MCP SERVER | NO CODE | CLOUD HOSTED

BuiltWith Tech Lookup MCP for AI Agents

Identify website CMS and tech stacks through competitive research

BuiltWith Tech Lookup is your universal intelligence tool for profiling websites. It instantly detects the technology stack of any domain, identifying everything from Content Management Systems and analytics tools to hosting providers and JavaScript frameworks. Use this MCP to run competitive research, qualify leads based on their tech use, or audit digital infrastructure with simple prompts.

A+ Quality Score 100/100

tech-lookup | builtwith | website-profiling | cms-detection | market-intelligence

MAINTAINED BY VINKIUS CLOUD FOR AI AGENTS · JUNE 2026
vinkius.com/mcp/builtwith-tech-lookup

SCAN TO VIEW

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.

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.

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.

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	Ed25519	24h TTL	V8 Isolate
Encryption at rest	PKI vault signatures	Ephemeral session keys	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.

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.

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.

06 — Honeytoken Trap System

Phantom credentials are injected into isolated environments. If a honeytoken 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.

Agent Activity

Which AI clients are connecting, how often, and what they're doing — real-time session tracking.

FinOps

Cost tracking per tool, payload compression savings, budget optimization signals, and consumption trends.

Tool Health

Slowest and most error-prone tools, with actionable root-cause insights and performance baselines.

Firewall & DLP

PII redaction activity, sensitive data protection counters, and security event timeline.

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.

BuiltWith Tech Lookup MCP

8 tools available
Cloud-hosted on Vinkius

The BuiltWith Tech Lookup MCP gives your AI agent instant access to the technology stack of millions of websites. Instead of guessing what a competitor uses, you get a detailed breakdown of everything powering a domain—the CMS, analytics tools, advertising networks, and underlying frameworks. Whether you're doing deep competitive research or just vetting a potential lead, your agent acts like a technical consultant through natural conversation. This capability is hosted on Vinkius, the industry's largest catalog for connecting AI agents to specialized data sources.

Your agent can tell you if a site runs on WordPress, Shopify, Magento, or something custom. It pinpoints which tracking tools are integrated and identifies the hosting providers powering the infrastructure. This means your B2B sales team qualifies leads based on tech adoption, web developers find competitor migration gaps, and security researchers map out target domain dependencies—all without visiting a single website manually.

Core Capabilities

01 — Get company information for a domain

Retrieves basic details and identity markers for the specified domain.

02 — Get basic tech categories for a domain

Outputs fundamental technology profiles, useful for initial quick checks without using premium credits.

03 — Get keyword profile for a domain

Provides an analysis of the core search terms and topics associated with the domain.

04 — Get lists of domains using a specific technology

Generates market data by listing multiple domains that rely on one particular technology stack.

05 — Get infrastructure relationships for a domain

Maps out the interconnected services, including CDNs and hosting, used by the domain.

06 — Get usage trends for a technology

Delivers quantitative data showing how frequently specific technologies are being adopted across various domains.

07 — Get trust indicators for a domain

Calculates and returns metrics that suggest the overall reliability or trust level of the website.

08 — Lookup complete technology stack for a domain

Runs a full, deep dive to gather every detected piece of technology powering the site.

One Click on Vinkius — From Prompt to Execution

Available at **vinkius.com/mcp/builtwith-tech-lookup** — connect your AI agent in three steps.

01 Subscribe to the BuiltWith Tech Lookup MCP and enter your unique API key.

02 Your agent receives instructions, such as 'What tech powers tesla.com?'.

03 The MCP uses its built-in tools to query the domain data and returns a structured report detailing the technology stack.

The bottom line is that you simply ask your AI client to analyze a website, and it delivers a comprehensive technical profile in response.

Built For

This MCP is essential for anyone whose job involves researching digital properties or evaluating competitors. It's perfect for the B2B sales rep who needs to know if a prospect uses HubSpot before calling them, or the agency owner tracking which CMS platforms their clients are migrating from.

