

Brancher l'IA sur tes outils

Ce qu'un connecteur ajoute, et les questions à poser avant d'accorder un accès

Module BR1 - COMPRENDRE - 13 min - version 1.1

Tu demandes une information qui se trouve dans ton agenda, ton stockage ou un autre outil. Sans accès à cette source, une application d'IA ne peut pas déduire fidèlement ce contenu privé simplement parce que tu le mentionnes. Une connexion peut lui donner un moyen de consulter une source ou d'appeler une action - selon les permissions réellement accordées.

Le module ne suppose pas qu'un produit donné appelle ses intégrations « connecteurs », qu'il utilise MCP, ni qu'il expose les mêmes permissions qu'un autre produit.

Ce que tu sauras faire en sortant

- Dire si une tâche a réellement besoin d'un accès externe ou si la matière peut être fournie autrement.
- Distinguer une capacité de lecture d'une capacité qui agit ou modifie.
- Poser quatre questions avant connexion : besoin, périmètre, conséquence, révocation.
- Demander une preuve de la source réellement utilisée lorsque la réponse dépend d'un document externe.

L'essentiel, en trente secondes

Une intégration peut permettre à une application d'IA d'accéder à des données, des outils ou des workflows externes. La portée exacte dépend du produit, de l'offre et des permissions.

Quatre questions suffisent pour commencer :

- Pourquoi ai-je besoin de cet accès ?
- À quoi donne-t-il réellement accès ?
- Que peut-il faire ou modifier ?
- Comment l'accès se réduit-il ou se révoque-t-il ?

Si l'une de ces réponses est inconnue, le bon résultat de l'exercice est « à vérifier avant connexion ».

Un connecteur ne remplace pas une source

Dans un cas simple, tu peux copier un extrait autorisé dans une conversation. Avec une intégration, l'application peut parfois récupérer elle-même la matière nécessaire.

Le bénéfice potentiel est d'éviter certaines navettes manuelles. Ce module ne mesure ni minutes gagnées, ni réduction d'erreurs, ni qualité supérieure du texte. Ces gains dépendent du processus réel et doivent être mesurés chez toi si tu veux les revendiquer.

La contrepartie : tu ne vois plus forcément toute la matière intermédiaire au moment où la réponse est produite. La vérification devient donc plus importante, pas moins.

MCP : un exemple de protocole, pas le nom générique de toutes les intégrations

La documentation officielle du Model Context Protocol décrit MCP comme un standard ouvert permettant de relier des applications d'IA à des systèmes externes, notamment des sources de données, outils et workflows.

Source : Model Context Protocol - introduction

(<https://modelcontextprotocol.io/docs/getting-started/intro>), rouverte le 19/08/2026.

La spécification décrit des hôtes, clients et serveurs et un mécanisme standardisé d'échange. Cela permet de comprendre un type d'architecture.

Ce que cette source ne prouve pas :

- qu'une fonction appelée « connecteur » dans un produit utilise MCP ;
- qu'une intégration MCP particulière est sûre ou correctement configurée ;
- que deux clients exposent les mêmes permissions ;
- qu'une application « comprend » automatiquement le métier ou la portée de tes documents.

Lecture et action : regarder les permissions réelles

Deux catégories sont utiles pour raisonner :

- consulter / lire : obtenir des données ou documents ;
- agir / modifier : créer, envoyer, mettre à jour, supprimer ou déclencher une opération.

Une permission de lecture peut déjà exposer des informations sensibles. Une permission d'action ajoute un autre type de conséquence. Le module ne dit donc pas « lecture = sans risque » ; il demande de regarder le contenu accessible et l'effet possible.

Règle Solutio : privilégier le plus petit périmètre suffisant et reporter toute action externe tant que la validation humaine, le mécanisme de contrôle et la révocation ne sont pas clairs.

Micro-défi

Quatre tâches fictives :

- reformuler un mail déjà affiché à l'écran ;
- retrouver régulièrement une référence stockée dans un dossier dédié ;
- traduire un message court déjà fourni ;
- structurer des notes déjà collées.

Attendu : la 2 est la seule qui présente ici un besoin évident d'accès à une source externe. Cela ne veut pas encore dire qu'il faut connecter l'outil : il reste à examiner le périmètre et les données.

Quand la réponse dépend d'une source externe

Demande à la sortie de fournir des éléments permettant de retrouver la matière utilisée : titre ou identifiant du document, date si elle existe, et extrait pertinent.

``text Indique la source précise utilisée pour cette réponse. Donne le titre ou identifiant du document et recopie le passage qui soutient l'information. Si tu ne peux pas retrouver la source, marque l'information « non vérifiée ».

