openbee
THE ORGANIC SOFTWARE COMPANY

Garantissez la sécurité de vos données

LA SÉCURITÉ ET LA CONFIDENTIALITÉ DE VOS DONNÉES SONT NOTRE PRIORITÉ

Nous sommes engagés dans la protection de vos données à chaque instant. La sécurité de votre information est au coeur de nos préoccupations.

Pour permettre à vos équipes d'évoluer dans un monde qui change constamment et de répondre à leurs nouvelles habitudes de travail, nous avons implémenté un système avancé composé d'une sécurité multicouches.

Que vous soyez en télétravail, au bureau ou sur le terrain, cela vous demande de la flexibilité, surtout une sécurité sans faille à tous les niveaux afin de prévenir les fuites et abus d'information ou de limiter l'impact des cyber-attaques.

Ce document explique comment la plateforme Open Bee fonctionne en termes de sécurité opérationnelle, de confidentialité et de respect des normes en vigueur afin de garantir l'intégrité et l'accessibilité de vos données.

SÉCURITÉ APPLICATIVE

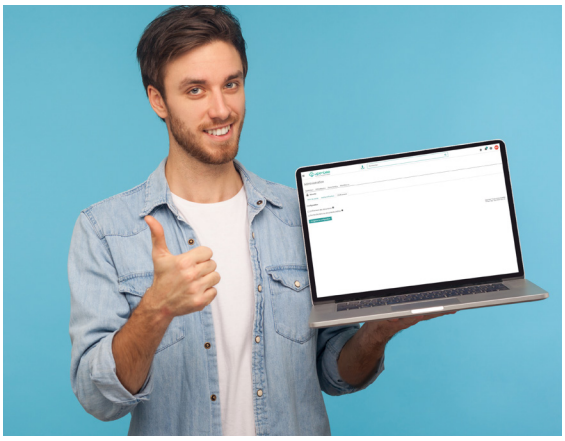
Politique de mot de passe fort :

Afin de protéger des attaques par force brute basées sur des dictionnaires (tentative visant à craquer un mot de passe ou un nom d'utilisateur), la plateforme Open Bee intègre un module dédié à la gestion des fonctionnalités avancées et à la sécurité accessible par l'administrateur.

- **Politique d'authentification :** les mots de passe doivent respecter une longueur et une complexité minimum avec l'intégration de caractères spéciaux. L'administrateur peut également forcer le renouvellement des mots de passe à une période donnée...
- **Politique de verrouillage :** les comptes utilisateurs sont verrouillés après un nombre de tentatives de connexion et selon une période personnalisable. Possibilité de déconnexion automatique en cas de changement d'adresses IP.
- **Expiration de la session :** après un temps d'inactivité défini, les utilisateurs doivent renouveler leur connexion.
- **Double-authentification (2FA) :** lors de la connexion, les utilisateurs doivent renseigner un code de sécurité à cinq chiffres (reçu par email ou via Google Authentificator) en complément de leur mot de passe.

Les mots de passe sont transférés via une connexion utilisant le protocole HTTPS.

SÉCURITÉ APPLICATIVE



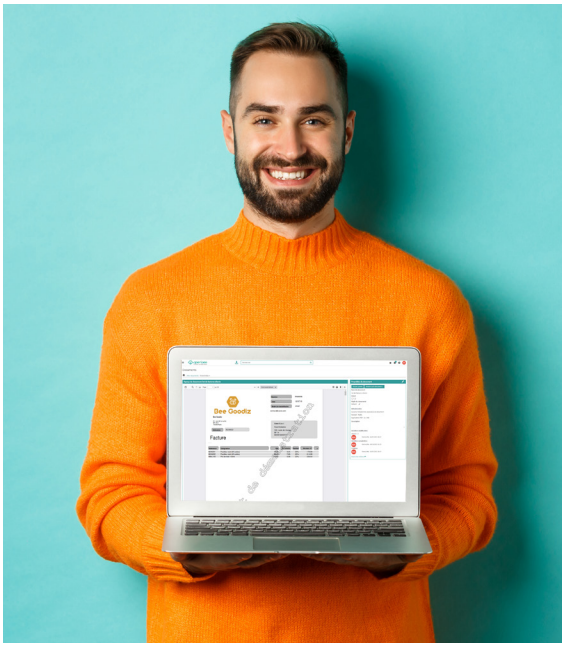
Chiffrement :

