MCP SERVER | NO CODE | CLOUD HOSTED

Patchstack Security MCP

Audit WP/PHP vulnerabilities across all your sites.

Patchstack Security monitors WordPress and PHP installations for vulnerabilities and compliance issues. This MCP lets your AI agent check site software health across dozens of sites, track known CVEs in plugins/themes, and retrieve real-time security alerts from a single chat window.

A+ Quality Score 100/100

wordpress-security | vulnerability-tracking | plugin-security | threat-intelligence | patch-management

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

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.

Patchstack Security MCP

9 tools available
Cloud-hosted on Vinkius

Using this MCP, you can manage the entire security posture of your WordPress sites without logging into a dozen dashboards. Your AI client directs your agent to monitor all connected sites, providing an instant security overview that pinpoints outdated plugins or themes. Need to know if 'Contact Form 7' has any recent CVEs? Just ask. You can search massive databases for known vulnerabilities in specific components and even check the latest active firewall alerts. If you're running a large agency or managing client sites, this MCP consolidates site auditing, vulnerability tracking, and patch management into one conversation stream. It gives you immediate visibility into which sites are secure and which need attention.

Core Capabilities

01 — Audit Site Software Inventory

Retrieves a comprehensive list of all installed plugins, themes, and core software versions across your monitored accounts.

02 — Search Vulnerability Databases

Queries the Patchstack database to find known vulnerabilities for specific components or general WordPress parts.

03 — Review Security Status Across Sites

Gets a high-level security score and software overview for every site you manage, allowing quick risk assessment.

04 — Check Live Threat Alerts

Pulls the most recent security alerts and triggered firewall rules to confirm if an attack is happening right now.

05 — Examine Vulnerability Details

Retrieves deep technical information about a specific vulnerability, including recommended fixes or affected versions.

One Click on Vinkius — From Prompt to Execution

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

01 Subscribe to this MCP and provide your unique Patchstack User Token.

02 Connect your AI client using the token. Your agent can now access all site monitoring data.

03 Ask a natural language question, like 'What are the latest alerts for my dev site?' and get instant security answers.

The bottom line is that you talk to your agent, and it translates complex WordPress security data into simple, actionable text.

Built For

Anyone responsible for maintaining multiple live websites—especially agencies or enterprise developers. You're the person staring at 30+ client dashboards trying to figure out which one is actually failing and why.

Agency Owner

You oversee dozens of clients, needing to quickly run a report on all sites for outdated plugins or critical vulnerabilities without manually checking each dashboard.

WordPress Developer

You need to audit site components and check the latest vulnerability data against your local development environment before pushing code live.

Security Researcher

You require access to deep, structured threat intelligence—like querying specific component vulnerabilities or listing all monitored sites for a compliance report.

What Changes When You Connect

01 Consolidated Site Auditing: Instead of opening dozens of client dashboards, you can use the `list_sites` tool to get a single security score overview for every site, instantly flagging risks and poor compliance scores.

02 Deep Vulnerability Research: Need technical proof? Use `search_vulnerabilities` or `get_component_vulnerabilities` to query massive databases directly. You get immediate details on CVEs that would take hours of manual searching.

03 Real-Time Threat Response: Don't wait for an alert email. With `get_latest_alerts`, your agent pulls the latest security events and triggered firewall rules immediately, giving you a live view of threats.

04 Proactive Patch Management: Review settings using `get_autoupdate_settings` to confirm if patches are running automatically. You can also use `get_software_overview` to see exactly which components need updating across the board.

05 Targeted Deep Dives: If a search is too broad, you can narrow it down. Use `get_vulnerability_details` on a specific ID or CVE number for the precise technical info needed by a developer.

Real-World Applications

Pre-Sale Client Health Check

A prospective client asks if their current WordPress installation is secure. You use your agent to run `get_software_overview` across their main site, retrieving a single report that confirms the software versions and highlights any critical outdated components.

Responding to a Breach Report

A client reports suspicious activity. Your agent immediately runs `get_latest_alerts` and cross-references it with `get_site_software` on the affected site, giving you instant confirmation of what was hit and when.

Routine Agency Compliance Audit

It's month-end. You use your agent to run `list_sites`, checking every client for security scores below 90. Then, for the lowest scoring ones, you use `get_component_vulnerabilities` to find the exact offending plugin.

Development Environment Testing

Before merging a new theme, a developer uses your agent with `search_vulnerabilities`. They query the database using the theme's dependencies to ensure no known CVEs exist in the code they are about to ship.

Patterns to Avoid

Treating it like a generic bug tracker

✗ AVOID

Asking the agent, 'Did my site break?' and waiting for vague answers. The AI will just list what it sees without context.

✓ INSTEAD

Don't ask if something broke. Ask specific questions using the tools: 'Check `get_latest_alerts` on Site X.' or 'What are the known vulnerabilities for this plugin? Use `get_component_vulnerabilities`.'

