

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

Outbound Briefing is your pre-call intel.

Stop sending generic openers and start using real motion signals.

Outbound Briefing builds concrete, verifiable briefing cards for any target using only public data. It pulls from DNS, certificate logs, job boards, and federal spending records to tell you exactly who a company is, what they just shipped, if they are hiring, and if they just landed a government contract. No accounts or keys required.

A+ Quality Score 98.33/100

outbound

gtm

prospecting

icp-score

motion-signals

hiring-signals



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.

Outbound Briefing MCP

7 tools available

Cloud-hosted on Vinkius

Generic outreach dies because it lacks a hook. You can't win a conversation with assumptions. This MCP solves that by assembling a grounded first line for every call or email you make. It pulls from the target's own homepage, public DNS, certificate logs, and federal spending APIs to give you a complete picture. You get a clear view of their mail infrastructure, their tech stack, and recent subdomains they've launched. If they just won a federal contract, you'll know. If they're hiring for specific roles on a job board, you'll see it. It even scores targets based on these signals so you know who to hit first. Because it relies on public reads, you don't need to manage any extra credentials or accounts. You just connect it to your AI client and start getting the intel you need to write better openers.

Core Capabilities

01 — Identify Motion Signals

Your agent uses this to find new subdomains or hiring activity that justifies an immediate outreach.

02 — Verify Email Deliverability

Your agent checks DNS records to see if a target's mail posture is strict or easy to reach.

03 — Track Federal Spending

Your agent pulls recent government contract awards to find companies with fresh budget.

04 — Score Prospect Lists

Your agent ranks multiple domains by their readiness to buy based on gathered signals.

05 — Analyze Tech Stacks

Your agent reads public certificate logs to see what infrastructure a company is running.

One Click on Vinkius — From Prompt to Execution

Available at vinkius.com/en/ai-agent-connect/outbound-briefing — connect your AI agent in three steps.

- 01 Connect the MCP to your AI client like Claude or Cursor.
- 02 Provide a domain or a list of domains to your agent.
- 03 The MCP reads the target's homepage, DNS, certificate logs, and federal spending data.
- 04 Your agent receives a structured briefing or score.
- 05 You use that data to write a personalized opening line.

The MCP connects your AI client to a variety of public data sources to build instant intelligence.

Built For

This MCP is built for outbound teams who need to move away from generic templates and toward event-based selling.

SDRs

They use the briefing cards to write highly specific opening lines for cold emails.

Account Executives

They use the motion signals to time their outreach when a target is most active.

Founders

They use the ICP scoring to prioritize which leads to pursue during early-stage prospecting.

What Changes When You Connect

- 01 Eliminates generic openings by providing concrete, verifiable events.
- 02 Removes the need for managing multiple API keys or third-party accounts.

-
- | | |
|----|---|
| 03 | Prioritizes outreach based on real-time motion rather than static lists. |
| 04 | Provides a clear view of technical infrastructure and email deliverability. |
-

Real-World Applications

Trigger-Based Outreach

When a company launches a new subdomain, your agent identifies it so you can mention it in your first sentence.

List Prioritization

Take a raw list of domains and have your agent rank them by who has the most active hiring or tech changes.

Government Sector Prospecting

Find companies that just landed federal contracts to pitch compliance or specialized tooling.

Technical Qualification

Check if a target's email setup is strict before you attempt a high-volume email campaign.

Patterns to Avoid

Blind Mass Outreach

❌ AVOID

You send a generic email to a list of 500 companies without checking if they actually have any recent activity or budget.

✓ INSTEAD

Use `multi\_domain\_brief` to get a quick overview of your entire list first. This lets you filter for companies showing actual motion before you write a single word.

Ignoring Technical Readiness

❌ AVOID

You launch a massive email campaign only to find out your messages are being blocked by strict recipient mail filters.

✓ INSTEAD

Run `email\_reachability` on your target list first. It checks their SPF and DMARC posture so you know if your emails will actually land.

Static Prospecting

❌ AVOID

You rely on a stale lead list from last quarter and miss the companies that just won major government contracts.

✓ INSTEAD

Check `federal\_budget\_signals` to find targets with fresh budget. This ensures you are pitching companies that actually have the money to spend right now.

The Right Fit

Connect this MCP if your outbound team relies on event-based selling and needs verifiable hooks for cold outreach. Do not connect it if you prefer high-volume, low-context blasting. The decision comes down to whether you value precision and timing over raw volume.

Outbound Briefing: 7 Specialized Intelligence Tools

These tools pull real-time signals from DNS, certificate logs, and federal spending data to build grounded outreach profiles.

