MCP SERVER | NO CODE | CLOUD HOSTED

Intruder MCP

Audit cloud assets & vulnerabilities instantly

Intruder provides automated vulnerability scanning and security monitoring by connecting directly to the Intruder.io API. Use this MCP to audit cloud infrastructure, track security issues, list targets, and review historical scan reports for DevSecOps workflows.

A+ Quality Score 100/100

cybersecurity | vulnerability-assessment | security-monitoring | cloud-security | threat-detection | audit-logs

MAINTAINED BY VINKIUS CLOUD FOR AI AGENTS · JUNE 2026
vinkius.com/mcp/intruder

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.

Intruder MCP

10 tools available
Cloud-hosted on Vinkius

Managing security compliance used to mean clicking through dozens of dashboards and cross-referencing spreadsheets. Now, your agent can handle the heavy lifting. This connector lets you pull all necessary data points into a single conversation thread. You can start by seeing which assets need vetting using the list targets tool, then check for vulnerabilities across the board with the list issues tool. From there, you can drill down to get the remediation advice on any specific problem found with the get issue tool. It’s essential for automating security audits and maintaining a clear picture of your cloud infrastructure's health. Just connect this MCP through Vinkius, and your AI client gets immediate access to all these deep-level auditing capabilities.

Core Capabilities

01 — Reviewing Security Vulnerabilities

Fetch comprehensive lists of identified security issues, including severity levels (Low, Medium, High, Critical).

02 — Tracking Asset Scope

List all infrastructure and application targets that the system includes in its scans.

03 — Auditing Cloud Connections

View which cloud platforms (AWS, Azure, Google Cloud) are configured to feed target data into Intruder.

04 — Reviewing Scan History

Pull detailed records of past vulnerability assessments and the assets they covered.

05 — Checking Account Credentials

Verify your account identity, check licensing status, or list organizational teams for access control checks.

One Click on Vinkius — From Prompt to Execution

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

01 Tell your agent which security scope you need to audit; this might mean starting with listing all configured cloud integrations.

02 Ask the agent to pull a list of vulnerabilities or scan records. This generates a large dataset that needs filtering and prioritization.

03 Use the detailed results, such as getting a specific issue description, to generate immediate remediation steps for your team.

The bottom line is you get actionable security reports directly into your conversation thread without leaving your primary workflow tool.

Built For

This MCP is for the DevSecOps engineer who can't trust a dashboard to tell them everything, or the Security Auditor who needs proof of compliance across multiple cloud environments. If you spend time manually correlating vulnerability reports with asset lists, this is for you.

DevSecOps Engineer

Automates post-deployment security checks by querying the list scans tool and cross-referencing findings with target metadata.

Security Auditor

Performs compliance checks by listing all configured cloud integrations and reviewing account licenses to prove coverage across environments.

Platform Architect

Verifies the security status of new or existing assets by getting target details and understanding organizational team access controls.

What Changes When You Connect

01 Pinpoint exact remediation steps immediately. Instead of just seeing a critical vulnerability, you can use the get issue tool to pull detailed advice on how to fix it.

02 Maintain an accurate security inventory by using list targets and get target together. You'll know exactly which assets are currently being scanned and what their metadata is.

03 Verify cloud coverage without logging into three different provider consoles. The list cloud integrations tool shows you all connected AWS, Azure, and Google Cloud sources in one place.

04 Keep track of compliance over time. Using list scans gives you a verifiable history, letting you prove how often your vulnerability checks run for an audit.

05 Simplify user management by listing teams or getting account details. You can verify organizational access controls without calling multiple internal directories.

Real-World Applications

Auditing a new cloud deployment

A platform architect needs to ensure all three major clouds are covered. They ask their agent, which uses list cloud integrations, to confirm AWS, Azure, and Google Cloud connections exist. The agent confirms the integration status across all platforms.

Responding to a compliance audit request

A security auditor must prove that vulnerabilities are tracked weekly. They use list scans to get a chronological record of assessment runs, and then list issues to summarize the current risk level for management.

Debugging an unknown vulnerability

An engineer finds a suspicious finding but needs more context. They identify the issue using list issues, then use get issue on that specific ID to pull detailed remediation advice and understand exactly which target was affected.

Preparing for a major system migration

A team lead is migrating systems and needs an asset checklist. They run list targets first to see every asset name, then use get target on each one to pull all relevant metadata before the migration even starts.

