MCP SERVER | NO CODE | CLOUD HOSTED

Contrast Security MCP

Audit AppSec posture right from your chat.

Contrast Security MCP connects your AI agent directly to AppSec monitoring data. Instantly audit application security posture and pinpoint critical vulnerabilities across your entire software portfolio, all from a chat window. It eliminates dashboard digging by giving you direct access to vulnerability traces, server status, and application details.

A+ Quality Score 100/100

appsec | runtime-security | vulnerability-management | security-monitoring | devsecops

MAINTAINED BY VINKIUS CLOUD FOR AI AGENTS · JUNE 2026
vinkius.com/mcp/contrast-security

SCAN TO VIEW

The infrastructure that powers AI agents in the real world.

Vinkius connects AI to the world's software through secure, enterprise-grade infrastructure — enabling real-world execution at scale, built on the Model Context Protocol (MCP).

Your AI Connections Run Through Vinkius Cloud

The world's largest managed MCP catalog

Vinkius is the cloud infrastructure where AI agents connect 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.

Contrast Security MCP

10 tools available
Cloud-hosted on Vinkius

This MCP brings powerful Application Security (AppSec) insights right into your conversation flow. Instead of logging into the complex Contrast UI just to check if your apps are secure, your AI agent handles it. You can query specific security risks, list every app monitored by your sensors, or pull detailed reports on vulnerabilities without ever leaving your chat interface. It's like having a dedicated security analyst sitting next to you who knows exactly where to look. Whether you need to prioritize remediation efforts or just verify that all your production environments are covered, this MCP delivers the data instantly. The Vinkius catalog makes connecting these specialized tools simple; you authorize it once and get access to complex monitoring capabilities across any compatible client.

Core Capabilities

01 — Assess overall application coverage

List all applications currently monitored by Contrast Security sensors.

02 — Identify immediate critical risks

Filter and list only the highest-severity (CRITICAL) vulnerabilities across your entire codebase.

03 — Deep dive into specific flaws

Pull complete technical details on any single vulnerability trace using its unique UUID.

04 — Check system operational status

View which servers have active Contrast agents deployed and running.

One Click on Vinkius — From Prompt to Execution

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

01 First, subscribe to this MCP and authorize it using your specific Contrast Application API keys and Organization ID.

02 Next, ask your AI agent a natural language question, like 'List all critical vulnerabilities on the payment engine.'

03 The agent calls the appropriate tool, pulls the precise vulnerability data, and summarizes the findings for you in plain English.

The bottom line is, you get immediate security answers by talking to your AI client, instead of clicking through dashboards.

Built For

This MCP is essential for Security Engineers and DevOps Leads who spend too much time context-switching between ticketing systems, monitoring dashboards, and IDEs. It helps developers get specific security details without leaving their coding environment.

Security Engineer (SecOps)

They query the system to list all monitored applications or find critical vulnerabilities while actively writing a remediation ticket.

Developer

They ask the agent for full technical details on a flagged vulnerability trace, getting the exact code location without opening external security platforms.

DevOps Lead

They run checks to confirm which servers have active Contrast agents deployed across their fleet applications automatically through conversation.

What Changes When You Connect

01 Instantly audit application security by listing all monitored apps using the list_applications tool, ensuring you never miss a production environment.

02 Prioritize remediation efforts immediately. Use list_critical_vulnerabilities to pull only high-severity flaws, cutting through noise and focusing on what matters.

03 Go deep into specific issues. Calling get_vulnerability_details gives you the full technical breakdown of any vulnerability trace UUID, pinpointing vulnerable code lines.

04 Stay aware of your infrastructure health by running list_monitored_servers to confirm where agents are deployed across your entire fleet.

05 Quickly check coverage or search for specific systems using search_applications_by_name without navigating complex web forms.

Real-World Applications

Initial Security Audit

A new SecOps Engineer needs to know if all staging environments are protected. Instead of clicking through three separate dashboards, they ask their agent to list_applications, getting a comprehensive, single view of every monitored system.

Incident Triage

A developer is working on a fix and needs to know the exact nature of a flaw. They use get_vulnerability_details with the UUID, pulling the precise technical context—like which controller file and line number is vulnerable—without leaving their IDE.

Compliance Check

A DevOps Lead needs proof that only critical flaws are addressed first. They use list_critical_vulnerabilities to immediately pull a filtered list of the highest-risk items, streamlining compliance reporting.

System Verification

The team lead suspects an old application might not be monitored. They run search_applications_by_name for 'Legacy' and get confirmation or find new targets they need to add immediately.

Patterns to Avoid

Manual dashboard diving

✗ AVOID

Trying to check the status of all apps by clicking through three different web dashboards, cross-referencing dates and IDs manually.

✓ INSTEAD

Just ask your agent to list_applications. It pulls the current state and coverage in one step.

Ambiguous search queries

✗ AVOID

Typing 'show me security stuff' into a generic chat box and getting an overwhelming wall of unprioritized data.

