Gap Analysis Report: *Velonix* AI Security

Organization: *Velonix*

Date: April 2025

1. Objective

The objective of this gap analysis is to assess the current shortcomings in enterprise AI systems, specifically those utilizing Retrieval-Augmented Generation (RAG)—and outline how Velonix's role-aware middleware platform effectively addresses these limitations. The focus is on enhancing secure AI adoption across regulated industries while aligning with Saudi Vision 2030's strategic priorities in cybersecurity, innovation, and digital sovereignty.

2. Context and Strategic Relevance

As enterprises in Saudi Arabia accelerate their adoption of artificial intelligence, a critical gap has emerged between AI capability and cybersecurity readiness. AI platforms, especially those using LLMs and RAG pipelines, are vulnerable to unauthorized access and data leakage. Without embedded, role-aware controls, sensitive knowledge can be inadvertently exposed, undermining compliance with local regulations (e.g., NCA, SDAIA, PDPL) and threatening organizational trust.

Velonix addresses this challenge by providing a middleware solution that applies **Role-Based Access Control (RBAC)** at the knowledge retrieval layer—ensuring that AI responses are filtered and shaped by user roles **before** any sensitive data is exposed.

3. Gap Analysis Table

Dimension	Current State	Target State with Velonix	Gap Identified

AI Access Control	Access control is typically enforced at the app or perimeter level, not integrated with AI logic. LLMs respond without considering user roles.	Fine-grained RBAC enforcement embedded within the AI query pipeline; aligned with identity providers like Azure AD.	Lack of context-aware access enforcement across AI systems.
Regulatory Compliance	Incomplete audit trails for AI decisions. Limited mechanisms to trace who accessed what information via AI.	Integrated logging of all query decisions, session context, and access policies enforced. Supports compliance with PDPL, SDAIA, and NCA mandates.	Enterprises cannot demonstrate audit readiness or compliance confidence.
RAG System Security	Vector search exposes semantically relevant but potentially unauthorized documents to LLMs.	Middleware filters results based on role metadata **before** vector search results reach the LLM.	Uncontrolled knowledge exposure during retrieval leads to data leakage.
Integration Complexity	Enterprises must customize LLM prompts, retrain models, or build in-house guardrails.	Middleware sits between front-end and backend systems, providing plug-and-play integration.	High development and maintenance burden deters secure AI adoption.
Market Readiness in KSA	High interest in AI but low deployment due to security gaps. Lack of trusted compliance tools hinders implementation in regulated sectors.	Security-first AI middleware accelerates adoption while aligning with Vision 2030.	Absence of scalable, compliant middleware solutions tailored for the Saudi market.

4. Key Observations

1. **Security Enforcement is Post-Hoc or Superficial:** Most current AI security efforts focus on masking outputs or redacting after-the-fact, rather than preventing access at the data layer.
2. **Lack of Identity Integration:** AI systems operate independently of enterprise identity infrastructure, making role validation and access control inconsistent.
3. **Auditability is Reactive, Not Proactive:** Organizations struggle to explain or track how and why AI responses were generated, which hinders trust and regulatory reporting.
4. **Technical Complexity is a Barrier:** Security solutions today often require deep technical changes to AI architecture, resulting in high cost and resistance.

5. Strategic Alignment with Saudi Vision 2030

Saudi Vision 2030 prioritizes:

- **Data Sovereignty**
- **National Cybersecurity Posture**
- **Smart Government and Cities**
- **AI-Driven Public and Private Sector Transformation**

Velonix contributes directly to these national priorities by:

1. Providing secure middleware that ensures **AI knowledge stays within approved access boundaries.**
2. Delivering **compliance-aligned logging and policy enforcement** compatible with local regulations.
3. Enabling organizations like NEOM, SDAIA, and NCA to deploy **AI securely and responsibly**.

4. Reducing AI risk to **accelerate adoption** in sectors including healthcare, finance, and energy.

6. Conclusion and Recommendation

There is a significant and urgent gap between AI capability and AI security. Without proactive access control embedded in the AI pipeline, organizations face substantial risks—from data leaks to regulatory fines. Velonix fills this gap with a **middleware solution that enables safe, role-aware use of generative AI systems**.

As AI continues to evolve, so must the architecture around it. Velonix ensures that enterprises don't have to compromise between innovation and control. It's not just about protecting data—it's about enabling **secure intelligence** as a core pillar of digital transformation.

Prepared by:
Velonix AI Security
April 2025