Solution Brief

SUPER

Verifiable Compute for End-to-End AI & Data Sovereignty

Provable privacy from data collaboration to training and inference

This brief outlines Super Protocol's core capabilities, real-world case studies from clinical diagnostics to regulatory compliance, demos showing Confidential AI with built-in verification in action from an expert session at AI Engineer World's Fair, and references from NVIDIA, the University of Miami, and other industry leaders.

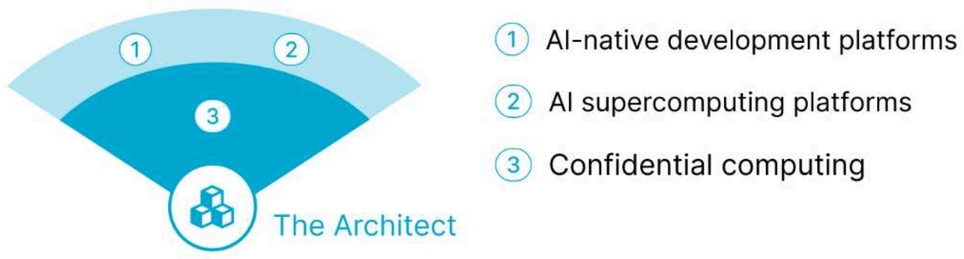
Solving the Healthcare Data Paradox

The healthcare industry faces a Data Paradox: high-performance AI is constrained by infrastructure and compliance challenges. On-premise hardware often lacks the capacity for modern AI, yet scaling beyond local infrastructure typically requires trusting public clouds with sensitive patient data. Furthermore, meaningful collaboration is restricted without moving or exposing data. As a result, organizations are forced to compromise between performance, privacy, and their ability to collaborate across healthcare organizations.

Super Protocol resolves this paradox by providing a verifiable secure execution environment for AI training, inference, and collaboration. Confidentiality is enforced at the architecture level, with Confidential Computing as a foundational security layer that protects data and models during execution. Sensitive data, proprietary AI models, and agents are never exposed to hardware operators or to Super Protocol itself.

This approach aligns with the global shift toward hardware-enforced security. Gartner's 2026 Strategic Technology Trends identify Confidential Computing as a top priority and a core architectural requirement for secure AI, enabling high-stakes analytics across untrusted infrastructure. This is mirrored by market adoption: IDC reports that 75% of organizations are already adopting Confidential Computing – either in production or active piloting – as their strategic foundation for securing AI workloads.

Gartner Top Strategic Technology Trends for 2026



Unlock the Power of AI for Healthcare

Super Protocol delivers a secure infrastructure layer that turns modern NVIDIA H100, H200 and Blackwell GPU Hardware into a verifiable, privacy-preserving AI workspace. Open source by design, it works seamlessly across any cloud or hospital servers, ensuring that everything, from sensitive data to proprietary AI models and agents, remains provably protected. This architecture transforms privacy from a policy promise into a practical, high-performance reality across key healthcare frontiers.

1. Building Specialized AI (Confidential Fine-Tuning)

By training general-purpose or medical foundation models on proprietary clinical and administrative data, Super Protocol enables the creation of specialized medical assistants that understand nuances of individual departments, including oncology, radiology, cardiology, as well as internal workflows, delivering medical-grade accuracy.

Case Study: ↗ Learn More

Yma Health fine-tuned Google MedGemma on real clinical dialogues and patient-doctor consultations within Super Protocol. Independent evaluations by practicing endocrinologists demonstrated that the model matches human safety levels: **79%** (vs. **82%** human baseline), far outperforming ChatGPT-4 **(70%)**. By unlocking access to previously restricted sensitive data, the AI achieved a **9.4/10** clinician recommendation score.

2. **Protecting AI in Action** (Confidential Inference)

Super removes the need to rely on promises of confidentiality by making protection automatic. AI workloads run only when both the environment and workload itself are verified as trusted. If either does not meet security requirements, execution does not start. This enables healthcare organizations to safely apply AI to highly sensitive data and automate critical processes without exposing data to cloud providers, infrastructure operators, or third parties.

Case Study: ↗ Learn More

By using Tytonyx's AI-agent within Super Protocol, Brain Electrophysiology Laboratory (BEL) transformed its regulatory workflow. BEL automated the auditing of its FDA applications for medical devices without exposing its proprietary **"trade secrets"** to any third party. This shift reduced compliance review times from **4 weeks to just 2 hours,** and eliminated the risk of human-caused iterations that typically delay product launches by up to **120 days.**

3. **Seamless AI Integration** (The "Smart Hospital" Upgrade)

Super enables hospitals to scale their AI capabilities without re-architecting their IT environment or changing how teams work. It removes the hidden security and compliance complexity behind medical AI, allowing NVIDIA GPU infrastructure – on-premises or in the cloud – to be used safely and on demand. As a result, organizations can deploy and use AI solutions through familiar workflows, accelerate time to value, and avoid the need to build or maintain specialized in-house security or infrastructure expertise.