- **Données en transit :** Open Bee établit une connexion TLS sécurisée des données échangées sur les réseaux publics, en chiffrant toutes les communications entre le serveur web et le navigateur des utilisateurs.
- **Sécurité des documents «au repos» :** tous les documents archivés sur le serveur Open Bee (instance en Cloud ou sur site) peuvent être cryptés en utilisant un chiffrement AES 256 bit (Advanced Encryption Standard).

Intégration et provisionnement des utilisateurs

Pour automatiser la création et la suppression de comptes utilisateurs, les administrateurs Open Bee bénéficient de multiples options sécurisées :

- **Active Directory (AD) et Azure AD :** intégration de l'annuaire LDAP de l'Active Directory ou Azure AD existant à Open Bee afin de simplifier et centraliser la gestion des utilisateurs et des groupes.
- **Authentification unique (SSO) :** en cas d'import des utilisateurs depuis un AD ou un Azure AD.
- **API :** l'API REST (Web Services) permet de connecter une application tierce pour provisionner les utilisateurs et les groupes.

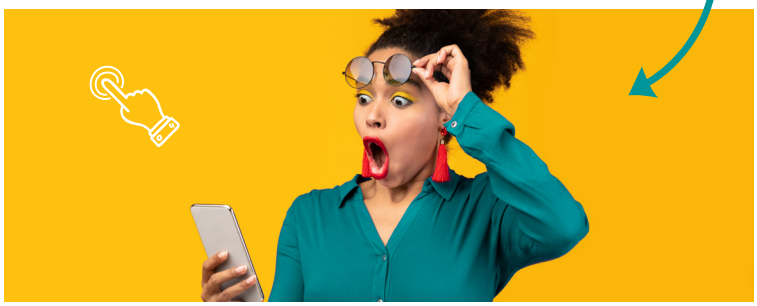


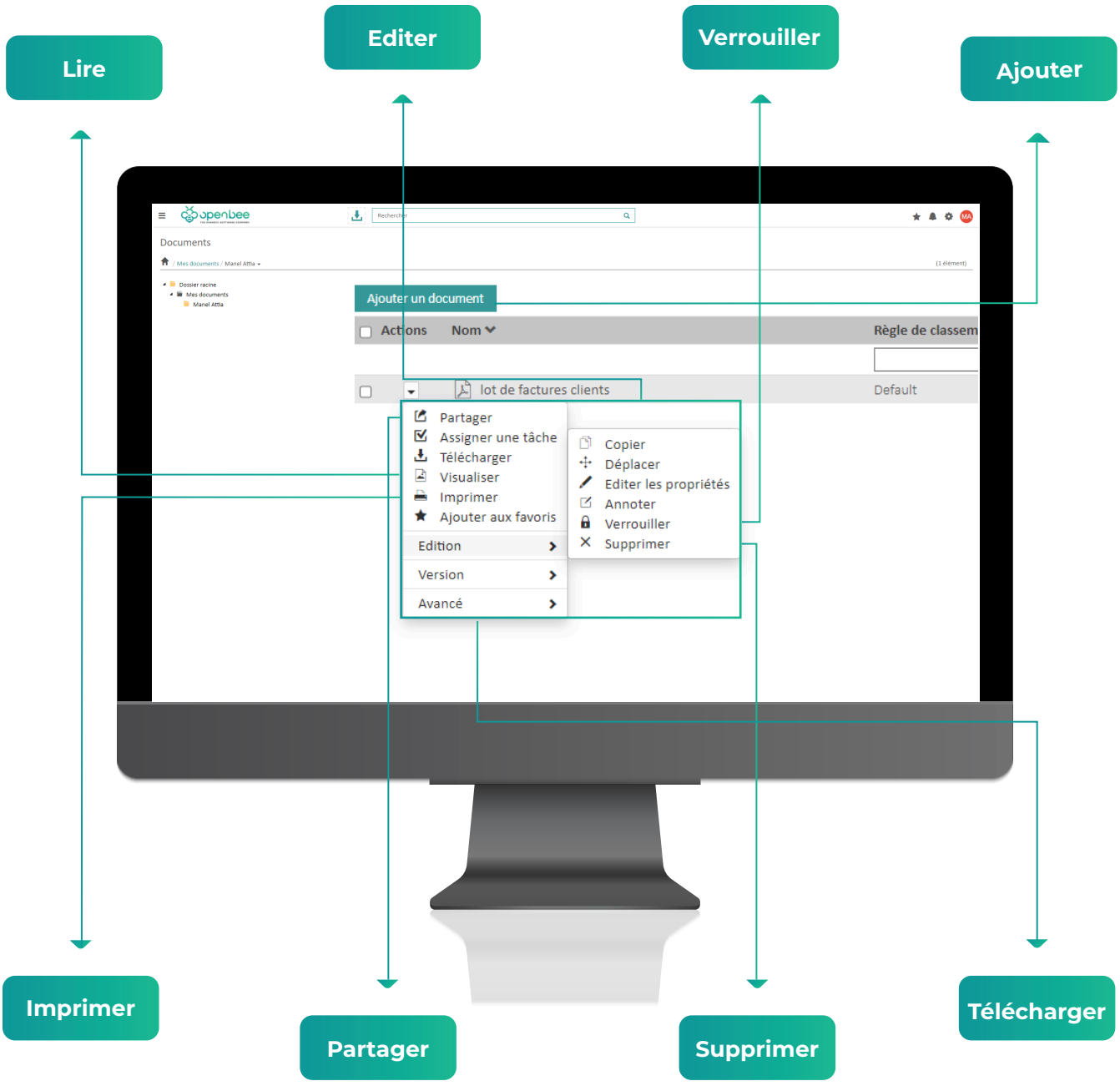
Sécurité du contenu

- **Permissions de contenu granulaires :** les administrateurs peuvent gérer les droits d'accès aux dossiers en attribuant des droits d'accès à des groupes et à des utilisateurs (éditer, lire, imprimer...)
- **Filigrane numérique :** les filigranes permettent de lutter contre le vol et la fuite de données par l'apposition d'un tampon (incluant le login utilisateur et la date) sur le document en empêchant l'impression et le téléchargement de ce dernier.
- **Traçabilité des actions :** possibilité de vérifier l'intégrité des journaux de log, vérification de l'horodatage par lot.
- **Contrôles des partages :** les administrateurs peuvent autoriser des liens partagés avant que les documents ne soient envoyés à des contacts externes.

GESTION FINE DES PERMISSIONS

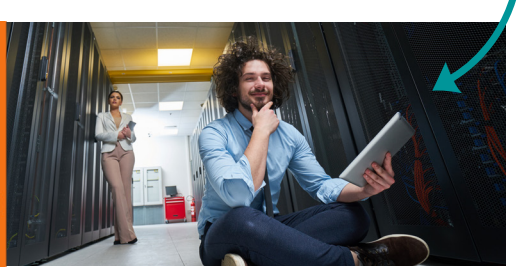
Dans Open Bee, l'administrateur du système peut gérer les droits d'accès aux dossiers et documents pour les utilisateurs et les groupes selon les critères suivants :





