MCP SERVER | NO CODE | CLOUD HOSTED

HetrixTools MCP

Check service health and IP reputation instantly.

HetrixTools lets you monitor critical infrastructure health and manage IP reputation using natural conversation. Check the uptime of websites, list all monitors for a service, or scan any domain against 90+ global blacklists directly from your AI agent. It gives system admins real-time visibility into both availability and digital standing.

A+ Quality Score 100/100

uptime-monitoring | blacklist-checking | server-health | ip-reputation | availability-reports | network-monitoring

MAINTAINED BY VINKIUS CLOUD FOR AI AGENTS · JUNE 2026
vinkius.com/mcp/hetrixtools

SCAN TO VIEW

The infrastructure that powers AI agents in the real world.

Vinkius connects AI to the world's software through secure, enterprise-grade infrastructure — enabling real-world execution at scale, built on the Model Context Protocol (MCP).

Your AI Connections Run Through Vinkius Cloud

The world's largest managed MCP catalog

Vinkius is the cloud infrastructure where AI agents connect to the software your business already runs. We handle the hosting, the security, the credentials, the uptime — you get agents that actually do things.

We operate the world's largest managed MCP catalog. Major SaaS platforms, CRMs, databases, and cloud providers — running, monitored, production-ready. This MCP server is hosted and maintained by the Vinkius Cloud for AI Agents.

> *The agent doesn't manage credentials, doesn't manage uptime, doesn't manage security. Vinkius does.*
>
> — Architecture principle

Four Pillars of the Vinkius Runtime

01 — Security by design

Credentials stay encrypted at rest via AES-256. The AI agent never touches raw keys — they're injected into a sandboxed V8 isolate at runtime. Actions are logged, and connections have an emergency kill switch.

02 — Built on MCP Fusion

This MCP server was built with **MCP Fusion**, the open-source framework (Apache 2.0) that powers the entire Vinkius catalog. Schema-as-firewall strips undeclared fields, compiled PII redaction runs at zero overhead, and cryptographic lockfiles produce git-diffable audit trails.

03 — Deterministic observability

Eight immutable metrics per endpoint: request volume, p95 latency, error rate, active connections, cost attribution. A live payload feed logs every tool call with mutation detection.

04 — Autonomous operations

Servers are deployed, monitored, and patched autonomously. New capabilities and security patches ship weekly. Zero-downtime deployments ensure continuous availability across all managed MCP servers.

AES-256	Ed25519	24h TTL	V8 Isolate
Encryption at rest	PKI vault signatures	Ephemeral session keys	Sandboxed execution

One Token. Instant Access.

Every MCP server on Vinkius is accessed through a **Connection Token**. Tokens are generated in the cloud dashboard and produce a unique MCP endpoint URL. Paste this URL into any MCP-compatible client — no SDK required.

A single token can serve **multiple AI clients simultaneously**, or you can issue separate tokens per client for granular access control. Each token tracks its own request count, last activity timestamp, and can be individually enabled or revoked.

MCP ENDPOINT

```
https://edge.vinkius.com/{token}/mcp
```

Claude · Cursor · VS Code · Windsurf · Grok · Gemini

Security Is the Architecture

Security in Vinkius is not a feature — it's the foundation of the runtime. The gateway enforces multiple independent protection layers between AI agents and third-party APIs.

01 — Ed25519 PKI Vault

Every workspace has an Ed25519 Master Key. Session keys are generated ephemerally (24h TTL) and signed by the Master Key. Credentials never leave the vault boundary.

02 — V8 Isolate Sandboxing

Tool code runs inside isolated-vm V8 isolates with 64 MB memory caps and per-request timeouts. No filesystem access, no network access except through the SSRF-guarded fetch bridge.

03 — SSRF Guard

All outbound HTTP requests are DNS-resolved and validated before execution. Private IP ranges (10.x, 172.16-31.x, 192.168.x, AWS metadata 169.254.x) are blocked at the network layer.

04 — DLP & PII Redaction

A ResponseGuard pipeline intercepts every tool response. Configurable redaction patterns strip sensitive fields (emails, SSNs, card numbers) before data reaches the AI agent.

05 — Cryptographic Audit Trail

Every request is signed into a SHA-256 hash chain with Ed25519 signatures. Events form a tamper-proof, SIEM-exportable forensic record.

