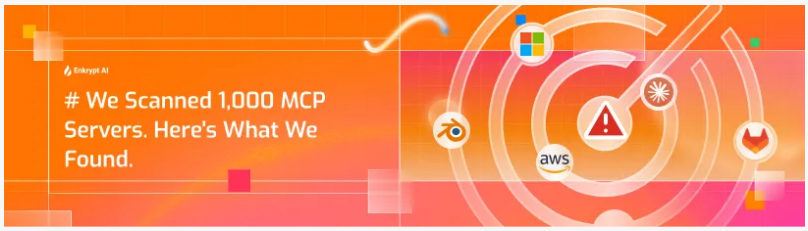
Enkrypt AI Launches First MCP Security Scanner After Study Finds One Third of Servers Critically Vulnerable

Research highlights urgent risks in AI agent infrastructure; Enkrypt AI's MCP Scanner delivers protocol specific protection at scale.



Enkrypt AI unveils MCP Scanner following analysis of 1,000 MCP servers that revealed alarming security gaps.

BOSTON, MA, UNITED STATES, October 9, 2025 /EINPresswire.com/ -- **Enkrypt AI**, a leader in AI security and compliance, today announced the launch of **MCP Scanner**, the first security platform designed specifically for Model Context Protocol (MCP) servers. The announcement follows an industry first study by Enkrypt AI that revealed nearly **one in three MCP servers contain critical vulnerabilities**.

> MCP is becoming to AI agents what APIs were to Web 2.0 — a universal gateway to critical systems, but without dedicated security, it could quickly become the soft underbelly of enterprise AI."
>
> *Sahil Agarwal, CEO of Enkrypt AI*

In an analysis of more than **1,000 MCP servers** across GitHub, enterprise registries, and open source deployments, the company found:

- **32 percent contained at least one critical vulnerability**
- Servers averaged **5.2 vulnerabilities each**
- Some popular projects had **20 or more flaws**, including command injection and authorization bypasses
- **Zero percent included security documentation**

MCP has quickly become the standard for connecting AI agents to production systems such as databases, Kubernetes clusters, SaaS tools, and cloud infrastructure. Yet the findings show that traditional scanners miss MCP specific risks, leaving enterprises exposed to significant attack surfaces.

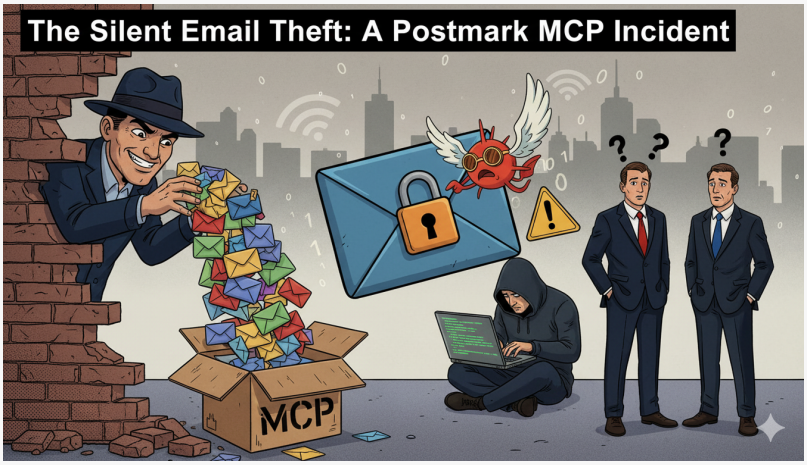
Real World Risks Already Emerging

The research highlights critical exposures already seen in practice:

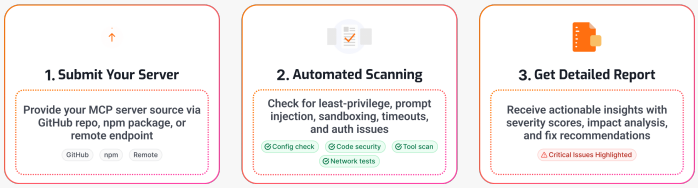
- A widely used **Kubernetes MCP server** contained **26 vulnerabilities**, including six critical command injection flaws (CVSS 9.8), leaving entire clusters open to takeover.
- A malicious **Postmark MCP server** was discovered exfiltrating every email it processed while appearing fully legitimate to users.

