Sécurité Beekeeper

Livre blanc

Version 2022

BEEKEEPER

SOMMAIRE

CHARTE D'ENGAGEMENT

Beekeeper propose ses produits et services à de nombreuses entreprises du monde entier, dans divers segments de marché. Nos clients nous font confiance pour assurer la sécurité et la confidentialité de leurs données, et en retour, tous les **employés de Beekeeper s'engagent à se montrer dignes de cette confiance**.

À cette fin, la direction de l'entreprise met à leur disposition tous les outils et processus de sécurité de l'information dont ils ont besoin. Nous respectons notre engagement sans jamais compromettre la fluidité de la livraison des produits et services Beekeeper, et nous **garantissons la confidentialité, l'intégrité et la disponibilité des données de nos clients**.

Pour satisfaire, voire surpasser les attentes de nos clients, nous avons mis en place un système de gestion de la sécurité de l'information conforme aux **meilleures pratiques de sécurité de l'information et de confidentialité des données**, telles qu'elles sont décrites dans le processus de certification ISO 27001:2013, ISO 27017:2015 et ISO 27018:2019.

Le présent document atteste de notre engagement envers la protection des données de nos clients. Beekeeper restera vigilant et travaillera sans relâche pour continuer à améliorer notre système de gestion de la sécurité de l'information et respecter l'engagement que nous avons pris en matière de confidentialité des données envers nos clients et nos employés.

« Pour garantir votre droit à la protection des données et à la confidentialité, nous nous engageons à gérer le risque dans le respect des normes les plus élevées en matière de développement d'outils et de processus de sécurité. »

Cris Grossmann
PDG et cofondateur

LES PILIERS BEEKEEPER DE LA SÉCURITÉ

Beekeeper considère la confidentialité, l'intégrité et la disponibilité des données comme une priorité absolue. Nous démontrons notre engagement envers la protection continue des données des clients et les processus de confidentialité des données des manières suivantes :

1. Pour protéger les données de nos clients, Beekeeper utilise des technologies de sécurité des données de pointe et applique des pratiques complètes de défense en profondeur.

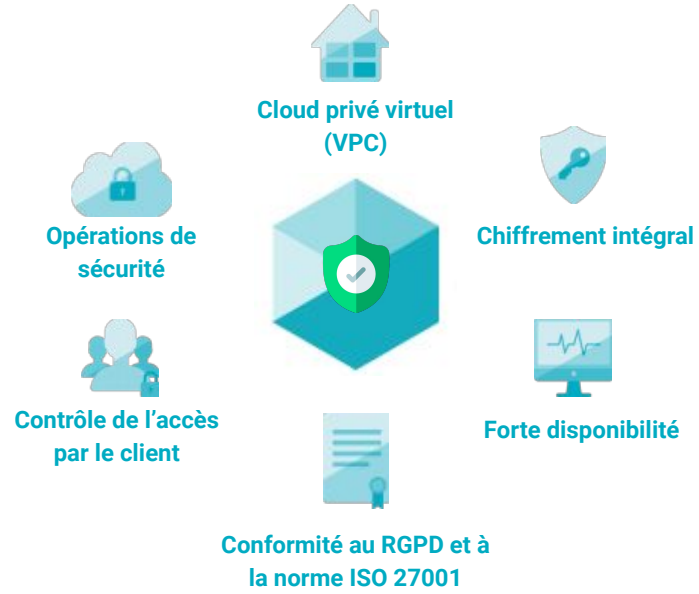
2. Beekeeper utilise un système de sécurité hautement performant pour surveiller en permanence son produit et sa plateforme afin de détecter les vulnérabilités de sécurité.

3. Disponible 24h/24, 7j/7, l'assistance technique de Beekeeper garantit un temps de réponse rapide pour détecter et répondre à toute menace de sécurité.

4. Beekeeper fait tout son possible pour mettre en œuvre et respecter les plus hautes normes de sécurité existantes et les contrôles de sécurité de l'information promus par l'Organisation internationale de normalisation (ISO).

5. Dans une démarche d'amélioration continue, Beekeeper s'engage à maintenir les normes de sécurité les plus élevées. À ce titre, Beekeeper est régulièrement soumis à des audits internes et externes indépendants et à des évaluations de sécurité.

Les pratiques de sécurité de Beekeeper sont structurées selon les six piliers de la sécurité de l'information présentés à droite. Chaque pilier contribue à l'utilisation de technologies et de contrôles de sécurité avancés. Ensemble, ils répondent aux exigences de notre système de gestion de la sécurité de l'information. Cette démarche va au-delà des exigences les plus rigoureuses du processus d'accréditation mondial validé par les normes ISO 27001:2013, ISO 27017:2015 et ISO 27018:2019.



LES PILIERS BEEKEEPER DE LA SÉCURITÉ

Cloud privé virtuel

Les produits et les services Beekeeper sont déployés dans des clouds privés virtuels régis par des mesures et des évaluations de la sécurité robustes. Tous nos clouds privés virtuels sont hébergés dans les centres de données certifiés de nos fournisseurs de solutions cloud. Nous proposons nos produits et services dans diverses juridictions, et nos clients peuvent choisir de stocker leurs données en Suisse, dans l'UE ou aux États-Unis.

Les tenants de nos clients dans nos clouds privés virtuels sont conçus pour être hautement sécurisés et disponibles. De plus, le contenu de chaque tenant client est entièrement isolé de nos autres tenants clients à l'aide de conteneurs logiques distincts, afin que chaque tenant agisse tel un environnement client indépendant.

Opérations de sécurité

Beekeeper a développé et applique des pratiques de sécurité extrêmement rigoureuses, en commençant par une mentalité Shift Left. La sécurité est prise en compte dès le début du cycle de vie produit, qui est basé sur une architecture de microservices. Des processus automatisés sont en place pour amener dans l'environnement de production le produit le plus récemment testé et dont la qualité a été rigoureusement contrôlée, ce avec une intervention humaine minimale.

Nous avons implémenté des capacités de journalisation et de surveillance robustes et modernes appuyées par des technologies de pointe. Nos audits et tests de sécurité incluent un programme complet de gestion des vulnérabilités. Le plan de réponse aux incidents de Beekeeper nous permet de gérer les situations et les incidents affectant la sécurité de manière standard et cohérente.

Contrôle de l'accès par le client

Beekeeper a été conçue en tant que plateforme de communication interne. Le client conserve le plein contrôle de l'accès à son tenant. Seuls les utilisateurs ayant un rôle administratif peuvent contrôler l'accès au tenant via le tableau de bord de Beekeeper ou les processus de contrôle automatisés.

