

Armet AI

Turnkey Agentic AI Platform Built on Confidential Computing

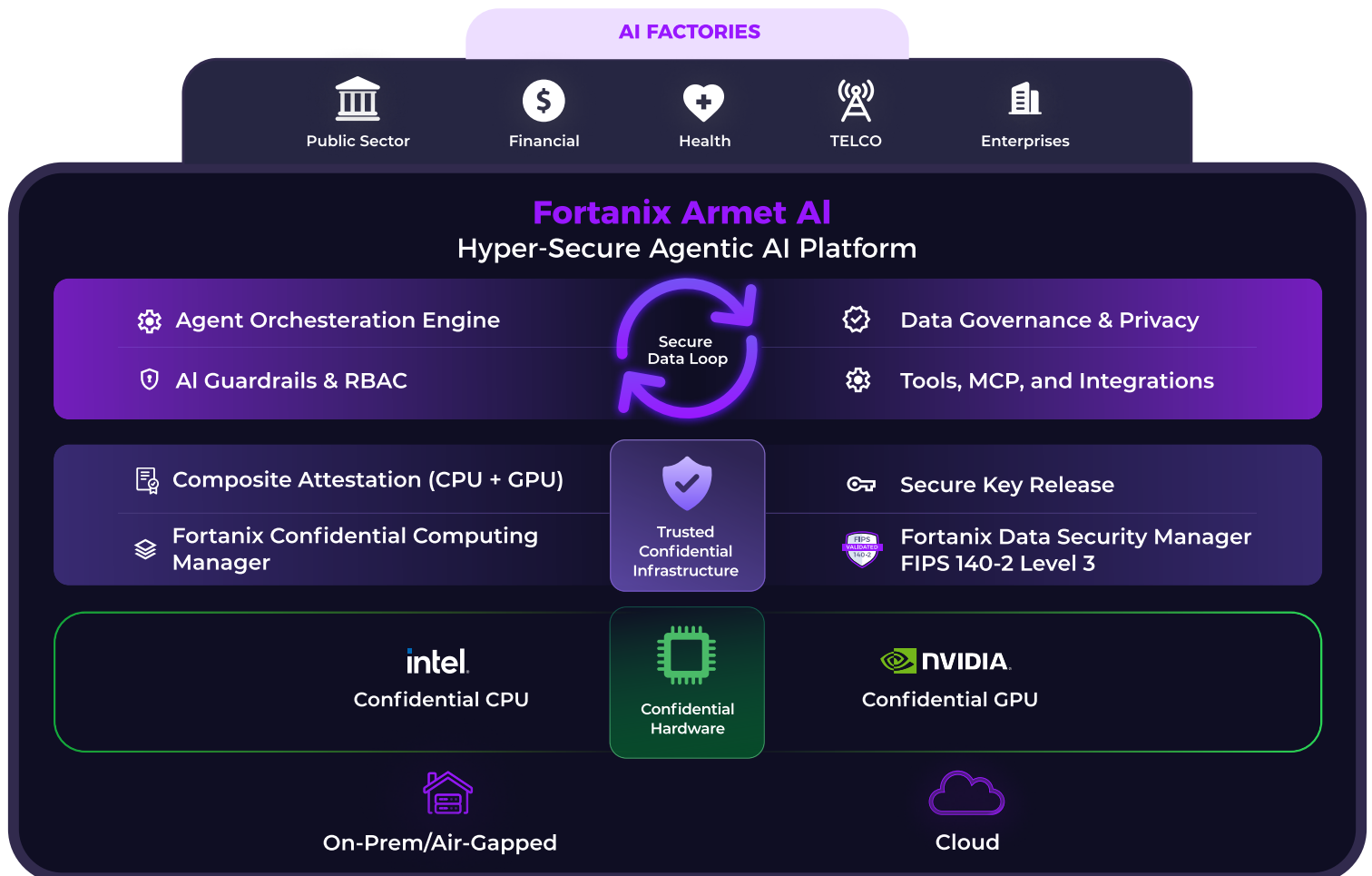
Enterprises are eager to adopt AI to enhance customer experiences, drive competitive advantage, innovate and push boundaries. As teams explore Agentic AI -- the main concern overshadowing every potential breakthrough is security. Worries about exposing sensitive data, losing control over models, falling short of compliance mandates and sovereignty requirements, or opening the door to new cyber vulnerabilities is holding organizations back. To overcome the roadblocks, organizations need to have complete trust in the security of the AI deployments, backed by auditable proof.

