mcpnest.io

ENTERPRISE GOVERNANCE FOR MCP

Secure, *govern*, and deploy MCP servers at scale.

The control plane for engineering teams adopting Model Context Protocol with Claude, Cursor, and Windsurf — access control, audit, and hosted infrastructure for AI tool usage.

7,554+	2	EU
MCP SERVERS INDEXED	GATEWAY SECURITY LAYERS	HOSTED & DATA-RESIDENT

Prepared for enterprise buyers, partners, and strategic conversations

Company Presentation · Updated 20 May 2026

mcpnest.io
malasartes@mcpnest.io

CONTENTS

What's *inside*

01 Executive Summary

02 The Enterprise Problem

03 Who Buys This

04 The MCPNest Platform

05 MCP Gateway

06 Security Layers 1 & 2

07 Governance & Audit

08 Enterprise Workspaces

09 Hosted MCP Infrastructure

10 Why MCPNest Is Different

11 Complementarity with Data & AI Governance

12 Technical Integration

13 Services Companies Can Buy

14 Features & Developer Tools

15 Marketing to Date

16 Pricing, Pilot & Next Step

> This document explains the platform, then goes deep on **security architecture** and **governance**, and closes with a dedicated section on **complementarity and technical integration with data & AI governance platforms**.

IN ONE PARAGRAPH

The governance layer for *MCP adoption* inside organizations

AI clients are moving from assistants to agents. Through the Model Context Protocol they connect to codebases, databases, internal systems, and deployment workflows. That creates a new control problem: companies need to know which tools are approved, who can use them, what each agent accessed, and how access is revoked without breaking the team. mcpnest.io is the control plane that answers those questions.

POSITIONING

Enterprise MCP governance, deployment, and audit infrastructure for teams adopting Claude, Cursor, Windsurf, VS Code, and agentic development workflows.

CORE PRODUCT

A governed MCP Gateway with workspace routing, per-member tokens, tool allowlists, hosted MCP servers, and protocol-level audit logs.

COMMERCIAL OFFER

A 30-day MCP Governance Pilot: a private workspace, governed Gateway, hosted servers, access controls, and a final security and governance report.

WHY IT MATTERS NOW

MCP adoption is moving faster than internal security processes. mcpnest.io gives platform and security teams a control plane before unmanaged AI tool access becomes operational risk.

> Understand the company as **infrastructure, not a directory**. The registry aids discovery; the enterprise value is governance — access control, deployment standardization, auditability, and operational control over AI tool usage. **The registry is the entry point. The business value is control.**

THE GOVERNANCE GAP

MCP works for individuals. It becomes *risky* for teams.

The buyer pain is not discovery. It is safe operationalization — adopting MCP without creating shadow AI tooling, uncontrolled credentials, and untraceable agent activity.

ZERO GOVERNANCE

Developers install MCP servers ad hoc. Security has no approved list, no process, and no visibility into which tools are connected to AI clients.

SHARED ACCESS

Teams share workspace tokens and config files. Every member effectively receives the same access, regardless of role or responsibility.

LOCAL CHAOS

Many MCP servers run as local stdio processes on laptops. They cannot be centrally monitored, shared, revoked, or audited.

NO FORENSICS

When an agent queries a database or triggers a workflow, teams need to know who initiated it, when, and whether it was allowed.

> This is the same shift data governance went through a decade ago — from "what data do we have?" to "who is using it, how, and was it allowed?" **MCP now needs the same discipline, applied to executable tools — and it becomes mandatory before broad enterprise rollout.**

THE BUYER

Built for *platform, security, and AI enablement* teams

MCP governance is bought by the people accountable for safe AI tool adoption — the teams that own infrastructure, access, and risk. Each sees a different part of the same value.

PLATFORM ENGINEERING

Standardizes MCP deployment and workspace operations across the organization, instead of every developer wiring up servers by hand.