Même avec cela, tu ouvres la source toi-même lorsque l'information compte. Une citation fournie par le même système n'est pas encore une vérification indépendante.

Le cas où ça se passe mal

Cas reconstitué.

Tu demandes le résumé d'un document qui n'est pas dans le périmètre réellement accessible. La sortie fournit malgré tout un texte cohérent.

Le contrôle n'est pas « le résumé a l'air plausible ». Tu demandes la source précise et tu l'ouvres. Si le document ne peut pas être identifié ou récupéré, tu ne traites pas le résumé comme celui du document demandé.

Données personnelles : ne pas qualifier automatiquement le fournisseur

La CNIL définit le sous-traitant comme l'acteur qui traite des données personnelles pour le compte d'un responsable de traitement. Elle précise aussi, pour les fournisseurs de systèmes d'IA, que la qualification doit être appréciée au cas par cas : selon la configuration, un fournisseur peut avoir un autre rôle.

Sources rouvertes le 19/08/2026 :

- CNIL - définition du sous-traitant (<https://www.cnil.fr/fr/definition/sous-traitant>)
- CNIL - déterminer la qualification juridique des fournisseurs de systèmes d'IA (<https://www.cnil.fr/fr/determiner-la-qualification-juridique-des-fournisseurs-de-systemes-dia>)

Conséquence pédagogique : ne conclus pas « mon fournisseur est sous-traitant » à partir du seul fait qu'un connecteur existe. Vérifie le cadre contractuel et le rôle réel avec la personne compétente.

Ce qu'une connexion ne règle pas

- Elle ne garantit pas l'exactitude de la réponse.
- Elle ne remplace pas F3 : le périmètre accessible doit être acceptable pour le traitement envisagé.
- Elle ne prouve pas que la permission affichée correspond à ce que tu imagines ; observe et teste le périmètre.
- Elle ne garantit pas que la fonction restera disponible dans une autre offre ou une autre version.
- Elle ne transforme pas une source non vérifiée en fait.

Quand tu t'arrêtes

- Tu ne sais pas ce que l'accès voit ou peut modifier.
- Tu ne sais pas révoquer l'accès.
- Le périmètre contient des données qui n'ont pas passé le tri F3.
- L'action peut toucher un tiers, de l'argent ou un processus engageant et le contrôle humain n'est pas défini.
- Tu ne peux pas retrouver la source utilisée pour une information importante.

À toi

L'exercice ne demande aucune connexion réelle.

Pour trois tâches de ton travail, remplis :

| Tâche | Source nécessaire | Permission minimale imaginée | Conséquence d'une erreur | Preuve à demander | Révocation à vérifier | |---|---|---|---|---| | ... | ... | ... | ... | ... |

Puis passe la colonne « source nécessaire » au tri F3.

Réussi si tu élimines une connexion inutile, ou si tu peux justifier précisément le besoin et le périmètre d'une connexion à tester ultérieurement sur terrain neutre.

Vérifie ton geste

- La réponse dépend d'un document externe mais ne l'identifie pas. Source non vérifiée.
- Le produit demande lecture + action alors que ton besoin est seulement de lire. Cherche un périmètre plus étroit ou reporte.
- Tu ne trouves pas la révocation. Ne connecte pas encore.
- Le dossier contient des données de la pile rouge F3. Le gain attendu ne change pas le tri.
- Une intégration utilise MCP. Cela décrit un protocole, pas la conformité ni la sécurité de sa configuration.

Seuil de réussite : 4 sur 5, questions 2 et 4 obligatoires.

Selon ce que tu obtiens

- Aucun besoin de connexion résultat valide : garde le processus simple.
- Besoin réel mais périmètre trop large réduis le périmètre ou renonce.
- Source introuvable ne garde pas l'affirmation importante.
- Tu hésites sur le rôle RGPD/contractuel le module s'arrête ; qualification au cas par cas.

Fiche mémo

- Besoin avant connexion.
- Périmètre minimal observé.
- Lecture absence de risque ; action = conséquence supplémentaire.
- Source importante document identifiable et ouvert.
- Données de tiers F3 + cadre approprié.
- Révocation connue avant activation.

Ce que tu viens de pratiquer

- Tu as séparé protocole, permission et résultat.
- Tu as retiré les promesses de minutes gagnées et les règles universelles de comportement.
- Tu sais que le rôle juridique d'un fournisseur ne se déduit pas du mot « connecteur ».

Sources et statut : docs/br1-PROVENANCE.md`. BR1 reste S2 et brouillon jusqu'au fact-check, à la recette et au contrôle de date prévus.