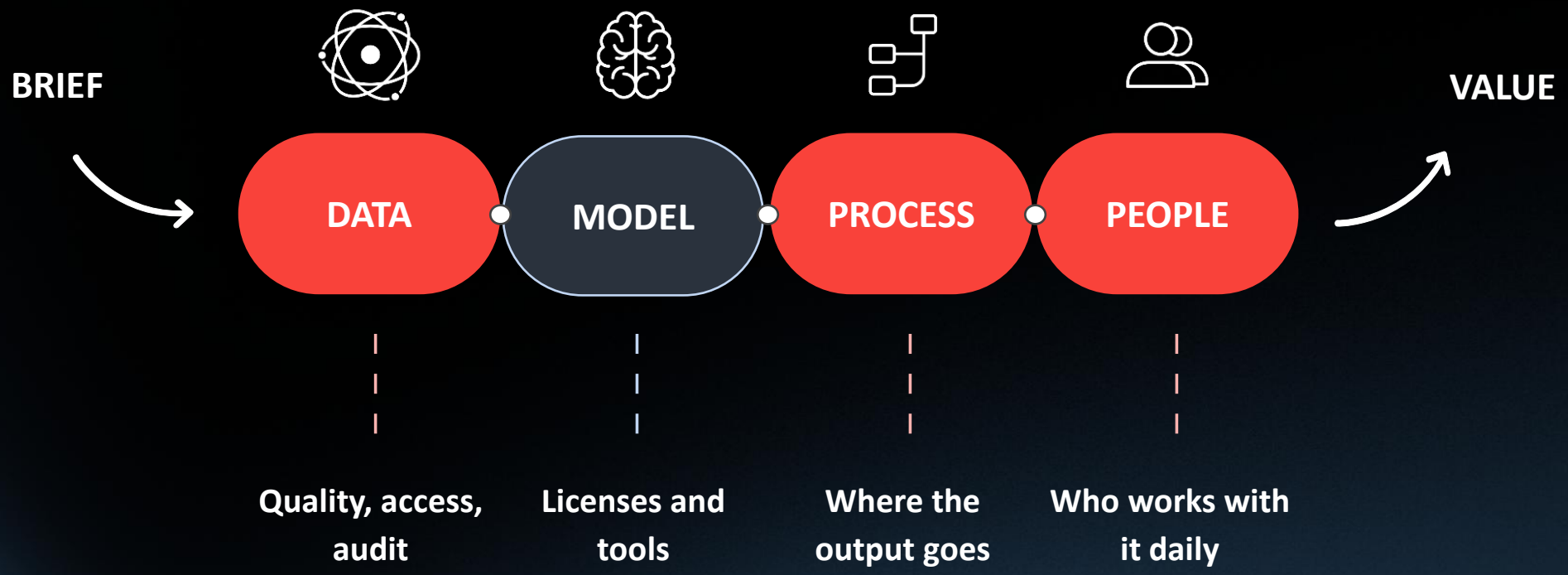
AI Platforms: enabling Agentic AI in production



Jiří Čermák VP of Innovation, Adastra AI

ADASTRA: Non-public

Systematic approach considers full AI value chain



Your enterprise can buy the model...
But Data, Processes and People have to be built from ground up.

Building AI Platforms

So far: preparing data for AI. Now: operating AI safely in production — and what one standard platform has to enforce before any agent is allowed on it.



ADASTRA: Non-public

AI Is No Longer Just a Chat.

It's taking actions inside your systems.

Your teams use ChatGPT, Copilot, Claude, and Gemini every day. Your developers are connecting AI to SAP, SharePoint, and your CRM.

Nobody has a single view of what AI does, what it costs, or what it risks.

91%

of organizations encountered sensitive data leakage risk (Check Point, 2025)

€5–20M

potential fine per incident under NIS2 and AI Act

ADASTRA: Non-public

Agents meet the same five conditions as any production system

01	02	03	04	05
Named identity	Least-privilege access	Tested behavior	Monitored cost and quality	Full audit trail

Without all five, an agent does not go to production, however well it performs.

