MCP SERVER | NO CODE | CLOUD HOSTED

IPinfo MCP

Map IPs to ownership, location, and network context.

IPinfo provides instant deep intelligence on IP addresses. Your AI client can instantly map an IP to its precise location, determine network ownership details (ASN), and retrieve full WHOIS records for organizations or networks. It also lets you check which domains are hosted on a specific IP, making it essential for security analysis and traffic pattern mapping.

A+ Quality Score 100/100

ip-lookup | geolocation | asn | whois | threat-intelligence

MAINTAINED BY VINKIUS CLOUD FOR AI AGENTS · JUNE 2026
vinkius.com/mcp/ipinfo-alternative

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.

IPinfo MCP

10 tools available
Cloud-hosted on Vinkius

When your agent needs to figure out where an IP address belongs, this MCP delivers instant intelligence. Instead of manually checking multiple databases—one for geography, another for ownership, and yet another for domain records—you send the IP, and the data comes back enriched. You can get precise city, region, and country details instantly. Need to know who owns a large block of IPs? It identifies Autonomous System numbers and associated ranges. The agent also pulls full WHOIS reports detailing network owners or specific points of contact. Furthermore, you can enrich massive sets of IP addresses at once, handling up to 1,000 in one go. If you're building automated security checks, this MCP gives your client the deep visibility it needs, all connected easily through Vinkius.

Core Capabilities

01 — Determine IP location and carrier details

Fetch detailed geographic data, including city, country, and carrier information for any given IP address.

02 — Check network ownership and ranges

Look up Autonomous System (ASN) details or gather all associated IP ranges linked to a specific domain name.

03 — Analyze organization and network records

Retrieve comprehensive WHOIS data covering the entire network, owning organization, or point of contact.

04 — Reverse lookup hosted domains

Discover which web domains are registered to use a particular IP address.

05 — Process large batches of IPs

Enrich multiple IP addresses simultaneously, supporting high-volume data analysis.

One Click on Vinkius — From Prompt to Execution

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

01 First, you connect this MCP to your preferred AI client and input your unique access token.

02 Next, you ask your agent to check an IP address or a list of IPs for specific data points, like location or ownership.

03 Finally, the client executes the necessary lookup tools and returns structured, enriched data directly to your workflow.

The bottom line is that it turns complex, multi-database investigations into a single conversational query.

Built For

Security researchers who need instant visibility into suspicious traffic. Data analysts tasked with mapping user movement and network context. DevOps engineers managing large-scale infrastructure deployments.

Cybersecurity Analyst

Using this MCP, they quickly investigate the origin of malicious IPs during an incident response to identify ownership and potential threat vectors.

Data Analyst

They enrich user log data with geographic context—city, country, etc.—to accurately model traffic patterns for business intelligence reports.

DevOps Engineer

They verify network ranges and map hosted domains against known infrastructure blocks to troubleshoot connectivity issues or plan deployments.

What Changes When You Connect

01 Instant threat identification: Instead of guessing an IP's origin during an incident, you get immediate details on its geographic source and carrier using lookups like `get_lookup_ip`.

02 Scale your analysis with batch processing. Use `batch_enrich_ips` to process hundreds of IPs in a single request, making large log file reviews feasible for the first time.

03 Pinpoint domain hosting: Need to know which websites share an IP? The `get_hosted_domains` tool runs a reverse lookup, telling you exactly what domains are tied to that address.

04 Understand organizational structure: You can use `get_whois_org` and `get_whois_net` to trace ownership back to the core corporation or network owner, bypassing simple domain checks.

05 Verify infrastructure boundaries: When planning a new service, use `get_ranges` to find all official IP ranges associated with a key domain, ensuring you don't overlap resources.

Real-World Applications

Investigating suspicious web traffic

A security analyst gets an unusual IP address from a firewall log. Instead of running three separate manual checks (GeoIP service, WHOIS lookup, ASN check), they ask their agent to use `get_lookup_ip` and `get_whois_org`. The resulting data immediately flags the location as suspicious and identifies the corporate owner.

Analyzing API usage logs

A data analyst receives a massive log file of user IP addresses. They feed this list to their agent, which uses `batch_enrich_ips` to instantly map every single entry to a country and carrier detail. This allows them to build accurate regional revenue models.

Debugging domain conflicts

A DevOps engineer finds an IP address used by multiple, unrelated services. They ask the agent to use `get_hosted_domains`. The MCP instantly lists every single domain name that has ever been associated with that problematic IP.

Validating network boundaries

A team setting up a new internal service needs to know if their chosen IP range is already in use by another major entity. They run `get_ranges` against the target domain, confirming which specific blocks of IPs are legally associated with it.

Patterns to Avoid

Treating this like a simple geolocation tool

✗ AVOID

Assuming that just knowing the city and country is enough to solve ownership disputes or understand network topology.

✓ INSTEAD

Always go deeper. Use `get_whois_net` if you need the full block owner, not just the point-of-sale location. Supplement basic lookups with `get_enterprise_ip` for advanced flags.

Processing IPs one by one

✗ AVOID

Having to run a separate lookup query every time you find a new IP address in a massive dataset, which takes hours.

