Securing Intellectual Property in the AI Era: From Legacy APIs to Agent2Agent (A2A) Protocols

A White Paper on Protecting Data Assets and Unlocking New Revenue Streams for Research Firms

Published by Backflipt (Xenovus, Inc), November 2025

Executive Summary

In an increasingly AI-driven world, research firms face a critical dilemma: how to share valuable market data with enterprise clients without exposing proprietary intellectual property (IP) to irreversible risks. Traditional API and Market Data Platform Client (MCP) models accelerate data access but often lead to IP leakage through public large language models (LLMs), compliance violations, and missed monetization opportunities.

This white paper examines a real-world scenario in which a Fortune 500 enterprise attempts to forecast sales of emerging RISC-V 64-bit servers in Latin America, utilizing a research firm's historical x86 server data. We contrast the "before" state—legacy APIs leading to high costs, security threats, and commoditization—with the "after" state enabled by Agent2Agent (A2A) protocols and Lumen from Backflipt.

By adopting A2A, research firms can facilitate secure, agentic collaborations that deliver insights without exposing raw data. This shift not only safeguards IP but also opens premium service lines, transforming data feeds into high-value, monetizable models. Enterprises benefit from faster, compliant access to expert projections, reducing DIY inefficiencies.

Key takeaways:

- Legacy systems expose IP at machine speed, risking permanent loss.
- A2A protocols enable interoperable communication among AI agents, focusing on goals and results rather than raw datasets.
- **Lumen** automates A2A deployment, ensuring sovereignty over IP while fostering deeper, more strategic partnerships.

Introduction

The rapid adoption of artificial intelligence (AI) has revolutionized how enterprises consume market intelligence. Research firms provide essential data on technology trends,

market sizing, and competitive landscapes, empowering clients to make informed decisions. However, as AI agents and LLMs become integral to enterprise workflows, traditional data-sharing mechanisms—such as APIs and MCPs—pose significant risks to IP protection.

Introduced in April 2025 by Google and now an open standard under initiatives such as the Linux Foundation's Agent2Agent Protocol Project, the A2A protocol represents a significant paradigm shift. It allows AI agents to communicate securely across platforms, exchanging context, status, actions, and results without sharing underlying data, memory, or tools. This interoperability is crucial for industries such as market research, where proprietary datasets form the core of a competitive advantage.

This white paper examines the vulnerabilities of legacy systems through a practical scenario and demonstrates how A2A, powered by Backflipt's Lumen, can mitigate these risks. Drawing on industry insights and protocol specifications, we outline a path forward for research firms to maintain control, comply with regulations like GDPR and HIPAA, and capitalize on AI-driven opportunities.

The Challenge: IP Risks in Data Sharing

Research firms invest heavily in curating high-quality datasets, often derived from proprietary surveys, models, and analyses. These assets are licensed to clients via APIs or MCPs, which promise seamless integration into enterprise systems. While MCPs enhance interaction speed—enabling data retrieval in seconds—they inadvertently amplify risks.

Key challenges include:

- **IP Leakage via LLMs:** Clients may feed raw data into public or in-house LLMs for custom modeling, embedding proprietary insights into third-party model weights. Once trained, this data cannot be retracted, leading to permanent exposure.
- **Compliance Violations:** Uncontrolled data flows pose a risk of breaches in data privacy laws, leading to fines and reputational damage.
- **Commoditization and Lost Revenue:** APIs reduce research services to low value "data pipes," missing upsell opportunities for tailored insights on emerging technologies.
- **Enterprise Inefficiencies:** Clients face escalating costs for in-house modeling, including hiring experts and building non-standard projections, often without leveraging the research firm's domain expertise.

These issues are exacerbated in scenarios involving novel technologies, where historical data must be extrapolated creatively—yet securely.

Scenario: Forecasting Emerging Server Sales in Latin America

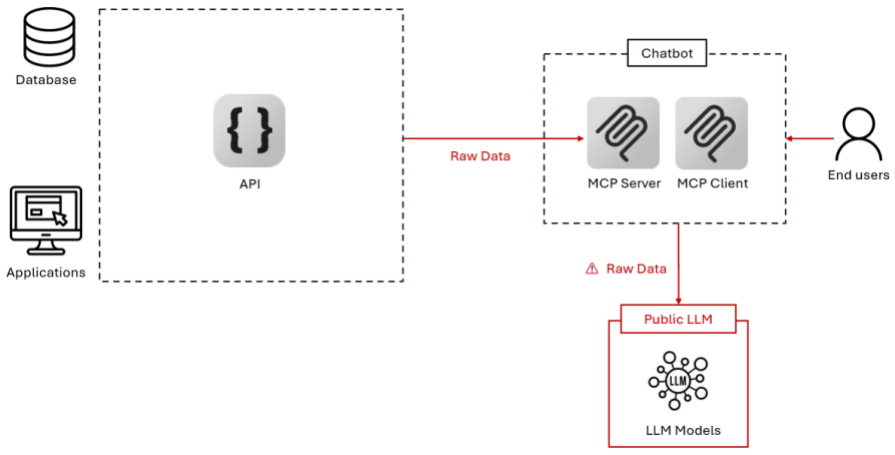
Consider a Fortune 500 enterprise client aiming to enter the Latin American market with new RISC-V 64-bit servers. RISC-V, an open-standard instruction set architecture, represents a disruptive alternative to traditional x86 processors. However, leading research firms primarily hold data on x86 server sales, lacking direct historical data on RISC-V due to its relatively nascent status.

