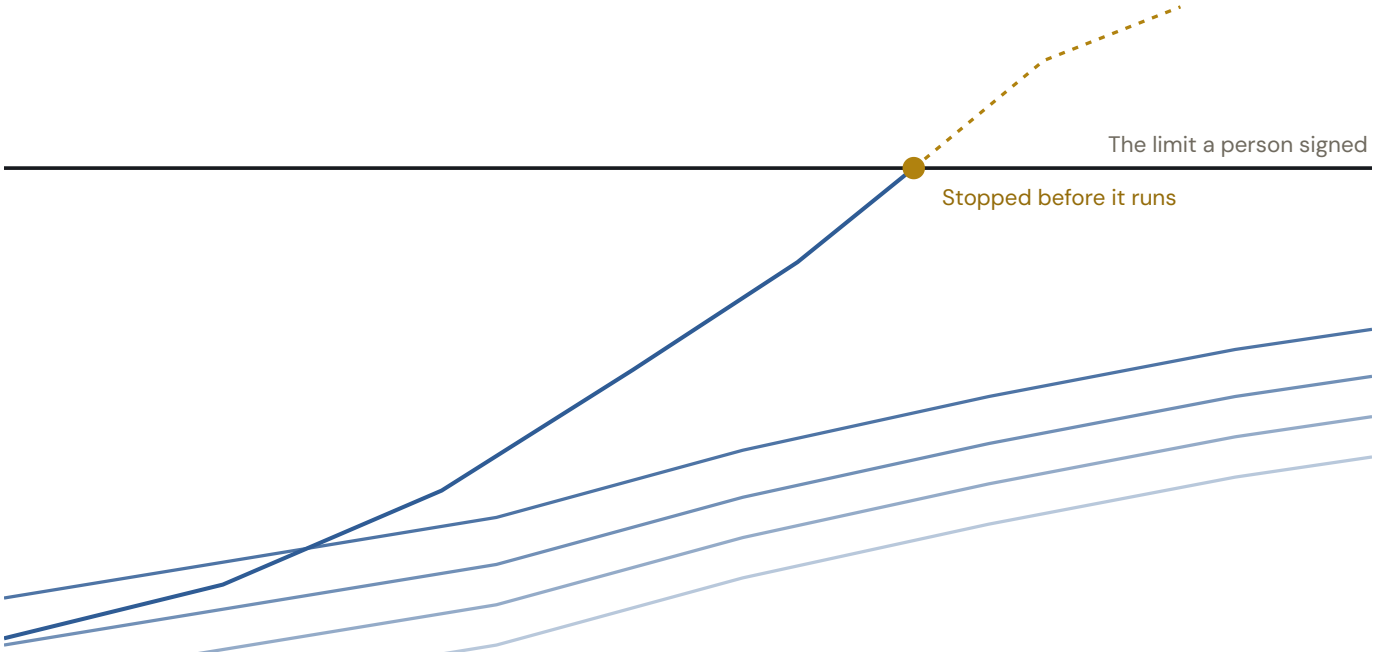
DiaCroma for Agents (D4A)