SECURITY ENGINEERING

Gets per-member attribution, tool allowlists, instant revocation, and a complete audit log of AI tool activity.

AI ENABLEMENT

Enables teams to adopt Claude, Cursor, and Windsurf safely — accelerating rollout without creating shadow tooling.

AI CONSULTANCIES

Deploy governed MCP stacks per client engagement, with a repeatable workspace, controls, and audit model.

> The common thread: each of these teams is now **accountable for AI tool usage they cannot yet see or control**. mcpnest.io is the control plane that gives them both.

ONE CONTROL PLANE

A full *control plane* for secure MCP adoption

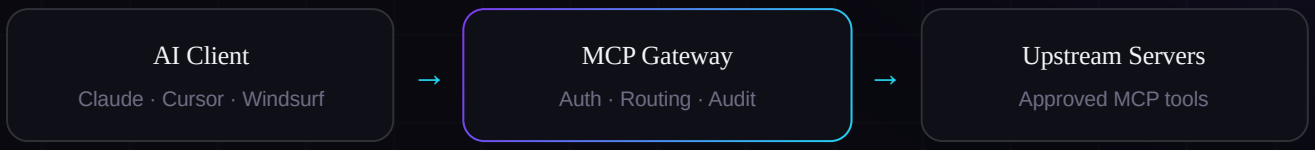
AREA	WHAT MCPNEST.IO PROVIDES
Registry & Marketplace	Discover MCP servers, compare trust signals, review compatibility, and install approved tools. 7,554+ servers with an A–F Quality Score.
MCP Gateway	One governed endpoint per workspace for tool discovery, routing, authentication, and audit logging.
Enterprise Workspaces	Team structure, roles, members, shared configurations, workspace-level governance, and private registries.
Orchestrator	The deployment engine behind hosted servers: container lifecycle, tool namespacing, and webhook-driven auto-deploy on dedicated EU infrastructure.
Hosted MCP Infrastructure	Deploy MCP servers as isolated containers with runtime credentials and operational monitoring.
Security Layer	Per-member tokens, allowlists, instant revocation, audit attribution, and governance-first access control.
Developer Tools	Generator, Composer, Validator, Bundle Sharing, AI Discovery, Risk Scanner, and install helpers.

> Each layer solves a distinct problem, and together they form a complete plane: from **discovery** (registry) to **access** (Gateway) to **deployment** (hosted infrastructure) to **evidence** (audit and governance).

THE CORE PRODUCT

One governed *endpoint* per workspace

The Gateway turns scattered MCP configs into governed infrastructure. AI clients connect to the workspace Gateway instead of connecting directly to many ungoverned servers.



ONE WORKSPACE ENDPOINT

A single endpoint aggregates tools across approved servers and simplifies client configuration across Claude, Cursor, Windsurf and other MCP-compatible clients.

AUTHENTICATED ACCESS

Bearer-token authentication protects the Gateway while keeping client-side setup simple for engineering teams.

TOOL ROUTING

The Gateway aggregates tool discovery (tools/list) and proxies invocations (tools/call) to the correct upstream MCP server.

PROTOCOL AUDIT

Every call is logged with operational metadata: workspace, member, tool name, latency, and execution status.

```
# Before — every developer, every machine
client config × 12 servers × 12 credentials × N developers

# After — one governed endpoint
https://gateway.mcpnest.io/w/your-workspace + 1 per-member token
```

AUTHENTICATION & AUDIT

Layer 1 — the secured endpoint and the *visitor log*

Layer 1 gives each workspace one authenticated endpoint and a complete record of activity. It is the foundation: the lock on the door and the log of everyone who passed through.

