



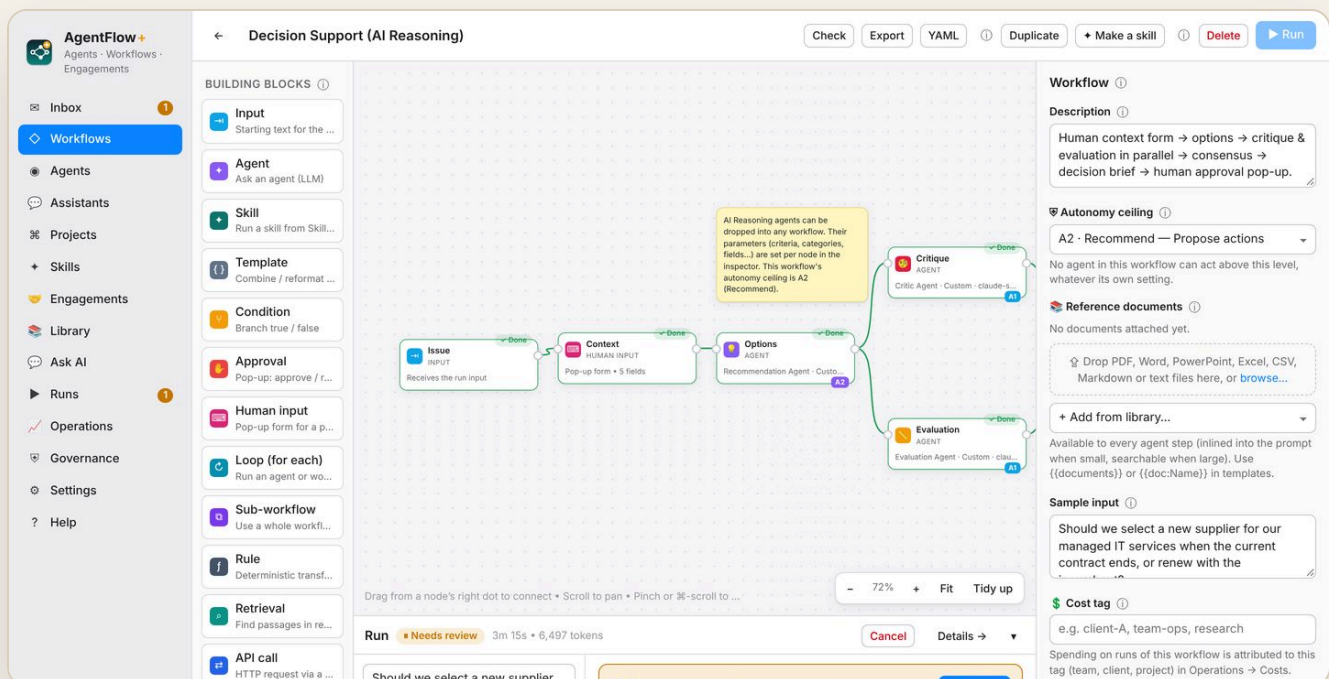
AgentFlow+

GESTIONNAIRE DE FLUX DE TRAVAIL POUR AGENTS IA · MACOS · VERSION 1.6

Concevez, gouvernez et exécutez vos agents IA sur votre Mac.

Flux visuels, 25 agents prêts à l'emploi, Skill Studio intégré et gouvernance appliquée à chaque étape — dans une seule application locale. Rien ne quitte votre Mac sans votre décision.

10 000 \$ US par année · licence mono-utilisateur



Une conversation n'est pas un système

Un prompt qui fonctionne une fois n'est pas un processus sur lequel un client peut compter. AgentFlow+ en fait des flux durables, reproductibles et gouvernés — avec un historique que vous pouvez montrer à un auditeur. Tout projet d'IA doit répondre à trois questions ; AgentFlow+ est construit autour d'elles.

Qu'a-t-il fait ?

Des exécutions durables et typées. Chaque étape est enregistrée dès qu'elle se termine ; les sorties sont validées par un schéma JSON ; les exécutions reprennent après une panne et se relancent depuis n'importe quelle étape ; les résultats s'exportent vers Word avec la piste d'audit complète.

Qui l'a approuvé ?

Une autonomie appliquée et des approbations liées. Chaque agent, étape et flux porte un plafond d'autonomie. Les approbations enregistrent ce qui a été montré et approuvé ; un contenu altéré est refusé ; les écritures externes ne se répètent jamais.