Chiffrement intégral

Beekeeper utilise des techniques de chiffrement dans divers cas d'utilisation. Nous chiffrons notamment toutes les données transmises via les canaux de communication externes ainsi que les données au repos, qu'elles se trouvent dans un centre de stockage ou sur le terminal mobile de l'utilisateur final.

LES PILIERS DE LA SÉCURITÉ

Conformité au RGPD et à la norme ISO 27001 (suite)

Beekeeper respecte toutes les règles de protection des données personnelles du Règlement général sur la protection des données (RGPD), ainsi que d'autres exigences de confidentialité des données imposées par les juridictions. Beekeeper a mis en place un système de gestion de la sécurité de l'information certifié conforme à la norme ISO 27001:2013. Notre contrat de traitement des données lie Beekeeper à ses clients et précise toutes les exigences juridiques et réglementaires applicables. Beekeeper est certifié conforme aux normes ISO 27017:2015 et ISO 27018:2019. Ces normes de sécurité attestent de la conformité de Beekeeper en tant que prestataire SaaS, à la fois en tant que fournisseur de solutions cloud et en tant que responsable du traitement de données personnelles à l'aide de solutions cloud.

Forte disponibilité

Beekeeper assure que ses services seront disponibles 99,9 % du temps, conformément aux contrats d'abonnement conclus avec ses clients. Beekeeper remplit cette obligation avec une redondance multiple et des tests fréquents de la disponibilité des services.

CERTIFICATION ATTRIBUÉE À BEEKEEPER

L'Organisation internationale de normalisation est une organisation non gouvernementale indépendante composée de membres d'organismes nationaux de normalisation de 164 pays. La norme ISO 27001 regroupe les meilleures pratiques en matière de sécurité de l'information et de confidentialité des données clients. Elle énonce les exigences relatives à la mise en œuvre, au maintien et à l'amélioration d'un système de gestion de la sécurité de l'information. La norme ISO est le résultat d'un consensus d'experts du monde entier et de la mise en commun d'une vaste expérience internationale et de connaissances issues de tous les secteurs d'activité.

Les données qui relèvent des contrôles de gestion des risques mis en place par la norme ISO 27001 comprennent les coordonnées client ou employé et toute information à caractère personnel qui nous est confiée. De plus, les certifications ISO 27017 et ISO 27018 posent le cadre des objectifs de contrôle applicables aux fournisseurs de solutions cloud et aux responsables du traitement de données à caractère personnel dans un environnement basé sur le cloud.

Découvrez-en plus sur ce que Beekeeper a mis en œuvre pour obtenir les certifications de la série ISO 27000 et veiller à son adhérence continue aux normes de sécurité de l'information ISO 27001, 27017 et 27018.

Centres de données certifiés

Beekeeper fait uniquement appel à des fournisseurs de services de centre de données ayant obtenu des certificats de conformité reconnus à l'échelle internationale en matière de gestion de la sécurité de l'information :

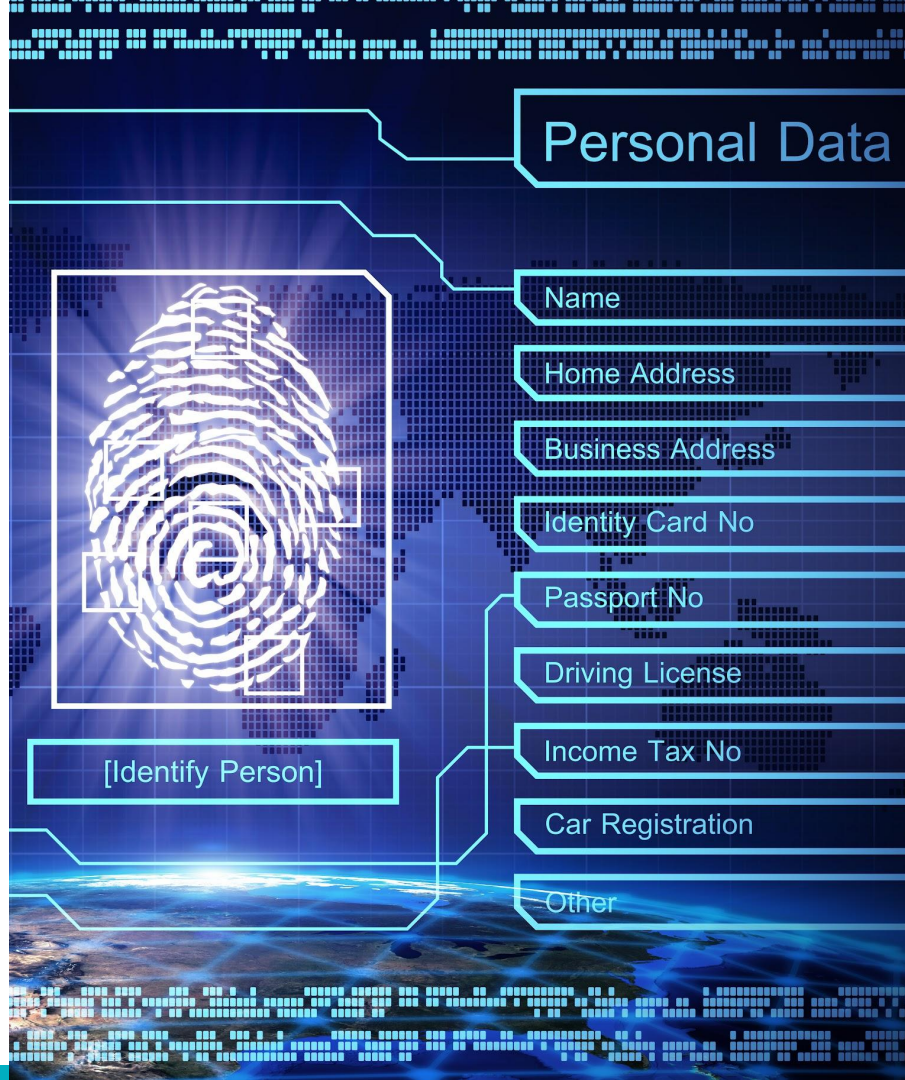
- Amazon Web Services : aws.amazon.com/compliance/
- Plateforme Google Cloud : cloud.google.com/security/compliance/

