

EntPEP

# Agent Fleet Manager

---

**Each session starts its own isolated agent.**

Approve what it can reach: files, company data, the web. Choose where the model runs. Every agent is a sealed VM with no OS and no disk, and every action lands in your data lake.

● NEW SESSION

EntPEP

Agent Fleet Manager

Agents

Data Lake

Admin

Each session starts its own isolated agent. Approve what it can reach.

NEW SESSION

SharePoint

A SharePoint folder, copied into a sealed RAM workspace for the session. The agent can reach nothing else in SharePoint.

Connected

Data Lake MCP

Data with row-level authorization.

Connected

Web Search

Filtered results, injection guardrails.

Connected

Launches an agent with

label · external

model · anthropic api

audit on

sharepoint off

data lake off

web on

skills on

sub-agents 1

archive: session-oct6-1037

Advanced ▾

Launch Agent

RECENT AGENTS >

Pick one to three sources and launch. Audit, skills, sub-agents and an archive are already on, shown as pills beside the button.

EntPEP · Agent Fleet Manager

01 / 18

● NEW SESSION

EntPEP

Agent Fleet Manager

Agents

Data Lake

Admin

Each session starts its own isolated agent. Approve what it can reach.

NEW SESSION

SharePoint

A SharePoint folder, copied into a sealed RAM workspace for the session. The agent can reach nothing else in SharePoint.

Site

Folder

EntPEP Credit Review

Barclays · 99 KB

Access

RAM workspace

Read-only

Read-write

512 MB

1 GB

2 GB

Barclays: 99 KB · 10 GB of 10 GB RAM free

Data Lake MCP

Data with row-level authorization.

All desks (compliance vi

Connected

Web Search

Filtered results, injection guardrails.

Connected

Launches an agent with

label · confidential + external

model · anthropic api

audit on

sharepoint Barclays · read-only · 512 MB

data lake all

web on

skills on

sub-agents 1 + workspace

archive: session-oct6-1037

Advanced

Launch Agent

RECENT AGENTS >

Each source shows its choices only when it is on: a SharePoint folder, read-only or read-write, in a RAM workspace; one desk's data.

● SHAREPOINT + DATA LAKE

 **SharePoint** 

A SharePoint folder, copied into a sealed RAM workspace for the session. The agent can reach nothing else in SharePoint.

Site

EntPEP Credit Review ▼

Folder

Barclays · 99 KB ▼

Access

Read-only

Read-write

RAM workspace

512 MB

1 GB

2 GB

Barclays: 99 KB · 10 GB of 10 GB RAM free

 **Data Lake MCP** 

Data with row-level authorization.

All desks (compliance vi ▼

Connected

The chosen folder is copied into RAM inside the agent, and it is all of SharePoint the agent can reach. It vanishes when the agent stops. Company data is scoped by desk.

● ADVANCED

NEW SESSION

SharePoint

A SharePoint folder, copied into a sealed RAM workspace for the session. The agent can reach nothing else in SharePoint.

Site

EntPEP Credit Review

Folder

Barclays · 99 KB

Access

Read-only

Read-write

RAM workspace

512 MB

1 GB

2 GB

Barclays: 99 KB · 10 GB of 10 GB RAM free

Data Lake MCP

Data with row-level authorization.

All desks (compliance vi

Connected

Web Search

Filtered results, injection guardrails.

Connected

Audit

Prompts, replies and signals are written to the data lake.

Interception

Skills

Load approved skills.md file.

Sub-agents

At most 1 at a time, each with this agent's permissions.

1

3

5

☒ Share parent Workspace

Archive

Saved after every reply and when the agent stops.

New

Resume

barclays-review

Launches an agent with

label · confidential + external

model · anthropic api

audit on

sharepoint Barclays · read-only · 512 MB

data lake all

web on

skills on

sub-agents 1 + workspace

archive: barclays-review

Advanced ▴

Launch Agent

Advanced opens audit, skills, sub-agents and archive. The launch line spells out what the agent may reach before it exists.

EntPEP · Agent Fleet Manager

04 / 18

● MODEL SERVERS

EntPEP

Agent Fleet Manager

Agents

Data Lake

Admin

Choose which model servers agents may use and which options appear on the Agents page. Hidden options are also switched off at launch.

