LIVRE BLANC

Sécurité et confidentialité sur Asana

Asana et la protection de vos données

asana

Table des matières

Dernière mise à jour : février 2022[1]

[1] Ce livre blanc décrit l'état actuel de la sécurité sur Asana. Cette dernière est susceptible de connaître des évolutions à la suite du lancement de nouvelles fonctionnalités ou de nouveaux produits.

Introduction

Aujourd'hui, les entreprises du monde entier adoptent de nouveaux outils pour gérer et organiser leur travail, des tâches journalières aux initiatives stratégiques. Ces outils appartiennent à une nouvelle catégorie de logiciels, que l'on appelle des solutions de gestion du travail. Asana en est l'un des leaders.

Asana aide des équipes comme la vôtre à planifier, organiser et accomplir leur travail afin qu'elles puissent gagner en productivité et obtenir de meilleurs résultats. Plus de 100 000 organisations payantes et des millions d'utilisateurs dans 190 pays font confiance à Asana pour améliorer la transparence de leurs activités et travailler en synergie. Asana leur permet de s'assurer que chaque membre de l'équipe est en mesure d'identifier le travail à accomplir, mais également le responsable et l'échéance de chaque tâche.

Nos clients confient leurs données à Asana de façon à pouvoir se concentrer pleinement sur leurs activités essentielles. C'est la raison pour laquelle nous avons à cœur de leur proposer une solution de gestion du travail à la fois collaborative et ergonomique, mais également d'assurer la sécurité de leurs données.

La sécurité des données tient une place centrale dans la culture d'entreprise d'Asana et nous y sensibilisons tous nos employés. Cette culture, qui prône confiance et transparence, reflète notre attitude générale ainsi que le degré de sensibilisation et d'importance que nous accordons à la protection des éléments d'information appartenant à nos clients. Cette sensibilisation est renforcée par nos valeurs et normes de conduite communes, au travers de déclarations de principes, de codes de conduite, ou encore d'énoncés de mission et de valeurs, communiqués par notre équipe de direction. En outre, cette dernière prend des mesures pour créer un environnement qui favorise aussi bien la prise de responsabilités que la capacité à déléguer.

Lors de la conception et de la mise en place de nos programmes et pratiques de sécurité, nous mettons l'accent sur les principes suivants :

- Garantir la sécurité physique et environnementale nécessaire à la protection de nos applications Web et mobiles face aux accès non autorisés
- Assurer le maintien de la disponibilité de nos applications
- Fournir la confidentialité requise pour protéger les données de nos clients
- Faire preuve d'intégrité afin de garantir l'exactitude et la cohérence des données tout au long de leur cycle de vie

Ce livre blanc aborde les questions de sécurité et de confidentialité sous plusieurs angles : infrastructure, produit, opérations, respect des réglementations et certifications.

La majeure partie de ce livre blanc s'applique à l'ensemble des formules Asana. Toutefois, celui-ci s'adresse tout particulièrement aux formules Asana payantes (Premium, Business et Enterprise).[2] Les fonctionnalités réservées à certaines formules sont signalées dans ce document.

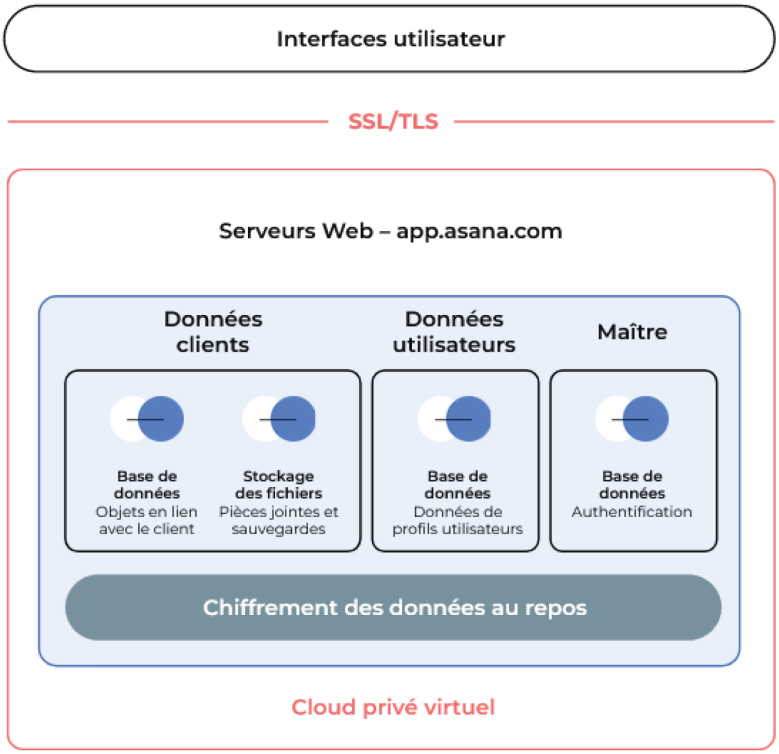
[2] Pour en savoir plus sur les différentes formules Asana, veuillez consulter asana.com/fr/pricing.

Infrastructure

Asana a recours à des offres de service de cloud computing (informatique dématérialisée), essentiellement auprès d'Amazon Web Services (AWS), pour les composantes clés de sa plateforme.

AWS gère la sécurité et la compatibilité de l'infrastructure de cloud computing, tandis qu'Asana assure la sécurité et la compatibilité des logiciels et des données sensibles conservés dans cette même infrastructure. Pour en savoir plus, veuillez consulter le modèle de responsabilité partagée d'AWS.[3]

Asana fait appel au Cloud privé virtuel d'Amazon. L'architecture de son réseau a été conçue à partir des services de réseaux et composantes de base offerts par AWS, dans le but de garantir un maximum de sécurité, d'évolutivité et d'ergonomie. La majorité de la plateforme Asana fonctionne grâce aux services *Elastic Compute Cloud* (EC2) d'Amazon, permettant ainsi un traitement fiable, évolutif et sécurisé des données clients. Le schéma simplifié ci-dessous présente l'infrastructure générale d'Asana.