Patterns to Avoid

Assuming full coverage

✗ AVOID

A manager sees a vulnerability report and assumes the problem is fixed. They only check the last few results, missing issues from older scans.

✓ INSTEAD

Always use list targets to see all assets included in scope, then call list scans to ensure you are reviewing history, not just the most recent snapshot.

Ignoring cloud sources

✗ AVOID

A team assumes their security coverage is complete because they checked one dashboard, missing critical targets hosted on a secondary cloud platform.

✓ INSTEAD

Start by calling list cloud integrations to confirm every source—AWS, Azure, Google Cloud—is connected and feeding data into the system.

The Right Fit

Use this MCP if your job requires continuous security compliance checking across diverse, multi-cloud environments. If you need a single point of truth for vulnerability status, asset inventory, or scan history, this is it. Don't use it if you only need to check basic account credentials; that's just an API call. You also shouldn't rely on it to *fix* the vulnerabilities—it gives remediation advice via get issue, but your team still has to do the work. If all you want is a simple list of

users and nothing related to infrastructure or compliance, this MCP provides too much context.

The Security Audit Process Is a Click-Heavy Nightmare

Today, auditing security risks means logging into the cloud provider console, then hopping over to the vulnerability dashboard. You pull one report, copy the asset ID, paste it into a second tool to check metadata, and if you find an issue, you have to open a third system just for remediation advice. It's hours of context switching and manual data correlation.

With this MCP, your agent handles the whole chain. You ask one question—like 'What is our current risk profile?'—and it pulls together the list issues report, confirms all cloud integrations are active, and even provides specific get issue advice for every high-severity finding.

Get a Complete Security Picture with Intruder MCP

The manual steps that disappear include cross-referencing asset lists against scan reports, checking license expiration dates across multiple accounts, and summarizing findings from various cloud sources. Your agent handles the sequencing.

You stop compiling data and start making decisions. The output is a cohesive narrative of risk, not just a pile of raw JSON objects.

Intruder: 10 Tools for Security Auditing

These tools give you granular control over every aspect of your security posture, from listing specific vulnerabilities to checking account licenses.

#	TOOL	DESCRIPTION
01	`get_account`	Retrieves your core Intruder account details to verify identity.
02	`get_issue`	Fetches detailed descriptions, remediation advice, and affected targets for a specific security flaw.
03	`get_scan`	Retrieves the full list of included targets, scan duration, and summary findings for one assessment run.
04	`get_target`	Gets metadata and associated tags to deeply examine a specific asset's security status.
05	`list_cloud_integrations`	Lists all configured cloud integrations (AWS, Azure, Google Cloud) for auditing purposes.
06	`list_issues`	Provides a list of identified vulnerability issues, including severity and status, for general posture checks.
07	`list_licences`	Lists all account licenses to verify subscription status and capacity.
08	`list_scans`	Retrieves a record of all vulnerability scans, including types and timestamps for historical tracking.
09	`list_targets`	Lists every infrastructure and application target that is currently available to be scanned.
10	`list_teams`	Displays a list of all organizational teams set up within the account for access control understanding.

See It in Action

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

U List all active targets in my Intruder account.

I'll fetch the list of your infrastructure and application targets.

U Show me the latest vulnerability issues found.

I'll retrieve the most recent security issues identified by Intruder.

U Check the status of my recent scans.

I'll look up the history and current status of your vulnerability scans.

Frequently Asked Questions

01 **How do I find out which assets are included in my security scans using Intruder MCP?**

You list targets to see all infrastructure and application endpoints that the system is currently scanning. This tool gives you a definitive count of your scope.

02 **What if I need remediation advice for a specific vulnerability found by Intruder MCP?**

Use the get issue tool, passing in the unique ID of the finding. It returns detailed descriptions and actionable steps to fix the flaw immediately.

03 **Can Intruder MCP check if all my cloud providers are integrated for auditing?**

Yes, you call list cloud integrations. This tool audits your setup across AWS, Azure, and Google Cloud, confirming connectivity status in one place.

04 **Does Intruder MCP help me track historical scan performance?**

You use the list scans tool to retrieve a record of all past assessments. This lets you prove compliance by showing consistent monitoring over time.

05 **What does get target do with my asset information in Intruder MCP?**

The get target tool retrieves deep metadata and associated tags for any specific asset, allowing you to verify its exact role or owner within the infrastructure.

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 `"intruder": { "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

Intruder 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 Intruder. 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	Intruder MCP
Server ID	`019d75bb-0e60-7020-9b30-d464254f80f9`
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/intruder.