Protection des données Atlassian Cloud

Introduction

Les données sont les actifs les plus critiques de votre organisation, mais elles sont de plus en plus difficiles à protéger et à sécuriser. Si les données ne sont pas correctement protégées, le coût d'une violation de données peut être élevé. En 2022, IBM estimait le coût moyen d'une violation de données à 4,35 millions de dollars.

Quels sont les défis ?

Gérer des systèmes informatiques complexes et interconnectés	La gestion de votre infrastructure informatique représente un travail conséquent. Le nombre de produits et d'apps utilisés par les équipes ne cesse d'augmenter. En moyenne, les entreprises utilisent entre 100 et 200 apps, dont la plupart sont gérées par des sociétés externes à leur service informatique. Quel que soit le propriétaire, ces apps et produits sont utilisés de concert pour que les données circulent entre eux, permettant ainsi la collaboration entre des équipes transverses. Les environnements complexes multi-apps augmentent la surface d'attaque et présentent des risques en raison des différents niveaux de sécurité des apps.

Veiller à ce que seules les bonnes personnes aient accès aux données	À mesure que votre organisation se développe, de plus en plus de personnes, d'appareils et d'apps accèdent à vos données, ce qui augmente les risques d'accès non autorisé. Il n'en est que plus difficile de trouver un équilibre entre productivité des utilisateurs et réduction des points d'accès.
S'adapter aux exigences réglementaires	Les secteurs et les zones géographiques ont des exigences qui précisent les contrôles qui doivent être mis en place dans un but de respect des obligations réglementaires et de protection des données personnelles. Mais le paysage évolue constamment et les exigences constituent une cible mouvante dont la surveillance demande un investissement important en temps. De plus, ces organes directeurs obligent de plus en plus les organisations comme la vôtre à prouver leur conformité à ces exigences.
Protéger les données sensibles	Les données de votre entreprise sont importantes, mais certaines peuvent être plus sensibles, comme les informations juridiques ou les dossiers des employés. Il est essentiel de classer correctement les données et de mettre en place des mesures de protection appropriées pour protéger les données sensibles telles que les informations d'identification personnelle, les informations de carte de crédit, et bien d'autres encore.
Rétablir le service à la suite d'une panne	L'impact d'une panne sur une organisation ne fait qu'augmenter à grande échelle. En moyenne, une minute de temps d'arrêt peut coûter 9 000 dollars à une entreprise. Si l'on multiplie ce chiffre par le nombre total de temps d'arrêt, une panne peut représenter un coût de plusieurs centaines de milliers de dollars. Mais les pannes n'ont pas seulement un impact sur votre chiffre d'affaires. Elles peuvent également entraîner des perturbations métier, des pertes de productivité interne, des sanctions financières et des litiges.
Détecter les menaces et y répondre	Vous ne pouvez pas contrôler les menaces que vous ne pouvez pas détecter. Votre organisation doit disposer de fonctionnalités intégrées de détection, de surveillance et de signalement des menaces. De nombreux produits ne proposent pas de solutions

	prêtes à l'emploi, ce qui oblige les organisations à gérer des produits supplémentaires qui s'ajoutent à une liste d'apps déjà bien longue.
Évaluer la sécurité et la confidentialité des apps du Marketplace	Les apps du Marketplace offrent la flexibilité nécessaire pour personnaliser et étendre votre solution complète. Cependant, de nombreuses apps sont créées et gérées par des tiers. L'installation d'une app nécessite une relation distincte avec l'entreprise qui la propose. Il est important de vérifier les apps installées sur votre instance, car elles peuvent traiter les données différemment du produit qu'elles étendent.

À ces défis s'ajoutent de bons et de mauvais acteurs : les personnes.

Les bons acteurs : peut-être avez-vous une équipe de sécurité dédiée à la protection de vos données, mais la plupart des membres de votre organisation ne sont pas des experts en la matière. Ils ne savent pas en quoi leurs actions peuvent contribuer à une violation de données. Par exemple, de nombreuses personnes réutilisent le même mot de passe. Si ces identifiants sont compromis, des hackers peuvent accéder aux données de votre organisation.