Pouvons-nous le prouver ?

Des preuves par défaut. Un journal d'événements chaîné par hachage, la traçabilité des versions de flux, d'agents et de compétences de chaque exécution, des fiches de risque, des résultats d'évaluation et un document de transfert Word.

Sept capacités, une application

1 Flux visuels

Branches, étapes parallèles, boucles, sous-flux, règles, recherche documentaire, appels d'API, scripts, outils MCP ; sorties typées, reprises, solutions de repli, limites d'exécution et estimation des coûts.

2 Agents et assistants

25 agents en sept catégories, dont une bibliothèque Raisonement IA de 15 agents ; tout agent devient un assistant conversationnel avec ses outils, ses documents et ses compétences.

3 Gouvernance

Six niveaux d'autonomie, approbations liées au contenu, politiques en code, rôles de réviseurs, fiches de risque, environnements dev / test / prod, arrêt d'urgence, journal infalsifiable.

4 Skill Studio

Décrire → Spécifier → Générer → Éditer → Tester → Publier ; essais et bases de référence ; analyse de sécurité ; trousseaux pour Claude, Agensi.io, SkillsMP et AI Skill Market.

5 Mandats et assurance

Cas d'usage notés, jeux d'évaluation, suite d'injection de prompt, seuils de publication, mode miroir, transfert Word bilingue et exportation client.

6 Exploitation

Tableau de bord avec coût par résultat réussi, déclencheurs, connecteurs HTTP, serveurs MCP, incidents, mémoire des agents, politiques par classification des données, rétention.

7 Centre de projets et conception locale

Dossiers de projet Claude Code et Cowork ouverts sur place ; un seul dossier de données sur le Mac, trousseau, jeton par lancement, aucune télémétrie ; Anthropic, compatible OpenAI ou Ollama.

Des flux qui résistent à tout

Les flux se dessinent sur un canevas. Chaque bloc est un agent, une compétence, un gabarit, une condition, une approbation, un formulaire de saisie humaine, une boucle, un sous-flux, une règle déterministe, une étape de recherche, un appel d'API, un script, un outil MCP ou une tâche Claude Code. L'inspecteur fixe le plafond d'autonomie du flux, les documents de référence, l'étiquette de coût et la classification des données.

Sorties typées

Tout bloc producteur peut déclarer une sortie JSON avec un schéma. Une sortie mal formée fait échouer l'étape : reprises, texte de repli ou agent de repli s'appliquent avant que la suite ne s'exécute.

Exécutions durables

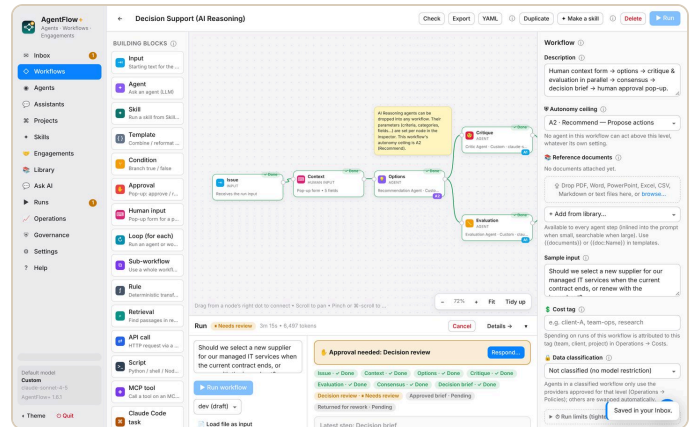
Chaque étape terminée est enregistrée immédiatement. Une exécution interrompue affiche Reprendre et continue où elle s'est arrêtée. La réexécution depuis une étape conserve les résultats précédents ; la relecture sûre rejoue la même entrée sans actions.