✓ INSTEAD

Use `batch_enrich_ips`. This tool handles the high volume. Feed your agent the whole list up front and get all data back in one optimized call.

Assuming WHOIS is enough

✗ AVOID

Relying solely on basic domain registration info when investigating a network, missing key details about the actual infrastructure owner.

✓ INSTEAD

Always cross-reference with `get_whois_org` to get corporate records and check network boundaries using `get_whois_net`. This gives you the full picture.

The Right Fit

Use this MCP if your work involves correlating IP addresses with identity, ownership, or geography. You need to answer questions like 'Who owns this block of IPs?' or 'Where exactly did this traffic originate?'. If you primarily deal with simple website content generation or basic text transformation, then this is overkill. Don't use it if all you need is a list of domain names; check for that first. But if those domains belong to an IP address, you must use `get_hosted_domains` to connect the dots. If your goal is purely tracking user behavior over time without needing ownership data, consider a simple web analytics tool instead.

The tedious process of investigating unknown IPs today

Right now, when you see an IP in a log file that looks suspicious, your process is manual. You copy the address into one database to check the city; then you open another site to look up the ASN number; finally, you run yet a third search just to find out who owns the organization. This involves switching tabs, copying data fragments, and piecing together context piece by agonizing piece.

With this MCP, your agent handles all of that in one step. You give it the IP, and it runs the full suite of checks—location, ownership, network details—and hands you a single, cohesive intelligence report. You get immediate answers without leaving your workflow.

Getting deep visibility with IPinfo MCP

The biggest time sinks disappear: no more bouncing between GeoIP services and public WHOIS sites. No more copying data into spreadsheets to count how many IPs share a common network block. You simply ask the question, specifying whether you need `get_whois_org` or `get_whois_net`, and it delivers.

The result is reliable, comprehensive intelligence delivered directly where you're working. It changes investigation from a multi-hour archaeological dig into an instant data query.

IPinfo Alternative: 10 Tools Available

These specialized tools let your agent perform deep dives into IP intelligence, covering everything from basic geolocation to complex organization and network ownership lookups.

#	TOOL	DESCRIPTION
01	`get_asn`	Retrieves details about a specific Autonomous System (ASN) using its number or prefix.
02	`batch_enrich_ips`	Enriches and pulls detailed intelligence for up to 1,000 IP addresses at once.
03	`get_hosted_domains`	Lists specific domains that are known to be hosted on a particular IP address.
04	`get_enterprise_ip`	Retrieves advanced, enterprise-level intelligence data for an IP address.
05	`get_lite_ip`	Fetches basic geographic and network details for a standard IP address lookup.
06	`get_lookup_ip`	Performs comprehensive core IP lookups, providing detailed location and carrier information.
07	`get_ranges`	Finds all associated IP ranges linked back to a specific domain name.
08	`get_whois_net`	Gets WHOIS data specifically for an entire network range or block of IPs.
09	`get_whois_org`	Retrieves official WHOIS records detailing the owning organization associated with an IP.
10	`get_whois_poc`	Fetches WHOIS data focused on a specific point of contact for an IP address.

See It in Action

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

U Lookup the location and carrier details for IP 8.8.8.8.

I've retrieved the data for 8.8.8.8 using `get_lookup_ip`. It is located in Mountain View, California, United States. The carrier is Google LLC and it is associated with AS15169.

U What domains are currently hosted on the IP 1.1.1.1?

Using `get_hosted_domains`, I found several domains hosted on 1.1.1.1, including 'one.one.one.one', 'cloudflare-dns.com', and 'cloudflare.com'. Would you like to see more results from the next page?

U Get the IP ranges for the domain microsoft.com.

I've queried `get_ranges` for microsoft.com. I found multiple IP ranges associated with this domain, such as 20.112.52.0/24 and 20.103.85.0/24. These belong to Microsoft Corporation (AS8075).

Frequently Asked Questions

01 **How does the IPinfo MCP handle large numbers of IPs?**

It uses the `batch_enrich_ips` tool. This allows you to send up to 1,000 IP addresses in a single request, making it highly efficient for analyzing massive log files.

02 **What is the difference between `get_whois_net` and `get_whois_org`?**

`get_whois_net` provides details about an entire network range, showing who controls the block of IPs. `get_whois_org` focuses specifically on the corporate or organizational owner.

03 **Can I find out what domains are using a specific IP?**

Yes, use the `get_hosted_domains` tool. This performs a reverse lookup to list every domain name that has been associated with that particular IP address.

04 **Is this MCP useful for general traffic analysis?**

Absolutely. You can enrich user logs using `get_lookup_ip` to map raw IPs to precise geographic details, which is crucial for accurate regional pattern recognition.

05 **Does IPinfo help verify network ranges?**

Yes, the `get_ranges` tool finds all official and associated IP ranges linked to a given domain name, helping you confirm infrastructure boundaries.

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 `"ipinfo-alternative": { "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

IPinfo 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 IPinfo. 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	IPinfo MCP
Server ID	`019e38af-c3da-7254-b9bb-19afc7b59444`
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/ipinfo-alternative.