

The Base Machine

Two hundred hours of engineering, running on day one, owned by your company.

Most AI engagements begin by signing a company up for a stack of tools, each billed monthly, each holding a piece of its data, none of them its own. Ownbox begins differently. Our forward-deployed engineer arrives with a built machine: one system, on a server your company owns, already running the groundwork every AI build needs. Your budget goes on the problem you brought us in to solve.

WHY WE ARRIVE WITH A MACHINE

A consultant with nothing but advice leaves a company renting. We leave it owning an asset: the platform, the work built on it, and the data inside it.

An asset, not a stack of subscriptions. The groundwork is paid for once, already tested, and already running before the first hour of your project.

WHAT OUR ENGINEER DOES WITH IT

- Stands it up on your company's own server and AI account
- Builds the machines your business needs on top of it
- Keeps all of that work in a folder our updates never touch
- Leaves a build guide, a stable toolkit and a checker, so your team keeps going

We bring the machine. You keep it.

WHAT YOUR COMPANY KEEPS

- The machine, and every machine built on it
- All of its data, exportable to CSV and JSON on any day
- Its AI, on its own Claude or ChatGPT account
- A copy it can move to its own cloud account
- A system that keeps running, with or without a support plan

THE FOUR THAT TAKE A GOOD DEVELOPER 50 HOURS ON THEIR OWN

Admin console

16 h

Personal sign-in, owner and member roles, invitations and settings in four plain groups, designed for a mobile device first.

Your own AI

12 h

Your company's Claude or ChatGPT plan, or an Anthropic API key. Checked before it is saved, metered on every request, under a hard monthly ceiling.

Mobile app

10 h

Installs from the browser on iPhone and Android, wearing your company's name and logo, with a printable install guide for staff.

MCP server

14 h

A secure door for AI agents: standard OAuth or a key, two permission levels, every action recorded. No connected agent can send, publish or spend.

AND THE OTHER 150 HOURS

SECURITY AND OWNERSHIP

28 h

- Single-tenant: shares nothing with any other company
- Automatic HTTPS, for approved addresses only
- Signed releases, checked against a trust file on the box
- Downgrades and unknown signers refused
- Only a root key can change who may sign
- Separate keys for the console, the job queue and updates
- Cross-site protection on every change
- Passwords hashed, sign-in attempts throttled
- Credentials never shown, exported or logged
- Our setup key deleted at first boot
- Server access with your own SSH key
- Every dependency pinned and verified
- Background services locked down

UPDATES THAT CAN'T BREAK YOU

20 h

- Signed updates checked twice a day
- Spread out, never the whole fleet at once
- Undone by itself if not healthy in two minutes
- Database snapshot before every change
- Never follows an unreviewed branch

- Pauses if the box's own files were edited
- One button saves those edits and restores the files
- An Updates page: version and last check
- Every update decision recorded on the box

RELIABILITY

24 h

- Watchdog every 30 minutes: AI, disk, web, worker
- A job queue that never runs a job twice
- Stuck work re-queued, never lost
- Every job's outcome recorded
- Nightly backup, seven days kept
- Continuous off-site backup, ready to switch on
- A restore drill and a self-check tool
- Back by itself after a restart
- A health check that names the exact version
- A broken add-on never takes the box down
- A signed six-hourly check-in: health, plan, head count, no customer data. Can be switched off

AI YOU CONTROL AND CAN AFFORD

16 h

- One gateway for every AI request
- Work that needs no AI never pays for it
- Cost checked against the ceiling before each request

- Every request logged against the job behind it
- Reused context cached to cost less
- A lighter model for simple tasks
- A plan's usage limit pauses work, never fails it
- Automatic retry when a provider is busy
- A knowledge folder rides along on every request
- Paid outside services held to their own caps

YOUR TEAM

12 h

- Invite, revoke and restore people on one page
- Invitees set their own password
- A revoked person is out on their next click
- Members see only what they can use
- One place for every setting, with who changed it
- Light, dark or automatic, per person
- A stop-everything switch for the owner
- The system wears your company's name
- Type and tap targets sized for a mobile device

THE MORNING REVIEW

14 h

- Built every 15 minutes, every day kept
- A section for each machine; a quiet day stays quiet
- Owner-only spend meters
- By email, through your own Resend or SMTP account

- Sent at most once a day, even if retried
- By Slack when connected
- Emails only your own people, never your customers
- Your AI can read it over MCP

BUILT TO GROW

26 h

- A folder of your own that updates never touch
- Each new machine in one folder
- A stable SDK, version 1, promised not to break
- ownbox new writes a working starter machine
- ownbox check flags anything unsafe, with the fix
- A build guide for people and for AI coders
- Machines add their own tools for your AI
- A knowledge folder and settings file of your own
- An update that stops a machine says which one, and whose fix it is
- Export everything to CSV and JSON
- Its own tests ship with it

DELIVERED RUNNING

10 h

- Built automatically when ordered
- Server, address and HTTPS set up
- Running 10 to 15 minutes after checkout
- Handed to its owner with a one-time code
- A set-up checklist that disappears when done

52 + 150 = about 200 hours of a good developer's time, before the first hour of your project. Conservative estimates, part by part.

Ownbox · info@ownbox.io · www.ownbox.io

Hours are Ownbox's estimates of the time a good developer would spend building each part. Features are those in the Base Machine as of September 2026; add-on machines, Coworkers and managed support are separate. Updates arrive while a box is on managed support; the box keeps running either way.