MCP SERVER | NO CODE | CLOUD HOSTED

Rapid7 InsightVM MCP

Query Assets & Validate Vulnerabilities Instantly

Rapid7 InsightVM MCP connects your AI client directly to a major vulnerability assessment platform. It lets you query detailed asset inventories, check for specific vulnerabilities (like CVEs), track historical scan results, and even force immediate scans on network sites—all from one chat window or IDE. You get real-time security intelligence without having to jump between multiple dashboards.

A+ Quality Score 98.33/100

cybersecurity | threat-remediation | risk-management | network-scanning | asset-inventory | security-audit

MAINTAINED BY VINKIUS CLOUD FOR AI AGENTS · JUNE 2026
vinkius.com/mcp/rapid7-insightvm

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.

Rapid7 InsightVM MCP

10 tools available
Cloud-hosted on Vinkius

This MCP makes your AI client a full cybersecurity assistant that operates directly within the Rapid7 InsightVM platform. Instead of logging into separate consoles, you ask questions about your network assets and get answers instantly. For instance, you can ask what vulnerabilities are active on a specific machine or check if a patch deployment worked by triggering an immediate scan. The tool's first function allows you to retrieve complete inventory lists, telling you everything about every piece of hardware and software running in your environment. You can also review detailed vulnerability reports, seeing which CVE numbers apply and how to fix them. If you need to manage sites, you can view all configured network locations or initiate a fresh assessment on a subnet after making changes. Since Vinkius hosts this MCP, your agent gets access to this entire suite of security tools through one single connection point.

Core Capabilities

01 — Inventory Network Assets

You can retrieve full details for every tracked computing asset, including its operating system and hardware type.

02 — Check Asset Vulnerabilities

The MCP lists all known vulnerabilities found on a single machine, providing associated advisories and fixes.

03 — Review Scan History

You can view assessment scans chronologically to track their execution status and results without switching windows.

04 — Manage Network Sites

It lets you explore configured network sites, checking their scope and overall risk level.

05 — Force New Scans

You can trigger an immediate re-evaluation scan on a specific site to validate security fixes.

One Click on Vinkius — From Prompt to Execution

Available at **vinkius.com/mcp/rapid7-insightvm** — connect your AI agent in three steps.

01 First, you authorize this MCP within your preferred environment. You'll need to provide the URL and port for your Rapid7 Security Console, plus dedicated credentials configured for Basic Authentication.

02 Next, you chat with your AI agent and ask a question about your domain servers or network status. Your agent sends an API call through this connection.

03 Finally, the MCP processes the request using InsightVM's data and returns a concise, actionable report directly to you in your workspace.

The bottom line is that you get deep security visibility without leaving the application you're already working in.

Built For

This MCP is for security professionals who spend too much time manually switching between dashboards to correlate asset data with vulnerability findings. It's perfect for the SOC analyst who needs immediate threat intelligence or the SysAdmin who has to verify a patch deployment across multiple subnets.

Cybersecurity Analyst (SOC)

Analyzing identified security flaws and fetching CVE details plus remediation steps without leaving their incident response platform.

DevOps Engineer

Quickly ordering a vulnerability assessment on a subnet after applying OS updates to confirm the threat is successfully patched.

Network Engineer

Evaluating site configurations directly when setting up new subnets to ensure full scanning coverage.

What Changes When You Connect

01 Stop switching between tabs to check security status. Using the `list_assets` command, your agent builds a complete picture of every machine you own in one go.

02 Need to know what's wrong with a specific host? Use `get_asset_vulnerabilities`. This instantly shows all associated CVE numbers and tells you exactly how to patch them up.

03 Don't trust old reports. If you patched something, use the `trigger_scan` command. It forces InsightVM to re-evaluate that site right now, giving you proof of resolution.

04 Tracking security changes is easier than ever. You can use `list_scans` and `get_scan` to see a clear timeline of every assessment run against your environment.

05 When setting up new subnets, the MCP lets you explore configured network sites using `list_sites` and check their full scope coverage before it's too late.

Real-World Applications

Post-Patch Verification

A DevOps engineer applies a critical OS update across three subnets. Instead of waiting for the next scheduled scan, they ask their agent to run `trigger_scan` on those specific sites immediately. The agent confirms the new assessment is running and reports back when it's ready.

Incident Response Triage

The SOC analyst spots a suspicious IP address in an alert. They use `get_asset` to quickly pull up all asset data for that IP, confirming its hardware type and OS fingerprint without leaving the incident response dashboard.

Quarterly Audit Prep

A network engineer needs a full list of all sites and their current risk profiles. They ask the agent to run `list_sites` and then use `get_site` on each one, compiling all necessary data for auditors in minutes.

Understanding Vulnerability Scope

A team lead wants to know if a specific vulnerability (CVE-2023-XXXX) affects any assets. They use `list_vulnerabilities` first, then query the results against all known assets using `get_asset_vulnerabilities`.

Patterns to Avoid

Checking vulnerability status by reading screenshots.

✗ AVOID

The analyst downloads a PDF report showing 10 vulnerabilities. They then have to manually cross-reference the CVE IDs against an internal spreadsheet to determine which are critical and if they've been patched.

✓ INSTEAD

Instead, ask your agent to use `get_asset_vulnerabilities` for the specific asset in question. The result is a clean, actionable list of vulnerabilities with clear remediation guides.

