MCP SERVER | NO CODE | CLOUD HOSTED

Drata MCP for AI Agents

Automating continuous compliance monitoring across cloud assets and personnel records

Drata lets you automate continuous compliance monitoring directly through your AI agent. Use it to audit security policies, track personnel onboarding statuses, verify cloud asset encryption, and assess readiness for frameworks like SOC 2 or HIPAA without leaving conversation mode.

A+ Quality Score 100/100

compliance-automation | security-audits | evidence-collection | soc2 | iso27001 | risk-management

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

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.

Drata MCP

10 tools available
Cloud-hosted on Vinkius

Managing compliance and security often means jumping between dashboards—a tedious process that slows down audits and increases risk. This MCP connects your Drata account to any compatible AI agent, letting you manage continuous compliance through natural language. You stop clicking tabs and start asking questions.

Need to know if a specific employee completed their mandatory annual training? Just ask your agent. Need the current pass/fail status of an AWS S3 bucket against our encryption policy? Ask it. The system pulls that data, synthesizes it, and gives you a clear answer immediately. Furthermore, since Vinkius hosts this MCP, you get access to Drata's entire catalog of monitoring tools right from your single connection point in any AI client.

It’s about transforming complex audit evidence—like tracking policy acknowledgments or reviewing vendor risk scores—into conversational data points. You get a real-time security posture assessment without ever needing to manually navigate the compliance dashboard.

Core Capabilities

01 — Review control status and test evidence

Get detailed pass/fail states for specific controls, including which automated tests provide evidence or if manual uploads are required.

02 — Check employee compliance records

Pull an individual's current onboarding state: background check status, security training completion, and device enrollment details.

03 — Audit policy readiness and renewal dates

Retrieve the status of key policies to see who needs to acknowledge them, when they are due for review, and the current version history.

04 — Verify cloud infrastructure compliance

List all monitored cloud assets (like RDS or EC2) and check their adherence to defined security controls, including encryption status.

05 — Assess overall framework readiness scores

View high-level progress across multiple frameworks (SOC 2, HIPAA), showing the percentage of passing controls and the target audit date.

06 — Manage third-party vendor risk inventory

Examine a list of vendors to track their data risk classification, security questionnaire status, and last SOC 2 review date.

One Click on Vinkius — From Prompt to Execution

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

01 First, subscribe to this MCP on Vinkius. Then, provide your Drata Public API Key from your Drata Dashboard settings.

02 Next, connect the MCP credentials to your preferred AI client (Claude, Cursor, etc.).

03 Finally, ask your agent a natural language compliance question—for example, 'Which personnel have overdue training?' and get an immediate, structured answer.

The bottom line is that you manage your entire security audit workflow conversationally, using the power of your AI client.

Built For

Compliance Officers and CISOs who spend too much time clicking through dashboards to gather evidence. It's also for HR Ops teams needing instant status checks on employee clearances, and Security Engineers monitoring real-time cloud deviations.

Chief Information Security Officer (CISO)

Uses this MCP to audit control statuses across multiple frameworks and track overall compliance readiness without manual dashboard navigation.

Compliance Officer

Assesses policy documentation status, checks vendor risk classifications, and verifies cloud asset alignment against required controls for audits.

HR Operations Manager

Monitors personnel records to quickly identify if employees have completed necessary security training or background checks before their access rights are granted.

What Changes When You Connect

01 Instead of manually cross-referencing multiple dashboards, your agent compiles comprehensive reports on failing controls using the `drata_list_controls` tool.

02 You instantly check an employee's full record with `drata_get_person`, confirming if they are compliant regarding training and device enrollment in one prompt.

03 Drastically simplify audit readiness. By running checks across all policies via `drata_list_policies`, you know exactly which documents need a review before the next quarter ends.

04 Eliminate manual asset reviews. The `drata_list_assets` tool gives an immediate picture of infrastructure compliance, showing if resources are unencrypted or improperly placed.

05 Get executive-level summaries using `drata_list_frameworks`, providing readiness scores for SOC 2 and ISO 27001 without digging into raw data sheets.

Real-World Applications

Investigating a missing security training record

An HR manager needs to know if John Doe completed his mandatory annual compliance module. Instead of checking the LMS and then the directory, they ask their agent, which uses `drata_get_person` to confirm the specific training date.

Preparing for an external audit review

A Compliance Officer needs a summary of all policies that haven't been reviewed in two years. They ask their agent, which uses `drata_list_policies` to flag the overdue documentation and gives them a prioritized checklist.

Responding to an alert about unencrypted data

A Security Engineer gets an alert that some EC2 instances might be non-compliant. They ask their agent, which uses `drata_list_assets` to pinpoint the exact resources lacking required encryption at rest.

Assessing third-party vendor risk quickly

The procurement team needs a quick security posture check on a new vendor. They ask their agent, which uses `drata_list_vendors` to retrieve the vendor's data risk classification and whether they have submitted recent SOC 2 reports.

Patterns to Avoid

Checking compliance status via multiple tabs

✗ AVOID

Opening the 'Policies' dashboard, then opening the 'Assets' tab to check encryption, and finally pulling up the 'Personnel' report—this takes 15 minutes of clicking.

✓ INSTEAD

Ask your agent directly. For example: 'Show me all unencrypted cloud assets linked to personnel who haven't completed training.' This combines data points from `drata_list_assets`, `drata_get_person`, and `drata_list_controls` in one prompt.

Only checking for pass/fail status

✗ AVOID

Seeing that a control is 'Fail' but not knowing *why* or what the evidence was. You get an alert, but no remediation path.

✓ INSTEAD

Use the `drata_get_control` tool to investigate failing controls. It gives you the explicit auditor language defining the risk and shows exactly what evidence supports the current status.