ADASTRA: Non-public

The platform enforces all five conditions for every agent

PLATFORM gives every agent by default

1

Named identity

Entra ID, agent ID and conditional access

2

Least-privilege access

Agent and user rights both apply; data via governed MCP

3

Tested behavior

Evaluation harness runs every change against the golden dataset

4

Monitored cost and quality

Tracing, cost and quality metrics; budget caps per agent

5

Full audit trail

Every input, output, tool call and decision logged immutably

AGENT TEAM still owns

Behavior specification

The outputs this agent must produce, written down

Golden dataset

Cases, scoring and the release threshold used to test it

Tool and data scope

The tools and data the agent may request

Business sign-off

A named owner confirms the agent is permissible

Agent teams spend their time on business logic; identity, monitoring and audit come with the platform.

ADASTRA: Non-public

Tested behavior: one golden dataset from build to production

GO-LIVE

BEFORE GO-LIVE

- KPIs: accuracy, compliance, latency
- Every prompt tested on one dataset
- Owner sets the release threshold

IN PRODUCTION

- Failures block the release
- New model must match the baseline
- Versioned runs justify each release

Golden dataset
Same cases, same scoring, same threshold in both phases

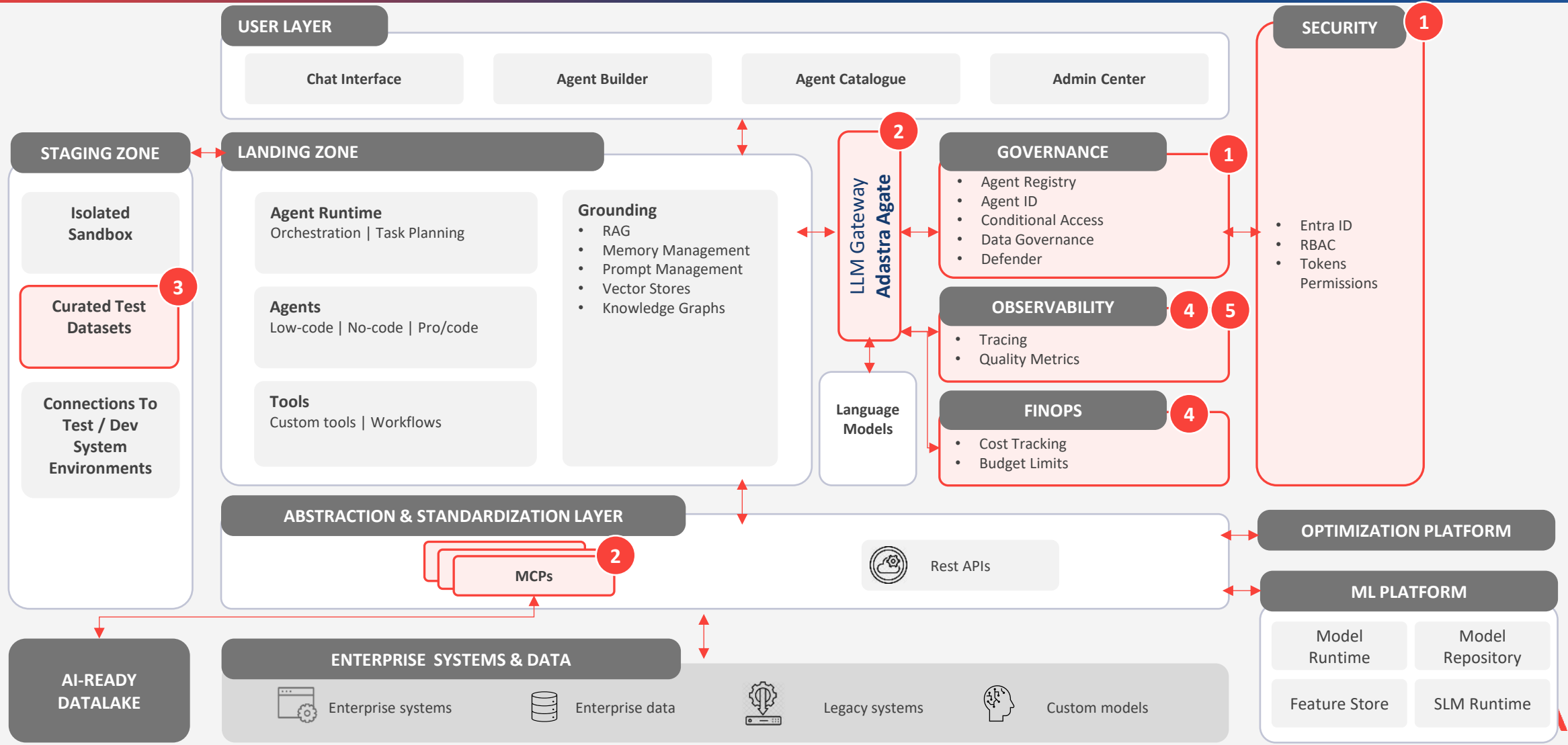
New cases from production incidents

WHAT'S INSIDE Real business cases · Expected outputs · Scoring rules · Release threshold · Business-owned and versioned

