MCP SERVER | NO CODE | CLOUD HOSTED

CyberArk Privilege Cloud MCP for AI Agents

Govern Access and Audit Vaulted Credentials Using Natural Language Commands

CyberArk Privilege Cloud connects your AI agents directly to your enterprise vaulting systems. You can audit secure safes, check out vaulted account passwords with mandatory justification, monitor user activity, and terminate active privileged sessions—all through natural conversation.

A+ Quality Score 100/100

privileged-access-management | vaulting | password-management | session-monitoring | zero-trust | audit-logs

MAINTAINED BY VINKIUS CLOUD FOR AI AGENTS · JUNE 2026
vinkius.com/mcp/cyberark-privilege-cloud

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.

CyberArk Privilege Cloud MCP

10 tools available
Cloud-hosted on Vinkius

This MCP lets your agent take full control of identity security without forcing you into complex consoles. Need to verify who has access to the domain controller? Your agent lists internal users and LDAP-mapped groups instantly. Curious if a service account needs rotation? Check its status or get detailed properties using `get_account`. For incident response, you don't need SSH keys; your agent can pull the clear-text password directly from the Vault with an auditable reason attached. It also handles session control—if something looks suspicious mid-session, it forces termination instantly. By connecting this MCP through Vinkius, you give your AI client a single pane of glass to manage critical privileged access and maintain strict compliance.

Core Capabilities

01 — Audit Vault Contents

List all secure Safes or search for specific accounts to understand the overall structure of your vaulting environment.

02 — View User & Group Permissions

Check which users, groups, and administrators have access to different parts of the system, verifying role-based access controls (RBAC).

03 — Retrieve Credentials on Demand

Pull actual vaulted passwords for specific accounts. This action is highly audited and requires a mandatory justification reason.

04 — Control Active Sessions

Instantly terminate an active privileged session when suspicious activity or unauthorized actions are detected during an incident response scenario.

05 — Manage Account Lifecycle

Provision new service accounts into the vault, or delete retired accounts to ensure proper credential management and cleanup.

One Click on Vinkius — From Prompt to Execution

Available at **vinkius.com/mcp/cyberark-privilege-cloud** — connect your AI agent in three steps.

01 You subscribe to this MCP in Vinkius, providing your CyberArk Subdomain and Bearer access token.

02 Your AI client connects using the provided credentials, giving it read/write control over specific vaulting functions.

03 You interact with the system using natural language prompts; the agent executes the required action and returns structured data.

The bottom line is you manage your entire privileged access infrastructure conversationally through your preferred AI client.

Built For

This MCP targets security teams who spend too much time clicking between consoles or waiting for manual reports. It's essential for Security Analysts and Auditors who need immediate, auditable visibility into every privileged action happening across the network.

Security Analyst / SOC Team

Monitoring active sessions to detect anomalous behavior or using `terminate_session` immediately when unauthorized activity is found during an incident.

IT Administrator

Onboarding new service accounts into the vault via `add_account` and managing Safe configurations without manually navigating the full Privileged Access Web Portal (PVWA).

Auditor & Compliance Officer

Running comprehensive checks to list all users, groups (`list_groups`), and account properties to verify that current access aligns with corporate security policies.

What Changes When You Connect

01 Instant Incident Response: Don't rely on manual checks during an incident. Your agent can `terminate_session` instantly upon detecting suspicious activity.

02 Zero-Touch Auditing: Quickly list all secure Safes using `list_safes` to locate critical credentials without navigating multiple security consoles.

03 Compliance Visibility: Use `list_users` and `list_groups` to verify current RBAC rules across the entire directory structure, making audits faster than ever.

04 Controlled Credential Access: Pulling a password via `retrieve_password` forces an auditable justification reason into the log, ensuring compliance even when emergency access is needed.

05 Simplified Onboarding: Instead of manual console work, use `add_account` to provision new service credentials with minimal clicks and maximum automation.

Real-World Applications

Investigating a Suspected Breach

A SOC analyst suspects an account is compromised. Instead of logging into the console, they ask their agent to `terminate_session` for the suspect connection and then run `list_accounts` to see which accounts were recently accessed.

Quarterly Compliance Audit

An auditor needs proof that only authorized teams access specific root credentials. They ask their agent to `list_groups` followed by checking Safe details using `get_safe` to verify group membership against policy.

Emergency System Maintenance

The DBA finds a critical service account password missing. They use their agent to `retrieve_password`, providing the required justification ('Emergency DB patch'), and securely get the credential instantly.

Service Account Cleanup

An IT Admin decommissioned an application. Instead of manually deleting credentials, they instruct the agent to use `delete_account` on the old service account ID, ensuring the Vault cleans up properly.

Patterns to Avoid

Trying to bypass audit logs

✗ AVOID

Asking your AI client to just 'show me the password for admin' without specifying a business reason. This fails because the agent requires a mandatory justification before calling `retrieve_password`.

✓ INSTEAD

Always provide context. Tell your agent: 'Retrieve the clear-text password for Admin account (ID 123). Reason: Emergency patching of critical system X.' This ensures the action is logged.

Forgetting credential status

✗ AVOID

Attempting to use an old service account that might have been rotated or marked inactive. The agent needs to run `get_account` first to verify its current operational state before attempting any actions.

✓ INSTEAD

Always check the status. Use `list_accounts` and then `get_account` on the specific ID. This confirms if the credential is ready for use, rotated, or otherwise flagged.