[3] https://aws.amazon.com/fr/compliance/shared-responsibility-model/

L'infrastructure de production d'Asana est sécurisée de façon à limiter la réception du trafic Web extérieur aux seules machines de répartition de charge. Chaque hôte se voit attribuer un certain rôle et différents groupes de sécurité servent à délimiter le trafic prévu entre ces rôles.

Serveurs Web

La capacité sécurisée, fiable et basée sur le cloud d'Amazon EC2 constitue la majorité de nos ressources en matière de serveurs Web. Ces derniers traitent les données de nos clients et fournissent les fonctionnalités d'application aux utilisateurs d'Asana. Ces serveurs communiquent également avec d'autres parties de notre infrastructure.

Bases de données

Asana a recours au service RDS (Relational Database Service) d'Amazon, qui fait tourner une base de données MYSQL gérée.

Maître

Stocke les mots de passe chiffrés (hachés et salés par bcrypt), les informations d'authentification des différents utilisateurs et d'autres métadonnées qui permettent le routage du trafic.

Données clients

Stocke toutes les informations importées ou téléchargées sur Asana par les clients, notamment liées aux tâches et projets.

Données utilisateurs

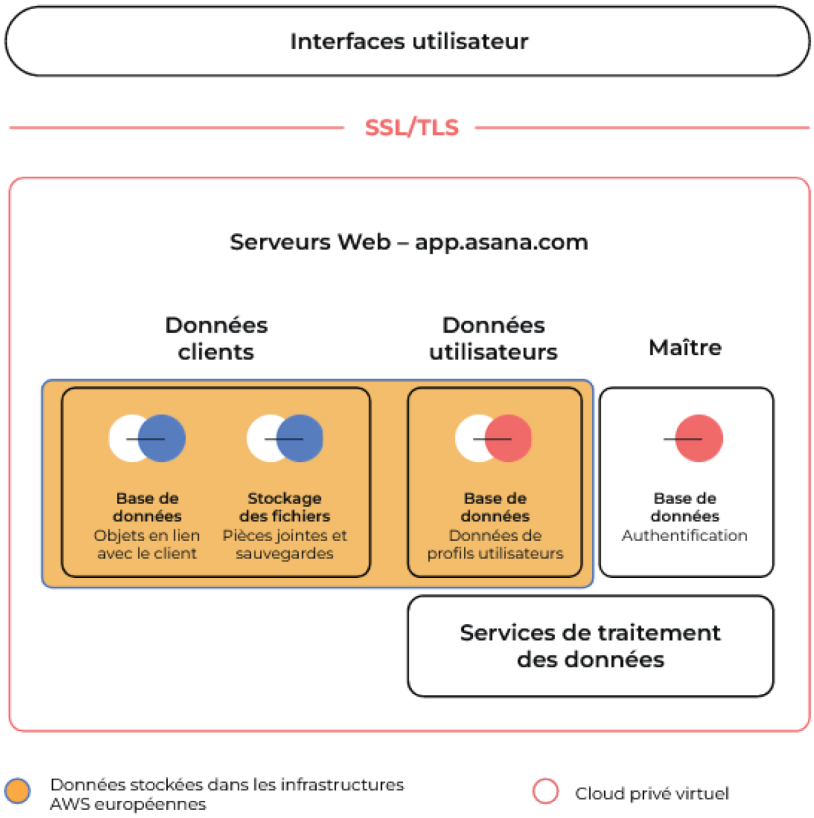
Stocke les informations en rapport avec les profils utilisateurs, comme les noms et les adresses e-mail.

Stockage des fichiers

Pour nos serveurs de stockage, nous faisons appel au Simple Storage Service (S3) d'Amazon. Ces serveurs stockent les pièces jointes et les sauvegardes des bases de données. Les pièces jointes représentent tous les fichiers importés dans des tâches Asana directement depuis un ordinateur. Les pièces jointes en provenance de plateformes de collaboration de contenu hébergées sur le cloud prennent la forme de liens vers ces plateformes, et ne sont pas stockées sur les serveurs de stockage d'Asana.

Infrastructure européenne

Asana met des centres de données européens à disposition des clients Enterprise qui ont besoin de stocker leurs données en Europe. Les données clients et la plupart des données utilisateurs seront stockées dans la région AWS de Francfort (Allemagne), tandis que les sauvegardes seront stockées dans la région AWS de Dublin (Irlande). Les installations AWS sont utilisées à la fois pour l'infrastructure américaine et pour l'infrastructure européenne. Le schéma simplifié ci-dessous présente l'infrastructure générale d'Asana applicable aux clients utilisant l'infrastructure européenne.



Sécurité des données

Chiffrement

Les connexions vers app.asana.com sont chiffrées en 128 bits et compatibles avec la norme TLS 1.2 et ses versions ultérieures. Les connexions sont chiffrées et authentifiées par chiffrement AES_128_GCM, avec échange de clés ECDHE_RSA. Asana prend en charge la confidentialité persistante et le chiffrement AES-GCM, et bloque les connexions non sécurisées utilisant le chiffrement RC4 ou le protocole TLS 1.1 et versions antérieures. Le transfert des données de connexion et des données sensibles se fait exclusivement par protocole TLS. Asana garantit le chiffrement au repos des données des clients par le biais de clés secrètes AES 256 bits.[4]

Clés de chiffrement Enterprise

Certains clients Enterprise ont la possibilité d'utiliser leurs propres clés de chiffrement pour chiffrer leurs données stockées sur Asana. Ils peuvent faire appel au KMS (Key Management Service) d'AWS (Amazon Web Services) pour leurs clés de chiffrement. Les clients utilisant les clés de chiffrement Enterprise d'Asana ont le contrôle sur les clés de chiffrement applicables à la base de données, aux pièces jointes et aux recherches de leur domaine, ainsi qu'à la plupart des données utilisateurs de leur Organisation. Pour en savoir plus et installer les clés de chiffrement Enterprise d'Asana, veuillez contacter notre service commercial à l'adresse sales@asana.com.

