INTERPRETOS LOCAL

Security Architecture

How Your Data Stays Safe

Code Development Ltd

ISO 27001 Certified (UKAS Accredited) | IBM Partner Plus Silver

February 2026

Version 1.0 | CONFIDENTIAL

interpretos.ai

interpretos.ai/security.html

TABLE OF CONTENTS

1. Executive Summary

Interpretos Local is an AI-powered enterprise application intelligence platform that runs entirely within the customer's infrastructure as a single Docker container. It enables natural language querying of complex enterprise systems — including Oracle E-Business Suite, PeopleSoft, and IBM Maximo — while maintaining complete data sovereignty and security.

This whitepaper details the security architecture of Interpretos Local and is intended for CISOs, security architects, and IT governance teams evaluating the product for enterprise deployment.

Key Security Principles

- **Zero vendor access.** On-premises deployment: no vendor access to your data, systems, or infrastructure at any time.
- **Complete data sovereignty.** Your data never leaves your network. No cloud dependency, no external data stores.
- **Read-only by design.** Three independent protection layers prevent any data modification to your ERP systems.
- **Air-gap capable.** When paired with a local Ollama instance, Interpretos operates with zero external network traffic.
- **Full customer control.** Credentials, configuration, audit logs, and all application data remain under your governance.

2. Architecture Overview

Interpretos Local is delivered as a single Docker container image, designed for minimal footprint and maximum isolation. The deployment architecture eliminates the attack surface inherent in multi-service, cloud-dependent solutions.

Deployment Model

Component	Detail
Packaging	Single Docker container (interpretos/local)
Default Port	8080 (configurable)

Privileged Access	Not required — runs as unprivileged container
Host Network	Not required — uses standard Docker bridge networking
Data Storage	Docker volume mounted at /app/data (customer-managed)
External Dependencies	Outbound HTTPS to LLM provider only (or none with Ollama)
Supported LLM Providers	Google Gemini, OpenAI, Anthropic, or local Ollama
Supported Platforms	Linux, macOS, Windows (any Docker-capable host)

The single-container model means there are no service meshes, message queues, sidecar proxies, or distributed databases to secure. The entire application — web interface, query engine, credential store, and audit log — runs within one isolated process boundary.

3. Data Flow Transparency

Interpretos categorises all data into two groups based on where it resides and whether it ever leaves the customer's network boundary. This section provides complete transparency about each category.

Category 1: Stays Inside Your Network (Always)

The following data is stored exclusively in the customer-managed Docker volume and never transmitted externally:

- ERP credentials and API keys
- Database connection strings
- Query results (all data returned from ERP systems)
- Conversation history and chat logs
- User accounts, roles, and access configuration
- Audit logs (query log, login activity, session history)

- All application configuration

Category 2: Sent to LLM Provider (Configurable)

When using a cloud-hosted LLM provider (Gemini, OpenAI, or Anthropic), the following data is transmitted via encrypted HTTPS:

- System prompts (query instructions and formatting guidance)
- The user's natural language question
- Conversation context for multi-turn interactions
- Formatted query results for natural language response generation

> **NEVER sent to LLM provider:**
> ERP credentials, database passwords, raw connection strings, personally identifiable information (PII) identifiers, API keys, or SSH private keys. Credentials are injected at query execution time only and are architecturally separated from the LLM communication path.

Air-Gap Option: Zero External Traffic

For organisations requiring complete network isolation, Interpretos supports local LLM inference via Ollama (or any OpenAI-compatible local endpoint). In this configuration, no data leaves the customer network under any circumstances. Every byte of data — including LLM inference — stays inside the customer's infrastructure.

4. Read-Only Guarantee — Three Protection Layers

Interpretos enforces read-only access to customer ERP systems through three independent, defence-in-depth protection layers. Each layer operates independently; even if one layer were bypassed, the remaining two would prevent data modification.

