Governance Studio
by Adapted Media Pty Ltd

OPENAI AGENT TUNNELS MAY CHANGE PRIVATE SYSTEM BOUNDARIES

OPERATIONAL SIGNAL

DOMAIN: RISK — Risk Surface **I CONFIDENCE LEVEL:** Preliminary
INSTITUTIONAL DIMENSIONS: Authority I Attribution I Visibility I Escalation I Continuity

Signal ID	Platform	Source	Audience	Status	Date
SIG-RISK-001	OpenAI	Link	PMO I Risk I Engineering	Pilot	2026-05-22

CAPABILITY SHIFT

OpenAI released Secure MCP Tunnel on 19 May 2026 for enterprise customers. It lets supported OpenAI products connect to private or on-prem MCP servers through a customer-hosted tunnel client, without exposing those servers to the public internet. This creates a supported path between AI agents and selected private systems.

ORGANISATIONAL CONSEQUENCE

Technical teams may now give AI agents a supported path into internal databases, ticketing systems, knowledge bases, or private APIs. These systems may have been separated from cloud AI by network architecture rather than explicit AI policy. A configured tunnel can change that boundary for connected systems.

WHAT TO WATCH

- Tunnel clients or MCP gateways deployed internally
- AI agents referencing private data sources
- Outbound connections to AI platform endpoints
- Security reviews assuming cloud AI cannot reach internal systems

WHY THIS MATTERS NOW

OpenAI has made this capability available for enterprise accounts. If similar gateway patterns spread across platforms, internal access reviews may need to move from “is this system public?” to “has this system been connected to an agent?”

WHAT TO REVIEW

- Approval processes for AI tunnel or gateway deployment
- Inventory of internal systems exposed through MCP servers
- Monitoring for outbound tunnel connections
- Least-privilege controls for connected systems
- Ownership of agent access to private tools or data

GOVERNANCE CONTEXT

This is a risk surface and authority issue. The network perimeter may no longer be the only practical boundary. For connected systems, review shifts to which internal resources were exposed, who approved access, and what activity is logged.

Scope Boundary: This artefact translates observed platform capability changes into operational considerations. It does not constitute policy, legal advice, or enforcement guidance.