CONFIDENTIALITÉ DES DONNÉES

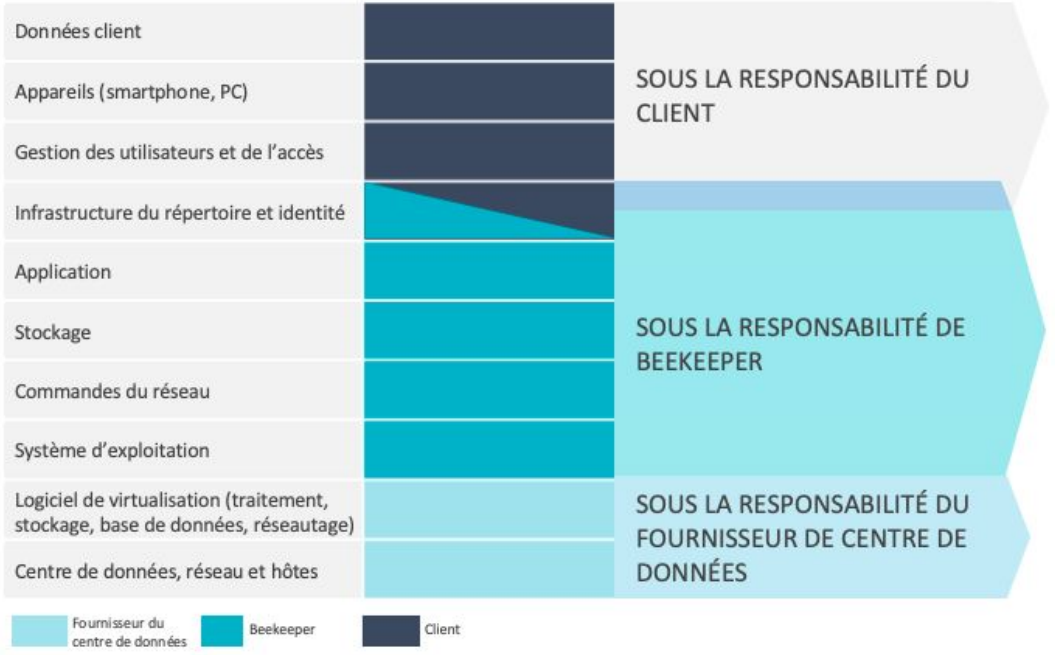
Nous avons pris pour modèle les exigences réglementaires les plus strictes du Règlement général sur la protection des données (RGPD) et de la Loi fédérale suisse sur la protection des données pour élaborer les exigences en matière de protection des données à caractère personnel inscrites dans notre Contrat de traitement des données et dans notre Politique de confidentialité.

Vos données sont traitées conformément aux sept principes de protection des données à caractère personnel énoncés dans le RGPD.

Les mesures techniques telles que l'utilisation de technologies de chiffrement sont standard et intégrées aux gammes de produits et services de Beekeeper. Divers processus, tels que des évaluations d'impact sur la vie privée avant le lancement de toute nouvelle gamme de produits ou de services, font partie intégrante du cycle de vie Beekeeper du développement de produits et services. La liste de ces processus organisationnels et techniques est disponible dans le Contrat de traitement des données (Annexe 2).



MODÈLE DE RESPONSABILITÉ PARTAGÉE



- Toutes les données client stockées et traitées dans Beekeeper
- Les appareils utilisés pour se connecter à Beekeeper et la façon dont ils sont gérés et sécurisés
- Le niveau d'accès au tenant Beekeeper qui est accordé aux comptes et aux utilisateurs

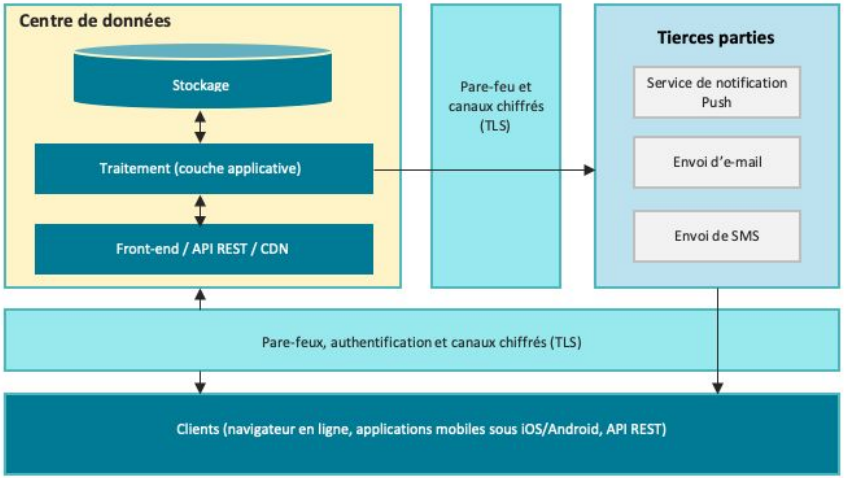
- *L'intégration des identités et des comptes peut être la responsabilité de tous*

- Confidentialité, intégrité et disponibilité de la plateforme Beekeeper et des données qui lui sont intégrées
- Chiffrement des données durant le transfert et au repos
- Haute disponibilité, sauvegarde et reprise après sinistre
- Sécurité du réseau, du cluster et de l'hôte, y compris le cloud privé virtuel, les sous-réseaux de pare-feu, les ressources à sécurité renforcée et les outils de sécurité

- Beekeeper est responsable des contrats avec les fournisseurs de centres de données chargés d'administrer les services de gestion et de virtualisation du cloud
- Exigences du centre de données haute disponibilité
- Contrôles du matériel et de l'environnement

ARCHITECTURE DE SÉCURITÉ

En tant que fournisseur de solution SaaS (Software as a Service), nous sécurisons notre plateforme cloud par une approche globale de défense en profondeur, comprenant une architecture à haute disponibilité, un contrôle de l'accès renforcé, une ségrégation sécurisée, des technologies de chiffrement, une sécurité renforcée et des sauvegardes fréquentes. Nos services sont déployés dans des clouds privés virtuels hautement sécurisés qui sont surveillés en permanence afin de détecter les menaces de sécurité et les vulnérabilités.



Stockage : Les données sont stockées à l'aide de services de stockage cloud avancés qui sont à la fois durables, hautement sécurisés, disponibles et performants.

Ségrégation : Chacun de nos clients est considéré comme un tenant indépendant et ses données sont isolées de celles de nos autres clients.

Pare-feux : Nous avons configuré des pare-feux de périmètre sur tous nos clouds privés virtuels. Nous avons également déployé un pare-feu applicatif web (WAF) pour protéger la couche applicative.

