

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

Blast Fragmentation Model MCP

Predict rock size distributions for better blast designs.

Blast Fragmentation Model MCP uses the Kuz-Ram model to predict how rock will break during mining operations. It calculates fragmentation statistics, assesses the risk of producing oversized boulders, and analyzes how changes in explosive energy or blast patterns affect muckpile uniformity. You can run these simulations directly within your AI client to refine your blast patterns before you ever hit the field.

A+ Quality Score 100/100

kuz-ram

fragmentation

mining-engineering

blast-design

rock-mechanics



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.

Blast Fragmentation Model MCP

4 tools available

Cloud-hosted on Vinkius

You can use this MCP to run predictive modeling for your mining operations. It uses the Kuz-Ram model to turn rock mass characteristics and blast parameters into actionable fragmentation data. Instead of guessing how a blast will break, you can input your specific charge, burden, and spacing to get precise P50 and P80 size estimates.

It helps you manage operational risks by identifying the likelihood of producing boulders that exceed your equipment's limits. You can also test different scenarios, like increasing explosive energy or adjusting your pattern, to see how those changes shift the distribution. This allows you to find the sweet spot between fragmentation quality and explosive costs without manual, repetitive calculations. Your agent handles the math, giving you the specific metrics you need to adjust your blast design on the fly.

Core Capabilities

01 — Fragmentation Prediction

Your agent calculates P50 and P80 sizes based on your blast parameters.

02 — Oversize Risk Assessment

The MCP identifies the likelihood of producing boulders that exceed your limits.

03 — Pattern Efficiency Analysis

Your AI client evaluates how pattern changes affect muckpile uniformity.

04 — Energy Impact Simulation

The tool models how changing explosive energy shifts the fragmentation distribution.

One Click on Vinkius — From Prompt to Execution

Available at vinkius.com/en/ai-agent-connect/blast-fragmentation-model — connect your AI agent in three steps.

- 01 Connect your AI client to Vinkius with one click.
- 02 Provide your rock mass and blast parameters to your agent.
- 03 The MCP runs the Kuz-Ram model calculations.
- 04 Receive specific fragmentation metrics and risk assessments in your chat interface.

Get running in minutes by connecting your preferred client to the Vinkius hosted MCP.

Built For

This MCP is built for professionals managing blasting and rock mechanics in mining and quarrying environments.

Blasting Engineer

Uses the tool to refine blast patterns and predict fragmentation results.

Mining Engineer

Relies on the data to optimize downstream processing and equipment efficiency.

Drill and Blast Technician

Uses simulations to verify if proposed patterns meet site requirements.

What Changes When You Connect

- 01 Reduces boulder production by identifying oversize risks early.
- 02 Optimizes explosive energy use by simulating distribution shifts.
- 03 Improves muckpile uniformity through pattern efficiency analysis.

- 04** Speeds up blast design iterations using direct mathematical modeling.
-

Real-World Applications

Blast Design Optimization

You can test different specific charges to find the most efficient energy level for a specific rock type.

Risk Mitigation

Check if a planned blast will produce boulders that are too large for your primary crusher.

Pattern Comparison

Compare two different spacing and burden layouts to see which produces a more uniform muckpile.

Cost Management

Simulate how reducing explosive energy affects fragmentation to balance cost and productivity.

4 Tools Available

#	TOOL	DESCRIPTION
01	calculate_oversize_risk	This tool assesses the probability of producing boulders that exceed your operational limits. It helps you avoid equipment damage and handling issues by flagging high-risk designs.
02	evaluate_pattern_efficiency	This tool analyzes how different blast patterns impact the uniformity of your muckpile. Use it to determine if your current layout will result in consistent fragmentation.
03	predict_fragmentation_distribution	This tool calculates primary fragmentation statistics for a specific blast design. It provides the P50 and P80 sizes you need for planning.
04	simulate_energy_impact	This tool predicts how shifts in explosive energy or specific charge will change the fragmentation distribution. It lets you model the impact of energy adjustments before execution.

See It in Action

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

- U** Calculate the fragmentation distribution for a rock with factor 10, burden 3, spacing 4, diameter 0.15, specific charge 0.5, and explosive energy 1.0.



The predicted median size (P50) is 12.4 cm, the P80 is 25.8 cm, the uniformity index is 1.15, and the oversize percentage is 4.2%.

- U** What is the risk of oversize if my P80 is 35cm and my maximum allowable size is 30cm with a rock factor of 12?



The calculated oversize probability is 28% and the risk level is Medium.

- U** How will increasing explosive energy by 20% affect my fragmentation?



Increasing the energy by 20% is predicted to reduce the P50 from 15.0 cm to 13.2 cm, representing a 12% improvement in median size.

Frequently Asked Questions

01 What mathematical model does this MCP use?

This MCP uses the Kuz-Ram model to calculate rock fragmentation size distributions.

02 Which AI clients can I use with this MCP?

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

03 Can I predict boulder production?

Yes, the `calculate_oversize_risk` tool specifically assesses the likelihood of producing boulders that exceed your operational limits.

04 Do I need to host the MCP myself?

No, Vinkius hosts and manages the MCP for you. You just connect and start using the tools.

05 Can I simulate changes in explosive energy?

Yes, the `simulate_energy_impact` tool predicts how changing explosive energy or specific charge will shift the fragmentation distribution.

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>"blast-fragmentation-model": { "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

Blast Fragmentation Model 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 Blast Fragmentation Model. 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	Blast Fragmentation Model MCP
Server ID	01a07f9b-4610-72f7-a994-c9e6d00963fc
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/blast-fragmentation-model.