Forgetting vendor risk context

✗ AVOID

Simply knowing a third party is connected, but not knowing if they handle 'Critical' data or if their security assessment was done last month.

✓ INSTEAD

Always check the `drata_list_vendors` tool. It provides the necessary data risk classification and tracks when the vendor's required reports (like SOC 2) were last assessed.

The Right Fit

Use this MCP if your primary pain point is synthesizing compliance evidence across multiple domains—personnel, cloud assets, policies, and vendors. You need a single source of truth that can answer complex questions like: 'Are all high-risk third parties using encrypted backups?' This tool excels at aggregating disparate data points into conversational answers.

Don't use it if you are doing granular, point-in-time data entry or creating custom reports in another system. For raw API scripting or building a dedicated compliance visualization dashboard, you might prefer direct integration with the underlying APIs (e.g., AWS CLI). However, if your goal is *understanding* the state of compliance through natural dialogue, Drata's tools are unmatched.

Drata MCP for AI Agents: Auditing Compliance Policies and Documentation

Right now, assessing audit readiness means navigating dozens of internal documents. You jump between the Policy dashboard to see renewal dates, then copy-paste names into a spreadsheet to track employee acknowledgments. It's tedious, prone to human error, and takes days just to compile the initial risk report.

With this MCP, you simply ask your agent about policy status. It instantly pulls data using `drata_list_policies` —giving you a clean list of policies needing review, who owns them, and what the next due date is. You get an immediate, actionable audit summary.

Drata MCP for AI Agents: Tracking Personnel Security Status

Before, checking if a new hire was cleared required contacting HR, IT, and the manager separately. You'd check one system for background checks, another for training records,

Now, you ask your agent about an employee by name. It uses `drata_get_person` to give you one consolidated view: whether their background check is clear, if they finished mandatory security

and a third for device enrollment status—a painful manual chain of custody.

training, and if their corporate laptop meets MDM standards. You get a complete compliance picture in seconds.

Drata MCP: 10 Tools for Compliance & Audit Evidence Collection

Use these tools to check policy renewals, list assets, review vendor risk, or track individual personnel compliance status.

#	TOOL	DESCRIPTION
01	drata_get_control	Investigates a specific compliance control's status, providing details on test evidence and the underlying risk language for auditors.
02	drata_get_person	Retrieves an employee's complete compliance profile, including training completion, background check clearance date, and device enrollment status.
03	drata_get_policy	Gathers detailed information about a specific policy, showing its renewal dates, who needs to acknowledge it, and the current version history.
04	drata_list_assets	Generates an inventory of cloud infrastructure assets, detailing their compliance status, encryption state, and associated region.
05	drata_list_controls	Lists all defined security requirements (e.g., 'MFA must be enabled') and reports on their current pass/fail status across mapped frameworks.
06	drata_list_frameworks	Provides a high-level overview of active compliance frameworks, including overall readiness scores and percentage completion for board reporting.
07	drata_list_personnel	Lists all tracked personnel, summarizing their security training status, device compliance, background check clearance, and policy acceptance rates.
08	drata_list_policies	Outputs a list of all corporate policies, detailing the last review date, next required renewal date, and employee acknowledgment completion rate.
09	drata_list_tests	Shows real-time automated monitoring results for specific technical requirements across AWS, Okta, or GitHub, noting any immediate failures.
10	drata_list_vendors	Tracks all third-party vendors, providing their data risk classification, security questionnaire status, and required report review dates.

See It in Action

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

U What are the top 3 failing controls right now?

Compliance Status Report

We currently have 3 critical controls flagged as non-compliant:

- ❌ **MFA for IdP Users:** Required, but two groups are missing enforcement.
- ❌ **Encrypted Backups:** Found in the `us-west-2` region. Manual verification needed.
- ❌ **Vulnerability Scanning:** Last run failed on the staging environment (ID: 456).

Would you like me to retrieve detailed test evidence for any of these?

U Give me a summary of our overall readiness scores.

Framework Readiness Snapshot

You are currently tracking two major frameworks:

- 🥈 **SOC 2 Type II:** 85% Complete (Target: Q4 2024). Needs focus on vendor risk management.
- 🥇 **ISO 27001:** 72% Complete (Target: Q1 2025). Policy acknowledgment rates are the biggest gap.

Overall, we're in a good position, but policy gaps and asset encryption need immediate attention.

U Who needs to complete their mandatory training?

Personnel Compliance Gaps

The following 5 users have overdue Security Awareness Training (SAT) or pending acknowledgments:

NAME	ROLE	GAP TYPE	DUE DATE
Jane Smith	Dev Op	SAT Overdue	Today
Tom Baker	HR Ops	AUP Missing	03/15/2024
Alex Kim	Contractor	Background Check	N/A (Failed)

Please send an automated reminder to these users?

Frequently Asked Questions

01 **How can the Drata MCP help me audit policies?**

The Drata MCP lists all official corporate policies. It tells you which ones are due for review, who is responsible for updating them, and what percentage of employees have acknowledged the latest version.

02 **Does Drata MCP check if my cloud resources are secure?**

Yes. You can list all monitored infrastructure assets, checking their compliance status against controls like encryption-at-rest and network boundary adherence instantly.

03 **What kind of personnel data can I get with Drata MCP?**

You can retrieve a full profile on any person. This includes their mandatory security training completion dates, background check clearance status, and whether their device is properly managed by MDM.

04 **Can I use the Drata MCP to assess vendor risk?**

Yes. It provides a clear inventory of all third parties, detailing their data risk classification (Critical/High/Medium) and when they last submitted required security reports.

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 `"drata": { "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

Drata 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 Drata. 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	Drata MCP
Server ID	`019d7589-3177-720b-b01d-9e9226361495`
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/drata.