



PROPHIX ONE INTELLIGENCE:

AI Security and Architecture Brief



Executive Summary

Today, finance teams face increasing complexity, change, and pressure to deliver insights faster – without compromising trust in their data. Prophix One Intelligence meets that need by embedding secure, explainable artificial intelligence within the Prophix One platform to enhance decision-making, automation, and accuracy.

Built on the same rigorous software quality and principles that define every Prophix product, Prophix One Intelligence delivers accurate, secure, and private AI that empowers the office of the CFO while protecting enterprise data.





Prophix One Intelligence is the AI engine powering the Prophix One platform, enhancing the financial performance management lifecycle with secure and governed artificial intelligence. This capability can be turned on or off based on organizational policy.

It leverages managed Large Language Models (LLMs) through AWS Bedrock to deliver secure, scalable, and compliant AI capabilities. These capabilities work together to deliver a comprehensive, role-aware AI ecosystem within Prophix One.

Type	Purpose
Agentic Intelligence	Executes finance workflows via intelligent Agents (Budgeting, Reporting, Reconciliation), using natural language and governed automation.
Applied Intelligence	Delivers intelligent automation across financial processes to enhance accuracy, control, and operational efficiency.
Generative Intelligence	Produces narrative insights, reports, and visual summaries derived from structured financial data.
Conversational Intelligence	Understands and responds to natural language questions to surface answers, perform actions, and assist with workflows.
Predictive Intelligence	Identifies trends, forecasts, and variances to anticipate outcomes and optimize planning.

How It Works

Prophix One Intelligence uses application APIs as the secure boundary between AI inference and customer data. LLMs never access raw data directly.

-  AI services translate user prompts into API calls that retrieve or update data within the platform.
-  Responses are rendered securely through the application interface.
-  Every interaction is logged and auditable.

This inference-only design ensures that customer data remains private, controlled, and never used for model training.