Verit Global Labs

# Make your AI safer.
# *Govern your agents.*
# And prove it to your auditor.



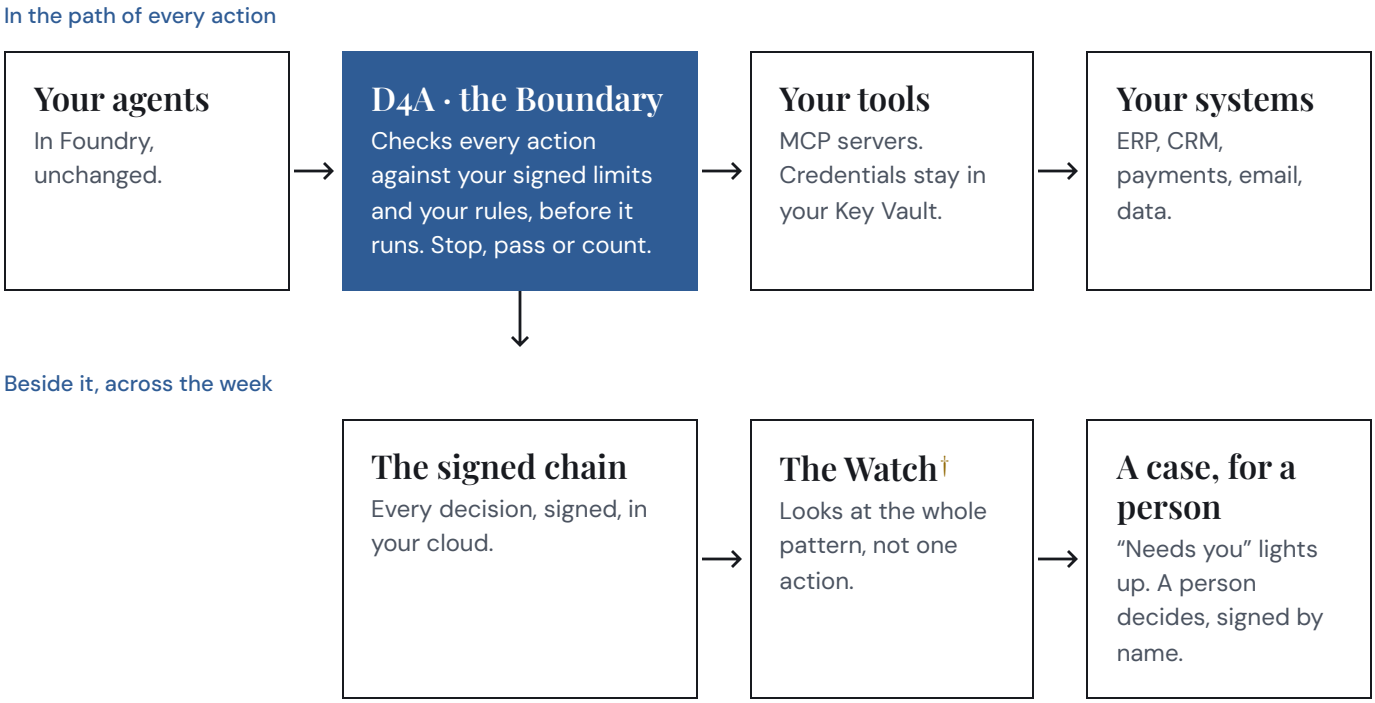

You decide your agents' limits. **D4A checks every action, before it runs.** Your auditor gets the proof.

Try it free for 30 days on Microsoft Marketplace

marketplace.microsoft.com/en-us/product/veritglobal.d4a

# It stops the wrong action. *And spots the wrong pattern.*

You decide your agents' limits. D4A checks every action. Your auditor gets the proof.




1 · The Boundary

## It stops the wrong action, before it runs.

Your agents touch many systems. D4A checks every action once, before it reaches any of them. If it doesn't pass, it never runs. No AI decides, and even if we're down, it keeps enforcing.

2 · The Watch†

## It warns you when an agent starts to drift.

Drift is quiet: every action is allowed, but the agent slowly does its job worse. D4A spots the trend and opens a case before it becomes a problem.

† in development

# Your policies are written down. *Your agents don't read them.*

With nothing to enforce them, every team puts its rules somewhere different, and no one sees whether they are followed or which one wins. **D4A brings them together and enforces them on every action.** Many sets of rules, each applied its own way: D4A applies them as one.

| Your rules | Today | With D4A |
|---|---|---|
| **Company policies**<br>OPA and Cedar† | Only if a system asks. | Before every action, of every agent. |
| **Your agents' instructions** | Only if the agent obeys. | Signed by a person, enforced from outside. |
| **Your tools** | Whatever the credential allows. | Only the tools someone approved. |
| **Business limits** | Nobody keeps the total. | Per deal, in total, per day and per customer. Per team. |

## Other guards you keep

**Foundry guardrails**
Content Safety: keep it at maximum.

**Foundry budgets**
Tokens and cost.

**Entra Agent ID**
Who each agent is.

**Your cage**
Where the agent runs.

If an agent is defined looser than your company's policies, *your policies win.* If you have no policies, the agent's limits win, signed by a person.

Whatever rules you have, every agent is covered. Like insurance.

† in development

# Your business rules can be as complex *as your business.*

Per deal, per day, per customer, per team, all at once. D4A enforces them on every agent, and adds up what no single agent can see.

## Ten discount agents, one team budget.

| | |
|---|---|
| Each agent | $100 per deal · $300 a day |
| The team | $500 a day |
| Any customer | $600 a month |

At 11:40 the team has given $400 today. Three agents ask for $100 at the same second.

## $700

**Each agent alone.** Everything stays green: every agent is inside its own limits. The team gives away $200 too much.

## $500

**With D4A.** One passes, two stop. The team total decides, in one step, so three agents asking at the same second can't all get through.

## Every action was allowed. *The total was not.*

Illustrative figures. Today D4A keeps running totals, in total or per hour, day or month, and per customer, for one agent, for the agents behind the same Boundary, or for a team of agents that share one limit.

† in development

# The Watch tells you where to look. *You decide.*†

Ten agents give discounts, each inside its limits. And yet one of them has given the maximum to the same customer three days running.

**Monday**
Max discount to customer 4471. Allowed.

**Tuesday**
Max again, same customer. Allowed.

**Wednesday**
Max again. Each one inside its limit. Allowed.

**Wednesday, 11:02**
The Watch opens a case with the actions that make the pattern, recorded in the signed chain. “Needs you” lights up.

**Wednesday, 11:20**
A person tightens the limit, signed with their name.

Always on and spending no tokens, the Watch sees drift that builds up, agents that move together and a mission left undone, with your Microsoft judges in your own Azure.† It never stops an action and never changes a limit: only a person does.