[4] Pour en savoir plus sur les données concernées par le chiffrement sur Asana, veuillez consulter le diagramme en page 4.

Architecture multi-tenant

Asana a recours à Amazon Web Services pour garantir l'évolutivité de son service. Un duplicata de la base de données est créé en simultané afin de permettre à Asana de récupérer rapidement les données en cas de défaillance. En guise de précaution supplémentaire, Asana effectue régulièrement des captures de la base de données, qui sont transférées en toute sécurité vers un centre de données séparé. Ainsi, les accès utilisateur peuvent être restaurés, même en cas de défaillance régionale d'Amazon.

Évolutivité et fiabilité

Asana s'engage à faire bénéficier ses clients Enterprise d'une garantie de disponibilité de 99,9 %. Les utilisateurs peuvent consulter et s'abonner aux mises à jour de statut pour rester informés de l'état du système à l'adresse status.asana.com. Cette dernière indique la disponibilité de nos applications Web et mobiles, sans oublier notre API, au cours des douze dernières heures, des sept derniers jours, des trente derniers jours et de l'année écoulée.

Niveau de disponibilité du système

Asana s'engage à faire bénéficier ses clients Enterprise d'une garantie de disponibilité de 99,9 %. Les utilisateurs peuvent consulter et s'abonner aux mises à jour de statut pour rester informés de l'état du système à l'adresse status.asana.com. Cette dernière indique la disponibilité de nos applications Web et mobiles, sans oublier notre API, au cours des douze dernières heures, des sept derniers jours, des trente derniers jours et de l'année écoulée.

Sauvegardes

Asana réalise des captures quotidiennes de sa base de données. Ces sauvegardes bénéficient du même niveau de protection que les bases de données de production. Nous effectuons également des sauvegardes interrégionales. Pour les clients rattachés à notre centre de données UE, les données sauvegardées sont conservées en Irlande

Fonctionnalités de sécurité du produit

Asana fournit aux utilisateurs et administrateurs toutes les fonctionnalités dont ils ont besoin pour protéger leurs données. Ces fonctionnalités leur permettent de bénéficier de commandes d'administration étendues et d'une visibilité optimale sur les données clients. La disponibilité des fonctionnalités présentées ci-dessous dépend de la formule Asana choisie. Pour découvrir nos formules, veuillez vous rendre sur asana.com/fr/pricing.

Administrateurs

Les administrateurs gèrent les équipes, et attribuent ou révoquent les privilèges d'accès des membres et invités au fur et à mesure que ces derniers rejoignent ou quittent l'entreprise, ou un processus. Ils peuvent également utiliser l'API d'administration d'Asana pour gérer les exportations de domaines, les configurations, les autorisations, les applications tierces, ainsi que les paramètres des utilisateurs et des équipes.

Attribution et révocation des accès utilisateurs

Asana permet aux utilisateurs et administrateurs de contrôler l'accès à leurs données.

- Les utilisateurs et administrateurs peuvent convier des membres et invités (contributeurs externes) à rejoindre leurs organisations et équipes.
- Les administrateurs peuvent retirer des membres et invités depuis la console d'administration.

Par ailleurs, les clients Enterprise peuvent intégrer Asana à leur fournisseur d'identité cloud avec la norme SCIM (System for Cross-domain Identity Management), ce dans le but d'attribuer et révoquer les accès utilisateurs pour plusieurs solutions SaaS.[5]

Sécurité de connexion

Sur Asana, les administrateurs peuvent décider du procédé suivi par les utilisateurs pour se connecter à leur compte. Trois options sont possibles : les identifiants Asana, l'authentification unique de Google (SSO) ou l'authentification unique par SAML 2.0.

Protection des mots de passe

Lorsque les utilisateurs sont autorisés à se connecter à leur compte en utilisant leurs identifiants Asana, les administrateurs peuvent spécifier le degré de complexité des mots de passe. Dans le cas de mots de passe « complexes », les utilisateurs devront employer au minimum 8 caractères, incluant au moins trois des éléments suivants : minuscules, majuscules, chiffres et caractères spéciaux.

Les administrateurs peuvent aussi forcer la réinitialisation du mot de passe de tous les membres de leur Organisation.

Authentification unique de Google (SSO)

Les administrateurs peuvent demander aux utilisateurs de l'Organisation de se connecter à Asana à l'aide de leur compte Google Workspace.

[5] https://asana.com/fr/guide/help/premium/scim

Authentification unique par SAML

Les administrateurs Enterprise peuvent configurer leur fournisseur d'identité et demander à ce que leurs utilisateurs se connectent sur Asana à l'aide de leurs identifiants de fournisseur d'identité cloud. Cette configuration se fait par le biais de la norme d'authentification SAML. Depuis la console d'administration d'Asana, les administrateurs Enterprise peuvent définir la durée pendant laquelle l'authentification SAML sera possible avant expiration du droit d'accès.

API Journal d'audit

L'API Journal d'audit d'Asana permet aux administrateurs Enterprise de détecter les menaces de sécurité éventuelles sur Asana via Splunk ou tout autre fournisseur SIEM (Security Information and Event Management) de votre choix. Grâce à son intégration unique à Splunk, les équipes informatiques ont une visibilité optimale sur les activités de conformité stratégiques sur Asana et peuvent en assurer la surveillance directement sur le tableau de bord Splunk. Par ailleurs, les administrateurs peuvent faire le nécessaire en amont pour sécuriser les données de leur structure et se fier à des alertes personnalisées pour prendre des mesures sans délai en cas d'activité suspecte.[6]

Autorisations d'accès

Les administrateurs et utilisateurs peuvent inviter d'autres utilisateurs à accéder à leurs données. Lorsque des utilisateurs sont conviés à rejoindre une Organisation, ils peuvent disposer de différents privilèges en tant qu'invités. Un utilisateur peut être invité pour un objet précis (tâche, projet, équipe ou Organisation) et disposer de différents types d'accès. Les autorisations sont définies au niveau de chaque objet pour un utilisateur donné et non à l'échelle d'un utilisateur individuel. Par exemple, un même utilisateur peut à la fois avoir accès à un certain élément en ayant uniquement l'autorisation de le commenter, n'avoir aucune visibilité sur un autre élément, avoir accès à un troisième élément exclusivement « sur demande », ou encore disposer des droits d'accès complets (consultation et modification) sur un quatrième élément. Pour en savoir plus sur chaque objet et les différents types d'autorisations, veuillez consulter le guide d'Asana : asana.com/fr/guide.

