Duality

SECURE AI APPLICATIONS WHILE DATA IS IN USE

Run your AI workloads and agents inside Trusted Execution Environments in your own environment, with the governance, security and monitoring to operate them.

Challenge: Your Data Is Protected Everywhere Except While AI Uses It

Banks, telecom providers, insurers and other commercial enterprises already encrypt data at rest and in transit. But an AI application has to decrypt data to work on it, and in that moment prompts, customer records and model weights sit in memory, open to anyone with privileged access to the host.

As more AI applications and agents handle regulated and proprietary data, that gap is the one security teams are asked to close.

The Solution: Add Protection While Data Is In Use

AT REST

Encrypted storage

Already in place in most enterprises.

IN TRANSIT

Encrypted networks

Already in place in most enterprises.

IN USE

Duality TEE

Applications run inside a hardware-isolated enclave that is attested before data is released.

Key Benefits

Better Security for AI

Protect data at rest, in transit and, with Duality, in use.

Deploy Any Application

Run AI applications, agents and custom apps inside a TEE without rebuilding them.

Govern Every Asset

Policies decide which applications may use each model and dataset.

Manage It All in One Place

One management layer for deployment, monitoring, security and governance.

HEADQUARTERS

5 Marine View Plaza, Hoboken, NJ 07030

CONTACT US

info@dualitytech.com

LINKEDIN

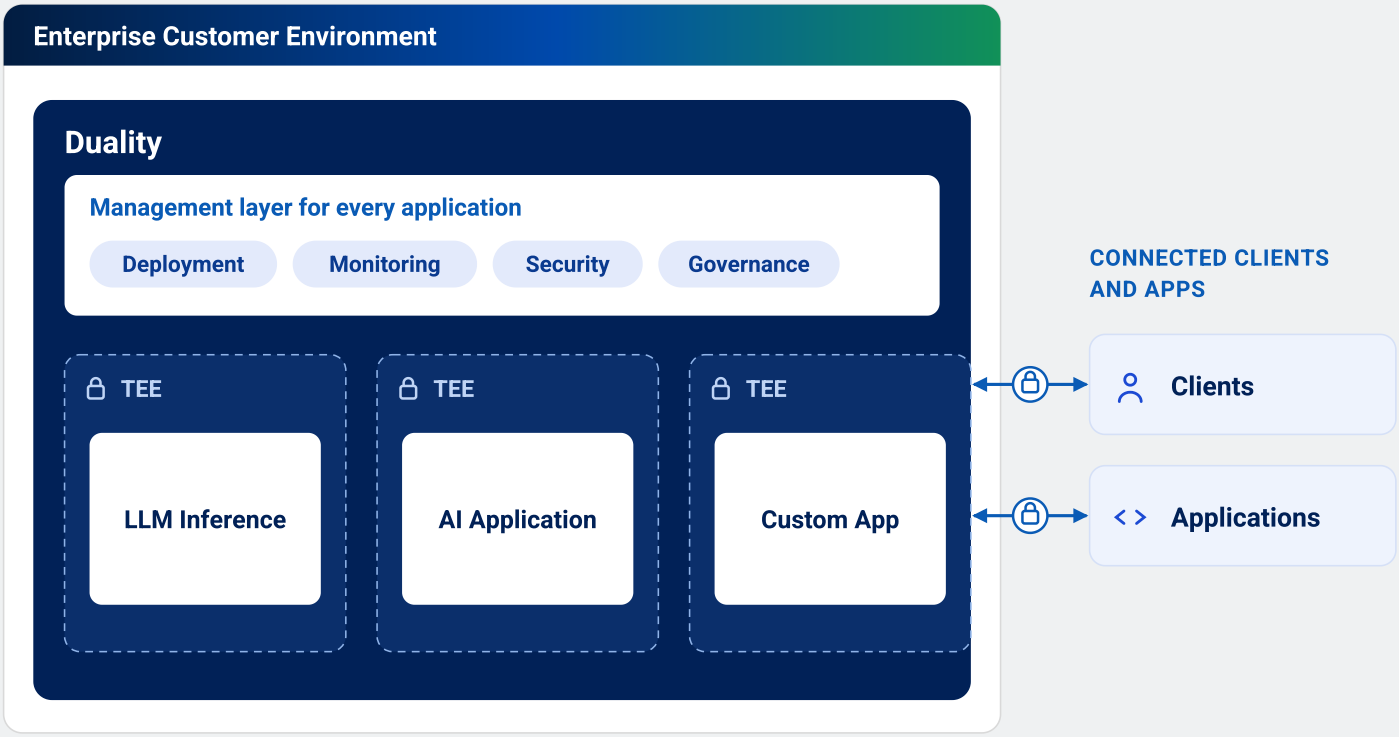
Duality Technologies

WEBSITE

dualitytech.com

SECURE AI APPLICATIONS IN USE

How It Works: Every App in a TEE, One Management Layer



1 Package and Protect

Your application is registered once and packaged encrypted. Its key stays in your own cloud KMS.

2 Govern Every Asset

Owners choose which applications may use each model or dataset. Nothing is released until the enclave is attested.

3 Operate With Controlled Access

