monday.com
Livre blanc sur la sécurité et la confidentialité

Date	Version	Description de la modification
Novembre 2021	1.0	Version finale

Table des matières

Ce livre blanc a pour but de présenter les pratiques de sécurité et de confidentialité en vigueur chez monday.com à la date de publication de ce livre blanc. Celles-ci sont susceptibles d'être modifiées sans préavis. Toute description des plans futurs peut être modifiée ou retardée à la seule discrétion de monday.com. Ce livre blanc est fourni à titre d'information uniquement et ne constitue pas un avis juridique ou ne doit pas être interprété comme complétant ou s'incorporant dans les modalités d'un contrat.

1. Introduction

Le système d'exploitation pour le travail (Work OS) de monday.com gère les données de plus de 127 000 entreprises dans le monde. C'est pourquoi nous nous engageons à faire bénéficier nos clients des normes les plus élevées en matière de sécurité et de protection des données. Nous gagnons la confiance de nos clients en faisant de la sécurité des données notre priorité.

Énoncé de notre mission

Assurer la sérénité de nos clients tout en gérant leurs données dans le Work OS de monday.com.

Nos équipes

Les efforts en matière de sécurité des informations de monday.com sont guidés et surveillés par notre CISO, notre équipe en charge de la sécurité et un groupe dédié à la sécurité composé de représentants des équipes Infrastructure, R et D, Opérations et TI.
Les efforts en matière de protection de la vie privée de monday.com sont guidés et surveillés par notre groupe chargé de la protection de la vie privée, composé de représentants des équipes Juridique, Protection de la vie privée et Sécurité, sous la direction de notre DPO.

Liens utiles

Centre de confiance monday.com
Portail juridique monday.com
Page des statuts monday.com
Sous-traitants, filiales et support
Sécurité et confidentialité chez monday.com - FAQ
Signalement de vulnérabilités
Support et base de connaissances
Tarifs et plans
Blog sur l'ingénierie monday.com

---

2. Sécurité de l'infrastructure

Prestataires d'hébergement

Pour atteindre une haute disponibilité et une résilience élevée, notre service est hébergé sur l'infrastructure Amazon Web Services (AWS) dans plusieurs régions, principalement en Virginie du Nord (États-Unis) et à Francfort (Allemagne),[1] dans plusieurs zones de disponibilité, avec des déploiements dédiés de reprise après sinistre établis dans différentes régions. Les comptes clients sont liés à une seule région.

Dans le cadre de son modèle de responsabilité partagée; AWS gère la sécurité de l'infrastructure de cloud computing, tandis que monday.com gère la sécurité des logiciels et des données résidant dans cette infrastructure.

Notre fonction Activity Log (journal des activités) (décrite plus loin dans ce document) sauvegarde les données sur la plate-forme Google Cloud (GCP) aux États-Unis.

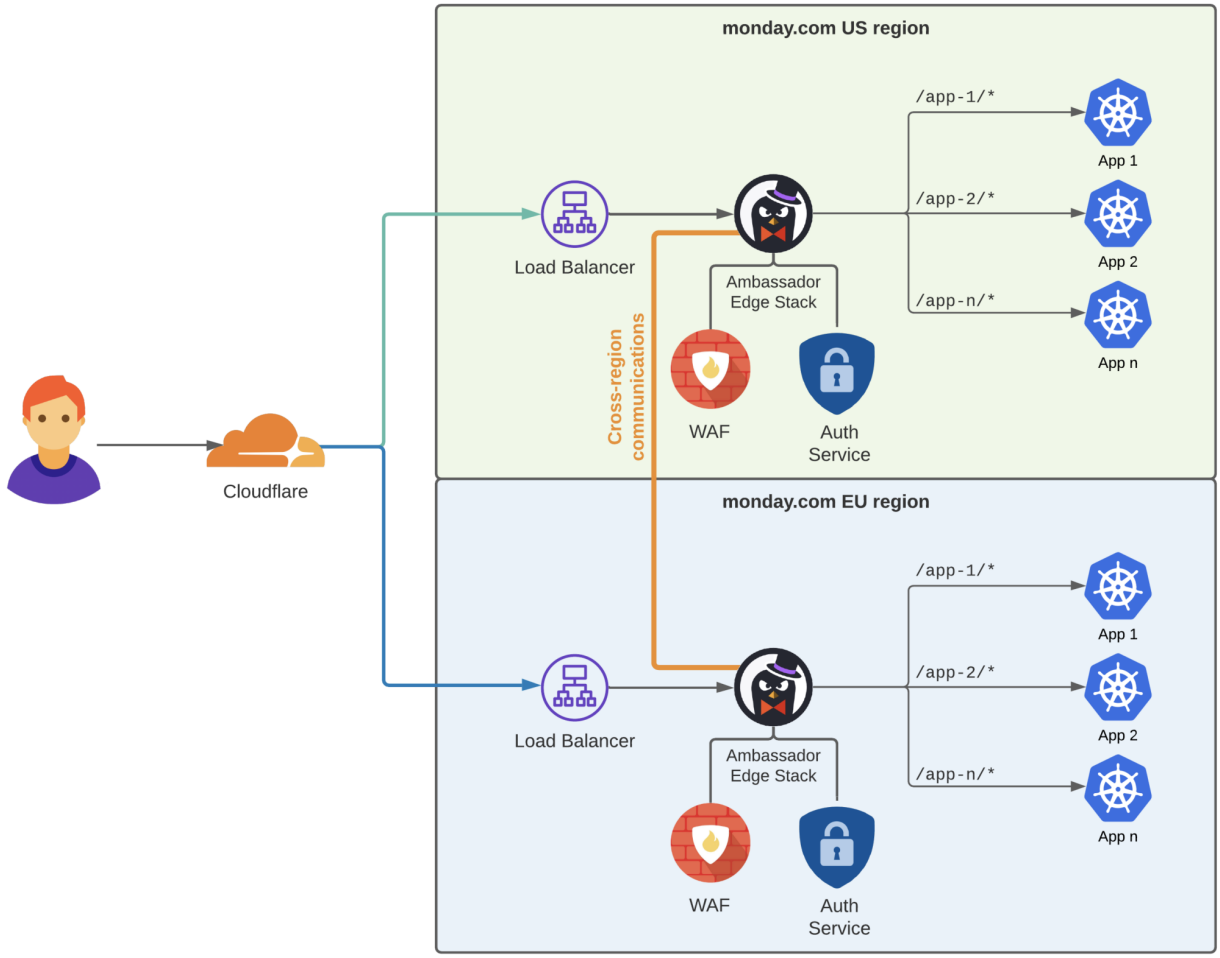
Architecture réseau

- L'architecture réseau de monday.com est conçue selon les meilleures pratiques d'AWS, y compris la séparation des sous-réseaux publics et privés.
- monday.com utilise plusieurs fournisseurs de CDN, dont Cloudflare et Fastly, pour empêcher les attaques de type DDoS et celles par force brute. La limitation de débit est configurée à la fois en périphérie et au niveau de l'application.
- Les équilibreurs de charge résident dans le sous-réseau public, tandis que les composants réseau internes, tels que les serveurs d'applications Web et les bases de données, résident dans le sous-réseau privé et n'ont pas d'adresse IP publique qui leur est attribuée.
- Un pare-feu d'application Web (WAF) est en place pour bloquer de façon dynamique des attaques basées sur le contenu.
- Des pare-feu sont utilisés dans l'ensemble du réseau pour appliquer les autorisations de la liste blanche d'adresses IP et accorder un accès via les ports autorisés uniquement aux ressources du réseau. Les règles des groupes de sécurité sont configurées pour autoriser l'accès uniquement à partir des ports requis.
- Les capteurs du système de détection d'intrusion dans le réseau (NIDS) sont utilisés de concert avec les services de sécurité natifs d'AWS qui sont activés pour toutes les ressources de production.

Vous trouverez à la suite les points saillants du schéma de réseau monday.com, tant dans la région de données des États-Unis que dans celle de l'UE :[2]

[1] Les clients du plan Entreprise peuvent choisir d'héberger leurs données dans notre centre de données de l'UE à Francfort, en Allemagne.

[2] Un schéma de réseau en grille de haut niveau peut être partagé en fonction de la demande et sous réserve de la conclusion d'un accord de non-divulgation mutuel.



L'infrastructure en tant que code est largement utilisée pour garantir le suivi et l'audit des modifications de configuration. L'équipe Infrastructure de monday.com effectue chaque trimestre un examen approfondi de la configuration du réseau périphérique et apporte toutes les modifications jugées nécessaires pour maintenir ou augmenter la sécurité.

Partenaire technologique du niveau AWS Avancé

monday.com est également un partenaire technologique du niveau AWS Avancé, ce qui atteste qu'AWS a elle-même rigoureusement approuvé notre organisation s'agissant de son infrastructure, de la sécurité de ses informations, de sa conception des pratiques exemplaires, et plus encore.

Sécurité du réseau

monday.com étant une solution purement basée sur le cloud, nous avons l'avantage d'utiliser des moyens de contrôle modernes et adaptés pour obtenir une vue précise du périmètre de notre réseau. Nous recueillons et surveillons les journaux réseau à l'aide d'un système NIDS (Network Intrusion Detection System) et des journaux de trafic provenant d'emplacements à la périphérie. Nous examinons aussi les alarmes pertinentes via notre système SIEM (Security Information and

Event Management). Nous utilisons des outils de surveillance de la sécurité qui récupèrent fréquemment la configuration de nos groupes de sécurité et de nos listes de contrôle d'accès réseau auprès du fournisseur de services dans le cloud, en plus d'établir une vue d'ensemble complète de notre réseau.