MODEL SERVERS

**Anthropic API**

Claude through Anthropic's API, with this box's key.

**Amazon Bedrock**

Claude in your AWS account (us-east-2, us.anthropic.claude-sonnet-5). No Anthropic key in the VM.

Region

Model ID

API key

us-east-2

us.anthropic.claude-sonnet-5

saved ..... paste to replace

Test & enable

**Private server**

qwen2.5:14b on private.entpep.com. Nothing leaves your network.

Host

Model

API key

private.entpep.com

qwen2.5:14b

saved ..... paste to replace

Test & enable

**Default for new agents**

With more than one enabled, the Agents page lets you choose.

Anthropic API

Amazon Bedrock

Private server

Admin enables one or more model servers: the Anthropic API, Claude on Amazon Bedrock in your own AWS account, or a private server on your premises.

EntPEP · Agent Fleet Manager

05 / 18

● CHOOSE WHERE THE MODEL RUNS

EntPEP

Agent Fleet Manager

Agents

Data Lake

Admin

Each session starts its own isolated agent. Approve what it can reach.

NEW SESSION

SharePoint

A SharePoint folder, copied into a sealed RAM workspace for the session. The agent can reach nothing else in SharePoint.

Connected

Data Lake MCP

Data with row-level authorization.

Equities desk

All tables

trade\_blotter

comms\_surveillance

Grant 1h

Revoke

Grant 1h

Connected

Web Search

Filtered results, injection guardrails.

Connected

Launches an agent with

label · confidential

model · private.entpep.com · qwen3:14b

audit on

sharepoint off

data lake equities

web off

skills on

sub-agents 1

archive: session-oct6-1037

Advanced

Private server · qwen3:14b

Launch Agent

Anthropic API

Amazon Bedrock

Private server · qwen3:14b

RECENT AGENTS >

With more than one enabled, the launch bar offers the choice and Admin sets the default. Every server gets the same sealed VM, hooks and audit trail.

## POLICY

### Keep confidential data internal

 Every agent is labelled at launch: **confidential** if it can reach the Data Lake, **external** if it has Web Search or an outside model (the Anthropic API). Nothing ever moves from a confidential agent to an external one. With this on, one agent can't be both.



### Sub-agents

A sub-agent gets exactly its parent's permissions and model server.

Same as parent

Research (Claude)

On. New agents with the Data Lake can only use an internal model server, without Web Search.

Every agent is labelled at launch: confidential if it can reach the Data Lake, external if it has Web Search or an outside model. Nothing moves from confidential to external.

● KEEP CONFIDENTIAL DATA INTERNAL

BLOCKED

NEW SESSION

SharePoint

A SharePoint folder, copied into a sealed RAM workspace for the session. The agent can reach nothing else in SharePoint.

Connected

Data Lake MCP

Data with row-level authorization.

Equities desk

All tables

trade\_blotter

comms\_surveillance

Grant 1h

Revoke

Grant 1h

Connected

Web Search

Filtered results, injection guardrails.

Connected

Launches an agent with

label · blocked: confidential + external

model · private.entpep.com · qwen3:14b

audit on

sharepoint off

data lake equities

web on

skills on

sub-agents 1

archive: session-oct6-1037

Advanced

Private server · qwen3:14b

Launch Agent

Policy: confidential data stays internal, so an agent with the Data Lake can't use Web Search. Turn off Web Search.

With the policy on, one agent can't be both. Data Lake plus Web Search is refused at launch, and the refusal is audited.

EntPEP · Agent Fleet Manager

08 / 18

● INTERCEPTION HOOKS

Audit

Prompts, replies and signals are written to the data lake.

UserPromptSubmit

PreApiCall

PreToolUse

PostToolUse

PreResponse

Interception

Skills

Load approved skills.md file.

Sub-agents

At most 1 at a time, each with this agent's permissions.

1

3

5

Share parent Workspace

Archive

Saved after every reply and when the agent stops.

New

Resume

barclays-review

Launches an agent with

label · confidential + external

model · anthropic api

audit on

sharepoint Barclays · read-only · 512 MB

data lake all

web on

skills on

sub-agents 1 + workspace

archive: barclays-review

Advanced ▲

Launch Agent

Five hooks in every agent: prompt, model request, tool call, tool result and reply. Each is on or off, all on by default.