LA SÉCURITÉ DE L'INFRASTRUCTURE DU DATACENTER

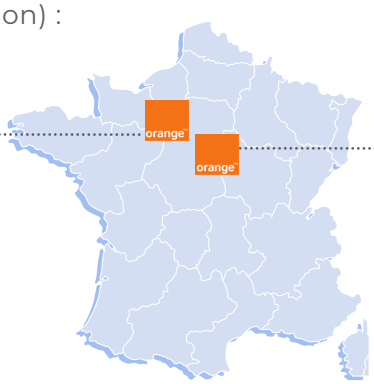
Les applications Open Bee Cloud sont hébergées dans les Datacenters Orange en France afin de garantir souveraineté et haute disponibilité*.



Sécurité physique

- Orange conçoit, construit et intervient sur les datacenters de façon à strictement contrôler l'accès physique aux emplacements où sont stockées vos données.
- Orange comprend l'importance de protéger vos données, et est engagé dans la sécurisation continue des datacenters qui contiennent vos données. Une division complète chez Orange est dédiée à l'élaboration, la construction et la maintenance des établissements physiques qui supportent Orange. Cette équipe est impliquée à maintenir une sécurité dernier cri.
- Orange choisit une approche à plusieurs niveaux concernant la sécurité physique, afin de réduire le risque d'accès physique aux données et aux ressources des datacenters par des utilisateurs non-autorisés. Les data centers gérés par Orange possèdent des niveaux étendus de protections : approbation des accès sur les périmètres des locaux/bâtiments, à l'intérieur et sur le sol des datacenters.

Datacenter Orange (production) :
Val de Reuil



Datacenter Orange (sauvegarde) :
Rueil Malmaison

*Le prestataire s'efforcera de rendre la solution disponible au moins 99% du temps.

LA SÉCURITÉ DE L'INFRASTRUCTURE DU DATACENTER

Conformité

Les infrastructures Orange répondent à un large éventail de normes conformité et spécifiques à des secteurs, telle que la norme ISO 27001. Des audits précis réalisés par des organismes tiers vérifient le respect des contrôles de sécurité stricts que ces normes imposent.

Sauvegardes automatiques

Les instances d'Open Bee hébergées sur le cloud sont sauvegardées selon une politique créée pour préserver l'intégrité et la disponibilité* des données limitant le risque de perte d'information et favorisant la restauration de données en cas de sinistres.

Le lieu de stockage se trouve en France, à Rueil Malmaison (78).

Les données sont sauvegardées quotidiennement selon ces règles de conservation (ensemble des politiques concernant la durée de rétention des sauvegardes) :