Deploy, configure, monitor and upgrade each service through the platform, without operators needing access to prompts, responses or weights.

4 Prove It to Every Client

Clients verify the attestation in the browser and connect with certificates issued by your own certificate authority.

HEADQUARTERS
5 Marine View Plaza, Hoboken, NJ 07030

CONTACT US
info@dualitytech.com

LINKEDIN
Duality Technologies

WEBSITE
dualitytech.com

SECURE AI APPLICATIONS IN USE

Governed End to End, and Where It Fits

Management Capabilities

	Feature / Benefit	With Duality
01	**Deployment**	Register an application once, then start, stop, restart and upgrade it as a service on a confidential-GPU TEE.
02	**Governance**	Policy selects which applications may be used and which models and datasets each can reach. Nothing is released until the enclave is attested.
03	**Security**	Packages are encrypted by default with keys in your KMS. A kernel-level mechanism blocks outbound connections from the application, and mutual TLS authenticates every client.
04	**Monitoring**	See lifecycle and trust state, plus CPU, GPU and memory use for each service. Prompts are never recorded.
05	**Attestation**	The enclave is attested at start and periodically, and users can verify it in the browser with no Duality software on their side.
06	**Your Environment**	Duality is installed in your own environment and runs the TEEs in your cloud account or on-prem, including TEEs with GPUs.

Where It Fits

Banks

AI assistants and agents working over customer records, transactions and internal knowledge.

Telecom

AI services that process subscriber and network data on infrastructure shared with others.

Insurance

Claims, underwriting and policy documents processed by models that stay under your control.

Deployment

Duality is installed in your own environment and works with the applications you already run. Duality is not a model vendor: the models, the data and the applications stay yours.