# A person decides. *Your auditor checks it.*

## Approve by hand

A stopped action is approved once, signed and tied to that exact action, and the agent retries it.†

## Your people are told

Every case opens in the console, where “needs you” lights up, and goes by email to the address you set in the console. By Teams,† and to whoever signed the limit.†

## Each with their role

The owner runs the organization; a Policy authority signs the limits; a Reviewer reads everything and closes cases, and cannot sign. No agent changes its own limits.

## The proof for your auditor

Every decision goes into a signed chain, in your cloud. Your auditor verifies it with an open tool, without calling you or us.† It proves the record was not altered, not that the agent reasoned well.

† in development

# Your agents' spending, *under control.*

An agent has two bills: what it does with your money, which arrives all at once, and its tokens, what it spends thinking, which grow every month. D4A stops the first and warns you about the second,† from about 1% of what your agents already cost to run.

## What it does with your money

D4A stops it before it reaches your system. In production, a $10,000 refund against a $250 per-call limit never ran.

| | |
|---|---|
| No refund over $250. | Per call |
| No more than $2,000 in total. | Agent's running total |
| $600 per customer per month. | Per period and customer |

## Token control

The token ceiling is set by the platform that serves the model (e.g. Microsoft); D4A doesn't duplicate it. It tells you what each action costs and cuts what burns the most unnoticed.†

| | |
|---|---|
| What each action costs in tokens.† | Cost |
| A warning to whoever signed the agent when its tokens climb.† | Warning |
| Cuts loops: the same call, again and again. | Loops |

### You pay for the agents you govern

One flat monthly fee for a number of governed agents. Governed calls are unlimited and never metered.

### 30 days free

Every plan starts with 30 days free: cancel before they are up and nothing is charged.

### On Microsoft Marketplace

On your Azure invoice, no sales call. For unique needs, from your own installation, by agreement, and with the partner kit.†

"You can't have agents roam around and drift around the company."

Jensen Huang, NVIDIA CEO, on CNBC · 28 Sep 2026

## An agent is not legally liable. You are. *And you pay for it too.*

† in development

# D4A and the agent security *you already have.*

Today, agents are protected in three ways: an **AI gateway** in front of the model, an **MCP gateway** in front of the tools, or an **agent security platform**, which finds your agents, detects threats and blocks risky actions. Each one does its job well, and D4A doesn't replace any of them. It adds one thing: before an action runs, it checks that it fits the limits a person in your business signed, counting everything already done.

| | AI gateway | MCP gateway | Security platform | With D4A |
|---|---|---|---|---|
| **What the agent does with your money** | Decides whether the agent may use the refund tool | Decides whether the tool is allowed for that agent | Blocks by tool, type of action or destination | Decides whether this action, with this data, fits what you signed, and keeps the running total |
| **Who sets the rules** | An administrator configures them | An administrator configures them | The security team, or an AI assistant | D4A proposes them, a person in the business signs them, and whoever reviews cannot change them |
| **The proof for your auditor** | A log you export and explain yourself | A log you export and explain yourself | A log you export and explain yourself | A signed chain your auditor checks without asking anyone† |
| **Your company rules** | You write them again in the gateway | You write them again in the gateway | You write them again in its console | D4A asks your OPA, or Cedar†, before every action |
| **What changes over time** | Sees each request on its own | Watches whether a tool changes | Compares the agent with its habits | Compares it with what it was asked to do† |

## Keep what you have. *D4A adds what it can't see.*

You don't need to change your agents, your gateway or your security platform. If you have any of the three, D4A adds to it; if you have none, it works too.

† in development

# Govern your first agent *this week.*

Plug and play. Limits are not written from scratch: they are read from what you already told your agents, and a person signs them.

## Nothing to change in your agents, your rules or your business

Same agents, same instructions, same models, same tools, and the rules you already have. One address changes: the agent's MCP tool points at D4A. The console shows what will change and writes nothing until you confirm, and it can be undone.

## Start with zero risk

No cost: the first 30 days are free. No stops: in Observing, D4A counts what it would have stopped and blocks nothing. Then you choose how hard it stops:

**Observing** — Enforcing — Strict — Explicit

## From 10 minutes, no code

1
### Store
Get D4A on Microsoft Marketplace, with a free trial.

2
### Login
Sign the agreement once, as the owner.

3
### Settings
Choose how strict D4A is; every change is signed.

4
### Discover
Your Foundry agents, read without changing anything.

5
### Scan
Each agent's instructions read into limits.

6
### Policies
You approve, and it is signed in your name.

7
### Gateway
D4A creates it in your own Azure.

8
### Status
What it stopped and what waits for you, live.

## Talk to us.

D4A is on Microsoft Marketplace today, for agents in Microsoft Foundry with tools over MCP. Coming next: Microsoft Copilot Studio, AWS Bedrock AgentCore and Salesforce Agentforce.

diacroma@veritglobal.com
www.diacroma.com

† in development