The client requires a sales forecast to model potential market penetration, total addressable market (TAM), and regional trends. In a legacy setup, this involves pulling raw x86 datasets and adapting them in-house—a process fraught with inefficiencies and risks.

Before A2A: The Legacy API/MCP Model

In the traditional model, the enterprise client interacts with the research firm's data via APIs or MCPs:

- **Process Flow:**
    1. The client pulls raw x86 datasets (e.g., sales volumes, regional breakdowns) via the API/MCP.
    2. Feeds rows into public LLMs for initial analysis.
    3. Hires external modelers to build custom RISC-V projections.



- **Impact on the Enterprise Client:**

Process Step	Impact
Pull raw x86 datasets via API/MCP	Fast access in seconds but triggers high downstream modeling costs and risks.
Feed rows into public LLM	Exposes proprietary data to breaches, IP theft, GDPR/HIPAA violations, and potential legal fines.
Hire external modeler & build custom RISC-V projection	Incurs costs and risks non-standard models.

- **MCP:** Accelerates data interaction—retrieval in seconds. **Greater Risks & Costs:** Escalating expenses, delays, security threats, and DIY inefficiencies far outweigh the speed.
- **Impact on Research Firms:**

Exposure	Consequence
Raw data enters public LLM	IP trains 3rd-party models → permanent loss.
No modeling involvement	Miss upsells on RISC-V forecast service.
API/MCP = commodity feed	Revenue capped at data access fees.

- **IP Loss Math:** 1 CSV row → 1B-parameter model → No recall. Speed of MCP = Speed of IP leakage.
- **Outcome (Before A2A):**

Client	Research Firm
Fast data, slow insight; DIY modeling burden.	IP exposed globally; Lost control + lost revenue.

Legacy API/MCP = faster access, faster IP death. Speed without control leads to commoditized data and diminished future value.

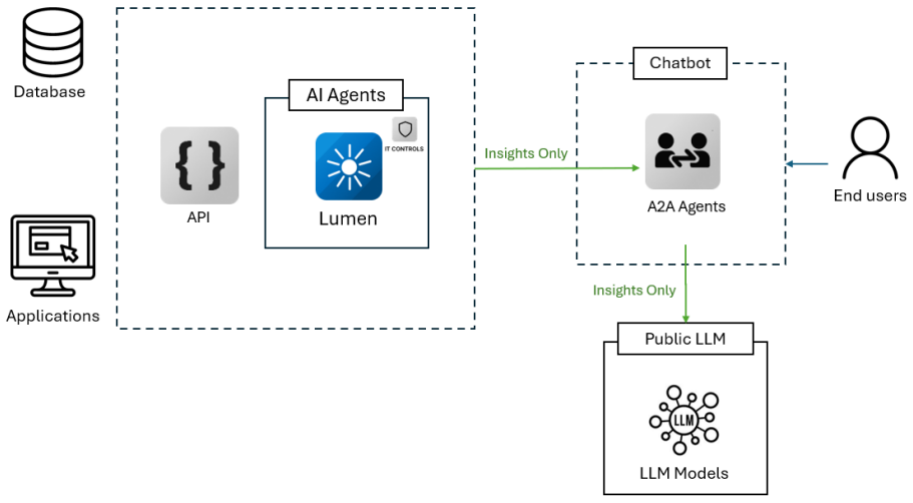
After A2A: Secure Collaboration with Lumen

The A2A protocol addresses these pain points by enabling AI agents to collaborate without raw data exchange. As an open standard, A2A facilitates secure, interoperable communication where agents share goals, context, state, actions, and results. This "team-like" interaction ensures auditability and trust, preventing data leaks while allowing complex problem-solving.

Backflipt's Lumen automates A2A agent generation for existing APIs, deploying seamlessly next to API gateways. Lumen integrates with secure managed file transfer (MFT) and business-to-business integration (B2Bi) environments, making it enterprise-ready for research firms.

How A2A Works in This Scenario

1. **Deployment:** Lumen fronts the research firm's API, auto-generating an A2A agent per client or query type.
2. **Query Handling:** The enterprise client's A2A agent sends a structured request (e.g., "Project RISC-V TAM from x86 trends in Latin America") via the A2A protocol.
3. **Internal Processing:** The research firm's A2A agent computes the forecast using proprietary x86 data and models, without exposing raw rows.
4. **Response Delivery:** Returns only insights (e.g., "LatAm RISC-V TAM = 180K units; Growth projection: 25% CAGR"), maintaining full audit logs.