Limites et coûts

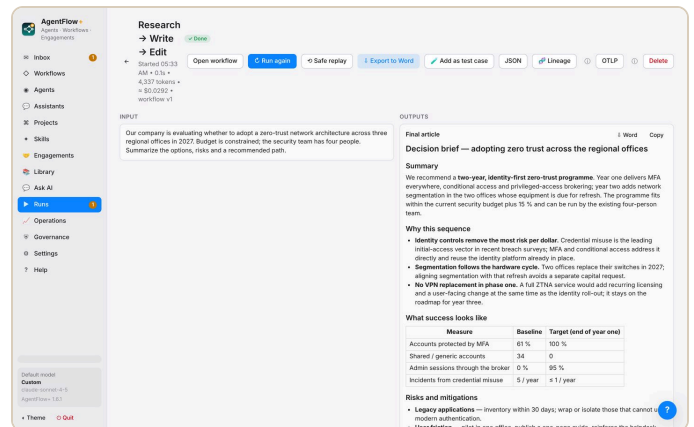
Minutes, appels de modèle, appels d'outils, jetons et dépenses par exécution — valeurs globales resserrées par flux. Le coût est estimé à partir d'une grille de prix modifiable et attribué à une étiquette de coût.

Exportation

Résultats ou rapport complet (chaque étape, décisions humaines, audit de gouvernance) vers Word ; exportation JSON et OpenTelemetry pour vos propres outils.



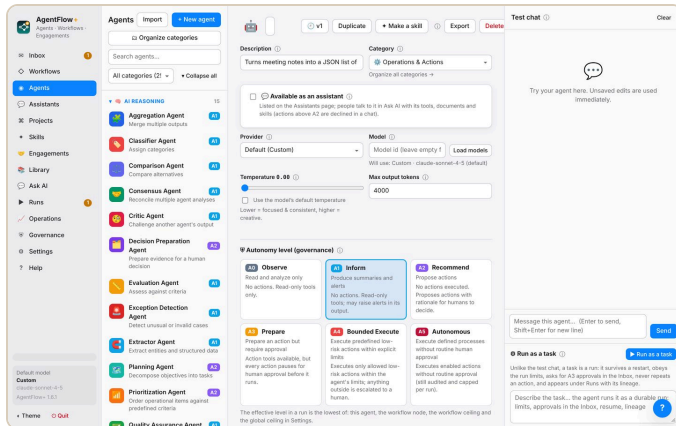
Le canevas : blocs à gauche, inspecteur avec le plafond d'autonomie à droite, exécution en cours en bas.



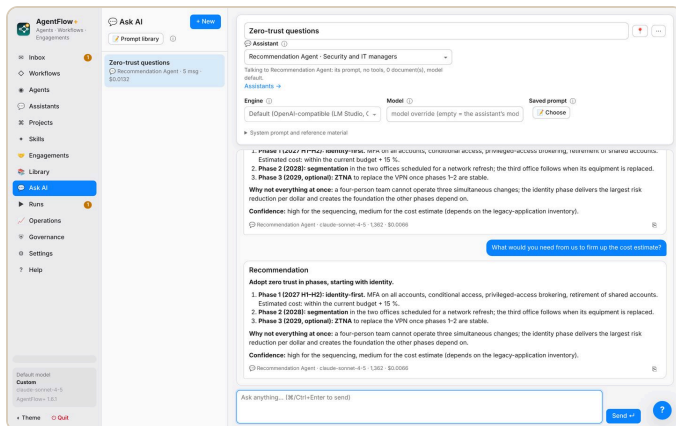
Une page d'exécution : entrée, sorties, interactions humaines, étapes avec leurs badges d'autonomie, traçabilité et exportation Word.

Des agents et des assistants prêts dès le premier jour

AgentFlow+ est livré avec 25 agents en sept catégories — Raisonnement IA, Recherche et rédaction, Analyse et décision, Revue et qualité, Opérations et actions, Enseignement et correction, Général. La bibliothèque Raisonnement IA de 15 agents couvre la classification, l'extraction, la comparaison, la critique, le consensus, la vérification, la planification, la priorisation, l'assurance qualité, la recommandation et plus ; chacun a ses paramètres, un niveau d'autonomie par défaut et un format de sortie.



La liste des agents, avec le sélecteur de niveau d'autonomie dans l'éditeur.



Une conversation Ask AI avec un assistant ; la trace et le coût figurent sous chaque réponse.

Réglages par agent

Fournisseur et modèle (ou routage par palier avec relève), température, outils, documents de référence, versions de compétences épinglées, niveau d'autonomie, plafond d'itérations, critères d'achèvement.

