MCP SERVER | NO CODE | CLOUD HOSTED

Tenable MCP

Check vulnerabilities and manage assets instantly.

Tenable connects your entire vulnerability management program directly to any AI agent. You can list all assets, check deep telemetry like OS fingerprints and IPs, find specific security findings (CVEs) on individual machines, or manually launch immediate scans—all without leaving your chat window or IDE.

A+ Quality Score 100/100

cybersecurity | exposure-management | asset-intelligence | cve-triage | vulnerability-assessment | cloud-security

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

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.

Tenable MCP

10 tools available
Cloud-hosted on Vinkius

This MCP brings your Tenable enterprise environment into your conversation flow. Instead of logging into multiple dashboards to build a risk profile, you talk to your agent about it. You can list all discovered assets and immediately pull deep details on any host, including its OS fingerprint and tags. Need to know what vulnerabilities are hitting a specific machine? Just ask for the security findings, and you get them directly. If you find an asset that looks risky, you don't have to wait; you can manually trigger an immediate scan run right through your chat. This ability to execute complex checks instantly is why having this connector available on Vinkius makes a huge difference in speed.

It lets security analysts pinpoint CVE details for compromised servers in seconds. DevSecOps engineers can launch scans on newly deployed infrastructure zones directly from their code editor, and IT admins can check the health of your scanning fleet to ensure everything is running right.

Core Capabilities

01 — Inventory Assets

List all host and cloud assets discovered in your Tenable environment.

02 — Check Asset Health

Pull detailed metadata, networking info, and the risk profile for any specific asset ID.

03 — Triage Vulnerabilities

Retrieve explicit security findings or CVEs affecting a single, targeted asset.

04 — Execute Scans On Demand

Manually trigger an immediate scan run using one of your configured assessment templates.

05 — View Scan Results

Get the full runtime analytics and vulnerability summaries for a specific, completed scan job.

One Click on Vinkius — From Prompt to Execution

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

01 Subscribe to this MCP and enter your Tenable Access Key and Secret Key.

02 Tell your agent what you need. For example, 'Check the vulnerabilities for asset X' or 'Launch a scan on the new zone.'

03 The agent talks directly to Tenable, pulls the data, and presents the results in plain text right where you are working.

The bottom line is you get actionable vulnerability data from your tenable platform without ever navigating complex web dashboards.

Built For

This MCP targets security analysts and devsecops engineers who are tired of spending hours clicking through multiple dashboards just to build a basic risk report. It's for anyone whose job requires real-time, deep visibility into network vulnerabilities.

Security Analyst

Needs to instantly pull CVE details or security findings for specific compromised servers when investigating an alert.

DevSecOps Engineer

Must trigger scans on newly deployed infrastructure zones directly from their code editor or terminal workflow.

IT Administrator

Needs to audit the operational status of scanning tools and verify that host tags match the organizational network topology.

What Changes When You Connect

01 Get immediate visibility into risk. You can check a specific asset's security findings, pulling explicit CVE details without navigating complex dashboards or running manual reports.

02 Manage infrastructure from your chat. DevSecOps teams can manually trigger scans on new zones directly from their code editor, making deployment and testing faster.

03 See the whole picture of your network. You can list assets and then check detailed telemetry—OS fingerprints, IPs, tags—to understand exactly what you're protecting.

04 Know if your scanners are working. Use this MCP to audit scanner health and confirm that host tags actually match the logical network topologies before a major project starts.

05 Quickly assess scope. You can list all configured scans and scan folders (like 'PCI Quarters') to ensure you've covered every required compliance area.

Real-World Applications

Investigating an alert on a critical server

A security analyst gets an alert for Asset ID X. Instead of logging into the Tenable UI, they ask their agent to retrieve all vulnerabilities for Asset ID X. The agent immediately returns a list of 3 critical severity issues and details which plugin caused them.

Validating network segmentation

An IT administrator needs confirmation that the newly deployed staging environment is properly segmented. They use the MCP to list logical networks, compare it against the asset tags, and verify that only authorized assets exist in that segment.

Proving compliance for an audit

A team needs proof of vulnerability assessment coverage for PCI requirements. Instead of manually running reports, they ask the agent to list all scans related to 'PCI Quarters' and then retrieve the full scan results from the most recent run.

Responding to a zero-day discovery

A vulnerability is announced for a common library. The engineer asks their agent to check specific assets against this CVE using the 'get_asset_vulnerabilities' tool, getting an instant list of all affected machines across the entire fleet.

Patterns to Avoid

Manual dashboard hopping

✗ AVOID

Copying asset IDs from one dashboard, pasting them into another section to check tags, then manually triggering a scan run via a web form.

✓ INSTEAD

Start by listing assets and then asking the agent to get all details for those assets. If needed, immediately launch_scan() directly through your chat interface.

Assuming data completeness

✗ AVOID

Believing that just seeing a list of scans is enough without knowing what was actually tested or if the scanner itself is healthy.