Objets Asana

Tâche

Sur Asana, les tâches peuvent être privées ou publiques et appartenir à un projet privé ou public.

Tâche :	Accessible par :
Tâche privée	Les collaborateurs de la tâche uniquement
Tâche publique	Tous les membres de l'Organisation
Tâche appartenant à un projet privé	Les collaborateurs de la tâche et les membres du projet
Tâche appartenant à un projet public	Les collaborateurs de la tâche, les membres du projet et de l'équipe
Sous-tâche	Les collaborateurs de la sous-tâche et les utilisateurs ayant accès à la tâche parente

[6] https://asana.com/fr//help/api/audit-log-api

Projets

Sur Asana, les projets peuvent être privés ou publics. Tout utilisateur qui a accès à un projet a également accès à toutes les tâches et discussions appartenant à ce projet. Lorsque des utilisateurs sont ajoutés à un projet, il est possible de leur octroyer des droits de modification ou un droit de commentaire uniquement. Les administrateurs Enterprise peuvent définir la confidentialité d'équipe par défaut au sein de leur Organisation.

Projet :	Accessible par :
Projet privé	Les membres du projet
Projet public	Les membres de l'équipe et du projet
Projet public appartenant à une équipe publique	Les membres de l'Organisation, de l'équipe et du projet

Équipes

Sur Asana, les équipes peuvent être masquées, publiques ou instaurer une adhésion sur demande. Tout utilisateur qui appartient à une équipe a également accès à l'ensemble des discussions et projets publics appartenant à cette équipe.

Équipe :	Accessible par :	Adhésion possible :
Masquée	Membres de l'équipe	Non
Publique au sein de l'Organisation	Les membres de l'équipe et de l'Organisation	Oui
Adhésion sur demande	Membres de l'équipe	Sous condition d'approbation

Organisations

Sur Asana, les Organisations sont les objets qui se trouvent au plus haut niveau. Elles contiennent les équipes, les projets et les tâches.

Utilisateurs

Sur Asana, les utilisateurs disposent de comptes individuels associés à leur adresse e-mail. Comme mentionné auparavant, chaque compte peut avoir accès à différents objets de données. En outre, par défaut, les comptes utilisateurs ont automatiquement accès à une Organisation en fonction de leur domaine de messagerie.

Membres à part entière

L'adhésion à une Organisation dépend du domaine associé à votre adresse e-mail. Pour devenir membre d'une Organisation, vous devez disposer d'une adresse e-mail associée à l'un des domaines de messagerie électronique approuvés par cette Organisation.

Un membre de l'Organisation peut effectuer les actions suivantes :

- Créer de nouvelles équipes
- Consulter la liste complète des équipes qu'il peut demander à rejoindre au sein de l'Organisation
- Consulter les noms et adresses e-mail des autres membres et invités de l'Organisation
- Accéder aux projets et tâches ayant été rendus publics au sein de l'Organisation

Invités

Vous pouvez collaborer avec des clients, sous-traitants, fournisseurs ou tout autre intervenant ne disposant pas d'une adresse e-mail associée à un domaine approuvé par votre Organisation. Ces utilisateurs deviendront des invités de l'Organisation. Les invités ont un accès limité à votre Organisation et peuvent consulter ce qui est explicitement partagé avec eux uniquement.

L'invité d'une Organisation ne peut rejoindre des équipes que sur invitation. Il ne peut pas créer, voir ou envoyer une demande pour rejoindre d'autres équipes.

Membres à accès limité

Chaque équipe a ses propres membres et projets. Les membres qui ne sont pas autorisés à accéder à tous les projets de votre équipe s'afficheront en tant que *membres ayant accès à des projets spécifiques* dans les paramètres de l'équipe, sous l'onglet « Membres ».

Les *membres ayant accès à des projets spécifiques* peuvent consulter les projets et tâches auxquels ils ont été ajoutés, mais pas les discussions ou autres projets de l'équipe concernée.

Gestion des invités

Les administrateurs Enterprise peuvent décider de qui est en mesure de convier des contributeurs externes (invités). Ces administrateurs ont accès aux trois options ci-dessous pour déterminer qui a l'autorisation de convier des utilisateurs à rejoindre l'Organisation en tant qu'invités :

- Les administrateurs uniquement
- Les administrateurs et les membres de l'Organisation
- Tout le monde (y compris les membres de l'Organisation et les invités)

Ajout d'applications à une liste blanche

Les administrateurs Enterprise peuvent décider d'autoriser l'usage de certaines intégrations tierces par leurs utilisateurs sur leur compte Asana, et bloquer les intégrations indésirables. Pour découvrir toutes les applications tierces disponibles, veuillez vous rendre sur la page asana.com/fr/apps.

Contrôle des données

Les clients peuvent exporter ou supprimer des données d'Asana en toute simplicité et de manière sélective, mais également automatiser des exportations intégrales de domaines grâce à son API.

Sécurité de l’application

Les services Asana sont proposés sur un logiciel accessible en ligne, sous la forme d’un service d’application. Les utilisateurs peuvent accéder à leurs données depuis un navigateur, une application mobile (Android et iOS) ou une interface de programmation d’application (API).