✓ INSTEAD

Be specific. Use list_critical_vulnerabilities to filter noise down to the absolute highest-risk items only.

Ignoring context

✗ AVOID

Seeing a vulnerability ID but not knowing if it relates to production or staging.

✓ INSTEAD

Always use get_application_details first. This confirms the app's environment and gives you full context for the flaw.

The Right Fit

Use this MCP when your primary need is structured, deep AppSec data retrieval from a specialized platform like Contrast Security. You should use it if you are asking questions that require filtering (like listing critical flaws), cross-referencing (getting application details for a vulnerability ID), or auditing scope (listing monitored servers). Don't use this MCP if your goal is simple chat messaging, general organizational info, or accessing non-security related APIs. For basic team communication, you need a generic messaging tool; for simply retrieving user names, list_organization_users might suffice, but for technical security monitoring, this is the right choice.

The Pain of Security Context Switching

Today, checking your application's security status means a tedious dance across multiple tabs. You have to log into the main dashboard, find the app list, then click on 'Backend-API,' navigate to the vulnerabilities tab, and finally search through dozens of results just to get the UUID for a specific flaw. It takes minutes, and you risk losing context or misinterpreting data.

With this MCP, that entire process disappears. You ask your agent what's up with the payment engine, and it pulls the full security picture—including all critical flaws and which server hosts the app—directly into your chat window. The result is immediate, actionable intelligence without opening a single external tab.

Get Vulnerability Details Instantly

Before this MCP, getting full technical details for a vulnerability trace meant hunting down the UUID, then navigating to a separate 'Deep Dive' report page. You'd copy the raw data and paste it into your ticketing system, often losing necessary context like the affected endpoint or line number.

Now, you just ask the agent to get_vulnerability_details using the trace ID. It pulls everything—the full technical write-up, the vulnerable file path, and the status—and gives it to you immediately. The data is ready for your ticket, period.

Contrast Security: 10 Tools for AppSec Data

Use these tools to pull structured data on application coverage, vulnerability status, server health, and organizational metadata directly into your conversation.

#	TOOL	DESCRIPTION
01	`get_application_details`	Retrieves detailed information about a specific application monitored by Contrast Security.
02	`get_organization_info`	Gets general metadata and details about your current Contrast organization setup.
03	`get_vulnerability_details`	Pulls the complete technical breakdown for a single, specified vulnerability trace UUID.
04	`list_applications`	Provides a comprehensive list of all applications that Contrast Security is monitoring.
05	`list_critical_vulnerabilities`	Quickly generates a filtered list containing only vulnerabilities classified as CRITICAL severity.
06	`list_monitored_servers`	Lists all servers where Contrast agents are currently deployed and active in the system.
07	`list_vulnerability_traces`	Generates a list of security vulnerability traces found across your application portfolio.
08	`list_organization_users`	Lists all user accounts within the Contrast Security organization.
09	`search_applications_by_name`	Filters and searches for monitored applications using a specific name or keyword.
10	`search_vulnerabilities`	Allows filtering and searching of vulnerabilities using complex criteria like severity or type.

See It in Action

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

U List all applications monitored in my Contrast Security organization.

I've fetched 3 active applications monitored under your umbrella: `Frontend-API`, `Backend-Payment-Engine`, and `Legacy-Staging-App`. Would you like to dig into the security score of a specific one?

U List all CRITICAL vulnerabilities found across my entire Contrast fleet.

I found 2 traces classified as CRITICAL priority. 1) SQL Injection mapping to UUID `1xx-bbxx-11x` on application 'Backend-API'. 2) Deserialization exploit UUID `4yxx-bbx-22` on 'Legacy-Staging-App'.

U Retrieve the full technical details for the vulnerability trace UUID '1xx-bbxx-11x'.

Decompressing trace `1xx-bbxx-11x` ... It's flagged as an untrusted SQL Injection caused by vulnerable code in controller `AuthRoute.js` line 45. The status is open and currently untriaged.

Frequently Asked Questions

01 **How do I list applications using Contrast Security MCP?**

You call the list_applications tool. This provides a comprehensive list of every app monitored by your sensors in one shot.

02 **Can I filter for only critical vulnerabilities with list_critical_vulnerabilities?**

Yes, that's exactly what list_critical_vulnerabilities does. It filters out all the lower-severity noise so you focus only on the highest risks.

03 **What is get_vulnerability_details for in Contrast Security MCP?**

get_vulnerability_details lets you pull the full, technical breakdown of any single vulnerability trace UUID. It's your deep-dive tool.

04 **Does this MCP show me which servers are monitored?**

Yes, running list_monitored_servers shows you all the physical or virtual servers where Contrast agents are currently deployed and active in your organization.

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 `"contrast-security": { "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

Contrast Security 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 Contrast Security. 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	Contrast Security MCP
Server ID	`019d757b-9272-730f-99af-bbdeb2af7637`
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/contrast-security.