TOKEN ARCHITECTURE

- SHA-256 Bearer tokens, `mng_`-prefixed for identification
- Tokens are hashed at rest — the plaintext is never stored
- Verification compares the hash, not the secret
- Tokens are scoped to a single workspace

WHAT GETS RECORDED

- Every tool discovery and every tool call
- Operational metadata for each event
- Outcome — success or failure — per call
- Stored as immutable operational records, not modified through normal product flows

AUDIT EVENT SCHEMA

FIELD	CAPTURED
`workspace_id`	Which workspace the call belonged to
`member_id`	Which individual member initiated the call (Layer 2)
`tool_name`	The specific tool invoked on the upstream server
`latency_ms`	Execution latency, for performance and anomaly review
`status`	Allowed / blocked / error outcome of the call

Daily aggregated views support reporting without scanning the full event stream.

PER-MEMBER IDENTITY & ACCESS CONTROL

Layer 2 — the *keycard system*

Layer 2 moves governance from workspace-level access to member-level accountability, enabling least-privilege access for AI tools. Every person has their own badge, opening only the doors they are allowed through — revocable in a single action.

PER-MEMBER TOKENS

Each workspace member receives individual credentials, enabling attribution of every call and independent revocation.

TOOL ALLOWLISTS

Admins define exactly which tools each member is allowed to call — least privilege, enforced at the Gateway.

INSTANT REVOCATION

When a member leaves or changes role, access is revoked without rotating the entire workspace configuration.

ENFORCEMENT TOGGLE

Run in audit-only mode during onboarding, then switch to strict allowlist enforcement when the team is ready.

Layer 2 is what makes MCP credible for teams: **identity, permissions, revocation, and auditability** — the same primitives an identity provider brings to applications, applied to AI tool calls.

THE ENTERPRISE VALUE LAYER

Evidence, accountability, and *control*

mcpnest.io is designed around the questions security and platform teams eventually ask: who used which tool, when, from which workspace, and what was the result?

AUDIT LOGS

Protocol-level events record every tool call with member attribution and execution metadata.

ACCESS REVIEWS

Admins inspect who has access to which tools and adjust permissions as teams evolve.

INCIDENT READINESS

When something unexpected happens, teams reconstruct the MCP activity trail instead of guessing.

COMPLIANCE POSTURE

Exportable records and retention policies support internal reviews, regulated environments, and procurement.

BUILT FOR REGULATED ENVIRONMENTS

EU data residency · Append-only audit trail · Per-member attribution · Exportable records · Self-host option · Least-privilege access

Designed to support internal control frameworks and regulated environments where auditability, attribution, retention, and data residency matter.

> The long-term value is not only the Gateway. It is the **trusted audit layer for AI tool usage** — a record that did not exist before, for activity that is becoming operationally critical.

THE TEAM OPERATING MODEL

Where teams *standardize* MCP adoption

A workspace is the unit of governance — where platform, security, and engineering teams collaborate around MCP. It turns experimentation into an operational standard.

PRIVATE WORKSPACE

Each company or team gets a governed environment for approved servers, members, tokens, and tool access.

ROLE-BASED OPERATION

Owners and admins manage workspace access, server approvals, member permissions, and security controls.

PRIVATE REGISTRY

Companies curate an internal list of approved MCP servers and reduce uncontrolled installation.

TEAM ONBOARDING

Workspaces standardize MCP usage across developers instead of copying local configs by hand.

DEPLOY YOUR WAY

Run on managed EU cloud, or bring the entire governance plane in-house with a self-host deployment — for teams where data residency is non-negotiable.

Cloud

Self-host

THE ORCHESTRATOR

Deploy a server *in one click*

Many MCP servers only speak stdio — they run locally and never reach production safely. The Orchestrator is the deployment engine that closes that gap: it runs approved servers as governed services on dedicated EU infrastructure, turning experimentation into enterprise operation.

ORCHESTRATOR — THE DEPLOYMENT ENGINE

- Full container lifecycle: deploy, start, stop, restart
- Tool namespacing prevents collisions across servers
- Webhook-driven auto-deploy on git push
- Runs on dedicated, EU-resident infrastructure

HOSTED SERVERS

Deploy approved servers as isolated containers instead of relying on local developer machines.

