Protocole MCP — le nouveau standard des ag
2026

16 mai 2026 • Mis à jour le 17 mai 2026 • 15 min de lecture • 3013 mots •

Comprenez le protocole MCP (Model Context Protocol) en 2026 : architec
sécurité, déploiement enterprise. Comment MCP remplace les intégrations
pour les agents IA et ses implications RSSI.

À RETENIR

A retenir -- Protocole MCP 2026

Le **MCP (Model Context Protocol)**, developpe par Anthropic et adopte comm
ouvert en 2025, est en passe de devenir le protocole universel pour connect
aux outils, ressources et services externes. Il remplace les integrations API a
(Function Calling OpenAI, plugins ChatGPT) par un standard uniforme : tout s
expose un serveur MCP est immediatement utilisable par tout LLM compatibl
RSSI, MCP cree une surface d'attaque unifiee qui doit etre securisee via des

> de permission strictes, une validation des inputs/outputs, et un audit trail des
> MCP.

Le **Model Context Protocol (MCP)** est un des developpements les plus significatifs l'ecosysteme IA en 2025-2026. Developpe initialement par Anthropic et publie en 2024, MCP a rapidement ete adopte par d'autres ecosystemes (OpenAI, Google D comme standard de facto pour l'integration des LLM avec les systemes exterieurs plus juste est le protocole HTTP pour le web : de la meme facon qu'HTTP a permis quel navigateur de communiquer avec n'importe quel serveur web selon un protoc MCP permet a n'importe quel agent LLM de communiquer avec n'importe quel out donnees, API ou service qui expose un serveur MCP. Avant MCP, chaque integrati necessitait un code custom specifique (function calling OpenAI, tool use Anthropi un serveur MCP ecrit une seule fois expose ses capacites a tous les LLM compati analyse l'architecture MCP, ses mecanismes de securite, les risques nouveaux qu son impact sur les architectures enterprise en 2026.

Architecture MCP -- clients, serveurs et protocole

L'**architecture MCP** suit un modele client-serveur ou :

- Le ***MCP Client*** est l'application LLM (Claude Desktop, un agent Python, une app enterprise) qui initie des requetes vers les serveurs MCP pour utiliser leurs cap clients decident quels serveurs MCP connecter et comment utiliser leurs outils.
- Le ***MCP Server*** expose des "primitives" (outils, ressources, prompts) que le LL Un serveur MCP peut exposer n'importe quelle capacite : lecture/ecriture de fic d'APIs tierces, requetes SQL, execution de code, etc.