Connexions tiers : Les notifications push, les e-mails et les SMS sont envoyés via des fournisseurs tiers. Tous les canaux de communication auxquels ces tiers ont accès sont chiffrés à l'aide de protocoles sécurisés.

CHIFFREMENT ET GESTION DES CLÉS

Beekeeper a mis en place une politique et une procédure de chiffrement et de gestion des clés afin de protéger la confidentialité, l'authenticité et l'intégrité des informations par le chiffrement.

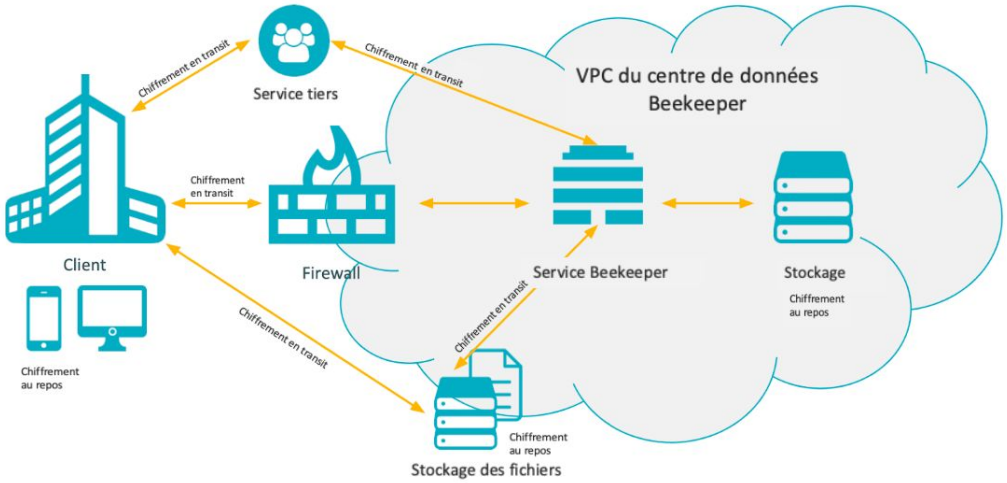
Au repos : Les données au repos sont chiffrées. Les bases de données des centres de données sont chiffrées à l'aide de l'algorithme de chiffrement symétrique AES 256. Les données des appareils fonctionnant sous iOS et Android sont chiffrées à l'aide de l'algorithme AES 256.

Durant le transfert : Toutes les communications vers la plateforme Beekeeper se font via des tunnels chiffrés utilisant les protocoles TLS 1.2 et 1.3. Grâce à des suites de codes robustes et un chiffrement basé sur l'algorithme AES 256 bits, ils garantissent la sécurité de la connexion lors du transfert de données dans un environnement internet non sécurisé.

Gestion des clés

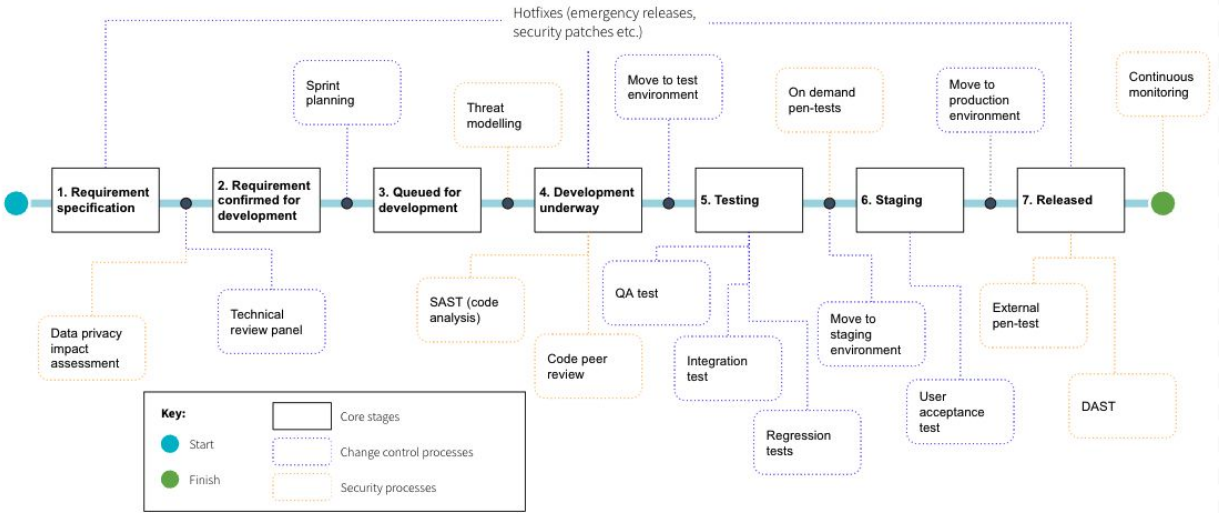
Conformément au modèle de responsabilité partagée, toutes les clés de chiffrement de l'infrastructure physique (c'est-à-dire les centres de données physiques) sont gérées par les fournisseurs de solutions cloud respectifs. Les clés de chiffrement utilisées pour la connexion et l'accès aux serveurs virtuels, aux bases de données, aux compartiments S3/de stockage et à la sauvegarde sont entièrement gérées par Beekeeper.

Diagramme de flux de données



CYCLE DE VIE DU DÉVELOPPEMENT PRODUIT

Beekeeper suit un processus de gestion des modifications clairement établi pour appliquer les modifications de code à ses produits et services. Notre équipe en charge du développement utilise des techniques de codage sécurisées et respecte les meilleures pratiques définies par les méthodologies OWASP ou SANS. Les développeurs sont formés aux pratiques de développement applicatif sécurisé dès leur intégration à l'entreprise et de manière continue par la suite. Élaborée pour satisfaire aux objectifs de contrôle de la norme ISO 27001, la politique de sécurité de l'information de Beekeeper impose une stricte séparation des tâches et des environnements afin de garantir la confidentialité, l'intégrité et la disponibilité de nos systèmes d'information.



- Beekeeper a élaboré un programme formel de gestion du changement pour s'assurer que les changements apportés aux processus officiels sont suivis en cas de modification des systèmes/applications.
- Les environnements de développement, de préproduction et de production sont isolés les uns des autres.
- Seuls les utilisateurs autorisés peuvent accéder aux applications permettant de modifier les systèmes de production.
- Les processus de sécurité sont entièrement intégrés au cycle de vie du changement et du développement produit.
- Beekeeper a élaboré et mis en œuvre un programme formel de gestion des correctifs de sécurité.

