OVERVIEW DECK

Castellan

Castellan protects your personal context across AI agents.

> Defend your keep. Level up with every agent.

Try the beta | How it works

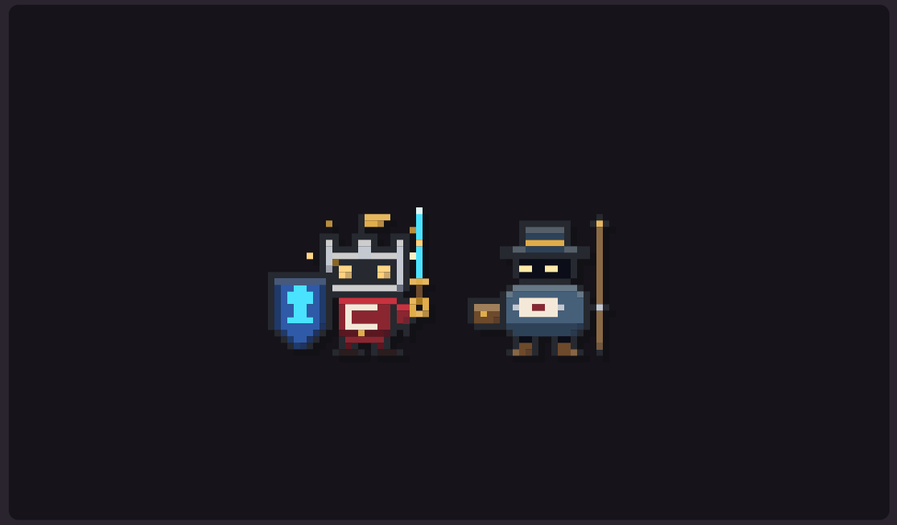


THE PROBLEM

Every agent starts at zero.

Your next agent can start from the knowledge and working methods you have already approved.

- Start in your browser, with an invitation and a passkey.
- Keep approved context in your encrypted account workspace.
- Use your personal Squot or connect a compatible agent with scoped access.
- Review suggested memories and carry a personal playbook across conversations.



HOME

A castle for your context

01



Records

Facts, preferences, goals and rules you choose to keep, with sources and history.

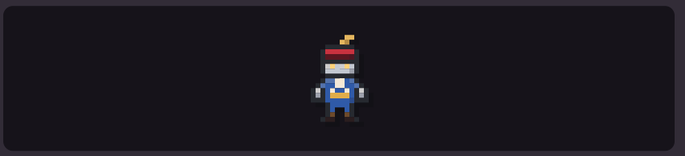
02



Drawbridge

Choose the scopes, selected records and expiry for each agent connection.

03



Squots

Find context, draft in your style and plan from selected approved knowledge.

04



Postern

Connect a compatible MCP app through OAuth or a scoped access key.

05



Watchtower

Check context history and external actions reported by authorized agents.

06



Data controls

Export and import explicitly, inspect sources and versions, or erase the workspace.

HOME

Two layers in one workspace

WHO YOU ARE

Knowledge you approve

- identity, people, goals, habits, preferences and routines
- Facts you write down or confirm, with dates and source evidence

HOW YOU WANT AGENTS TO WORK

Your personal playbook

- standing rules, style, privacy boundaries and working methods
- Approved rules accompany context reads. They guide behavior; grants enforce context access.

01

Build context

Keep useful knowledge and corrections once.

02

Choose access

Select scopes, records and an expiry.

03

Carry it forward

Give the next agent a stronger starting point.

HOW CASTELLAN WORKS

From approved context to useful work

01



Save context

Add records and rules. Imported candidates wait for your review.

02



Choose access

Select scopes, records and expiry. Preview what the agent can read.

03



Connect an agent

Use the MCP URL in a compatible app and approve OAuth or an access key.

04



Use your context

Authenticated requests retrieve records within the connection's access.

05



Review and refine

Approve proposed memories and inspect attributed action reports.

06



End access

End the connection or let it expire. Future requests are refused.

HOW CASTELLAN WORKS

Know what each control covers

ENFORCED ACCESS

Your context and approvals

- Authenticated connections read only the context their grant permits
- Selected-record access excludes future non-rule records
- Suggestions wait for your approval
- Expiry or End access prevents future requests

EXTERNAL WORK

Agent behavior and reports

- Standing rules guide the agent's work
- The provider controls its other tools and received copies
- External actions appear when an authorized agent reports them
- A report does not authorize, independently verify or stop execution

HOW CASTELLAN WORKS

Choose context and permissions

Scope access can include future approved records. Select individual records for a narrower connection.

Scope	What it permits
identity	Facts about you
rules	Standing instructions, included with context reads
preferences	Communication style and other choices
habits	Recurring patterns you approve
goals	What you want to accomplish
people	People and relationships you choose to record
procedures	Routines and ways of working
proposals:write	Suggest records for owner review
actions:report	Report external actions to Watchtower

THE CAST

Your loyal servants stand ready to defend you.



WORKSPACE

Castellan

Keeps approved knowledge and enforces access to personal context.



DRAWBRIDGE

Gate warden

Represents your choice of scopes, selected records and connection expiry.



