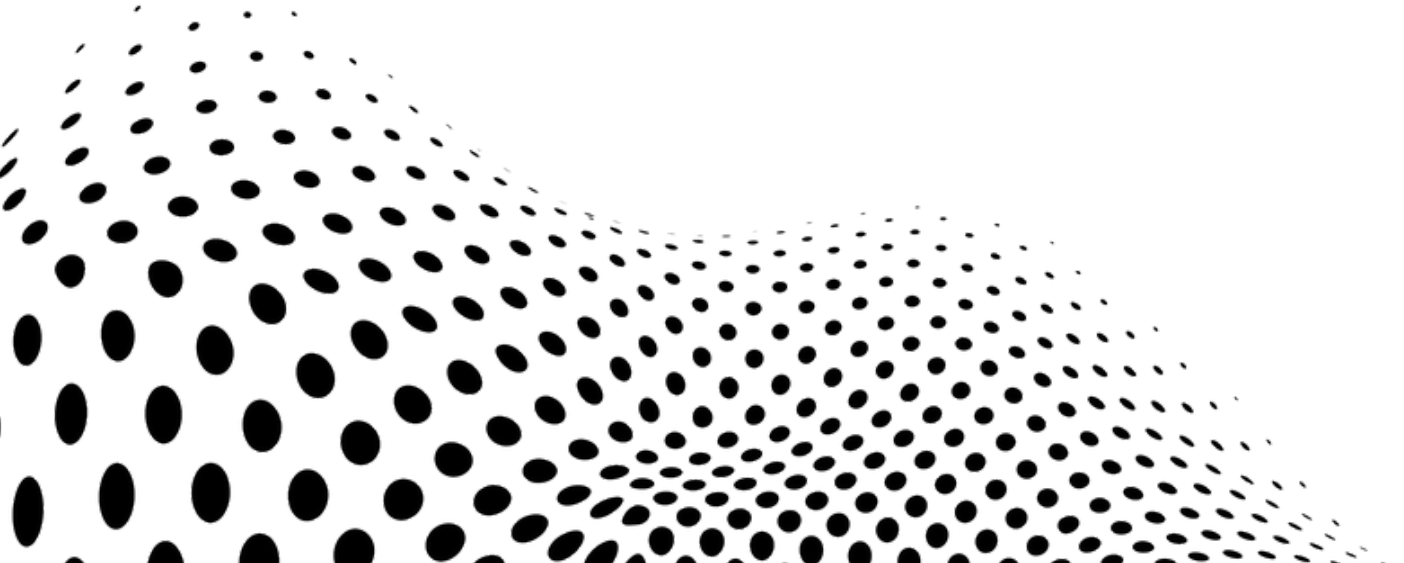
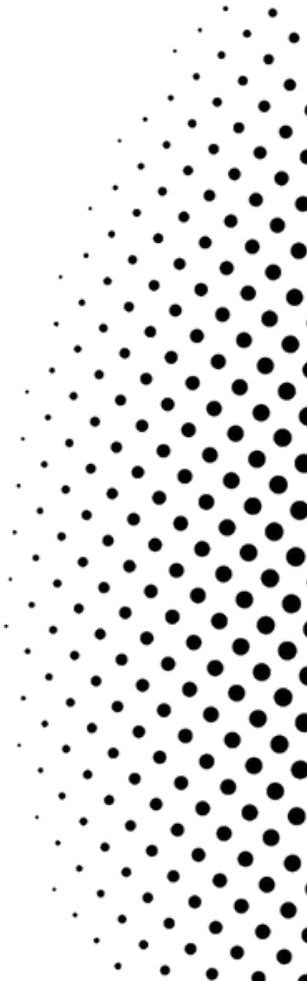
SPECIAL REPORT

TECHLED
EMPOWERING TECH LEADERS

The Next Generation of Enterprise Grade AI solutions has arrived

First to market, UNSEEN capabilities





Let's talk honestly about the current AI for Enterprise landscape:

The hidden pit-falls of fast-start licensing models

The prevailing enterprise AI adoption process is typically:

- subscribe to a leading API,
- prototype a few workflows,
- scale as usage grows.

This sequencing is rational for prototyping and optimises speed-to-market but crucially, it defers issues around control, cost governance and strategic leverage.

As pilots morph into production systems, these inherent inhibitors rapidly surface:

- competitors can access identical capability through the same API;
- spend becomes sensitive to external price changes and usage bursts;
- tailored strategic direction is sacrificed to provider roadmaps;
- your compliance story depends on vendor policies outside your boundary, with regulatory and assurance frameworks sharpening those tensions*;
- even uptime and geopolitical exposure depends on promises beyond your perimeter**.

These are not incidental bugs but features of the licensing model.

