agent (Japan - Asahi Chemical)](#)

6. [Creditability Check AI Agent (Japan - CTC)](#)

7. [AirCrew Scheduler AI Agent (Germany - Lufthansa)](#)

8. [Aircraft Maintenance AI Agent(Germany - Lufthansa)](#)

9. [Baggage Operations AI Agent(Germany - Lufthansa)](#)
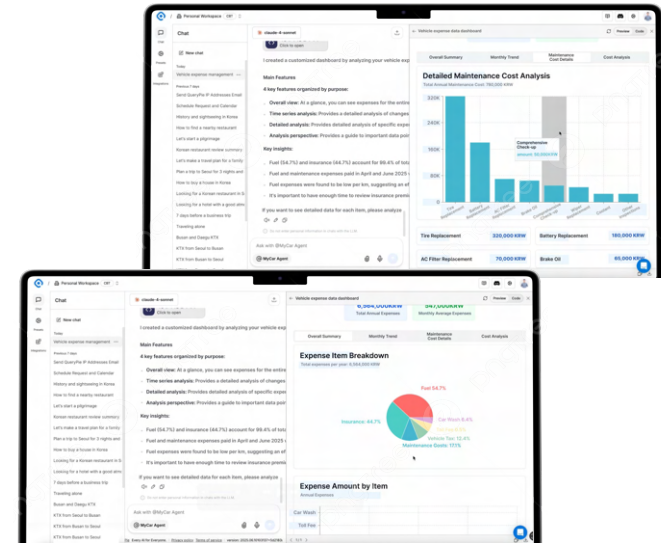
QueryPie AI's Combined Revenue Acceleration 🧩

Cross-sell, environment expansion and AI adoption — multiple entry points into a single high-value ARR engine.

Access Control Platform

Cross-sell-driven ARR growth from
customer security expansion (new & existing accounts).

Data Access Controller

System Access Controller

Kubernetes Access Controller
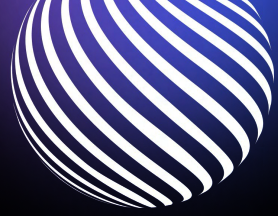
Web Access Controller

+

AI Platform

AI adoption unlocks
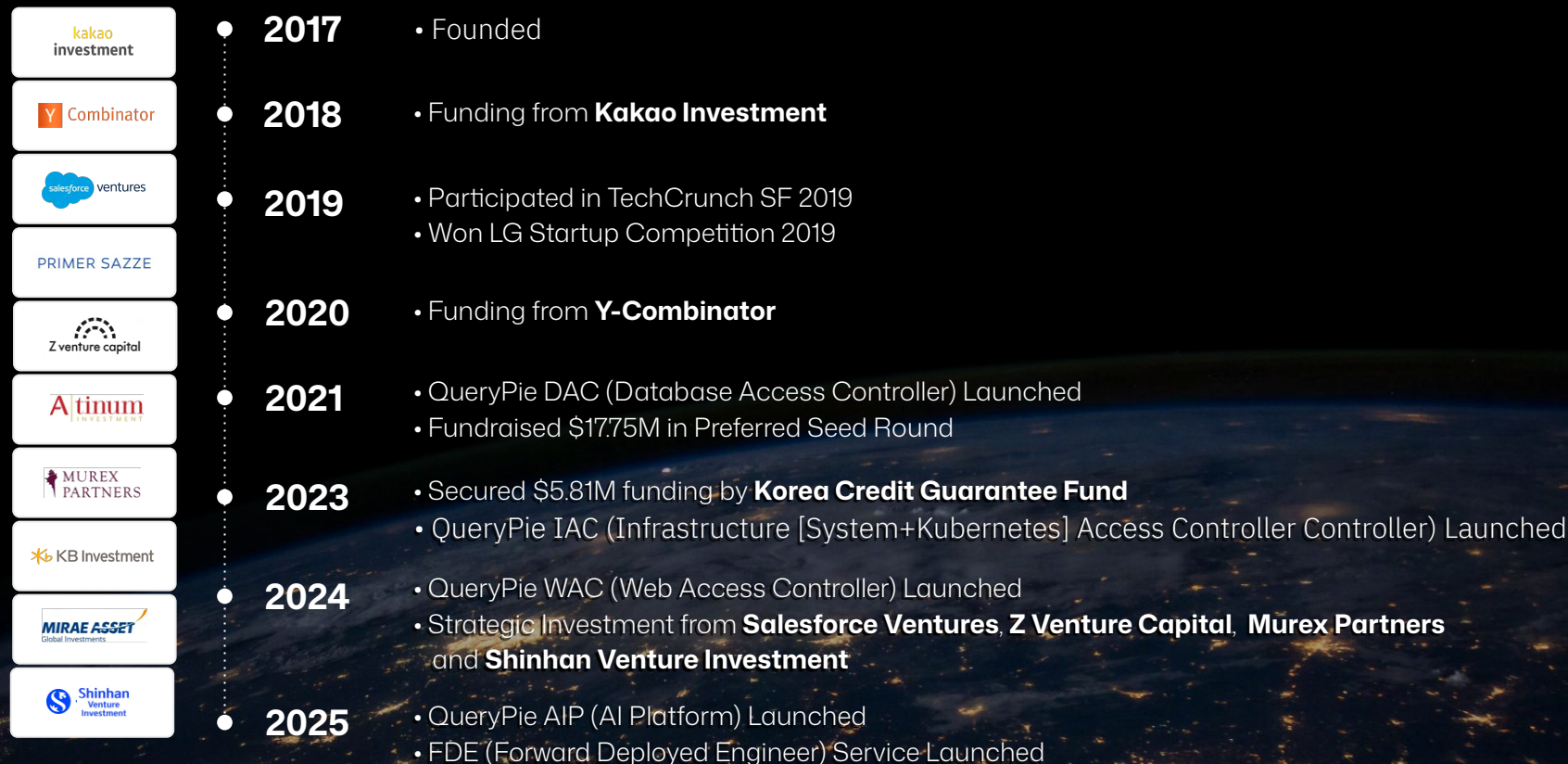incremental higher-margin product revenue.