Les mauvais acteurs : malheureusement, certaines personnes cherchent activement à accéder de manière non autorisée à vos données et à nuire à votre activité. S'il peut s'agir d'employés mécontents, les hackers cherchent souvent à exploiter les vulnérabilités de votre environnement.

L'humain reste un facteur important en matière de violations. Qu'il s'agisse de l'utilisation d'identifiants volés, d'hameçonnage ou simplement d'une erreur, les utilisateurs continuent de jouer un rôle important dans les incidents comme dans les violations.

- *Verizon, Data Breach Investigation Report (DBIR) 2022*

Surmonter ces défis n'est pas impossible, mais nécessite les bons outils. C'est pourquoi nous avons spécialement doté les produits et solutions Atlassian Cloud des fonctionnalités et des capacités dont vous avez besoin pour protéger vos données.

Collaboration sécurisée grâce à une plateforme connectée et à la responsabilité partagée

Contrairement aux environnements auto-gérés, le cloud fonctionne selon un modèle de responsabilité partagée, ce qui signifie que la protection de vos données s'inscrit dans un partenariat entre vous et Atlassian.

[Insérer un modèle de responsabilité partagée entre le client et Atlassian]

- **Atlassian** : s'assurer que l'infrastructure qui soutient nos produits cloud est sécurisée
- **Vous** : gérer les informations de votre compte ainsi que les utilisateurs et les comptes utilisateur qui accèdent à vos données conformément à vos obligations de conformité.

Lorsque vous installez une app du Marketplace, vous introduisez un tiers dans cette équation. L'installation de l'app nécessite une relation avec un Marketplace Partner distincte de votre relation avec Atlassian.

[Insérer le même graphique que ci-dessus, en incluant le Marketplace. Voici un exemple]

Dans ce contexte, Atlassian et les Marketplace Partners jouent tous deux un rôle important dans un nouveau modèle de responsabilité partagée :

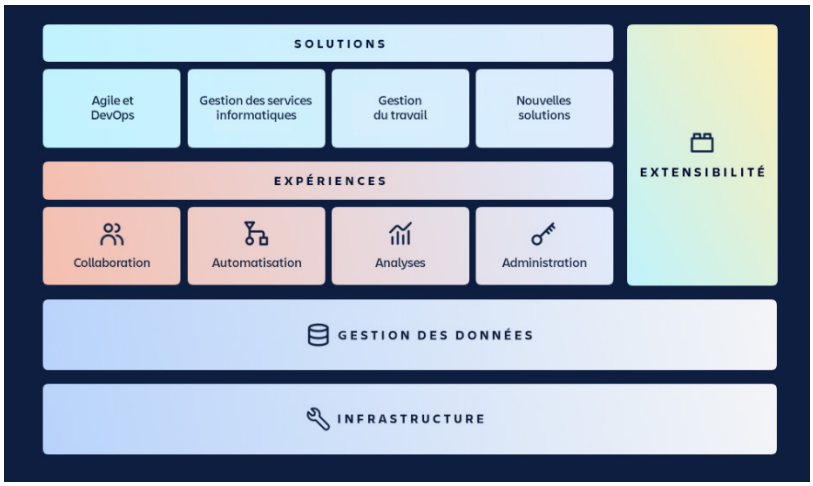
Marketplace Partners	Les Marketplace Partners sont responsables de leur propre infrastructure. Ils sont chargés de : ● concevoir des apps et des processus opérationnels conformément à leurs obligations légales, aux directives d'Atlassian pour les développeurs et aux bonnes pratiques générales du secteur pour créer et maintenir des apps fiables, conformes et sécurisées ; ● fournir une assistance et des informations pour aider les clients à prendre des décisions éclairées.
Atlassian	Atlassian est responsable de la sécurité de sa propre infrastructure et de l'assistance à ses partenaires et clients :

	• Nous fournissons des documents, des normes de sécurité et des fonctionnalités pour aider les partenaires à développer des apps fiables, conformément aux pratiques acceptées du secteur. • Nous nous efforçons également de fournir des informations et des contrôles centralisés sur un certain nombre de facteurs de confiance afin que vous puissiez évaluer et gérer les apps Cloud en fonction de vos besoins.
Vous	Vous faites votre part en utilisant les informations fournies par Atlassian et par les Marketplace Partners afin de déterminer si les apps sont conformes aux directives de votre organisation. Vous utilisez les contrôles disponibles pour gérer les apps installées.

