MCP SERVER | NO CODE | CLOUD HOSTED

Shodan MCP

Map exposed services and scan global assets.

Shodan MCP connects your AI client directly to Shodan's massive database of internet-connected devices. Use it to scan for exposed services, analyze network ports, and discover vulnerabilities across the global IoT landscape. Get detailed reports on specific IP addresses or search by OS, product, or country.

A+ Quality Score 100/100

cybersecurity | network-scanning | threat-intelligence | open-ports | banner-grabbing | attack-surface

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

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.

Shodan MCP

10 tools available
Cloud-hosted on Vinkius

This MCP lets you treat the entire internet like a searchable database. Instead of running separate tools—one for DNS lookups, another for checking banners, and yet another for finding open ports—you just ask your AI client. It handles connecting to Shodan's search engine automatically.

Need to check what services are exposed by an IP address? You can get a full breakdown: open ports, running hostnames, geographic location, and operating system details. Want to track down specific types of devices? You can filter searches by product name like 'nginx' or OS type like 'Windows'. Even if you just want to know your own external IP for firewall rules, the MCP handles that query instantly. Because Vinkius hosts this Shodan MCP, all these advanced networking tools are available in one place, letting you run complex network investigations without switching catalogs.

Core Capabilities

01 — Search for Exposed Devices

You can search across the internet using filters like country code, product name, or specific operating system.

02 — Get Detailed Host Info

Fetch a complete report on any IP address, including all open ports, banners, and associated vulnerability data.

03 — Resolve Hostnames to IPs

Translate one or more domain names into their corresponding numeric IP addresses.

04 — Check Usage Limits

Run a check to monitor your remaining query credits and API plan status for the Shodan service.

One Click on Vinkius — From Prompt to Execution

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

01 First, subscribe to this MCP in Vinkius and enter your unique Shodan API Key into your AI client.

02 Next, tell your agent exactly what you're looking for—for example, 'Find all open SSH ports running Debian in Germany.'

03 The system runs the query through Shodan and returns structured data showing matching IPs, services, and relevant vulnerability details.

The bottom line is that this MCP lets you run advanced network discovery queries using simple, natural language prompts.

Built For

This is for the security researcher who needs to map an entire attack surface in minutes. It's for the sysadmin tired of manually checking firewall rules and port lists. Use it if you deal with infrastructure exposure or threat intelligence daily.

Security Researcher

Runs targeted searches to discover forgotten or exposed services, mapping potential vulnerabilities across target networks.

System Administrator (Sysadmin)

Monitors the organization's external footprint, checking for misconfigured open ports or unusual service banners on public IPs.

IoT Analyst

Identifies trends and device distribution patterns by searching specific product types (e.g., smart cameras) across national boundaries.

What Changes When You Connect

01 You stop guessing what's out there. By running a search query, you can find specific devices by product (e.g., 'apache') or vulnerability ID, allowing precise threat hunting.

02 No more single-point checks. You get a comprehensive report on any IP address—open ports, location, OS, and service banners—all in one data dump using the detailed host info tool.

03 Quickly check your own network boundaries with get_my_ip to confirm what external services are visible to the outside world. This is great for compliance checks.

04 Save time on reconnaissance. Instead of running multiple manual lookups, you use dns_resolve or reverse_dns to map out an entire domain's infrastructure instantly.

05 Know your limits before you start. Use get_account_info to monitor usage credits and ensure your AI client doesn't fail halfway through a major scan.

Real-World Applications

Mapping a Target Company's Infrastructure

A security analyst needs to understand all internet-facing assets for a new client. They prompt their agent to 'Search for open ports across the target company's IP range, filtering by country and OS.' The agent uses search_hosts to return hundreds of potential entry points, which are then refined using get_host_info.

Investigating a Suspicious Domain

A team noticed an odd domain name. They first use dns_resolve to confirm the IP address, and then immediately run reverse_dns on that IP to see if any other hostnames are associated with it. This quickly builds a picture of potential ownership.

Auditing Internal Exposure

A sysadmin wants to know which services their own network exposes inadvertently. They run get_my_ip and then use that IP for a detailed host info check, identifying misconfigured ports or unneeded banners.

Analyzing IoT Device Trends

An IoT analyst needs to see how many 'Nest' cameras are exposed in specific regions. They run search_hosts using the product filter and limit by a country code, giving them actionable data on device distribution.

Patterns to Avoid

Thinking of it as a simple IP checker

✗ AVOID

Just typing 'what is 8.8.8.8' and expecting one clean answer.

✓ INSTEAD

You need to be specific. Use get_host_info for the full picture, or use reverse_dns if you suspect multiple hostnames are linked to that IP.