- Quotidienne : 14 jours
- Hebdomadaire : 12 semaines
- Mensuelle : 24 mois

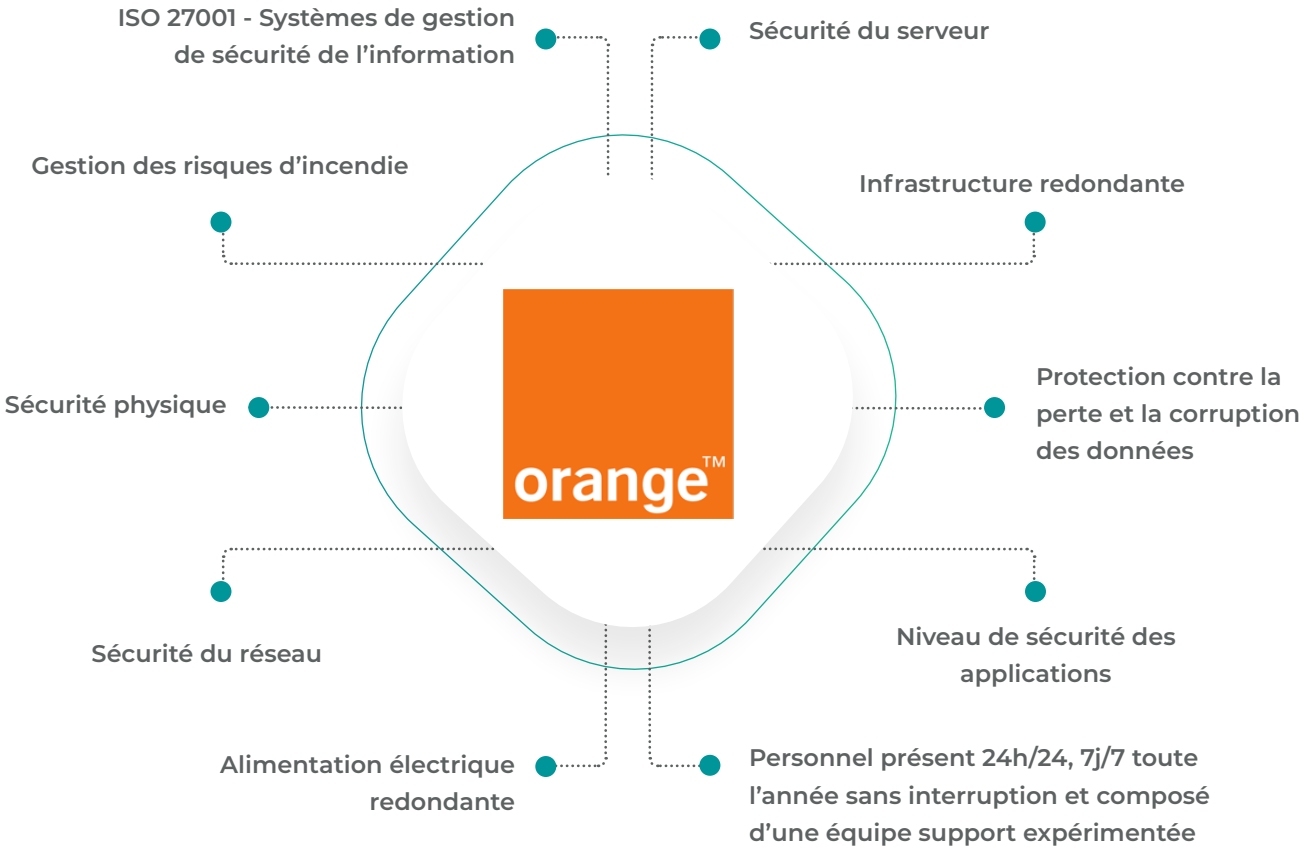
Cloud monitoring

Tous les serveurs et services Open Bee sont automatiquement monitorés et signalent instantanément toute faille ou goulot d'étranglement du système.

* Le prestataire s'efforcera de rendre la solution disponible au moins 99% du temps.

FOCUS SUR LA SÉCURITÉ DES INSTANCES OPEN BEE CLOUD

Le Datacenter Orange, certifié ISO 27001, est conçu pour protéger les systèmes d'information des dangers naturels et environnementaux ainsi que des intrusions non-autorisées.



GESTION DES RISQUES ET DE LA VULNÉRABILITÉ

Notre équipe dédiée à la sécurité réalise régulièrement des tests et patchs, tant automatiquement que manuellement. Elle travaille aussi étroitement avec des tiers spécialisés afin d'identifier et corriger les potentiels bugs ou vulnérabilités des applications qui compromettraient la sécurité de la plateforme.

Les applications Open Bee ont réussi les tests de pénétration sur :

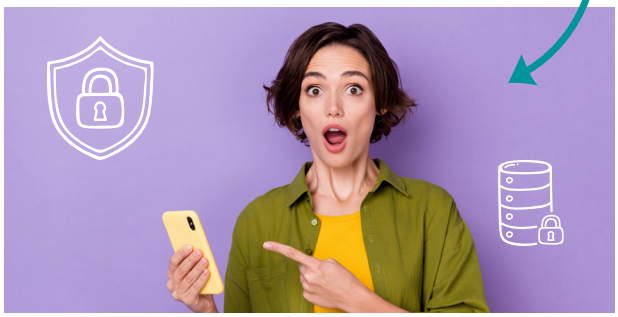
- Design et architecture de la solution
- Analyse et revue du code source
- Analyse des modules de la solution incluant la gestion utilisateur, l'authentification, l'autorisation, la confidentialité des données, l'intégrité, la comptabilité, la gestion de la session, la sécurité du transport
- Test de la pénétration automatique et manuelle utilisant des scanners de vulnérabilité web, des outils d'analyse binaire et des outils proxy