L'équipe Infrastructure de monday.com effectue chaque trimestre un examen approfondi de la configuration du réseau périphérique et apporte toutes les modifications jugées nécessaires pour maintenir ou augmenter la sécurité. De plus, nous faisons appel chaque année à un auditeur indépendant pour examiner la configuration de notre réseau.

Accès à la production

L'accès aux ressources de production est accordé en fonction du rôle et conformément aux principes du besoin de savoir et des privilèges les moins élevés. Les privilèges administratifs ne sont accordés qu'au personnel de notre équipe Infrastructure (une petite équipe d'ingénieurs experts). Tous les accès aux serveurs monday.com nécessitent l'utilisation de notre VPN, qui est authentifié via notre fournisseur d'identité d'entreprise (IdP), entièrement audité et applique des règles de complexité des mots de passe ainsi qu'une authentification multi-facteur (MFA).
L'accès aux ressources de production par nos développeurs se fait à l'aide du transfert de port Kubernetes et s'effectue également en vertu d'une authentification via notre IdP.

Renforcement

Les serveurs sont basés sur la dernière version d'Ubuntu LTS (20.04), renforcée en conformité avec les normes CIS (Center for Internet Security).

Base de données

Les bases de données utilisées par monday.com incluent MySQL, Elasticsearch et Redis. Les clés API des systèmes externes, utilisées par nos fonctions d'intégration, sont stockées dans un cluster HashiCorp Vault dédié à réplication automatique.

Stockage de fichiers

Le stockage de fichiers est hébergé sur Simple Storage Service (S3), fourni par AWS, qui stocke les pièces jointes et les sauvegardes de la base de données. Les pièces jointes contiennent tous les fichiers transmis par un client sur le service monday.com.
monday.com fournit un service automatisé de détection des programmes malveillants dans les fichiers transmis sur le service par les utilisateurs, ce qui garantit que les fichiers tiers chargés sur le service ne seront pas infectés. Nous avons en outre une liste noire contenant une liste des extensions de fichier interdites. La liste noire des extensions de fichier désigne celles qui peuvent être considérées comme dangereuses, telles que les exécutables ou le format HTML. En bloquant ces types de fichiers, nous réduisons considérablement le risque d'infection par des programmes malveillants.

Multi-région

Depuis janvier 2021, monday.com a étendu sa portée avec sa première région de données européenne à Francfort, en Allemagne (actuellement disponible pour les clients du plan Entreprise). En raison des principes identiques relatifs à l'infrastructure dans la région des États-Unis, les clients monday.com de l'UE peuvent profiter du même niveau de mesures et de contrôles de sécurité monday.com, à savoir qu'ils bénéficieront des mêmes principes de confidentialité, d'intégrité et de disponibilité.
Les principales caractéristiques de l'architecture réseau monday.com sont illustrées ci-dessus.

Nous prévoyons d'ouvrir ultérieurement des centres de données dans d'autres régions.

Chiffrement et gestion des clés

Chiffrement en transit

Les données en transit sur des réseaux ouverts sont chiffrées à l'aide du protocole TLS 1.3 (au minimum, TLS 1.2).

Chiffrement au repos

Les données au repos sont chiffrées à l'aide du protocole AES-256. Les clés de chiffrement sont stockées via le service de gestion des clés (KMS) d'AWS. Une clé client principale (CMK) à rotation annuelle est actuellement utilisée pour chiffrer toutes les données client soumises au service monday.com et traitées pour leur compte.

Séparation des locataires

Notre environnement multilocataire est doté d'une séparation logique entre les clients. Les données clients sont séparées au niveau de l'application à l'aide d'identifiants uniques qui résultent d'une combinaison de plusieurs paramètres.

Nous travaillons actuellement à l'activation du chiffrement au niveau des locataires (TLE ou Tenant-level encryption) pour nos clients. Le TLE est une couche qui garantit que les données au repos sont chiffrées avec une clé dédiée par compte, ce qui offre une protection contre la consultation des données par des systèmes ou du personnel non autorisés.

Le TLE offre une protection contre deux scénarios principaux :

1. **Attaquants :** les données des champs de la base de données sont chiffrées, de sorte qu'un pirate obtenant un accès à la base de données pour en extraire des données n'obtiendra que des données chiffrées.
2. **Partage accidentel :** les données sont chiffrées au moyen d'une clé dédiée par compte. Par conséquent, si les données sont accidentellement partagées entre les comptes, elles ne seront jamais partagées en texte clair.

Nous prévoyons de proposer aux clients du plan Enterprise la possibilité d'apporter leurs propres clés de chiffrement (BYOK ou Bring Your Own Key).

Sauvegarde

monday.com sauvegarde les données de ses clients soumises au service monday.com et traitées en leur nom. Nous sauvegardons systématiquement les données utilisateur toutes les cinq minutes et distribuons les sauvegardes chiffrées dans plusieurs zones de disponibilité AWS. Nous avons également établi des sites de reprise après sinistre dans des régions AWS distinctes à des fins de redondance. Les données du journal des activités sont sauvegardées dans la plate-forme Google Cloud (GCP).

Évolutivité et fiabilité

L'architecture des microservices est utilisée pour garantir un impact minimal sur l'intégrité du système en cas de défaillance d'un ou de plusieurs de ses composants. Le service monday.com est entièrement conteneurisé. Kubernetes organise son orchestration en offrant une infrastructure hautement évolutive, adaptée à la demande croissante des clients tout en offrant une expérience de qualité aux utilisateurs finaux.

L'infrastructure en tant que code est largement utilisée via Terraform pour garantir l'audibilité et la capacité de maintenance des ressources de l'infrastructure.

monday.com surveille en permanence les mesures de performances de tous les composants de son infrastructure et a conçu cette dernière à des fins d'évolutivité. En outre, nous effectuons des examens trimestriels à l'échelle avec les ingénieurs et les responsables de l'infrastructure pour nous assurer que notre feuille de route offre un service de qualité en tenant compte d'un nombre croissant de clients et de fonctionnalités de produits.

Accord de niveau de service (SLA)

La disponibilité de notre service peut être contrôlée via notre page des statuts. L'interruption du système à des fins de maintenance est rarement nécessaire. Si une telle interruption est nécessaire, elle sera prévue pendant les fins de semaine, aux heures de faible activité, dans la mesure du possible.

Les informations concernant les interruptions sont disponibles immédiatement sur la page des statuts, où les clients peuvent s'abonner aux notifications concernant la disponibilité et les efforts d'atténuation des temps d'arrêt de notre équipe par e-mail ou SMS.

Les clients du plan Entreprise bénéficient d'un engagement de disponibilité de 99,9 %.

---

3. Caractéristiques et fonctions de sécurité

Authentification

monday.com prend en charge les méthodes d'authentification suivantes :

Informations de connexion

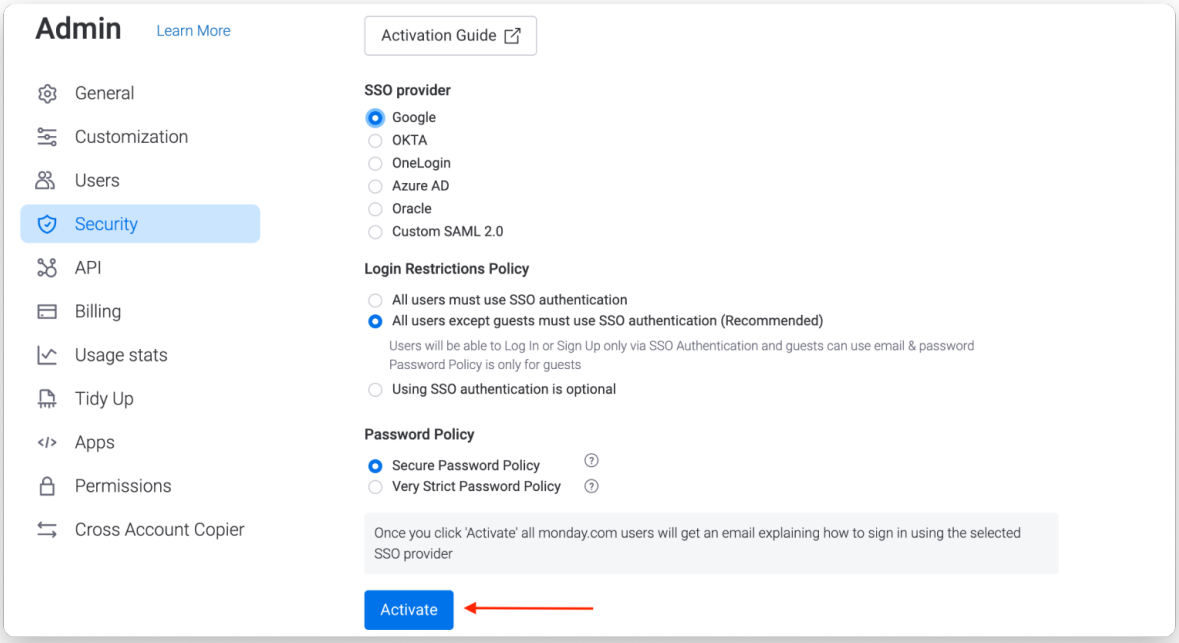
Si vous choisissez d'authentifier les utilisateurs de votre compte à l'aide d'informations de connexion, nous proposons aux administrateurs le choix parmi deux paramètres de complexité des mots de passe pour les comptes qu'ils gèrent :

1. 8 caractères minimum sans caractères répétés ou consécutifs autorisés, ou
2. 8 caractères minimum sans caractères répétés ou consécutifs autorisés et comprenant au moins un chiffre (1, 2, 3, etc.), une lettre minuscule (a, b, c, etc.) et une lettre majuscule (A, B, C, etc.).

Authentification unique (SSO) Google

Google SSO est un système d'authentification sécurisé qui réduit la charge d'avoir à mémoriser plusieurs mots de passe en permettant aux utilisateurs de se connecter au service monday.com à l'aide de leur compte Google.