B2B Sales Representative

Qualifies leads by detecting specific technologies they already use (e.g., finding out if a prospect is on an outdated CRM).

Web Developer or Agency Owner

Researches competitor tech stacks to identify migration opportunities or compatibility issues for new projects.

Security Researcher

Identifies the full infrastructure, including hosting and third-party services, of target domains for vulnerability mapping.

What Changes When You Connect

01 Quickly qualify leads: Your agent can detect which CRM or marketing automation tools a prospect uses, allowing your sales team to tailor pitches immediately.

02 Benchmark competitors: Use the MCP to map out exactly what technologies rivals are using. Spotting niche frameworks or outdated platforms provides immediate competitive edge.

03 Map infrastructure dependencies: The built-in relationships tool reveals hosting and CDN providers, which is crucial for security auditing or planning major digital migrations.

04 Track market trends: Instead of just looking at one site, you can use the technology trends API to see how widely a specific platform (like Shopify) is being adopted in your industry.

05 Efficiently audit sites: You don't need multiple tools. The MCP bundles CMS detection, analytics auditing, and tech stacking into one conversational workflow.

Real-World Applications

A competitor is launching a new feature

The marketing analyst asks, 'What technologies did CompetitorX use last quarter?' The agent runs `get_domain_company_info` and reports that they shifted from Magento to a custom React framework, signaling a major operational pivot.

A lead needs an integration recommendation

The sales rep prompts the MCP with 'Check LeadY's stack.' The agent runs `lookup_domain_tech` and finds they are running on WordPress but lack modern API hooks, allowing the rep to recommend a specific third-party tool.

Auditing internal company assets

The developer needs to know if their division's old site is still using legacy hosting. Running `get_domain_relationships` quickly confirms they are on an outdated provider, signaling a necessary migration project.

Understanding market adoption rates

A product manager wants to know if the industry is moving away from Google Analytics tracking. Using `get_tech_trends`, they get quantitative data showing usage decline for that specific tool over time.

Patterns to Avoid

Searching only by CMS type

✗ AVOID

A user searches for 'WordPress sites' and gets a simple list. This doesn't tell them if those WordPress sites are using modern plugins or outdated hosting.

✓ INSTEAD

Use the BuiltWith Tech Lookup MCP to run `lookup_domain_tech` on specific domains. This ensures you get the full stack details—CMS plus analytics, CDN, and frameworks—for accurate profiling.

Ignoring infrastructure links

✗ AVOID

A competitor's site looks clean and modern. The user assumes it was built in-house without checking who actually hosts or secures the domain.

✓ INSTEAD

Run `get_domain_relationships` with this MCP to uncover the actual hosting providers, CDNs, and security services behind the façade. This reveals the true operational cost.

Assuming basic data is enough

✗ AVOID

A user only checks for general company info using a simple lookup tool. They miss critical details like which keyword strategies are active.

✓ INSTEAD

Use `get_domain_keywords` to pull the domain's specific keyword profile alongside the tech stack data, giving you insight into their marketing focus.

The Right Fit

You should use BuiltWith Tech Lookup if your goal is technical visibility—you need to know *how* a site was built or *what* services it relies on. If you only care about the general business category (e.g., 'it's an e-commerce store'), this MCP might be overkill. Don't use it just because you want a list of technologies; always focus on actionable intelligence. For example, if you need to track how widely a technology is used across an entire industry segment, run `get_tech_domain_lists` or `get_tech_trends`. If your goal is simple contact data and not tech analysis, use a dedicated lead scraping tool instead. But for anything involving the site's underlying architecture, this MCP is necessary.

BuiltWith Tech Lookup: Deep dive into competitor CMS detection

Right now, researching competitors means manually visiting their site and guessing what they use. You have to toggle between developer tools in your browser—checking the source code for analytics scripts or looking up the hosting header. It's tedious clicking through tabs just to figure out if they switched from Magento last year.

