

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

NYC Flooding (FloodNet) MCP

Get real-time street flooding data and sensor details.

NYC Flooding (FloodNet) MCP provides direct access to New York City Department of Environmental Protection (DEP) records. Your agent can pull specific street-flooding events, sensor installation metadata, and historical flood depths recorded since 2020. It works without needing an API key, making it easy to connect to Claude, Cursor, or Windsurf.

A+ Quality Score 96.67/100

new-york

nyc

flood

floodnet

dep

sensors



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.

NYC Flooding (FloodNet) MCP

5 tools available

Cloud-hosted on Vinkius

You can query the NYC DEP FloodNet sensor network to analyze how streets flood across the five boroughs. This MCP gives your AI client the ability to pull precise data on street-flooding events, including how deep the water got and how long it took to drain. You can look up any of the roughly 500 installed sensors to find its exact location, installation date, and tidal influence. If you need to identify high-risk areas, you can pull a ranked list of sensors that record the most frequent flooding events. The data includes specific metrics like onset duration and the amount of time water stays above certain inch thresholds. It is a direct way to bring granular, city-managed environmental data into your agent's context for research or planning.

Core Capabilities

01 — Event Analysis

Your agent uses this to calculate flood durations and depths from historical records.

03 — Risk Identification

Your agent uses this to rank locations by the frequency of flooding events.

02 — Sensor Mapping

Your agent uses this to find the exact street and borough for any specific sensor ID.

04 — Spatial Filtering

Your agent uses this to narrow down sensor lists by ZIP code or borough.

One Click on Vinkius — From Prompt to Execution

Available at vinkius.com/en/ai-agent-connect/nyc-flooding-floodnet — connect your AI agent in three steps.

- 01
- Connect your MCP-compatible client to the Vinkius platform.
- 02
- Ask your agent to find specific sensors or flood events.
- 03
- The agent calls the FloodNet MCP tools to fetch data from the DEP.
- 04
- Your agent processes the raw sensor metrics into a readable format.

Connect your AI client to Vinkius to start querying NYC flood data immediately.

Built For

This MCP is built for professionals handling urban resilience and environmental data.

Resilience Planners

They use the data to identify high-risk zones for infrastructure upgrades.

Drainage Engineers

They pull depth and duration metrics to model stormwater runoff.

Environmental Journalists

They query specific sensor events to report on local flooding impacts.

What Changes When You Connect

- 01
- Access DEP data without managing API keys.
- 02
- Get precise water depth and duration metrics for specific streets.
- 03
- Filter hundreds of sensors by borough or ZIP code instantly.

04 Identify flood-prone hotspots using event frequency rankings.

Real-World Applications

Urban Risk Assessment

Compare flood frequencies across different boroughs to prioritize city investments.

Infrastructure Modeling

Use sensor depth data to test how new drainage systems might handle specific flood levels.

Real-time Reporting

Query recent flooding events to provide context for weather-related news stories.

Site Selection

Check the tidal influence and historical flood levels of a specific street before development.

Patterns to Avoid

Broad flooding queries

❌ AVOID

Asking your agent to find all flooding in New York City without any filters.

✓ INSTEAD

Use specific filters like borough or ZIP code with ``list_flood_sensors`` to narrow down the data to a manageable area.

Vague sensor searches

❌ AVOID

Trying to find data for a street without knowing the specific sensor ID.

✓ INSTEAD

First use ``list_flood_sensors`` to find the right location, then use ``lookup_flood_sensor`` to get the exact installation details.

General flood inquiries

❌ AVOID

Asking your agent if a certain neighborhood is flood prone without looking at historical counts.

✓ INSTEAD

Run ``top_flood_sensors`` to see which specific locations have the highest frequency of recorded flooding events.

The Right Fit

Connect this MCP if you need granular, street-level flood depth and duration data for NYC infrastructure or risk modeling. Do not connect it if you are looking for general weather forecasts or regional rainfall totals. The decision depends on whether you need specific sensor-recorded event data rather than broad meteorological estimates.

NYC Flooding (FloodNet) 5 Tools

These tools provide direct access to the DEP FloodNet sensor network to track street-level flooding across New York City.

#	TOOL	DESCRIPTION
01	flood_events_by_sensor	This tool retrieves all recorded flooding events for a specific sensor ID. It also returns the total event count and the deepest flood recorded at that location.
02	list_flood_sensors	Use this to get a list of the approximately 500 installed FloodNet sensors. You can filter the results by borough, NTA, or ZIP code.
03	lookup_flood_sensor	This tool pulls the full installation record for a specific sensor ID. It provides the street name, borough, coordinates, and tidal influence data.
04	search_flood_events	This tool searches the historical database of street-flooding events since 2020. You can filter by sensor name or specific date ranges.
05	top_flood_sensors	This tool identifies the most flood-prone locations by ranking sensors based on their recorded event counts.

See It in Action

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

U Which NYC locations have had the most recorded street floods?



The top sensors by event count are: 1. BK-richardson-st-n-11th-st-1×59w1, 2. MN-2nd-ave-e-74th-st-1×2v3z, 3. Q-beach-84-st-1×9p4r.

U How deep did the flood get at the Ditmars St / Hunter Ave sensor?



The deepest recorded flood at the Ditmars St / Hunter Ave sensor was 14 inches, with a total duration of 3 hours.

U Show me the most recent street-flooding events citywide.



The most recent events include: 1. Queens, Beach 84 St (12 inches), 2. Brooklyn, Richardson St (8 inches), 3. Manhattan, 2nd Ave (5 inches).

Frequently Asked Questions

01 Do I need an API key to use this NYC flooding data?

No. This MCP provides keyless access to the DEP FloodNet records.

02 What kind of flood data is available?

You can access start and end times, maximum depths in inches, and the duration water stays above 4, 12, and 24 inches.

03 How many sensors are in the network?

There are approximately 500 installed sensors across New York City.

04 How far back does the flooding data go?

The recorded street-flooding events in this dataset go back to 2020.

05 Can I filter sensors by location?

Yes, you can filter the sensor list by borough, NTA, or ZIP code.

06 Do I need an API key?

No. NYC Open Data serves all public datasets anonymously over its SODA API (data.cityofnewyork.us). This MCP defines no credentials and needs nothing configured.

07 How many FloodNet sensors are installed?

About 500 sensors are installed citywide and the table of flood events has a few thousand rows recorded since November 2020. `list_flood_sensors` shows the installed sensors and their IDs; `top_flood_sensors` ranks them by event count.

08 What does a FloodNet sensor ID look like?

Sensor IDs are slugs of the form "BK-richardson-st-n-11th-st-1×59w1" (borough letter, street intersection and a random suffix). `lookup_flood_sensor` and `flood_events_by_sensor` take the full slug; `list_flood_sensors` shows the installed IDs alongside the human-readable sensor names.

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>"nyc-flooding-floodnet": { "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

NYC Flooding (FloodNet) 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 NYC Flooding (FloodNet). 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	NYC Flooding (FloodNet) MCP
Server ID	01a0dfcd-d9be-712e-b0ac-ad99b6559660
Platform	Vinkius Cloud for AI Agents
Endpoint	<code>https://edge.vinkius.com/{token}/mcp</code>

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/nyc-flooding-floodnet.