

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

Distraction Time Total is a focus MCP.

Turn your interruption logs into clear productivity data.

Distraction Time Total helps you measure exactly how much time slips away during your workday. Your AI client uses this MCP to aggregate distraction events, calculate average interruption lengths, and track how often you lose focus. It turns raw interruption logs into actionable metrics so you can see where your attention actually goes.

A+ Quality Score 100/100

productivity

time-tracking

focus

analytics

distraction



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.

Distraction Time Total MCP

4 tools available

Cloud-hosted on Vinkius

You can't fix what you don't measure. This MCP gives your AI client the ability to dig into your distraction logs and pull out the numbers that matter. Instead of guessing how much time you lost to meetings or notifications, you can get hard data on your focus patterns.

Your agent can sum up every single interruption to find your total lost time or look at specific time buckets to see when you're most vulnerable to losing focus. It also handles the math for you, calculating the average length of an interruption so you know if you're dealing with quick pings or deep-work killers. If your data looks messy, the MCP can check it for errors to ensure your analysis stays accurate. It's a direct way to turn messy interruption records into a clear picture of your daily productivity.

Core Capabilities

01 — Total Time Calculation

Your agent sums up all recorded interruptions to find the total time lost.

02 — Frequency Analysis

The MCP groups interruptions into time buckets to show when you are most distracted.

03 — Average Duration Math

Your AI client finds the mean length of your distraction events.

04 — Data Integrity Checks

The MCP validates your logs to catch errors like negative time entries.

One Click on Vinkius — From Prompt to Execution

Available at vinkius.com/en/ai-agent-connect/distraction-time-total — connect your AI agent in three steps.

- 01
- Connect the MCP to your preferred client like Claude or Cursor.
- 02
- Provide your distraction logs to your AI agent.
- 03
- Ask the agent to run specific tools like total time or frequency metrics.
- 04
- Review the calculated data and patterns provided by the agent.

Connect the MCP to your client and start querying your distraction data.

Built For

This is for anyone trying to reclaim their focus by analyzing their interruption patterns.

Software Developers

They hand off interruption logs to the AI to see how much deep work is being broken up.

Project Managers

They use the metrics to understand team focus trends and scheduling bottlenecks.

Productivity Researchers

They use the data validation and frequency tools to study human attention patterns.

What Changes When You Connect

- 01
- Aggregates raw interruption logs into single, usable numbers.
- 02
- Identifies specific time periods where distractions are most frequent.
- 03
- Detects errors in your distraction records automatically.

- 04 Provides the math needed to understand the impact of interruptions.

Real-World Applications

Deep Work Analysis

Your agent calculates how much time you actually spend in flow versus how much is lost to pings.

Schedule Optimization

Use frequency metrics to find the best times of day to schedule meetings without breaking focus.

Data Cleaning

Run validation on messy logs to ensure your productivity reports are accurate.

Impact Assessment

Determine if frequent short distractions or rare long distractions are hurting your output more.

Patterns to Avoid

Analyzing Dirty Data

❌ AVOID

You try to calculate your total lost time immediately after exporting a messy log from a new tracking app.

✓ INSTEAD

Run ``validate_distraction_data`` first to catch errors or negative entries before you start your analysis.

Ignoring Interruption Length

❌ AVOID

You assume all distractions are equal and only look at the total number of pings you received.

✓ INSTEAD

Use ``get_average_distraction_duration`` to see if you are dealing with quick pings or long interruptions that kill deep work.

Missing Time Patterns

❌ AVOID

You look at your total lost time for the week but can't figure out why you feel so unproductive on Tuesdays.

✓ INSTEAD

Use ``get_distraction_frequency_metrics`` to see exactly which time buckets contain the most interruptions.

The Right Fit

Connect this MCP if you have raw interruption logs and need to quantify how much focus you are actually losing. Do not connect it if you only want to track tasks or project progress. The decision depends entirely on whether you have recorded distraction data to analyze.

Distraction Time Total: 4 Specialized Analysis Tools

These tools turn raw interruption logs into actionable metrics about your focus and time loss.

#	TOOL	DESCRIPTION
01	get_average_distraction_duration	This tool calculates the typical length of your interruption events. It helps your agent understand if your distractions are brief or long.
02	get_distraction_frequency_metrics	This tool breaks down how many distractions occur within specific time windows. Use it to find patterns in when you lose focus.
03	get_total_distraction_time	This tool sums up all recorded distraction events. It gives your agent the total amount of time lost to interruptions.
04	validate_distraction_data	This tool checks your interruption logs for errors or inconsistencies. It ensures your data is clean before you run any analysis.

See It in Action

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

U What is the total time lost if I had distractions of 5, 10, and 15 minutes?



The total time lost is 30 minutes across 3 distraction events.

U What was the average distraction length for 2, 4, and 6 minutes?



The average distraction duration is 4 minutes.

U Check if these distraction durations are valid: [10, 20, -5]



The data is invalid because it contains a negative duration.

Frequently Asked Questions

01 How do I use this MCP with Claude?

You connect the MCP through the Vinkius platform. Once connected, you can ask Claude to use the tools directly in your chat.

02 Can this MCP fix my broken distraction logs?

It uses the validation tool to identify errors like negative durations, but you will need to correct the source data yourself.

03 What kind of data does the MCP need?

The MCP works with recorded distraction durations and timestamps to calculate totals, averages, and frequencies.

04 Does this work with Cursor or Windsurf?

Yes, this MCP is compatible with any MCP-compatible client including Cursor and Windsurf.

05 Can I see when I am most distracted during the day?

Yes, the frequency metrics tool allows your agent to group distractions into time buckets to show you these patterns.

06 How do I calculate my total lost time?

You can use the ``get_total_distraction_time`` tool by providing an array of all your recorded distraction durations.

07 Can I see how frequent my distractions are?

Yes, the ``get_distraction_frequency_metrics`` tool allows you to group distractions into specific time buckets to see patterns.

08 How can I check if my distraction data is valid?

The ``validate_distraction_data`` tool checks the integrity of your data to ensure all durations are positive and numeric.

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>"distraction-time-total": { "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

Distraction Time Total 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 Distraction Time Total. 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	Distraction Time Total MCP
Server ID	01a0ccf7-a636-729b-ab79-97e625e7128f
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/distraction-time-total.