EntPEP · Agent Fleet Manager

09 / 18

● SUB-AGENTS

RECENT AGENTS ▾

| PORT    | CONFIGURATION                                                                                                                                                    | ARCHIVE              | STARTED             | STATUS             |
|---------|------------------------------------------------------------------------------------------------------------------------------------------------------------------|----------------------|---------------------|--------------------|
| :8001   | <div><div>audit on</div><div>sharepoint Barclays · rw</div><div>data lake off</div><div>web</div><div>workspace 1 GB</div><div>sub-agents 3</div></div>          | <div>ephemeral</div> | 2026-10-06 09:01:56 | <div>stopped</div> |
| :8002   | <div><div>audit on</div><div>sharepoint Deutsche Bank · ro</div><div>data lake off</div><div>workspace 512 MB</div><div>sub-agents 3</div></div>                 | <div>ephemeral</div> | 2026-10-06 09:52:41 | <div>stopped</div> |
| ↳ :8003 | <div><div>sub-agent of :8002</div><div>sub-2</div><div>Inventory your workspace: call list_workspace and read_note with name plan, then deliver i...</div></div> | —                    | 2026-10-06 09:52:52 | <div>done</div>    |

A sub-agent runs a task in the background with its parent's permissions. Its result lands in the parent's workspace.

## ● RESEARCH SUB-AGENTS

Admin › Policy › Sub-agents: Research (Claude)

### Analyst agent

label · confidential

Internal model server: Bedrock in your account, or your private server  
Data Lake, SharePoint, workspace  
No Web Search

/agent <task>

typed by a person

results flow back up

### Research sub-agent

label · external

Claude  
Web Search only  
No Data Lake, SharePoint or workspace  
Same hooks and audit trail

Before it starts, the typed task is checked against every value the Data Lake returned to this session, and audited in full.

/agent compare peers to our \$100.3M position

BLOCKED · Data Lake value

The analyst stays confidential on an internal model. A person hands public research to a Claude sub-agent, and only the results come back.

## ● INSIDE THE AGENT

```
● EntPEP · Claude Code ephemeral · nothing is saved sealed unikernel · no OS · no disk

session · audit on · onedrive none
○ Ephemeral session · nothing is saved. /save-snapshot <new-name> keeps a copy as a new archive.
☹ Data Lake connected. Type /datalake to see its tables, your access and example questions.
EntPEP Hermit harness ready. This UI is served from a unikernel with no operating system. Type a prompt and press Enter.
> /datalake
Data Lake MCP · desk role: Credit (the database returns only this desk's rows)

datalake.trade_blotter – access granted, 60 min left · 3 rows visible
  Trades by desk: trader, symbol, side, qty, price, notional (USD), counterparty, and status (FILLED / PARTIAL / FAILED /
  PENDING).
  columns: trade_id UInt32, ts DateTime, desk LowCardinality(String), trader String, symbol String, side Enum8('BUY' = 1,
  'SELL' = 2), qty UInt32, price Decimal(18, 4), notional Decimal(20, 2), counterparty String, status
  LowCardinality(String)
  try: What is our total notional exposure by counterparty? | Which trades are not FILLED, and how much notional is
  stuck? | Show this week's largest trades with trader and counterparty.

datalake.comms_surveillance – NO ACCESS: an admin must grant it in the Agent Fleet Manager
  Communications captured for surveillance: channel, desk, sender, recipient, a flagged marker, a 0–100 risk score and a
  one-line summary.
  columns: id UInt32, ts DateTime, channel LowCardinality(String), desk LowCardinality(String), sender String, recipient
  String, flagged UInt8, risk_score UInt8, summary String
  try: List flagged communications with risk above 60, highest first. | Which senders have more than one flagged message?
  | Summarise the policy concern behind each flagged Chat message.

Query with datalake_query: one read-only SELECT; results are capped at 200 rows.
```

/datalake shows the agent what it can see: trade\_blotter granted for 60 minutes, credit-desk rows only. comms\_surveillance: no access.