Cette fonction est disponible uniquement pour les plans Pro et Entreprise.



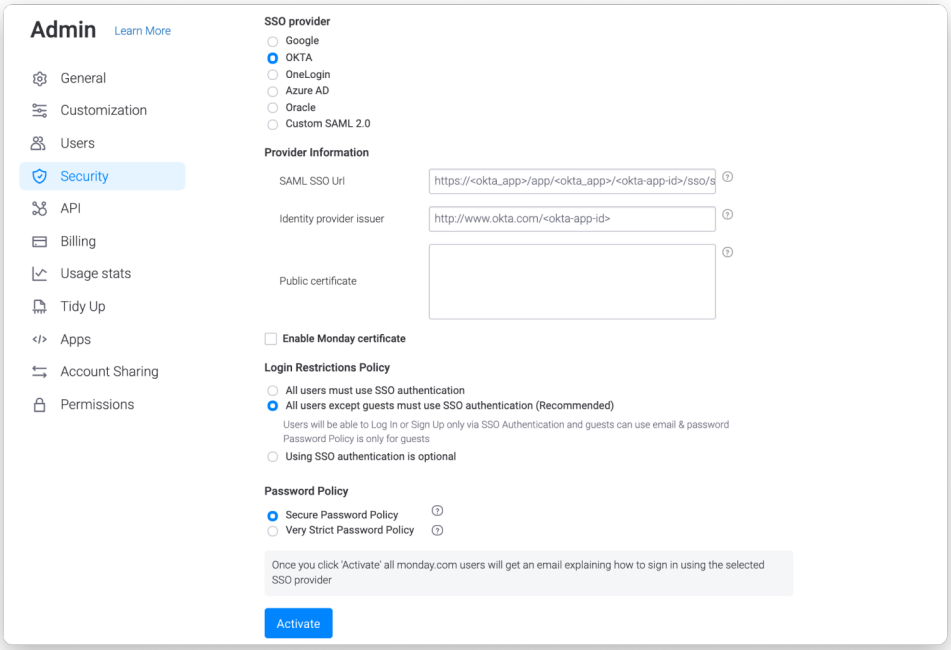
Fournisseur d'identité (IdP)

monday.com prend actuellement en charge trois principaux fournisseurs d'identité :

1. OKTA
2. Azure AD
3. OneLogin

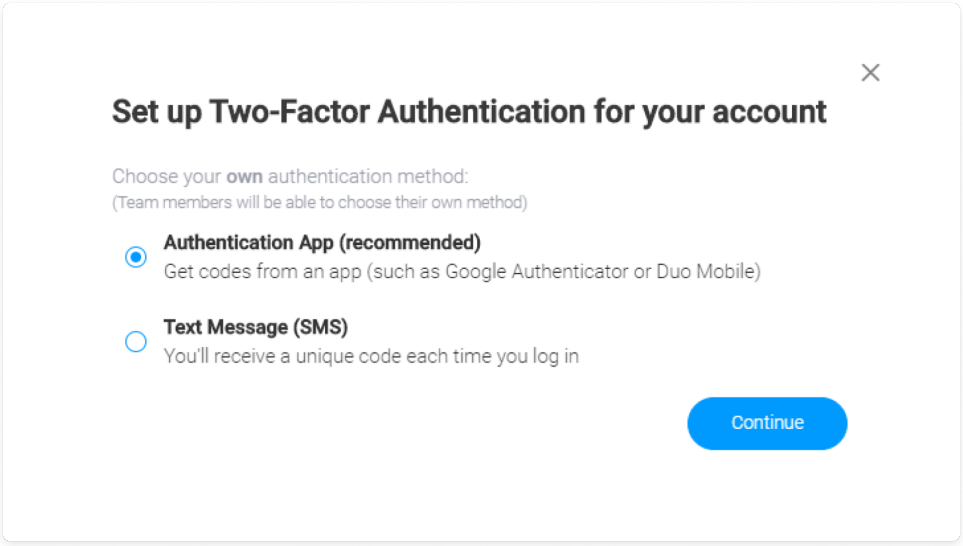
En outre, les clients ont la possibilité d'utiliser leur propre fournisseur à l'aide d'un protocole SAML 2.0 personnalisé.

Cette fonction est disponible uniquement pour les clients titulaires d'un plan Entreprise.



Authentification à deux facteurs (2FA)

En plus des méthodes d'authentification ci-dessus, les administrateurs peuvent configurer une couche supplémentaire de sécurité et activer la 2FA via un texto (SMS) ou une application d'authentification.
Veuillez noter que si vous choisissez d'intégrer votre IdP, la 2FA doit être activée de votre côté.



Autorisation

Provisionnement SCIM

Le SCIM (System for Cross-domain Identity Management) est un protocole de gestion des utilisateurs sur plusieurs applications qui vous permet de provisionner (ajouter), de déprovisionner (désactiver) et de mettre à jour facilement des données d'utilisateur et d'équipe sur plusieurs applications en même temps. monday.com prend en charge trois méthodes de configuration du provisionnement SCIM :

1. Applications SCIM existantes sur monday.com :
    a. OKTA
    b. Azure AD
    c. OneLogin
2. Intégration SCIM personnalisée avec les fournisseurs d'identité de votre choix
3. Provisionnement SCIM à l'aide d'une API

Le tableau suivant présente tous les attributs **utilisateur** pris en charge dans l'intégration SCIM de monday.com :

attribut monday.com	attribut(s) d'API SCIM	Description
Nom (requis)	name (nom), displayName (nom affiché)	Le nom affiché de l'utilisateur
Adresse e-mail (requise)	userName (nom d'utilisateur), email (adresse e-mail)	L'adresse e-mail utilisée par l'utilisateur pour se connecter au service monday.com.
Actif (requis)	active (actif)	Lors de la création d'un utilisateur, ce champ doit être défini sur « true ». La modification de la valeur « active » d'un utilisateur en « false » le désactivera dans le service monday.com.
Poste	title (poste)	Le poste de l'utilisateur dans l'organisation.
Fuseau horaire	timezone (fuseau horaire)	Le fuseau horaire de l'utilisateur (toutes les dates indiquées par la plate-forme seront calées sur ce fuseau horaire).
Langue	locale (langue)	monday.com affichera une version localisée pour différentes langues.
Numéro de téléphone	phoneNumbers (numéros de téléphone)	Les numéros de téléphone de l'utilisateur (seul celui marqué comme « principal » s'affichera).
Adresse du domicile	addresses (adresses)	L'adresse de l'utilisateur (seule celle marquée comme « principale » s'affichera).
Type d'utilisateur	userType (type d'utilisateur)	Le niveau de chaque utilisateur du compte. Les valeurs possibles sont : admin, member, viewer ou guest (la valeur par défaut est « member »).

Le tableau suivant présente tous les attributs d'**équipe** pris en charge dans l'intégration SCIM de monday.com :

attribut monday.com	attribut(s) d'API SCIM	Description

Nom (requis)	name (nom), displayName (nom affiché)	Le nom affiché de l'équipe :
Utilisateurs	members (membres)	Liste des utilisateurs affectés à l'équipe.

Cette fonction est disponible uniquement pour les clients titulaires d'un plan Entreprise.

Autorisations

monday.com vous aide à contrôler qui peut faire quoi sur votre compte. Nous vous proposons plusieurs types d'autorisations à personnaliser afin de restreindre l'affichage ou la modification des données, notamment :

1. **Autorisations concernant les tableaux**
    a. Types : tableaux « main » (principaux), « shareable » (partageables) et « private » (privés)
    b. Restrictions : « edit everything » (tout modifier), « edit content » (modifier le contenu), « edit by assignee » (modifier par attributaire) et « view only » (afficher uniquement)
2. **Autorisations concernant les colonnes** : « restrict column edit » (restreindre l'édition des colonnes) et « restrict column view » (restreindre l'affichage des colonnes)
3. **Autorisations du tableau de bord**
    a. Types : tableaux de bord « main » (principaux) et « private » (privés)
    b. Restrictions : seuls les titulaires d'un tableau de bord peuvent le modifier, ainsi que les applications et widgets qu'il contient
4. **Autorisations concernant les espaces de travail**
    a. Types: espaces de travail « open » (ouverts) et « closed » (fermés)
    b. Restrictions : « no one » (personne), « only admin » (admin uniquement), « workspace owners » (titulaires d'un espace de travail) et « anyone » (quiconque)
5. **Autorisations liées aux comptes :** les administrateurs peuvent définir des restrictions (« no one » (personne), « only admin » (admin uniquement) et « anyone » (quiconque) en ce qui concerne les fonctions suivantes :
    a. Charger des fichiers
    b. Diffuser des tableaux
    c. Créer des tableaux principaux
    d. Créer des tableaux privés
    e. Créer des tableaux partageables
    f. Créer des intégrations
    g. Créer des automatisations
    h. Créer des espaces de travail
    i. @mentionnez ou abonnez tous les utilisateurs du compte à une mise à jour ou à un tableau
    j. Exportez les tableaux, le journal des activités, les résultats de la recherche et les mises à jour vers Excel

Veuillez noter que certaines des fonctions ci-dessus peuvent ne pas être disponibles pour tous les plans.