Pour plus d'informations sur le modèle de responsabilité partagée, consultez notre synthèse.

Nous avons appliqué ce modèle à la plateforme Atlassian :

- Infrastructure sous-jacente professionnelle fiable et sécurisée à grande échelle
- Contrôles de protection des données améliorés vous permettant de sécuriser et de gérer vos données
- Expérience d'administration centralisée
- Extensibilité grâce à des milliers d'apps et d'intégrations



Dans ce livre blanc, vous découvrirez comment nous protégeons les données sur les trois niveaux de la plateforme, les fonctionnalités que vous pouvez utiliser pour répondre aux besoins de votre organisation et comment évaluer vos apps du Marketplace.

Section 1 : couche d'infrastructure Atlassian Cloud

Pour que vos équipes puissent donner le meilleur d'elles-mêmes, elles ont besoin d'accéder à leurs produits et à leurs données. Les temps d'arrêt ne sont pas une option. Des pannes peuvent toutefois se produire, et vous devez être en mesure de récupérer vos systèmes le plus rapidement possible sans perdre de données.

Les pannes peuvent être causées par un arrêt prolongé de l'infrastructure. Que vous gériez votre infrastructure ou que vous utilisiez des produits cloud, votre organisation compte sur vous et sur votre équipe informatique pour rétablir le service le plus rapidement possible. Malheureusement, il n'est pas toujours évident de savoir combien de temps prendra la récupération.

Nous avons développé Atlassian Cloud sur une infrastructure professionnelle fournissant des expériences fiables, pour que vous n'ayez pas à vous préoccuper des risques de perte de productivité de vos équipes ou de perte de chiffre d'affaires pour votre entreprise.

Ce que fait Atlassian : protéger vos données et limiter les pertes de données

Les produits Atlassian Cloud sont hébergés sur l'infrastructure en tant que service (IaaS) d'Amazon Web Services (AWS) dans de nombreuses régions du monde, notamment aux États-Unis, en Australie et dans l'Union européenne. Chacune de ces régions possède plusieurs zones de disponibilité (ZD) isolées les unes des autres. Comme les données sont répliquées vers les autres zones de disponibilité d'une région, en cas de panne de zone de disponibilité, vos données restent accessibles, ce qui garantit la haute disponibilité et le basculement.

> ***Remarque*** : nous proposons la résidence des données si vous avez besoin d'héberger vos données dans une région spécifique. Lorsqu'elle est activée, la résidence des données permet de rattacher les données concernées à une région spécifique.

La haute disponibilité et le basculement constituent la première ligne de défense pour rétablir les services en cas de panne de l'infrastructure. Nous utilisons également un programme de sauvegarde qui propose un autre moyen de récupérer des données.

Les systèmes internes et les services critiques, tels que nos produits, sont sauvegardés à l'aide de la fonction de création d'instantanés du service de base de données relationnelle (RDS) d'Amazon. Cela nous permet de créer des sauvegardes quotidiennes de chaque instance RDS. Ces instantanés sont conservés pendant 30 jours et sont chiffrés selon l'algorithme AES-256. Combinés aux journaux des transactions de base de données, les instantanés permettent une restauration à un point dans le temps, réduisant ainsi le risque de perte de données.

Ces sauvegardes sont également sécurisées et immuables. Les sauvegardes des magasins de données SQL des produits sont stockées et verrouillées dans un coffre-fort WORM (Write-Once-Read-Many). Ce processus protège les sauvegardes contre toute suppression potentielle par des acteurs et des logiciels malveillants, nous protégeant ainsi d'une perte complète de données.