## ● INSIDE THE AGENT

ALLOWED

BLOCKED

```
> Using the data lake: total notional by counterparty on the trade blotter, and how many rows can you see? Then try to count rows in comms_surveillance. Keep it short.
```

```
⊗ query_mcp → ok
```

```
⊗ query_mcp → error
```

```
⊗ query_mcp → ok
```

```
⊗ query_mcp → ok
```

```
⊗ query_mcp → ok
```

```
**Trade blotter** (Credit desk, 3 rows visible – all rows in my grant):
```

```
| Counterparty | Total Notional (USD) |  
|---|---|  
| Barclays | 962,961 |  
| Deutsche | 961,090 |  
| Goldman | 958,439 |
```

```
**comms_surveillance**: Blocked – no active grant for this table. An admin must approve access in the Agent Fleet Manager before I can count rows.
```

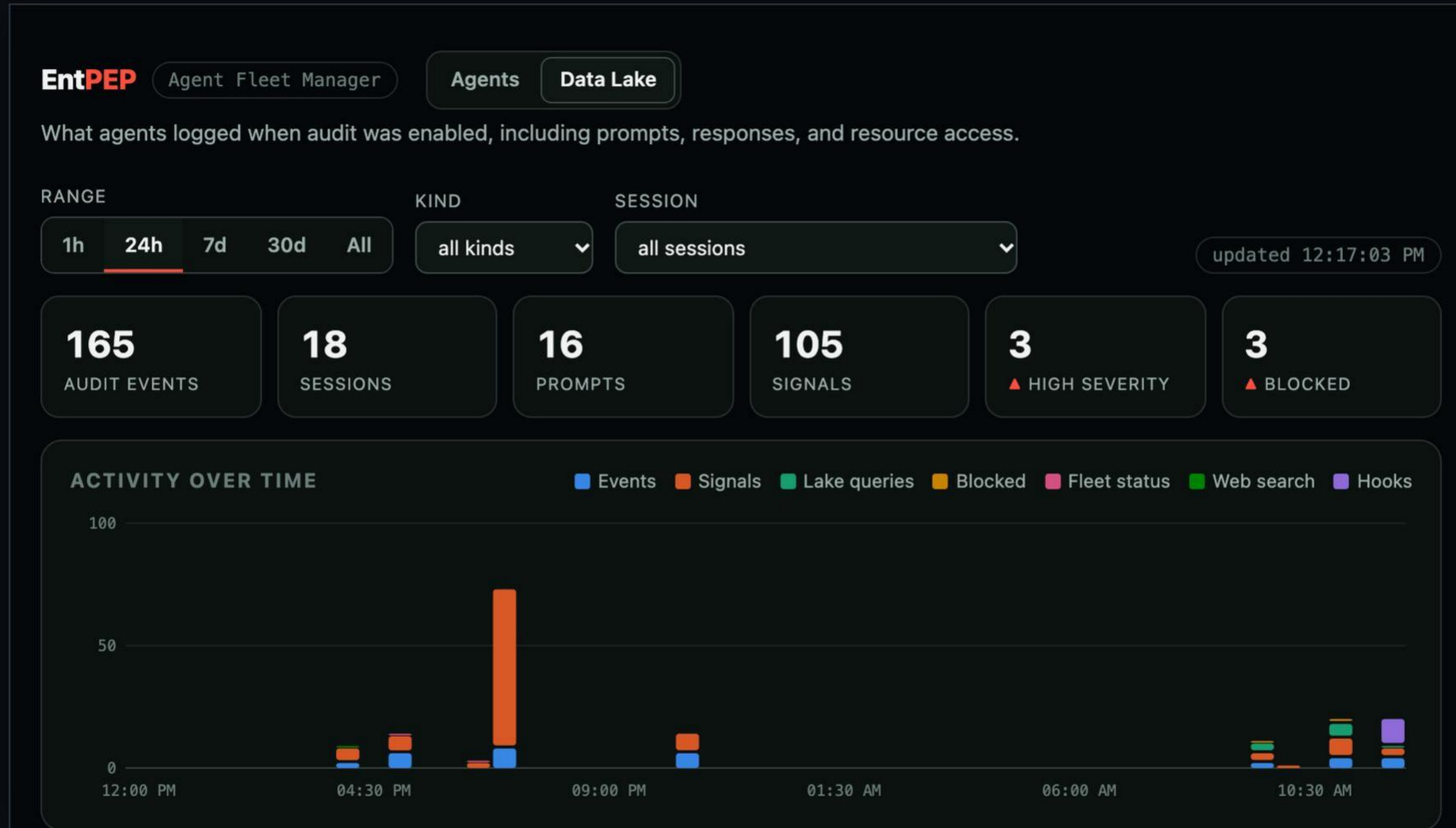
The database enforces the desk, not the prompt: the credit desk sees 3 of 36 trades. The ungranted table is blocked.