06 — Honeytoken Trap System

Phantom credentials are injected into isolated environments. If a honeytoken is used outside Vinkius infrastructure, the server is quarantined instantly.

Emergency Kill Switch

EU AI Act Art. 14(1) Compliant

The kill switch is an **emergency halt** mechanism — not a simple toggle. When triggered, it executes three actions atomically:

01 — Server deactivated

The MCP server is immediately taken offline across the entire cluster.

02 — All tokens revoked

Every connection token is invalidated. Total lockout — reconnection blocked until new tokens are issued.

03 — WebSocket connections killed

Active connections terminated via Redis pubsub broadcast. Propagates to every runtime node in the cluster.

Full Visibility. Zero Guesswork.

The Vinkius cloud dashboard includes a full MCP Governance suite — real-time analytics and security controls for production AI operations.

Control Plane

KPI dashboard with request volume, latency, success rate, token consumption, and AI-generated operational briefings.

Agent Activity

Which AI clients are connecting, how often, and what they're doing — real-time session tracking.

FinOps

Cost tracking per tool, payload compression savings, budget optimization signals, and consumption trends.

Tool Health

Slowest and most error-prone tools, with actionable root-cause insights and performance baselines.

Firewall & DLP

PII redaction activity, sensitive data protection counters, and security event timeline.

Incident Log

Error trends, failure rates, status-code breakdowns, and forensic audit trail access.

> Get started at **cloud.vinkius.com** — connect your AI agent in under 60 seconds.

HetrixTools MCP

11 tools available
Cloud-hosted on Vinkius

Connect this MCP to your preferred AI client, and you get instant control over monitoring infrastructure health and managing IP reputation without logging into a dashboard. You can ask your agent to check if a specific website is up right now or generate detailed reports on service history. If you're worried about mail delivery issues, you just ask it to run an on-demand blacklist scan for a domain. Need to know if an IP address got flagged anywhere? It handles that too, checking against dozens of global blacklists. This capability means your agent acts like a dedicated system administrator or DevOps engineer. When combined with the Vinkius catalog, you access all this deep infrastructure data from one place, letting your AI client do the heavy lifting so you don't have to manually check dashboards.

Core Capabilities

01 — Check service availability

The agent lists existing uptime checks and runs real-time tests on websites or services.

02 — Validate IP and domain reputation

It performs on-demand blacklist scans against global blacklists for any given IPv4 address or domain name.

03 — Manage monitoring reports

You can retrieve detailed availability history, list all generated bulk reports, and check your account's usage limits.

04 — Control maintenance modes

The agent toggles a monitor into specific maintenance states so you can perform updates without triggering false alerts.

One Click on Vinkius — From Prompt to Execution

Available at **vinkius.com/mcp/hetrixtools** — connect your AI agent in three steps.

01 First, subscribe to this MCP and provide your HetrixTools API Token in the account settings.

02 Next, prompt your AI agent with a request, like 'Check the status of my primary website' or 'Scan 192.168.1.1 for blacklisting'.

03 Your agent uses the tool to run the check and delivers a plain-language summary of the service health or blacklist result directly into your chat.

The bottom line is, you use natural language conversation instead of clicking through complex monitoring dashboards.

Built For

This MCP solves problems for Ops Engineers and System Admins who spend too much time jumping between multiple monitoring tools just to check if a service or IP is clean. If your job involves uptime guarantees, you need this.

DevOps Engineer

Runs health checks on services and toggles maintenance modes when deploying code so they don't trigger false alerts.

System Administrator

Automates the auditing of IP reputation and domain blacklist status across multiple networks without manual lookups.

Web Site Owner

Receives instant, summarized reports confirming their site's uptime or alerting them immediately if a service goes down.

What Changes When You Connect

01 Real-time status checks: Instead of checking a dashboard, you just ask your agent to list uptime monitors and get an immediate summary of what's working and what isn't.

02 Deep blacklist validation: You don't have to visit separate services; the agent runs on-demand blacklists for both IP addresses and domains across 90+ global lists in one go.

03 Control monitoring alerts: Need to update a site? Use set_maintenance_mode to put a monitor into maintenance mode, guaranteeing you won't get false outage alerts during deployment.

04 Comprehensive reporting access: You can list all generated bulk reports and check historical data using list_uptime_reports, giving you proof of service stability when needed.

