MCP SERVER | NO CODE | CLOUD HOSTED

OneTrust MCP

Automate compliance reporting across all data types.

OneTrust MCP manages your entire data privacy compliance stack. Automate everything from handling Data Subject Access Requests to mapping personal data across systems, assessing vendor risk, and tracking security incidents using natural conversation with any AI client.

A+ Quality Score 100/100

gdpr | ccpa | hipaa | data-privacy | compliance-automation | risk-assessment

MAINTAINED BY VINKIUS CLOUD FOR AI AGENTS · JUNE 2026

vinkius.com/mcp/onetrust

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.

OneTrust MCP

10 tools available
Cloud-hosted on Vinkius

Handling data governance used to mean opening a dozen separate dashboards just to get one answer. Now, you can connect your OneTrust account to your preferred AI agent via Vinkius, and manage privacy compliance through simple conversation. Your agent acts as a unified interface for all things sensitive: from managing Data Subject Requests (DSARs) to checking vendor risk profiles. It pulls data on which systems process personal information, reviews required consent purposes, and tracks incident severity levels—all without you having to click through complex menus. This MCP brings together everything needed to prove GDPR or CCPA compliance into one workflow. You simply ask your AI agent for the status of overdue assessments or a list of open DSARs, and it gives you an immediate, actionable summary.

Core Capabilities

01 — Audit data subject rights requests

Create, track, and get full details on any privacy request—like deletion or access—for compliance reporting.

02 — Map personal data flows

List every system that processes personal data, showing its purpose, legal basis, and risk classification.

03 — Assess third-party vendor security

View the status and risk scores of all connected vendors to verify due diligence requirements.

04 — Review privacy impact findings

List and retrieve full details on internal assessments, like DPIAs, used to measure project risk.

05 — Manage security incidents

Track all reported privacy breaches or near-misses, noting the severity and regulatory notification status.

One Click on Vinkius — From Prompt to Execution

Available at **vinkius.com/mcp/onetrust** — connect your AI agent in three steps.

01 Subscribe to the MCP on Vinkius and enter your OneTrust API token from the Admin Console.

02 Your AI agent connects directly to your OneTrust instance, granting it read/write access to compliance data.

03 Ask a specific question—for example, 'Show me all vendors with overdue assessments' or 'List open DSARs'—and your agent executes the necessary workflow.

The bottom line is you get an immediate, conversational summary of complex compliance data without ever leaving your AI client.

Built For

This MCP is built for seasoned privacy and security professionals. If you're the Data Protection Officer who spends half his day chasing down audit evidence, or the Privacy Team member tired of manually cross-referencing consent records with data inventories, this tool saves your sanity.

Data Protection Officer (DPO)

Uses it to monitor compliance posture by listing risks and tracking all security incidents across the organization.

Privacy Counsel

Needs to quickly generate data maps to prove legal basis for processing or verify data retention policies.

Security Compliance Manager

Uses it to perform vendor due diligence and review required assessments before a new partnership goes live.

What Changes When You Connect

01 Eliminate manual dashboard hopping. Instead of opening 5 different reports for DSARs, you simply ask your agent to 'List open DSARs' and get a consolidated status report instantly.

02 Prove due diligence easily. You can use `onetrust_list_vendors` to pull risk scores and assessment statuses in minutes, not days, which is crucial for board meetings.

03 Know exactly what data you have. Use `onetrust_list_assets` to generate the full data map, showing every system that processes personal data and why—essential for GDPR Article 30 compliance.

04 Stay ahead of breaches. If a security incident happens, your agent can use `onetrust_list_incidents` to report severity and track if regulatory notifications are required.

05 Streamline consent management. Reviewing cookie banners is easier when you run `onetrust_list_consent_purposes`, seeing exactly which trackers map to which marketing category.

Real-World Applications

Responding to a large data audit request

The Security Manager needs to show auditors that they track all risks and vendor compliance. They ask their agent to 'List privacy and security risks' and then immediately run `onetrust_list_vendors` to prove every partner has an up-to-date assessment.