*The NIST AI Risk Management Framework (AI RMF 1.0) and its Generative AI profile emphasise governance, measurement and context-appropriate controls throughout the AI lifecycle.

**The EU AI Act (final text published 12 July 2024) formalises risk-based obligations-transparency, oversight, data and model governance, especially for high-risk uses.

Which AI agent fits your enterprise solution?

Four structural pain points

1 Differentiation ceilings

When multiple firms license the same off-the-shelf model, innovation paths converge. Prompt engineering and orchestration can delay parity but rarely prevent it and the innovation ceiling becomes a painful reality for every organisation in the race for market share. By its nature, AI enablement for enterprise means that the 'one-size-fits-all-with-some-customisation' model is dead. In its place has emerged a domain-specific solution, with expert models orchestrated for particular task clusters - an architecture designed to compound unique performance and prove why "fit" beats monolithic generality, at scale.

2 Cost volatility and TCO drift

Consumption pricing (per-token fees, data egress and tiered limits) introduces budget unpredictability, as usage scales. Even "free" open-weights typically require significant GPU capacity, fine-tuning cycles and specialised MLOps talent to sustain quality. This merely shifts costs from OPEX to CAPEX, without eliminating them.
Now, enterprises can opt for highly-optimised AI deployments, with 5-8x efficiencies for real-time inference at enterprise load profiles and at an extra-lean price point exemplified at: $0.80 per 1M input tokens and $4.00 per 1M output tokens.

Compared to existing licensable solutions, this represents a huge price-differential, resulting in large unit-economics gains in an enterprise's steady-state processes and / or production.

3 Governance, privacy, and residency gaps

Regulated industries require verifiable control over data flows, audit trails and locality. SaaS abstractions make assertions ("no train," "no retain") but still move inference outside the enterprise boundary. Recent policy shifts at major providers (e.g., default inclusion of chat data for model training unless users opt-out) are reminders that vendor decisions can alter your risk profile overnight if you don't control the stack.
Now, enterprises can ensure their complete functionality is isolated in air-gapped environments with zero external dependencies, multi-layer encryption, and total ownership of their models, code and IP.
For regulated settings, this design tightens the compliance posture by construction rather than policy.

4 Operational mismatch

Mission-critical uses demand latency SLOs, failure isolation and deterministic behavior under network constraints. Sovereign or on-prem requirements (common in finance, health, critical infrastructure, public sector) magnify the operational appeal of architectures that can run **without external dependencies**, where monitoring, evaluation and update pipelines live inside the boundary.
An on-premise, private-cloud, hybrid and edge deployments, with self-contained operation and "zero external API dependencies" approach, removes network calls as a systemic bottleneck and raises the ceiling for deterministic performance.

The solution?

Enter the next generation of enterprise grade, AI capability.

A groundbreaking tech house has brought to market a foundational AI platform, where enterprises can build the unique solution that their business needs. The result? **Enterprises can now become 'designer-owners' of the AI technology.**

Deployed within the customer's own infrastructure, with air-gapped options, full IP ownership and built-in compliance scaffolding, Ultrasafe's team will clean all legacy data, manage the bespoke installation and enable every customer to develop the tech they need.

Analytical framework:
A Diligence-to-Decision Trajectory

A general, buyer-agnostic framework for evaluating AI options focuses on five dimensions:

