MCP SERVER | NO CODE | CLOUD HOSTED

Black Duck (Synopsys) MCP for AI Agents

Automating Open Source Security and Dependency Audits

Black Duck (Synopsys) MCP allows your AI agent to manage open source security compliance directly against your code inventory. You can list projects, find known vulnerabilities, check Bill of Materials (BOM) status, and audit security policies simply by asking natural language questions.

A+ Quality Score 100/100

open-source-security | vulnerability-scanning | license-compliance | software-supply-chain | cve-tracking | risk-management

MAINTAINED BY VINKIUS CLOUD FOR AI AGENTS · JUNE 2026
vinkius.com/mcp/black-duck-synopsys

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.

Black Duck (Synopsys) MCP

10 tools available
Cloud-hosted on Vinkius

Connect Black Duck (Synopsys) through this MCP to turn complex security auditing into a simple conversation with your AI agent. Instead of jumping between dashboards or running manual exports, you talk to the system about your code dependencies. The platform lets you locate all software projects and their versions across multiple repositories. You can ask for details on specific project components, check if the Bill of Materials (BOM) is current, or find out which users have access to sensitive data.

If a dependency has known vulnerabilities, you just ask, and your agent retrieves those CVEs along with severity levels. Furthermore, you can audit the entire organization's security posture by listing defined policy rules or checking who manages user accounts. It’s about getting immediate answers on compliance status and risk assessment right where you work. By connecting this MCP via Vinkius, you give any compatible AI client a single pane of glass for your entire open source supply chain.

Core Capabilities

01 — Identify all software projects

Retrieve a list and detailed metadata for every project tracked in Black Duck.

02 — Track specific versions and components

List all available versions for a given project or retrieve the full details of a target component.

03 — Audit known vulnerabilities (CVEs)

Query projects and versions to find listed Common Vulnerabilities and Exposures, along with their severity levels.

04 — Check compliance status

Verify the calculation status of the Bill of Materials (BOM) to confirm data freshness for regulatory reports.

05 — Review security policies and users

List all defined organizational security policy rules or retrieve profiles detailing platform user access controls.

One Click on Vinkius — From Prompt to Execution

Available at **vinkius.com/mcp/black-duck-synopsys** — connect your AI agent in three steps.

01 Subscribe to the MCP, providing your Black Duck Instance URL and API Token.

02 Your AI client authenticates with Vinkius and gains read-only access to your defined security scope.

03 You ask a question in natural language (e.g., 'What are the critical vulnerabilities for Project X?'), and the agent executes the necessary tool calls.

The bottom line is, you talk to your AI client like talking to a colleague; it does the API work behind the scenes.

Built For

This MCP is essential for Security Engineers and Compliance Officers who spend too much time manually exporting data from dashboards. If checking code dependencies or auditing policies is part of your routine, you need this tool.

Security Engineer

Audits vulnerabilities across dozens of projects quickly by requesting vulnerability listings and retrieving detailed CVE information without manual dashboard exports.

Compliance Officer

Generates reports for governance bodies by checking BOM statuses, listing policy rules, and reviewing user access controls for periodic audits.

Developer

Checks the security status of project dependencies directly from their code editor by querying specific project details or version history when committing code.

What Changes When You Connect

01 Immediate vulnerability assessment: Stop manually exporting reports. Your agent can list vulnerabilities or retrieve detailed CVEs instantly.

02 Compliance visibility: Use the MCP to check BOM status via get_bom_status, giving Compliance Officers real-time proof of data synchronization for audits.

03 Full project scope control: Need to know what you're auditing? List all projects and run a search_projects query to build your audit list quickly.

04 Policy enforcement checks: List policy rules (list_policy_rules) or review user access (list_users) directly through conversation, eliminating dashboard navigation time.

05 Pinpoint risk locations: Track security coverage by listing code locations (list_code_locations) and getting detailed project info via get_project.

Real-World Applications

Auditing a new service dependency

A developer needs to know the risk profile of a newly added library. They ask their agent, which then uses list_vulnerabilities and get_vulnerability_details to summarize all critical CVEs linked to that specific project version.

Preparing for quarterly compliance review

A Compliance Officer needs a report proving BOM data is current across all major applications. They use the agent to list projects, then check get_bom_status for each one before submitting their documentation.

Investigating unauthorized user access

The security team suspects an account has excessive privileges. The agent is used to run list_users and cross-reference that data with the platform's defined policy rules via list_policy_rules.

Determining project scope for a new audit

A lead engineer doesn't know all the applications in use. They ask the agent to list all projects, followed by search_projects to narrow down the targets before beginning the vulnerability scan.

Patterns to Avoid

Over-relying on manual dashboard exports

✗ AVOID

Manually generating a report for every project version and then compiling those CSVs into one master document takes days of tedious clicking.

✓ INSTEAD

Instead, use the MCP to ask your agent to list all projects (list_projects) and then iteratively check status using get_bom_status. The data comes compiled straight into your chat window.

Ignoring version specificity

✗ AVOID

Running a general vulnerability scan without specifying the exact project version can lead to outdated or irrelevant risk reports.

✓ INSTEAD

Always start by listing available versions (list_project_versions) and then instruct your agent to run list_vulnerabilities against that precise, identified version.

Treating the MCP as a simple search tool

✗ AVOID

Just typing 'security' into the chat assumes the agent knows exactly which policies or user accounts you mean.