Rôles au sein de monday.com

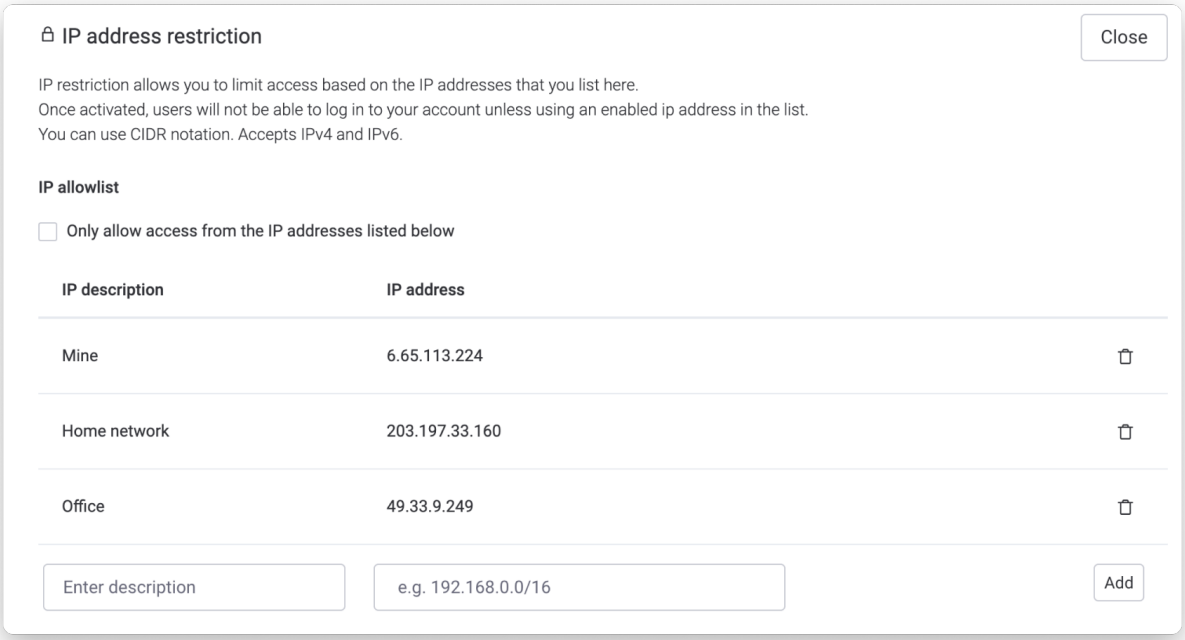
Les rôles au sein de monday.com comprennent :

Rôle	Description	Peut	Ne peut pas
Administrateur	Un membre de l'équipe (ou plus si vous le souhaitez) qui gère son équipe	Superviser l'ensemble du compte Tout gérer, des utilisateurs et des tableaux à la sécurité et à la facturation (comme décrit dans la section « Panneau Admin » ci-dessous)	
Membre	Dispose d'un accès en édition (Le nombre de membres que vous pouvez inviter dépend de votre plan)	• Créer et modifier des tableaux, des éléments et des dossiers • Inviter d'autres membres à accéder à un tableau et à des éléments • Consulter tous les tableaux principaux • Être invité à accéder à des tableaux partageables ou privés • Modifier son profil • Communiquer et ajouter des pièces jointes	
Spectateur	Peut uniquement consulter les tableaux, sans aucun droit d'édition (Vous pouvez inviter un nombre illimité de spectateurs, quel que soit le plan que vous avez acheté)	• Consulter tous les tableaux dans l'espace de travail principal du compte • Ouvrir un élément et lire les mises à jour • Rechercher ou filtrer dans un tableau • Être invité à accéder à des tableaux partageables ou privés • Modifier son profil • Inviter de nouveaux spectateurs • Ouvrir les vues des tableaux • Être affecté à un élément • Être ajouté à une équipe • Exporter les tableaux vers Excel	• Créer ou supprimer un tableau • Apporter des modifications au contenu, à la structure ou aux paramètres d'un tableau • Ajouter des mises à jour à un élément ou publier un « like » sur une mise à jour publiée par quelqu'un d'autre • S'abonner lui-même ou abonner d'autres personnes à un élément/tableau • Être désigné comme titulaire d'un tableau • Inviter un invité à un tableau partageable • Créer une équipe
Invité	Extérieur à votre organisation, comme un fournisseur, un client, un travailleur indépendant ou un consultant externe	Être invité à accéder à des tableaux partageables Fonction en tant que membres	Consulter des informations dans les tableaux principaux ou privés

Restrictions d'adresses IP

Les administrateurs ont la possibilité de prédéfinir un ensemble d'adresses IP autorisées à partir desquelles il sera possible d'accéder à votre compte. Cela vous permet de restreindre l'accès au

compte à certains utilisateurs dans des contextes spécifiques, comme ceux qui y accèdent depuis un emplacement spécifique (par exemple, depuis le bureau) ou qui utilisent un certain VPN. Tout utilisateur qui tente de se connecter avec une adresse IP qui ne figure pas dans la liste de celles autorisées recevra un message d'erreur et ne pourra pas continuer.
Cette fonction est disponible uniquement pour les clients titulaires d'un plan Entreprise.

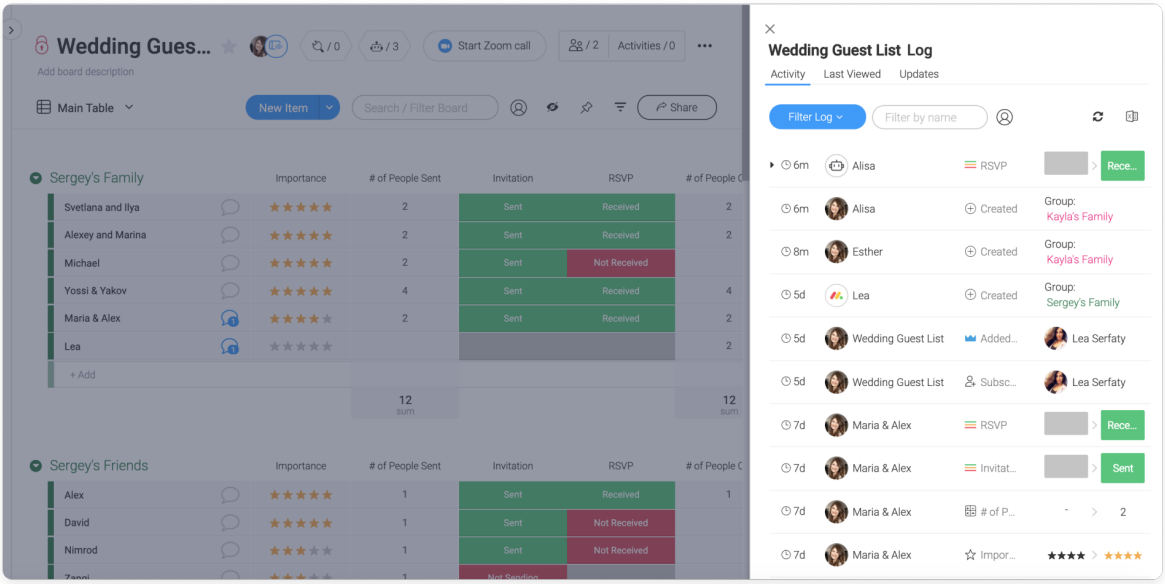


Journaux

Journal des activités

Il existe deux types de journaux des activités :

1. **Le journal des activités d'un tableau** affiche toutes les activités passées dans un tableau dans une seule liste, y compris les dates de modification, les statuts, les mouvements entre les groupes, les automatisations et les autorisations. Les informations affichées dans le journal des activités d'un tableau varient selon votre niveau : le plan de Base permet d'obtenir des informations sur l'activité de la semaine précédente uniquement ; le plan Standard porte cette limite à six mois ; tandis que les plans Pro et Entreprise sont associés à une limite d'un an.



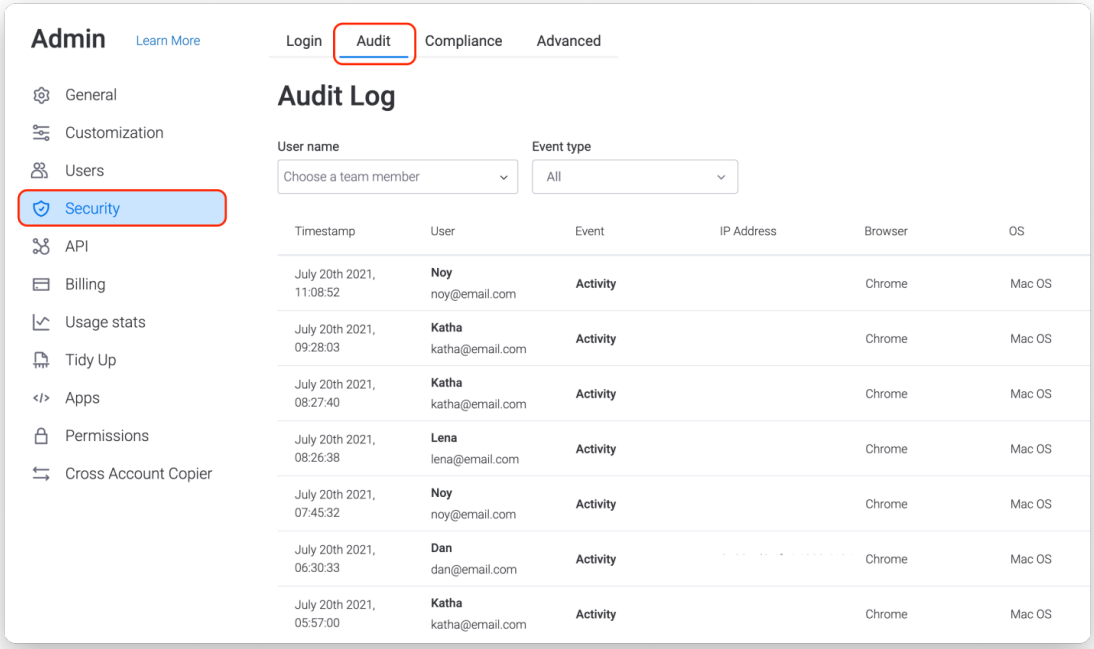
2. **Le journal des activités d'un élément** assure le suivi de toutes les mises à jour effectuées sur un élément individuel. Dans le journal des activités d'un élément, vous pouvez voir un historique complet de ses mises à jour et la date exacte de ces dernières. Toutes les mises à jour sont organisées de la plus récente à la plus ancienne. Vous pouvez définir un rappel d'alerte pour toute mise à jour.

