Fortanix | RESEMBLE.AI

About Resemble AI

Resemble AI builds AI detection models that tell enterprise teams in real time whether the audio, video, or image in front of them is real or AI-generated. Each result comes with intelligence and a recommended next action, so fraud, security, and trust and safety teams can respond to a threat quickly.

Many of the organizations that need detection most, like banks, insurers, and government agencies, handle data that can't leave their environment, so they ask to run Resemble AI on their own premises. Fortanix makes that possible without putting Resemble AI's model at risk

Enabling Secure Distribution of Resemble AI

Fortanix Confidential AI lets enterprises run Resemble AI's AI detection models on their own infrastructure. Built on NVIDIA Confidential Computing, it runs the model inside hardware-enforced Trusted Execution Environments (TEEs), so the model and the media it analyzes stay protected while in use, not only at rest and in transit. Enterprises get real-time detection without sending customer calls, meetings, or identity verification media outside their environment, and they keep full control of the workload. Resemble AI can serve banks, insurers, government agencies, and other regulated customers on their own premises while its model weights stay protected from copying and tampering.

Benefits

Bring Detection On-Premises

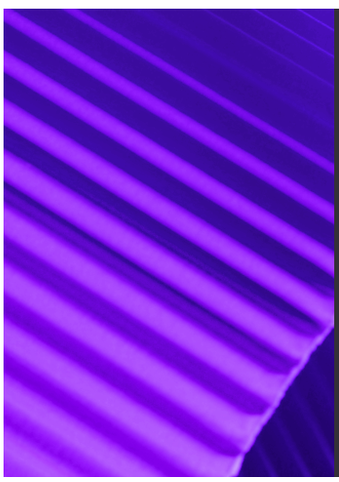
Run Resemble AI detection in your own data center or an isolated cloud environment. Confidential Computing answers the runtime exposure questions that slow down security reviews, so detection gets to production faster.

Prevent Sensitive Data Exposure

Analyze your most sensitive calls, meetings, and identity media inside a protected enclave on your own infrastructure. Detection runs in real time and the data stays under your control.

Stay Compliance-Ready

Keep complete visibility and command over every AI workload, from deployment to inference. Meet sovereignty and data protection mandates with auditable proof.



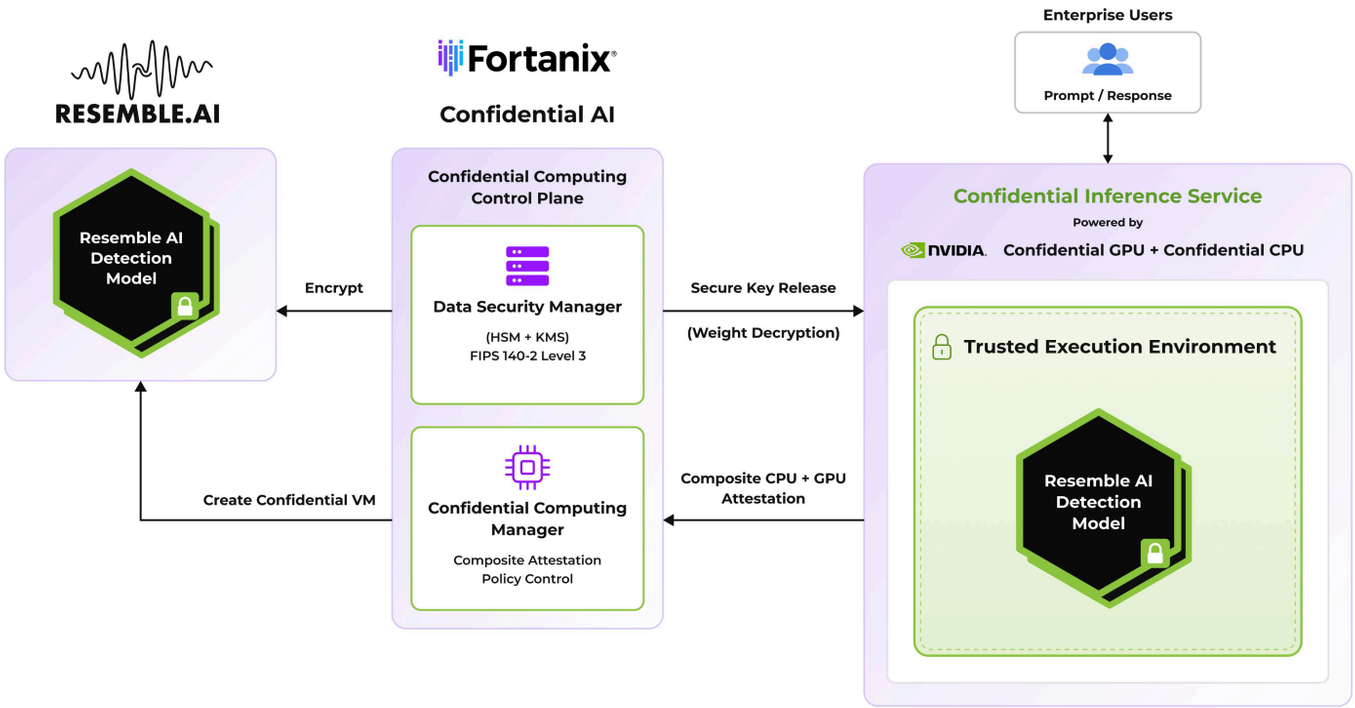
“The organizations facing the most AI fraud, like banks, insurers, and government agencies, are often the ones that can’t send their data to the cloud. Working with Fortanix on NVIDIA Confidential Computing lets us run our detection models inside their environment, with full end to end control over their data.”

- Zohaib Ahmed, CEO and Co-founder, Resemble AI

info@fortanix.com | 4500 Great America Parkway, Ste. 270 Santa Clara, CA 95054, United States

How Fortanix Confidential AI Works

- **Encrypt & Package:** Resemble AI model weights, code, and configurations are encrypted with a non-exportable key stored in Fortanix DSM (Data Security Manager), a FIPS 140-2 Level 3 Hardware Security Module, available on-prem and as SaaS. Each customer deployment gets its own key. The encrypted model is packaged into a Confidential VM image for distribution.
- **Composite Attestation:** Fortanix CCM (Confidential Computing Manager) manages the TEE, enforces attestation policies, and verifies the exact hardware CPU + GPU and software environments, confirming the enclave is genuine and untampered with before issuing a certificate.
- **Secure Key Release:** Only after both attestation checks pass are encryption keys released exclusively to the verified TEE. The Resemble AI model decrypts and runs inside the enclave. No admin, cloud operator, or privileged insider can access the weights.
- **Continuous Verification:** CCM re-checks the environment on an interval Resemble AI sets. If anything changes, Resemble AI can revoke the key and the model stops running. Every new Resemble AI model version goes through the same attestation and key release before it runs.



Supported Workloads

- Confidential VMs and Confidential Containers
- GPU: NVIDIA Hopper & Blackwell (Confidential Computing)
- CPU: Intel TDX & AMD SEV-SNP
- Deployments: On-premises, Air-Gapped, Sovereign AI Factory, Public Cloud

About Resemble AI

Resemble AI is the AI detection models company that delivers real-time, accurate detection results combined with intelligence and next-action recommendations. It's what enterprise teams need to detect a threat, protect their content, and make informed decisions quickly. Our models work across every modality, integrate with your workflows, and adapt to your deployment needs to make detection comprehensive, seamless, and secure. Learn more at resemble.ai.

About Fortanix

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.