Handling a CCPA deletion request

A user submits a deletion request. Instead of manually opening the system, the agent uses `onetrust_create_dsar` to register it immediately, ensuring the correct 30-day clock starts ticking.

Mapping new product data flows

The Product Owner needs to know where customer PII is going. They ask the agent to 'List data inventory assets' which generates a clear map of all systems processing personal data and their legal basis.

Reviewing vendor compliance before signing a contract

The Procurement team needs assurance that a new partner meets standards. They run `onetrust_list_vendors` to check the risk score, assessment status, and if a Data Processing Agreement is signed.

Patterns to Avoid

Trying to manually track audit evidence

✗ AVOID

Opening dozens of PDF reports or logging into multiple dashboards just to find out which vendor's assessment is overdue and why.

✓ INSTEAD

Use `onetrust_list_vendors` to get a single, consolidated list showing the name, risk score, and precise status (overdue/completed) of every third-party partner.

Forgetting regulatory deadlines

✗ AVOID

Receiving an access request but not knowing if it's over 30 days old or what the specific legal basis for deletion is.

✓ INSTEAD

Use `onetrust_list_dsars` to pull all requests, immediately highlighting which ones are overdue and requires action.

Assuming data mapping is complete

✗ AVOID

Stating that 'all customer data is safe' without being able to prove exactly where it lives or what purpose the system uses it for.

✓ INSTEAD

Run `onetrust_list_assets` to generate an auditable, definitive list of every application and database processing personal information.

The Right Fit

Use this MCP if your primary pain point is proving compliance across multiple regulated domains (GDPR, CCPA). You need a single source of truth for risk assessment, vendor management, data inventory, and privacy requests. Don't use it if you just need to manage general employee records or HR tasks—that requires a separate system connector. If your goal is simply to view internal documents without linking them to compliance status, a basic document search tool will suffice. But if the core of your job involves tracking regulatory deadlines, assessing data flows using `onetrust_list_assets`, or running through vendor risk checks with `onetrust_list_vendors`, this MCP is necessary.

The headache of proving compliance when an auditor walks in.

Today, if you need to prove your data governance posture for a major audit, you're clicking through half a dozen dashboards. You pull the vendor list from one place, but the risk scores are tracked in another spreadsheet. Finding out which systems process personal data requires manually checking multiple department heads and piecing together asset reports.

With this MCP, your agent handles the mess. Just ask it for an inventory of all assets that hold customer data. You get a structured map showing the legal basis, retention period, and purpose in one go. The result is clean, actionable compliance documentation.

OneTrust MCP: Control your entire privacy lifecycle.

The biggest manual step that vanishes is the investigation of data subject requests. You used to have to track a request through multiple departments, checking if it was an access or deletion request and manually calculating the remaining time until the deadline.

Now, you initiate the process with `onetrust_create_dsar` and monitor its progress using `onetrust_get_dsar`. The system handles the workflow. You simply ask your agent for the status, and it tells you exactly what needs to happen next.

OneTrust: 10 Tools for Data Governance

These tools let you programmatically manage every aspect of compliance, from listing assets to creating DSARs, giving you total control over your privacy data.

#	TOOL	DESCRIPTION
01	`onetrust_get_assessment`	Retrieves full details for a specific privacy impact assessment, including identified risks and recommendations.
02	`onetrust_create_dsar`	Registers a new data subject access request (DSAR) on behalf of an individual, calculating the necessary regulatory deadlines.
03	`onetrust_list_assessments`	Lists all completed privacy impact assessments (PIAs/DPIAs), showing their risk score, status, and owner.
04	`onetrust_list_vendors`	Shows a list of third-party vendors, their risk scores, assessment status, and contractual safeguards.
05	`onetrust_get_dsar`	Pulls the complete history and status of one individual's data subject request for detailed investigation or reporting.
06	`onetrust_list_assets`	Generates the full data map by listing every system that holds personal data, its purpose, and legal basis.
07	`onetrust_list_consent_purposes`	Reviews all configured consent purposes in your cookie banner, detailing categories, associated trackers, and default settings.
08	`onetrust_list_dsars`	Provides a dashboard view of all data subject access requests (DSARs), showing their status, deadline, and type.
09	`onetrust_list_incidents`	Lists security and privacy incidents, detailing the severity, affected subjects count, and regulatory notification status.
10	`onetrust_list_risks`	Aggregates all identified enterprise risks from the risk register, including impact level, likelihood score, and treatment plan.