RUNTIME CREDENTIALS

Credentials are injected at deployment time rather than stored in local config files.

STDIO-TO-HTTP BRIDGE

Legacy stdio servers are wrapped for Gateway-compatible, governable operation.

Operational surface: real-time deploy console with live container status, a configure-and-deploy flow, and per-instance log viewing.

> The stdio-to-HTTP gap is the single biggest blocker to running MCP in the enterprise. The Orchestrator and Bridge are what turn a directory of servers into **production infrastructure a team can depend on**.

THE ALTERNATIVE IS THE STATUS QUO

Why *mcpnest.io* and not the alternatives

The honest question every buyer asks: why not build this internally, or use something we already have? Each alternative solves a piece — none solves governance, deployment, and audit together.

ALTERNATIVE	LIMITATION	MCPNEST.IO
Manual MCP configs	Local, fragmented, no audit or attribution	Governed workspace + Gateway
MCP directories	Discovery only — no control after install	Governance, deployment, and audit
Generic API gateways	Not MCP-native; no tool-level model	Protocol-aware MCP routing
Internal build	Months of effort, expensive to maintain	Ready-to-use control plane
Local stdio servers	Cannot be shared, monitored, or governed	Hosted, containerized services

> The unaddressed combination is the moat: **governed access, native MCP routing, hosted deployment, and a protocol audit trail** — in one control plane, ready today, instead of a six-to-twelve-month internal build.

TWO SIDES OF AI GOVERNANCE

Data governance and *tool governance* are parallel layers

Data & AI governance platforms answer **which data exists, what it means, who owns it, and who may use it**. mcpnest.io answers **which tools an AI agent invoked, by whom, and what was allowed**. The same buyer needs both — and neither covers the other today.

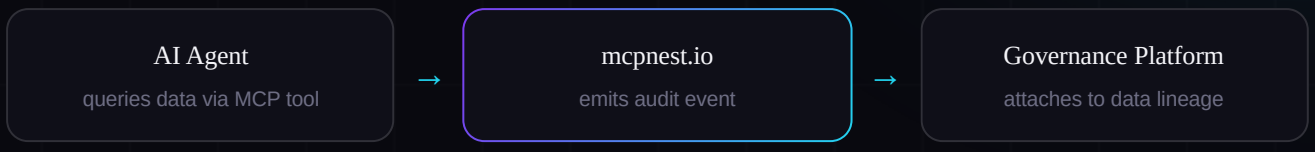
DIMENSION	DATA & AI GOVERNANCE PLATFORM	MCPNEST.IO
Governs	Data assets & AI products	MCP servers & tool calls
Core artifact	Catalog, glossary, lineage	Gateway, allowlists, audit log
Key question	What data, who owns it, who may use it?	Which tool ran, who ran it, was it allowed?
Access model	RBAC over data & metadata	Per-member tokens over tools
Audit object	Data usage & lineage	Protocol-level tool invocations
Blind spot it has	How an agent reached the data	What the touched data means / its sensitivity

The shared gap: when a developer uses Claude and an MCP server to query a governed table, the data platform sees the table but not the agent's tool call; mcpnest.io sees the tool call but not the data's classification. Data governance explains the asset. mcpnest.io explains the agent action. Connected, the two produce complete lineage — from business data asset to AI agent invocation.

CONCRETE INTEGRATION

MCP audit events → *data lineage*

mcpnest.io produces a structured, append-only event for every AI tool call. Those events can flow into a data & AI governance platform to extend its lineage graph downstream — to the agent activity that traditional ETL-based lineage never sees.



A tool call that touches a data asset becomes a node in the lineage graph, with member attribution.

