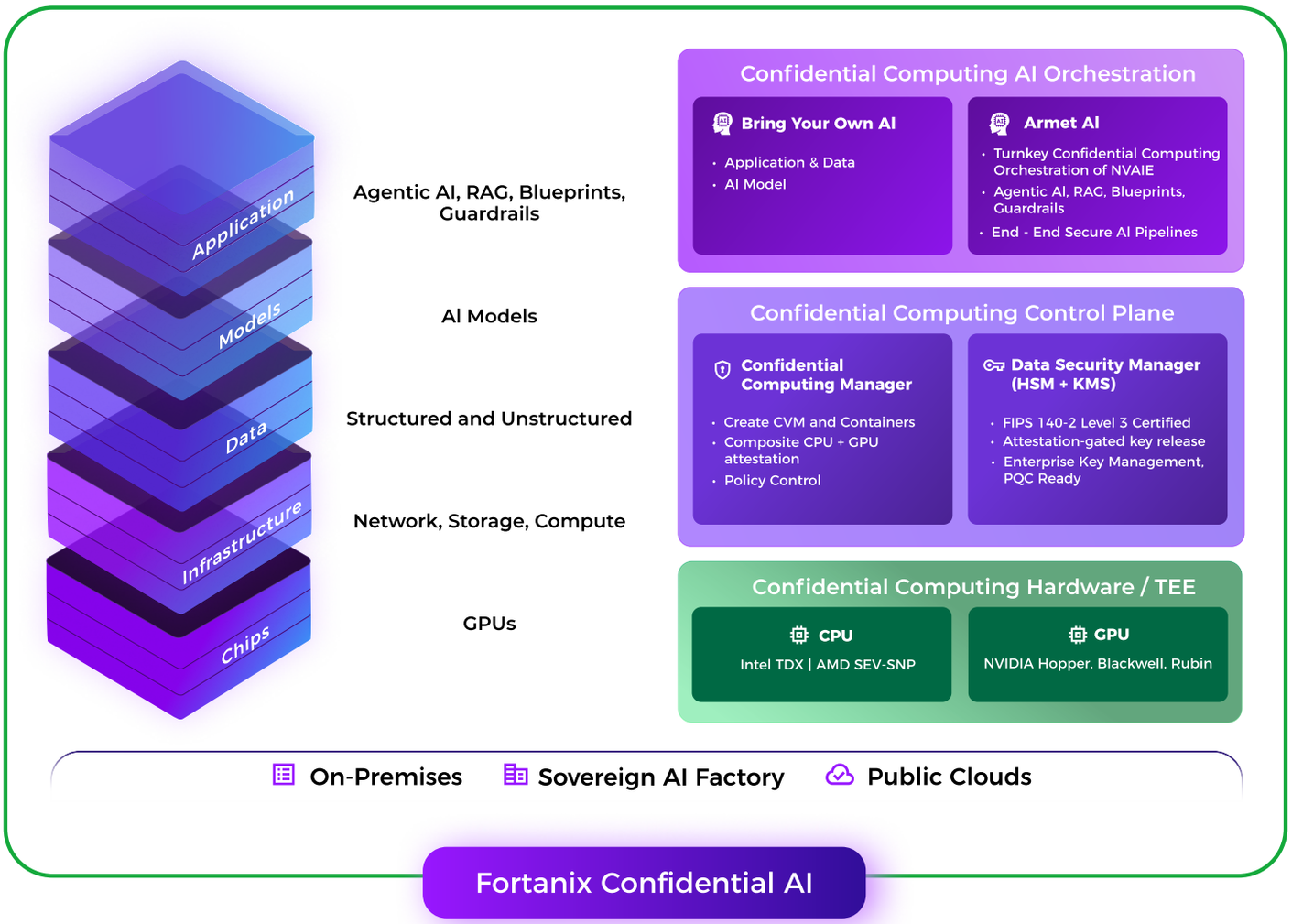
Fortanix Confidential AI

Protect AI Models and Sensitive Data Throughout the Entire AI Lifecycle

Data exposure and intellectual property theft are blocking AI adoption across enterprises and nations. Over half of enterprise IT leaders cite data security risks as a fundamental obstacle to AI deployment, while AI model owners hesitate to deploy their valuable intellectual property in third-party environments, whether AI Factories, cloud platforms, or edge infrastructure. In traditional infrastructure settings, administrative access provides complete visibility into both data and AI models during processing sensitive data sits unencrypted in memory during inference and training, while AI models remain vulnerable to extraction attacks. Thus the dilemma remains: how do you advance AI innovation without risk and exposure of your most precious assets?