TESTS DE SÉCURITÉ ET ASSURANCE QUALITÉ

Tests de sécurité externes

Notre politique de sécurité de l'information nous contraint à faire appel à des cabinets d' évaluation indépendants pour effectuer nos tests d'intrusion annuels. Leurs conclusions sont toutes enregistrées dans notre inventaire des risques, et des mesures d'atténuation sont élaborées et mises en œuvre conformément à nos processus de gestion du changement.

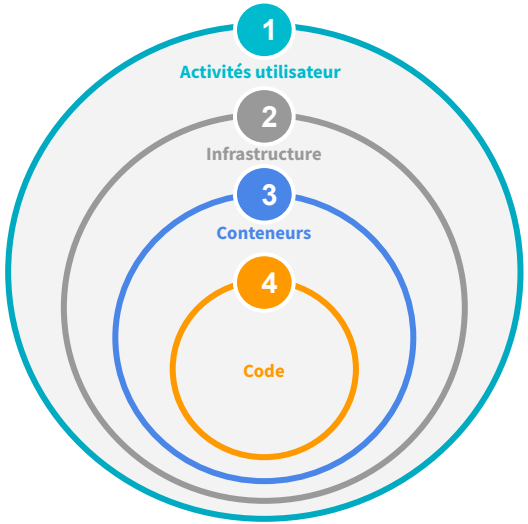
Tests de sécurité internes

Les tests de vulnérabilité internes suivants sont automatisés :

- Indépendamment de toute modification apportée au code :
  - Analyse quotidienne du certificat SSL
  - Analyse hebdomadaire de la configuration, suivi de l'activité et comparaison avec les meilleures pratiques figurant dans la bibliothèque
  - Tests hebdomadaires dynamiques de la sécurité des applications
- Pour toute modification apportée au code :
  - Évaluation par les pairs obligatoire
  - Tests statiques de la sécurité des applications
  - Suites de tests unitaires et d'intégration axées sur les permissions d'accès
  - Évaluation des vulnérabilités de la bibliothèque système

CONNEXION ET SUIVI

Nous avons développé et implémenté des capacités de journalisation et de surveillance robustes et modernes appuyées par des technologies de pointe. Nous disposons d'outils spécifiques et de processus solides pour la collecte, la corrélation et la conservation des journaux. Nous déployons le WAF devant toutes nos applications pour surveiller et filtrer en permanence les trafics suspects. Nous suivons une approche Confiance Zéro qui nous permet de détecter les activités suspectes des utilisateurs au sein de notre réseau. Les ingénieurs de notre service d'assistance sont disponibles 24h/24, 7j/7 pour répondre à tout événement de sécurité qui surviendrait en dehors des heures de bureau.



Couches de journalisation et de surveillance chez Beekeeper

1. Activités utilisateur

Nous enregistrons toutes les activités des utilisateurs, y compris les informations suivantes : adresse IP, nom d'utilisateur et identifiant, heure et date, type d'activités tentées et réalisées et systèmes consultés.

2. Infrastructure

En plus des services cloud natifs (par exemple, GuardDuty), nous exécutons des solutions supplémentaires pour enregistrer et suivre les données IAM, VPC et DNS, ainsi que d'autres événements liés à la sécurité.

3. Conteneurs

Nous avons mis en place des outils avancés qui nous permettent de journaliser, surveiller et agréger les événements de sécurité strictement liés aux conteneurs, ainsi que de lancer l'alerte.

4. Code

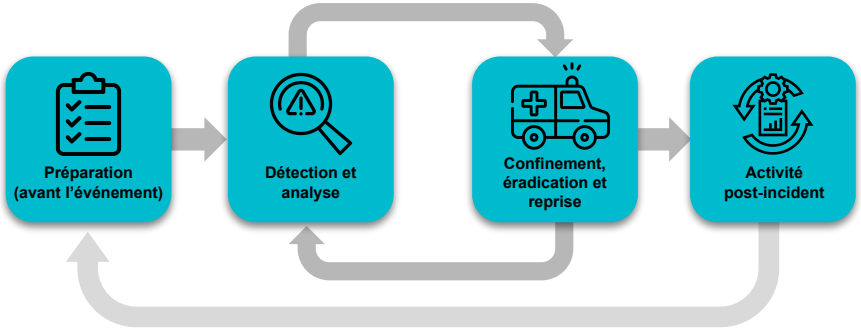
Nous surveillons activement notre codebase et nos bibliothèques pour identifier les vulnérabilités connues/divulguées. De plus, nous maintenons un inventaire de nos bibliothèques publiques, dépôts et dépendances.

RÉPONSE AUX INCIDENTS ET NOTIFICATIONS

Pour faire face aux incidents, nous avons élaboré un plan de réponse, ainsi qu'un plan d'urgence qui est déclenché lorsqu'un incident est remonté conformément à notre échelle de gravité des incidents. Afin de gérer au mieux les cyberattaques, notre plan de réponse aux incidents suit le guide de traitement des incidents de sécurité informatique du NIST. Ce plan comprend quatre phases :

Phase 1 : Préparation (avant l'événement)
Phase 2 : Détection et analyse
Phase 3 : Confinement, éradication et reprise
Phase 4 : Post-incident

Ce déploiement en quatre phases nous permet de gérer de façon souple les situations et les incidents affectant la sécurité de manière standard et cohérente.



Conformément aux réglementations applicables en matière de protection des données (CCPA ou RGPD, par exemple), Beekeeper vous informera de toute violation des données personnelles dans les plus brefs délais, et si possible, dans les 72 heures après en avoir pris connaissance. Pour ce faire, Beekeeper suivra son processus de notification et de gestion des incidents.

Notre processus de notification et de gestion des incidents est conforme aux objectifs de contrôle définis par la norme ISO 27001/27017/27018 relative à la gestion des incidents ainsi que par les articles 33 et 34 du RGPD. Ces deux textes de référence sont tous deux reflétés dans notre Contrat de traitement des données.

PLAN DE REPRISE APRÈS SINISTRE

Notre plan de reprise après sinistre vise à préparer Beekeeper à faire face à toute interruption de service prolongée causée par des facteurs indépendants de notre volonté (catastrophes naturelles ou événements d'origine humaine) et à rétablir les services dans toute la mesure possible en un minimum de temps. Nous avons élaboré un plan de reprise après sinistre pour chacun de nos centres de données et testons et évaluons trimestriellement l'efficacité de ces plans afin de procéder à des mises à jour en fonction des conclusions de ces tests.