WATCHTOWER

Owl sentry

Shows verified context history, reporting coverage and agent-reported external actions.



BITCASTLE

Stone golem

Represents access keys and workspace data controls. The developer vault is separate.



GUARDIAN

Circuit mage

Offers an optional advisory check of request wording and scopes in Settings.



POSTERN

Lantern warden

Keeps the MCP connection for compatible apps using OAuth or an access key.



PERSONAL HELPERS

Squots

Use selected approved knowledge for recall, writing and planning, with reviewed corrections.



DEFENSE

Palace guards

Represent approval and read limits. Developer escorts and standing orders belong to the separate runtime.

OUTSIDE THE WALLS

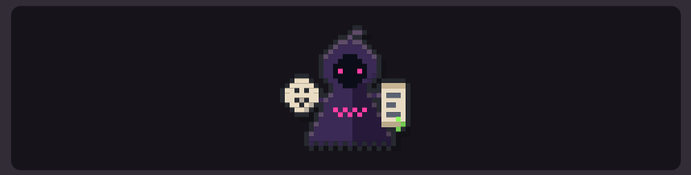
The RAIDERS and the access boundary



MULTIPLE CONNECTIONS

The swarmling

Each connection has its own approved access and expiry. Review active connections and end those you no longer need.



MISLEADING REQUESTS

The mimic

Confirm the connecting app, inspect its access and review proposed memories. The optional request checker advises; it does not approve.



UNAUTHORIZED ACCESS

The breaker

Passkey membership, scoped credentials and encryption at rest protect context access. Browser receipts check previously observed history.

SECURITY

Three principles

Choose what crosses

Approve context scopes and records, set an expiry and end access when the connection's work is done.

Deny by default

Agents need approved access. Suggested memories and Squot lessons wait for your review.

Storage you choose

Use encrypted account storage in your browser, or an optional local Mac or Windows workspace. Local records are not uploaded automatically.

SECURITY

The controls and their limits

Control	What it does
Passkeys	Your device confirms membership; biometric and screen-lock data stays on the device
Scoped access	Approved scopes, optional record selection and mandatory rules govern context reads
Expiry and End access	Stop future requests; online access otherwise continues after browser close
Encryption at rest	Separate workspace keys; the hosted service can decrypt approved context
Verifiable history	Hash-chained context history and browser sequence/hash receipts
Owner review	Imports, agent suggestions and submitted Squot lessons wait for approval
Data choices	Explicit export, import and erasure; provider copies remain outside deletion
Optional request checker	Advises on wording and scopes; does not automatically screen every call
Action reports	Attributed external reports and alerts; no independent execution verification
Squot consent	Hosted writing/planning use selected context after explicit consent; no external tools

SECURITY

Context access and agent execution

Castellan is not an AI gateway. Connected agents talk to their model providers directly.

CONNECTED AGENT	CASTELLAN
Chooses its model and tools	Controls access to your context
Works in external services	Keeps memories you approve
Reports its external actions	Shows the report and its source
Retains copies under its provider's terms	Ends future context access when you choose

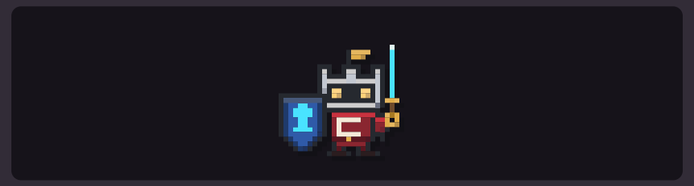
> Castellan's own optional Squot jobs run separately from connected agents. Rules guide agent behavior; reporting does not authorize or stop external work.

YOUR PROGRESS CARRIES FORWARD

Level up with every agent.

Each approved memory, correction and reviewed handoff can give your next agent a stronger start.

01



Build your base

Approve useful knowledge with its source and history.

02



Sharpen your playbook

Refine your personal Squot with selected context and approved lessons.

03



Start further ahead

Carry decisions, completed work and next steps into another conversation.

> The upgrade stays with you. You choose what each agent inherits.

EXPERIENCE THAT COMPOUNDS

Your Squot works from your playbook.

Find useful context

Search selected approved records and rules. Recall uses no model call.

Write in your style

Draft from your preferences and examples. Hosted writing uses explicit per-Squot consent.

Plan next steps

Turn a goal or reviewed handoff into a draft plan. Squots do not send, buy, book or execute external actions.

> Corrections you submit become proposed lessons. Only owner-approved knowledge enters the playbook. This is selected context and examples, not automatic training of a provider's model.

TRY THE BETA

Start in your browser

Activate your invitation, register a passkey and create your workspace at beta.castellan.us. No install or model download is required.

- Save useful context and use a personal Squot, or connect a compatible agent.
- Provider connector availability depends on the app, plan and organization settings.
- Optional Mac and Windows packages keep a local encrypted workspace while their runtime is running and unlocked.
- The repository's local socket broker, credential vault and additional Guardian integrations are a separate developer runtime.

Open workspace | Compare access modes



DEFEND YOUR KEEP

Give your next agent a head start.

Try the beta

How it works

Review Beta privacy and Beta terms at beta.castellan.us. Questions go to contactus@castellan.us.