Les services et composants qui forment Asana sont essentiellement écrits en code JavaScript, TypeScript, Python et Scala, et se basent sur le cadre d’applications React. Le développement d’Asana se fait dans le respect des bonnes pratiques de sécurité recommandées par la fondation OWASP, en adoptant une approche systématique de sécurité dès la conception. Asana a donc mis en place des mécanismes rigoureux pour maîtriser les risques de sécurité, dont voici une liste non exhaustive :

- Faille d’injection
- Violation de gestion d’authentification et de session
- Fuite d’informations sensibles
- Attaque XML External Entities (XXE)
- Violation de contrôle d’accès
- Faille de sécurité due à une mauvaise configuration
- Faille Cross-Site Scripting (XSS)
- Désérialisation non sécurisée
- Utilisation de composants tiers vulnérables
- Journalisation et surveillance insuffisantes
- Falsification de requête inter-site (CSRF)
- Faille de redirection et renvoi non validé

Tous les ans, Asana passe des audits de sécurité pour les 10 principales menaces identifiées par OWASP.

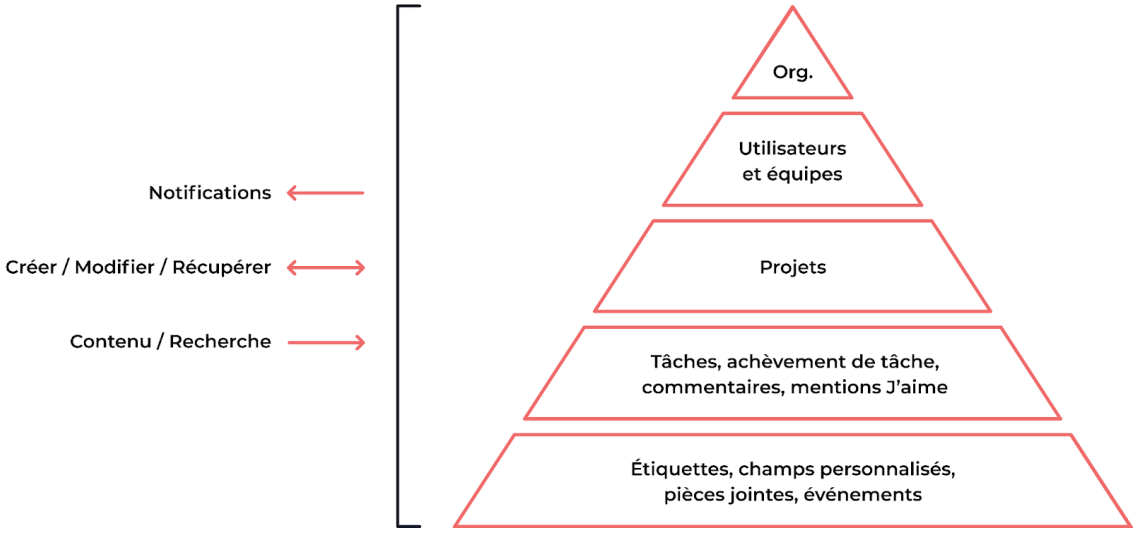
Plateforme Asana

Intégrations

Asana permet à ses utilisateurs d'accéder à leur compte depuis une API (Application Programming Interface)[7]. L'API d'Asana est une interface de type RESTful. Ses utilisateurs peuvent la programmer pour mettre à jour et accéder à une grande partie de leurs données sur la plateforme, et réagir automatiquement à tout changement. L'API fournit des URL prévisibles permettant l'accès aux ressources, et utilise des fonctionnalités HTTP intégrées pour la réception des commandes et l'envoi des réponses. Ce système facilite la communication avec Asana depuis un large éventail d'environnements, notamment des utilitaires en ligne de commande, des plugins de navigateur ou encore des applications natives. Les clients peuvent faire appel à ces API pour créer des solutions personnalisées ou les intégrer à d'autres logiciels. L'API d'Asana est compatible avec une authentification par protocole OAuth 2.0 ou par jetons d'accès personnels.

Pour en savoir plus sur l'API d'Asana, veuillez vous rendre sur la page asana.com/fr/developers.

L'illustration ci-dessous présente un résumé des actions envisageables et des objets de l'environnement de travail.



Par défaut, les logiciels et scripts disposent des mêmes autorisations que l'utilisateur qui les emploie. Les données de travail se limitent aux données auxquelles l'utilisateur a accès. Lorsqu'il leur faut des accès plus étendus, les clients Enterprise peuvent faire appel à des comptes de service.

Comptes de service

Les clients Asana Enterprise peuvent employer des comptes de service pour accéder à l'ensemble de leur contenu. Par exemple, ils peuvent les utiliser pour exporter la totalité des données d'une Organisation ou pour suivre l'activité d'une équipe. Pour en savoir plus, consultez le guide d'Asana[8].

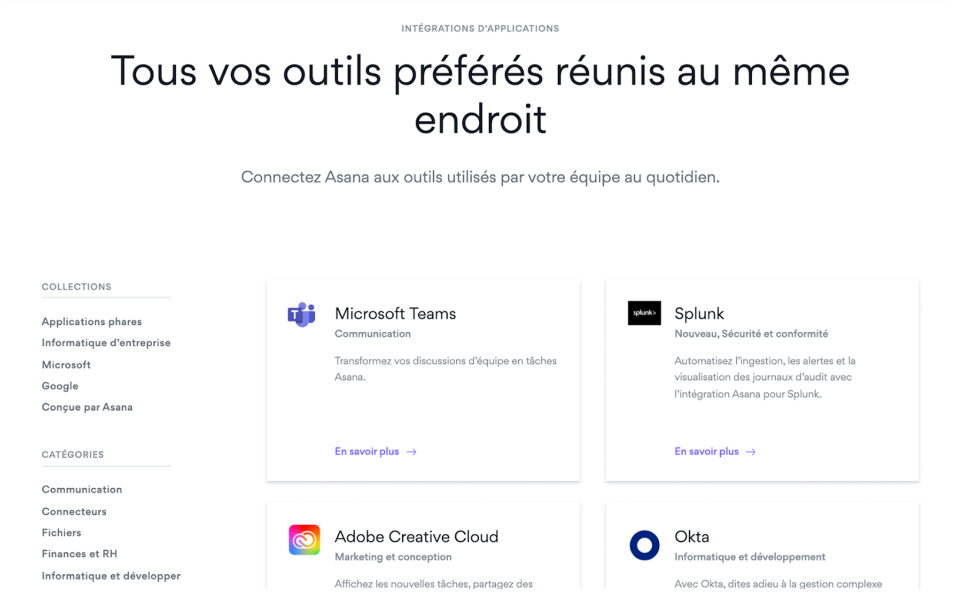
[7] https://asana.com/fr/guide/help/api/api
[8] https://asana.com/fr/guide/help/premium/service-accounts