Conservation des données et reprise

Conformément aux objectifs de contrôle de la norme ISO 27001 pour la continuité des activités et la reprise après sinistre, Beekeeper utilise des services de conservation des données gérés par ses fournisseurs de centres de données certifiés. Nos solutions sont conçues avec des capacités de redondance complètes et testées de nombreuses fois tout au long de l'année. Toutes les zones de disponibilité sont limitées à la même juridiction que le centre de données utilisé par Beekeeper. La plupart de nos services fonctionnent en mode sans état, de sorte qu'en cas de catastrophe, nous puissions fournir de nouveaux services et que les données soient disponibles à partir de la base de données.

Notre base de données fonctionne avec des zones multi-disponibilité pour améliorer la durabilité et la disponibilité (c'est-à-dire que la base de données principale se réplique de manière synchrone sur une instance de secours dans une zone de disponibilité différente). En cas de sinistre, Beekeeper s'appuie sur les sauvegardes automatisées et les instantanés de base de données effectués par notre fournisseur de centre de données. Le chiffrement au repos est également mis en œuvre pour tous les systèmes de sauvegarde.

ACCÈS À BEEKEEPER

Beekeeper est accessible via plusieurs interfaces numériques. Chaque interface fournit des paramètres de sécurité qui protègent les données des utilisateurs tout en garantissant l'accessibilité.

Navigateurs web : Les navigateurs ne stockent qu'un cookie sécurisé qui authentifie l'utilisateur actuel. Il n'y a pas de stockage local des données clients via cette interface.

Applications mobiles : Sur Android et iOS, les identifiants sont stockés dans les conteneurs chiffrés fournis par le système d'exploitation.

API REST sur mesure : Beekeeper a développé une API REST et fournit des ressources permettant de mettre en évidence les meilleures pratiques de sécurité lors de la programmation de clients personnalisés.

Connexions à Beekeeper

Toutes les connexions à Beekeeper se font via le protocole HTTPS (TLS 1.2 et 1.3 uniquement). Toute tentative de connexion via HTTP est redirigée vers HTTPS.

CONTRÔLE DE L'ACCÈS

Beekeeper considère le contrôle de l'accès comme étant composé de deux éléments clés :

- Authentification
- Autorisation

Pour gérer les exigences de contrôle d'accès, Beekeeper a développé des systèmes et des interfaces, ainsi qu'un tableau de bord de contrôle.

Authentification

Pour les processus internes, régis par les exigences énoncées dans nos principes de contrôle de l'accès aux produits et services Beekeeper, Beekeeper exige une authentification à deux facteurs pour ses employés.

Pour l'accès client, Beekeeper est en mesure d'assurer la conformité à la politique de l'entreprise lorsque l'authentification à deux facteurs est disponible via une solution d'authentification unique (SSO). Beekeeper peut également se connecter à l'annuaire des utilisateurs de l'entreprise, mais aussi envisager tout autre type de mécanisme d'authentification.

Autorisation

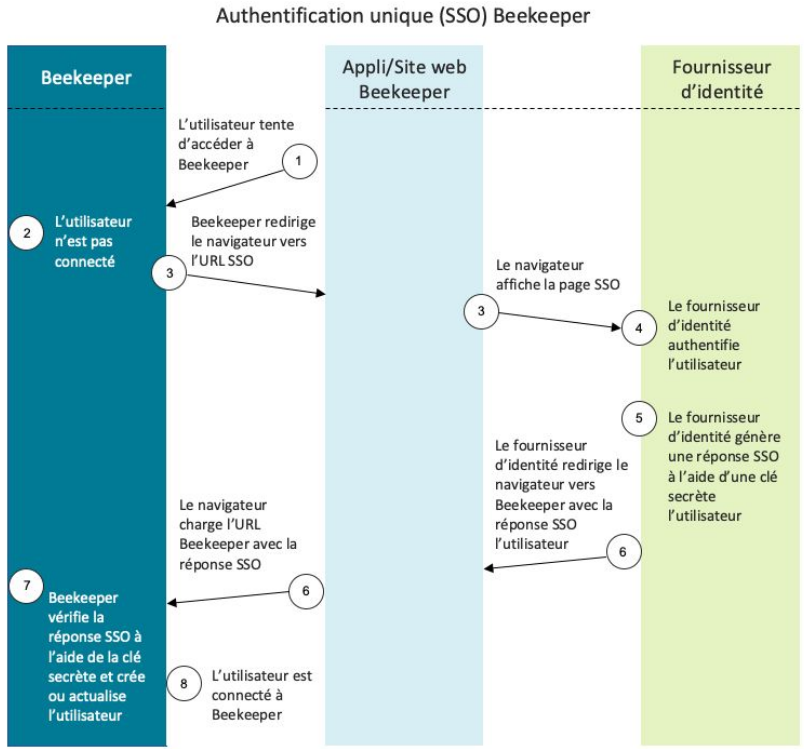
Beekeeper utilise un serveur d'autorisation conforme aux normes de l'industrie, qui est chargé de fournir les droits nécessaires pour accéder aux systèmes Beekeeper. L'administrateur défini par le client peut accéder à certaines fonctionnalités des capacités d'autorisation de Beekeeper via le tableau de bord Beekeeper.

