

M C P S E R V E R

N O C O D E

C L O U D H O S T E D

Caterpillar Cat Digital MCP

Bring real-time heavy equipment data to your AI agent.

Caterpillar Cat Digital MCP connects your AI client directly to the api.cat.com gateway. It gives your agent access to live diagnostic events, fault codes, and telemetry usage records from your connected Cat machine fleet. Use it to monitor machine health and track data consumption against your subscription limits.

A+ Quality Score 100/100

caterpillar

visionlink

heavy-equipment

telematics

construction-tech

equipment-diagnostics



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.

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.

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.

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

Encryption at rest

Ed25519

PKI vault signatures

24h TTL

Ephemeral session keys

V8 Isolate

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.

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.

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.

06 — Honeypot Trap System

Phantom credentials are injected into isolated environments. If a honeypot 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.

FinOps

Cost tracking per tool, payload compression savings, budget optimization signals, and consumption trends.

Firewall & DLP

PII redaction activity, sensitive data protection counters, and security event timeline.

Agent Activity

Which AI clients are connecting, how often, and what they're doing — real-time session tracking.

Tool Health

Slowest and most error-prone tools, with actionable root-cause insights and performance baselines.

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.

Caterpillar Cat Digital MCP

3 tools available

Cloud-hosted on Vinkius

This MCP acts as a direct bridge to the Caterpillar Cat Digital API gateway. Instead of manually checking portals, you can ask your AI client to pull diagnostic data or check how much telemetry data your fleet has consumed. It uses Bearer authentication from the Cat Developer Program to securely pull information from your connected machines. You can use it to identify fault codes, monitor machine health, and keep an eye on your telemetry billing to avoid exceeding plan limits. It is built for anyone managing heavy equipment who wants to automate data analysis or build custom monitoring tools using an AI agent.

Core Capabilities

01 — Machine Diagnostics

Your agent pulls fault codes and diagnostic events directly from connected machines.

02 — Usage Monitoring

The AI checks telemetry billing records to track data consumption.

03 — Configuration Access

Your client retrieves public configuration settings for the Cat Digital AI assistant.

One Click on Vinkius — From Prompt to Execution

Available at vinkius.com/en/ai-agent-connect/caterpillar-cat-digital — connect your AI agent in three steps.

- 01 Apply for access through the Cat Digital Developer Program.
- 02 Obtain your Bearer access tokens for your subscribed products.
- 03 Paste your token into the MCP credentials section in Vinkius.
- 04 Connect your preferred AI client to the Vinkius host.
- 05 Ask your AI agent to pull diagnostics or billing data.

Connecting to Caterpillar data is a straightforward process once you have your developer credentials.

Built For

This MCP is designed for professionals managing heavy machinery and construction technology.

Fleet Managers

They hand off machine health monitoring and diagnostic checks to their AI agent.

Construction Tech Builders

They use the API data to power custom applications and automated workflows.

Equipment Health Analysts

They use the diagnostic tools to identify patterns in machine failures.

What Changes When You Connect

- 01 Direct access to api.cat.com via Bearer authentication.
- 02 Automated monitoring of telemetry usage against subscription limits.

03 Instant retrieval of machine fault codes and diagnostic events.

04 Eliminates manual lookups in the Cat Digital portal.

Real-World Applications

Fleet Health Audits

An AI agent scans all connected machines for active fault codes to identify maintenance needs.

Automated Troubleshooting

Your AI client interprets diagnostic events to suggest immediate repair steps for technicians.

Data Budgeting

You check telemetry billing to ensure job site connectivity isn't driving up data costs.

Subscription Management

Monitor API consumption to stay within the limits of your Cat Digital developer plan.

3 Tools Available

#	TOOL	DESCRIPTION
01	get_telemetry_billing	This tool retrieves telemetry billing records for your Cat equipment. It helps you monitor how much data your machines are using against your specific plan limits.
02	get_diagnostics_services	This tool pulls diagnostic events and fault codes from connected Cat machines. It provides the raw diagnostic data needed to troubleshoot equipment issues through your AI client.
03	get_ai_assistant_config	This tool accesses the public configuration for the Cat Digital AI assistant. It provides guest access to the configuration settings used by the Cat AI assistant.

See It in Action

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

U Show me diagnostic events from my Cat machines



Cat Diagnostic Services: Recent diagnostic events from your connected fleet: D6T Dozer (S/N ABC123): Fault code 4592-14, aftertreatment. 320 Excavator (S/N DEF456): Sensor reading event, hydraulic temp. Each event includes machine S/N, code and timestamp.

U How much telemetry data usage have we billed this month?



Telemetry billing (Cat Digital): Current cycle shows X GB across N machines, which is within your plan allowance. A per-machine breakdown is included in the payload.

U Check if any machines have active fault codes



Cat Diagnostic Services: I found one active fault code. D6T Dozer (S/N ABC123) is reporting fault code 4592-14 related to the aftertreatment system.

Frequently Asked Questions

01 How do I authenticate this MCP?

You must use a Bearer token obtained from the Cat Digital Developer Program. You paste this token into the credentials tab of the MCP in Vinkius.

02 What should I do if I get a 401.006 error?

A 401.006 error indicates that your Bearer token is either missing or invalid. Check your credentials in the Vinkius settings.

03 Can I use this to check my data usage?

Yes, the `get_telemetry_billing` tool allows you to monitor your telemetry data usage against your plan limits.

04 What if the tool says I lack a product subscription?

If you receive a 403 error, it means your Cat Digital app does not have the specific product subscription required for that tool.

05 Which AI clients can use this MCP?

This MCP works with any MCP-compatible client, including Claude, Cursor, Windsurf, and VS Code.

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 <code>"caterpillar-cat-digital": { "url": "..." }</code>
 Windsurf	MCP Settings → <code>mcp_settings.json</code> → 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

Caterpillar Cat Digital 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 Caterpillar Cat Digital. 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	September 2026
MCP Server	Caterpillar Cat Digital MCP
Server ID	01a07eac-bae7-71ee-a298-b9009e6f6263
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/en/ai-agent-connect/caterpillar-cat-digital.