Applications tierces

L'API d'Asana permet de réaliser des centaines d'intégrations uniques, que les clients peuvent utiliser pour améliorer ou agrémenter leur expérience sur Asana. Asana s'intègre à de nombreux outils pour simplifier les processus clients et augmenter leur productivité. Des outils tiers d'autres fournisseurs peuvent également y être intégrés. Voici une liste non exhaustive de certaines des fonctions de ces outils :

- Synchronisation des messages entre plusieurs applications
- Automatisation des processus
- Extensions de plateforme
- Développement logiciel
- Importations de données
- Partage de fichiers
- Création de rapports (reporting)
- Suivi du temps
- Réception de données

Pour consulter l'annuaire des applications tierces, veuillez vous rendre sur la page asana.com/fr/apps.



Sécurité opérationnelle

Sécurité des informations Asana

Asana a mis en place un programme officiel de gestion de la sécurité de l'information et fait appel à une équipe de sécurité spécialisée, qui travaille sous la supervision du responsable de la sécurité d'Asana. Cette organisation est chargée de mettre en place des contrôles de sécurité et de repérer toute activité suspecte sur Asana.

Informations confidentielles

Toutes les données clients sont traitées par Asana de façon strictement confidentielle. Les politiques d'Asana restreignent l'accès aux informations confidentielles aux seuls employés ayant besoin d'accéder à ces informations dans le cadre de leurs fonctions, et dans la mesure où ledit accès est nécessaire pour fournir un service donné au client. Ainsi, l'employé a pour consigne de n'accéder qu'aux informations qui lui sont strictement nécessaires pour accomplir la tâche concernée.

Ressources humaines

Tous les employés et sous-traitants sont tenus de signer un accord de confidentialité et d'inventions. En outre, les employés d'Asana doivent suivre une formation officielle de sensibilisation à la sécurité, dès leur embauche, puis une fois par an.

Tous les ingénieurs employés par Asana signent un accord sur la politique d'accès aux données, laquelle décrit les modalités d'accès aux données clients et comment les utiliser de manière appropriée. Enfin, des passerelles ont été mises en place à tous les points d'entrée menant aux données clients et chaque accès aux données est répertorié et conservé indéfiniment.

Asana applique une politique disciplinaire et sanctionne les violations de politiques.

Accès des utilisateurs : analyses et politique

Chaque trimestre, l'administration fait le bilan des accès utilisateurs accordés aux différents systèmes pour s'assurer de leur pertinence et supprime les accès devenus superflus. Lorsque le contrat d'un employé arrive à son terme, ses droits d'accès sont révoqués.

Sécurité physique

Locaux d'Asana

L'accessibilité aux bureaux d'Asana est sécurisée et se fait par carte d'accès avec registre. Tous les bureaux sont munis de systèmes d'alarme anti-intrusion. Les visiteurs ont l'obligation de se signaler à la réception. Tous les employés sont tenus de déclarer d'éventuelles activités suspectes, accès non autorisés aux locaux ou vols/pertes d'objets.

Sécurité des centres de données

Asana se fie à AWS pour ses contrôles physiques et environnementaux.[9]

Sécurité des réseaux

Asana surveille la disponibilité du réseau de ses bureaux et des appareils qui s'y trouvent. Tous les journaux produits par les périphériques réseau tels que pare-feux, serveurs DNS, serveurs DHCP et routeurs sont recueillis au même endroit. Les journaux réseau des périphériques de sécurité (pare-feux), points d'accès sans fil et commutateurs sont conservés.

Sécurité informatique

Les disques durs de tous les ordinateurs portables et postes de travail sont sécurisés par chiffrement intégral et reliés à une image gérée de manière centralisée. Les machines des employés d'Asana sont mises à jour régulièrement et leurs postes de travail sont contrôlés pour détecter tout programme malveillant. Asana est également en mesure d'appliquer des correctifs critiques ou d'effacer les données d'une machine à distance depuis un gestionnaire de périphériques. Dans la mesure du possible, Asana utilise la double authentification pour sécuriser encore davantage l'accès à l'infrastructure de son entreprise. Des analyses de sécurité sont effectuées à intervalles réguliers.

Gestion des risques et vulnérabilités

Asana suit un processus de gestion des risques qui a pour but d'identifier par avance d'éventuelles vulnérabilités au sein de ses systèmes et d'évaluer l'émergence de nouveaux risques pour les opérations de l'entreprise.

Asana suit un processus visant à réaliser des analyses de vulnérabilité sur les systèmes internes et externes de son environnement de production. L'équipe de sécurité d'Asana effectue ces analyses au moins une fois par trimestre, et les vulnérabilités sont corrigées après exécution et analyse d'une évaluation des risques. Chaque évolution importante de l'environnement de production s'accompagne également d'analyses de vulnérabilité déterminées par le responsable de la sécurité.

Tests d'intrusion

Asana s'associe à des experts de la sécurité indépendants pour tester son code face aux failles de sécurité les plus courantes et pour soumettre ses serveurs de production à des outils d'analyse de réseau. Des tests d'intrusion sont réalisés chaque année. Les vulnérabilités vérifiables sont corrigées, puis testées de nouveau.

Chasse aux bugs

Asana a mis en place un programme externe de chasse aux bugs[10] destiné à rémunérer les chercheurs en sécurité qui découvrent des vulnérabilités.

Cycle de vie du développement logiciel

Asana s'appuie sur le système de contrôle de révisions Git. Les modifications apportées au code base d'Asana passent par une série de tests automatisés, puis par des révisions manuelles. Après avoir réussi les tests du système automatisé, les modifications sont envoyées sur un serveur de

[9] https://aws.amazon.com/fr/compliance/data-center/controls/
[10] http://asana.com/bounty

simulation, où des employés d'Asana peuvent procéder à des tests avant de les appliquer aux serveurs de production et aux clients. Les modifications et fonctionnalités particulièrement sensibles sont également soumises à un examen de sécurité spécifique. Enfin, les ingénieurs d'Asana peuvent sélectionner certaines mises à jour critiques et les appliquer instantanément aux serveurs de production.