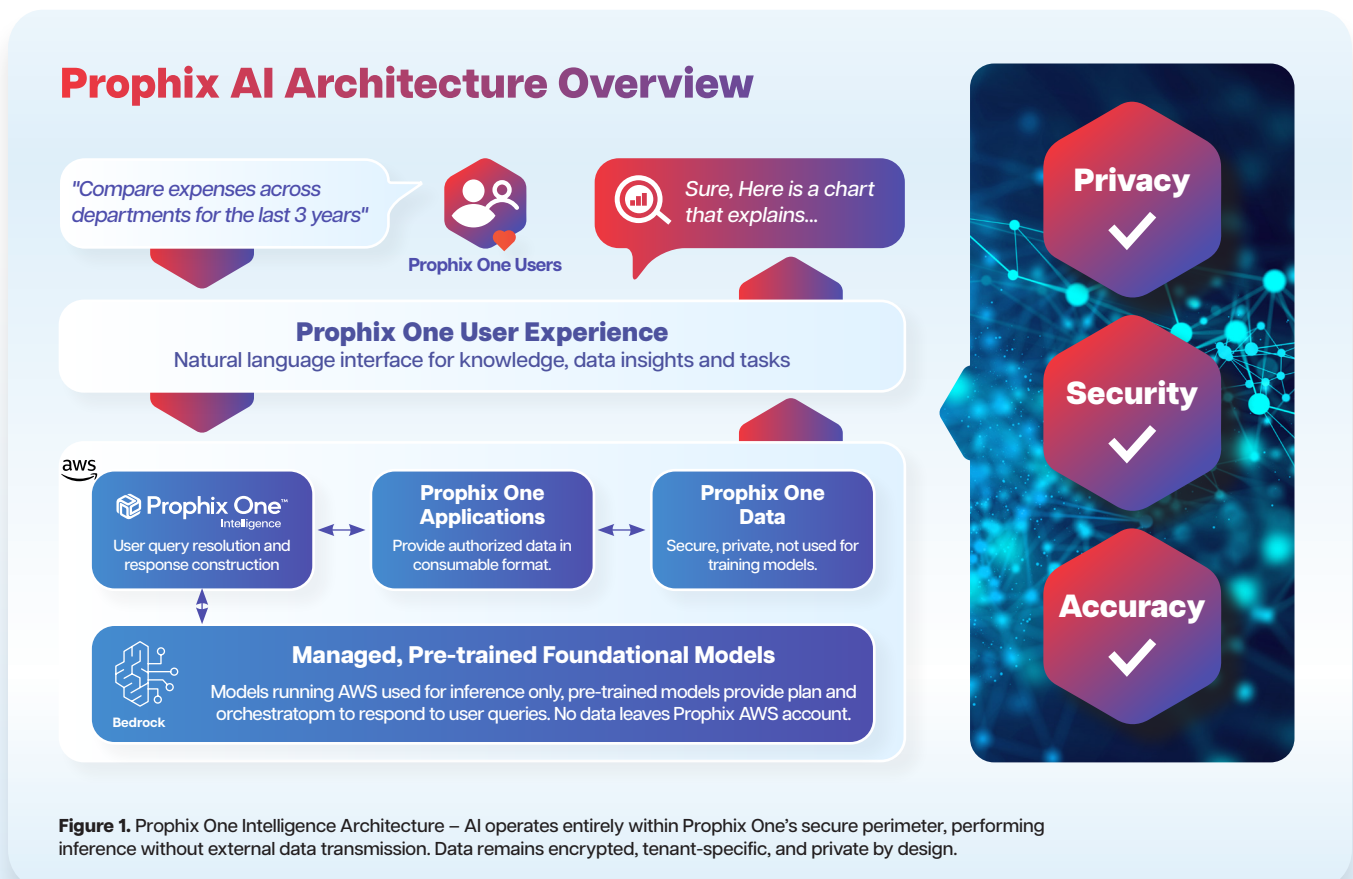
AI Architecture Overview

Prophix One Intelligence is a set of Python-based microservices deployed on AWS ECS Fargate, built for elasticity, security, and observability.

Core components:

- **Model Context Protocol (MCP)** – translates user intent into authorized API calls; models never access raw data directly.
- **OpenSearch memory store** – maintains secure short-term context for Agents.
- **Langfuse LLM Ops** – provides observability, evaluation, and controlled testing before model updates.
- **AWS Bedrock LLMs** – deliver managed, inference-only AI. Customer data is never used for model training.

All data access occurs through secure APIs within the Prophix One environment. Identity services and role-based access control (RBAC) enforce least-privilege access, while every activity is logged and auditable.





1. Prompt & Authentication

User submits a query through an Agent and identity verified via SSO, MFA, and RBAC.

2. Intent Translation

Prophix One Intelligence services convert prompts into structured, authorized API calls that follow existing data permissions.

3. Inference Execution

Managed Bedrock models perform inference securely within Prophix's environment.

4. Response & Audit

Results are returned to the application and all actions are logged for compliance.

5. Observability & Governance

Langfuse tracks accuracy, latency, and model performance.

Pillars of Trustworthy AI

Pillar	Architectural Assurance
Accuracy	Grounded in governed APIs; managed model versions ensure predictable, factual responses.
Security	Every layer is designed for protection, using zero-trust controls, encryption, and constant testing to keep customer data safe.
Privacy	Inference-only AI ensures customer data is never used for model training or stored outside the tenant environment.

Security & Privacy by Design

Prophix One Intelligence is developed within the secure software development lifecycle (SDLC) that governs all Prophix services, combining automation, peer review, and continuous testing.

Secure Development Practices

- **Automated testing for every code change** – Every code update passes through automated unit, integration, and performance tests to ensure consistent quality and prevent regressions before release.
- **Peer reviews by senior engineers for adherence to secure-coding standards** – Automated scanning tools analyze code both at rest and in runtime to identify security flaws, unsafe dependencies, and potential misconfigurations early in development.
- **Third-party penetration testing by independent experts** – External security firms conduct regular penetration tests to assess the platform’s resilience and uncover vulnerabilities before they can be exploited.
- **Zero-trust authentication for all services and users** – Every service-to-service and user request is explicitly verified and authorized, ensuring access is granted only to authenticated, approved identities regardless of network location.

Core Safeguards

- **Data Encryption:** AES-256 encryption at rest; TLS 1.3 for data in transit.
- **Access Control:** Role-based permissions, SSO, and multi-factor authentication.
- **Tenant Isolation:** Logical and physical data segregation ensures privacy by design.
- **Inference Boundary:** AI services process data transiently; no persistence outside customer environments.
- **Explainability & Auditability:** All AI interactions are traceable to source data and stored in audit logs.

Certifications & Compliance



SOC 2 Type II



GDPR, CCPA, and PIPEDA alignment



TrustArc verified privacy framework



Continuous vulnerability scanning and third-party penetration testing

Responsible AI & Explainability

Prophix's AI framework prioritizes transparency, traceability, and human oversight. Outputs are explainable, linked to governed data, and reviewed through a human-in-the-loop approach. Continuous monitoring and bias mitigation practices ensure fairness, reliability, and compliance.

