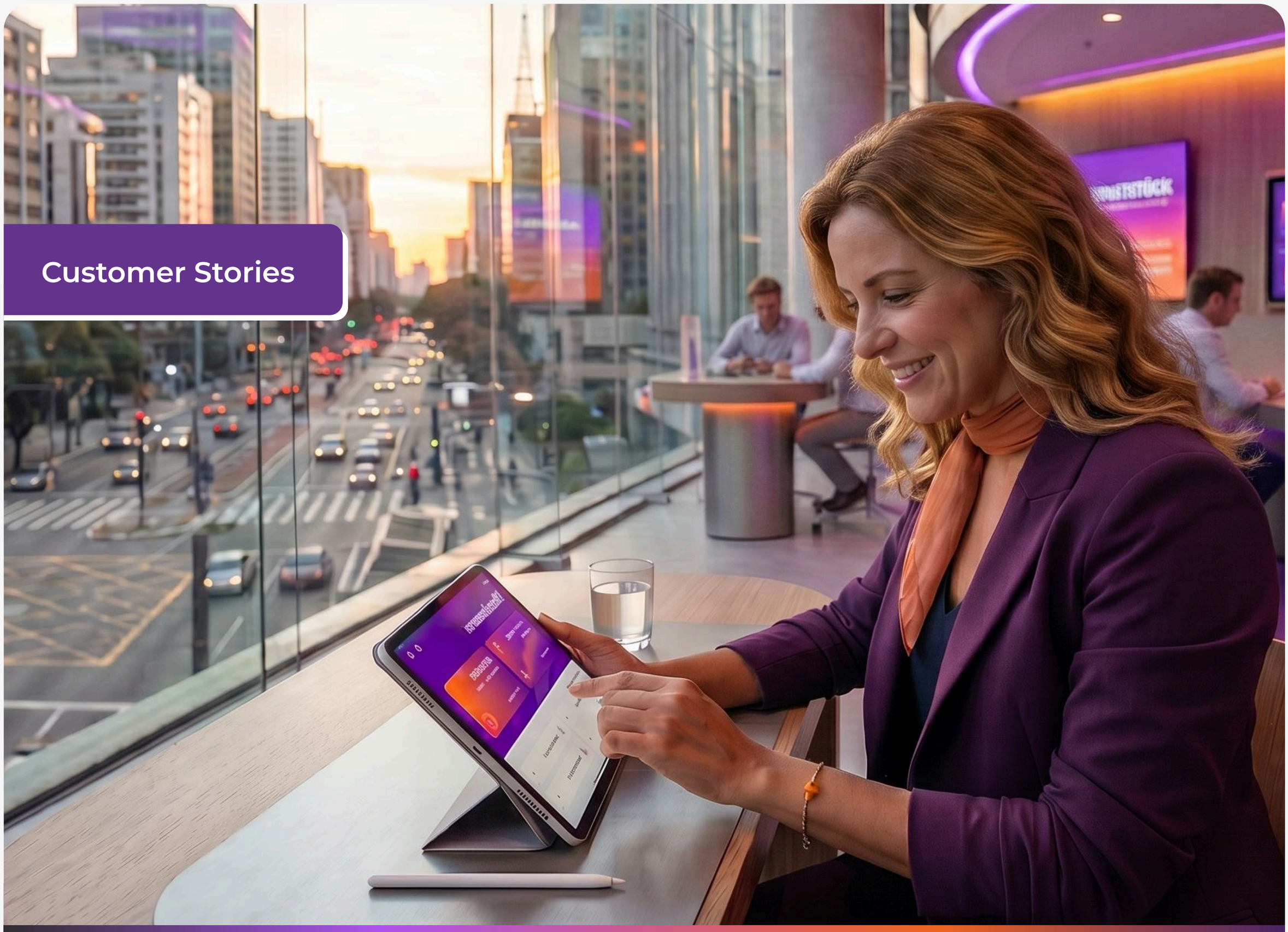


Financial Institution Optimizes Agentic Journey with MCP and Sensedia AI Gateway

sensedia®

AI is playing an increasingly strategic role in the financial market through the use of **autonomous AI agents.** In this context, **MCP** (Model Context Protocol) has established itself as a universal connectivity standard, enabling banks to transform their traditional APIs into plug-and-play tools ready to be consumed by AI ecosystems.

Building on its extensive API maturity and pioneering experience with transactions via WhatsApp Bot, a major financial institution identified an opportunity to become a true hub for **agentic connectivity.**

To accelerate its AI initiatives without compromising security, the institution turned to Sensedia to conduct a pilot of the **Sensedia AI Gateway,** seeking a **centralized governance layer** capable of orchestrating MCP adoption, protecting its infrastructure against prompt injection attacks and sensitive data leakage, and maintaining full control over costs and model usage limits.

