MCP SERVER | NO CODE | CLOUD HOSTED

Graph Analysis Toolkit MCP for AI Agents

Deep Network Topology Mapping and Connectivity Modeling

Graph Analysis Toolkit performs deep structural analysis on any directed or undirected network map. It calculates critical metrics like node influence, connection density, and component isolation. Use it to find bottlenecks, verify if two networks are structurally identical, or pinpoint exactly which nodes maintain the system's overall connectivity.

A+ Quality Score 100/100

graph-theory | network-analysis | topology | connectivity | centrality

MAINTAINED BY VINKIUS CLOUD FOR AI AGENTS · JULY 2026
vinkius.com/mcp/graph-analysis-toolkit

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.

Graph Analysis Toolkit MCP

5 tools available
Cloud-hosted on Vinkius

When you need to understand how things connect—the relationships between data points, people, or systems—this MCP is your engine. It moves beyond simple lists of connections; it analyzes the structure itself. For instance, if you're mapping a supply chain, this toolkit doesn't just tell you which facilities are connected; it tells you *how* connected they are and where the single point of failure lies. You can find key nodes that act as central hubs or identify smaller groups within a massive network that aren't talking to anyone else. It even checks if two completely different networks, like an old infrastructure map and a new one, share the exact same underlying structure. If you use Vinkius, you connect this MCP alongside dozens of others, giving your AI agent total access to advanced topological analysis for any industry.

Core Capabilities

01 — Determine node connection counts

Get precise figures for how many incoming and outgoing connections each node has within the graph.

02 — Assess overall network connectedness

Measure the degree of interconnectedness across the entire map, helping you identify completely isolated groups or components.

03 — Rank nodes by influence and position

Calculate complex metrics that show which nodes are most central or influential to the overall network structure.

04 — Identify critical structural vulnerabilities

Pinpoint specific nodes or edges whose removal would drastically break the graph's connectivity.

05 — Compare two graph structures for identity

Check mathematically if two separate graphs, regardless of how they are labeled, have the exact same structural pattern.

One Click on Vinkius — From Prompt to Execution

Available at **vinkius.com/mcp/graph-analysis-toolkit** — connect your AI agent in three steps.

01 You provide your AI client with a graph structure—a list of nodes and the edges connecting them.

02 Your agent uses this MCP to run specific analyses, selecting tools like `calculate_centrality_metrics` or `detect_structural_vulnerabilities` based on your question.

03 The tool returns detailed metrics: connection counts, influence rankings, or confirmation that two graphs are isomorphic.

The bottom line is, you give it a network map, and it gives you the mathematical proof of its structural health and weaknesses.

Built For

This MCP is essential for data scientists, network architects, and quantitative analysts. You need this if your job involves mapping complex relationships—be it IT infrastructure dependencies or biological pathways. If you're tired of manually charting connections to find a single point of failure, this toolkit gives your agent the power to model the entire system.

Network Architect

Mapping out physical or logical network paths to ensure redundancy and identify critical backbone components.

Data Scientist

Analyzing datasets of relationships (e.g., user interactions, citation graphs) to find hidden clusters or influential data points.

Supply Chain Analyst

Modeling complex logistical flows to pinpoint nodes that represent single points of failure in the distribution network.

What Changes When You Connect

01 Pinpoint Single Points of Failure: Use `detect_structural_vulnerabilities` to instantly find which critical nodes or edges, if compromised, will break your entire system.

02 Understand Influence: `calculate_centrality_metrics` gives you a score for every node, telling you precisely who or what holds the most weight in the network.

03 Verify Structural Integrity: Need to know if two systems are fundamentally the same? `check_graph_isomorphism` provides a definitive structural comparison.

04 Map Connections Fast: Quickly get connection counts and assess overall interconnectedness using tools like `get_node_degrees` and `analyze_graph_connectivity`.

05 Identify Hidden Groups: Figure out isolated components that might be overlooked. This MCP helps you map every corner of your network, no matter how disconnected it seems.

Real-World Applications

Mapping Infrastructure Dependencies

A utility company needs to know if a single substation failure will cause widespread outages across multiple grids. They ask their agent to run structural vulnerability detection, immediately identifying the primary feeder lines that must be prioritized for redundancy.

Analyzing Social Network Influence

A marketing team wants to find the most influential users in a community chat dataset. The agent runs centrality metrics on the connection graph, delivering a ranked list of nodes whose activity drives the most engagement.

Comparing Legacy and Modern Systems

An IT department receives two network diagrams—one old, one new. They use isomorphism checking to determine if the underlying structure is identical, saving months of manual comparison work.

Identifying Data Clusters in Research

A researcher maps out how genes interact with different proteins. The agent uses connectivity analysis to separate distinct, isolated functional groups that were previously hidden within the large dataset.

Patterns to Avoid

Treating connections as simple links

✗ AVOID

A user assumes finding a high degree count means the node is important. They only use `get_node_degrees` and think they've solved influence mapping.

✓ INSTEAD

Don't just check counts; run `calculate_centrality_metrics` to get true importance scores, or use `detect_structural_vulnerabilities` to understand if a node is merely connected or truly critical.

Ignoring structural comparisons

✗ AVOID

A team wants to know if two datasets relate but only compares the number of nodes. They miss that one network might be an exact copy of another.

