

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 Crime & Shootings MCP

Pull official NYPD crime records directly into your AI agent.

NYC Crime & Shootings MCP provides direct access to official city crime records. You can query gunshot incidents, victim and offender details, hate crime complaints, and historic NYPD datasets. It works with any MCP-compatible client like Claude, Cursor, or Windsurf, allowing your agent to verify crime claims against the city's actual system of record without needing an API key.

A+ Quality Score 98.33/100

new-york

nyc

crime

shootings

nypd

public-safety



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 Crime & Shootings MCP

7 tools available

Cloud-hosted on Vinkius

You can now give your AI agent access to the official NYPD complaint system and shooting incident databases. This MCP acts as a direct bridge to NYC Open Data, letting you move past general knowledge and into verified, granular facts. If you need to check if a specific shooting occurred in a certain borough or want to see the demographic breakdown of victims in a recent incident, you can do it through a simple chat interface.

Instead of digging through messy government spreadsheets, you can ask your agent to count incidents by precinct, identify top shooting areas within a specific timeframe, or pull specific hate crime reports. It includes the historic NYPD complaint dataset, which covers arrests and non-arrests recorded in the city's primary system of record. Whether you are verifying a news report or analyzing urban safety trends, this MCP provides the raw, official data needed to back up your findings.

Core Capabilities

01 — Incident Counting

Your agent uses this to quantify crime trends by borough or precinct.

03 — Hate Crime Tracking

Your agent can filter and list bias-motive complaints by category or year.

05 — Geospatial Context

The AI retrieves latitude, longitude, and precinct data for every shooting incident.

02 — Demographic Analysis

The AI pulls age and sex data for victims and offenders from specific shooting records.

04 — Historical Record Search

The agent queries the official NYPD historic complaint database for specific offense descriptions.

One Click on Vinkius — From Prompt to Execution

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

- 01 Connect the NYC Crime & Shootings MCP to your client via Vinkius.
- 02 Ask your agent a question about NYC crime or shootings.
- 03 The agent selects the appropriate tool, like `list_shootings` or `count_shootings`.
- 04 The agent executes the tool and parses the official city data.
- 05 You receive a direct answer based on verified NYPD records.

Connecting to this MCP gives your AI client immediate access to NYC Open Data.

Built For

This MCP is built for professionals who need to verify real-world events against official government records.

Journalists

Use the agent to fact-check crime claims or pull data for local reporting.

Urban Researchers

Hand off data aggregation tasks to the agent to analyze safety trends across boroughs.

Civic Analysts

Use the tool to pull precinct-level data for public safety studies.

What Changes When You Connect

- 01 Access official NYPD data without managing your own API keys.
- 02 Verify crime claims using the city's actual system of record.

-
- 03** Get granular victim and offender details through a single chat interface.
-
- 04** Analyze shooting trends by precinct or borough instantly.
-

Real-World Applications

Fact-Checking News

Verify if a reported shooting matches the official NYPD incident records and location.

Safety Trend Analysis

Identify which precincts have seen an increase in shootings over a specific timeframe.

Hate Crime Research

Pull specific lists of bias-motive complaints to study patterns in certain boroughs.

Demographic Studies

Extract age and sex data from shooting incidents to support urban research projects.

Patterns to Avoid

Vague crime searches

❌ AVOID

Asking your agent to find all crimes in New York City to see if things are getting worse.

✓ INSTEAD

Use `count_shootings` to get specific volumes by borough or precinct instead of asking for general crime data.

Missing incident identifiers

❌ AVOID

Trying to find out who was involved in a shooting without having a specific incident key.

✓ INSTEAD

First use `list_shootings` to find the correct incident key, then use `list_shooting_victims` to get the specific victim details.

Broad hate crime queries

❌ AVOID

Requesting a list of all bias crimes without any filters.

✓ INSTEAD

Use `list_hate_crimes` to filter results by a specific borough, offense category, or year to get useful data.

The Right Fit

Connect this MCP if you need to verify real-world crime reports against official city records. Do not connect it if you are looking for real-time police scanner feeds or non-official social media reports. The decision depends on whether you require the official NYPD system of record for your research or reporting.

NYC Crime & Shootings MCP Tools

These tools provide direct access to official NYPD shooting records and historic complaint databases. You can query specific incident details, victim profiles, and precinct activity levels.

#	TOOL	DESCRIPTION
01	count_shootings	Counts shooting incidents based on your specific filters. Use this to get a quick sense of volume before pulling individual incident details.
02	list_hate_crimes	Retrieves bias-motive crime complaints. You can filter these results by borough, offense category, or a specific year.
03	list_shooting_offenders	Provides details on suspected offenders for a specific shooting. You'll need the incident_key from the list_shootings tool to use this.
04	list_shooting_victims	Returns information on victims involved in a shooting. This requires an incident_key from the list_shootings tool.
05	list_shootings	Lists NYC gunshot and shooting incidents including location, date, and precinct. Use the incident_key from these results to look up specific offender or victim data.
06	search_nypd_complaints	Searches the historic NYPD complaint system for arrests and non-arrests. You can filter by borough, offense description, or a date range.
07	top_shooting_precincts	Identifies the precincts with the highest number of shooting incidents over a chosen number of days.

See It in Action

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

U How many shootings in Brooklyn last year?



The count_shootings tool shows 42 incidents in Brooklyn for the requested period.

U Show the top shooting precincts over five years



Using top_shooting_precincts with a 1825 day window, the highest activity was found in precincts 70, 41, and 44.

U What happened in shooting incident INC-KEY-123?



The incident_key shows one victim, a male in the 20-29 age group, and one suspected offender, a female.

Frequently Asked Questions

01 Do I need an API key to use this?

No. Vinkius hosts the MCP, so you can use these tools without managing your own API credentials.

02 Is this data real-time?

The data comes directly from NYC Open Data and the official NYPD complaint system of record.

03 Can I get specific details about a person in a shooting?

You can use the list_shooting_offenders or list_shooting_victims tools to get age groups and sex, provided you have the incident_key.

04 What is the difference between the shooting tools and the complaint tools?

The shooting tools focus on gunshot incidents, while the search_nYPD_complaints tool accesses the broader historic NYPD complaint system.

05 Which AI clients can I use with this MCP?

You can use this with any MCP-compatible client, including Claude, Cursor, and Windsurf.

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 Are these official records?

Yes. All datasets are published on NYC Open Data by the city: shooting incident/offender/victim extracts from NYPD reporting, the bias-motive complaints series and the historic complaint system of record.

08 How are ages and races reported?

Offender and victim tables report age groups (not exact ages) plus sex and race, as recorded in the incident. The victim table carries a fatality flag (stat_murder_flg).

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-crime-shootings": { "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 Crime & Shootings 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 Crime & Shootings. 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 Crime & Shootings MCP
Server ID	01a0dfcd-051b-7084-8318-e26ca1cd82e9
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/nyc-crime-shootings.