Manually running scans on every site.

✗ AVOID

A network team needs to test a new subnet scope change across five different locations. They spend half a day logging into the console and manually initiating five separate scan jobs, hoping nothing fails.

✓ INSTEAD

Use `list_sites` first to verify all target sites are listed, then send one command via your agent calling `trigger_scan` for all required sites simultaneously.

Assuming asset data is up-to-date.

✗ AVOID

A sysadmin deploys a new OS patch but forgets to document the change. They rely on old reports, which show the system still running vulnerable software.

✓ INSTEAD

Always run `get_asset` for core details and follow up with `trigger_scan` immediately after any major infrastructure or software change to validate the fix.

The Right Fit

Use this MCP if your primary pain point is correlating real-time, deep technical security data (CVEs, asset OS fingerprints, scan status) with your daily workflow. You need an AI agent that acts like a super-powered console viewer for vulnerability management.

Don't use this if you just need to send messages, manage contacts,

or query simple business records. If your task involves anything outside of network security auditing—like managing tickets in a CRM or scheduling meetings—you should look at different categories of MCPs. This tool is purely for deep technical infrastructure assessment.

Dealing with Security Dashboards Is Exhausting

Today, checking your network's security posture means jumping through hoops: logging into the main console to see a high-level risk score, opening a secondary tab to pull up asset inventory details, then clicking yet another section just to get vulnerability reports for specific CVE IDs. It's tedious copy-pasting and context switching that slows down incident response.

With this MCP, you ditch the dashboard fatigue. You talk to your agent like you're talking to a teammate who actually knows the system. You simply ask: 'What are the critical vulnerabilities on asset 1052?' and get the direct answer and remediation details right where you're working.

Rapid7 InsightVM MCP: Security Data, Delivered.

Manual processes used to require running `list_assets` to build a list, then using that ID to check the vulnerability status with `get_asset_vulnerabilities`, and finally calling `trigger_scan` if anything needed fixing. This is slow, error-prone work.

Now you just tell your agent what you need—'Scan this subnet for critical vulnerabilities.' Your agent handles the entire sequence of checks in the background, giving you a single, consolidated report without any manual orchestration.

Rapid7 InsightVM: 10 Tools for Security Auditing

These tools let you perform deep security audits by querying asset details, listing vulnerability definitions, tracking scan status, and forcing new network assessments.

#	TOOL	DESCRIPTION
01	`get_asset`	Retrieves specific, detailed information for a single asset you identify.
02	`get_asset_vulnerabilities`	Lists every vulnerability found on one particular machine or host.
03	`get_scan`	Retrieves the execution status and results for a specific assessment scan run.
04	`get_site`	Retrieves all details about one designated network site.
05	`get_vulnerability`	Gets detailed information for a specific vulnerability ID number.
06	`list_assets`	Shows you an inventory list of all computing assets that have been discovered and tracked.
07	`list_scans`	Lists assessment scans in chronological order so you can see their history.
08	`list_sites`	Shows all the network sites that are configured for scanning.
09	`list_vulnerabilities`	Provides a list of global vulnerability definitions used by the system.
10	`trigger_scan`	Forces an immediate, new vulnerability scan to run for any specified site.

See It in Action

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

U Fetch the list of network sites currently managed by Rapid7.

Using the `list_sites` command, I found 3 network targets: 'London Head Office' (ID: 10), 'Cloud AWS Infrastructure' (ID: 12), and 'Guest WiFi Segment' (ID: 15).

U What vulnerabilities are discovered on asset 1052?

I queried `get_asset_vulnerabilities` for asset 1052. The host has 5 active vulnerabilities, primarily unpatched OpenSSL packages triggering high-severity CVE-2023-XXXX listings.

U Force a new scan on Site ID 15 immediately.

I submitted the `trigger_scan` command for Site ID 15. The InsightVM engine has confirmed the execution, and the scan is now running in the background. You can check its progress shortly using queries.

Frequently Asked Questions

01 **How does Rapid7 InsightVM MCP get asset data?**

This MCP connects directly to your running Rapid7 InsightVM instance. It retrieves inventory data by using the `list_assets` tool, giving you real-time visibility into tracked computing resources.

02 **Can I use Rapid7 InsightVM MCP to patch vulnerabilities?**

No, this MCP doesn't apply patches. It helps you identify them. You use `get_asset_vulnerabilities` to see the CVE details and remediation guidelines so your team knows what needs fixing.

03 Is Rapid7 InsightVM MCP better than just looking at reports?

Yes, because you aren't reading a static report. You ask specific questions about assets or sites, and the agent uses tools like `get_site` to retrieve only the exact information you need.

04 What if I change my network after using Rapid7 InsightVM MCP?

You can force a fresh check by using the `trigger_scan` tool. This command initiates an immediate scan on that site, validating your changes against current threat data.

05 Does Rapid7 InsightVM MCP show me old scans?

It does. Use the `list_scans` and `get_scan` tools to review assessment history and track the status of previous security runs for compliance purposes.

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 `"rapid7-insightvm": { "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

Rapid7 InsightVM 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 Rapid7 InsightVM. 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	Rapid7 InsightVM MCP
Server ID	`019d75fc-a3a2-7166-b411-45f93d027691`
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/rapid7-insightvm.