ADASTRA: Non-public

AI Platform Framework | Key Components

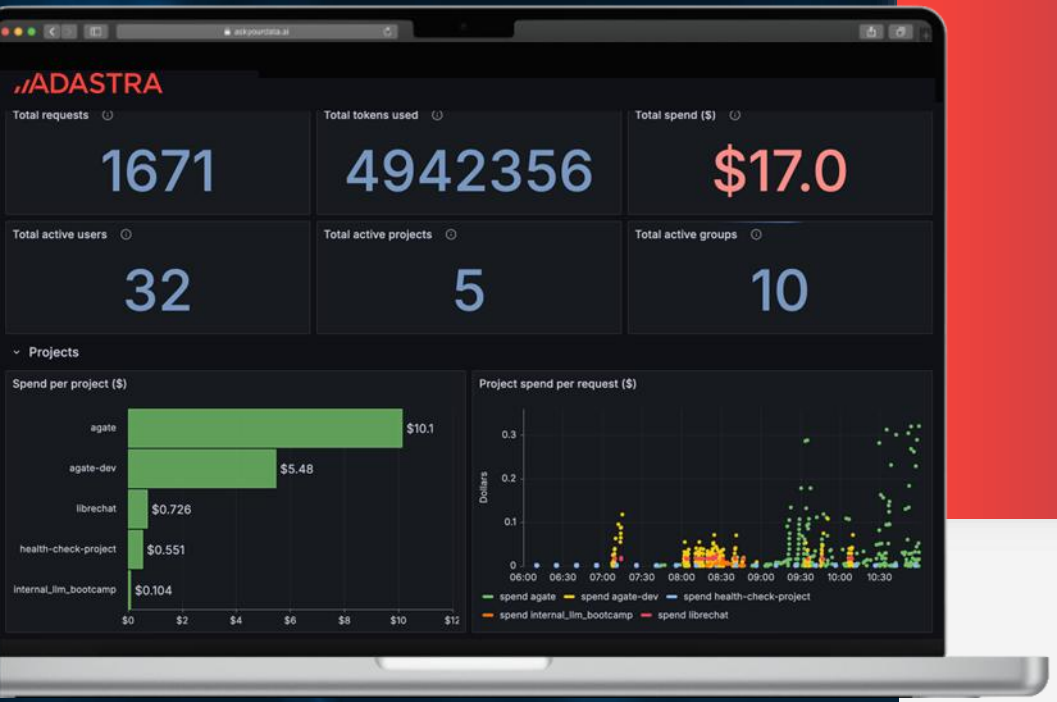
1 Named identity | 2 Least-privilege access | 3 Tested behavior | 4 Monitored cost and quality | 5 Full audit trail



ADASTRA: Non-public

AGate

More about AGate



One gateway for chat, agents and coding assistants — the conditions are enforced once, in the platform, not once per team.

https://solutions.adastracorp.com/solutions/agate-enterprise-ai-governance/



NLB

Transforming Banking Operations Through Centralized AI Hub

Agentic platform on Agate — marketing, AML/KYC and service agents live

< 5 months

from kick-off to the first agent in production

One standard

process and tech stack for agents, across all vendors

Two years in: What worked and what we would do differently

WHAT WORKED

Split ownership of AI-ready data

The bank's data team loads bronze in Databricks; the AI team owns transformation and enrichment from there — no tickets.

Shared document ingestion

Standardized, monitored document pipelines reused across every use case.

A versioned API between GenAI and apps

GenAI components and the application stack ship changes independently.

One team monitors platform and agents

Platform monitoring sits with the team running the cloud stack.

Two years in: What worked and what we would do differently

WHAT WE WOULD DO DIFFERENTLY

Some agents still start off-platform

A few units still prototype outside the platform — and outside the five conditions.

We joined use-case prioritization too late

Sensitive-data cases went first; compliance proof outran the build.

We had no ROI figure next to the risk review

Specs said what an agent should do, not what it was worth.

ADASTRA

Thank you.



Jiří Čermák
VP of Innovation, Adastra AI