MCP SERVER | NO CODE | CLOUD HOSTED

Censys MCP for AI Agents

Map Internet Attack Surface and Discover Exposed Services

Censys allows your AI agent to explore the world's largest internet scanning platform. You can discover exposed services, analyze SSL certificates, and map an organization's full attack surface by querying internet-facing hosts, ports, and infrastructure changes.

A+ Quality Score 98.33/100

internet-scanning | attack-surface | ssl-certificates | threat-intelligence | network-security | ip-lookup

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

SCAN TO VIEW

The connectivity layer between AI and the world's software.

Vinkius sits between AI and every application. All communication passes through Vinkius Cloud via the Model Context Protocol (MCP) — with governance, observability, and security at every layer.

Your AI Connections Run Through Vinkius Cloud

The world's largest managed MCP catalog

Vinkius is the connectivity layer where AI connects 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.

Censys MCP

9 tools available
Cloud-hosted on Vinkius

This MCP gives your AI client access to deep network intelligence, allowing you to investigate what parts of the internet are visible to an attacker. Instead of manually checking dozens of dashboards or running multiple CLI commands, you can ask your agent to look at a target IP address and get all the data in one go—open ports, services running there, OS detection, and even who issued any associated certificates.

For example, if you suspect a misconfigured web server, you can use this MCP to search for hosts running specific services, like finding every machine using an Nginx banner across different countries. It's powerful data mapping. If you subscribe through Vinkius, your agent gets access to the entire catalog of specialized tools, making it easy to correlate host findings with certificate details or check historical changes over time. It turns raw internet scan data into actionable intelligence for security teams.

Core Capabilities

01 — Map and search exposed hosts

Search the entire internet-facing landscape by service, port number, operating system, or geographical location.

02 — Analyze host details and history

Retrieve detailed information on any IP address, including all open ports, services, certificates, and a timeline of how the host's profile has changed.

03 — Investigate SSL/TLS certificates

Find specific certificate details by fingerprint or search for expiring certificates issued by certain authorities.

04 — Correlate infrastructure data

Compare two different hosts to pinpoint exactly what services, ports, or OS features have changed between them.

05 — Analyze service distributions

Group search results by fields like country or autonomous system name to understand the overall distribution of exposed infrastructure.

One Click on Vinkius — From Prompt to Execution

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

01 First, subscribe to this MCP and provide your Censys API ID and Secret credentials.

02 Next, direct your AI client to perform an inquiry—for instance, asking it to find all hosts running a specific service port in a certain region.

03 The tool returns structured data detailing the open ports, services, certificates, or historical records for the requested IP range.

The bottom line is that you get automated access to massive-scale network scan data without needing to run the complex queries yourself.

Built For

Security researchers, threat hunters, and systems administrators rely on this MCP. If your job requires understanding what infrastructure is visible or exposed on the public internet, this tool saves hours of manual investigation.

Security Researcher

Uses the MCP to discover unknown vulnerabilities, map an opponent's attack surface, and track certificate usage across multiple domains.

Sysadmin / Infrastructure Engineer

Monitors their organization's external exposure by comparing current host data against baseline profiles to catch misconfigurations.

Threat Hunter

Tracks related infrastructure and identifies suspicious hosts or unusual certificate patterns that signal potential breaches.

What Changes When You Connect

01 Identify infrastructure changes: Use `view_host_diff` to instantly compare two hosts and pinpoint exactly what services or ports have been added or removed.

02 Deep dive on IPs: The `get_host` tool pulls everything—OS, open ports, banners, certificates—for a single IP in one request.

03 Certificate tracking: Never miss an expired credential. Use `search_certificates` to find all SSL/TLS certs issued by specific authorities or nearing expiration.

04 Historical view: Need to know if a host was compromised last month? Run `get_host_history` to see the full timeline of service changes for any IP.

05 Broad pattern analysis: Use `aggregate_hosts` to analyze large datasets, grouping results by country or ASN to understand global exposure trends.

Real-World Applications

Checking a competitor's public footprint

A security researcher wants to know if a rival company is using any old certificates. They run `search_certificates` for specific issuers and then use `get_certificate_hosts` to find every domain attached to those credentials, mapping out the full infrastructure.

Monitoring internal network drift

A sysadmin runs a scan on two IPs: one from last year and one today. By using `view_host_diff`, they quickly see that three critical ports were opened unexpectedly, signaling a possible misconfiguration or breach.

Assessing general network risk

A threat hunter needs to gauge the global prevalence of a specific service. They use `search_hosts` for 'ftp' and then run `aggregate_hosts` by country, instantly creating a map showing which countries have the highest concentration of exposed FTP services.

Vetting a target system

A penetration tester gets an IP address. They use `get_host` to gather all foundational data—OS, ports, certificates—and then run `get_account_info` to ensure they have enough quota for the deep dive.

Patterns to Avoid

Assuming a simple IP lookup is enough

✗ AVOID

A user only runs basic port scans on an IP, assuming that's all the data they need to assess risk.

✓ INSTEAD

Don't stop at ports. Use `get_host` for comprehensive details and run `get_certificate_hosts` to find every domain associated with any found certificate.

Ignoring historical context

✗ AVOID

A team notices a suspicious port today but doesn't know if it was always there or if it's brand new.

✓ INSTEAD

Always use `get_host_history` to check the full timeline. This shows whether the service is a persistent feature or a recent, potentially unauthorized change.

Missing certificate correlation

✗ AVOID

A user finds a suspicious domain name but doesn't know which IPs are actually using its associated certificates.