Case Study: ↗ Learn More

Using Super Protocol, Yma developed an anonymization middleware. It creates a protected tunnel that enables hospitals to apply advanced AI to real patient data without exposing identities or changing existing EHR/IT systems.

Customer Quote:

> "We wanted to use AI for personalized patient communication, but sending data to external APIs was a non-starter. YMA's anonymization service solved this perfectly – now we can leverage advanced AI while our patient data stays completely protected."

4. Multi-Party Collaboration

Super Protocol enables institutions to securely collaborate on joint assets without ever exposing them. Inside a "double-blind" workspace, one provider can run their proprietary AI directly against another's factual clinical datasets. Both the data and model logic remain completely invisible and inaccessible to each party, allowing them to retain full control and protect the proprietary IP of their assets, while ensuring privacy, compliance, and improved clinical outcomes.

George Jimsheleishvili, M.D. University of Miami:

> "Interinstitutional collaboration in healthcare relies on access to real-world clinical data. However, constraints associated with protected health information (PHI) and regulatory compliance (e.g., HIPAA, IRB) frequently render data sharing impractical or infeasible. Super Protocol enables hospitals and research institutions to perform approved analytical and AI workloads on sensitive data without data transfer or direct access, while maintaining patient privacy, data ownership, and governance."

▶ Watch Podcast

From Theory to Action

Selected from over 1,000 global submissions, Super Protocol was chosen to showcase the Verifiable Confidential AI at the AI Engineer World's Fair.

A clear, accessible introduction to the fundamentals of Verifiable Confidential AI and Super's real-world case studies

▶ Watch Expert Session

Demos

Collaborative Training	▶ Provable medical AI training with on-chain reporting
Agents	▶ n8n Automated Healthcare AI Workflows
Marketplace	▶ Verify isolated execution in seconds

Tech Deep Dive

From the fundamentals of Confidential Computing to Super Protocol implementation, automatic verification demo, and hardware requirements.

1. **The Fundamentals:** Remote Attestation

Learn the core logic of hardware-level verification

↗ Technical Intro ↗ Advanced Use Cases

2. **Super Protocol:** Certification System & Trusted Loader

Learn how Super Protocol simplifies Remote Attestation, turns GPU fleets into confidential execution environments, automates environment verification, and extends hardware security to the workload level — ensuring integrity and confidentiality by architecture.

↗ How We Use Attestation ↗ The Trusted Loader ▶ Demo

3. Core Hardware Requirements

Confidential mode requires compatible GPU and CPU TEE support.

↗ GPU + CPU TEE Requirements

Strategic Partnership & Trust

Our core team is a pioneer in decentralized confidential computing and verifiable AI infrastructure, with over a decade of experience securing intellectual property, personal data, and AI for global brands. This expertise is validated by:

NVIDIA

> "Super Protocol extends protection to every layer of AI workflows, ensuring verifiable security and performance in trusted execution environments from the infrastructure core all the way to frontline clinics." **John Fanelli, VP Enterprise AI**

↗ Read More

Exploring the Case of Super Protocol with Self-Sovereign AI and NVIDIA Confidential Computing

↗ NVIDIA Blog

intel

Over a decade of collaboration with Intel's Confidential Computing team, shaping the real-world adoption of Confidential Computing for sensitive workloads through a decentralized approach.

▶ Watch Expert Session

Super Protocol's Certification System uses Intel Software Guard Extensions (SGX) as the root of trust for automatic verification, while AI and data processing run across heterogeneous CPU and GPU Confidential Computing environments.

↗ Intel SGX Product Offerings

Google

The completed integration enables fully automated Verifiable Confidential AI within Google Cloud and extends the same verifiable protections to cross-cloud collaboration with external partners – without shared trust or manual coordination.

↗ Google Cloud Blog

CANONICAL

↗ Read More

> "Super Protocol builds the industry's first confidential Web3 AI and Data marketplace with Ubuntu confidential VMs."

↗ Canonical Case Study

Proven Expertise

Our core team's track record of developing and scaling platforms for global market leaders includes:

Super Protocol (2021 – Present)

A verifiable, privacy-preserving AI infrastructure layer with no central operator or trust assumptions. Implemented through real-world projects in Healthcare, Research, and other highly data-sensitive industries.

Confidential Data Collaboration Platform (2019 – 2021)

A platform used by large enterprises to securely collaborate on analytics over sensitive datasets, leveraging confidential computing and decentralized execution – enabling practical outcomes such as improved targeting, without disclosing raw data.

Media Management Platform (2015 – 2019)

An enterprise media platform used by global leaders such as **Disney and Pearson**, handling digital entitlements, complex access control, and multi-partner content distribution at scale.

Further details and examples of these projects can be found in Super Protocol's collection of case studies.

↗ Check Case Studies

Next Steps

Explore business use cases and deep dive into implementation at superprotocol.com