



Confidential AI infrastructure

Jipa

BY TAQADUM · SERVICE BROCHURE

AI for work
that must stay private.

Jipa by Taqadum · Confidential AI infrastructure
www.taqadum.investments/jipa

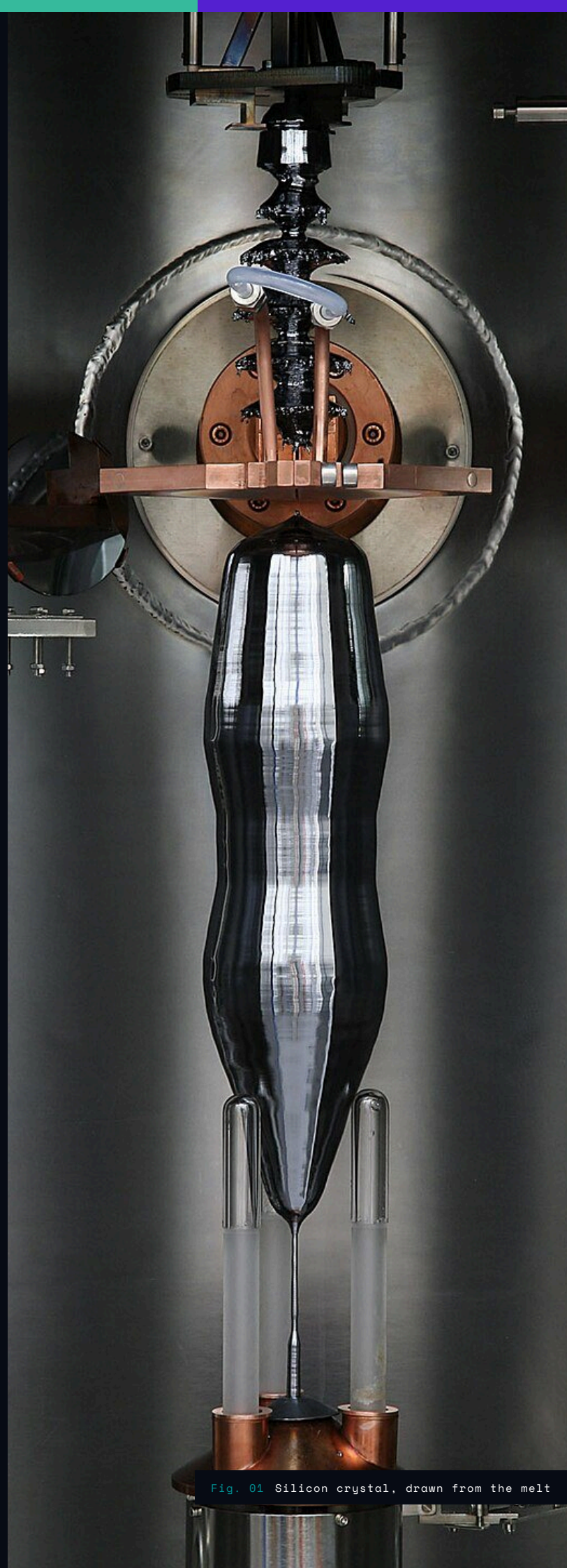
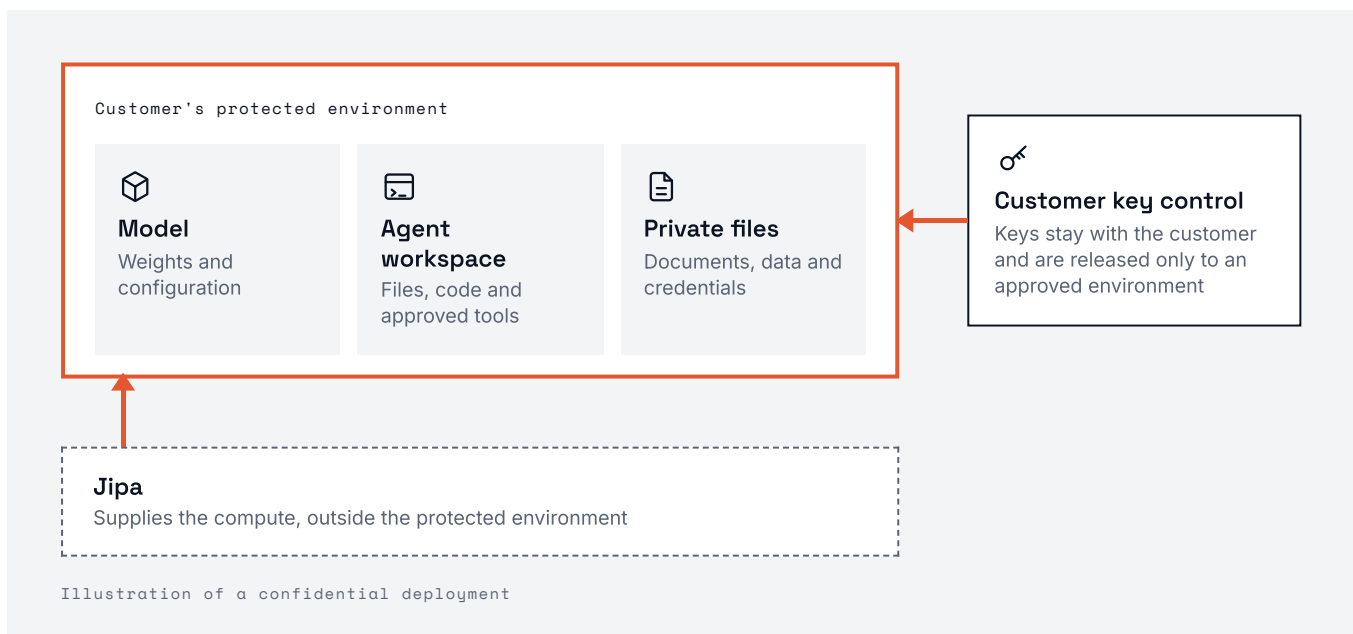
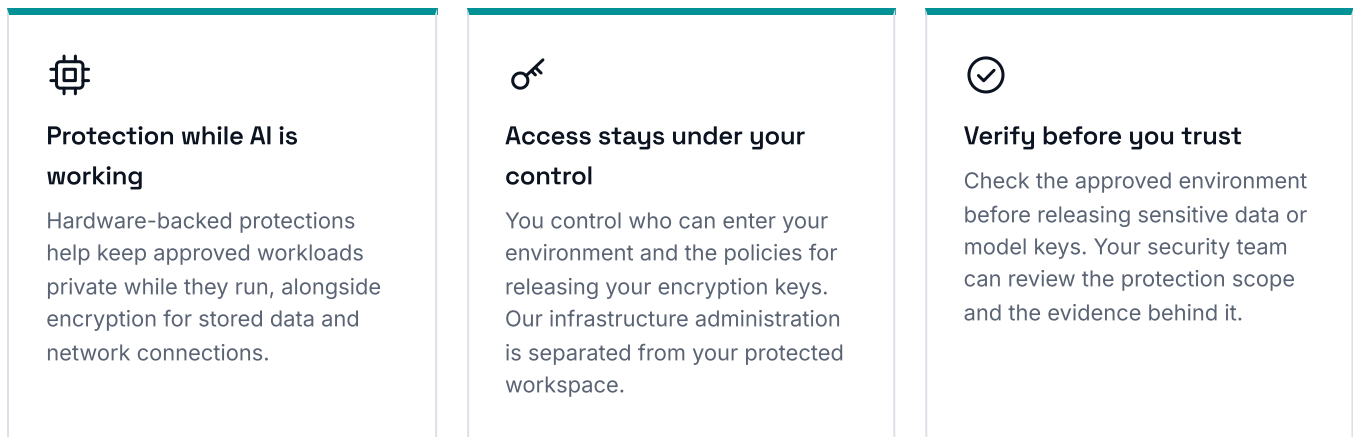