✓ INSTEAD

Use `search_certificates` to find the cert details, then run `get_certificate_hosts` to map out every IP that is presenting that specific certificate.

The Right Fit

Use this MCP if your goal is mapping external network exposure or tracking infrastructure drift. You need visibility into what services and certificates are publicly visible across the internet, regardless of whether you own those assets. If you only need to check a single website for current uptime status, a standard HTTP ping tool works fine. But if you want to know *every* possible way that site is reachable—checking its history, every associated IP, or all related certificates—then this MCP is required. Don't use it just because you think an 'AI agent' can check things; use it because the data volume and complexity (like correlating hosts via `get_certificate_hosts`) requires this specialized intelligence.

Censys MCP for AI Agents: Mapping Internet Attack Surface

Manually assessing an organization's attack surface is a nightmare. You have to run separate scans for IPs, check historical changes in port configurations, and then use different tools just to map out who owns the certificates. It’s copy-pasting IP ranges into one dashboard, running another scan for every single service banner, and spending hours trying to connect all those disparate data points.

With this MCP, your agent handles the whole picture. You ask it to investigate a target range, and it automatically gathers live host details, finds associated certificates, and maps out any infrastructure changes using tools like `view_host_diff`. The result is one cohesive intelligence report.

Censys MCP for AI Agents: Analyzing SSL/TLS Certificate Intelligence

Tracking certificates used by an entire fleet of servers requires multiple steps. You first have to search manually using criteria like expiration dates or issuers, then take the resulting certificate fingerprint and run it through a separate tool just to get the list of hosts that use it.

Now you can ask your agent once to find all certs issued by 'Let's Encrypt' expiring in the next 30 days. It automatically collects the details using `search_certificates` and then maps every single host using those credentials via `get_certificate_hosts`. The visibility is total.

9 Tools in Censys MCP for Network Security Analysis

Use these tools to query, compare, and aggregate network data across millions of exposed hosts and certificates.

#	TOOL	DESCRIPTION
01	aggregate_hosts	Groups search results by fields like country or port to calculate counts, showing the distribution of exposed services or infrastructure types.
02	get_account_info	Checks your remaining API quota and account limits so you know when you need to top up your access.
03	get_certificate	Pulls all detailed data for a specific certificate, including its issuer, validity period, key information, and extensions.
04	get_certificate_hosts	Finds every host (IP address) that is using a particular SSL/TLS certificate, detailing the ports and timestamps.
05	get_host	Gets all open ports, service banner text, TLS certificates, OS detection, and location data for one specific IP address.
06	get_host_history	Shows a timeline of how an IP's services, ports, and certificates have changed over time, marking all observed modifications.
07	search_certificates	Searches for SSL/TLS certificates using criteria like issuer names, subject fields, or specific validity dates.
08	search_hosts	Performs powerful searches on internet-connected hosts using services (e.g., 'ssh'), ports, OS types, or geographic locations.
09	view_host_diff	Compares two different IP addresses to highlight infrastructure differences, making it easy to spot what changed between them.

See It in Action

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

U Find all exposed SSH servers in Germany.

DE Exposed Infrastructure Report

We found **3,120** hosts running SSH (Port 22) in the DE region.

- **Top OS:** Linux (Ubuntu/CentOS)
- **Common ASNs:** AS64512 (Deutsche Telekom), AS7019 (Vodafone).
- **Key Findings:** Several hosts are running outdated SSH protocols. We recommend checking the `get_host_history` for specific IP ranges to confirm if these ports were opened recently.

U Show me all certificates issued by DigiCert expiring this quarter.

🔍 **Certificate Expiry Alert: Q3 2026**

Found **1,542+** certificates matching the criteria. Key details:

ISSUER	EXPIRATION DATE RANGE	COMMON SUBJECT DOMAINS
DigiCert Inc	Jul - Sep 2026	

.com, .net, banking.

*Most certificates use RSA 4096-bit keys. Check the `get_certificate` tool for full parsing details on any specific fingerprint.

U Compare these two IPs and tell me what changed.

Host Comparison: IP A vs IP B

The following infrastructure changes were detected:

- ✅ **New Service:** IP B opened port 8080 (HTTP Alternate) which was closed on IP A.
- ❌ **Removed Feature:** IP A had a specific TLS banner that is missing from IP B.
- 🌐 **Location Change:** The ASN associated with IP B has changed since the last scan.

Use `view_host_diff` to track these subtle but critical changes in your infrastructure.

Frequently Asked Questions

01 **How can Censys MCP help me map my network's attack surface?**

It lets you search the entire internet for exposed services and ports without needing to be physically connected. You can use your agent to find every publicly visible credential or service running on a target IP.

02 **Does Censys MCP track changes over time?**

Yes, it tracks host history. It shows you if an open port or a service banner was added recently, allowing you to detect potential misconfigurations that happened after the fact.

03 **What kind of certificate information can I get with Censys MCP?**

You can find detailed data on certificates, including who issued them, when they expire, and critically, every single IP address or domain name using that specific certificate.

04 **Is this better than running manual network scans?**

It's more comprehensive. It automates the correlation of data points—linking a port finding to its associated certificate and then tracking its history—in one workflow, saving massive amounts of time.

05 **Can Censys MCP help me find similar infrastructure?**

Absolutely. You can compare two different IP addresses using the tool to spot differences in open services or OS types, which is helpful when auditing related systems.

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 `"censys": { "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

Censys 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 Censys. 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	Censys MCP
Server ID	`019d8423-ccbd-70e6-b47d-f5bc2ae859d4`
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/censys.