

MCP SERVER

NO CODE

CLOUD HOSTED

Mention MCP

Know brand sentiment from any source.

Mention MCP connects your social listening and brand monitoring data directly to your AI client. Track every mention, analyze public sentiment, and get real-time alerts across all channels simply by talking to your agent. Stop checking dashboards; start having conversations.

A+ Quality Score 98.33/100

brand-monitoring

social-listening

alerting

sentiment-analysis

media-tracking



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.

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.

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.

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

Encryption at rest

Ed25519

PKI vault signatures

24h TTL

Ephemeral session keys

V8 Isolate

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.

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.

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.

06 — Honeypot Trap System

Phantom credentials are injected into isolated environments. If a honeypot 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.

FinOps

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

Firewall & DLP

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

Agent Activity

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

Tool Health

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

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.

Mention MCP

10 tools available

Cloud-hosted on Vinkius

Monitoring what people are saying about your brand used to mean juggling ten different platforms and manually compiling reports. Now, you connect Mention to any AI client through Vinkius, giving your agent complete control over social monitoring and brand alerts. Instead of digging through feeds, you just ask your agent questions. You can list all active alerts or search for specific topics across thousands of mentions. Need to know how the conversation is trending? Your agent runs a sentiment analysis on recent posts, letting you see volume stats instantly. It's about turning massive amounts of public chatter into actionable insights without ever leaving your chat window.

Core Capabilities

01 — Manage Brand Alerts

List all monitoring alerts and grab detailed metadata for any specific alert configuration.

03 — Analyze Mention Details

Get full content, metadata, and sentiment scores for any single mention you point out.

05 — Audit Account Access

List all authorized users or connected social media accounts associated with the Mention profile.

02 — Search and Retrieve Mentions

Pull recent social media mentions, search by keyword, or filter the list down to your favorites.

04 — Measure Brand Performance

Access volume and sentiment statistics for your alerts to track changes over time.

One Click on Vinkius — From Prompt to Execution

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

- 01** First, subscribe to this MCP and enter your unique Mention Access Token and Account ID.
- 02** Next, connect your preferred AI client—Claude, Cursor, or any compatible agent—to Vinkius.
- 03** Finally, simply ask your agent to perform an action; it handles the rest of the data retrieval.

The bottom line is that you treat complex social data like a simple conversation with your AI client.

Built For

This MCP is built for PR professionals and marketing managers who wake up needing to know how the brand narrative shifted overnight. It solves the pain of spending hours switching between monitoring dashboards just to compile a single report.

PR Manager

Uses this MCP to check for negative sentiment immediately after a product launch, asking the agent to run deep inspection on mentions mentioning competitors.

Content Strategist

Asks the agent to search mentions for specific keywords and then list connected external accounts to see where they should focus their next campaign.

Marketing Analyst

Runs brand analytics queries to compare volume and sentiment statistics month-over-month, giving management hard data on public perception.

What Changes When You Connect

- 01** Instant Sentiment Scoring: When you need to know if people are happy or angry, your agent runs deep inspection on specific mentions and provides an immediate sentiment score. You don't read thousands of comments; you get the consensus.

-
- 02** Track Everything at Once: Instead of checking separate dashboards, simply ask your agent to list all monitoring alerts, and it gives you a single overview of every brand conversation happening.

 - 03** Deep Dive Data Access: Need more than just the text? Use `get_mention_details` to fetch full content, metadata, and detailed analysis for any post. It's the complete picture in one go.

 - 04** Measure Trends Instantly: When you want hard numbers, ask your agent about brand analytics; it gives volume and sentiment statistics instantly, letting you compare performance against yesterday or last month.

 - 05** Stay Organized: Keep track of everything with `list_favorite_mentions`. You can mark the most important posts right in conversation and pull them up later without searching.
-

Real-World Applications

Crisis Response

A PR manager notices a spike in negative chatter. They ask their agent to list mentions, filter for those mentioning the product name, and then run `get_mention_details` on the top five results to understand the core complaint.

Competitive Analysis

The team needs to know what competitors are doing. They use `search_mentions` to track competitor names alongside their brand name, allowing them to see how often the discussion shifts from your company to theirs.

Campaign Performance Review

A marketing analyst wants to measure a new campaign's reach. They ask their agent to check brand analytics for the associated alert, seeing volume and sentiment statistics that prove the campaign moved the needle compared to last quarter.

Account Health Check

A new employee joins the team and needs access. The agent runs `list_account_users` to confirm who has permissions, while also checking `list_connected_external_accounts` to ensure all necessary social channels are linked.

Patterns to Avoid

Manual Dashboard Comparison

X AVOID

Trying to manually compare today's volume stats on the Mention dashboard against a separate spreadsheet of last month's data. This is slow and prone to copy/paste errors.

✓ INSTEAD

Ask your agent directly for brand analytics, specifically requesting the comparison metrics using `get_alert_statistics`. It handles the cross-referencing instantly.