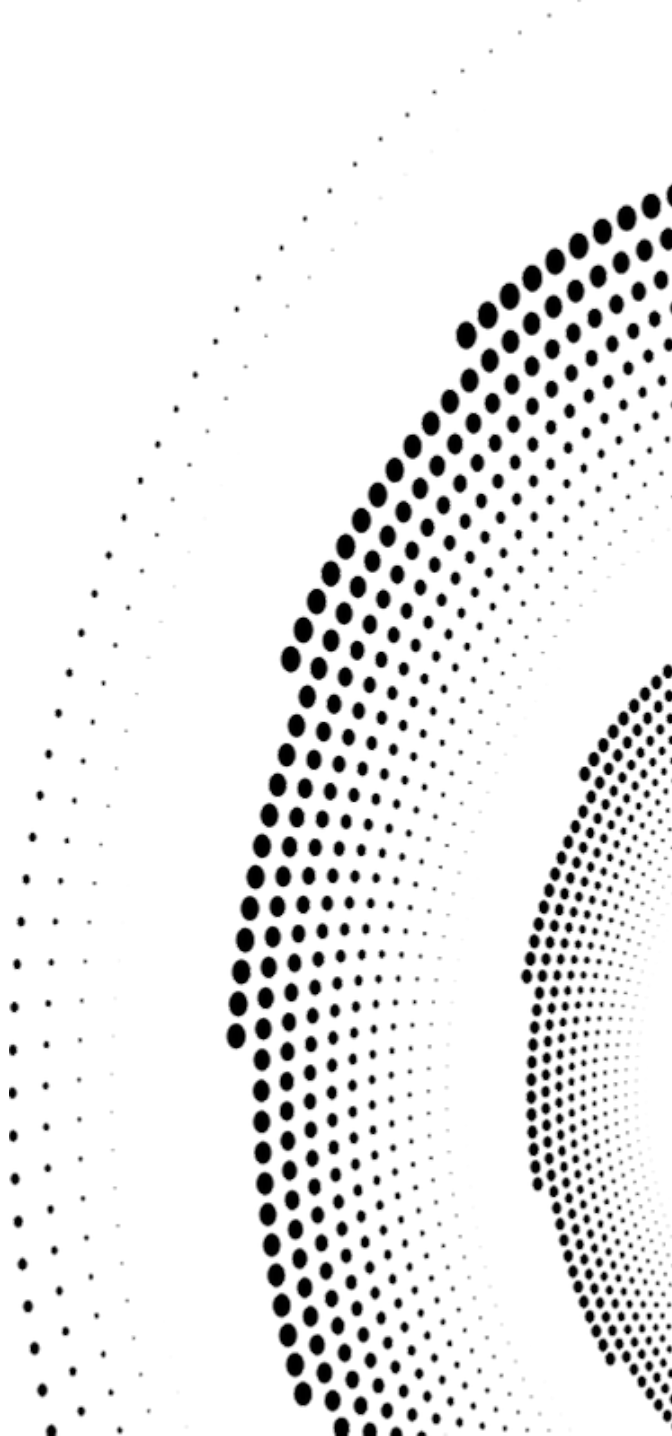
Control & sovereignty. Can the system operate entirely inside your boundary (including air-gapped) with auditable controls and no mandatory external calls? This determines how well you can satisfy regime-specific duties and your own risk posture. **Enterprises can now select an AI solution that offers this as a default design choice, not an exception.**

Ownership of IP and artifacts. Do you own model weights, fine-tunes, prompts, agents and application logic—or are you effectively renting them? Ownership not only actively creates value through growing proprietary capabilities that compound value over time, it prevents subsidising an external platform, either intellectually or financially, and crucially prevents leakage of competitive signals across customers on the same platform.

Fit-for-purpose performance. Do you have the latitude to move beyond a monolith e.g., to expert-routed or task-specialised models that better match domain workloads? Now, models are fine-tuned for industry-specific tasks, avoiding wasted cycles on irrelevant outputs.

Cost stability and efficiency. What is the steady-state cost at your expected task mix (context length, generation length, latency targets)? Token prices, feature surcharges, and hosting assumptions should feed a **per-workflow** unit-economics model, not just a per-token one. **The latest AI enterprise technology is capable of stabilising TCO, whilst demonstrating an absolute $/token advantage of 3-4x lower than existing, leading models.**

End-to-end operability. Production needs more than a base model: data pipelines, RAG/tool use, agent orchestration, monitoring, evaluation, rollback and incident workflows. Now, this full application layer can be deployed within the enterprise's stack, significantly closing the gap between experimentation and durable operations.



A foundation for ownership, control and performance

A mid-market financial-technology firm (~$2B valuation) initially doubted whether a genuine, end-to-end, foundational product was available to Enterprises at this point and, if so, whether it could outperform a licensed stack it already knew. It dispatched senior technical architects to perform an on-site, multi-day evaluation. Observing a full stack running privately—model routing, application layer, monitoring and evaluation, and air-gapped operation—shifted the decision: **within two months, the company committed to an exclusive, seven-figure annual engagement**.

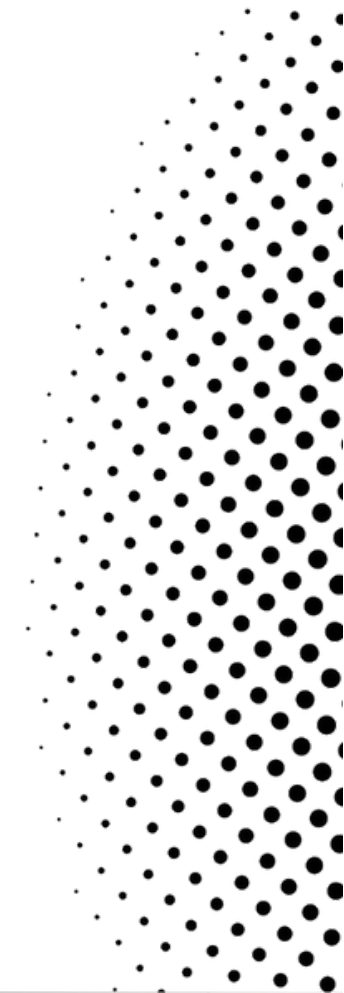
UltraSafe - The NextGen enablers of Enterprise AI capability