✓ INSTEAD

Be specific: ask your agent to list all security policy rules (list_policy_rules) and then narrow down results using keywords like 'data handling' for better accuracy.

The Right Fit

Use this MCP if your primary bottleneck is translating complex, structured compliance data into natural language questions. If you need to audit software supply chains or manage open source risks across multiple applications, this tool is necessary. However, don't use it if you only need basic project directory listings; other file system tools might be faster. Also, note that while the MCP can list all projects and users (list_projects, list_users), it doesn't provide a way to actually *change* those user accounts or delete policies—it's purely for reading and auditing state. If your goal is execution rather than observation, you need a different type of integration.

Black Duck (Synopsys) MCP: Automating Open Source Vulnerability Audits

Today, assessing open source risk means logging into Black Duck and clicking through dozens of dashboards. You have to copy project names, find specific versions, then run separate reports for vulnerabilities, BOM status, and user access. This process is slow, error-prone, and often leaves you with a mountain of disconnected spreadsheets.

With this MCP, the same task becomes conversational. Tell your agent which projects need review; it handles retrieving project metadata (get_project), listing versions (list_project_versions), and immediately checking for known vulnerabilities via list_vulnerabilities. You get one single summary report instead of a dozen manual exports.

Black Duck (Synopsys) MCP: Managing Software Supply Chain Compliance

Compliance requires checking more than just vulnerabilities; you must prove the Bill of Materials is accurate and that policies are enforced. Manually verifying BOM status across all development lines, or auditing every policy rule using list_policy_rules, is a massive time sink.

The MCP solves this by consolidating these checks. You can ask your agent to confirm the compliance state for a project and its dependencies in one query, giving you immediate confidence that your supply chain documentation is current.

Black Duck (Synopsys) MCP: 10 Tools for Code Dependency Auditing

Use these tools to list projects, track versions, query vulnerabilities, check BOM statuses, and manage security policies via your AI agent.

#	TOOL	DESCRIPTION
01	`get_bom_status`	Checks if the Bill of Materials (BOM) calculation for a given project version is up to date.
02	`get_project`	Retrieves specific metadata and details about a targeted software project.
03	`list_vulnerabilities`	Generates a list of known vulnerabilities associated with a particular project version.
04	`get_vulnerability_details`	Pulls deep technical details for a specific CVE or vulnerability ID.
05	`list_code_locations`	Lists the exact locations within code where components were scanned.
06	`list_policy_rules`	Provides a comprehensive list of all security policy rules defined for your organization.
07	`list_project_versions`	Lists every version available for a specific software project, defining the scope of the audit.
08	`list_projects`	Retrieves an exhaustive list of all projects managed within Black Duck.
09	`list_users`	Lists every user account and profile within the platform for access auditing.
10	`search_projects`	Searches across all tracked projects using keywords or partial names.

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 critical security risks found in our 'Client Portal' service?

Project: Client Portal

We identified 3 high-risk CVEs linked to outdated libraries:

- **CVE-2024-1234:** Medium severity (Dependency X v1.0).
- **CVE-2023-5678:** Critical severity (OpenSSL component). Requires immediate patching.
- **CVE-2024-9012:** High severity (Logging library Y). Check user access controls for this dependency.

Action recommended: Update OpenSSL and review policy rules.

U Check the compliance status and list all versions for 'Core API' project.

Project: Core API
Versions Found: 4 total (v1.0, v1.1-beta, latest)

BOM Status: ✅ UP_TO_DATE. The Bill of Materials is fully synchronized with the current compliance policy guidelines.

Vulnerability Snapshot (latest): No critical CVEs detected right now.

U Who has admin access and what policies govern them?

Here's a summary of user permissions and governing rules:

Users with Admin Rights: John Doe, Jane Smith (2 accounts)
Governing Policies Found:
1. *Data Access Policy:* Limits read/write based on department.
2. *Audit Scope Policy:* Requires all changes to be logged via user profile tracking.
3. *BOM Integrity Policy:* Enforces get_bom_status before deployment.

Frequently Asked Questions

01 **How does the Black Duck (Synopsys) MCP help me audit my code dependencies?**

This MCP allows you to talk directly to your security tool. You can ask it to list all projects, then request vulnerabilities for a specific version, getting immediate reports on CVEs without using any manual dashboard exports.

02 **Can I use the Black Duck (Synopsys) MCP to check compliance?**

Yes. You can run checks like verifying the Bill of Materials status and listing organizational policy rules, which is critical for proving regulatory adherence during audits.

03 **What kind of information does this Black Duck (Synopsys) MCP provide about users?**

It allows you to list all user profiles within the platform. This helps compliance officers review who has access and what policies govern their activity across different projects.

04 **Is the Black Duck (Synopsys) MCP better than running reports manually?**

Absolutely. Instead of spending hours navigating multiple menus, you ask your agent a single question—like 'What's wrong with Project X?'—and it consolidates the data from all necessary tools into one answer.

05 **Does this MCP only look at open source code?**

No. It gives you visibility across your entire software supply chain, allowing you to check project metadata and dependency risks regardless of where they originate in the codebase.

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 `"black-duck-synopsys": { "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

Black Duck (Synopsys) 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 Black Duck (Synopsys). 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	Black Duck (Synopsys) MCP
Server ID	`019d755d-f2ec-70e4-962b-2b66dd956dd0`
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/black-duck-synopsys.