Vous pouvez facilement exporter votre journal des activités d'un élément ou votre journal des activités d'un tableau vers Excel en cliquant sur un bouton.

Journal d'audit

Le journal d'audit fournit aux administrateurs de comptes un rapport détaillé de toutes les activités liées à la sécurité des comptes. Dans cette section, vous pouvez voir quand les utilisateurs se sont connectés et se sont déconnectés pour la dernière fois du compte, à partir de quel périphérique et de quelle adresse IP pour la session en question. De cette façon, vous pouvez surveiller les activités suspectes et activer le mode Panique si nécessaire.

Le journal affiche également les événements démontrant de potentielles vulnérabilités, tels que les échecs de connexion, les pièces jointes téléchargées et les données de tableaux exportées. Cette fonction est uniquement disponible pour les clients du plan Entreprise.



Interopérabilité et portabilité

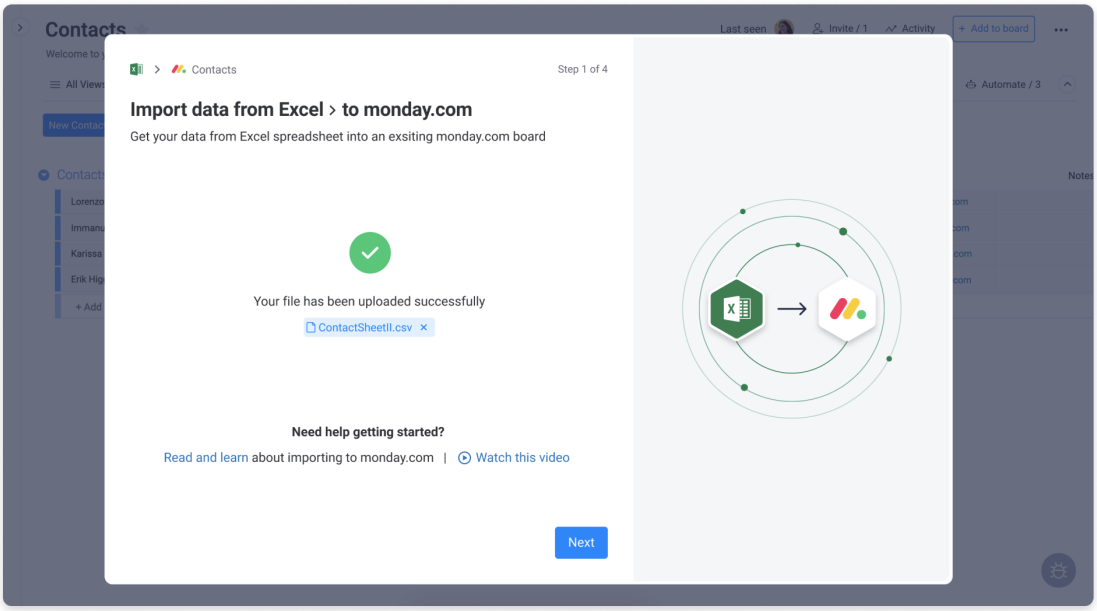
Intégrations

monday.com prend en charge des intégrations avec diverses autres solutions logicielles pour créer des flux de travail personnalisés. Vous pouvez connecter monday.com aux outils que vous utilisez déjà pour gérer tout le travail de votre équipe en un seul endroit.
Les intégrations sont facultatives et peuvent être désactivées via le panneau Admin.

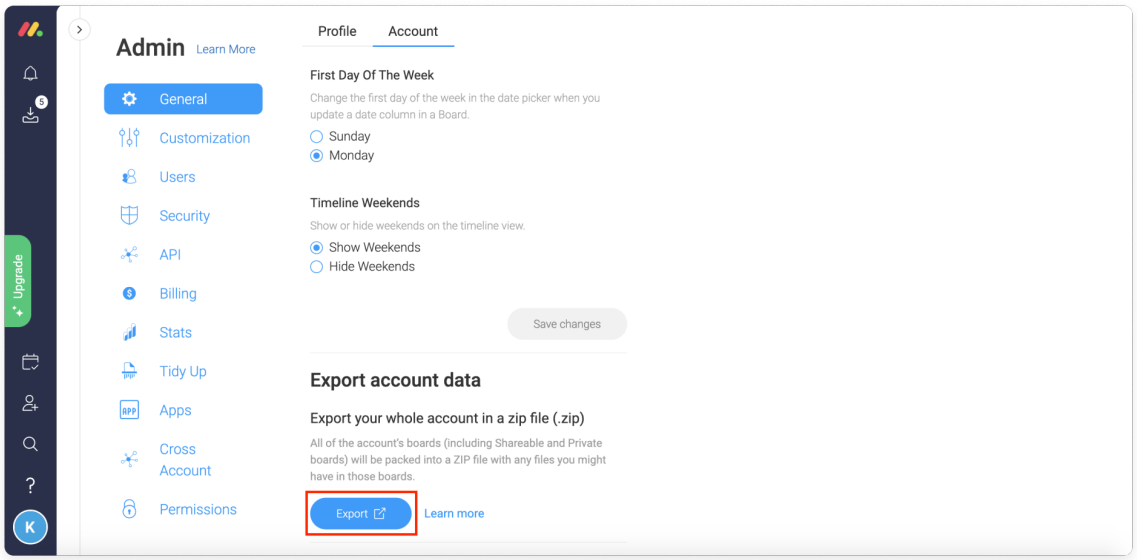
Importations et exportations Excel

monday.com offre aux clients deux fonctionnalités de gestion des données :

1. transformer les données d'une feuille de calcul Excel en un tableau monday.com (nouveau ou existant).



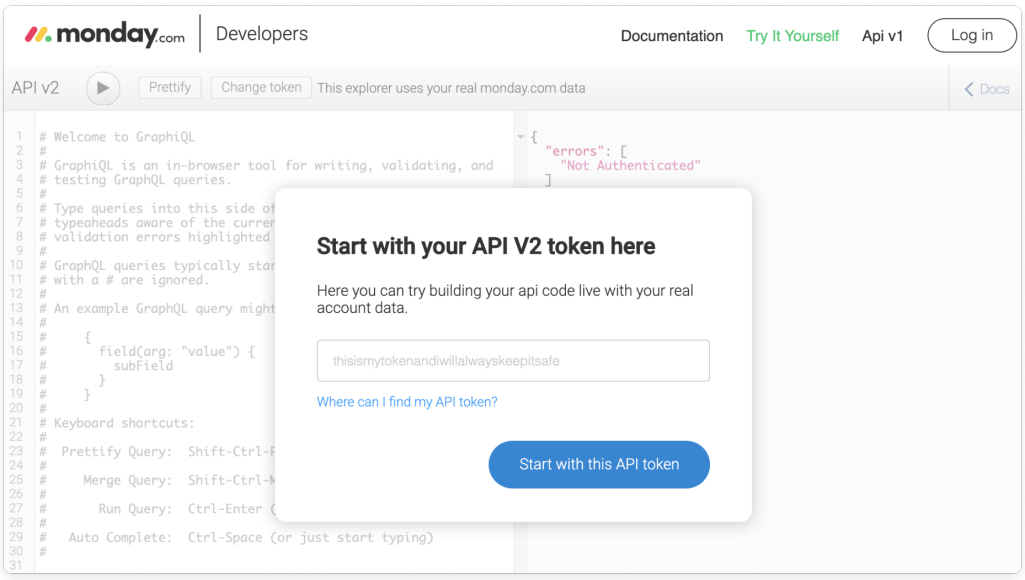
2. exporter les données depuis monday.com :
    a. exporter des tableaux vers Excel.
    b. exporter l'intégralité des données du compte via le panneau Admin. Il sera exporté sous forme d'archive .zip contenant des feuilles Excel et les fichiers chargés sur le compte.



API

monday.com met à disposition une API GraphQL. Cela fait partie du cadre des applications monday et permet aux développeurs d'accéder aux données et de les mettre à jour par programmation à l'intérieur de leurs comptes monday.com.
Exemples d'utilisation de l'API :

- accès aux données d'un tableau pour afficher un rapport personnalisé dans un tableau de bord monday.com
- création d'un nouvel élément dans un tableau lorsqu'un enregistrement est créé sur un autre système
- importation de données d'une autre source par programmation



Le panneau Admin

Dans le panneau Admin, les administrateurs de votre compte peuvent tout gérer, y compris les paramètres de sécurité, les utilisateurs du compte, la personnalisation du compte, la facturation, etc.

Domaine autorisé

Les administrateurs peuvent choisir entre deux paramètres :

1. seuls les administrateurs peuvent inviter des membres et des spectateurs dans le compte à partir de n'importe quel domaine de messagerie.
2. les administrateurs déterminent un domaine de messagerie à partir duquel les utilisateurs peuvent s'inscrire au compte.

Blocage de domaine de messagerie

Les administrateurs peuvent empêcher les utilisateurs de créer de nouveaux comptes monday.com à partir de certains domaines de messagerie. Cette fonctionnalité est utile pour éviter les comptes monday.com redondants dans la même organisation, en particulier celles qui possèdent plusieurs domaines d'entreprise, ce qui peut avoir des implications pour maintenir la conformité aux règles de gouvernance des données d'entreprise.