05 Resource awareness: The tool provides get_account_usage, so you always know how much API quota you've burned. No unexpected bill shocks.

06 Team coordination: Manage notification systems by listing contact lists, ensuring outage alerts go to the right people every time.

Real-World Applications

Post-deployment verification

The DevOps Engineer just pushed a new version. They ask their agent to list uptime monitors and then use set_maintenance_mode on all endpoints, ensuring no one gets alerted while they test the rollout. Once done, they restore the monitors.

Investigating mail bounces

A user is getting constant bounce messages. They ask their agent to check_domain_blacklist for the domain in question. The agent scans 90+ lists and reports back if it's flagged, saving hours of manual research.

Quarterly audit prep

The System Administrator needs proof that their main API endpoint has been stable for the last quarter. They ask the agent to list_uptime_reports and retrieve a comprehensive report showing minimal downtime.

Pre-launch risk assessment

A Website Owner is about to launch a major service change. Before they commit, they use check_ip_blacklist on their primary IP address to verify it has zero negative reputation listings anywhere globally.

Patterns to Avoid

Checking status one by one

✗ AVOID

Opening the monitoring dashboard and manually checking five different websites' colored lights, then opening a separate tool to check blacklists.

✓ INSTEAD

Instead, ask your agent to list_uptime_monitors for an overview. Then, use check_ip_blacklist or check_domain_blacklist in one prompt to validate reputation instantly.

Ignoring maintenance windows

✗ AVOID

Running a major update and getting multiple 'DOWN' alerts because the monitoring service was briefly offline during deployment.

✓ INSTEAD

Always use set_maintenance_mode before updates. This prevents false alarms and keeps your team focused on real problems.

Not tracking usage

✗ AVOID

Running dozens of blacklist checks until the API key hits a hard limit, causing service interruption.

✓ INSTEAD

Check get_account_usage first. This tool shows exactly how close you are to hitting your plan limits.

The Right Fit

Use this MCP if your primary pain point is visibility across two specific areas: service uptime and internet reputation. You need a single chat interface that can query complex, external data sources like global blacklists and historical monitoring logs. Don't use it if you only need to send simple status messages; for that, a basic notification tool works fine. If you just need to track resource usage without checking service health, stick with a billing or analytics integration. But if the question is 'Is this IP clean?' or 'Was my site up last week?', this MCP has the tools.

The Pain of Manual Infrastructure Audits

Right now, checking your infrastructure means logging into five different web portals. You check uptime on one dashboard, then you copy-paste an IP address into a separate blacklist checker, and finally, you have to manually sift through usage reports just to know if you're over budget. It takes clicks, tabs, and ten minutes of coffee.

With this MCP, that process collapses. You talk to your agent like talking to a teammate. You ask the question—whether it’s 'Is my site up?' or 'Is this IP clean?'—and get an immediate, actionable answer without ever leaving the chat window.

HetrixTools Gives You Instant Infrastructure Insight

You no longer have to jump between monitoring tools. The agent runs checks like list_uptime_monitors and check_domain_blacklist for you, pulling data from multiple sources into one response.

The difference is that your AI client doesn't just provide a link; it executes the full task and tells you what happened. It’s immediate control, not delayed reporting.

HetrixTools: 11 Infrastructure Tools

Use these tools to manage all aspects of your network health, from scheduling uptime checks to validating IP and domain blacklisting status.

#	TOOL	DESCRIPTION
01	`add_uptime_monitor`	Creates a brand new scheduled monitor to check the availability of a website or endpoint.
02	`check_domain_blacklist`	Performs an immediate blacklist scan specifically for checking if a domain name is flagged.
03	`check_ip_blacklist`	Runs an on-demand check to see if an IPv4 address is listed on any blacklists.
04	`delete_uptime_monitor`	Removes an existing uptime monitor from your list of scheduled checks.
05	`get_account_usage`	Retrieves statistics on how much API and resource usage you've consumed for the month.
06	`list_blacklist_monitors`	Shows all the IP address and domain name monitors currently set up to track blacklisting status.
07	`list_bulk_reports`	Lists every comprehensive bulk report that has been generated by the system.
08	`list_contact_lists`	Retrieves a list of contact groups used for sending out outage notifications.
09	`list_uptime_monitors`	Lists all the scheduled uptime checks and their current health status to give an overview of your services.
10	`list_uptime_reports`	Fetches detailed, historical reports for a specific monitor ID showing its past performance.
11	`set_maintenance_mode`	Toggles an uptime monitor into maintenance mode (Normal, Maint. w/ notifications, or Maint. without notifications).