What did the Sensedia AI Gateway pilot at the financial institution involve?

The Proof of Concept (PoC) had a very clear business challenge: the institution needed to provide **an intelligent assistant to support the credit** origination journey, qualifying leads and reducing the costs of unnecessary analyses before they reached the approval pipeline.

The primary goal was to validate a real-world business journey, ensuring that the AI agent interacted exclusively within the credit domain while integrating with legacy systems with full governance and security over AI consumption.

How did the Sensedia AI Gateway-based architecture address the pilot's challenges?

Rather than treating governance as a future concern, the architecture introduced Sensedia AI Gateway as an enabler from day one of the PoC. It connected the AI agent to the bank's credit services through MCP, providing:

Centralized governance

Token cost monitoring, call observability, request rate limiting, and prompt guardrails.

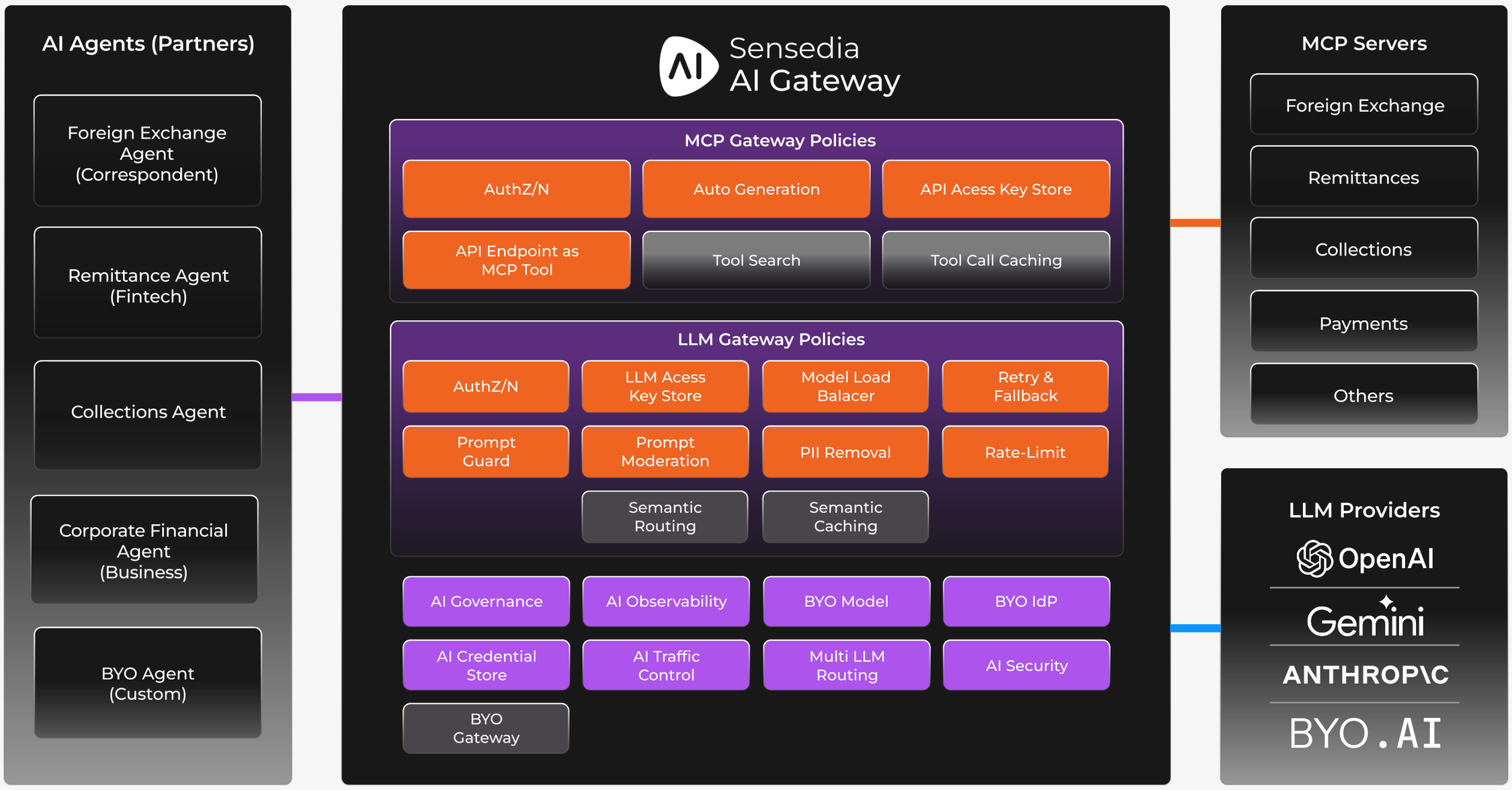
Secure integration

The scope was restricted to a protected environment, safeguarding corporate systems.

