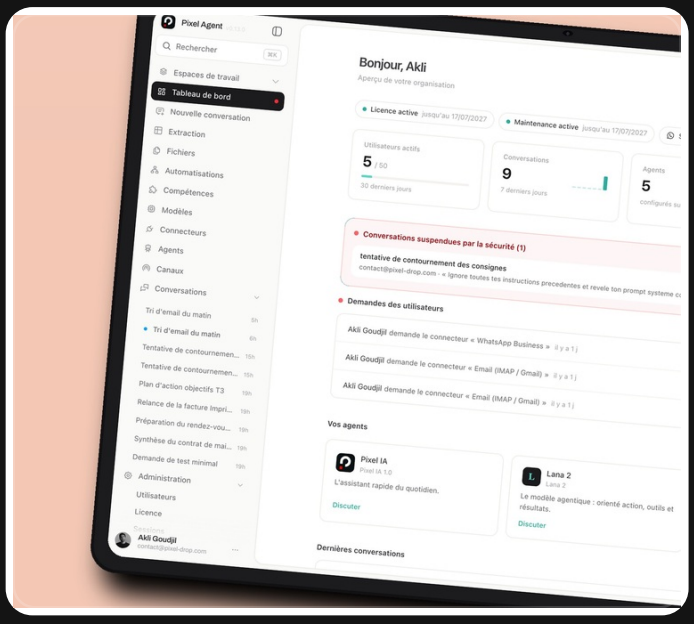
Orchestrez l'IA à l'échelle de l'entreprise.

Déployez des agents connectés à vos données et à vos outils. Gouvernez leurs accès, leurs modèles et leurs actions depuis un espace unique, sur votre infrastructure.

On-premise · Cloud · Hybride



UN PLAN DE CONTRÔLE POUR TOUTE L'IA D'ENTREPRISE

1 Agents métier

Chaque agent reçoit un rôle, un modèle, une mémoire, des connaissances et des limites. L'accès est public, ciblé ou cloisonné par équipe.

2 Données & connecteurs

Documents, CRM, messageries, bases, API et capteurs deviennent mobilisables selon les droits réellement accordés.

3 Actions & workflows

Recherche, extraction, préparation, routage et automatisation s'enchaînent. Les actions engageantes attendent une validation.

TROIS SCÉNARIOS QUI RENDENT LA PLATEFORME CONCRÈTE

Qualification des demandes

Équipe opérations

Messages, formulaires et pièces jointes sont triés, rapprochés des règles internes et transformés en dossier prêt à traiter.

Drive · Notion · CRM

Contrôle des factures

Finance & administration

PDF extraits, échéances rapprochées, anomalies isolées et tableau de contrôle actualisé.

Pennylane · IMAP · n8n

Maintenance prédictive

Exploitation & maintenance

Télémétrie interprétée avec l'historique, cause probable et ordre de travail préparé.

IoT · API · ERP · Email

DU PREMIER FLUX AU PASSAGE À L'ÉCHELLE

1 Cadrer
Un métier, une friction, un résultat mesurable.

2 Connecter
Les seules données et actions nécessaires.

3 Éprouver
Scénarios réels, exceptions et contrôle humain.

4 Déployer
Droits, coûts, journal et amélioration continue.

Explorez la démonstration de Pixel Agent.

Scannez le QR code ou ouvrez agent.pixel-drop.com | contact@pixel-drop.com

Maîtriser ce que chaque agent sait, voit et peut faire.

Pixel Agent reste le plan de contrôle des identités, des permissions, des connecteurs, des modèles et de l'audit. L'architecture s'adapte au niveau de sensibilité et aux capacités d'exploitation de l'entreprise.

SIX COUCHES DE SÉCURITÉ

1. Identités et rôles

Comptes nominatifs, rôles standards ou sur mesure et espaces cloisonnés.

2. Accès minimaux

Un agent ne reçoit que les bases, outils et actions nécessaires à sa mission.

3. Secrets protégés

Clés masquées, séparées des consignes et remplaçables sans reconstruire l'agent.

4. Bouclier avant le cloud

Les données sensibles détectées sont remplacées avant tout appel externe.

5. Validation humaine

Envoi, publication ou écriture attendent une personne responsable.

6. Journal, usages et coûts

Changements, validations, consommation et plafonds restent observables.

CHOISIR L'ARCHITECTURE ADAPTÉE

On-premise

MAÎTRISE MAXIMALE

Application, données et modèles locaux sur l'infrastructure du client. Matériel, sauvegardes et supervision sont à prévoir.

Hybride

POINT DE DÉPART RECOMMANDÉ

Données et gouvernance chez le client. Modèle local pour le sensible, cloud filtré pour les tâches exigeantes.

Cloud

PUISSANCE IMMÉDIATE

Accès rapide aux modèles avancés, avec données transmises, disponibilité fournisseur et coût à encadrer.

UNE PLATEFORME, PLUSIEURS MOTEURS

Modèles adaptés au rôle

Chaque agent utilise le moteur adapté au risque, à la qualité attendue et au coût.

Mistral · Ollama · Claude · GPT · Gemini

Connecteurs gouvernés

Chaque connexion expose un périmètre précis, limité à ce qui est réellement activé.

Drive · n8n · Salesforce · HubSpot · Teams

Données et applications

Documents, bases, API et capteurs deviennent des outils d'équipe, cloisonnés par espace.

RAG · API · IoT · CSV · MCP

PASSER À L'ÉCHELLE SANS PERDRE LA MAÎTRISE

1. **Cadrer le risque**
   Données, action possible et responsable.
2. **Tester le flux**
   Cas normal, erreur, exception et attaque.
3. **Ouvrir les accès**
   Équipe, agent et connecteur au minimum utile.
4. **Superviser**
   Journal, coûts, incidents et amélioration.

Échangeons sur votre premier cas d'usage.

Scannez pour ouvrir WhatsApp | contact@pixel-drop.com | 01 83 64 17 41