AI in the Cloud vs. AI in Prophix One

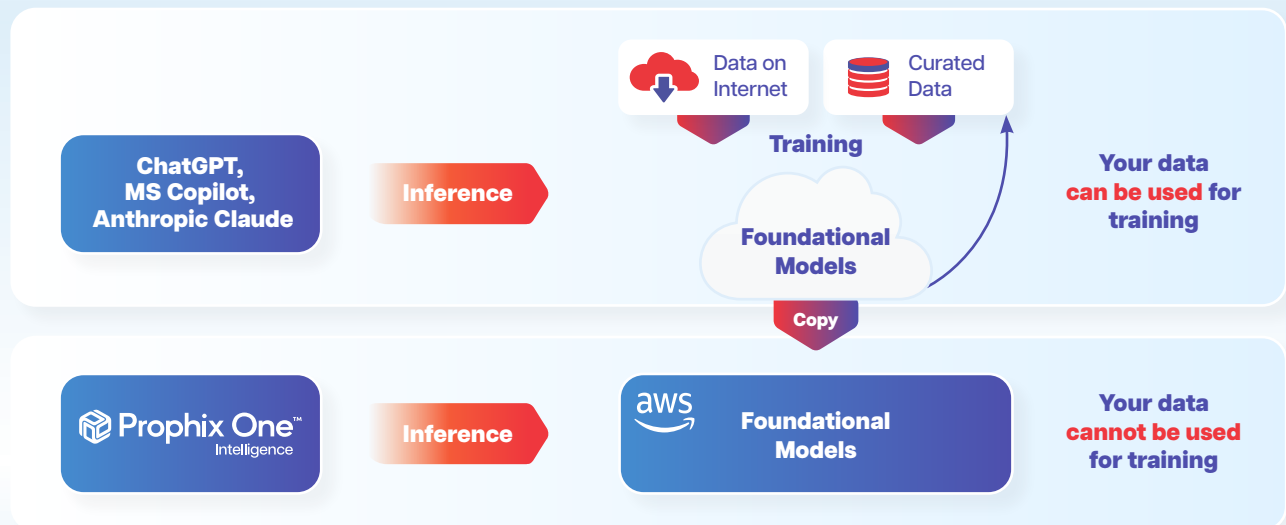


Figure 2. AI in the Cloud vs. AI in Prophix One – Unlike public cloud AI models, which may reuse or retain data for training, Prophix One AI operates privately within a SOC 2–certified infrastructure. Your data cannot be used for training.

Concern	Public Cloud AI	Prophix One Intelligence
Security	Public inference endpoints	Private inference within SOC2 certified environment
Privacy	Data may be logged or retained	No customer data stored or logged for inference
Training	User data may train models	Customer data is never use for training
Governance	Uncontrolled data sources	AI grounded in governed financial data
Traceability	Opaque outputs	Explainable, auditable results



Conclusion

Prophix's AI framework prioritizes transparency, traceability, and human oversight. Outputs are explainable, linked to governed data, and reviewed through a human-in-the-loop approach. Continuous monitoring and bias mitigation practices ensure fairness, reliability, and compliance.

In a financial landscape defined by complexity, speed, and data volume, finance leaders need intelligence they can trust – not just automation.

Prophix One Intelligence enables that transformation by delivering:

-  **Clarity** Natural language turns complex models into accessible insights.
-  **Capacity** Automation frees teams to focus on strategy and business partnership.
-  **Confidence** Governed, explainable AI ensures every recommendation is grounded in trusted data.

Prophix One Intelligence ensures that every AI-driven insight is both powerful and provable – a foundation of trust for finance and IT leaders alike.

For a deeper technical discussion or architecture review, contact your Prophix representative.



About Prophix®

Prophix® is a global leader in financial performance management, empowering finance teams to lead with clarity, capacity, and confidence. From planning and budgeting to forecasting, reporting, reconciliation, and consolidation, Prophix brings it all together in one intelligent platform.

Prophix One™, the flagship Autonomous Finance Platform, combines AI, automation, and intuitive technology to simplify complex work and elevate finance to a more strategic role. With nearly four decades of innovation and a global footprint serving more than 3,000 customers in 100+ countries, Prophix is the trusted partner for organizations ready to transform finance into the driving force behind business growth.



www.prophix.com

info@prophix.com