WHAT MCPNEST.IO CONTRIBUTES

- Per-call event: workspace, member, tool, latency, status
- Identity attribution for every AI tool invocation
- The "last mile" of agent-to-system access activity
- Exportable, append-only records

WHAT THE PLATFORM CONTRIBUTES

- Business meaning and classification of the touched asset
- Ownership, policies, and sensitivity tags (e.g. PII)
- End-to-end lineage across systems
- Compliance reporting and value tracking

THREE WAYS TO PARTNER

MODEL	DESCRIPTION
Co-sell	Parallel layers, same enterprise buyer (platform, security, CDO). Mutual referral into existing deals.
Technical integration	mcpnest.io audit events feed the partner's lineage and governance graph for AI tool activity.
Joint go-to-market	Co-marketing around "governance for AI agents" — data + tools as one enterprise control story.

COMMERCIAL PACKAGING

What companies can *buy*

OFFER	WHAT IT INCLUDES
30-Day Governance Pilot	Fixed-scope setup of a private workspace, Gateway, hosted servers, member access, audit logs, and a final governance report.
Team Workspace	Recurring subscription for teams needing Gateway access, hosted servers, allowlists, and operational governance.
Enterprise Governance	Advanced controls: centralized visibility, private deployment, audit exports, and procurement support.
Hosted MCP Operations	Managed deployment and operation of selected MCP servers as governed services.
Private Registry	Curated internal catalog of approved MCP servers for company-wide AI tooling standards.
Self-Hosted Deployment	Private deployment of the Gateway and workspace model inside the organization's own infrastructure.
Publisher Verification	A path for MCP server creators to become enterprise-ready through verification, hosted deployment, and trust signals.

THE WIDER PRODUCT SURFACE

Tools that *accelerate* adoption

MCP COMPOSER

Visual builder for combining multiple MCP servers into a coherent client configuration.

MCP GENERATOR

Generate server code and clean install configs from natural-language requirements.

CONFIG VALIDATOR

Detect malformed MCP configs before they break AI clients.

BUNDLE SHARING

Share curated MCP stacks for teams, use cases, or internal standards.

RISK SCANNER

Free, client-side security scan of an MCP configuration — zero data leaves the browser — returning an A–F risk report. The top of the governance funnel.

AI DISCOVERY

Describe a use case and receive server recommendations from the registry.

These tools create the developer-experience and top-of-funnel layer. The enterprise monetization remains **governance, Gateway, hosted infrastructure, and auditability**.

ORGANIC EXECUTION

Technical credibility, *focused narrative*

1,900	~42	45
VISITORS SINCE 5 APR	AVG VISITORS / DAY	ELAPSED DAYS

ORGANIC CHANNELS

Technical articles, LinkedIn, community launches, direct founder-led outreach, and partner-led awareness. No paid acquisition in the current validation phase.

PRODUCT-LED ENTRY POINT

The Risk Scanner acts as the free assessment that turns abstract MCP risk into a concrete, graded report.

> Marketing now shifts from awareness to conversion: scanner usage, pilot calls, workspace demos, and paid pilots. **Partner-led distribution** — co-selling with adjacent governance platforms — is the next lever.

SIMPLE PACKAGING ALIGNED WITH VALUE

Start with a *governed pilot*

PLAN	PRICE	INCLUDED
Free	€0 / month	Marketplace, Risk Scanner, Validator, Discovery tools.
Team	€199 / workspace / month	Gateway, per-member tokens, allowlists, audit logs, hosted servers.
Enterprise	From €999 / month	Enterprise governance, audit exports, private deployment options, procurement support.
Pilot	€1,000 / 30 days	Private workspace in 48h, governed Gateway, hosted servers, controls, final report.

48h
WORKSPACE CONFIGURED

7 days
AUDIT LOGS & ACCESS REVIEW

30 days
EVIDENCE TO DECIDE

The recommended entry point is the **30-Day MCP Governance Pilot** — specific, fast, and outcome-oriented. **Best next step: choose one team, five MCP servers, and one governed workspace.** A company gets a working workspace, governed Gateway, access controls, hosted servers, and a final recommendation report.