Powering Innovation with Verifiable Trust, Security, and Sovereignty

Fortanix Armet AI delivers industry-first turnkey Agentic AI platform, powered by NVIDIA breakthrough confidential computing GPU. By combining Confidential Computing with turnkey Agentic AI orchestration, backed by composite attestation and secure key release, Armet AI ensures that:

- ✓ Each agent or model instance proves its integrity before accessing sensitive data
- ✓ All actions (training, inference, data access) are audited and policy-enforced
- ✓ Keys, models, and datasets are released only to attested workloads through HSM-gated secure key release

Unlike other solutions that offer a piecemeal approach, Armet AI is a holistic solution built on the world's most secure technology. It gives enterprises a proven path to innovation-- teams now can streamline deployments and go from pilot to production in days, with data and AI security, trust, and sovereignty at the core.



Key Benefits



Security Without Compromise

Protect your business with a Trusted Execution Environment to isolate and process data and AI privately



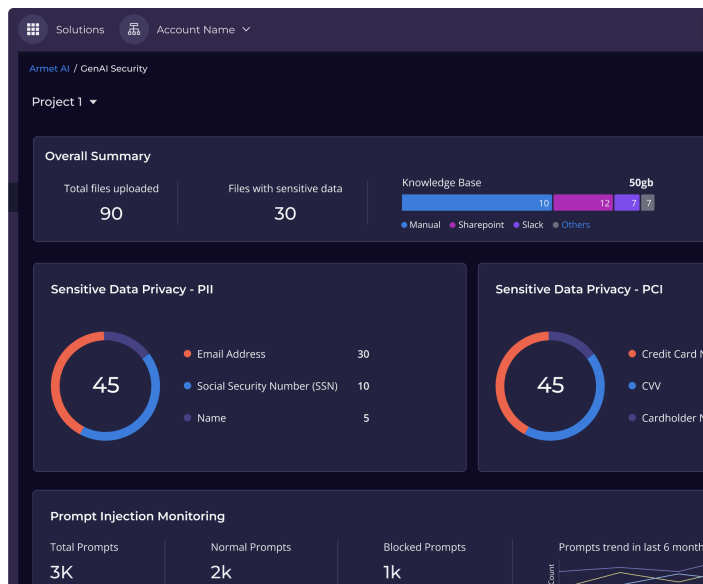
Compliance by Design

Drive regulatory compliance, maintain sovereignty, and enable frictionless audits



Drive Speed and Agility

Tailor to your needs and go from pilots to production in days with turnkey solution



Key Features



Turnkey Agentic AI Platform: Secure data, agents, and models at every stage with ready-to-use holistic Confidential AI solution



Composite Attestation Across CPUs and GPUs: Prove the integrity of the entire AI runtime stack with Fortanix Confidential Computing Manager and NVIDIA Remote Attestation Service (NRAS) for a single verified chain of trust



Secure Key Release: Ensure access to datasets and model artifacts only after verified attestation with Fortanix Data Security Manager, FIPS 140-2 Level 3 certified next-gen Hardware Security Model with built-in Key Management System



AI Guardrails: Protect data and model from insider and outside threats. Shields sensitive data by anonymizing it and filter harmful inputs and outputs



Consistent Control and Governance: Universal policy enforcement across the complete AI pipeline, applied at the source-level with granular permissions and rules that define who can train, use, and see what data



API-First Architecture: Bring data from any source and support integration SIEM frameworks and automation workflows

The Fortanix Difference

- ✓ State of the art data and AI security platform, built end-to-end on Confidential Computing
- ✓ Built-in AI guardrails and governance
- ✓ Secure Key Release and uniform policy enforcement

About Fortanix

Fortanix is a global leader in data security. We prioritize data exposure management, as traditional perimeter-defense measures leave your data vulnerable to malicious threats in hybrid multi-cloud environments. Our unified data security platform makes it simple to discover, assess, and remediate data exposure risks, whether it's to enable a Zero Trust enterprise or to prepare for the post-quantum computing era. We empower enterprises worldwide to maintain the privacy and compliance of their most sensitive and regulated data, wherever it may be.

For more information, visit www.fortanix.com.