✓ INSTEAD

For deep comparison, you must use `check_graph_isomorphism` to prove that the underlying mathematical structure is identical, regardless of labels.

Missing weak links

✗ AVOID

A developer only checks for direct connections between two services. They fail to account for a critical intermediary node.

✓ INSTEAD

Always run `detect_structural_vulnerabilities` first. This flags the hidden, yet essential, nodes and edges that keep the whole system running.

The Right Fit

Use this MCP if your problem is fundamentally about structure: 'Is A connected to B? Who is most important in this group? Is this network resilient?' You need it when you are dealing with topology, dependencies, or relationships that can't be reduced to a simple list. Don't use it if all you need is basic data retrieval—for example, if you just need to count how many users live in California, standard

database tools work fine. If your goal involves determining structural identity between two different maps, this MCP's `check_graph_isomorphism` tool is unmatched. But beware: this toolkit doesn't tell you *why* connections exist; it only measures the resulting structure.

Graph Analysis Toolkit for Network Topology Mapping

Mapping out complex dependencies—like which systems rely on each other or how data flows through a large enterprise—is usually a nightmare. You spend days clicking between dashboard views, cross-referencing dependency charts, and manually drawing connections just to get a rough idea of the system's fragility. It’s tedious copy-pasting across multiple tabs.

With this MCP, your agent handles that entire process in seconds. Instead of guessing at dependencies, you ask it to map the topology. The result isn't a chart; it's an analysis showing exactly which components are isolated or which single link represents a critical point of failure.

Graph Analysis Toolkit for Centrality and Influence Measurement

Traditionally, figuring out who holds the most power in a network—whether it's an employee, a server, or a dataset—requires qualitative assessment. You gather opinions, build consensus reports, and spend hours trying to quantify 'influence.'

Now, you just ask your agent for centrality metrics. The toolkit calculates this mathematically, delivering a quantitative ranking of every node based on its structural importance. You don't guess who matters; the numbers tell you.

Graph Analysis Toolkit: 5 Tools for Network Topology Mapping

These tools allow your agent to perform deep mathematical analysis on graph structures, from finding node degrees to verifying structural identity between networks.

#	TOOL	DESCRIPTION
01	`analyze_graph_connectivity`	Assesses how interconnected a graph is and identifies any completely isolated groups or components within the network map.
02	`calculate_centrality_metrics`	Ranks every node in the graph based on its calculated influence, showing which entities are most important to the system.
03	`check_graph_isomorphism`	Determines mathematically if two separate graphs share the exact same structure, even if they use different labels or nodes.
04	`detect_structural_vulnerabilities`	Flags specific edges and nodes that are critical to maintaining network connectivity; removing them causes failure.
05	`get_node_degrees`	Provides a direct count of the connections for each node, tracking both incoming and outgoing relationships.

See It in Action

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

U Hey, check out this network diagram. Which nodes are acting as bottlenecks, and why?

Structural Vulnerability Report

The following edges/nodes represent critical single points of failure:

- `Edge (A → C)` : If this fails, the connection between A and C is severed.
- `Node B` : This node is a bridge. Losing it disconnects Cluster 1 from Cluster 2.

Recommendation: Focus redundancy efforts on Node B.

U I have two maps of our network, one old and one new. Are they actually the same structure?

Isomorphism Check Result:

✅ **Result: ISOMORPHIC**

The underlying graph structures are identical. The pattern of connections is preserved, even though the nodes and edges have been relabeled.

Similarity Score: 100%

U In this dataset showing user interactions, who has the highest influence score?

Top 3 Centrality Rankings

The most influential nodes are:

1. **User X**: (Centrality Score: 0.89) Acts as the primary hub connecting departments.
2. **Admin Portal**: (Centrality Score: 0.75) Connects all major subsystems.
3. **API Gateway**: (Centrality Score: 0.61)

Frequently Asked Questions

01 **How does the Graph Analysis Toolkit find single points of failure in a system?**

It pinpoints specific nodes or connections that, if they fail or are removed, would break the overall network into smaller, non-connected pieces. This helps you focus on building redundancy where it matters most.

02 **Can this MCP tell me which part of a business process is most critical?**

Yes. By modeling processes as nodes and interactions as edges, the toolkit calculates centrality metrics to give you an objective score showing which parts of your operation are most influential.

03 **Do I need this MCP if I just want to count connections?**

While it can list counts using `get_node_degrees`, the real power is in understanding *why* those connections matter—which nodes are crucial versus which ones are simply numerous.

04 **Is there a way for Graph Analysis Toolkit to compare two different network diagrams?**

Absolutely. The toolkit includes an isomorphism check that mathematically proves if two graphs share the same fundamental structure, even if they use completely different labels or nodes.

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 `"graph-analysis-toolkit": { "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

Graph Analysis Toolkit 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

DOCUMENT INFORMATION

Generated	July 2026
MCP Server	Graph Analysis Toolkit MCP
Server ID	`019f2d2c-a97b-7213-9ca1-7bf8c31e32ff`
Platform	Vinkius Cloud for AI Agents
Endpoint	`https://edge.vinkius.com/{token}/mcp`

LICENSE & USAGE