✓ INSTEAD

First, use list_scanners() to check plugin health. Then, use get_scan_results() on a specific scan ID to confirm the actual findings.

Ignoring asset context

✗ AVOID

Running a generic vulnerability assessment without knowing if the host is in production or staging, leading to false positives.

✓ INSTEAD

Use list_asset_tags() first. Then use get_asset_details() on that specific asset ID before deciding which scan run to launch.

The Right Fit

Use this MCP if your workflow demands deep, immediate data retrieval from Tenable across multiple domains: assets, vulnerabilities, and historical scans. You need the ability to check a vulnerability against a single host (get_asset_vulnerabilities) and then immediately launch a remediation scan (launch_scan) without switching tools or logging in. Don't use this if your goal is simply to read Tenable reports into PDF format; you still need to export those files manually. Also, don't use it if you only want general system health checks outside of the scope of vulnerability assessment; for that, a different monitoring tool might suffice.

The Pain of Dashboard Overload

Today, checking asset risk means clicking through tenable.io's web interface: you jump to the assets list, pull IDs, check tags in a separate section, find the correct scan folder, and then manually initiate an assessment run. You end up copying data from one tab, pasting it into another, and spending fifteen minutes just gathering context before you even start investigating.

With this MCP, you simply ask your agent what you need. The process collapses into a single conversation. You get the asset list, its current vulnerabilities, and the ability to launch an immediate scan—all while staying right where you are working.

Tenable Vulnerability Management with MCP

You don't have to manually list scans and then cross-reference the results. You can ask your agent to retrieve all scan analytics for a specific job ID, and it handles the data aggregation for you.

It changes the game from tedious manual investigation into instant, conversational intelligence. Your focus shifts entirely to remediation, not navigation.

Tenable: 10 Tools for Security Operations

These tools let you interact with Tenable's core functions, allowing your agent to list inventory, check specific vulnerabilities, or launch scans programmatically.

#	TOOL	DESCRIPTION
01	`list_assets`	Lists all hosts and cloud assets discovered in Tenable.io.
02	`get_asset_details`	Retrieves detailed metadata, networking information, and the risk profile for a specific asset.
03	`get_scan_results`	Pulls runtime analytics and vulnerability summaries for a specific scan job ID.
04	`launch_scan`	Manually triggers an immediate execution of one of your configured vulnerability scans.
05	`list_scan_folders`	Lists the different operational scan folders, like 'PCI Quarters' or 'My Scans'.
06	`list_logical_networks`	Retrieves a list of Tenable's defined logical routing networks.
07	`list_scans`	Lists all historical vulnerability assessment scans configured in Tenable.io.
08	`list_asset_tags`	Displays organizational tags mapped across your assets, like 'Critical' or 'Production'.
09	`list_scanners`	Lists all Nessus scanners that are managed by Tenable.io.
10	`get_asset_vulnerabilities`	Retrieves explicit security findings, or Workbench results, for a specific asset ID.

See It in Action

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

U Find the status and schedule of the 'Weekly PCI Scan'.

I've queried your configured scans. The 'Weekly PCI Scan' is currently 'enabled' and actively on schedule (UUID: eb92f03f-xxxx). It is mapped to the 'PCI Quarters' logical folder. Last execution was 4 days ago. Do you want me to list its historical results?

U Retrieve all extreme vulnerabilities on asset ID 1383da-xxx.

I pulled the Workbench findings for asset 1383da-xxx. I found 3 critical severity issues detected via plugin 104743 (Windows OTD exploit) and plugin 51192 (OpenSSL RCE). It seems the host is missing 4 months of standard OS patches. Shall I provide the exact CVE payload?

U Launch the scan with ID a981bf93 immediately.

Scan a981bf93 has been successfully commanded to start. The job run ID is c2f90a1-xxxxx. It has been pushed to the scanner queues and will evaluate all tied network zones independently. Let me know when you want to retrieve the results.

Frequently Asked Questions

01 **How do I check if a specific asset has vulnerabilities using Tenable MCP?**

You use get_asset_vulnerabilities() to pull the explicit security findings for that single machine. This gives you immediate details on CVEs without needing a full scan.

02 **What is the best way to start a new vulnerability assessment?**

You first use list_scans() to see what assessments are configured, and then manually trigger an immediate run using launch_scan().

03 **Can I find out what tags my assets have?**

Yes, you can run list_asset_tags() to see all the organizational tags available across your environment.

04 **Does Tenable MCP help with compliance reporting?**

It helps by allowing you to easily list and retrieve results from specific scan folders (like 'PCI Quarters'), making it easier to prove coverage for an audit.

05 **How do I view the full data of a host?**

Use get_asset_details() with the asset ID. This pulls comprehensive metadata, networking details, and the overall risk profile in one go.

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 `"tenable": { "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

Tenable 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 Tenable. 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	Tenable MCP
Server ID	`019d7611-892b-712a-bd3c-466166d1f4ca`
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/tenable.