MCP SERVER | NO CODE | CLOUD HOSTED

# Vanta MCP

## Audit Compliance Status in Conversation.

Vanta MCP connects your AI agent directly to your compliance and security data. It lets you audit users, devices, vendors, and vulnerabilities by asking natural questions instead of clicking through complex dashboards. Get a real-time view of your continuous compliance posture across SOC 2, HIPAA, GDPR, and more.

A+ Quality Score 100/100

compliance-automation | security-auditing | vulnerability-management | soc2 | risk-assessment | endpoint-security

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

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.

# Vanta MCP

10 tools available
Cloud-hosted on Vinkius

Need to prove your company meets specific regulatory standards? This MCP brings your Vanta security monitoring directly into your chat workflow. Instead of spending hours cross-referencing reports or building massive spreadsheets, you just ask your agent questions like, 'Are we ready for the SOC 2 audit?' The agent pulls together all the necessary data—from personnel training records to the latest vulnerability scan results—and gives you a single answer. It's less about looking at dashboards and more about having a conversation with your compliance status. With Vinkius, connecting this MCP means any AI client can access these deep security metrics on demand. You get immediate visibility into everything from endpoint encryption status to pending policy approvals, turning complex audits into simple Q&A sessions.

## Core Capabilities

**01 — Get overall compliance health**

Check your current compliance readiness score and view pass rates across major frameworks like SOC 2 or HIPAA.

**02 — Audit endpoints and devices**

List all monitored computers, checking their operating system version, disk encryption status, and antivirus compliance instantly.

**03 — Manage personnel records**

Pull lists of employees to check who has overdue security training or whose access reviews are pending completion.

**04 — Track vulnerabilities**

Review all detected security flaws, seeing the severity level (Critical/High) and the deadline set for fixing them.

**05 — Review audit evidence status**

See which required documents or screenshots are outstanding, who owns them, and when they are due.

**06 — Assess governance risks and policies**

List the company's risk register to understand high-impact areas needing attention, or review policy versions for acknowledgment rates.

## One Click on Vinkius — From Prompt to Execution

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

01 Subscribe to this MCP in your Vinkius catalog and enter your Vanta Developer API Token.

02 Your AI client connects the tokens and authenticates with Vanta's secure endpoints.

03 You ask a natural language question (e.g., 'What are our outstanding risks?') and receive an immediate, structured answer from the data.

The bottom line is you get instant access to deep security posture metrics without ever leaving your chat interface.

## Built For

Compliance Officers who hate compiling evidence for audits, IT Administrators managing device fleets, and DevSecOps Engineers tracking vulnerabilities. If your job involves proving regulatory adherence or patching gaps, you need this.

**Compliance Officer**

Runs continuous checks on user training status, reviews policies for acknowledgment rates, and pulls evidence lists for auditors.

**IT Administrator**

Checks the compliance state of all monitored workstations to ensure disk encryption and antivirus are active before a major audit.

**DevSecOps Engineer**

Queries the vulnerability backlog in real-time, prioritizing resources that need patching based on their severity and SLA deadlines.

## What Changes When You Connect

01 Stop searching dashboards. You can query personnel compliance directly, using the `vanta_list_people` tool to find out instantly who has overdue training or non-compliant devices.

02 Drill down deeper than ever before with the `vanta_get_test` tool. Instead of reading a generic failure notice, you get specific remediation guidance linked to the failing control.

03 Gain immediate risk visibility by running the `vanta_list_risks` tool. You can summarize board-level security risks and identify high-impact areas needing attention without leaving your chat window.

04 Keep track of every compliance requirement using `vanta_list_evidence_requests`. Your agent shows you exactly what evidence is still outstanding and who needs to submit it before the deadline.

05 Automate endpoint checks. Use `vanta_list_computers` to quickly verify if new hardware has disk encryption enabled or if its antivirus software is running, which saves hours of manual spot-checking.

## Real-World Applications

**The quarterly audit prep**

A Compliance Officer needs to know the current risk picture for the board meeting. They ask their agent to check `vanta_list_risks`. The agent instantly pulls a summary of all identified risks, showing the impact level and the status of required mitigation controls.

**Onboarding/Offboarding compliance**

An IT Administrator needs to confirm an employee is properly offboarded. They use `vanta_list_people` to check the user's employment status and ensure their access review was completed, preventing orphaned accounts.

**Handling a security incident**

A DevSecOps engineer discovers a vulnerability. Running `vanta_list_vulnerabilities` immediately gives them the CVE ID, the affected resource, and the mandated remediation SLA deadline, letting them prioritize fixes instantly.

**Checking overall readiness**

A team lead needs to confirm if they are ready for a new certification. They check `vanta_compliance_status`, which provides an immediate score and highlights exactly which frameworks or controls are failing, guiding their next steps.

# Patterns to Avoid

### Manual spreadsheet cross-referencing

✗ AVOID

Copying lists of user names from the People dashboard into an Excel sheet and manually checking them against a different tab for training completion dates.

✓ INSTEAD

Use `vanta_list_people` to ask your agent directly: 'Which employees have overdue security training?' The data comes pre-filtered, giving you a clean list immediately.

### Relying on dashboard filters

✗ AVOID

Opening the Vulnerability report and clicking through dozens of filters (severity, owner, date) to find all high-risk issues older than 90 days.

✓ INSTEAD

Ask your agent to run `vanta_list_vulnerabilities` filtered by 'Severity: High' AND 'SLA Deadline: Past Due'. The query does the filtering for you.

### Confusing policy status

✗ AVOID

Trying to determine if a company policy is ready without opening the Policy Management module, requiring manual date checking.

