

Nexfire, fiche sécurité et conformité

Fiche générée le 04/09/2026. Contenu aligné sur nexfire.fr/plateforme.

L'essentiel en cinq points

- Plateforme hébergée en Europe ; version installée sur vos serveurs, sur devis.
- Validation humaine des actions sensibles (envoyer, payer, supprimer), non désactivable, même en mode autonome.
- Secrets (clés d'API, identifiants de connecteurs, jetons) chiffrés dans un coffre, jamais affichés en clair, jamais écrits dans les journaux.
- Durée de conservation des exécutions réglable par espace, 90 jours par défaut, de 1 jour à 10 ans.
- Export et effacement des données d'un utilisateur en libre-service depuis son profil (RGPD).

Anatomie d'un agent

Un agent, c'est six réglages et une boucle.

Ses instructions Ce qu'il doit faire, dans quel ton, avec quelles règles métier. Écrites en français, versionnées, exportables.	Ses outils Uniquement ceux que vous lui donnez : recherche web, lecture et écriture de fichiers, production de documents, génération de médias, et les connecteurs que vous avez autorisés. Il ne voit pas les autres.	Ses connaissances Une ou plusieurs bases de documents, synchronisées depuis vos sources. Il y cherche par sens et par mots-clés, et cite ce qu'il a trouvé.
Son modèle Le fournisseur d'IA et le modèle qui le font raisonner, choisis par agent parmi quinze fournisseurs. Changeables à tout moment. La Forge, qui assemble un agent par conversation, utilise votre propre clé d'IA.	Son autonomie Supervisé ou autonome, et la liste des actions qui exigent une validation : enregistrer, supprimer, envoyer, payer. Les actions à risque attendent toujours, quel que soit le mode.	Sa mémoire Ce qu'il retient d'une exécution à l'autre, dans votre espace, avec la durée de conservation que vous fixez.

Puis, à chaque tâche :

1. Il reçoit la tâche. Par le chat, par un déclencheur (email, message, deal, page, réunion, webhook), par une planification, par l'API ou depuis votre site.
2. Il planifie et exécute. Il découpe la tâche, appelle ses outils un par un, lit vos documents, interroge vos données. Chaque étape est visible dans le Studio pendant qu'elle se déroule, et conservée ensuite.
3. Il produit. Un livrable Word, Excel, PowerPoint ou PDF, un média, ou une réponse. Le code qu'il écrit pour fabriquer un fichier tourne dans un bac à sable isolé, sans accès à votre réseau. Le livrable est relu visuellement avant remise.
4. Il s'arrête. Devant toute action sensible, il attend dans la file de validation. Vous approuvez, refusez, ou corrigez. Il reprend avec vos remarques.
5. Il livre. Dans votre espace Livrables, et par le canal que vous avez choisi : email, Slack, Teams, WhatsApp, Telegram, Discord, webhook.

Ce qu'un agent peut toucher

Il n'accède qu'à ce que vous avez autorisé, et vous pouvez tout retirer.

Vos applications : plus de 120, par autorisation Connexion par le bouton Autoriser de chaque application, avec les seuls droits demandés. Nexfire ne stocke aucun mot de passe. L'accès se révoque en un clic, chez nous ou chez l'éditeur.	Vos documents SharePoint, Google Drive, Notion, Confluence, Jira, ou envoi direct de fichiers texte, Markdown, PDF, Word et Excel. Synchronisation planifiée. Les identifiants de connexion sont chiffrés dans un coffre et ne s'affichent jamais en clair.
Vos bases de données PostgreSQL, MySQL, SQLite, via un serveur de connexion que vous configurez avec un compte aux droits que vous choisissez. Vous pouvez brancher vos propres serveurs d'outils, en local ou en HTTP, avec authentification par en-tête, jeton ou clé.	Vos systèmes Une API avec des jetons personnels à portée lecture ou écriture, figés à la création, plafonnés en nombre. Des intégrations entrantes testées avant activation. Des webhooks signés, avec rotation de jeton et journal des appels.
Vos réunions Un bot rejoint Meet, Teams, Zoom ou Webex uniquement après consentement explicite dans votre espace. Il est visible des participants. Vous choisissez la région de traitement.	Votre site Un assistant en trois lignes de code, limité aux domaines que vous déclarez, avec des clés révocables, un plafond de coût et une protection contre l'abus.

Ce qu'il ne peut pas faire sans vous

Le frein est dans le moteur, pas dans les réglages.

Toute action à risque attend Chaque outil porte un niveau de risque. Au-dessus d'un seuil, l'exécution se met en pause et attend une décision humaine. Ce seuil ne se désactive pas, même en mode autonome. Un administrateur ne peut pas l'oublier, un agent ne peut pas le contourner.	Envoyer, payer, supprimer, enregistrer Quatre familles d'actions supervisées, réglables agent par agent. Le mode autonome ne peut relâcher que celles-ci, jamais le seuil de risque.
Il ne dépense que dans un mandat Un agent ne peut payer que dans le cadre d'un mandat que vous approuvez, avec un plafond mensuel. Le budget d'IA de chaque espace est suivi en temps réel.	Il demande quand il ne sait pas Une question de clarification interrompt l'exécution et vous est adressée. Il ne devine pas, il ne remplit pas les blancs.
Les capacités payantes s'activent par un administrateur Génération d'images, de vidéos, de voix, de musique : désactivées par défaut, activées seulement par un propriétaire ou un administrateur de l'espace.	Le bot de réunion demande la permission Le premier envoi d'un bot en réunion exige un consentement explicite, horodaté, dans votre espace.

