Fortanix

SOLUTION BRIEF

A Single Control Plane for Your Confidential Computing Stack

Confidential Computing technology protects data, AI models, and applications in use by performing computations in a hardware-based, isolated Trusted Execution Environment (TEEs). It ensures workloads remain inaccessible to unauthorized parties, including infrastructure providers, operating systems, and privileged insiders, while they are processed, in active use. While TEEs are not new, managing them at enterprise scale is. From navigating a fragmented landscape of management interfaces, attestation flows, and operational demands to different management interfaces, configuring Confidential CPUs and GPUs, on –prem or across cloud providers, is not a small feat. Manually coordinating attestation or writing custom integrations, all while trying to maintain consistent security policies and audit trails across the full Confidential Computing stack, leads to security vulnerabilities, operational overhead, or key release decisions without full visibility into the environment. For enterprises running sensitive data and valuable AI models, those gaps are unacceptable.

Unified Approach to Managing Confidential Computing

With Fortanix Confidential Computing Manager (CCM) you now can easily manage secure enclaves, verify firmware and software integrity, and enforce attestation policies at scale. CCM provides a single control plane to create, attest, and manage the full lifecycle of Trusted Execution Environments across your entire AI infrastructure. From enclave provisioning to signaling secure key release from Fortanix Data Security Manager, CCM enforces trust and consistent security, giving organizations the foundation to run sensitive AI workloads and third-party frontier models without compromising security, sovereignty, or compliance.

info@fortanix.com | 3910 Freedom Circle Suite 104, Santa Clara, CA 95054, United States

Key Capabilities

- Single control plant to manage policy and monitor your entire Confidential Computing infrastructure CPUs and GPUs
- Streamlined workflows with low code/no code interface facilitate mutli-party secure collaboration
- Composite attestation for CPUs and GPUS for a single chain of trust ensures no gaps exist between the different components
- Firmware and software integrity verification check before signaling secure key release from Fortanix Data Security Manager, a FIPS 140-2 Level 3 next-gen HSM with built-in KMS
- Support for
  - Intel TDX and AMD SEV-SNP CPUs
  - NVIDIA Blackwell and Hopper Confidential GPUs
- Available on-premises and as SaaS

How It Works

Provision & Configure

Deploy Trusted Execution Environments across your CPU and GPU infrastructure from a single control plane, abstracting the complexity of Intel TDX, AMD SEV-SNP, and NVIDIA Confidential GPU configuration into unified, repeatable workflows.

Attest & Verify

Perform composite attestation for CPU and GPU, along with software stack integrity before running any workloads. Tampered or unverified environments are automatically denied.

Release Keys & Run

Signal secure key release to Fortanix DSM only after attestation is verified and run data and AI models exclusively inside the TEEs. They are encrypted in memory, inaccessible to the host OS, hypervisor, cloud administrators, and privileged insiders while in active use

Monitor & Scale

Maintain continuous visibility across your entire Confidential Computing stack. Monitor enclave health, attestation status, and policy compliance from a single dashboard to scale AI workloads across your infrastructure.

Benefits

Run Powerful AI Without Compromise

Ensure data and model weights are never exposed, eliminate insider threats, and close the attack surface across the full inference lifecycle

Meet Compliance by Design

Cryptographic proof of data isolation at the hardware level satisfies GDPR, HIPAA, and data sovereignty requirements, turning compliance bottleneck into a built-in guarantee.

Maintain Full Sovereignty and Control

Run AI entirely on your own terms with zero-trust architecture. Have full control over deployments, data access, and model choices.

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. Learn more at www.fortanix.com.

info@fortanix.com | 3910 Freedom Circle Suite 104, Santa Clara, CA 95054, United States