Pour bloquer la création de nouveaux comptes, les domaines de messagerie peuvent être soumis au service monday.com pour examen et vérification de la titularité. Ils seront transmis à ou aux administrateurs de comptes pour être intégrés au compte de l'organisation principale.
Cette fonction est disponible uniquement pour les clients titulaires d'un plan Entreprise.

Mode panique

En activant le mode Panique, vous bloquerez temporairement votre compte. Personne ne pourra y accéder tant que l'administrateur du compte n'aura pas envoyé de demande à notre équipe Customer Success. Cette fonctionnalité est essentielle si les informations d'identification de l'un des membres de votre équipe ont été compromises.
Cette fonction est disponible uniquement pour les clients titulaires d'un plan Entreprise.

Gestion de session

Dans la section sécurité du panneau Admin, les administrateurs peuvent cliquer sur l'onglet sessions pour afficher les données de session de tous les utilisateurs et contrôler et réinitialiser l'une d'elles.
Cette fonction est disponible uniquement pour les clients titulaires d'un plan Entreprise.

Génération de tokens d'API

Seuls les administrateurs peuvent accorder des autorisations pour générer des tokens d'API GraphQL personnels dans leur compte (soit à tout le monde, soit uniquement aux administrateurs, soit à personne). Cela empêche les utilisateurs de générer des tokens d'API et de les partager par erreur avec des outils tiers, ou même de les rendre publics en les envoyant vers le référentiel public et en exposant les données sensibles du compte. Un avertissement s'affichera pour les utilisateurs non autorisés à générer des tokens.
Cette fonction est disponible uniquement pour les clients titulaires d'un plan Entreprise.

Répertoire de contenu

Dans le répertoire de contenu, vous trouverez une vue d'ensemble de tous les espaces de travail, tableaux, tableaux de bord et documents de travail situés dans le compte. En outre, pour toutes ces fonctionnalités, vous pourrez voir leurs titulaires, abonnés, dates de création, dates de dernière mise à jour et si elles sont accessibles publiquement pour les autres membres du compte ou non.

* * Veuillez noter que ce livre blanc ne contient pas la liste complète des fonctionnalités gérées via le panneau Admin. Des informations supplémentaires se trouvent dans nos articles d'assistance.
Des fonctions supplémentaires gérées par les administrateurs de compte peuvent être abordées dans divers chapitres de ce document, tels que la connexion, l'authentification à deux facteurs, le provisionnement SCIM, les autorisations, la restriction d'adresses IP, les applications monday, le journal d'audit, les tokens d'API et la configuration de la conformité à l'HIPAA.

---

4. Sécurité des applications

Cycle de développement de logiciel sécurisé (S-SDLC)

- monday.com utilise la méthodologie OWASP Top 10 pour renforcer la sécurité de notre cycle de vie du développement logiciel sécurisé (S-SDLC).
- Tout le code est analysé de façon statique (SAST) et examiné par les pairs dans le cadre du processus CI/CD afin de garantir sa qualité avant son déploiement en production.
- Les tests de sécurité dynamique des applications (DAST) sont effectués au moins une fois par semaine.
- Nous avons mis l'accent sur l'écriture de tests dédiés pour les nouvelles fonctionnalités qui sont lancées, tandis que les fonctionnalités plus anciennes ont été testées dans des conditions réelles pendant plusieurs années.
- Nous évaluons et surveillons en permanence les vulnérabilités de notre application pendant et après le déploiement.
- Toutes les bibliothèques tierces côté serveur sont automatiquement vérifiées pour détecter les vulnérabilités divulguées publiquement à l'aide d'un outil d'analyse de la composition logicielle (SCA).

Pare-feu d'application Web (WAF)

Un pare-feu d'application Web (WAF) est en place pour filtrer, surveiller et bloquer le trafic au niveau des applications afin d'offrir une protection contre les attaques connues.

Gestion des vulnérabilités

Les vulnérabilités sont centralisées dans un registre de développement et sont classées en fonction de notre évaluation de leur impact sur la confidentialité, l'intégrité et la disponibilité du service et des données clients. L'indice de gravité d'une vulnérabilité est déterminé par le système CVSS (Common Vulnerability Scoring System). Notre service R et D applique ensuite des mesures correctives dans des délais prédéfinis basés sur la gravité, conformément à notre politique interne de gestion des correctifs.

Champions de la sécurité

Notre communauté de champions de la sécurité interne comprend des développeurs de toutes les équipes de R et D. Les champions de la sécurité reçoivent une formation avancée en la matière et sont qualifiés pour fournir des conseils pertinents et effectuer des révisions du code de sécurité chaque fois que nécessaire.

Tests de pénétration

Des tests de pénétration des applications sont effectués chaque année par un tiers indépendant différent, au moyen de méthodes manuelles et automatiques.
En outre, notre équipe interne chargée de la sécurité des applications effectue régulièrement des audits de sécurité et des tests de pénétration pour diverses fonctionnalités qui nécessitent une connaissance approfondie de nos mécanismes de protection internes et de notre architecture.
Dans le cadre de nos tests de pénétration externes et internes, des outils d'analyse réseau sont utilisés pour viser nos serveurs de production.

Programme de recherche de bogues

monday.com utilise un programme de recherche de bogues privé et géré en interne sur HackerOne, permettant aux chercheurs en failles informatiques du monde entier de rechercher et de divulguer de manière éthique et responsable les vulnérabilités à notre équipe chargée de la sécurité. Certaines fonctionnalités feront l'objet de promotions spéciales sur HackerOne afin de concentrer sur celles-ci les recherches et les efforts de cette communauté.

Dans le cadre de ce programme, nous avons recours à un tableau de classement des pirates informatiques.

---

5. Sécurité informatique

Sécurité des points de terminaison

Tous les postes de travail des employés sont protégés par une solution EDR (Endpoint Detection and Response) gérée de manière centralisée pour la détection et la mise en quarantaine des programmes malveillants. Notre solution EDR est continuellement surveillée par une équipe du SOC (Security Operations Center) travaillant 24 h/24 et 7 j/7.
Tous les postes de travail sont cryptés à l'aide de FileVault/BitLocker, protégés par mot de passe et configurés pour s'éteindre après 10 minutes d'inactivité.
En outre, nous pouvons appliquer des correctifs et effacer à distance une machine via un gestionnaire de dispositifs.

Règle applicable aux mots de passe

Notre règle interne applicable aux mots de passe interne stipule qu'ils doivent comporter au moins 12 caractères et contenir les éléments suivants :

1. lettre majuscule
2. lettre minuscule
3. chiffre
4. symbole

Une solution de gestion des mots de passe d'entreprise est utilisée, les mots de passe par défaut sont modifiés régulièrement, leur réutilisation et les mots de passe couramment employés sont techniquement interdits et ils expirent au bout de 120 jours.

Gestion de l'accès et de l'identité

L'accès aux systèmes est accordé par notre équipe informatique en fonction du rôle via notre solution de fournisseur d'identités d'entreprise (IdP), conformément aux principes du besoin de savoir et des privilèges les plus restreints.
L'accès utilisateur est modifié dans les 24 heures suivant un changement ou une cessation d'emploi. De plus, des examens trimestriels de l'accès des utilisateurs sont effectués pour nous assurer de la pertinence des privilèges d'accès. Tout accès qui n'est plus nécessaire est supprimé et documenté.

Protection du courrier électronique

monday.com utilise Google Workspace comme fournisseur de services de messagerie. Ces services sont protégés par un relais de messagerie tiers. Les protocoles DMARC et SPF sont appliqués. Les employés sont informés en permanence des meilleures pratiques d'évitement du phishing et des tests sont effectués régulièrement.

Points d'accès sans fil

monday.com utilise des technologies standard pour garantir la sécurité des communications sans fil dans notre siège social. Nous utilisons le protocole WPA2 Entreprise, entre autres outils, pour garantir le déprovisionnement et la non-répudiation en temps opportun sur le réseau et avons mis en place une surveillance des points d'accès indésirables.

6. Sécurité opérationnelle

Accès aux données des clients
monday.com traite toutes les données que les clients soumettent au service monday.com. Nous les traitons uniquement pour le compte du client, sous la forme d'une « black box ». Cela signifie que les données client ne sont généralement pas accessibles pour l'exécution du service monday.com et que nous traitons toutes les données client soumises avec le plus haut niveau de sensibilité et de confidentialité.
L'accès aux données clients par monday.com est limité, au cas par cas, conformément à nos conditions de service ou à l'accord que nous avons conclu avec le client.

Ressources humaines
Vérification des antécédents
Notre siège social est situé en Israël, où les vérifications des antécédents ne sont pas habituelles et sont limitées par la loi. Les contrôles que nous effectuons incluent l'examen des antécédents professionnels et des appels avec d'anciens supérieurs hiérarchiques visant à obtenir des références.

Contrats de travail
Tous les contrats de travail monday.com contiennent des dispositions en matière de confidentialité permettant un licenciement immédiat en cas de violation de certains engagements et obligations. En outre, monday.com applique une politique de sécurité des RH qui définit les activités et responsabilités requises en la matière pendant la période d'emploi, du recrutement au départ.

Utilisation acceptable
monday.com applique une politique d'utilisation acceptable qui est révisée chaque année par notre équipe chargée de la sécurité et l'ensemble du groupe en charge de la sécurité. Nos employés sont tenus de signer la politique lors de leur intégration ou d'un changement important dans ses dispositions.

Formation et sensibilisation
Dans le cadre de leur processus d'intégration initial et au moins une fois par an ensuite, les employés de monday.com doivent participer à une formation sur les obligations en matière de sécurité et de confidentialité des informations. La formation comprend des didacticiels ainsi que des tâches écrites, sous la supervision de l'équipe chargée de la sécurité.
Des semaines dédiées à la sécurité et à la confidentialité sont organisées chaque trimestre afin d'accroître la sensibilisation des employés.
En outre, des sessions de formation dédiées sont organisées selon les besoins (par exemple, les développeurs suivent une formation sur le codage sécurisé).

