VibeControls

PRODUCT OVERVIEW · 2026

AGENTIC ENGINEERING CONTROL PLANE

One console for every machine

Every session, tunnel and AI assistant your team runs — laptop to production.

For engineering, platform and security leaders evaluating VibeControls

vibecontrols.com

01

The short version

A single, secure command centre where a team can see and control every machine, session, tool and AI assistant it uses.

1

Console

Replaces the daily juggle of terminals, SSH managers, tunnels and AI tabs.

Day 1

Onboarding

A new joiner opens a project and inherits its context, credentials and history whole.

10s

To an answer

“Who restarted that at 3 a.m.?” becomes a search, not an investigation.

BYOK

AI, on your keys

No resold inference, no training on your prompts, no vendor in between.

02

Who it is for

Engineering and platform leaders

Paying for a stack of disconnected tools and still unable to answer who has access to what.

Development teams of 5 to 50

Inconsistent setups and tribal knowledge slow every sprint. Project context becomes shared.

DevOps and platform engineers

A live fleet map, governed tunnels and scheduled tasks instead of ad-hoc port forwards.

Teams adopting AI coding agents

AI doing real work on real systems without handing it the keys.

Freelancers and consultants

One dashboard for every client machine — on a free plan with every feature unlocked.

Enterprise and regulated orgs

SSO, role-based access, tenant isolation and audit ship with the product, not after an incident.

03 What breaks today

Nobody has one view of anything

Terminals, tunnels, servers and sessions scattered across a dozen machines and a dozen tools.

One control plane, drawn as a live fleet map of reachability, health and activity.

Close the laptop and the work is gone

A dropped connection takes the context with it, and long-running work has to be babysat.

Sessions persist across reconnects, stream to a browser tab, and can be replayed.

Production access has no guardrails

Access sprawls, sensitive actions skip approval, and nobody can reconstruct the incident.

Role-based access at the API edge, human approval, and a searchable trail of every action.

AI assistants are stuck in a chat window

Either little real leverage from AI, or it runs unsupervised on a laptop with full blast radius.

Bring-your-own-key AI, an MCP server, plans a human approves, and isolated sandboxes.

04

Nine building blocks, one workspace

FLEET

Agents and targets

Every laptop, VM and server registered as a managed node, drawn as a live topology.

WORK

Terminal sessions

tmux, WezTerm, Zellij or SSH — surviving reconnects, streaming to the browser, shareable.

CONTEXT

Projects

Path, git remote, environment, notes and docs — owned by the workspace, not one laptop.

REACH

Tunnels and forwarding

Named public tunnels and port forwards: permission-checked, expiring, metered.

SAFETY

Sandboxes

Time-boxed isolated environments for AI-generated code and untrusted build steps.

AI

AI orchestration

One governed surface in front of many providers, on your own keys and your own bill.

EXTEND

Plugins

A three-tier contract: adding capability means shipping a plugin, not patching the agent.

RUN

Automation

One-click action decks, reusable actions, cron-style schedules and signed webhooks.

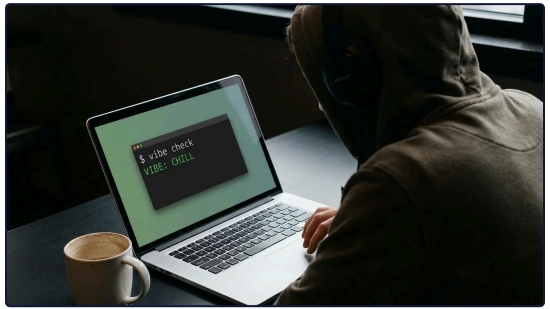
PROVE

Catalog and audit

Typed components, readiness scorecards, and every mutation recorded before and after.

05

Put to work



INDIVIDUAL DEVELOPER

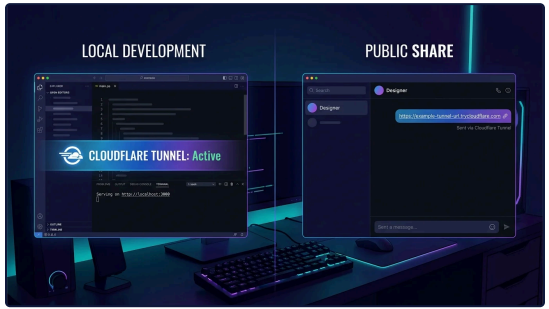
Turn any machine into a managed node with one command

Install the agent, paste the key, and the machine appears live with health and plugin inventory.

ON-CALL ENGINEER

Turn your runbook into buttons your on-call can press

Each button bound to a reusable action and a machine, recording output, exit code and duration.



FRONTEND DEVELOPER

Give anyone a working URL for something on your machine

A workspace-owned tunnel with an owner and an expiry — no deploy, no VPN, no stale back door.

