

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

Encrypted Archive Inventory MCP

Keep your encrypted data accessible and audit-ready.

Encrypted Archive Inventory MCP gives your AI client a way to track, organize, and audit your encrypted digital archives. It handles the heavy lifting of monitoring recovery key availability, tracking storage locations, and flagging archives that need immediate maintenance or are hitting retention deadlines. You can manage the entire lifecycle of your encrypted data through a single interface.

A+ Quality Score 100/100

encryption

audit

archives

lifecycle

recovery



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.

Encrypted Archive Inventory MCP

5 tools available

Cloud-hosted on Vinkius

Managing encrypted data is a liability if you can't prove you can actually get to it. This MCP turns your AI client into a specialized auditor for your digital archives. Instead of digging through spreadsheets to see if your decryption keys are still valid, you can ask your agent to scan your inventory for risks.

You can use this to keep a tight grip on your data lifecycle. It tracks where things are stored and, more importantly, whether the keys needed to unlock them are actually available. If a key is missing or a verification date has passed, your agent will find it. You can also register new archives or log successful integrity checks to keep your audit trail clean. It's built to ensure that when you need to recover data, you aren't staring at a broken link or a lost key.

Core Capabilities

01 — Risk Detection

Your agent identifies archives where decryption keys are missing.

02 — Lifecycle Tracking

The MCP monitors retention deadlines and verification requirements.

03 — Inventory Management

You can add new archives or view your entire collection through your AI client.

04 — Integrity Auditing

The system logs successful integrity checks to maintain an accurate audit trail.

One Click on Vinkius — From Prompt to Execution

Available at vinkius.com/en/ai-agent-connect/encrypted-archive-inventory — connect your AI agent in three steps.

- 01 Connect your preferred MCP-compatible client to Vinkius.
- 02 Grant your agent access to the Encrypted Archive Inventory tools.
- 03 Ask your agent to list, register, or audit your archives.
- 04 Review the results and maintenance alerts directly in your chat interface.

Connect your AI client to the Vinkius-hosted MCP to start managing your archives immediately.

Built For

This MCP is designed for professionals managing large volumes of sensitive, encrypted data who need to ensure long-term accessibility.

Data Security Officers

They use the agent to audit key availability and verify archive integrity.

Compliance Managers

They rely on the tool to track retention deadlines and maintenance schedules.

IT Administrators

They use it to register new archives and manage storage locations.

What Changes When You Connect

- 01 Prevents data loss by flagging missing decryption keys.
- 02 Automates the tracking of retention and verification deadlines.
- 03 Maintains a clean audit trail for all integrity checks.

- 04 Centralizes archive management within your existing AI workflow.
-

Real-World Applications

Key Availability Audits

Run a check to ensure every encrypted archive has a valid, locatable recovery key.

Retention Compliance

Identify archives that have reached their expiration date and need to be purged or moved.

Integrity Verification

Log the results of periodic data integrity checks to prove archives remain uncorrupted.

New Asset Onboarding

Quickly add new encrypted datasets to your managed inventory via your AI client.

Patterns to Avoid

Manual spreadsheet tracking

❌ AVOID

You keep a separate Excel sheet to track which decryption keys belong to which archives and manually check dates.

✓ INSTEAD

Use ``register_archive`` to bring your data into the system and ``get_maintenance_schedule`` to let your agent handle the deadline tracking for you.

Reactive key auditing

❌ AVOID

You wait until a data recovery request comes in to realize the decryption key is missing or the archive is corrupted.

✓ INSTEAD

Run ``check_recovery_health`` regularly to find missing keys before they become a crisis.

Ignoring integrity check results

❌ AVOID

Your team performs manual checks on data but never records the results, leaving no proof of archive health.

✓ INSTEAD

Always use ``update_verification_status`` after a successful check to maintain a clean, verifiable audit trail.

The Right Fit

Connect this MCP if you manage large volumes of sensitive, encrypted data that require long-term accessibility. If you only handle small, transient datasets that don't need lifecycle tracking, you don't need this. The deciding factor is whether you need a verifiable audit trail for your decryption key availability.

Encrypted Archive Inventory Tools

These tools let your agent manage the entire lifecycle of encrypted data, from initial registration to periodic integrity audits.

#	TOOL	DESCRIPTION
01	check_recovery_health	This tool scans your inventory for archives that are at risk because their decryption keys cannot be located.
02	get_maintenance_schedule	Use this to find archives that need attention due to expired verification dates or upcoming retention deadlines.
03	list_archives	This tool provides a full overview of every encrypted archive you have managed in the system.
04	register_archive	This tool adds a new encrypted archive to your inventory once all mandatory fields are filled out.
05	update_verification_status	Use this to record that an archive has passed a successful integrity check.

See It in Action

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

U Show me all archives that need immediate attention.



You have 2 archives requiring attention: Archive ID 'FIN-2023-01' is due for verification, and Archive ID 'LEG-99' is approaching its retention expiry.

U Are there any archives missing recovery keys?



Yes, Archive ID 'ID-882' (Category: Identity) is missing a recovery key location.

U List all my Technical archives.



Found 3 Technical archives: 'SYS-BACKUP-01', 'CONF-FILE-A', and 'REPO-CORE'.

Frequently Asked Questions

01 How does this MCP help with data recovery?

It identifies archives that are at risk because their decryption keys cannot be found, allowing you to fix the issue before the data becomes inaccessible.

02 Can I use this with Claude or Cursor?

Yes, you can connect this MCP to any MCP-compatible client including Claude, Cursor, and Windsurf.

03 How do I know if an archive is due for a check?

The `get_maintenance_schedule` tool identifies archives that require attention due to expired verification dates or upcoming retention deadlines.

04 Do I need to host the MCP myself?

No, Vinkius hosts and manages the MCP for you, so it is ready to use as soon as you connect your client.

05 Can I add new archives to the list?

Yes, you can use the `register_archive` tool to add new entries to your inventory.

06 How can I see which archives need verification?

You can use the ``get_maintenance_schedule`` tool to identify archives that are due for verification or approaching their retention expiry.

07 What happens if a recovery key location is missing?

If a recovery key location is missing, the archive will be flagged as a risk when you run ``check_recovery_health``.

08 Can I filter my archives by category?

Yes, the ``list_archives`` tool allows you to filter the entire inventory by specific categories like Legal, Financial, or Personal.

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>"encrypted-archive-inventory": { "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

Encrypted Archive Inventory 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 Encrypted Archive Inventory. 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	October 2026
MCP Server	Encrypted Archive Inventory MCP
Server ID	01a0eee2-099e-73b2-97fa-00e60982e8cb
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/encrypted-archive-inventory.