



LIVRE BLANC

MCP : rendre vos données utilisables par l'IA

Le Model Context Protocol permet à un assistant IA d'interroger vos outils et vos données en toute sécurité. Cas d'usage, architecture et étapes pour vous lancer.

En quelques mots

Vos équipes utilisent déjà des assistants IA, mais ceux-ci ne connaissent ni vos clients, ni vos stocks, ni vos procédures. Ce guide montre comment le Model Context Protocol (MCP) leur donne un accès encadré à vos outils et à vos données.

Il présente, sans jargon, six cas d'usage concrets, l'architecture type d'un serveur MCP, les règles de sécurité et de confidentialité à respecter, et la démarche pour mettre en service un premier agent en quelques jours. Destiné aux directions, DSI et responsables métier.

Ce que vous allez apprendre

- ✓ Ce qu'est le Model Context Protocol, en termes simples
- ✓ 6 cas d'usage concrets en entreprise
- ✓ L'architecture type d'un serveur MCP
- ✓ Les règles de sécurité et de confidentialité
- ✓ La démarche pour un premier serveur MCP en quelques jours

L'IA sans vos données reste générique

Les assistants IA (Claude, ChatGPT, Copilot...) sont excellents pour rédiger, résumer ou analyser. Mais tant qu'ils n'ont pas accès à vos données (clients, commandes, stocks, documents, plannings), leurs réponses restent générales, et vos équipes passent leur temps à copier-coller.

Le MCP en une phrase

Le **Model Context Protocol (MCP)** est un standard ouvert qui permet à un assistant IA de se connecter à vos outils et à vos données, avec des droits d'accès précis : lire un dossier client, créer un devis, consulter un stock... Un serveur MCP joue le rôle de « traducteur » sécurisé entre l'IA et votre système d'information.

6 cas d'usage concrets

- ✓ **Service client** : l'assistant retrouve la commande et l'historique avant de répondre
- ✓ **Commerce** : préparer un devis à partir du catalogue et des tarifs réels
- ✓ **Direction** : interroger ses indicateurs en langage naturel
- ✓ **Collectivités** : croiser données publiques et données internes (élus, associations, entreprises)
- ✓ **Qualité / conformité** : vérifier un dossier contre une liste de règles
- ✓ **Interne** : retrouver une procédure ou un document dans une base documentaire

L'architecture type

1. Vos sources : ERP, CRM, base de données, API, fichiers
2. Un serveur MCP qui expose quelques actions claires (« rechercher un client », « créer un devis »)
3. Une authentification et des droits par utilisateur
4. Un journal de chaque appel, pour savoir ce que l'IA a consulté ou fait
5. L'assistant IA de votre choix, qui utilise ces actions

Sécurité et confidentialité

Un serveur MCP bien conçu n'ouvre jamais toute la base : il expose uniquement les actions utiles, avec les droits de l'utilisateur connecté. Les actions sensibles (modifier, supprimer, envoyer) demandent une confirmation humaine, et l'ensemble est hébergé dans un cadre maîtrisé, en France ou au Canada sur OktoCloud.

Démarrer en quelques jours

1. Atelier : choisir 1 à 3 cas d'usage à fort impact
2. Prototype : un serveur MCP connecté à une source de données réelle
3. Supervision : tests, droits d'accès, journalisation
4. Déploiement et accompagnement des équipes

Nos données ouvertes ([OktoCloud Open Data](#), plus de 35 millions d'entrées) sont un bon terrain d'essai : elles permettent de tester un agent sur des données réelles avant de brancher les vôtres.



Passons à votre projet

Décrivez-nous votre besoin : nous revenons vers vous avec un devis et un premier prototype fonctionnel, sans engagement.

Estimer mon projet

Oktopod · Cité Numérique du Pensio, 4 rue du Pensio Nd de France, 43000 Le Puy-en-Velay
04 44 05 32 35 · contact@oktopod.io · oktopod.io