● **AUDIT**

| AUDIT STREAM                          |           |         |                  |                                                                          | filter text... |
|---------------------------------------|-----------|---------|------------------|--------------------------------------------------------------------------|----------------|
| TIME                                  | SESSION   | KIND    | RULE             | DETAIL                                                                   |                |
| 09-28 16:05:14                        | hooks-e2e | ■ Hooks | PreApiCall       | allow · 5 messages · 1 tools · system 778 chars · 5545 bytes             |                |
| 09-28 16:05:14                        | hooks-e2e | ■ Hooks | PostToolUse      | allow · ok · 1533 chars                                                  |                |
| 09-28 16:05:14                        | hooks-e2e | ■ Hooks | PreToolUse       | allow · {"method":"tools/call","params":{"arguments":{},"name":"datal... |                |
| 09-28 16:05:14                        | hooks-e2e | ■ Hooks | PreApiCall       | allow · 3 messages · 1 tools · system 778 chars · 3606 bytes             |                |
| 09-28 16:05:14                        | hooks-e2e | ■ Hooks | PostToolUse      | allow · ok · 1158 chars                                                  |                |
| 09-28 16:05:14                        | hooks-e2e | ■ Hooks | PreToolUse       | allow · {"method":"tools/list","server_id":"datalake"}                   |                |
| 09-28 16:05:14                        | hooks-e2e | ■ Hooks | PreApiCall       | allow · 1 messages · 1 tools · system 778 chars · 1581 bytes             |                |
| 09-28 16:05:14                        | hooks-e2e | ■ Hooks | UserPromptSubmit | allow · 55 chars                                                         |                |
| 8 of 8 events · click a row to expand |           |         |                  |                                                                          |                |

Every intercepted action is logged: one question, eight hook rows, from UserPromptSubmit to the final PreApiCall.

## ● DATA LAKE



Every prompt, reply, hook and resource access lands in your own data lake, with high-severity and blocked events called out.

● **AUDIT**

**SIGNALS & BLOCKS BY RULE**

|                              |                        |    |
|------------------------------|------------------------|----|
| session_stopped ○ low        | <div><div></div></div> | 39 |
| session_launched ○ low       | <div><div></div></div> | 39 |
| archive_created ○ low        | <div><div></div></div> | 8  |
| workspace_staged ○ low       | <div><div></div></div> | 6  |
| ungranted_access ▲ high      | <div><div></div></div> | 3  |
| grant_revoked ● medium       | <div><div></div></div> | 3  |
| grant_created ● medium       | <div><div></div></div> | 3  |
| external_write ○ low         | <div><div></div></div> | 3  |
| websearch_connected ● medium | <div><div></div></div> | 1  |
| response_redacted ○ low      | <div><div></div></div> | 1  |
| lake_table_viewed ○ low      | <div><div></div></div> | 1  |
| snapshot_loaded ● medium     | <div><div></div></div> | 1  |

**GRANTS**

| GRANT                                       | SCOPE                  | EXPIRES   |
|---------------------------------------------|------------------------|-----------|
| datalake:trade_blotter<br>granted by erik   | datalake:trade_blotter | 2026-09-2 |
| datalake:trade_blotter<br>granted by erik   | datalake:trade_blotter | 2026-09-2 |
| datalake:trade_blotter<br>granted by dl-e2e | datalake:trade_blotter | 2026-09-2 |

Grants are per table and time-boxed. Revoke one and the next query is refused.

EntPEP

# Patent pending

**Every action, intercepted before it takes effect.**

Intercept each action an AI requests, evaluate it against central policy, enforce the decision before it takes effect, and log it. In Agent Fleet Manager: at five points inside every agent.

Ask about the patent · [entpep.com](https://entpep.com)

EntPEP

# One agent per session.

**Approve what it can reach.**

Sealed unikernel agents · your choice of model server · confidential and external labels ·  
per-desk data access · time-boxed grants · interception hooks · sub-agents ·  
a full audit trail · on your own server.