Layer	Mechanism	What It Blocks	Scope

Layer 1 SQL Validation	Pre-execution SQL statement analysis. Every SQL statement is parsed and validated before execution.	INSERT, UPDATE, DELETE, DROP, ALTER, TRUNCATE, CREATE, GRANT, REVOKE	All SQL queries to Oracle EBS and PeopleSoft databases
Layer 2 HTTP Method Restriction	Protocol-level enforcement. Only HTTP GET requests are permitted to REST/API endpoints.	POST, PUT, DELETE, PATCH	All REST API calls to Maximo, PeopleSoft, and other HTTP-based integrations
Layer 3 Code Executor Sandbox	Restricted Python execution environment with whitelisted functions only.	File I/O operations, os/subprocess calls, arbitrary network access, import of restricted modules	All code generated by the LLM for query execution

This three-layer architecture ensures that even in the theoretical scenario where the LLM generates malicious code, no destructive operation can reach the customer's ERP system. Only SELECT statements (SQL) and GET requests (HTTP) pass through all three layers.

5. Credential Management

Interpretos implements per-user credential isolation, ensuring that each user's ERP access is governed by their own credentials and the permissions defined within the ERP system itself.

Feature	Detail
Isolation Model	Per-user credential storage — each user's ERP credentials are stored and managed independently
Encryption	AES-128 Fernet symmetric encryption at rest
Credential Injection	Credentials are injected at query execution time only, never included in LLM prompts or conversation context
Storage Location	Docker volume under customer control —

	standard backup, rotation, and revocation apply
Provisioning	Admin provisions user credentials via the built-in Setup Wizard
User Visibility	End users never see raw credentials — credentials are managed entirely by administrators
RBAC Enforcement	Per-user credentials enforce ERP-native role-based access control — users see only what their ERP permissions allow

Credential Lifecycle

1. Administrator creates user account in Interpretos.
2. Administrator provisions ERP credentials for that user via the Setup Wizard.
3. Credentials are encrypted and stored in the Docker volume.
4. At query time, the user's credentials are decrypted and injected into the query executor.
5. After query execution, credentials are discarded from memory.
6. Credential rotation and revocation follow the customer's standard IT procedures.

6. Network Security

Interpretos Local is designed with a minimal network footprint. The container requires no inbound network access from outside the customer's network and makes only outbound connections to a customer-chosen LLM provider.

Property	Detail
Inbound Connections	Port 8080 only (configurable), accessible within the customer's internal network
Outbound Connections	HTTPS (port 443) to the customer's chosen LLM provider
Phone-Home Capability	None — no telemetry, analytics, or license verification calls unless explicitly enabled
License Server	None required — the product operates

	without any external license validation
DNS Requirements	DNS resolution for LLM provider hostname only (or none with local Ollama)
Air-Gap Operation	Fully supported with local Ollama — zero external network traffic

Recommended Firewall Rules

Direction	Protocol	Port	Destination	Purpose
Outbound	HTTPS	443	LLM provider (e.g., generativelanguage.googleapis.com)	LLM inference requests
Inbound	HTTP/HTTPS	8080	Internal network only	User web interface access
Internal	Varies	Varies	ERP system endpoints	Database/API queries to ERP systems

For air-gapped deployments, the outbound HTTPS rule is eliminated entirely. All LLM inference is handled by the local Ollama instance, and no traffic leaves the customer's network.

7. Audit & Logging

Always-On Local Logging

Interpretos maintains a comprehensive local audit trail that is always active and cannot be disabled. All logs are stored in the Docker volume under customer control.

- **Natural language queries:** Every user question is logged with timestamp and user identity.
- **SQL statements and API calls:** Every query executed against ERP systems is recorded.

- **Conversation history:** Full per-user conversation history for review and compliance.
- **Login and session activity:** User authentication events, session creation, and session expiry.

All logs are queryable, exportable, and deletable by the customer. They can be integrated with existing SIEM solutions and comply with any data retention policy the customer defines.

Optional Telemetry (Disabled by Default)

Interpretos includes an optional telemetry feature that, when explicitly enabled by the customer, sends a daily heartbeat containing aggregate statistics only:

- Total query count (number, not content)
- Active user count
- Uptime duration
- Software version

> **Never collected via telemetry:**
> Query text, natural language questions, usernames, data records, credentials, IP addresses, ERP data, or any personally identifiable information.