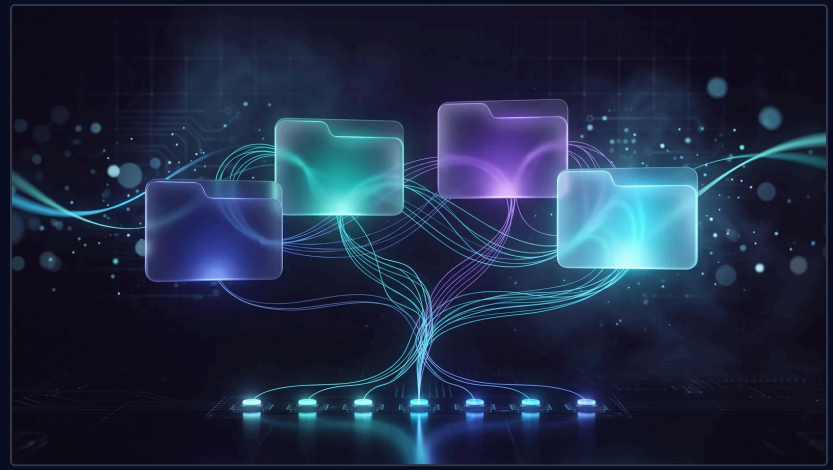
06

Built AI-native

Bring your own coding agents. Keep control of every machine they touch.

Claude Code, Codex, Gemini, OpenCode, Cursor, OpenRouter, Minimax and Ollama run as first-class sessions on machines you own — calling models with keys that never leave those machines.

Model, mode, tool reach and working folder are chosen per turn, in one tabbed workbench.



Acts as you, never beyond you

Every AI action runs under the caller's own login and permissions; the audit entry names the human.

Your models, your machines

Provider keys live in the machine's own configuration; a generic slot takes any compatible endpoint.

613 governed tools over MCP

Outside agents drive the platform through schema-validated calls, enforced as the signed-in user.

07

Autonomy is a dial, not a switch

LAYER 1 · SESSION

Three autonomy levels

Plan is read-only. Accept-edits is the default. Full auto needs an explicit confirmation and is never inherited.

LAYER 2 · MACHINE

Machines start locked

Remote shell, scripts and file writes are denied until you opt that machine in — granted separately, failures resolving to denial.

LAYER 3 · APPROVAL

Plan-mode review gate

The agent produces a plan a human annotates and approves before any tool call fires. A denial leaves zero side effects.

Stated plainly: nothing in VibeControls acts unattended today. Every capability carries a shipped, in-progress or roadmap status, and the planned decision layer is opt-in, off by default and budget-bounded.

08 Who does what

Platform engineering lead	Owns the estate end to end — the agent fleet, its credentials and the governance posture on top of it.
Application developer	The primary user: opens terminals, shares them, builds the automation around their own work — and never holds another machine's credentials.
Security & compliance lead	Sets the baseline and decides what blocks a release, with read-only visibility into the fleet and the sole power to grant a waiver.
On-call engineer	Executes what already exists — runbooks, terminals, tunnels, agent restarts — without reshaping projects or policy.
Compliance auditor	Reviews and exports evidence, and changes nothing — deliberately unable to delete audit records.

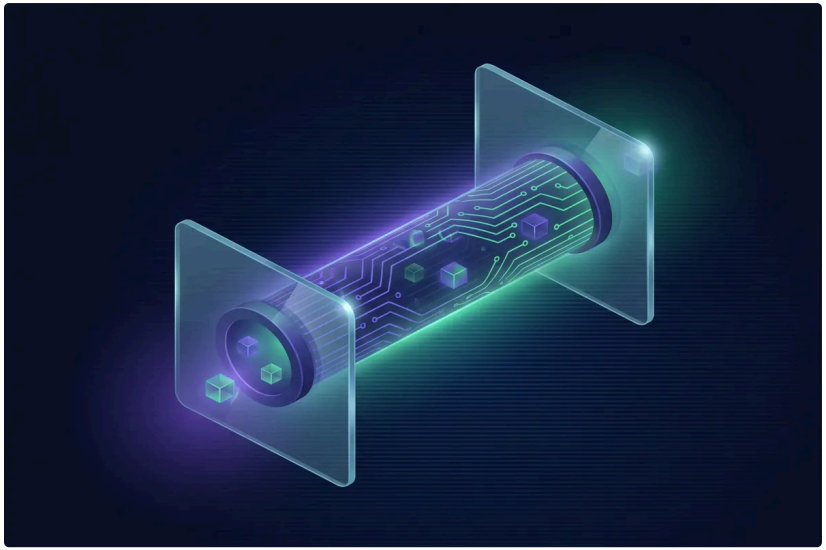
Six roles ship seeded into every workspace, each granting admin, editor or viewer per resource type. A resource a role does not list grants nothing.