- **A2A Model Flow:**

Process Step	Secure Flow
Lumen fronts Research API	Auto-spins A2A agent; shields raw x86 data behind protocol.
Client A2A agent queries	Sends structured request via A2A.
Research A2A agent responds	Computes insight internally; delivers only results.

- **A2A Advantage:** The protocol ensures interoperability, auditability, and zero raw exposure—agents collaborate like teams, not as data dumps. **Lumen Edge:** Deploys in minutes; scales to multi-agent workflows.
- **Impact on the Enterprise Client:**

Process Step	Impact
Query via A2A agent	Instant access to expert forecasts; no data pulls or security overhead.
Receive structured insights	Zero exposure to breaches, IP theft, or compliance violations.
Integrate ready projections	Saves costs and time on modeling; taps industry expertise directly.

- **A2A Speed:** Collaboration in seconds—far beyond MCP, with built-in trust. **Net Gain:** Accurate, compliant results without the DIY drag.

- **Impact on Research Firms:**

Control	Consequence
A2A gates all interactions	Raw IP stays internal; trains only your models → permanent sovereignty.
Protocol enables custom services	Capture upsells on RISC-V modeling; bill for agentic insights.
Beyond commodity APIs	Revenue unlocks at premium tiers (e.g., $0.50+/query).

- **Secure Value Math:** 1 A2A exchange → Auditable insight → Infinite reuse. Protocol speed = Locked IP + Exponential revenue.
- **Outcome (After A2A):**

Client	Research Firm
Seamless insight, full compliance; Expert accuracy, no burden.	IP fortified, zero leakage; New service lines + deepened partnerships.

Legacy MCP = raw risk. A2A + Lumen = agentic gold.

Lumen vs. Alternatives: Why Lumen Wins

Lumen delivers an **out-of-the-box A2A experience** that transforms legacy APIs into secure, monetizable agent endpoints in minutes—without coding, AI expertise, or fragmented workflows.

Criteria	Backflipt Lumen	DIY/Open-Source (e.g., Langflow, LangGraph)	Native Cloud Tools (e.g., AWS Bedrock, Azure AI, Google Vertex)
Core Focus	**Instant API-to-AI transformation:** MCP servers & A2A agents in minutes, enterprise-hosted for control & monetization	Low-code AI workflows; manual prototyping	General AI agents; platform-specific integrations
Speed to Market	**Fastest:** Deploys in minutes via Swagger/gateways, shrink-wrapped instrumentation	**Slowest:** Manual build, test, deploy; needs expertise	**Moderate:** Fast prototyping, but custom dev for enterprise
Enterprise Governance	**Built-in:** CI/CD integration, automated consistency, unified dev portal	**Manual:** Governance from scratch; fragmented	**Component-Based:** Manual config for governance
Ease for Non-Experts	**High:** No-code POET for customization, no AI expertise needed	**Medium:** Visual UI, but coding for advanced features	**Variable:** Some no-code, but devs needed for complexity
Scalability & Security	**Enterprise-Grade:** Kubernetes auto-scaling, DevSecOps, compliance (HIPAA, GDPR)	**Custom:** Scaling/security depend on expertise	**Scalable:** Cloud-native, but custom app logic/security
Total Cost of Ownership	**Lowest:** 80–90% dev cycle reduction, minimizes talent needs, 2–3x revenue	**Highest:** High maintenance, dedicated teams	**High:** Low initial cost, but escalates with dev hours

Out-of-the-Box Advantage of Lumen:

- **Zero-code agent generation** from existing APIs
- **Auto-instrumented A2A compliance & audit trails**
- **One-click deployment** next to API gateways
- **Built-in monetization layer** (per-insight billing, usage tiers)
- **No AI or agent framework expertise required** — non-technical teams launch in under 15 minutes

Benefits of Transitioning to A2A

- **For Research Firms:** Retain IP control, reduce breach risks, and monetize advanced services like custom AI-driven forecasts. A2A positions firms as strategic partners rather than mere data providers.
- **For Enterprise Clients:** Access precise, ready-to-use insights without the overhead of data handling, modeling costs, or compliance worries. This accelerates decision-making in dynamic markets.
- **Broader Ecosystem:** Promotes standardization via open protocols, fostering innovation in AI agent frameworks while ensuring security and interoperability.

Early adopters report **30–50% revenue uplift** from premium insights and up to **80% reduction** in data exposure incidents.

Conclusion

The era of unchecked data sharing is over. As AI agents proliferate, research firms must evolve from legacy APIs to A2A protocols to protect their most valuable assets. Backflipt's Lumen makes this transition effortless, enabling secure, intelligent collaborations that benefit all parties.

By embracing A2A, firms can "own the model and sell the future"—turning potential risks into revenue opportunities. We recommend piloting A2A integrations with Lumen for high-value scenarios like emerging tech forecasts to realize immediate gains.

For more information on implementing A2A with Lumen, contact Backflipt or visit backflipt.com/lumen.