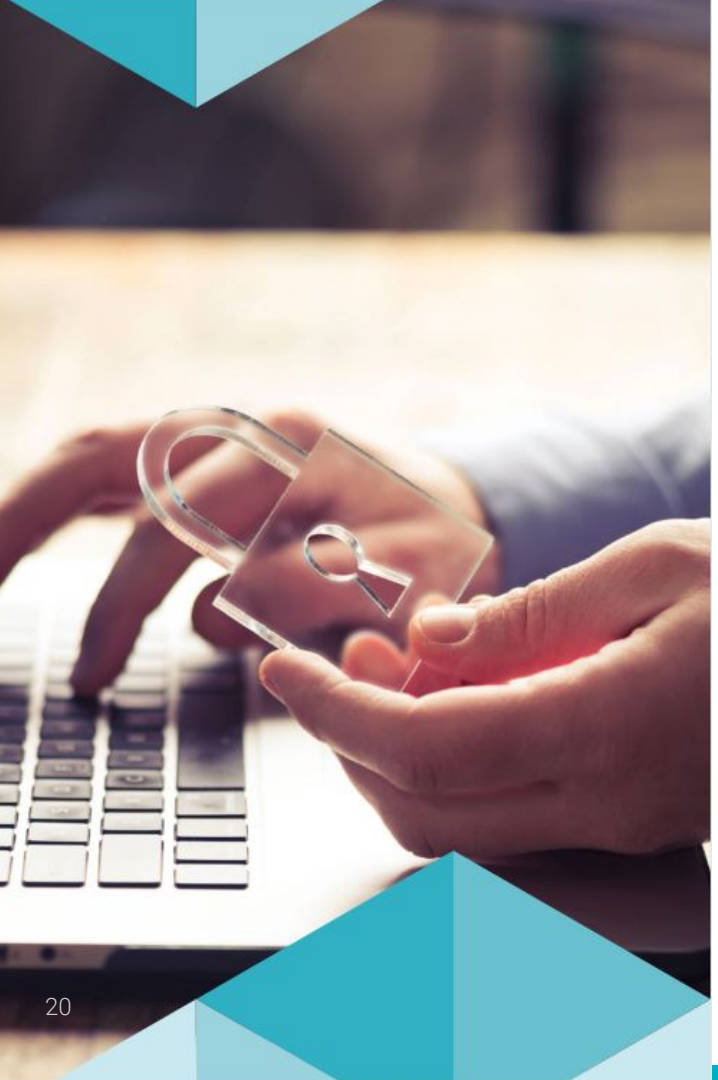
CONTRÔLE DE L'ACCÈS

Tableau de bord de Beekeeper

Les administrateurs définis par l'entreprise peuvent utiliser le tableau de bord Beekeeper via des canaux de communication internes sécurisés pour contrôler les fonctions d'administrateur utilisateur suivantes :

- Créer, mettre à jour ou supprimer un utilisateur
- Déconnecter un utilisateur actif
- Suspendre un accès utilisateur
- Configurer l'authentification unique SAML
- Importer et actualiser en masse les utilisateurs depuis un fichier Excel





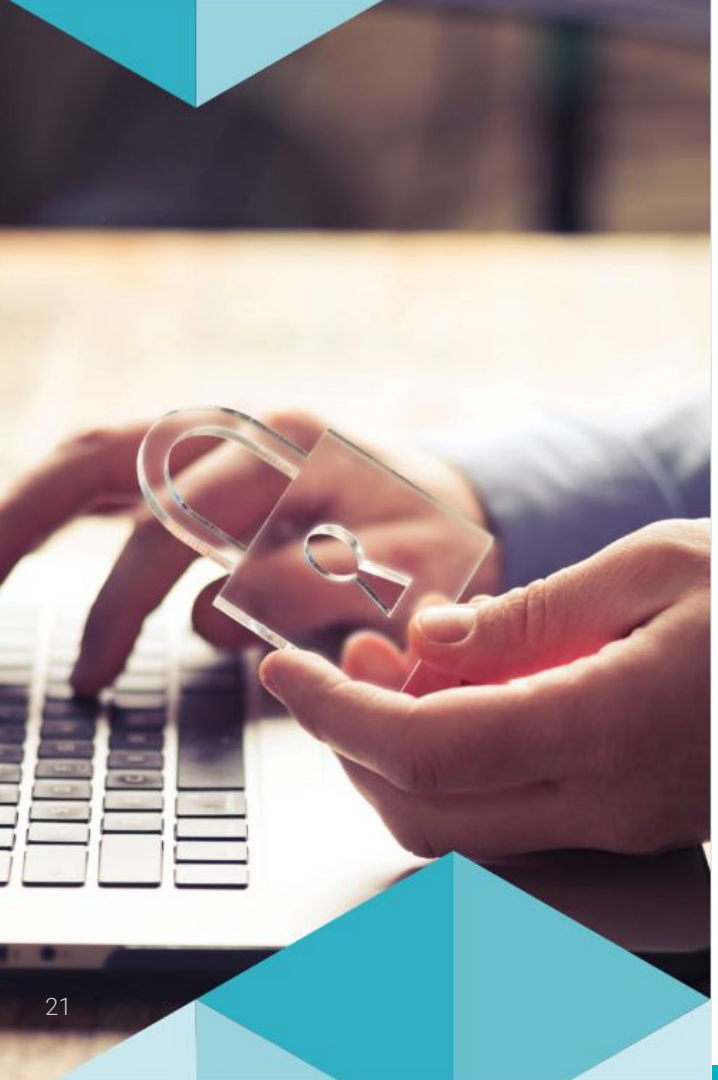
CARACTÉRISTIQUES DE SÉCURITÉ DU PRODUIT

Authentification

- Connexion à l'aide d'une adresse e-mail, d'un numéro de téléphone ou d'un nom d'utilisateur associé à un mot de passe
- Critères de force du mot de passe prédéfinis (8 caractères ou plus, lettres majuscules et minuscules et au moins un caractère numérique)
- Les administrateurs peuvent réinitialiser les mots de passe
- Après la première connexion, le mot de passe doit être modifié
- Lors de la réinitialisation du mot de passe, aucun mot de passe précédemment utilisé ne peut être choisi
- Déconnexion automatique des utilisateurs après X jours (le nombre de jours est défini par les administrateurs)
- Connexion à l'application mobile via le QR code
- Alerte e-mail à propos de la connexion via un QR code à usage unique
- Les administrateurs peuvent déconnecter les utilisateurs et suspendre les comptes
- La déconnexion d'un utilisateur par un administrateur déconnectera l'utilisateur de chaque appareil où il est connecté
- Compte verrouillé après 10 tentatives de connexion infructueuses

Autorisation

- Chaque utilisateur se voit attribuer un rôle, qui définit ce qu'il est en droit de faire dans l'application (se reporter au centre d'aide des administrateurs).



CARACTÉRISTIQUES DE SÉCURITÉ DU PRODUIT

- Expiration de la session
  - Le délai sous lequel expire une session peut être configuré pour les utilisateurs accédant à Beekeeper à partir d'un ordinateur public.
- Suspension d'un utilisateur
  - Les administrateurs peuvent suspendre des utilisateurs à tout moment. Un utilisateur suspendu sera immédiatement déconnecté de tous ses points d'accès et perdra l'accès à toutes les données. Les données d'un utilisateur suspendu sont conservées et peuvent être mises à disposition de la justice.
- Liste des domaines autorisés et interdits d'accès pour empêcher certains domaines de messagerie de se connecter
- Authentification unique (SAML)
- Alerte par e-mail lors de la connexion sur un appareil jusqu'alors inconnu
- Sauvegarde
  - Des sauvegardes régulières des informations utilisateur et de toutes les données sont effectuées pour éviter leur destruction accidentelle ou malveillante.
- Rôles
  - Rôles disponibles : administrateur général, administrateur d'unité organisationnelle, administrateur de groupe, administrateur de stream et modérateur de contenu (se reporter au centre d'aide des administrateurs).
- Surveillance des activités disponible via le méta-tableau de bord (le client doit demander l'accès aux données pour voir ces informations)
  - Possibilité d'afficher la dernière connexion et les informations sur l'appareil
  - Liste des appareils utilisés pour se connecter
- Antivirus pour analyser les fichiers envoyés via l'application Beekeeper
- Interdire ou restreindre la possibilité d'intégrer l'application dans une autre page

RÉPONSES AUX QUESTIONS LES PLUS FRÉQUENTES

Q : Les données et les messages peuvent-ils être exportés à des fins d'archivage ou de révision interne ?
R : Oui, selon un processus défini, Beekeeper peut octroyer un accès aux données à des fins d'automatisation de l'archivage.

