MCP SERVER | NO CODE | CLOUD HOSTED

Hexometer MCP

Run deep website audits from your AI agent.

Hexometer connects your website monitoring data to any AI agent. It lets you manage technical site health and performance from a simple conversation. Need to check if a page is fast on mobile or identify broken links across dozens of sites? Your AI client runs deep audits, checks historical uptime logs, and validates SSL certificate status—all without you opening a dashboard. Stop manually checking monitoring reports; just ask your agent.

A+ Quality Score 100/100

website-health | page-speed | performance-monitoring | uptime-tracking | technical-seo | asset-analysis

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

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.

Hexometer MCP

11 tools available
Cloud-hosted on Vinkius

Tired of logging into multiple dashboards to check if your website is still running smoothly? This MCP lets your AI client act as a dedicated web performance engineer for all your properties. You can ask it to analyze speed, triggering on-demand page tests for both desktop and mobile devices. It pinpoints heavy scripts, large images, or JavaScript errors that slow things down. Need to know if every link works? The agent checks broken links across your domain. Furthermore, you can pull historical uptime statistics or run a full SEO audit against meta tags and headers. If you're looking for an easy way to manage technical web assets through natural conversation, connecting this MCP via Vinkius is the quickest way to get control.

Core Capabilities

01 — Test Page Speed

Analyzes how quickly a specific URL loads when viewed on desktop or mobile devices.

02 — Check Site Health Status

Retrieves the overall health score and monitors critical elements like SSL certificate expiry for any connected property.

03 — Monitor Uptime History

Accesses historical data to show if a site experienced service interruptions over time, listing recent alerts as well.

04 — Audit SEO Elements

Performs on-demand scans of pages to check meta tags, headers, and detect broken links (404 errors).

05 — Scan for Code Errors

Scans a page specifically to identify JavaScript errors or overly heavy assets that hurt performance.

One Click on Vinkius — From Prompt to Execution

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

01 Subscribe to the Hexometer MCP and provide your API Key. You'll find this key in the property settings on the Hexometer site.

02 Connect this MCP to any compatible AI agent, like Cursor or Claude.

03 Ask your agent a specific question—for example, 'What is the mobile speed score for my main landing page?' The agent then uses the necessary tool to fetch and summarize the data.

The bottom line is that you talk to your AI client like talking to an engineer, and it handles all the background checking across multiple tools.

Built For

This MCP serves web developers who hate manual testing, technical SEO specialists who manage dozens of sites, and e-commerce owners worried about conversion rate dips due to slow loading times. It's for anyone whose job involves keeping a website running fast and healthy.

Web Developer

Uses the agent to run `check_page_errors` or `check_speed_desktop` during staging to instantly get JS error logs, eliminating manual testing cycles.

Technical SEO Specialist

Runs bulk checks using `list_monitored_sites` and then `run_seo_audit` to ensure every client property has correct meta tags and no broken links.

DevOps Engineer

Uses the MCP to check overall site integrity by running `get_site_health` and reviewing historical alerts via `list_recent_alerts`, ensuring service reliability.

What Changes When You Connect

01 Stop guessing about site performance. Running `check_speed_mobile` or `check_speed_desktop` gives you concrete scores and details on what's slowing the user down, whether it’s a heavy script or a large image asset.

02 You get immediate visibility into your entire portfolio by using `list_monitored_sites`. This tool shows every website Hexometer tracks, so you never lose sight of an important property.

03 Never worry about forgotten maintenance tasks again. Use `get_security_status` to confirm SSL certificate expiry and check the general security health across all your digital assets in one query.

04 Eliminate wasted time on link checking. Instead of manually crawling, ask for `check_broken_links`, and the agent returns a clean list of every 404 error found.

05 Maintain trust with clients by having real-time data access. Running `get_uptime_stats` provides irrefutable proof of service reliability over months or years.

Real-World Applications

A client reports slow loading times after a site update.

The developer asks their agent to check the site performance. The agent runs `check_page_errors` and quickly identifies that three new JavaScript files are causing bloat, allowing the developer to fix them immediately.

A marketing manager needs to audit 50 product pages for SEO compliance.

The specialist asks their agent to list all properties via `list_monitored_sites`. Then, they run `run_seo_audit` on a sample set, quickly spotting missing alt tags and incorrect meta titles across the entire catalog.

A site owner is worried about an upcoming SSL certificate renewal deadline.

The agent runs `get_security_status` and immediately flags that the SSL certificate expires in 14 days. The owner can then set a reminder and get ahead of a critical outage.

A maintenance team needs to check overall site reliability after an overnight deployment.

The engineer asks for `get_site_health` and reviews `list_recent_alerts`. The agent confirms the score is high, but points out a recent minor service interruption that needs investigation.

Patterns to Avoid

Assuming performance metrics are always available.

✗ AVOID

Asking the agent to 'check speed' without specifying if you want mobile or desktop results, leading to a generic or incomplete report.

✓ INSTEAD

Always specify your target device. To get accurate data, run `check_speed_mobile` for user experience insights, or use `check_speed_desktop` when optimizing for high-resolution screens.

Treating the agent as a simple search engine.

✗ AVOID

Asking the agent to 'fix my broken links.' The MCP only reports data; it doesn't execute code or fix the underlying 404 errors for you.