HEADQUARTERS
5 Marine View Plaza, Hoboken, NJ 07030

CONTACT US
info@dualitytech.com

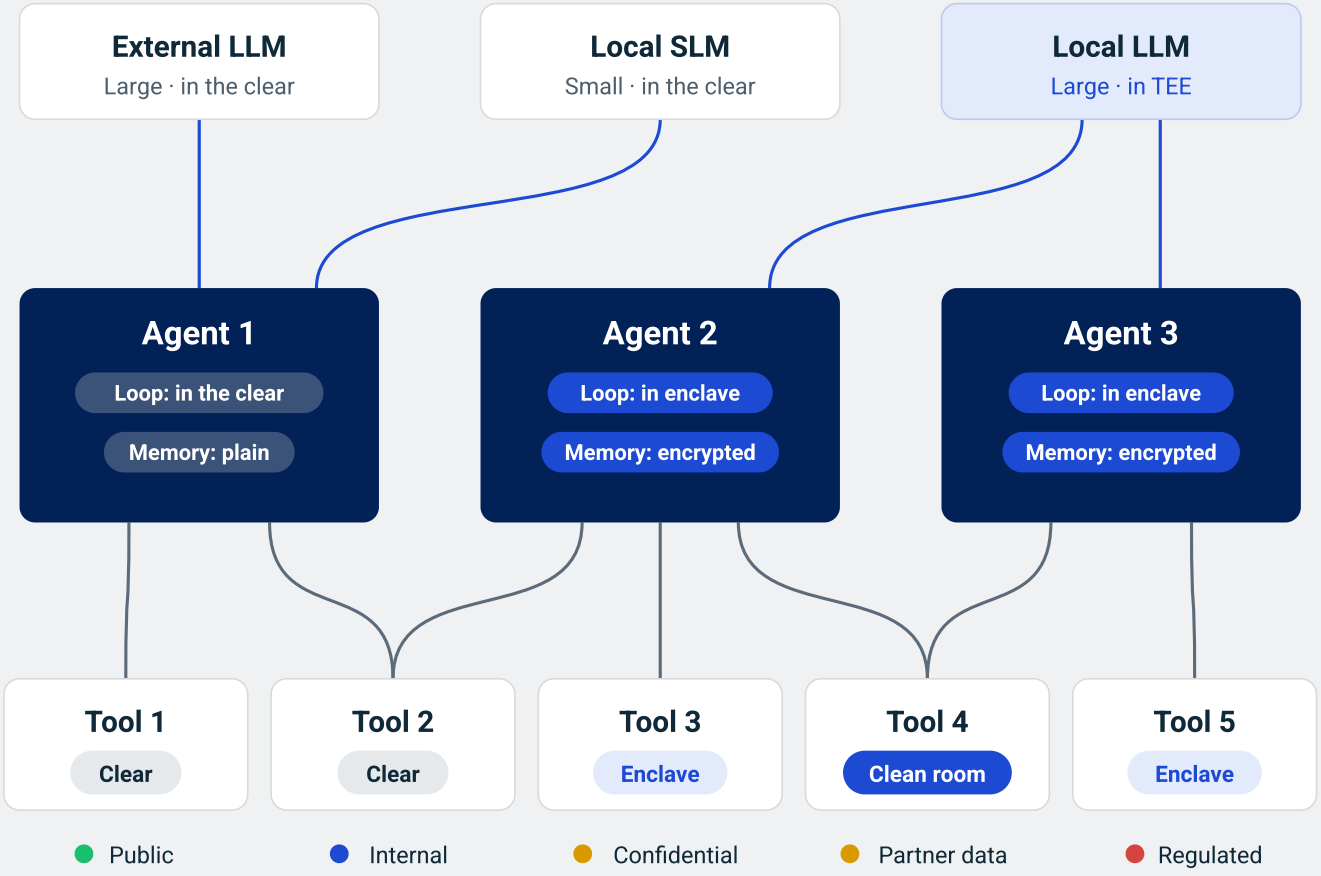
LINKEDIN
Duality Technologies

WEBSITE
dualitytech.com

SECURE AI APPLICATIONS IN USE

How Duality Protects Agents

An agent is a loop that reads data, calls tools and asks models for answers. Match each step to the sensitivity of the data it touches: public steps stay in the clear, and the steps that handle confidential or regulated data run inside a TEE.



Five Control Points

1 Tool Access
Which tools may each agent use?

2 Tool Execution
Run each tool in the clear, in a secure enclave or in a clean room.

3 Agent Loop
Does the agent need an enclave for sensitive prompts or tool output?

4 LLM Access
Which models may it call, given the tools it used?

5 Memory
Encrypt stored memories, or keep them in the clear.

The Result
Each agent gets only the tools, models and memory that its data class allows.

HEADQUARTERS
5 Marine View Plaza, Hoboken, NJ 07030

CONTACT US
info@dualitytech.com

LINKEDIN
Duality Technologies

WEBSITE
dualitytech.com