Où vont vos données

Vous choisissez qui traite, combien de temps on garde, et quand on efface.

Hébergement Plateforme hébergée en Europe. Pour les organisations qui l'exigent, une version installée sur vos serveurs, préparée sur devis et accompagnée.	Traitement par l'IA Le fournisseur se choisit par agent. Avec Mistral, acteur français, vos données ne quittent pas l'Union européenne. Avec vos propres clés, vos conditions contractuelles avec le fournisseur s'appliquent, pas les nôtres.
Conservation Durée de conservation des exécutions réglée par espace, 90 jours par défaut, de 1 jour à 10 ans. Les instantanés d'exécution sont chiffrés au repos et purgés à l'échéance.	Secrets Clés d'API, identifiants de connecteurs, jetons : chiffrés dans un coffre, jamais affichés en clair, jamais écrits dans les journaux.
Droits des personnes Export et effacement des données d'un utilisateur, en libre-service depuis son profil, pour alimenter votre registre et répondre dans les délais du RGPD.	AI Act Un questionnaire intégré qualifie chaque usage et génère le rapport PDF correspondant, à joindre à votre dossier de conformité.

Ce que nous ne prétendons pas.

Nous n'affichons aucune certification que nous n'avons pas obtenue. Ce que nous affirmons ci-dessus est vérifiable dans le produit, et nous le montrons lors de la revue technique.

Gouvernance et coûts

Chacun voit ce qui le regarde. Vous voyez tout.

Espaces de travail Un espace par équipe, par client ou par projet, avec ses agents, ses connecteurs, ses documents, son budget. Dans le cloud Nexfire, les données d'exécution, la base de connaissances et les secrets sont isolés par espace au niveau de la base de données elle-même (row-level security PostgreSQL), pas seulement dans le code.	Rôles Propriétaire, administrateur, membre, lecteur dans chaque espace ; administration de l'organisation au-dessus. Seuls les administrateurs activent les capacités payantes et gèrent les accès.
Journal d'audit Chaque action de chaque agent et de chaque utilisateur : qui, quoi, quand, avec quelles données, à quel coût. Consultable par espace et pour toute l'organisation, exportable.	Observabilité Exécutions en cours, taux de réussite, durée, coût par agent et par modèle. Alertes de gouvernance quand un seuil est dépassé.
FinOps Budget d'IA par espace, suivi consolidé pour l'organisation, coût réel par exécution. Vos propres clés ne sont jamais débitées ; les nôtres le sont au tarif catalogue du fournisseur, sans coefficient.	Politiques Niveau d'autonomie, actions supervisées, fournisseurs autorisés, réglés par espace et appliqués à tous ses agents.

Modèles

Quinze fournisseurs, choisis par agent, changeables sans rien casser.

Fournisseurs d'IA disponibles : Anthropic, OpenAI, Google, Mistral, xAI, DeepSeek, Kimi, Qwen, Z.ai, MiniMax, Perplexity, Groq, Together, OpenRouter, Ollama, en local.

Chaque modèle est classé selon sa fiabilité pour le travail d'agent, et ce classement s'affiche au moment du choix. Vous pouvez imposer un fournisseur par espace, ou laisser chaque agent au mieux adapté. Vos propres clés d'API sont acceptées et chiffrées ; avec elles, la facturation de l'IA passe directement par votre contrat.

Pour les livrables visuels et sonores, les modèles d'image, de vidéo, de voix et de musique se choisissent de la même façon, et ne s'activent que par un administrateur.

Déploiement

Vous entrez en une minute. Vous sortez avec vos agents et vos données.

Critère	Cloud Nexfire	Sur vos serveurs
Pour qui	Toute entreprise, de 0 à 99 € par mois, et l'offre Entreprise	Organisations avec exigences de souveraineté totale
Hébergement	Europe	Votre infrastructure
Modèles	Quinze fournisseurs, vos clés ou les nôtres	Idem, plus modèles locaux
Mise en place	Une minute, en autonomie	Préparée sur devis, installation accompagnée
Accompagnement	Centre d'aide, support ; interlocuteur attitré en offre Entreprise	Interlocuteur attitré

Ce que nous avons choisi de ne pas faire

Pas de pilotage d'ordinateur Un agent ne clique pas dans vos logiciels à votre place. Il passe par des connexions autorisées, dont les droits sont connus et révocables. C'est moins spectaculaire, et c'est auditable.	Pas d'autonomie sans frein Il n'existe pas de mode où un agent envoie, paie ou supprime sans qu'un humain l'ait vu. Ce mode ne sera pas ajouté.	Pas de certification affichée sans l'avoir Nous montrons ce que nous pouvons prouver. Quand une certification sera obtenue, elle sera ici, avec sa date.
---	---	--

Contact

contact@nexfire.fr · nexfire.fr/plateforme