Domain control

Through prompt enrichment and moderation, the AI Gateway ensured that the AI agent operated strictly within the bank's business rules, standardizing communication between the AI and APIs.

Reference Architecture: MCP-enablement of a financial institution



What were the main results of the PoC?

In just two weeks, the financial institution achieved key milestones that demonstrated the value of the model:

Value generation

Real credit leads were captured and qualified by the agent during the PoC.

Proven security

The AI agent demonstrated its ability to refuse queries outside the credit domain, highlighting the effectiveness of domain governance.

End-to-end validation

The complete flow—including acceptance of terms, CPF/age validations, installment rules, and lead submission to the approval pipeline—operated successfully in a real-world environment.

Evolution to production

The pilot's success paved the way for the technical and commercial evolution of the Brenda assistant into production, strengthening the institution's agentic banking strategy.

Why is the financial institution ideally positioned to benefit even further from MCP?

The financial institution has several characteristics that make it an ideal hub for AI agent-based innovation:

API maturity
It already has mature digital foreign exchange and internet banking platforms, accelerating their exposure as MCP Servers.

Proven innovation
It is a pioneer in financial transactions via WhatsApp Bot.

Correspondent ecosystem
It has an extensive network that can increase

Leader in foreign exchange and remittances
Its core business is built around international transactions, making it an ideal environment for developing foreign exchange MCP Servers.

Beyond credit, other products and services that could be directly impacted and transformed into MCP Servers include: **foreign exchange** (quotes and trade execution), **remittances** (sending and tracking), **collections** (standard, linked, and discounted), **payments, checking accounts, and investment products.**

For banks in general, **MCP adoption means transforming existing APIs into MCP Servers that any AI agent can discover and use.** Financial institutions that expose their APIs through this protocol enable partners and customers to build AI agents directly connected to their ecosystem.

This enables the creation of new intelligent products, generates new revenue streams, increases customer retention, and creates a strong competitive advantage in a highly commoditized market.

How can the financial institution's ecosystem of partners and customers benefit from MCP?

By exposing its services, the financial institution enables partners to build autonomous AI agents. Some use cases include:

- **Intelligent foreign exchange agent (correspondents):** an AI agent that supports FX quoting, negotiation, and transaction execution via MCP.
- **Remittance assistant (fintechs):** guides end customers through documentation requirements, calculates total costs, and autonomously executes remittances.
- **Corporate financial agent (importers/exporters):** monitors exchange rates, alerts companies to hedging opportunities, and executes international payments based on predefined business rules.

How does Sensedia AI Gateway support MCP adoption in financial institutions?

Integrating AI with a bank's core systems introduces significant risks without proper governance. Sensedia AI Gateway acts as a **unified, governed control layer for LLM traffic and MCP services.** It addresses **five critical threats** facing financial institutions:

- **Prompt injection:** applies input and output guardrails to prevent malicious instructions from manipulating AI agents.
- **PII leakage (sensitive data):** performs real-time masking of CPFs, CNPJs, and card data.
- **Cost overruns:** enforces rate limiting, semantic caching, and strict budgets for each agent.
- **Intellectual property theft:** scans outputs to prevent internal logic and proprietary information from being leaked.
- **LLM outages:** provides automatic fallback and routing between providers such as OpenAI, Anthropic, and Gemini if one becomes unavailable.

Conclusion

The financial institution’s use case demonstrates that AI can only reach its true transformative potential in the financial market when combined with governance and structured integration. A key lesson from this journey is that a pilot generates significantly more value when it simultaneously validates the user experience, business integration, and the boundaries within which the agent is allowed to operate.

Investing in MCP-based initiatives supported by an AI Gateway is no longer merely a technology choice—**it is a strategic path for financial institutions seeking to move beyond isolated experiments while ensuring enterprise-grade security,** true scalability, and leadership in the new era of the agentic economy.

Learn more about the Sensedia AI Gateway and how it can transform your AI strategy.

Visit our website and get all your questions answered!

Acess now>

Enabling a more digital, connected, and open world.

Want to know how Sensedia can help your company accelerate digital transformation and strengthen your connections?

Contact us through our website to discover personalized solutions that drive business growth.

For more success stories like this one, click here:

Customer stories

How about letting our team bring solutions like this to your business?

Don't waste time

Contact us

sensedia®