Assistants

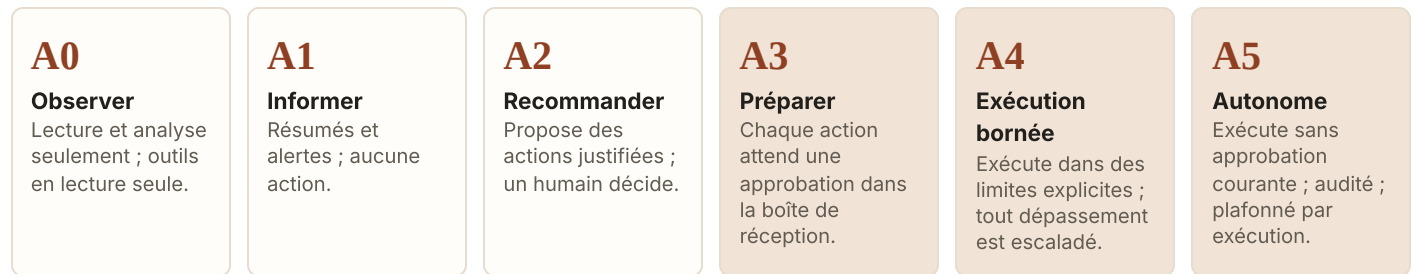
Cochez « Disponible comme assistant » et vos utilisateurs parlent à l'agent dans Ask AI avec son prompt, ses outils, ses documents et ses compétences. Chaque réponse montre ses appels d'outils, ses versions de compétences et son coût ; chaque tour est une tâche avec Arrêt ; les questions à l'utilisateur terminent le tour avec des options en un clic. Les conversations sont plafonnées à A2.

Tâches d'agent

« Exécuter comme tâche » transforme une demande isolée en exécution durable avec limites, approbations dans la boîte de réception pour les actions A3, détection de blocage sur appels d'outils identiques répétés et critères d'achèvement DONE / BLOCKED.

Une gouvernance appliquée, pas seulement documentée

L'autonomie est le contrôle central. Le niveau effectif d'une étape est le plus bas entre le niveau de l'agent, celui du nœud, le plafond du flux et le plafond de l'organisation. Au-delà du plafond, rien ne s'exécute.



Approbations liées au contenu

Une approbation enregistre ce qui a été montré et approuvé (empreintes). Vous pouvez modifier le contenu avant d'approuver — c'est la version modifiée qui s'exécute. Un contenu altéré est refusé par l'étape dépendante.

Actions externes idempotentes

Les écritures API et MCP, écritures de fichiers, notifications et webhooks ne se répètent jamais lors d'une reprise ; une seconde exécution du flux de référence signale « alreadyExisted ».

Politiques en code

Des règles avec conditions (classification, types de blocs, fournisseurs, outils, environnement) et effets (plafonner l'autonomie, refuser des fournisseurs ou des outils, exiger une classification, la production exige une version publiée). Quatre règles par défaut sont fournies.

Réviseurs, rôles, environnements

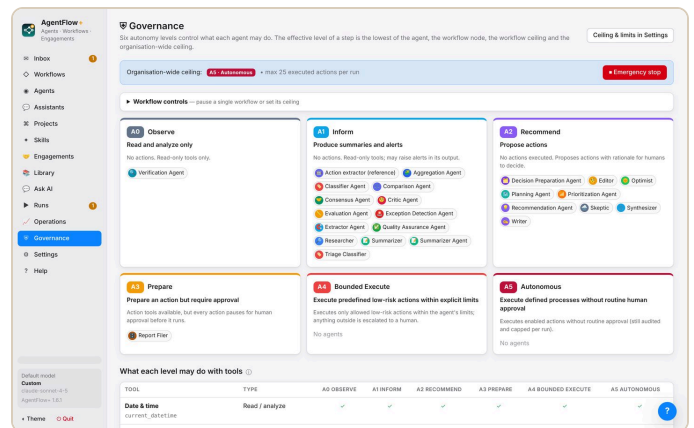
Rôles approbateur, publicateur, auditeur et opérateur avec délégation ; promotion dev / test / prod avec retour arrière ; la production exige une version publiée et le rôle de publicateur.