Misidentifying data scope

✗ AVOID

Asking about 'all users' without specifying whether you mean local domain users or only those listed in a specific Safe. The agent needs `list_safes` first to narrow down the scope of your search.

✓ INSTEAD

The Right Fit

You need this MCP if your security process requires immediate, auditable access to credentials and session management across multiple systems. It's perfect for compliance teams who must prove 'who did what, when.' Don't use this if you only need general directory information; in that case, a standard LDAP connector might suffice. You should connect it if your primary pain point is the time delay between identifying suspicious activity and forcibly stopping it, as `terminate_session` solves that problem instantly. However, don't rely on it to *replace* policy—it only executes what you tell it; proper access control must still be managed within CyberArk itself.

CyberArk Privilege Cloud MCP: Streamlining PAM Audit Requirements

Today, auditing privileged access is a nightmare of clicking. You have to jump between the directory service and the vaulting portal just to verify group membership or check account rotation dates. It's tedious copy-pasting across multiple tabs, making compliance checks slow and prone to human error.

With this MCP, you simply tell your agent what you need—like listing all users who can access a specific Safe. The agent gathers the data from every necessary corner of the vaulting system and presents it in one structured list. You get verifiable answers instantly.

CyberArk Privilege Cloud MCP: Real-Time Session Control for Incident Response

In a crisis, every second counts. Normally, detecting unauthorized activity means scrambling to find the console link and manually initiating termination protocols. This delay is unacceptable when dealing with potential data breaches.

Now, if your agent spots an anomaly, you just ask it to terminate the connection. The MCP executes `terminate_session` instantly across the PSM/PSMP layer. You cut off the threat immediately without ever logging into a console.

CyberArk Privilege Cloud: 10 Tools for PAM Vaulting & Credential Auditing

Use these tools to list users, audit safes, retrieve passwords, or terminate active sessions directly from your AI agent.

#	TOOL	DESCRIPTION
01	add_account	Automatically provision a new privileged service account into the Vault Safe after mapping it to its specific platform ID.
02	delete_account	Remove a retired or decommissioned privileged account from the CyberArk Vault, stopping any failed rotation attempts.
03	get_account	Fetch detailed property data for an existing vaulted credential before making changes or interacting with it.
04	get_safe	Retrieve metadata and specific details about a designated Privileged Access Manager (PAM) Safe container.
05	list_accounts	Search and retrieve high-sensitivity credentials, including Root or Administrator accounts, along with their current rotational status and allocated Safe.
06	list_groups	List all user groups in the CyberArk Vault to verify how access permissions are structured across your organization.
07	list_safes	Get a list of every secure Safe container used in the system, identifying where critical tier-0 credentials reside.
08	list_users	Identify all human or service accounts that consume privileged sessions across local and synchronized directories.
09	retrieve_password	Pull the actual, clear-text password for a specific account. This action requires a mandatory justification reason and triggers full auditing.
10	terminate_session	Forcefully cut an active privileged session (PSM/PSMP) immediately when required as part of an incident response procedure.

See It in Action

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

U What are all the service accounts for my web servers?

Vault Account Report: Web Servers

- Root-Web01 (ID: 902): Status **Active**. Last rotated: Yesterday. Safe: Linux-Servers.
- ServiceUser-DB (ID: 456): Status **Requires Attention**. Rotation due in 7 days. Safe: Database Vault.

Need me to check the access permissions for these accounts?

U I need the root password for the staging database right now.

Password retrieved successfully! For Root-Staging (ID: 123), the clear-text password is: `**`.

⚠️ **ACTION LOGGED:** This retrieval was triggered by you. Justification provided: 'Urgent patch deployment on staging environment'. Would you like me to check-in this account now?

U Who are the people with administrator rights in the finance department?

Based on user and group listings, these users have admin access:

1. **John Doe:** Member of 'Finance_Admins' Group.
2. **Jane Smith:** Direct Admin Role (ID: 789).
3. **SystemGroup-Audit:** System service account with read-only admin rights.

Frequently Asked Questions

01 **How do I audit who can access my critical accounts using CyberArk Privilege Cloud MCP?**

You list all users and groups to verify the RBAC structure. This lets you see exactly which roles have permissions to certain safes, ensuring compliance before any changes are made.

02 **Can I use CyberArk Privilege Cloud MCP for AI Agents during an active security incident?**

Yes. The most critical function is session control; your agent can forcibly terminate suspicious connections instantly when a threat is detected, drastically reducing response time.

03 **What if I need to check out a password for emergency use via the MCP?**

The system handles this with mandatory controls. When you request a password using CyberArk Privilege Cloud MCP for AI Agents, you must provide a justification reason that is logged instantly.

04 **Does this tool help me manage service accounts and their rotation schedules?**

Yes. You can list all privileged accounts to check rotational status or use the MCP to onboard new credentials via `add_account`, ensuring automated lifecycle management.

05 **What is the difference between listing safes and listing users with CyberArk Privilege Cloud MCP?**

Listing safes shows you the physical containers where secrets are kept. Listing users tells you which human or service accounts have access to those containers in the first place.

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 `"cyberark-privilege-cloud": { "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

CyberArk Privilege Cloud 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 CyberArk Privilege Cloud. 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	CyberArk Privilege Cloud MCP
Server ID	`019d7580-9602-7191-9ee5-a06f2026f3ae`
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/cyberark-privilege-cloud.