THE AFFINIDI CHALLENGE

Build agents you'd confidently offer publicly

Don't build an agent and bolt trust on later. Start from zero with Boris, and switch trust, safety and governance on as you build, not after.



We want to see more than a capable agent. We want to see what becomes possible when that agent can be trusted.

01 · START

From zero

Begin with an idea and let Boris build the agent. Or bring your own.

02 · TRUST

Built in

Identity, tool gating, screening and limits, ready to switch on.

03 · SHOW

What it unlocks

Show what your agent can be trusted to do.

THE CHALLENGE

A great demo is easy. An agent someone can rely on is not.

As agents grow more capable, so does a different problem: how do we make them trustworthy enough for the real world? Ask yourself:

- What could your agent do if trust was there from the start?
- What could you let it handle that you otherwise would not?
- Where would safety or governance let you give it greater responsibility?

THE TRUST DIVIDEND

Show the difference trust makes

Pick one thing you would normally keep behind a human: spending money, sending a message, touching personal data, calling a risky tool. Show what you could hand over because trust was there from the first line. The bigger the responsibility, the stronger the story.

A TYPICAL AGENT	BUILT WITH BORIS
Impressive, but supervised	**Capable, and accountable**
A human approves every step. Risky tools stay off. Nobody leaves it running.	Callers are verified, tools gated, replies screened and spend capped. It can take on more.

Don’t add complexity to show off technology. Use Boris where it creates real value. You don’t need to demonstrate every feature.

USE CASES

Ideas to spark your imagination

Each card has a Research or Commerce idea. Or come up with your own.

SECURE MY AGENT

Only my team can call it

Every caller proves who they are, with a project key or a company sign-in.

COMMERCE IDEA · Supplier comparison for your buying team only.

MCP TOOL GATING

Dangerous tools, admins only

Decide which of your agent's tools each caller may use. Blocked tools stay hidden.

COMMERCE IDEA · Everyone checks stock, only admins change prices.

PROTECT MY LLM

Screen what goes in and out

Screens prompts and replies, and can mask personal data.

RESEARCH IDEA · Interview research with personal details masked.

AGENT THROTTLE · MODEL THROTTLE

Stop runaway spend or traffic

Cap calls to your agent, and requests and tokens to your model.

COMMERCE IDEA · A shopping assistant that survives a crowd.

ALWAYS ANSWER · RIDE OUT A WOBBLE

Stay up when a model fails

Backups and retries keep replies flowing when a model provider has a bad day.

RESEARCH IDEA · A research agent that survives a live demo.

YOUR OWN MODELS AND KEYS

Prompts that stay private

Point Boris at a model running in your own environment, so prompts stay with you.

RESEARCH IDEA · Market research on a model you run.

ALSO IN BORIS

AGENT IDENTITY & ACCESS · RESPONSE CACHING · BRING YOUR OWN KEY · TRY BEFORE YOU SWITCH · LLM DRIFT MONITOR · PRO

QUICK START

Four steps to your first trusted agent

Do steps 1 and 2 before kickoff. For an agent that Boris builds on your machine you need Docker running, and a Mac or Linux computer. On Windows, use WSL.

STEP 1

Get in

Open trustboris.ai and sign in with an email code or one of the options shown. Your first sign-in creates your account.

STEP 2

Install the CLI

The CLI runs agents and tunnels on your machine. On a Mac with Homebrew:

```
brew install --cask affinidi-ai/tap/boris
```

```
boris --version
boris doctor
boris login --url https://trustboris.ai
```

On Linux, use the install line the dashboard shows under Agent Gateway → Target. Safari can't connect the dashboard to the CLI, so use the command line there.

STEP 3

Create a project

Choose "Create an agent, hosted on your machine". In Agent Builder, say what the agent should do, add tools and skills, set what it may touch, then save. Or bring an agent you already run.

STEP 4

Run, then protect

Start the agent, and say yes at the terminal when it asks:

```
boris agent run --project <your-project>
```

Then open Agent Gateway → Features and LLM Gateway → Features, choose Enable feature on what you need, and try it on the Test tab.

BUILDING THE INTERNET OF TRUST

About Affinidi

Affinidi is a Temasek-founded technology company building trust infrastructure for AI agents and the digital economy.

NEW · AFFINIDI'S NEWEST LAUNCH

TrustBoris

Trust, safety and control for agents and models, managed from one place. This challenge puts it in your hands.



TEMASEK-FOUNDED	CERTIFIED	COMPLIANT
2020	ISO 27001	GDPR · PDPA

BUILT ON OPEN STANDARDS, WITH CONTRIBUTIONS TO

DIF · W3C · GLEIF · ayra

DIDCOMM V2.1 · TSP REV3 · DID:WEBVH · SD-JWT · DCQL · EUDI

ALONGSIDE THE AFFINIDI PLATFORM

affinidi **trust fabric** · affinidi **radix** · affinidi **elements**

THE PRIZES

Trust has its rewards

1ST PLACE	2ND PLACE	3RD PLACE
2 months Pro	**1 month Pro**	**3 months Starter**
Package in Boris	Package in Boris	Package in Boris

WIN IT, THEN WATCH YOUR INBOX

WITHIN 2 WEEKS OF THE HACKATHON	IN THE SAME EMAIL
Winners receive their prize by email.	Clear instructions for using your digital gift.

WHAT WE'RE LOOKING FOR

01

A job worth doing

A real task, done from start to finish.

ASK · Would someone use this tomorrow?

02

Trust you can see

Boris's controls are part of how it works.

ASK · What breaks without Boris?

03

More freedom, safely

What you'd normally keep a human on.

ASK · What did you let it do alone?

04

Only what matters

Use the features that help, not all.

ASK · Why is each one there?



Ready to build trusted agents?

Build yours, from zero.

Go to trustboris.ai →