Outre la liste de toutes les modifications apportées au contrôle d'accès, Asana met en place toute une série de tests unitaires automatisés destinés à vérifier que les règles de contrôle d'accès sont correctement établies et appliquées.

Réponse aux incidents

Asana a adopté un plan de réponse aux incidents, lequel a pour but d'opposer un plan d'intervention rationnel et cohérent aux incidents de sécurité (présumés ou avérés). Ces derniers impliquent, de manière accidentelle ou illicite, la destruction, la perte, le vol, l'altération, la divulgation ou l'accès non autorisé à des données exclusives ou personnelles transmises, conservées ou traitées par Asana. Ces procédures à suivre en cas d'incident précisent les méthodes employées par l'équipe de sécurité d'Asana pour classifier, enquêter, corriger et communiquer à propos des incidents de sécurité. Asana a conclu des contrats avec des spécialistes indépendants en investigation numérique et d'entreprises spécialisées dans la réponse aux incidents afin d'être en mesure de répondre à d'éventuelles violations de données.

Reprise après sinistre et continuité des activités

Asana a établi un plan de continuité des activités applicable dans le cadre d'arrêts prolongés de ses services en raison de désastres imprévus ou inévitables, ceci afin de rétablir ses services du mieux possible dans un délai raisonnable. L'entreprise a documenté par écrit les politiques et mesures de reprise après sinistre à adopter pour assurer la reprise ou la continuité de ses infrastructures technologiques clés à la suite d'un sinistre.

Les principaux centres de données d'Asana sont hébergés sur les sites AWS de Virginie (USA) et de Francfort (Allemagne) pour les États-Unis et l'Europe respectivement, avec des doublons[11] dans ces mêmes régions AWS. En cas de sinistre dans l'un des centres de données AWS, les procédures de récupération activent les nœuds d'un autre centre de données. Pour se prémunir de sinistres majeurs, un centre de reprise des activités en cas de sinistre est hébergé dans un centre de données AWS de l'Ohio (USA) pour les États-Unis et de Dublin (Irlande) pour l'Europe.

Conservation et suppression des données

Asana conserve les informations du client durant toute la période nécessaire à l'accomplissement des objectifs qui figurent dans sa politique de confidentialité. Sur simple demande de la part d'un représentant autorisé par le client, et après vérification, ce dernier peut demander l'exportation ou la suppression de ses données de domaine. Asana peut également convenir de préserver la confidentialité des données clients conservées et de ne traiter activement ces données qu'après la date de demande, conformément aux lois auxquelles l'entreprise est assujettie.

[11] Zone de disponibilité multiple via déploiement multi-AZ d'Amazon RDS.

Surveillance

Asana s'appuie sur Amazon Cloudwatch et Cloudtrail et les combine à des scripts personnalisés pour extraire les données clés de ses journaux et les transférer vers ses services de surveillance. L'entreprise contrôle la capacité d'utilisation de ses infrastructures physiques et informatiques, que ce soit pour répondre à ses besoins internes comme pour s'assurer que le service offert à ses clients correspond au niveau de service garanti dans ses accords. Le réseau et les applications d'Asana sont soumis à des analyses de sécurité automatisées, et nous avons mis en place une surveillance et un système d'alerte au niveau du noyau des serveurs. Un script de surveillance est lancé chaque semaine pour s'assurer que les modifications de code ont bien été validées.

Certains journaux d'application et journaux machine sont conservés indéfiniment, généralement à l'aide de la solution de stockage à long terme Amazon S3. Les journaux machine les plus détaillés sont exclusivement conservés sur la machine qui les a produits, habituellement pendant deux semaines.

Sous-traitance et gestion des fournisseurs

Asana prend toutes les mesures nécessaires pour sélectionner et fidéliser des tiers fournisseurs de services qui ont à cœur de respecter et mettre en œuvre des mesures de sécurité conformes à ses propres politiques. Avant d'utiliser un logiciel ou de faire appel à un fournisseur de logiciels, les équipes informatique, de sécurité et celle chargée de la confidentialité chez Asana examinent attentivement les protocoles de sécurité du fournisseur concerné, ses politiques de conservation des données, de confidentialité, ainsi que ses antécédents en matière de sécurité. Ces équipes se réservent le droit de rejeter l'utilisation de tout logiciel ou fournisseur de logiciel n'ayant pas démontré une capacité suffisante à protéger les données d'Asana et de ses utilisateurs finaux. Les fournisseurs sont chaque année soumis à de nouvelles évaluations critiques.

Afin de permettre à un sous-traitant de traiter les données personnelles des clients, Asana (et ses filiales le cas échéant) doit conclure un accord écrit avec chaque sous-traitant. Cet accord inclut des obligations en matière de protection des données, lesquelles doivent garantir un niveau de protection au minimum équivalent à celui des mesures techniques et organisationnelles mises en place par Asana pour protéger les données personnelles de ses clients contre toute destruction accidentelle ou illégale, perte, altération, ou contre toute divulgation ou tout accès non autorisés.

Pour consulter la liste de nos sous-traitants actuels et connaître les dernières informations à ce sujet, inscrivez-vous sur notre page dédiée aux sous-traitants.[12]

[12] http://asana.com/fr/terms#subprocessors

Confidentialité, certifications et conformité

Politique de confidentialité

La politique de confidentialité d'Asana détaille nos pratiques actuelles en matière de traitement des données. Elle est régulièrement mise à jour. Outre des précisions sur les données collectées et traitées par Asana, ladite politique renseigne les utilisateurs sur la marche à suivre pour exercer leurs droits en matière de confidentialité, conformément à la législation applicable.[13]

Transferts internationaux de données

Les lois européennes sur la protection des données exigent des organisations qu'elles recourent à un cadre législatif reconnu pour tout transfert de données de l'UE vers des pays qui ne disposent pas d'un cadre législatif de protection des données similaire, notamment les États-Unis.