Cessation d'emploi
L'accès utilisateur est modifié dans les 24 heures suivant un changement ou une cessation d'emploi, le matériel de l'entreprise devant être rendu. De plus, des examens trimestriels de l'accès des utilisateurs sont effectués pour nous assurer de la pertinence des privilèges d'accès.

Évaluations « Red team »
Deux fois par an, nous avons recours à des évaluations Red team afin de tester nos moyens défensifs. Il s'agit notamment de tests de pénétration internes, d'attaques de l'infrastructure et

d'une simulation de violation. Les évaluations Red team sont effectuées par des sociétés de conseil tierces en sécurité offensive et défensive qui utilisent des techniques d'attaque sophistiquées offrant une visibilité unique sur nos risques et vulnérabilités potentiels.

Gouvernance et gestion des risques
monday.com applique un processus continu de gestion des risques visant à identifier de manière proactive les vulnérabilités dans les systèmes de monday.com et à évaluer les menaces nouvelles et émergentes pour les opérations de l'entreprise. monday.com fait l'objet d'une évaluation des risques dans le cadre de la certification ISO 27001 qui est effectuée annuellement.

Réaction aux incidents et leur gestion
Le plan d'intervention en cas d'incident (IRP) de monday.com établit des lignes directrices pour détecter les incidents en matière de sécurité et de confidentialité, les signaler au personnel concerné, et concernant les communications (internes et externes), les mesures d'atténuation et les analyses post-mortem.
L'équipe d'intervention en cas d'incident (IRT) de monday.com est composée de représentants des services de la sécurité, de la R et D, du service juridique, de représentants d'autres équipes au cas par cas et, si nécessaire, d'une société tierce offrant des services d'intervention en cas d'incident.

Notification
Conformément aux dispositions de l'article 7 de notre Addenda au traitement des données (« Gestion et notification des incidents liés aux données »), monday.com, après avoir été informée d'un incident lié aux données, avertira les clients concernés sans retard indu.
Les clients concernés seront informés de la nature de la violation, des effets néfastes dont monday.com a connaissance, des actions que monday.com a entreprises et des plans de résolution ou d'atténuation de l'incident au moment de la notification.

Reprise après sinistre et continuité des activités
monday.com dispose d'un plan de continuité des activités conforme à la norme ISO 27001 pour faire face aux catastrophes affectant nos bureaux physiques (où aucune partie de notre infrastructure de production n'est conservée).
Nous disposons en outre d'un plan de reprise après sinistre (DRP) pour faire face aux catastrophes affectant notre environnement de production, ce qui inclut la restauration des fonctionnalités de base du service depuis notre site de reprise après sinistre dédié. Des tests sont effectués au moins deux fois par an. Les tests de reprise après sinistre de monday.com peuvent être systématiques, cibler les composants ou s'appuyer sur un sinistre fictif.

Conservation et mise au rebut des données
Conservation des données
monday.com conservera vos informations qu'elle contrôle pendant la période nécessaire pour remplir les objectifs décrits dans notre politique de confidentialité. Les données que monday.com traite pour le compte de nos clients seront conservées conformément à nos conditions de service, à notre addenda au traitement des données et à d'autres accords commerciaux avec les clients.

Effacement des données
Les clients de monday.com conservent le contrôle total des données qu'ils soumettent et peuvent les modifier, les exporter ou les supprimer à tout moment en utilisant les moyens disponibles via l'interface utilisateur du service.

Lors de la résiliation ou de l'expiration de leur abonnement, les clients peuvent demander la suppression de leurs données dans le cadre de la procédure de clôture de compte. Les données client seront ensuite supprimées dans les 90 jours suivant la demande, ce qui inclut une période de 30 jours pour permettre leur restauration et 60 jours supplémentaires pour poursuivre le processus de suppression.
Les clients peuvent également choisir de conserver les données de leur compte sur la plate-forme, auquel cas nous pourrons continuer à les conserver, mais nous serons également en droit de les supprimer à tout moment, à notre discrétion.

Destruction des données

Notre service est hébergé sur AWS, avec certaines données sauvegardées sur GCP. Les deux fournisseurs de services de cloud computing mettent en œuvre des stratégies exclusives de distribution et de suppression des données pour permettre un stockage sécurisé des données sensibles dans un environnement multi-locataire. La mise hors service des supports de stockage est effectuée par les fournisseurs mentionnés ci-dessus en utilisant les techniques détaillées dans les directives NIST 800-88.

Contrôle et consignation dans les journaux

monday.com collecte et surveille les journaux réseau à l'aide d'un système de détection des intrusions réseau (NIDS), les journaux de trafic des emplacements périphériques, la journalisation au niveau des applications pour le suivi et l'audit des événements, ainsi que la journalisation au niveau du système pour l'audit des accès et des opérations à privilèges élevés. Les journaux sont diffusés dans notre solution de gestion des événements et des informations de sécurité (SIEM), où ils sont surveillés en permanence (24/7/365) par une équipe du SOC (Security Operations Center) gérée.

Gestion de la chaîne d'approvisionnement

Sous-traitants

monday.com s'assure que ses sous-traitants (à la fois dans la région des données mondiale et celle de l'UE) respectent les normes de l'industrie en matière de sécurité et de confidentialité des données, et considère ses deux aspects comme essentiels dans son processus de sélection des sous-traitants. Entre autres mesures, nous avons veillé à ce que les addenda relatifs au traitement des données et d'autres documents et garanties pertinents soient en place avec tous nos sous-traitants. Nous effectuons également des évaluations de confidentialité, juridiques et de sécurité des informations, ainsi que des audits basés sur des questionnaires, le tout conformément aux normes et aux exigences réglementaires de l'industrie. Des évaluations de nos sous-traitants sont effectuées au moins sur une base annuelle.

Gestion des fournisseurs

monday.com a mis en place un programme central de gestion des ressources du référentiel pour les services et les logiciels que nous utilisons. Les ressources du référentiel sont conservées de façon continue par nos équipes Sécurité, Juridique, Confidentialité et Approvisionnement. Le processus d'approbation est communiqué à tous les employés.
Dès le début de l'utilisation et du renouvellement des services ou des logiciels, les différentes équipes classent les fournisseurs avec lesquels nous travaillons en fonction du niveau de sensibilité le plus élevé des données auxquelles ils ont accès, afin de déterminer leur niveau de risque pertinent et de les évaluer conformément aux normes de l'industrie et aux exigences réglementaires.

Sécurité physique

Bureaux monday.com

Les ressources informatiques physiques des bureaux monday.com sont limitées aux ordinateurs portables et aux périphériques réseau. Les périphériques réseau des bureaux sont protégés dans une salle de serveurs surveillée par vidéosurveillance 24/7/365 et à environnement contrôlé dont l'accès est verrouillé par un mot de passe. L'accès physique aux bureaux est contrôlé par identification biométrique. Les visiteurs sont enregistrés à l'entrée dans nos bureaux et doivent être accompagnés à chaque moment par un employé de monday.com pendant leur présence. Tous les employés doivent signaler toute activité suspecte, tout accès non autorisé aux locaux et tout vol ou perte d'objets.

Sécurité du centre de données

monday.com s'appuie sur les mesures de sécurité physique et environnementale de classe mondiale d'AWS et de GCP, ce qui se traduit par une infrastructure hautement résiliente. Pour obtenir plus d'informations concernant ces pratiques en matière de sécurité, veuillez visiter les liens suivants :
https://aws.amazon.com/security/, https://cloud.google.com/security/

7. Conformité, confidentialité et certifications

Vérification au moyen d'audits et conformité
monday.com a développé ses programmes de sécurité et de confidentialité conformément à plusieurs programmes de conformité aux normes de l'industrie, ainsi qu'aux principales réglementations en matière de confidentialité et de protection des données dans les territoires où notre service est offert :

ISO 27001, 27017, 27018, 27032 et 27701
monday.com respecte les normes internationales de l'ISO (International Organization for Standardization) et gère la sécurité des informations, le service cloud et la confidentialité conformément à celles-ci. Nous faisons l'objet d'un audit annuel par un tiers indépendant et nous détenons 5 certificats ISO :

- **ISO/IEC 27001:2013** est la norme de sécurité mondiale la plus rigoureuse pour les systèmes de gestion de la sécurité des informations (ISMS).
- **ISO/IEC 27018:2014** établit des objectifs et des moyens de contrôle, ainsi que des lignes directrices généralement acceptées pour la mise en œuvre de mesures de protection des informations personnellement identifiables (IPI) conformément aux principes de confidentialité de la norme ISO/IEC 29100 pour l'environnement de cloud computing public.
- **ISO/IEC 27017:2015** fournit des conseils concernant les contrôles et la mise en œuvre pour les fournisseurs et les clients de services cloud. Elle fournit des directives pour les contrôles de sécurité des informations applicables à la fourniture et à l'utilisation des services cloud en fournissant des conseils supplémentaires pour la mise en œuvre des contrôles pertinents.
- **ISO/IEC 27032:2012** fournit des conseils pour améliorer l'état de la cybersécurité, en tirant parti de ses aspects uniques et de ses liens de dépendance avec d'autres domaines de sécurité, en particulier : la sécurité des informations, la sécurité du réseau, la sécurité Internet et la protection de l'infrastructure d'information critique (CIIP).
- **ISO/IEC 27701:2019** précise les exigences et fournit des conseils pour l'établissement, la mise en œuvre, la maintenance et l'amélioration continue d'un système de gestion des renseignements personnels (PIMS).

Toutes nos certifications sont disponibles ici.