Keyword Overload

X AVOID

Writing a massive list of 50 keywords into a search form and hoping it catches everything relevant. The system usually misses nuances.

✓ INSTEAD

It's better to use the agent to run targeted searches using `search_mentions` for groups of related terms, like 'AI ethics' OR 'responsible AI'.

Ignoring Alert Scope

X AVOID

Looking at general mentions when you really only care about a specific alert (like one monitoring product reviews). This gives too much noise.

✓ INSTEAD

Always start by listing alerts with `list_alerts`, and then narrow your focus using the dedicated tool for that topic, like `list_mentions`.

The Right Fit

Use this MCP if your primary job is monitoring public conversation, tracking brand sentiment, or managing social media alerts. You need to know what people are saying *right now* about your company or industry. Don't use it if you only need historical database lookups (use a dedicated CRM tool instead). Also, don't use it just because you want to see raw API endpoints; the power is in asking natural language questions. If your goal is simply to draft social media posts based on internal data, use a content generation MCP. But if you need external public opinion and sentiment analysis, this is your tool.

The Pain of Social Monitoring Reports

Every Monday morning, you open the monitoring dashboard, switch to the analytics tab, then pivot over to the mentions feed. You copy volume stats into a spreadsheet, grab sentiment percentages from one section, and pull raw mention data into another. By the time you compile the report, it's already late afternoon, and half your findings are based on stale data.

With this MCP, all that manual clicking vanishes. You tell your agent, 'What was our brand sentiment last week?' It doesn't open a dashboard; it runs the query instantly and gives you one synthesized answer right where you're chatting. The outcome is immediate insights instead of tedious data compilation.

Getting Full Brand Context with Mention MCP

You no longer have to open a mention, copy the text, paste it into a separate sentiment analyzer tool, and then manually record the score. The process of getting full content, metadata, and sentiment analysis for specific mentions is consolidated.

Now you get the complete context—the who, what, and how people feel—in one step. It's about moving from simply collecting data to actually understanding the story behind it.

Mention MCP with 10 Tools

These tools let you perform every necessary action for comprehensive social listening: listing accounts, tracking mentions, and running detailed analytics.

#	TOOL	DESCRIPTION
01	<code>get_account_info</code>	Retrieves high-level information about the main Mention account settings.
02	<code>get_alert</code>	Fetches specific configuration details for a single monitoring alert you manage.
03	<code>get_alert_statistics</code>	Provides key performance metrics, like total mention volume, for any given alert.
04	<code>get_mention_details</code>	Pulls the full content, source metadata, and sentiment analysis for a single public post.
05	<code>list_account_users</code>	Shows who has access to the account by listing associated users.
06	<code>list_alerts</code>	Retrieves a comprehensive list of all active and inactive monitoring alerts you have set up.
07	<code>list_connected_external_accounts</code>	Lists which external social media accounts are currently linked to the Mention dashboard.
08	<code>list_favorite_mentions</code>	Retrieves a curated list of mentions you have specifically marked as favorites for an alert.
09	<code>list_mentions</code>	Lists the most recent social media mentions tied to a specific monitoring alert.
10	<code>search_mentions</code>	Searches through all historical and current mentions using custom text keywords.

See It in Action

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

U List all active alerts in my Mention account.



Retrieving alerts... I found 3 active alerts including 'Brand Monitor', 'Competitor A', and 'Industry Trends'.

U Search mentions for 'artificial intelligence' in alert ID 123.



Searching mentions... I found 5 recent posts mentioning AI in your brand alert stream.

U Show volume statistics for my primary brand alert.



Calculating statistics... You had 150 mentions today, a 10% increase compared to yesterday.

Frequently Asked Questions

01 How do I check if a specific alert is active with Mention MCP?

You can use `list_alerts` to see all your monitoring alerts and verify their current status. This gives you a quick overview of everything that's running.

02 Can Mention MCP search for mentions across different topics?

Yes, the `search_mentions` tool lets you run keyword searches across various topics. You can combine keywords to track complex narratives or multiple product lines at once.

03 What if I want to see how my brand performance has changed? Do I use Mention MCP?

You should use the `get_alert_statistics` tool. This pulls volume and sentiment statistics for your alerts, letting you measure changes over time accurately.

04 Does `list_account_users` help with security on Mention MCP?

Absolutely. Using `list_account_users` lets you see exactly who has access to the account, which is crucial for maintaining proper internal controls and data security.

05 How do I analyze a single mention's sentiment using Mention MCP?







You use `get_mention_details`. This tool fetches all the necessary context—the full content, metadata, and the detailed sentiment score for that one specific post.

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 <code>"mention": { "url": "..." }</code>
 Windsurf	MCP Settings → <code>mcp_settings.json</code> → 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

Mention 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](https://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 Mention. 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	Mention MCP
Server ID	019d75d2-6469-7038-bb91-9d83e7700ef7
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/mention.