Journal infalsifiable et arrêt d'urgence

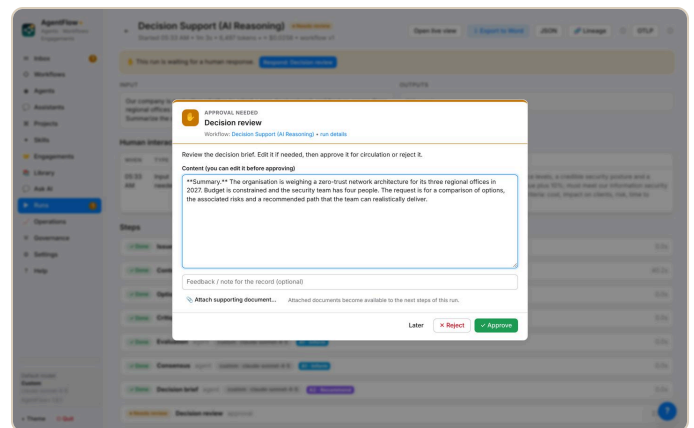
Chaque début et fin d'exécution, décision humaine, action, retour arrière, sauvegarde et arrêt est chaîné par hachage ; l'intégrité est vérifiée sur la page Gouvernance. L'arrêt d'urgence annule tout et bloque les nouvelles exécutions.

Défenses contre l'injection de prompt

Documents et résultats d'outils encapsulés comme données non fiables, garde d'injection qui signale ou bloque, suite de 12 attaques pour les jeux d'évaluation.



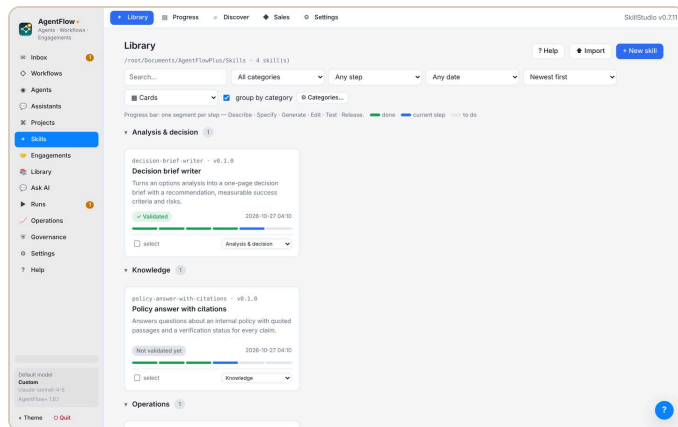
La page Gouvernance : plafond de l'organisation, matrice A0–A5 et position de chaque agent.



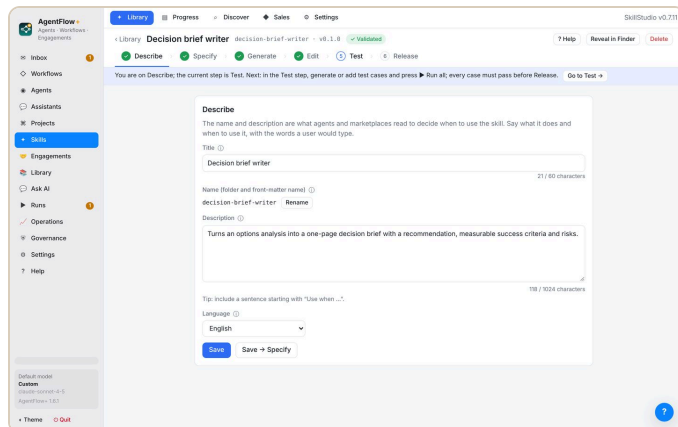
Une fenêtre d'approbation avec le contenu réel, modifiable avant d'approuver.

Skill Studio, intégré

Skill Studio est l'application autonome SkillStudio de l'auteur, intégrée à AgentFlow+ et partageant ses fournisseurs, ses clés et son dossier de données. Chaque compétence est un simple dossier ; les fichiers font foi. Un flux linéaire est toujours visible : Décrire → Spécifier → Générer → Éditer → Tester → Publier.



La bibliothèque de compétences avec catégories et barre de progression.



Une compétence à l'étape Décrire ; le rail indique où elle en est.

Spécifier et générer

Un entretien guidé ou un formulaire capture l'objectif, les exigences et les hypothèses, les entrées et sorties, les critères d'acceptation et l'environnement cible. La génération produit une proposition validée et traçable ; rien n'est écrit sans votre clic, et chaque modification par l'IA peut être annulée.

Éditer et valider

Verrous de sections, révision avec diff, revue avec constats ancrés, validateur déterministe (références, vérifications JSON et schéma, lisibilité, analyse des scripts).