✓ INSTEAD

Use `check_broken_links` to generate a list of all bad URLs. You take that actionable list and use your developer tools to implement the fixes.

Ignoring site inventory management.

✗ AVOID

Focusing only on one known URL, forgetting about other properties under the same client account.

✓ INSTEAD

Start by calling `list_monitored_sites` to get a full manifest. Then loop through that list and run checks like `get_site_health` for every single property.

The Right Fit

Use this MCP if your job requires proactive, repeatable analysis of technical web assets across multiple domains. Specifically, use it when you need to audit things like page speed (e.g., running `check_speed_mobile`), check structural integrity (using `run_seo_audit`), or verify uptime history (`get_uptime_stats`). Don't use this MCP if your problem is purely conceptual, like 'How should I improve my brand copy?' If you need to perform deep code changes, complex database writes, or integrate with a non-web

service (like an internal CRM), you need a different kind of tool. This MCP reports data; it doesn't change the core business logic.

The Website Health Checklist You Never Finish

Right now, keeping track of site health means clicking into Hexometer, opening a new tab for every property, running the speed test manually, copy-pasting URLs to check for broken links, and then compiling all that data in a spreadsheet. You spend hours just gathering status reports instead of fixing problems.

With this MCP, you tell your agent exactly what you need—'Check the mobile performance and look for security issues on our top 10 landing pages.' Your agent does the heavy lifting, pulling speed scores, checking SSL expiry, and listing assets in a single response. You get actionable insights instantly.

Hexometer MCP Gives You Complete Site Oversight

You don't have to juggle separate tools for performance, security, and SEO anymore. Instead of opening three different dashboards, you ask the agent to perform a holistic check using `get_site_health` and combine it with running an SEO scan via `run_seo_audit`. It’s all one conversation.

What changes now is that your AI client doesn't just report data; it acts as a unified command center for your entire web presence. You go from manual dashboard review to single-prompt site oversight.

Hexometer: 11 Site Audit Tools

Use these tools to audit page speed, check for broken links, review security status, and track historical uptime across all your monitored web properties.

#	TOOL	DESCRIPTION
01	check_broken_links	Finds and lists any detected 404 errors or broken links for a specific web property.
02	check_page_errors	Scans an entire page to pinpoint JavaScript errors and heavy assets that impact performance.
03	check_speed_desktop	Analyzes the speed score and asset details for a given URL when accessed on a desktop computer.
04	check_speed_mobile	Performs an analysis of page load speed specifically for mobile devices, giving you crucial user insight.
05	get_site_health	Retrieves the comprehensive overall health score and status report for a specific website property.
06	get_security_status	Checks the SSL certificate expiry date and general security posture of a site.
07	get_uptime_stats	Provides historical data showing how consistently available a website has been over time.
08	list_recent_alerts	Pulls a list of the most recent monitoring alerts and notifications for your monitored sites.
09	list_monitored_sites	Generates an inventory by listing all websites (properties) that are currently tracked in Hexometer.
10	list_wordpress_syncs	Lists all active WordPress plugin synchronizations running within the system.
11	run_seo_audit	Executes an on-demand SEO scan against a specific URL to check for structural and meta tag issues.

See It in Action

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

U Analyze the mobile page speed for 'https://example.com'.

Analyzing mobile performance... Example.com has a mobile speed score of 82/100. The largest contentful paint (LCP) is 2.4s. I also detected 3 heavy image assets that could be optimized. Would you like the full list of errors?

U Show me the health status for property ID 'prop_123'.

Accessing site health... Property prop_123 is currently Healthy (Score: 94/100). Uptime is 100% for the last 30 days. However, the SSL certificate expires in 12 days. Should I set a reminder for the renewal?

U Run an SEO audit for 'https://myblog.com/post-1'.

SEO audit complete! I've scanned the post. Meta titles and descriptions are well-optimized. However, 2 images are missing alt tags and there is no H1 header defined. Would you like me to suggest some improvements?

Frequently Asked Questions

01 **How does the Hexometer MCP check if my links are broken?**

The agent uses `check_broken_links` to scan a specified property and returns a list of all detected 404 errors. This saves you from having to crawl link by link.

02 **Can I get mobile speed data using the Hexometer MCP?**

Yes, run `check_speed_mobile` to analyze page load speed specifically for mobile users. This is vital because mobile performance often differs greatly from desktop results.

03 **What information does list_monitored_sites provide?**

`list_monitored_sites` gives you a complete inventory of every web property currently tracked in your Hexometer account, helping you ensure nothing is missed during an audit.

04 **Does the Hexometer MCP check for JavaScript errors?**

Yes. You can use `check_page_errors` to scan a page and specifically identify JavaScript errors or pinpoint assets that are overly heavy, helping you optimize code.

05 **How often should I run get_site_health with the Hexometer MCP?**

You should use `get_site_health` anytime major changes occur to a site, or weekly if you suspect performance degradation. It provides your overall health score and security status.

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 `"hexometer": { "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

Hexometer 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 Hexometer. 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	Hexometer MCP
Server ID	`019d75b0-bdde-7215-8ed2-c0fde6e85582`
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/hexometer.