Fortanix Confidential AI

Fortanix Confidential AI help eliminate the barrier of AI adoption by protecting both proprietary AI models and sensitive data while in use to accelerate AI innovation without compromising security, trust, and sovereignty. The joint NVIDIA and Fortanix solution is built on specialized Confidential Computing GPUs to protect AI models and data in use by performing computations in secure, hardware-isolated environments. Those Trusted Execution Environments (TEEs) are isolated from the rest of the hardware and operating system. You now can run your AI workloads with cryptographic guarantees that sensitive data and proprietary models remain confidential even from privileged insiders.



How Fortanix Confidential AI Works

Secure Enclave Management

Leveraging Intel TDX and AMD SEV-SNP CPUs alongside NVIDIA Hopper, Blackwell, and upcoming Rubin confidential computing GPUs, create and manage secure enclaves with Fortanix Confidential Computing Manager (CCM). Isolate your AI workloads from OS, hypervisor, and administrators. Control and enforce policy for your Trusted Execution Environments.

Bring Your AI Workload

Bring Your Own AI model, or a model from 3rd party provider, including Fortanix Armet AI, a turnkey Agentic AI orchestration platform, to support your AI strategy and needs.

Attestation Verification

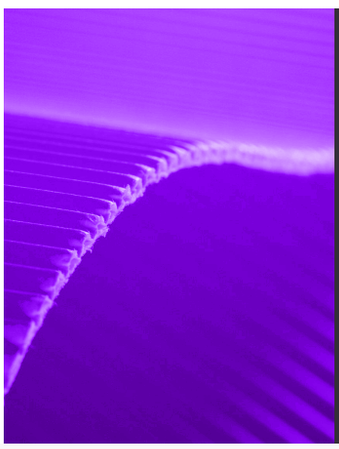
Before sending encrypted assets and artifacts, verify the remote TEE through cryptographic attestation with Fortanix CCM. Confirm the exact code is running, and that hardware isolation is genuine and has not been tampered with.

Secure Key Release

Encryption keys are sent only to verified, attested TEEs. Using Fortanix Data Security Manager (DSM), a FIPS 140-2 Level 3 HSM with built-in KMS, enforce strict key custody and role-based access controls to ensure that data and models remain encrypted in memory, while in use, inaccessible to anyone outside the TEE.

Benefits of Comprehensive AI Lifecycle Protection

- **Protect Model IP:** Deploy AI models to third-party environments, cloud platforms, or edge locations without revealing IP.
- **Confidential Inference:** Process sensitive inputs and outputs without exposure to infrastructure providers.
- **Prevent Data Leakage:** Ensure data used in the AI workload remains encrypted even while being processed.
- **Multi-Party Collaboration:** Enable data sharing and model access across organizations without exposing underlying assets.
- **Zero-Trust Architecture:** Protection is backed by attested cryptographic verification for CPU and GPU silicon, not software policies, eliminating the need to trust cloud providers, infrastructure operators, or administrators.
- **Compliance-Ready:** Meet regulatory requirements for Cloud act, PII, PHI, and sensitive data protection.



"AI is foundational to the initiatives we've launched to tangibly transform pharmaceutical research and development, but models require extremely large amounts of data that often contain sensitive or personal information. Confidential Computing from Fortanix and NVIDIA essentially alleviates those privacy and security concerns while also improving model accuracy, which will prove to be a win-win situation for the entire industry."

Hiroki Makiguchi
CTO at Xeureka.

Xeureka

About Us

Fortanix is the global leader in data and AI security and a pioneer of Confidential Computing, delivering a unified platform to protect sensitive data, AI models, and applications across on-premises and multi-cloud environments—at rest, in transit, and in use. Built on hardware-enforced security, Fortanix enables workloads to run in tamper-proof, isolated enclaves, protecting against data leakage, model extraction, and unauthorized access, even from privileged insiders.