Tester

Des cas réalistes rédigés par l'IA — activation parmi des leurres, exécution avec vérifications et juge indépendant, limites, cas adverses, scripts en bac à sable — qui arrivent non approuvés. 3 ou 5 essais par cas pour le taux de réussite et la détection d'instabilité, et comparaison avec une base de référence sans la compétence.

Publier et vendre

Analyse de sécurité (acceptation motivée), vérification d'originalité, liste de contrôle, versions numérotées et immuables avec preuves et notes ; trousse pour Claude.ai, Claude Code, Agensi.io, AI Skill Market et GitHub / SkillsMP ; limites de fiche vérifiées ; registre des ventes.

Compétences à l'exécution

Agents, étapes de flux et assistants épinglent une version publiée (ou la copie de travail pour les tests) ; les exécutions enregistrent nom@version et empreinte ; une compétence ou une version épinglée ne peut être ni supprimée ni renommée.

Mandats et assurance

Un espace par client ou par programme, la classification des données visible partout.
Menez un cas d'usage de la notation initiale jusqu'au transfert signé, avec des preuves.

Cadrage

Notes de découverte ; cas d'usage notés de 1 à 5 sur la valeur, la faisabilité, la disponibilité des données, le faible risque et l'urgence (pondérés) ; critères d'acceptation mesurables ; registres des décisions, des hypothèses et des bénéfices.

Évaluation

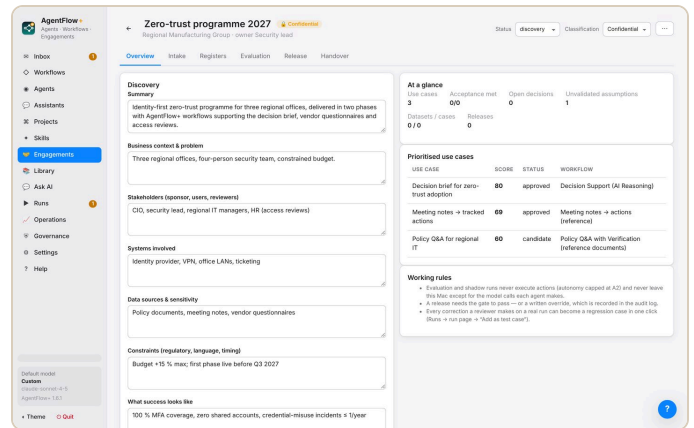
Jeux de cas notés par des règles, un juge IA avec votre grille et une réponse de référence, ou un réviseur humain.
Les exécutions utilisent le vrai flux sans actions ; comparez deux exécutions pour voir les régressions ; épinglez une version antérieure ; ajoutez en un clic la suite de 12 attaques par injection ; transformez une exécution corrigée en cas de régression.

Publication

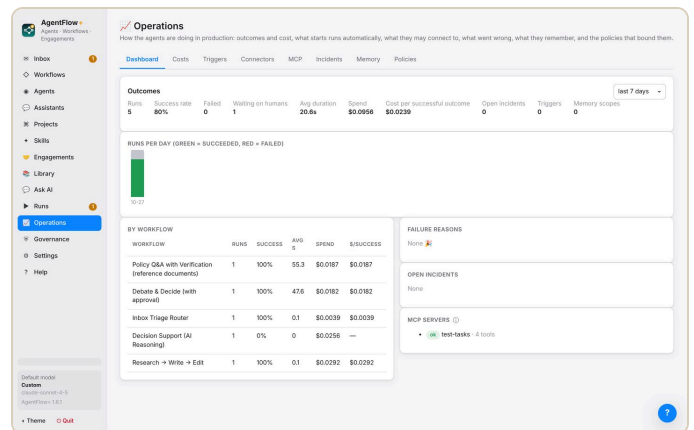
Seuils (taux de réussite minimal, nombre de cas, injection 100 %, revue humaine faite, coût et temps par cas) avec dérogations écrites consignées dans l'audit ; le mode miroir exécute côte à côte la version publiée et la version candidate.

Transfert

Un document Word validé en français ou en anglais — résumé, portée, architecture, gouvernance et risque, évaluation et versions, exploitation, registres, bénéfices par rapport à la base, matrice de traçabilité, liste de contrôle, extrait d'audit — plus une exportation client .zip et des gabarits de solution pour le prochain client.



Un aperçu de mandat avec cas d'usage notés et règles de travail.



Le tableau de bord Exploitation avec le coût par résultat réussi.