Forgetting credentials

✗ AVOID

Running a complex query and getting an 'API Limit Exceeded' error mid-process.

✓ INSTEAD

Always start by running get_account_info. This confirms your credit balance before you commit to a long, resource-heavy search.

Confusing location data

✗ AVOID

Assuming the geographic location returned is the physical site owner's address.

✓ INSTEAD

Remember that location data comes from network records. To check for specific services, use get_facets to see available filters before constructing your search.

The Right Fit

Use this MCP if your goal is deep, structured reconnaissance of internet-facing infrastructure or open ports. You need to map what's physically or digitally exposed on the public internet—that's its core function. It excels at answering 'What services are available here?' and 'How many devices match these criteria?'. Don't use this if you just want simple information, like finding a single URL; for that, your standard web search is fine. If your goal is purely to check firewall rules on a private network segment (e.g., 192.168.x.x), Shodan won't help because it only scans the public internet. For internal asset management, you need an internal monitoring tool instead.

The Network Blind Spot

Today, figuring out what a target organization or even your own network is exposing feels like clicking through three different dashboards: one for DNS records, another for open ports, and a third for known vulnerabilities. You're constantly copy-pasting IPs from one tool into the next just to piece together a full picture of their attack surface.

With this MCP, you skip all that manual work. Your agent runs complex queries against Shodan's massive index. Instead of fragmented data points, you get a single, structured report detailing every open port, banner grab, and associated vulnerability across the entire internet.

Shodan MCP: Full Asset Discovery

You no longer need to manually run separate lookups for hostnames, IP addresses, or ports. The capability to perform a broad search using powerful filters—like product name and country code—and then follow up with get_host_info means you can map the entire digital footprint in minutes.

It's about depth over breadth. You go from simply knowing an IP exists to understanding exactly what services are running on every open port, right down to the specific banner version.

Shodan With 10 Tools

These tools let you perform every kind of advanced network investigation, from simple IP lookups to deep vulnerability analysis.

#	TOOL	DESCRIPTION
01	`get_account_info`	Checks your current Shodan account limits, showing remaining usage credits for the service.
02	`get_api_info`	Retrieves specific details about your API plan and associated billing information.
03	`dns_resolve`	Converts a list of domain names (hostnames) into their corresponding IP addresses.
04	`get_facets`	Lists available search filters and groupings, helping you build complex query logic like grouping by country or OS.
05	`get_host_info`	Pulls all open port data, hostnames, location, and service banners for a single IP address.
06	`get_host_count`	Estimates the total number of results that would match a specific search query before running the full scan.
07	`get_my_ip`	Identifies and returns your current public, external IP address for network documentation.
08	`get_ports`	Provides a definitive list of all ports that Shodan actively scans and monitors across the internet.
09	`reverse_dns`	Converts known IP addresses back into their associated domain names (hostnames).
10	`search_hosts`	Conducts a broad search across the internet using powerful filters like product, vulnerability ID, or country code.

See It in Action

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

U Search for nginx servers in Brazil.

Found 125,000+ nginx servers in Brazil. Top results show servers in São Paulo, Rio de Janeiro and Brasília running nginx versions 1.18 through 1.25. Common ports: 80, 443, 8080.

U Look up info for IP 8.8.8.8.

8.8.8.8 (Google Public DNS): Located in Mountain View, CA, US. Organization: Google LLC. Open ports: 53 (DNS), 443 (HTTPS). Services: DNS server, DoH (DNS over HTTPS). Hostnames: dns.google.

U Resolve google.com and github.com to IPs.

DNS resolution: google.com → 142.250.189.14, github.com → 140.82.121.4. Use get_host_info for detailed information on any IP address.

Frequently Asked Questions

01 **How does Shodan MCP help me find vulnerabilities?**

It helps by allowing you to search for devices using vulnerability identifiers (vuln:CVE-...) and then retrieving detailed host info that includes known service banners.

02 **Can I use the Shodan MCP to check my own IP address?**

Yes. Use get_my_ip to confirm your current public IP, which is useful for documenting firewall rules and access control lists.

03 **What if I only have a list of domain names? How do I start the scan?**

Start with dns_resolve. This tool takes your comma-separated hostnames and converts them into IP addresses, which you can then use for reverse_dns or get_host_info.

04 **Is this MCP better than running a traditional port scanner?**

Yes, because it uses Shodan's index of millions of devices. It gives you global visibility across the internet, not just what your local machine can reach.

05 **How do I check my usage credits with Shodan MCP?**

Use get_account_info to run a quick check on your remaining query credits and API plan details before launching any major search operation.

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 `"shodan": { "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

Shodan 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 Shodan. 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	Shodan MCP
Server ID	`019d847f-6a5c-70fc-8e08-4f93c4dffb3c`
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/shodan.