With this MCP, you simply ask your agent to identify the CMS used by a domain. It instantly tells you whether the site runs on WordPress VIP, Shopify Plus, or an older platform like Joomla. You get actionable answers immediately.

BuiltWith Tech Lookup: Mapping core infrastructure dependencies

Manually checking a domain's infrastructure involves running multiple checks against different services—one for the CDN, one for the DNS records, and another for the security provider. You end up with three separate reports that don't connect.

This MCP consolidates all that data through tools like `get_domain_relationships`. It connects the dots, showing you which third-party services are actually supporting the domain, giving a single source of truth about its operational backbone.

BuiltWith Tech Lookup: 8 Tools for Domain Analysis & Tech Profiling

Use these tools to pull everything from basic company info to complex tech stack breakdowns and usage trends across the web.

#	TOOL	DESCRIPTION
01	`get_domain_company_info`	Retrieves basic company information associated with a given domain name.
02	`get_free_domain_profile`	Gathers fundamental technology categories and profiles for a specified domain without consuming premium credits.
03	`get_domain_keywords`	Outputs a keyword profile to help understand the search focus of a given domain.
04	`get_tech_domain_lists`	Generates lists of domains that utilize a specific technology, useful for market sizing.
05	`get_domain_relationships`	Maps out the infrastructure relationships and associated services for a domain.
06	`get_tech_trends`	Provides usage trend data, showing how popular specific technologies are across various domains.
07	`get_domain_trust`	Calculates and retrieves trust indicators for a domain based on its online presence.
08	`lookup_domain_tech`	Performs a comprehensive lookup, returning the complete technology stack used by any specified domain.

See It in Action

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

U What tech stack does Netflix use?

Netflix Technology Profile

- **CMS:** Custom internal system (No standard CMS detected)
- **Hosting/CDN:** AWS CloudFront, Akamai CDN
- **Frameworks:** React.js, proprietary backend services
- **Analytics:** Google Tag Manager (via custom implementation)

This indicates a high degree of internal development control and reliance on major cloud providers.

U Check the tech for TechCrunch

TechCrunch Domain Analysis

COMPONENT	DETECTED TECHNOLOGY	NOTES
CMS	WordPress VIP	High-performance, enterprise grade.
Hosting	Cloudflare	Used for DDoS protection and optimization.
Analytics	Google Analytics 4	Standard tracking implementation found.

This profile suggests a focus on high availability and scalability.

Frequently Asked Questions

01 **How does BuiltWith Tech Lookup help me research competitors?**

It gives you deep visibility into exactly what technologies your rivals use. You can find out if they are using outdated platforms or adopting newer, more powerful frameworks, which is key for planning competitive strategies.

02 **Can BuiltWith Tech Lookup tell me if a site uses WordPress?**

Yes, it detects the CMS used by any domain. You can confirm if a site runs on WordPress, Shopify, or another platform without guessing, saving hours of manual investigation.

03 **What kind of data do I get when I check a website's tech stack?**

You receive a complete breakdown that covers CMS detection, the analytics tools installed, the hosting provider, and even the underlying JavaScript frameworks. It's a full technical report.

04 **Is BuiltWith Tech Lookup only for large corporations?**

No. While it works on massive sites, you can use it to check smaller domains too. The results still provide valuable insight into their operational stability and digital maturity level.

05 **Does this MCP show me the domain's keyword focus?**

It does. Beyond technology, you can get a keyword profile for the domain that helps you understand what topics they are trying to rank for in search engines.

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 `"builtwith-tech-lookup": { "url": "…" }`
Windsurf	MCP Settings → `mcp_settings.json` → 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

BuiltWith Tech Lookup 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 BuiltWith Tech Lookup. 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	June 2026
MCP Server	BuiltWith Tech Lookup MCP
Server ID	`019d8421-6b05-73f4-8d5a-d3b31753ced6`
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/mcp/builtwith-tech-lookup.