8. Compliance & Certifications

Certification / Standard	Status	Detail
ISO 27001	Certified	UKAS-accredited certification. Information security management system covering development, deployment, and support operations.
IBM Partner Plus Silver	Active	Official IBM technology partner status, covering Maximo integration development.
GDPR Readiness	Compliant by Architecture	All data remains under customer control within their infrastructure. No personal data is transmitted

		to or processed by Code Development Ltd.
SOC 2 Type II	Roadmap (2026)	SOC 2 Type II audit planned for 2026. Note: since Interpretos runs on customer infrastructure, SOC 2 certification of the vendor is less relevant than in a SaaS model.

Because Interpretos Local runs entirely on customer infrastructure, the traditional vendor-centric compliance model is inverted. The customer's own security controls, certifications, and governance policies apply to the deployment. Code Development Ltd certifies the software; the customer certifies the infrastructure.

9. Deployment Checklist for Security Teams

The following checklist is designed for security teams evaluating and approving an Interpretos Local deployment. Each item maps to a specific security control discussed in this document.

#	Item	Section Ref.	Notes
1	Docker host provisioned (Linux, macOS, or Windows)	Section 2	Standard Docker installation; no privileged mode required
2	Outbound HTTPS to LLM provider configured (or Ollama for air-gap)	Section 6	Port 443 outbound to chosen provider, or no outbound for air-gap
3	Per-user ERP credentials provisioned by admin	Section 5	Use Setup Wizard; credentials encrypted at rest with AES-128 Fernet
4	RBAC configured for user access control	Section 5	Each user sees only what their ERP permissions allow
5	Docker volume	Section 2	Volume at /app/data

	included in backup procedures		contains all state, credentials, and logs
6	Local audit logs configured for compliance review	Section 7	Always-on logging; integrate with SIEM as needed
7	Network firewall rules verified (outbound 443 only)	Section 6	No inbound from internet required; port 8080 internal only
8	Telemetry configuration reviewed	Section 7	Disabled by default; enable only if desired
9	Read-only enforcement verified in test environment	Section 4	Test all three protection layers before production deployment
10	Credential rotation procedures documented	Section 5	Standard IT rotation; credentials stored in Docker volume

10. On-Premises vs SaaS Security Model

The following comparison illustrates the fundamental difference in the security model between a traditional SaaS deployment and the Interpretos Local on-premises model. In the SaaS model, the customer must trust the vendor's security controls. With Interpretos Local, the customer retains full control.

Security Aspect	Typical SaaS Vendor	Interpretos Local (On-Prem)
Data Residency	Vendor's cloud infrastructure	Customer's own infrastructure
Data Encryption at Rest	Vendor manages keys	Customer manages keys
Data Encryption in Transit	Vendor's TLS certificates	Customer's TLS certificates
Access Controls	Vendor's IAM policies	Customer's IAM policies

Audit Logs	Vendor provides (may be limited)	Customer owns completely
Credential Storage	Vendor's vault/HSM	Customer's Docker volume (AES-128)
Network Security	Vendor's VPC/firewall	Customer's network/firewall
Breach Notification	Depends on vendor's process	Customer detects directly
Compliance Scope	Shared responsibility model	Customer controls everything
Vendor Employee Access	Possible (with controls)	None — no vendor access
Data Portability	Export tools (vendor-dependent)	Docker volume — fully portable
Service Continuity	Depends on vendor viability	Customer runs independently

> **Key Takeaway:**
> With Interpretos Local, there is nothing to trust the vendor with. Your data, your credentials, your audit logs, your network — all remain under your governance. The vendor provides the software; you provide the security.

11. Contact

For security-related questions, requests for additional technical documentation, or to schedule a security architecture review:

Email: info@interpretos.com
Website: https://interpretos.ai
Security Page: https://interpretos.ai/security.html
Live Demo: https://demo.interpretos.com