See It in Action

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

U How many open data subject requests do we have?

You have **7 open DSARs**:

- **2 overdue** — Both are deletion requests (GDPR Art. 17) past the 30-day deadline
- **3 in progress** — 1 access request, 2 portability requests (due in 12, 18, 22 days)
- **2 new** — Submitted today, auto-routed to the Privacy Team

The 2 overdue requests need immediate attention — shall I show the details?

U Which vendors have overdue security assessments?

There are currently 4 vendors with overdue security assessments:
1. CloudHost Inc. (High Risk) - Overdue by 15 days
2. DataFlow Analytics (Medium Risk) - Overdue by 8 days
3. MailSender Corp (Low Risk) - Overdue by 3 days
4. CDN Partners (Medium Risk) - Overdue by 1 day
Would you like me to trigger automated reminders for these vendors?

U Show the data map for our CRM system.

Here is the data map for the CRM System:
- **Personal Data Processed:** Names, email addresses, phone numbers, purchase history.
- **Purpose:** Customer relationship management, direct marketing.
- **Legal Basis:** Legitimate interest (CRM), Consent (Direct Marketing).
- **Retention Period:** 5 years after last contact.
The CRM system is fully compliant with current policies.

Frequently Asked Questions

01 **What is the difference between `onetrust_list_assets` and `onetrust_get_dsar`?**

`onetrust_list_assets` gives you a map of your entire data ecosystem—every system that processes PII. `onetrust_get_dsar` provides deep details on one specific request, showing its history and fulfillment steps.

02 **Can I use OneTrust MCP to check vendor status?**

Yes, you can list third-party vendors using `onetrust_list_vendors`. This tool shows the current risk score and whether their security assessments are overdue or pending a contract.

03 **How does OneTrust MCP manage data deletion requests?**

You use the `onetrust_create_dsar` tool to log a deletion request. The system automatically tracks the regulatory deadline and initiates the required internal workflow for removal.

04 **Does this MCP help with security incident reporting?**

Yes, you can use `onetrust_list_incidents` to pull all logged privacy breaches or near-misses. This tool shows severity and whether regulatory notifications are required.

05 **What is the purpose of running `onetrust_list_risks`?**

`onetrust_list_risks` aggregates your enterprise risk register. It gives you a consolidated view of identified risks, their potential impact, and what treatment plan (like mitigating or accepting) has been assigned.

06 **How do I get started with OneTrust?**

Subscribe, then enter your OneTrust API token (from **Admin Console → Integration → API Access**) and your base URL (e.g., app.onetrust.com or app-eu.onetrust.com). Your AI agent connects instantly. No code, no SDK — just connect and start managing privacy compliance.

07 **Can my AI agent handle GDPR data subject access requests?**

Yes. Create DSARs directly from conversation — specify the subject's name, email, and request type (access, deletion, rectification, portability, opt-out). OneTrust automatically calculates regulatory deadlines (30 days for GDPR, 45 days for CCPA) and routes the request to the right handler.

08 **How do I check which vendors have overdue security assessments?**

Ask your agent "show me vendors with overdue assessments" and it lists every third-party vendor with their risk score, questionnaire status, and last review date. You see exactly which processors need follow-up — all without logging into OneTrust or switching tabs.

09 **Is this suitable for multi-regulation compliance (GDPR + CCPA + HIPAA)?**

Absolutely. OneTrust is built for multi-regulation environments. Browse your entire data inventory mapped to processing purposes and legal bases, track DSARs across any regulation, manage privacy impact assessments, and monitor incidents with regulatory notification requirements — perfect for enterprises, healthcare organizations, and global companies operating across jurisdictions.

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 `"onetrust": { "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

OneTrust 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 OneTrust. 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	OneTrust MCP
Server ID	`019d75e5-ed80-709e-9960-f5b0aa88d1e6`
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/onetrust.