UltraSafe gives enterprises full flexibility in how they deploy AI.
They offer a complete AI operating system covering the full lifecycle of enterprise intelligence:

- **Data Structuring** to clean and prepare raw data.
- **Multimodal Intelligence** across text, voice, images, video, and documents.
- **Vision AI** for document processing, surveillance, and industrial inspection.
- **Reasoning & Analysis** aligned with enterprise business logic.
- **Agent Orchestration** to automate workflows and connect APIs.
- **Voice AI** for speech recognition, translation, and synthesis.
- **Code AI** for development assistance, DevOps, and system optimization.

The modular design allows clients to adopt the full stack or only the components that match their roadmap.

LICENSING AI IS RENTING INTELLIGENCE. PARTNERING WITH A FOUNDATIONAL AI GIVES YOU OWNERSHIP AND CONTROL.



Ultrasafe AI vs. Open-Source & proprietary models

Feature	GPT-2.0 / LLAMA / DeepSeek	Mistral	GPT-4o / Grok (OpenAI, xAI)	ULTRASAFE
Model Type	Open-source, general-purpose	Optimized open models	Closed, black-box SaaS	**Custom-built expert model per client**
Knowledge	General, outdated or average	Better general knowledge	Broad-scale, general knowledge	**In-depth domain-specific knowledge**
Customization	Fine-tuning, basic config	LoRA, fine-tune possible	No access to internals	**Full customization: model, memory, logic, prompts**
Quality on Real Tasks	Unstable without tuning	General, not focused	High on general tasks	**High precision on specific enterprise tasks**
Expert Model Strategy	Single large model	One-size-fits-all	Monolithic multimodal	**Multiple expert models for task clusters**
Speed / Latency	Infra-dependent	Fair	Fast but external API adds delay	**Ultra-low latency, real-time optimized**
Data Privacy	Self-managed	Possible	Data leaves Infra	**Full privacy: on-prem or private infra**
IP Ownership	Public, reused by anyone	Open weights, reusable	You own nothing	**Custom weights = your private IP, never reused**
R&D Updates	Rare (6–12 months)	Irregular, community-based	Internal only	**Regular improvements, applied directly to your stack**
Multimodal Support	Mostly text-only	Some vision support	Full multimodal (closed)	**Native: text, image, video, audio, sensors, robotics**
Deployment	Self-setup	DIY required	SaaS only	**Cloud, edge, on-prem, hybrid – full flexibility**
Running Cost	▲▲ Very High (infra + tuning)	▲ High infra + tuning	▲▲▲ Extremely expensive long-term	✅ **Highly optimized: 5–8x compute-efficient deployment**

UltraSafe’s core business differentiators?

Exclusive IP Ownership:
Your customised model weights, your prompts.
No one else can access or use what is built for you

Privacy-First Deployment:
No data leaves your environment. Ideal for finance, defense, healthcare and secure domains

Expert Ecosystem:
From data to deployment, UltraSafe’s AI/ML teams design, train, tune, and integrate the full solution

Speed + Quality:
With modular expert models, UltraSafe offer faster, higher-quality results than general-purpose LLMs$

Real-World Ready:
Unlike open models that require heavy DevOps, Ultrasafe is optimised for quick, low-cost, high-performance deployment.

Ultrasafe are reframing licensed AI as a transitional convenience, while positioning foundational AI as “graduation to ownership.”

The Chief Architect at Ultrasafe will be running just two live, online events to take questions and run an introductory demonstration on their work.

REGISTER HERE

To ensure each session allows adequate time for all attendees to interact as fully as possible with the team, spaces are limited to 50 per event, with each seat for separate organisations.

The NextGen enablers of Enterprise AI capability

The legacy way

- Renting Intelligence - not owning it, limits your strategic leverage
- Leaves you exposed to external pricing policies, compliance and geographical risks outside of your company's domain
- Adopting "me too" licensed models, chokes your scope for market differentiation

The new way

- 100% bespoke intelligence, cultivated from your own processes and data sets
- Autocratic control of costs, data governance, technology roadmap and strategy
- All legacy data cleaned, aggregated and replicated in an air-locked, on-premise environment

ULTRASAFE

Unique ROI

Never before has a tech vendor included its source code in its product offering, enabling enterprises to ‘build and own’ their bespoke solution, from the foundation up.

What does this actually mean?

Delivering the expected returns is a given. Ultrasafe are offering a business model beyond that. They are enabling enterprises to develop specialist AI solutions, unique to their sector, own the prototype and onward sell that solution to their market peers.