Fig. 01 Silicon crystal, drawn from the melt

01 Confidentiality

Your infrastructure provider should not need access to your work.

Your AI environment can contain far more than prompts. It can hold source code, business documents, model weights, browser sessions and the credentials your agents use. **Jipa's confidential deployment approach is designed to protect that entire working environment.**



DESIGNED AROUND

■ Protection during processing

■ Customer-controlled keys

■ Verifiable deployment

Confidential capabilities and availability will be confirmed in your deployment proposal.

02 How it works

From your requirements to a confidential AI environment.

STEP 01

Define what needs to stay private

Tell us what you want to run, who needs access and which systems your AI should connect to. We agree the deployment, responsibilities and data-handling requirements with your team.

STEP 02

Prepare the environment

We provision suitable compute and prepare the software with you. You approve the model, tools, access settings and security configuration before confidential material is introduced.

STEP 03

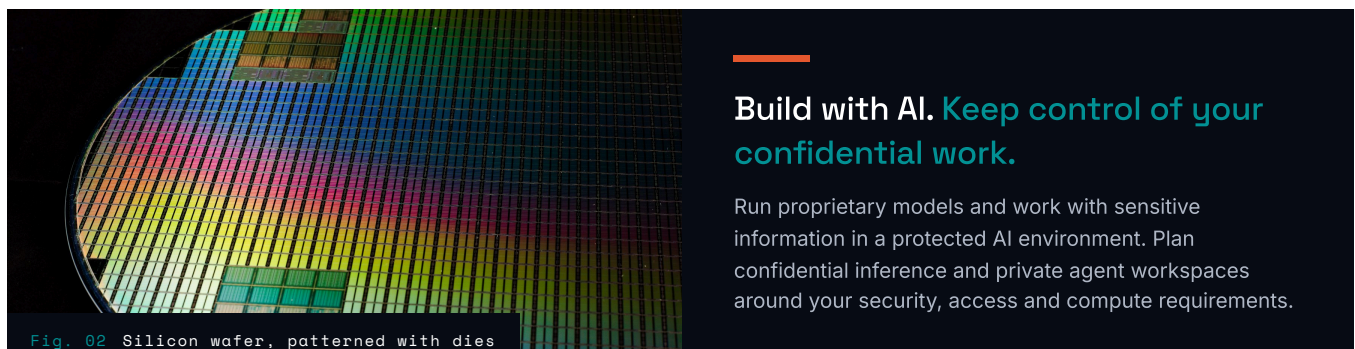
Verify and connect

The environment is checked against your approved policy before keys are released. Connect your application or enter your private workspace to begin using your model and tools.