#	TOOL	DESCRIPTION
01	email_reachability	This tool checks public DNS to see a domain's SPF and DMARC posture. It tells you if their email infrastructure is set up to take outreach seriously.
02	tech_shift_signals	This tool identifies recent changes in a target's tech stack. It uses public certificate logs to find new subdomains and identifies what mail services they run.
03	prospect_briefing	This tool generates a full pre-call card for a single domain. It includes their identity, mail posture, tech stack, hiring status, and federal contract activity.
04	sales_motion_signal	This tool flags whether a target has shown recent activity like new subdomains or active hiring. It tells you if it is time to attack or if you should wait.
05	federal_budget_signals	This tool queries public federal spending data for a specific recipient name. It identifies recent contract awards that signal new budget and compliance needs.
06	icp_score	This tool calculates a score for a target based on all available readable signals. It categorizes targets as hot, warm, or cold and suggests your next move.
07	multi_domain_brief	This tool provides a compact enrichment of a list of domains. It returns a single row per domain covering presence, mail posture, job boards, and motion flags.

See It in Action

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

U Give me the full pre-call briefing for acme.io before I talk to them about our API platform.



Pre-call card: acme.io (Acme Corp). Who they are: Developer tools for small teams. Mail: Microsoft 365, SPF present, DMARC quarantine. Runs on: AWS CloudFront and Google Firebase. Hiring: Greenhouse board, 14 open roles, 3 are API platform engineers. Fresh surface: ai.acme.io and partners.acme.io. Federal angle: \$4.5M in contract dollars from DoD and NASA. Move: Open with the partners subdomain and the API hiring news.

U I have this list of prospects: stripe.com, notion.so, linear.app, figma.com, cal.com. Which do I attack first this week?



List brief: linear.app is first because it shows motion with Ashby hiring (9 roles) and 4 new subdomains. cal.com is second with 2 new surfaces. stripe.com and notion.so show no recent motion. figma.com had unreadable sources this time, so re-check it later.

U Did Acme Corp just win federal money? I want the freshest contract angle for the pitch.



Federal budget for Acme Corp: \$6.5M in the last 365 days. Most recent award is a \$4.5M DoD contract that started in July 2026. Angle: Use the August NASA performance start to mention that new teams often re-baseline their tooling when standing up.

Frequently Asked Questions

01 Do I need to provide my own API keys for federal data or job boards?

No. This MCP uses keyless public reads for all data sources, including federal spending and job boards.

02 How fresh is the data?

Readings are cached for one hour. The motion signals specifically look for changes within your defined window.

03 What happens if a data source is unavailable?

The MCP will report the source as unreadable rather than giving you an empty or negative result. This ensures you don't mistake a technical error for a lack of signal.

04 Can I use this with any AI client?

Yes, it works with any MCP-compatible client such as Claude, Cursor, or Windsurf.

05 Is the ICP score a definitive verdict?

No, the score is based only on the signals that were successfully read. If a source is unreadable, it contributes zero to the score.

06 Do I need an API key or an account?

No. Every read is public: the target's own website, the keyless public endpoints of the detected job boards, the public certificate log, public DNS, and the public federal spending API. There is no credential anywhere in the chain — nothing to issue, rotate or store.

07 How is the ICP score computed, and what does a low score mean?

Five readable signals, each with its own points: web presence (15), hiring (20), fresh subdomain motion in 90 days (20), mail-infrastructure maturity (15) and federal contract dollars (30). 70+ is hot (attack now), 40–69 warm (time the next move to the freshest event), below 40 cold (nurture and re-check). Any source that did not answer is listed as unreadable and contributes zero — so the score is what is visible, not a verdict on the whole target; re-read after the flagged sources come back.

08 Is the job-board read a complete census of their hiring?

No — it is the board linked from the homepage, and the open-role count is read only where the provider publishes a keyless endpoint (Greenhouse and Lever give exact counts; other providers report the board's presence but not the number). A board linked only from a careers page, or a provider that is not scanned, does not show up: "no board detected" is a read limit, not proof of no hiring. The result says exactly what it read.

09 What exactly does the federal read measure?

Federal contract dollars paid to the company's registered name in the US, inside your window: the total for the top matching recipient, how many recipients matched, and the three most recently modified awards with public links. It answers one GTM question — "did this target just receive fresh government budget that forces new tooling decisions?" — and it is US-only, by the nature of the source; for a target outside the US federal scope, that angle simply does not apply and the score says so.

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>"outbound-briefing": { "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

Outbound Briefing 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 Outbound Briefing. 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	Outbound Briefing MCP
Server ID	01a0d9c9-f317-72d1-b113-992b58bc8130
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/outbound-briefing.