Le transfert de données personnelles de l'UE et de la Suisse vers les États-Unis dans le cadre des boucliers de protection des données UE - États-Unis et Suisse - États-Unis n'est plus en vigueur. Cela étant, l'addendum d'Asana sur le traitement des données inclut les clauses contractuelles types, lesquelles constituent toujours un cadre juridique adapté pour le transfert de données personnelles en dehors de l'Espace économique européen (EEE). En outre, Asana a instauré ces clauses contractuelles types avec tous ses sous-traitants.

Pour assurer la protection des données personnelles transférées depuis l'EEE, Asana a adopté de nombreuses mesures supplémentaires, à commencer par celles détaillées dans le présent livre blanc. Asana se conforme aux bonnes pratiques du secteur, notamment le chiffrement des transferts de données de l'UE vers les États-Unis effectués par Asana par le biais de sa propre plateforme.

Bien qu'il ne soit pas possible de s'appuyer sur le bouclier de protection des données pour transférer des informations issues de l'EEE et de la Suisse, Asana a décidé de conserver sa certification liée à ce bouclier de protection des données pour continuer à assurer la protection des données déjà transférées dans le cadre de ce même bouclier, conformément à son engagement à garantir la sécurité des données.

Les directives réglementaires dans ce domaine continuent d'évoluer et Asana reste particulièrement attentif aux éventuelles nouvelles directives émises par les autorités chargées de la protection des données. Asana reste engagé à honorer le droit de ses clients au respect de leur vie privée et continuera de veiller à respecter les principales réglementations en matière de protection des données.

Règlement général sur la protection des données (RGPD)

Entré en vigueur le 25 mai 2018, le règlement général sur la protection des données (RGPD) est un règlement européen relatif à la protection des données personnelles des résidents européens. En vertu du RGPD, les organisations qui recueillent, conservent, utilisent ou traitent des données personnelles appartenant à des résidents européens (quelle que soit la localisation de l'organisation) doivent mettre en œuvre un certain nombre de mesures pour garantir la confidentialité et la sécurité de ces données. Asana a mis en place un programme détaillé de conformité RGPD et s'engage à coordonner ses efforts de mise en conformité avec ceux de ses clients et fournisseurs. Voici quelques-unes des mesures importantes prises par Asana pour faire correspondre ses pratiques aux exigences du RGPD :

- Des révisions des politiques et contrats conclus avec ses partenaires, fournisseurs et utilisateurs
- Des améliorations apportées à ses pratiques et procédures de sécurité

[13] https://asana.com/fr/terms#privacy-policy

- Une surveillance et un inventaire étroits des données recueillies, utilisées et partagées par Asana
- La création d'une documentation plus fiable concernant la politique de confidentialité et de sécurité d'Asana
- La formation des employés d'Asana aux exigences du RGPD, et plus généralement aux bonnes pratiques de confidentialité et de sécurité
- Après une analyse minutieuse, la création d'une politique concernant les droits des personnes sur les données, ainsi que du processus de réponse associé. Consultez la section ci-dessous pour en savoir plus sur les grands axes du programme de conformité au RGPD adopté par Asana et sur la façon dont les clients peuvent s'appuyer sur Asana pour leurs propres initiatives de conformité au RGPD.
- La nomination d'un responsable de la protection des données (« DPO ») que vous pouvez contacter à l'adresse dpo@asana.com.

Addendum relatif au traitement des données (DPA)

En vertu du RGPD, les « contrôleurs de données » (les entités qui déterminent les buts et moyens de traitement des données) doivent conclure des accords avec d'autres entités (les « processeurs de données »), qui traitent les données en leur nom. Asana offre à ses clients contrôlant des données personnelles européennes la possibilité de signer un addendum rigoureux sur le traitement des données (« DPA »), en vertu duquel Asana s'engage à traiter et assurer la sécurité des données personnelles conformément aux exigences du RGPD. À ce même titre, Asana a instauré des clauses contractuelles types et s'engage également à traiter les données personnelles suivant les instructions du contrôleur de données. Pour consulter l'addendum sur le traitement des données, rendez-vous sur la page des conditions générales.[14]

Application des lois

Asana respecte les directives sur l'application des lois concernant les demandes de données, comme indiqué sur la page concernée sur son site Web.[15]

Certifications et respect de la législation en vigueur

Asana a été évalué sur plusieurs standards de sécurité et de confidentialité, et a obtenu les certifications suivantes :

Norme SOC 2 (Service and Organization Controls)

Asana a réussi son audit SOC 2 (Type II) relatif aux contrôles adoptés en matière de sécurité, de disponibilité et de confidentialité. En pratique, l'obtention de l'attestation SOC 2 (Type II) se traduit par la mise en place de processus et pratiques respectant ces trois principes de contrôle, et par leur validation par un tiers indépendant.

Norme ISO/IEC 27001:2013

Asana a obtenu la certification ISO/IEC 27001:2013, laquelle témoigne de sa conformité aux exigences définies dans la norme ISO/IEC 27001:2013.

[14] https://asana.com/fr/terms#data-processing
[15] https://asana.com/fr/terms#law-enforcement-guidelines

Conclusion

Asana utilise au quotidien sa propre plateforme pour coordonner ses équipes partout dans le monde et travailler efficacement. Plus de 100 000 entreprises font déjà confiance à Asana pour ces mêmes raisons. Assurer la sécurité de vos données constitue la priorité d'Asana afin que vous puissiez accomplir vos tâches en toute sérénité.

Asana garantit une sécurité produit intégrale pour l'ensemble de votre organisation, en s'appuyant sur un programme de confiance et de conformité établi pour protéger vos données. Pour en savoir plus sur les formules payantes proposées par Asana, contactez notre service commercial à l'adresse sales@asana.com.

Vous souhaitez signaler un problème de sécurité ? Contactez-nous par e-mail à l'adresse security@asana.com.