03 Platform

The compute and tools to build useful AI.

 Confidential model hosting Deploy a supported open-weight or proprietary model in a protected environment. Keep control of the weights, configuration and people who can use it.	 Private agent workspaces Give your team an AI workspace with the files, code and approved tools needed to complete real tasks.	 An API your developers can use Connect applications through an OpenAI-compatible API, with capabilities confirmed for your selected model and deployment.
 Control of your environment Install approved software, choose your agent tools and set access policies for your team. Deployment options are matched to your security and operating needs.	 Compute matched to the workload Choose resources around model size, expected traffic and confidentiality requirements. We help you assess performance before committing to production capacity.	 Clear operating visibility Review agreed usage and service-health information while keeping prompts, documents and other private content inside your protected environment.



04 Private agent workspaces

Give your AI a private place to work.

Move beyond a chat window. Build an agent workspace that can work with documents, write and run code, use a browser and connect to the business tools you approve. Keep its files, sessions and credentials within your controlled environment.

Capability	What your team can do
Files and documents	Review reports, extract information and prepare new documents.
Code and terminal	Build applications, run scripts and work with your repositories.
Browser tools	Research websites and carry out approved browser tasks.
Business connections	Connect authorised data sources and tools through approved connectors and APIs.
Action permissions	Define tool access and require approval for sensitive actions.

You decide which tools are enabled, which services can receive information and which actions need approval. External services receive the data you choose to send to them under their own terms.

05 Use cases

Put confidential information to work.

01 Assistants for internal knowledge

Help your teams find answers across authorised policies, manuals and company documents, with access aligned to their roles.

02 Proprietary model deployment

Bring a fine-tuned or privately developed model into production while protecting the weights and the knowledge they represent.

03 Private software development

Give coding agents controlled access to your repositories, development tools and project files.

04 Document and workflow automation

Extract information, draft outputs and run approved workflows over sensitive business material.

05 Specialist AI workloads

Discuss confidential deployment for supported vision, speech, embedding and language models.

06 Service options

Choose how you want to use Jipa.

Model hosting

Confidential Inference

For teams connecting AI to an application. Run a supported model behind a protected API endpoint, with deployment and access controls agreed with your technical team.

[Discuss model hosting →](#)

Agent workspace

Private Agent Workspace

For teams that want AI to carry out work. Bring together a model, agent software and approved tools in a protected working environment.

[Discuss an agent workspace →](#)

Dedicated

Dedicated Confidential Deployment

For organisations with specialised capacity, software or security requirements. Plan a dedicated deployment around the hardware, ownership and assurance your workload needs.

[Plan a dedicated deployment →](#)

Your proposal sets out compute capacity, deployment support, security responsibilities and operating costs before you commit.

07 Why Jipa

Practical AI infrastructure, backed by Taqadum.

Jipa is Taqadum's AI infrastructure service, developed alongside Taqadum Sigma's GPU and AI infrastructure practice. We help organisations put models and agents to work with confidentiality at the centre of the deployment.

A Confidentiality shapes the deployment

Access, keys and data handling are part of the design from the start.

B Work directly with the technical team

Discuss your model, workloads and security requirements with the people preparing your environment.

C Build around your requirements

Choose the model, tools and deployment approach that fit the way your organisation works.

D Support with clear boundaries

Agree how installation, updates and troubleshooting are handled, including any access your team chooses to authorise.



Fig. 03 Data centre hall

Your infrastructure provider should not need **access to your work.**

Good to know before you commit.

Can we choose where our data is hosted?

We confirm the hosting location and applicable storage, backup and support arrangements in your proposal. Tell us your residency requirements before deployment.

Does confidentiality mean there are no security risks?

No system removes every risk. Your approved software, authorised users, connected services and devices remain part of your security responsibilities. We define the protection scope and remaining responsibilities with your team.

Can we bring any model or application?

We review compatibility, licensing, resource needs and security requirements before deployment. Your technical proposal identifies the supported models, tools and capabilities.

Questions about administrator access, encryption keys, verification and agent tools are covered in your deployment discussion.

Contact

Bring your AI plans. Keep your confidential work private.

Tell us what you want to build and what needs to stay protected. We will help you plan the compute, tools and access arrangements for a confidential deployment.

jipa@taqadum.investments

Confidential capabilities and availability will be confirmed in your deployment proposal.