L'application Open Bee est régulièrement testée sur les failles de sécurité les plus critiques telles que celles listées dans le Top 10 OWASP :

1. Injection, Failles par injection, telles que SQL, NoSQL, OS, et injection LDAP.
2. Gestion incorrecte de l'authentification
3. Exposition des données sensibles
4. XXE (XML External Entities)
5. Défaillance du contrôle d'accès
6. Mauvaise configuration de la sécurité, Faible gestion de la session
7. Failles XSS (Cross Site Scripting)
8. Sérialisation non-sécurisée
9. Empoisonnement des cookies
10. Dépassement de tampon

ASSUREZ-VOUS D'ÊTRE PRÉPARÉ...

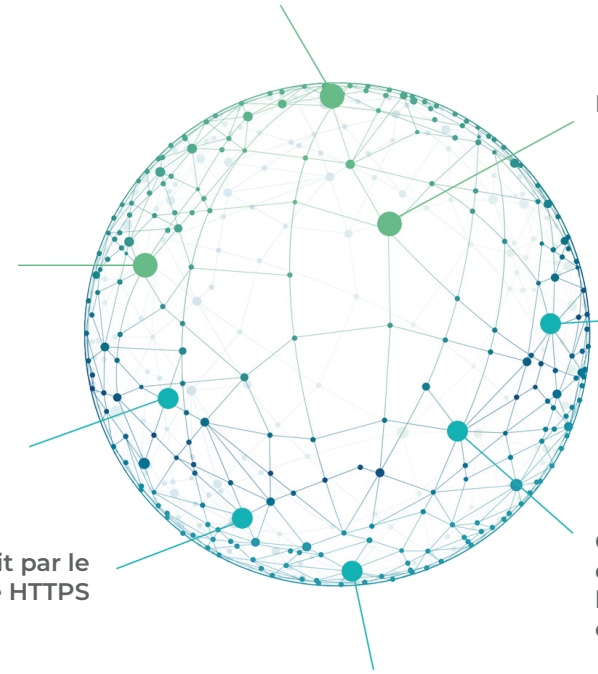
Open Bee intègre les technologies de sécurité informatiques les plus avancées pour un maximum de sécurité et de confidentialité.



Partage externe : mot de passe de protection + politique d'expiration

Double authentification

Permissions avancées (de l'accès consultation uniquement à l'édition totale, cachets électroniques dynamiques...)



Séparation des données : isolation logique pour séparer les données de chaque client les unes des autres

Fichiers et dossiers stockés chiffrés à l'aide de l'agorithme AES 256

Capacités approfondies d'enregistrement et de suivi de l'activité utilisateur et de l'historique des dossiers

Chiffrage en transit par le protocole HTTPS

Sauvegarde des données

openbee
THE ORGANIC SOFTWARE COMPANY

CONTACTEZ-NOUS

Open Bee propose une gamme compète de solutions concernant les contrôles d'accès, la sécurisation des données, du réseau et de l'analyse avec des fonctionnalités qui varient d'un appareil à un autre.

Contactez-nous aujourd'hui afin de définir ensemble la solution la plus adaptée à vos besoins de sécurisation de vos données et de votre environnement professionnel.

info@openbee.com
www.openbee.com

0809 541 920
+ 33 (0)4 50 64 99 29

Open Bee™ France
PAE Les Longeray
74370 Epagny Metz-Tessy