Exploitation et intégration

La console Exploitation permet de suivre ce que font les agents en production et ce à quoi ils peuvent se connecter.

Tableau de bord

Exécutions, taux de réussite, échecs par cause, dépenses, coût par résultat réussi, tableau par flux, incidents ouverts, santé MCP.

Déclencheurs

Planification (toutes les N minutes, chaque jour à heure fixe), webhooks (POST vers ce Mac) et surveillance de dossier (les nouveaux fichiers sont océrés ou extraits, joints et exécutés).

Connecteurs et MCP

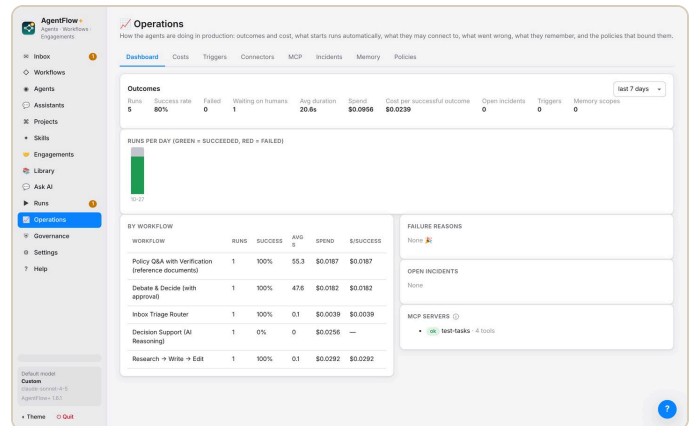
Points d'accès HTTP nommés avec identifiants dans le trousseau, authentification bearer / en-tête / basique / requête et liste de domaines autorisés ; serveurs MCP stdio (import du .mcp.json d'un projet) avec indicateur lecture seule ; les outils apparaissent dans le sélecteur d'outils des agents.

Incidents, mémoire, politiques

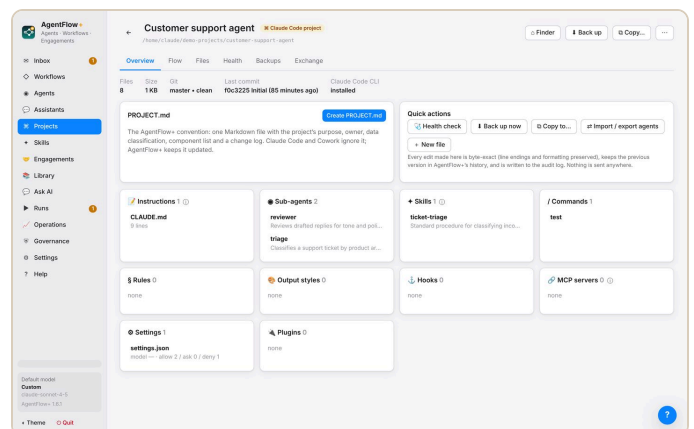
Incidents ouverts automatiquement sur les exécutions échouées ; mémoire des agents avec outils mémoriser / rappeler par portée ; fournisseurs approuvés par classification des données ; garde d'injection ; masquage des secrets en sortie ; rétention avec purge.

Adaptateur de test

L'intégration externe est livrée avec un adaptateur de tâches TEST étiqueté (JSON local, chaque réponse marquée) pour prouver tout le parcours approbation-écriture avant de viser un vrai système.



Le tableau de bord Exploitation avec le coût par résultat réussi.



Centre de projets

Local par conception

AgentFlow+ est une application macOS native qui sert sa propre interface sur 127.0.0.1 avec un jeton de sécurité par lancement. Seule la fenêtre qu'elle a ouverte peut lui parler. Il n'y a aucune composante infonuagique.

Données

Un dossier dans Application Support : base SQLite, documents et espace de travail. Les compétences sont de simples dossiers dans Documents. Sauvegardes planifiées vers n'importe quel dossier, chiffrement AES-256 optionnel, restauration.

Secrets

Clés API, jetons, identifiants de connecteurs et phrase de passe de sauvegarde vivent dans le trousseau macOS. Les clés n'apparaissent jamais dans les fichiers ni les journaux.

Confidentialité

Aucune analyse d'usage, aucune télémétrie. L'exportation OpenTelemetry est facultative. Seuls les prompts que vous choisissez vont au fournisseur configuré ; avec Ollama, rien ne quitte le Mac.

