Natoma

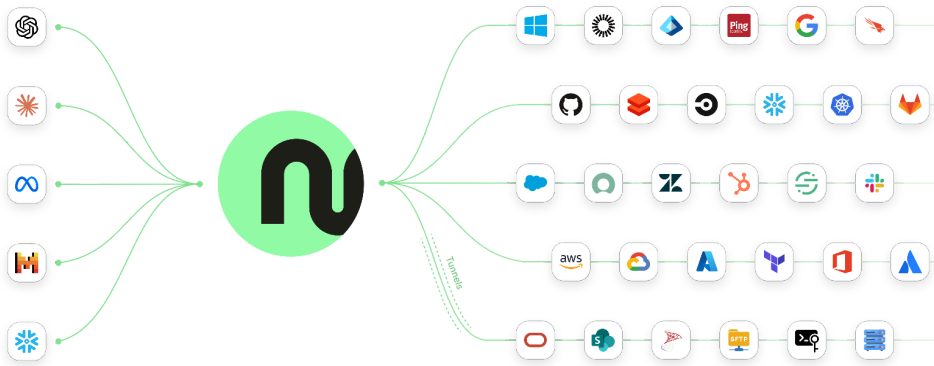
Agent Access

AI's promise—both practical and magical—has become the topic among CIOs, CISOs, and technical practitioners alike. One of the most thrilling developments is the rise of agentic AI: systems capable of operating with considerable autonomy. While the potential that agentic AI unlocks is groundbreaking, it also introduces new challenges. Organizations must grapple with new access paradigms, in which over-permissioned systems can act without human oversight. AI agents themselves face constraints due to fragmented enterprise systems and data stored in legacy systems, that hinder their efficacy.

> *By 2028, over 33% of enterprise software will incorporate Agentic AI.*
>
> Gartner

Beyond the complexity of integrating these agents with an organization's tools and data, security leaders must also contend with the risks associated with these non-human actors, especially when their activities blur the line between interactive user and automated client. To securely adopt agentic AI, it's critical for security leaders to gain visibility into agentic AI usage across the business, adopt strong policy management, and adhere to strict access & governance standards.

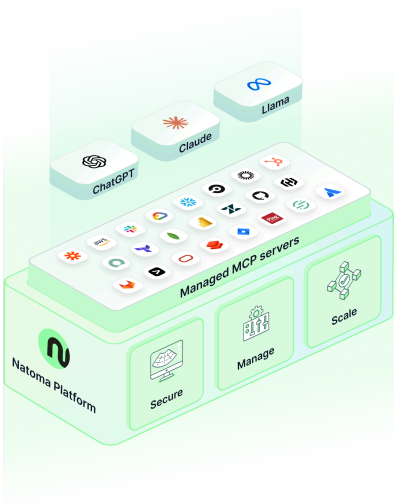
The Natoma Edge



As we usher in a new wave of Agentic AI adoption, organizations must adopt seamless, secure, and scalable ways of integrating agents with their tools and data. Natoma Agent Access is a hosted MCP Platform that leverages Model Context Protocol (MCP) to deliver the fastest, easiest, and most intuitive way to

empower your AI agents to interact seamlessly with your applications and data. Gone are the days of complex API integrations, version management, and tedious server configurations. Natoma delivers simplicity, so you can focus on what matters most. And it's easy to deploy and manage – in literally three steps, our cloud-hosted MCP servers can help you deploy agentic AI at scale:

- Connect LLMs & AI apps to tools & data sources in a consistent, structured way
- Authenticated tool access & governance policies control access and monitor AI agent behavior
- Secure tracing and audits for full visibility over every tool and action, backed by robust logs and reporting



Business Outcomes

Grow confidently

Effortlessly scale and manage your deployments with automation and infrastructure-as-code capabilities.

Fine-grained authorization

Maintain control over what end users can see and do based on their roles and responsibilities.

Accelerate time to value

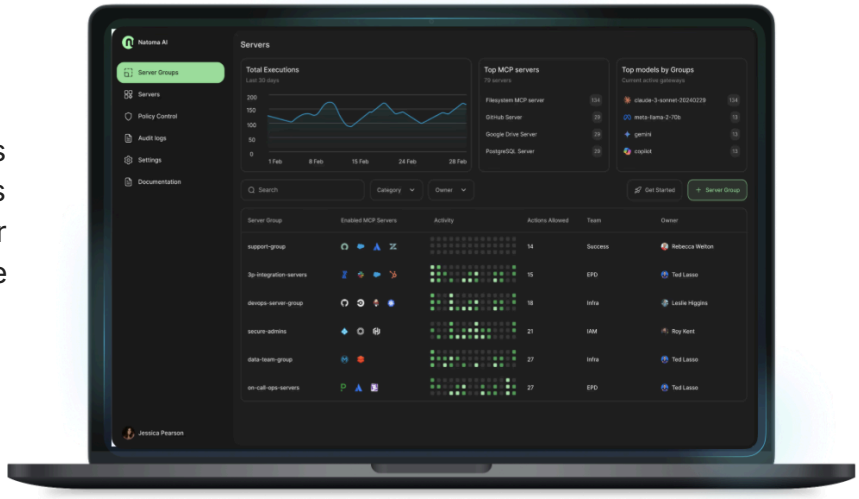
Get the most out of your AI investments by enabling employees to connect LLMs like Claude, OpenAI, or Gemini to your tools and data. This allows you to derive more value, securely and scalably.

Secure Data Handling

Safeguard your data in transit & at rest by leveraging the robust security controls of the hosted MCP platform.

Policy Controls & Audit Logs

Establish granular access policies and ensure compliance with reporting & audit logs.



For more information, visit mcp.natoma.id or connect with our directly team at natoma.id/book-a-demo.