✓ INSTEAD

Use `vanta_list_policies` and ask: 'Show me all policies that are currently in draft status or require a review within the next 30 days.' This flags immediate governance needs.

## The Right Fit

You need this MCP if your job involves continuous evidence collection, managing compliance deadlines, or auditing complex security postures. If you find yourself opening multiple tabs—one for users, one for policies, and a third for vulnerabilities—you should use this. It collapses all that data into conversational tools. Don't use this if you just need to know 'who is the owner of X.' For simple lookups outside of Vanta (like checking an employee's phone number), your general AI client works fine. But for anything tied to compliance status, evidence tracking, or risk scoring, you must run through a dedicated tool like `vanta_compliance_status` or `vanta_list_risks` via this MCP.

## The Compliance Evidence Headache

Right now, proving compliance is a nightmare. You open Vanta and you're faced with dozens of dashboards. To build an audit report for one control, you have to navigate from the People tab, cross-reference that data against the Policy Approval module, and then check if the device list matches up. It’s clicking through six different tabs, copying lists into a spreadsheet, and hoping you don't miss a single date.

With this MCP, you just talk to your agent. You ask: 'What evidence do we need for HIPAA?' The system runs `vanta_list_evidence_requests`, pulls data from `vanta_list_people` regarding training status, and compiles the entire answer in one go. You get actionable answers, not raw dashboards.

## Vanta MCP: Real-Time Security Posture

You no longer have to wait for a quarterly report or spend an afternoon compiling the 'Who has non-compliant devices?' list. You can execute `vanta_list_computers` and get a real-time, filtered list showing only those endpoints that lack disk encryption or are running old OS versions.

This MCP turns compliance from a manual annual exercise into a continuous conversation. Your security status is always available, instantly queried by your agent.

# Vanta MCP: 10 Tools for Compliance Auditing

These tools let you pull deep security data from Vanta—from personnel training status to current vulnerability scores—all through conversational commands.

| # | TOOL | DESCRIPTION |
|---|---|---|
| 01 | `vanta_compliance_status` | Gets your overall compliance score, showing pass rates, critical alerts, and the audit readiness status across all frameworks. |
| 02 | `vanta_get_test` | Drills down into a specific failing test to get detailed information on evidence, linked controls, and remediation guidance. |
| 03 | `vanta_list_computers` | Lists all monitored endpoints, providing the OS version, encryption status, antivirus presence, and overall compliance state for each device. |
| 04 | `vanta_list_evidence_requests` | Shows outstanding audit evidence requests in Vanta, including who needs to submit documents or screenshots and their deadlines. |
| 05 | `vanta_list_integrations` | Lists all connected services, showing if they are syncing correctly, when the last sync was, and any configuration warnings. |
| 06 | `vanta_list_people` | Provides a list of personnel detailing their security training completion status, device compliance, access review state, and employment status. |
| 07 | `vanta_list_policies` | Lists all internal security policies, tracking their approval status, next review due date, version number, and employee acknowledgment rates. |
| 08 | `vanta_list_risks` | Retrieves the full risk register, detailing identified risks with impact scores, likelihoods, calculated scores, and mitigation plans. |
| 09 | `vanta_list_tests` | Lists all compliance monitoring tests (SOC 2, HIPAA, etc.), showing their pass/fail status, last run dates, and associated control requirements. |
| 10 | `vanta_list_vulnerabilities` | Shows detected security flaws across your infrastructure, including severity level, CVE IDs, affected resources, and the remediation SLA deadline. |

# See It in Action

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

**U** List pending Trust Center requests for our security documentation.

I've retrieved the pending Trust Center requests. You currently have 3 prospects awaiting access: 'sarah@piedpiper.com' requested SOC 2 Type II reports yesterday, and 'admin@hooli.xyz' requested Pen-Test summaries this morning. Would you like me to approve these specific emails for viewing?

**U** Retrieve the Vanta framework compliance details and mapped status of our organization.

I retrieved your Vanta organization details. Your company 'Acme Corp' is currently actively tracking towards SOC 2 Type II and HIPAA frameworks. Your continuous monitoring health score sits firmly at 92%. Would you like a breakdown of any failing domains?

**U** What subprocessor vendors are we actively syncing in Vanta right now?

You have 14 active integrations serving as authorized subprocessors logged in Vanta. Major ones include Amazon Web Services, GitHub, Slack, and Datadog. Three minor vendors are currently unverified and missing full justification descriptions in the system policy context.

# Frequently Asked Questions

01 **How do I check my overall compliance score using Vanta MCP?**

You use the `vanta_compliance_status` tool. It provides a single dashboard view of your pass/fail rates and shows if you are ready for major audits like SOC 2 or HIPAA.

02 **Can I see which employees need training using Vanta MCP?**

Yes, run the `vanta_list_people` tool. It lists all personnel and flags anyone whose security awareness training is overdue for immediate attention.

03 **What is the best way to check device encryption status with Vanta MCP?**

Use `vanta_list_computers`. This function gives you a clear inventory of all monitored devices and explicitly states if disk encryption or firewall protection is active on each one.

04 **How do I track pending security risks using Vanta MCP?**

Use `vanta_list_risks`. This tool pulls the full risk register, allowing you to see the impact score and if a mitigation plan has been assigned for each high-risk area.

05 **Does Vanta MCP help me with vulnerability tracking?**

Yes. The `vanta_list_vulnerabilities` tool lists all detected security flaws, including the CVE ID and most importantly, the mandated remediation SLA deadline for every issue.

# 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 `"vanta": { "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

# Vanta 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 Vanta. 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 | Vanta MCP |
| Server ID | `019d761a-f5b9-726e-b88d-ed23434fa828` |
| 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/vanta.

© 2026 Vinkius · vinkius.com · support@vinkius.com