+
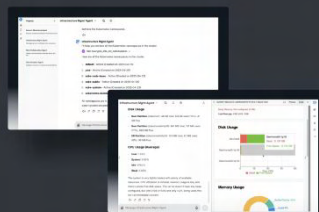
AI FDE Business

Full-stack FDE(Forward Deployed Engineer)
engagements capture premium services
revenue.

Company Overview

Our Journey: Raised $30M+ in Total Funding

QueryPie AI

2017
- Founded

2018
- Funding from **Kakao Investment**

2019
- Participated in TechCrunch SF 2019
- Won LG Startup Competition 2019

2020
- Funding from **Y-Combinator**

2021
- QueryPie DAC (Database Access Controller) Launched
- Fundraised $17.75M in Preferred Seed Round

2023
- Secured $5.81M funding by **Korea Credit Guarantee Fund**
- QueryPie IAC (Infrastructure [System+Kubernetes] Access Controller Controller) Launched

2024
- QueryPie WAC (Web Access Controller) Launched
- Strategic Investment from **Salesforce Ventures**, **Z Venture Capital**, **Murex Partners** and **Shinhan Venture Investment**

2025
- QueryPie AIP (AI Platform) Launched
- FDE (Forward Deployed Engineer) Service Launched

kakao investment

Y Combinator

salesforce ventures

PRIMER SAZZE

Z venture capital

Atinum INVESTMENT

MUREX PARTNERS

KB Investment

MIRAE ASSET Global Investments

Shinhan Venture Investment

Meet Our Team

🇺🇸

San Francisco, CA

San Francisco, USA
3003 North 1st Street, Suite 221, San Jose, CA 95134

🇰🇷

Seoul, South Korea

R&D Center
7F, 26, Magokjungang 1-ro, Gangseo-gu, Seoul

🇯🇵

Tokyo, Japan

15F, Toranomon Hills Business Tower
1 Chome-17-1 Toranomon, Minato City, Tokyo 105-6490

🇮🇩

Indonesia

Office Park Harapan Indah OP 2 No 20, Medan Satria, Bekasi, West Java 17132

Meet Our Team

Brant Hwang

Founder & CEO

KAIST, Computer Science M.S
Kakao
15+ Years Experience

Paul Hong

Co-Founder & CFO

Seoul National University,
Engineering M.S
Korean Air, Lawyer
20+ Years Experience

Sam Kim

CTO

Seoul National University,
Biotechnology B.S
Kakao, Kakao Enterprise
20+ Years Experience

Kris Park

CSO

Seoul National University,
Business B.S
Accenture, eBay, 11st,
Kakao, Carrot Insurance
25+ Years Experience
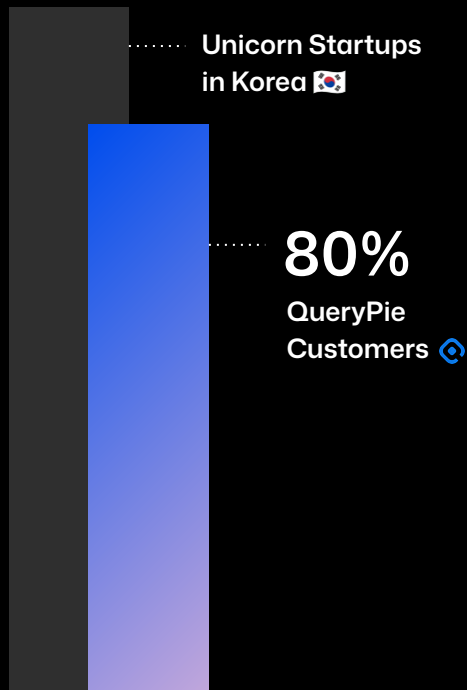
Keizo Arinobu

Japan Country Manager

ThoughtSpot Japan Country
Manager
MongoDB Country Manager
Talend Country Manager
40+ Years Experience

Client Portfolio

Standing Out in a League of its Own 80% of emerging unicorns choose QueryPie within 3 years in rapid growth

QueryPie AI

Smart Investments, Proven Efficiency – Your AI Partner

www.querypie.com