09 Under the hood

A multi-tenant cloud service owns durable, workspace-scoped state — machines, projects, sessions, tunnels, policy, audit. A lightweight agent on each machine owns execution.

The console reads state over authenticated GraphQL and talks straight to the agent over TLS for live work. Nearly all machine-side capability arrives as plugins, so swapping a backend never changes how anyone works.

Authorisation is enforced once, at the API edge — the same API behind the CLI, the SDKs, the MCP server and the extensions.



THE SPLIT THAT MATTERS

Terminal output, source contents and AI prompts stream from your machine to your browser and are never persisted by the cloud service, which holds metadata only.

10

Security & trust

Authorisation at the API edge

Every operation declares the action, resource and scope it needs; a denied call never reaches a service.

Identity and single sign-on

OIDC everywhere, SAML and SCIM on Enterprise, per-machine rotatable agent credentials.

Encryption in transit and at rest

TLS 1.2+ with HSTS, AES-256 at rest, machine-held secrets encrypted under per-workspace keys.

Control-plane data minimisation

Metadata only. No terminal output, source contents or prompts — and tunnel payloads are never inspected.

Audit logging and export

Every mutation with actor, resource and before-and-after state, tamper-evident and exportable as evidence.

Findings stay on your machine

Scan runs, findings and exceptions live in the agent's encrypted local store; the control plane proxies only.

> No certification is claimed today. Controls are designed against SOC 2 and ISO/IEC 27001:2022 with audits on a published roadmap, and a DPA covering GDPR, UK GDPR and India's DPDP Act is available.

11

One product, many front doors

Web console
The full product in a browser.

Desktop app
Signed builds for macOS, Linux and Windows.

The agent
The local runtime on every machine you develop on.

Command line
Device-code login, JSON output, scriptable.

Node & Python SDKs
Typed, async-first, with token refresh and retry.

MCP server
613 governed tools for any compatible AI client.

Editor & browser
VS Code sidebar and a Chrome side panel.

Mobile apps
Approve actions on the move — in active development.

12

Plans: quota-based, not feature-gated

FREE

$0 / month

1 machine, 3 projects, 5 sessions. No card, no time limit.

HOBBY

$9 / user

5 machines, 10 projects, 25 AI sessions a day.

PRO

$29 / user

20 machines, 100 projects, 25 tunnels, priority support.

TEAM

$29 / user annual

Pooled quotas from 5 seats, org-wide access control, 99.9% uptime.

ENTERPRISE

From $60 / user

SAML, SCIM, residency, dedicated tenant or self-host.

Every plan unlocks every feature and every first-party plugin — only capacity scales.

Warned at 80% of a quota, blocked at 100%. No silent overage billing, ever.

Four regional pricing bands in native local currency, plus add-on quota packs from $5.

13

Why teams choose it

It starts on your machines

Laptop, remote VM, cloud host or container — genuinely hybrid, under one workspace identity.

A live map of the fleet

Reachability, health and active sessions as a topology reflecting what is really running.

Tunnels as governed resources

An owner, an access policy, an expiry and metering — not a link nobody can revoke.

AI that proposes, humans who approve

Reviewable plans, isolated sandboxes, and the AI acting under the caller's own identity.

Everything is a plugin

Terminal backends, tunnel providers and model providers swap without changing anyone's workflow.

Pricing you can read

No usage credits, no per-hour meter — roughly half the list cost of per-hour cloud environments.

14

Honest answers to hard questions

“We already have a great terminal. Why add another tool?”	A terminal is one surface; this is the control plane around it — fleet, tunnels, AI governance, catalog, access control and audit, with execution staying on your machines.
“A cloud dev environment is cheaper than $29 a seat.”	For light use, yes. Full-time it flips: ten developers on four-core cloud environments run about $6,912 a year versus roughly $3,480 on Team — without the month-to-month variance.
“Your catalog is shallower than the dedicated portals.”	Correct, and said openly. Those products stop at the portal — no agent runtime, sessions, tunnels or sandboxes. Teams needing maximum catalog depth today can run both.
“How do we stop an AI agent doing something destructive?”	Three stacked layers: machines default-deny, sessions carry an autonomy level, and plan mode holds high-blast-radius work for approval. All bounded by permissions and recorded.

START TODAY

Install the agent. Run your first session in minutes.

The Free plan is the whole product, sized to one person: no credit card, no time limit, no expiry.

START FREE
app.vibecontrols.com

PRODUCT AND PRICING
vibecontrols.com

DOCUMENTATION
docs.vibecontrols.com

SECURITY POSTURE
vibecontrols.com/security

VibeControls

© 2026 Burdenoff Consultancy Services Pvt. Ltd. All figures are list prices.