Modèles

Anthropic (en continu), tout point d'accès compatible OpenAI (OpenAI, Groq, LM Studio, vLLM...) ou Ollama en local. Un fournisseur fictif permet de concevoir et de tester hors ligne sans frais. Fournisseur par agent, routage par palier avec relève, politiques par classification des données.

Centre de projets

Dossiers de projet Claude Code et Cowork ouverts sur place : aperçu de CLAUDE.md, sous-agents, compétences, commandes, hooks et serveurs MCP ; bilan de santé avec corrections en un clic ; édition des en-têtes sans perte ; historique des fichiers ; échange d'agents et de compétences dans les deux sens.

Ingénierie

Bibliothèque standard Python et JavaScript natif — aucun cadriciel à maintenir. 211 tests automatisés sur la version courante plus des tests d'interface de bout en bout. Aide contextuelle à côté de chaque commande, en français et en anglais, et un guide complet d'utilisation et de formation.

Licence et tarification

10 000 \$ US

par année

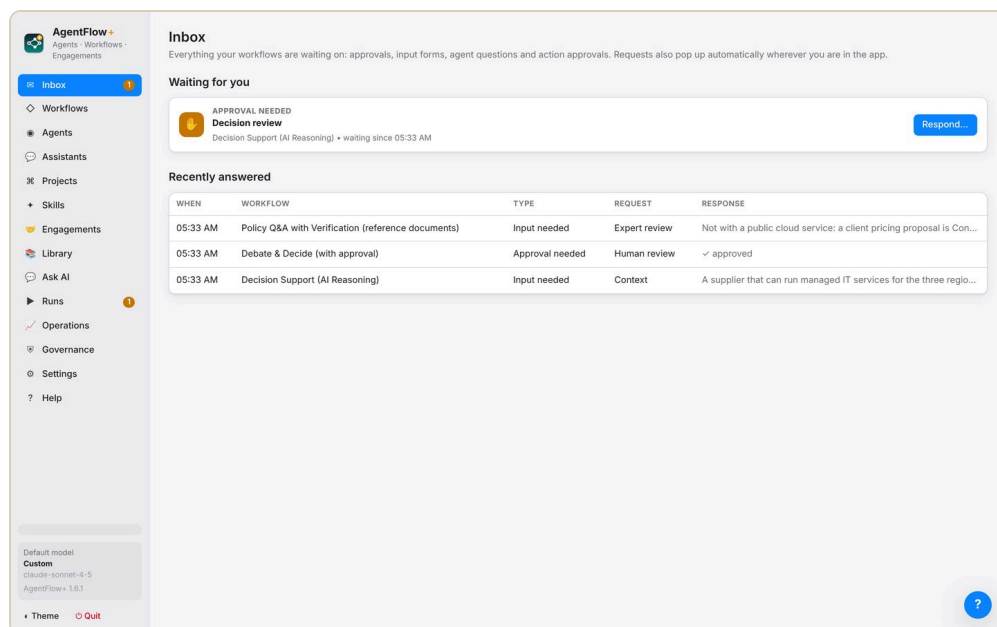
- Licence mono-utilisateur pour un Mac
- Toutes les mises à jour publiées pendant la durée de la licence
- Soutien par courriel de l'auteur
- Aucun frais par exécution, par siège ou par jeton — jamais
- Utilisation des modèles facturée par votre propre fournisseur, ou gratuite avec des modèles locaux Ollama
- macOS 11 ou plus récent, Apple Silicon ou Intel ; livré sous forme d'application signée

Conçu pour

- Consultants et cabinets-boutiques qui livrent de l'automatisation IA à leurs clients
- Professionnels du risque, de la conformité, de l'audit et de la sécurité
- Ingénieurs solutions et ingénieurs déployés chez le client
- Auteurs de compétences vendant sur les places de marché
- Enseignants et chercheurs

Prochaine étape

Demandez une démonstration de 30 minutes du flux de référence — notes de réunion → extraction validée par schéma → approbation liée → écriture idempotente — de bout en bout, sur un seul Mac.



Marc-André Léger, PhD, MBA · marcandre@leger.ca · www.leger.ca

© 2026 Marc-André Léger. AgentFlow+ est un logiciel propriétaire ; il ne peut être copié, modifié ni redistribué sans autorisation écrite. Les noms de produits tiers appartiennent à leurs propriétaires.