SOC 1, SOC 2 et SOC 3
monday.com a mis en places des contrôles du service et de l'organisation :

- **audit SOC 1 Type II**, qui examine les contrôles qui peuvent être pertinents pour le reporting financier des clients.
- **audit SOC 2 Type II**, qui démontre notre engagement à respecter les normes de sécurité, de disponibilité et de confidentialité les plus rigoureuses de l'industrie. Il vérifie que les contrôles de sécurité de monday.com sont conformes aux principes et critères des services de confiance AICPA (The American Institute of Certified Public Accountants) et aux exigences de sécurité l'HIPAA.

- **rapport SOC 3**, qui est une version plus courte de notre rapport SOC 2 Type II et est accessible au public.

Chaque année, des audits sont effectués par un tiers indépendant et un rapport couvrant les mois d'avril à mars est publié.
Les rapports SOC de monday.com sont disponibles via les liens suivants : SOC 1, SOC 2 et SOC 3.

Cloud Security Alliance (CSA)

La Cloud Security Alliance (CSA) est une organisation à but non lucratif dont la mission est de « promouvoir l'utilisation des meilleures pratiques pour garantir la sécurité dans le cloud computing et de fournir une formation sur son utilisation pour aider à sécuriser toutes les autres formes d'informatique ».

monday.com participe à l'auto-évaluation volontaire STAR (CSA Security, Trust, Assurance, and Risk Registry) pour documenter notre conformité aux pratiques exemplaires publiées par la CSA. Le questionnaire de l'Initiative d'évaluation consensuelle de la CSA (CAIQ) que nous remplissons est gratuit et accessible au public sur le site Web de la CSA.

Health Insurance Portability and Accountability Act (HIPAA)

L'Health Insurance Portability and Accountability Act (HIPAA) est conçue pour protéger les données de santé. Les organisations telles que les hôpitaux, les cabinets de médecins, les plans de santé ou les entreprises traitant des informations de santé protégées doivent se conformer à l'HIPAA. Cela peut également s'étendre aux entreprises qui collaborent avec des sociétés et qui entrent en contact avec des informations de santé protégées en leur nom.

monday.com propose à ses clients une configuration de compte conforme aux dispositions de l'HIPAA pour qu'ils puissent soumettre leurs informations médicales sensibles. Nos clients relevant de l'HIPAA doivent conclure notre accord de partenariat commercial pour garantir la protection et le traitement approprié des informations de santé protégées en leur nom avant de soumettre des données régies par l'HIPAA.

monday.com et le RGPD

Notre programme mondial de protection de la vie privée est basé sur les réglementations de protection des données les plus complètes et les plus avancées au monde, le Règlement général sur la protection des données (RGPD) de l'UE et du Royaume-Uni servant d'« étoile polaire ».

Entre autres choses, le groupe chargé du respect de la vie privée au sein de monday.com surveille en permanence les développements de produits et de processus dans notre organisation, ainsi que les diverses activités impliquant l'utilisation des données personnelles pour s'assurer que les principes du RGPD sont respectés, comme les principes de confidentialité dès la conception, de minimisation des données et de limitation de leur stockage,

de légalité et d'équité dans leur traitement, et la transparence de nos activités et de nos objectifs.

Politique de confidentialité

La politique de confidentialité de monday.com, qui décrit nos pratiques en matière de protection de la vie privée et de traitement des données à l'égard des données personnelles que nous traitons à nos propres fins en tant que responsables de leur traitement, se trouve dans le lien suivant.

Addenda au traitement des données (DPA)

Les conditions de service et les contrats avec les clients monday.com contiennent tous un addenda relatif au traitement des données afin d'assurer la protection et le traitement approprié des données personnelles au nom de nos clients. Vous pouvez consulter et signer en ligne notre addenda au traitement des données (DPA).

Transferts transfrontaliers de données personnelles

monday.com a son siège social en Israël, avec des filiales aux États-Unis, au Royaume-Uni, en Australie et au Brésil, et dispose d'équipes d'assistance en Ukraine et au Guatemala. Nos sous-traitants sont également enregistrés dans différents pays, comme détaillé sur notre page relative aux sous-traitants.

Lorsque nous transférons des données personnelles de l'EEE et du Royaume-Uni vers d'autres pays, nous nous appuyons sur les mécanismes de transfert licites prévus par le RGPD, tels que les « décisions d'adéquation » prises par la Commission européenne (par exemple, les décisions considérant le Royaume-Uni et Israël comme offrant un niveau adéquat de protection des données à caractère personnel originaires de l'UE), et les clauses contractuelles types de l'UE, qui se trouvent ici et ici.

Responsables du traitement et sous-traitants

Le RGPD définit et distingue deux rôles principaux lorsqu'il s'agit de collecter et de traiter des données personnelles : les responsables du traitement et les sous-traitants. Un responsable du traitement détermine les moyens et les fins du traitement des données personnelles, tandis qu'un sous-traitant est une partie qui traite les données pour le compte du responsable.

- monday.com est le responsable du traitement des données personnelles relatives à ses clients, utilisateurs et visiteurs de son site Web. Ceci est expliqué plus en détail dans notre politique de confidentialité.
- monday.com est le responsable du traitement des données personnelles que ses clients et utilisateurs soumettent à la plate-forme (dans les tableaux et les éléments de leur compte monday.com), et traite ces données pour le compte de ses clients. Nous le faisons conformément à l'addenda au traitement des données conclu avec nos clients. Les fournisseurs de services tiers que nous utilisons pour nous aider à traiter ces données sont nos « sous-traitants ».

monday.com et la CCPA

En tant que « prestataire de services », monday.com s'engage à se conformer aux exigences applicables de la California Consumer Privacy Act de 2018 (CCPA) et aux réglementations du procureur général de Californie, à la lumière de réglementations similaires dans le monde entier (telles que le RGPD) et de l'évolution des normes de l'industrie – pour nous assurer que nos clients peuvent continuer à utiliser monday.com sans interruption et que nous pouvons traiter les informations personnelles des consommateurs californiens conformément à la CCPA.

De plus amples informations se trouvent ici.

L'Australian Privacy Act (APA) les Australian Privacy Principles (APP)
L'Australian Privacy Act (APA) et les Australian Privacy Principles (APP) établissent un cadre structuré s'agissant de recueillir, traiter, utiliser et partager des renseignements personnels, donnant aux personnes concernées un plus grand contrôle sur la façon dont leurs informations sont traitées. monday.com s'engage à se conformer aux exigences de l'APA et des APP.
De plus amples informations se trouvent ici.

Audits internes
Nos équipes Sécurité, Confidentialité, Infrastructure, R et D, Informatique, Opérations et Juridique organisent des semaines trimestrielles en matière de sécurité et de confidentialité. Elles incluent la réalisation de diverses activités d'audit, y compris des examens des accès des utilisateurs, des examens de la configuration des pare-feu, des inspections dans le cadre de la politique du rangement des bureaux, des formations et des activités de sensibilisation, et bien plus encore.

Divulgation aux autorités
monday.com ne permet pas aux autorités d'accéder de façon injustifiée aux données des clients que nous détenons. Nous recevons rarement des demandes des autorités (aux États-Unis ou ailleurs) de divulguer des données sur les clients. Les quelques cas dans lesquels nous avons reçu de telles demandes au cours des années précédentes avaient une portée limitée et se rapportaient à des motifs très légitimes (par exemple, une activité illégale présumée liée à un compte particulier). Une fois qu'une demande a été examinée par nos équipes Juridique et Confidentialité afin de nous assurer qu'elle est valide et justifiée, la divulgation se limiterait aux données strictement nécessaires en vertu de la loi. Nous faisons tout notre possible pour informer nos clients avant de procéder à une telle divulgation, à moins que cela nous soit interdit ou que nous ne soyons pas en mesure de le faire en raison d'un risque potentiel.[3] Nous nous engageons également à prendre des mesures commercialement raisonnables pour nous opposer, sous réserve des lois applicables, à toute demande de surveillance en masse relative aux données personnelles protégées par le RGPD européen ou le RGPD britannique, y compris en vertu de l'article 702 de la FISA.

PrivacyTeam et le DPO
monday.com est protégée par PrivacyTeam, le principal cabinet de conseil en matière de confidentialité en Israël, et s'efforce au maximum, de concert avec lui, de garantir la protection des données et de la vie privée des clients. De plus amples informations se trouvent ici.
monday.com a nommé M. Aner Rabinovitz, responsable senior de la protection de la vie privée de PrivacyTeam, en tant que délégué à la protection des données. Il est chargé de suivre et de donner des conseils sur la conformité permanente de monday.com en matière de protection de la vie privée et de servir de point de contact sur les questions de confidentialité pour les personnes concernées et les autorités de surveillance.

---

[3]Des renseignements supplémentaires sont disponibles à l'article 4 (« partage de données ») de notre politique de confidentialité.

8. Épilogue

Ce livre blanc a livré un aperçu général de l'approche de monday.com en matière de sécurité et de protection de la vie privée. Bien sûr, étant donné la complexité de ces sujets, vous pouvez avoir des questions supplémentaires.
Vous trouverez de plus amples informations dans notre Centre de confiance et de sécurité et sur notre portail juridique.
Pour plus de précisions sur la sécurité des informations ou la protection de la vie privée au sein de monday.com, vous pouvez également contacter nos équipes aux adresses security@monday.com ou dpo@monday.com, en plus de l'assistance générale fournie 24/7/365 en écrivant à support@monday.com.
Vous souhaitez signaler un problème ou une vulnérabilité menaçant la sécurité ? Écrivez-nous à security@monday.com ou signalez-le via notre formulaire HackerOne à l'adresse https://monday.com/security/form/.

AVERTISSEMENT : Cette version est une traduction de la version originale en anglais et elle est fournie uniquement à des fins de commodité. La version originale anglaise est la version officielle et juridiquement contraignante et c'est elle qui prévaudra en cas de divergence.