In coverage of this issue, **VentureBeat** recently warned of the risks of insecure MCP defaults.

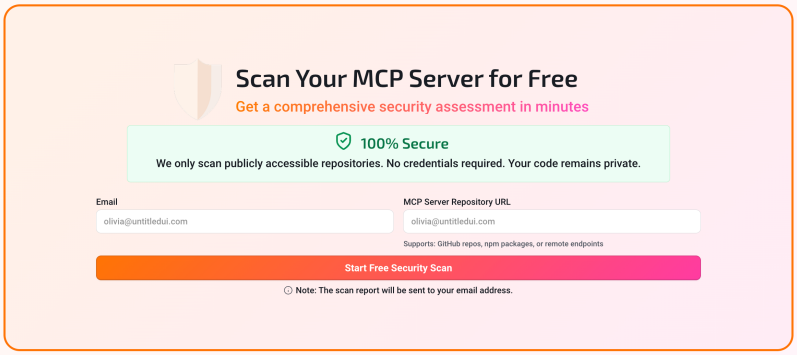
“MCP is shipping with the same mistake we have seen in every major protocol rollout: insecure defaults,” said Merritt Baer, Chief Security Officer at Enkrypt AI, in an interview with VentureBeat. “If we do not build authentication and least privilege in from day one, we will be cleaning up breaches for the next decade.”



Researchers uncovered a malicious Postmark MCP server that silently exfiltrated every email it processed — a real-world incident demonstrating the urgent need for MCP security.



How Enkrypt AI’s MCP Scanner works: submit your server, run automated protocol-aware scanning, and receive a detailed report with severity scores and remediation guidance.



Enkrypt AI is offering free MCP server security scans — comprehensive assessments delivered in minutes, with zero credentials required.

MCP Scanner: Purpose Built Protection

Enkrypt AI’s **MCP Scanner** provides a four layer assessment across:

- **Configuration** — Authentication, sandboxing, timeouts
- **Code security** — Command injection, path traversal, denial of service vectors
- **Tool level checks** — Hidden malicious tools, permission escalation
- **Network posture** — TLS validation, SSRF, open ports

Reports are delivered in minutes, including **CVSS severity scores, line level references, and remediation guidance**. MCP Scanner integrates with **CI/CD pipelines, registries, and runtime gateways**, enabling enterprises to block vulnerabilities before deployment.

Since the private beta, MCP Scanner has scanned more than **1,000 servers**, remediated **1,000 vulnerabilities**, and onboarded **500 organizations**, achieving **zero false positives** in critical findings.

Availability

MCP Scanner is available immediately, with **free assessments** for individual servers. Organizations can submit a GitHub repo, package, or endpoint at www.enkryptai.com/mcp-scan.

About Enkrypt AI

Enkrypt AI is a purpose built AI security and compliance platform that helps enterprises safely deploy agents by detecting, removing, and monitoring risks such as data leakage, jailbreaks, hallucinations, and compliance gaps. Its unified platform combines red teaming, guardrails, and compliance automation to deliver end-to-end protection across the AI lifecycle. Trusted by Fortune 500 companies in finance, healthcare, and insurance, Enkrypt AI was founded in 2022 by Yale PhD experts and is backed by Boldcap, Berkeley SkyDeck, ARKA, and Kubera.

For any questions, please reach out:

 hello@enkryptai.com or connect on **LinkedIn/Twitter**.

Sheetal Janala
Enkrypt AI
sheetal@enkryptai.com
Visit us on social media:
LinkedIn
YouTube
X

This press release can be viewed online at: https://www.einpresswire.com/article/856821636

EIN Presswire's priority is source transparency. We do not allow opaque clients, and our editors try to be careful about weeding out false and misleading content. As a user, if you see something we have missed, please do bring it to our attention. Your help is welcome. EIN Presswire,

Everyone's Internet News Presswire™, tries to define some of the boundaries that are reasonable in today's world. Please see our Editorial Guidelines for more information.
© 1995-2025 Newsmatics Inc. All Right Reserved.