Forgetting multi-site scope

✗ AVOID

Running a single manual check on one site, only to realize you have 40 other sites with similar issues.

✓ INSTEAD

Always start by running `get_software_overview` or `list_sites`. This confirms the overall health of your entire portfolio before diving into individual component checks.

Confusing alerts with vulnerabilities

✗ AVOID

Assuming that because an alert fired, it means a vulnerability exists. Alerts are just signs something happened.

✓ INSTEAD

If you see an alert from `get_latest_alerts`, follow up by using `get_vulnerability_details` to understand the underlying threat and whether a patch is available.

The Right Fit

Use this MCP if your primary job involves managing compliance, security posture, or software inventory across multiple WordPress sites. If you need to know 'What's wrong with Site X?' or 'Is Component Y vulnerable?', this is the right tool. Don't use it if you just need simple content updates; that's a CMS task. Also, don't rely on it for debugging PHP code logic—it checks version numbers and known flaws, not custom runtime errors. If your goal is purely to manage user accounts or payment systems, you should look at dedicated user management or billing connectors instead.

Security Audits Used To Be a Dashboard Nightmare

Today, checking the security of an agency's client portfolio means logging into dozens of separate dashboards. You click through site lists, open individual reports, copy vulnerability IDs, and cross-reference them with external databases just to build one single status report. It takes half a day, minimum.

With this MCP, you tell your agent exactly what you need—like 'Give me an overview of all sites that are running outdated plugins.' The agent runs the necessary checks and gives you an immediate, consolidated list of every site needing attention. You get instant intelligence.

Patchstack Security Gives You Full Visibility

You don't have to manually check if a core component has been compromised or what the latest CVEs are. Instead of copy-pasting version numbers into search engines, you simply ask your agent to run `get_component_vulnerabilities` for that specific plugin.

Your security workflow changes from tedious data gathering to direct conversation. You get immediate answers and a complete audit trail without leaving your chat interface.

Patchstack Security: 9 Tools

Use these nine tools to query specific data points about your sites, including vulnerability details, component inventories, and live security alerts.

#	TOOL	DESCRIPTION
01	`get_autoupdate_settings`	Retrieves the current settings that govern automatic security patching of vulnerable components.
02	`get_component_vulnerabilities`	Fetches all known vulnerabilities associated with a specific software component or library version.
03	`get_latest_alerts`	Pulls the most recent security alerts and any firewall rules that were recently triggered.
04	`get_latest_vulnerabilities`	Gathers a list of the newest vulnerabilities added to the Patchstack threat database.
05	`get_site_software`	Gets a complete inventory list of all software installed on one specific monitored site.
06	`get_software_overview`	Provides a broad security overview, summarizing the health and software status across all your connected sites.
07	`get_vulnerability_details`	Delivers detailed technical information for any specific vulnerability you name or reference.
08	`list_sites`	Retrieves a comprehensive list and security score summary of every site Patchstack is monitoring.
09	`search_vulnerabilities`	Allows you to execute a targeted search query against the entire vulnerability database for specific keywords or CVEs.

See It in Action

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

U List all my monitored sites in Patchstack.

Fetching sites... I found 3 sites: 'my-blog.com' (Score: 95), 'online-store.net' (Score: 82), and 'dev-site.io' (Score: 100). Would you like to check the software for any of them?

U Search for vulnerabilities in the 'Contact Form 7' plugin.

Searching the database... I found 5 recent vulnerabilities for 'Contact Form 7'. The most severe is an 'Arbitrary File Upload' (CVE-2023-XXXXX) fixed in version 5.7.3. I recommend updating all instances immediately.

Frequently Asked Questions

01 **How do I see the overall health of all my WordPress sites with Patchstack Security MCP?**

You run `get_software_overview`. This tool aggregates data from all monitored websites and gives you a single, high-level security score for your entire portfolio.

02 **Can I find out if a specific plugin has been compromised using Patchstack Security MCP?**

Yes. Use `search_vulnerabilities` or `get_component_vulnerabilities`. You can search the database by name, version, or even CVE identifier.

03 **What is the difference between alerts and vulnerabilities using Patchstack Security MCP?**

Alerts (`get_latest_alerts`) show what happened right now—like a firewall rule being triggered. Vulnerabilities (found via `search_vulnerabilities`) are weaknesses that *could* be exploited.

04 Does Patchstack Security MCP help me manage automatic updates?

It helps by checking your current settings with `get_autoupdate_settings`. You can confirm if automatic patching is enabled and what components are covered.

05 Is this better than just using the Patchstack dashboard?

Using this MCP lets you talk to the data. Instead of navigating menus, you ask natural questions like 'List all sites with a score under 80,' and get an instant report.

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 `"patchstack-security": { "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

Patchstack Security 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 Patchstack Security. 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	Patchstack Security MCP
Server ID	`019d846a-52c5-709d-94d0-8730a840bd1a`
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/patchstack-security.