See It in Action

Real prompts you can use once this MCP is connected to your AI agent through Vinkius Cloud.

U List all my uptime monitors and their current status.

I've retrieved your monitors. You have 5 active checks: 'Primary Website' (Up), 'API Endpoint' (Up), 'DB Server' (Up), 'Mail Gateway' (Up), and 'Staging Site' (Down - since 5 mins ago). Would you like to see the error log for the Staging Site?

U Check if the IP address 1.2.3.4 is blacklisted.

Blacklist check initiated for 1.2.3.4. I've scanned 94 global blacklists. The IP is currently CLEAN (0/94 listings). Would you like to add this IP to your permanent blacklist monitors?

U Put monitor ID 'm123' into maintenance mode without notifications.

Maintenance mode updated! Monitor m123 is now in mode 3 (Maintenance without notifications). You can perform your updates without triggering any alerts. Should I list your other monitors?

Frequently Asked Questions

01 **How do I find my HetrixTools API Token?**

Log in to your HetrixTools account, navigate to **Account Settings**, and click on the **API** tab. You will be able to generate and copy your unique API Token from there.

02 **Can I perform on-demand blacklist checks?**

Yes! Use the `check_ip_blacklist` or `check_domain_blacklist` tools. These trigger real-time scans across 90+ blacklists. Note that these requests can take a few minutes to complete.

03 What are the maintenance modes for monitors?

The integration supports three modes: 1 (Normal), 2 (Maintenance with notifications enabled), and 3 (Maintenance without notifications). Use `set_maintenance_mode` to toggle these.

04 Is the integration secure for monitoring data?

Absolutely. The integration uses industry-standard Bearer tokens (v3) or secure URL tokens over HTTPS. Your credentials are encrypted and stored securely within the Vinkius Cloud infrastructure.

Go Live in 60 Seconds

Get your connection token from **cloud.vinkius.com**, then paste the endpoint URL into any MCP-compatible client.

YOUR MCP ENDPOINT

```
https://edge.vinkius.com/[TOKEN]/mcp
```

CLIENT	WHERE TO CONFIGURE
Claude AI	Profile → Customize → Connectors → "+" → Add custom connector → Paste endpoint
Cursor	Settings → Features → MCP Servers → "+ Add New MCP Server" → Type: SSE → Paste endpoint
VS Code	Ctrl/Cmd+Shift+P → "MCP: Add Server" → add `"hetrixtools": { "url": "…" }`
Windsurf	MCP Settings → `mcp_settings.json` → Add endpoint URL
ChatGPT	Settings → Tools & plugins → Add MCP server → Paste endpoint
Gemini	Extensions → Add MCP Server → Paste endpoint URL

ASK AN AI ABOUT THIS

Let your preferred AI explain this MCP server

- Ask ChatGPT
- Ask Claude
- Ask Perplexity
- Ask Gemini
- Ask Grok

READY TO CONNECT

HetrixTools is live on Vinkius Cloud.

Get your connection token, paste it into your AI agent, and start building. No SDK. No deployment. Just results.

Start at cloud.vinkius.com →

vinkius.com · support@vinkius.com

INDEPENDENT PLATFORM DISCLAIMER

Vinkius is an independent platform and is not affiliated with, endorsed by, sponsored by, verified by, or otherwise authorized by HetrixTools. All third-party trademarks, logos, and brand names are the property of their respective owners. Their use in this document is strictly for informational purposes to identify service compatibility and interoperability.

DOCUMENT INFORMATION

Generated	June 2026
MCP Server	HetrixTools MCP
Server ID	`019d75b0-2801-7175-bb18-c5c61fce3168`
Platform	Vinkius Cloud for AI Agents
Endpoint	`https://edge.vinkius.com/{token}/mcp`

LICENSE & USAGE

This document is generated automatically by the Vinkius PDF Engine. Content reflects the MCP server configuration at the time of generation and may change as updates are deployed. For the most current information, visit vinkius.com/mcp/hetrixtools.