Q : Les rapports des tests d'intrusion de sécurité sont-ils disponibles pour examen ?
R : Oui, nous pouvons partager les rapports des tests d'intrusion réalisés précédemment sur simple demande.

Q : La plateforme Beekeeper est-elle hébergée sur une infrastructure cloud partagée ?
R : Oui, mais nos centres de données certifiés offrent des fonctionnalités de cloud privé virtuel (VPC) pour garantir l'isolement de vos données des données de nos autres clients.

Q : Proposez-vous un service d'hébergement sur site ?
R : Nous ne proposons pas de solution d'hébergement sur site.

Q : Un journal d'audit est-il disponible ?
R : Un journal d'audit peut être mis à disposition de nos clients au format CSV.

Q : Les produits et services Beekeeper sont-ils conformes à l'HIPAA ?
R : Les produits et services Beekeeper satisfont aux exigences définies par les contrôles de sécurité de l'HIPAA, du fait de la mise en place d'un système de gestion de la sécurité de l'information reprenant les meilleures pratiques de sécurité de l'information décrites par l'organisme d'accréditation de l'ISO 27001. Notons que Beekeeper est une plateforme de communication interne et non une plateforme de traitement de données de santé.

Q : Qu'en est-il des services d'assistance et de maintenance de Beekeeper ?
R : En tant que solution SaaS, le produit de Beekeeper est pris en charge et actualisé à partir des centres d'assistance de Beekeeper situés à Zurich (Suisse) et à Cracovie (Pologne). Beekeeper fournit également des services d'assistance locaux depuis ses bureaux aux États-Unis et en Allemagne.

Pour plus d'informations, consultez beekeeper.io/security.

Contactez-nous
Si vous avez d'autres questions liées à la sécurité, contactez-nous à security@beekeeper.io.

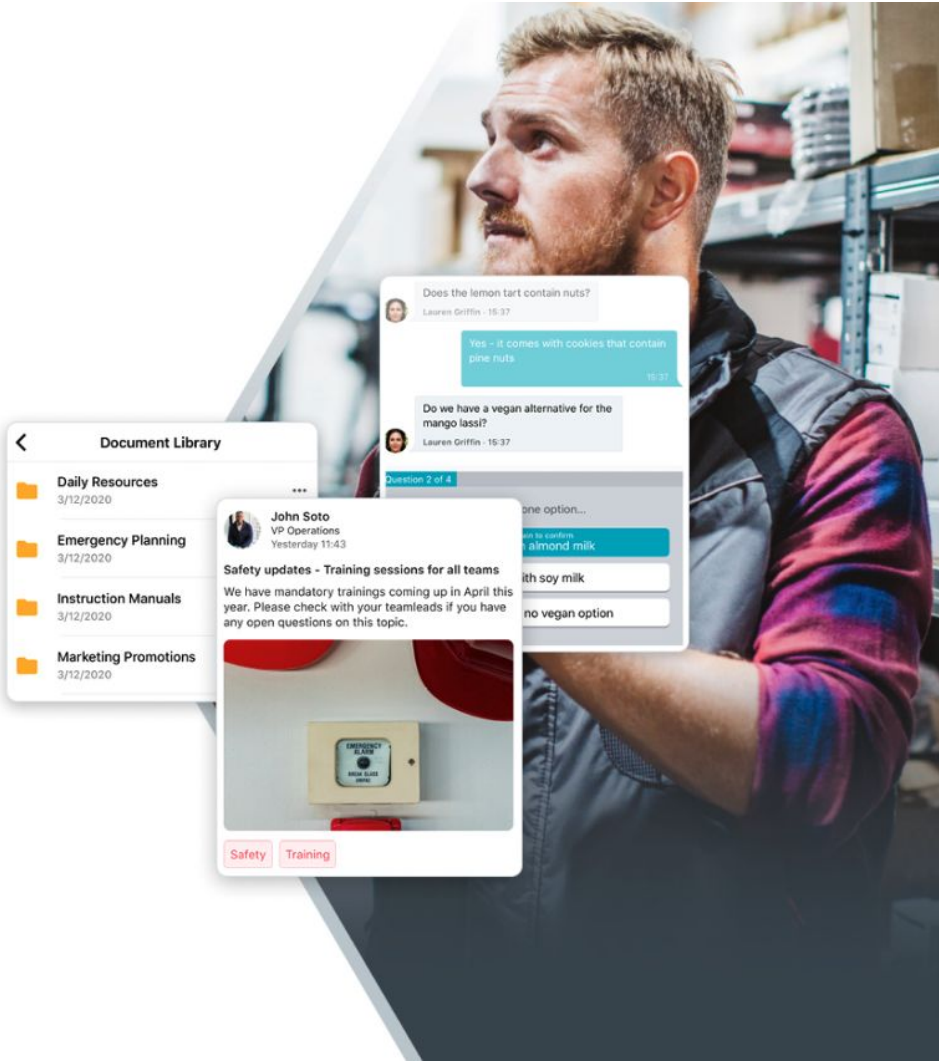
BEEKEEPER

Beekeeper transforme la façon dont les entreprises de terrain fonctionnent. Conçue pour le terrain, notre plateforme aide les entreprises à se défaire des processus papier et manuels pour améliorer l'engagement, la rétention et la performance des employés.

Collaborateurs, processus, systèmes... Permettez à vos employés d'accéder à tout ce dont ils ont besoin pour donner le meilleur d'eux-mêmes. Les entreprises du monde entier utilisent Beekeeper pour connecter leurs équipes, unifier leurs systèmes et développer leur activité.

Premiers pas

Pour plus d'informations, consultez beekeeper.io/security.



Date de version (R3.0) : Juin 2022