> ***Remarque***
> Nous n'utilisons pas nos sauvegardes pour annuler les changements apportés par les clients, tels que la suppression de tickets ou de projets. Pour limiter les pertes de données, vous devez effectuer des sauvegardes régulières de vos données. Pour en savoir plus sur ces fonctionnalités, consultez la *section Gestion des données*.

Ce que fait Atlassian : identifier et limiter les vulnérabilités

L'un des facteurs les plus courants des défaillances des systèmes est l'exploitation de vulnérabilités. Pour limiter ce risque, nous avons mis en place les éléments suivants :

- **Tests d'intrusion externes** : les sociétés de conseil en sécurité effectuent des tests d'intrusion (tels que des tests de type boîte blanche, assistés par code et basés sur des menaces) sur des produits à haut risque. La validation et les résultats sont fournis par le biais de lettres d'évaluation publiées plusieurs fois par an.
- **Red Team d'Atlassian** : équipe qui reproduit des scénarios informatiques réels pour identifier les vulnérabilités de nos systèmes et de nos services.
- **Programme Bug Bounty** : programme facultatif conçu pour identifier les vulnérabilités de nos produits en demandant aux utilisateurs finaux de les tester. Les résultats des rapports sont publiés régulièrement.

Ce que fait Atlassian : répondre à vos besoins métier

Notre approche en matière de fiabilité et de disponibilité ne se limite pas à mettre en place les bonnes technologies. Nous avons établi des programmes et des politiques qui nous permettent de répondre à vos besoins métier et vous permettent de fonctionner conformément aux normes du secteur.

- **Continuité de l'activité** : capacité stratégique et tactique d'Atlassian à planifier les perturbations de l'activité et à y répondre afin de maintenir les opérations métier à un niveau d'activité acceptable et prédéfini.
- **Programme de reprise d'activité** : processus, politiques et technologies qui garantissent la récupération rapide des systèmes et services informatiques critiques en cas de panne. Lorsqu'une panne se produit, le RTO (délai de récupération maximal) et

le RPO (objectif de point de récupération) définissent le délai maximal que nous nous fixons pour rétablir les services.

- **Accords de niveau de service (SLA)** : pourcentages de disponibilité mensuelle garantis financièrement pour les expériences clés de Jira Software, Confluence et Jira Service Management avec les offres Cloud Premium et Enterprise.
- **Simulations de panne d'infrastructure** : les tests garantissent que nous sommes capables, en cas de panne de ZD, de rétablir la situation avec le temps d'arrêt le plus court possible.

Principaux avantages

Ce que fait Atlassian :

- La plateforme, les produits et les solutions Atlassian Cloud sont hébergés dans les régions AWS du monde entier avec plusieurs ZD qui fournissent un basculement et une haute disponibilité afin de faire face aux défaillances au niveau de l'infrastructure.
- Nous avons mis en place un programme qui fournit un autre mécanisme de sauvegarde des systèmes et des services internes.
- Nous disposons d'un programme de reprise d'activité bien établi qui nous permet de restaurer les systèmes et les services en cas de panne. Notre programme de continuité d'activité permet de faire face à des événements imprévus et fournit aux utilisateurs des produits fiables.
- Les tests d'intrusion externes, le programme Bug Bounty et la Red Team d'Atlassian nous permettent de confirmer notre résilience face aux menaces dynamiques.

Section 2 : protection, gestion et contrôle des données

Protéger vos données à grande échelle est un défi. Point final. À mesure que vous faites évoluer votre organisation, vous vous exposez à de plus en plus de risques, ce qui vous confine, vous et vos équipes de sécurité, dans une approche réactive. Bien qu'il soit possible de continuer à agrandir votre équipe, vous pouvez facilement vous sentir débordé.

L'avantage de l'utilisation du cloud est qu'une autre entreprise (Atlassian) est désormais à vos côtés pour veiller à la sécurité des systèmes et développer des fonctionnalités qui vous permettront de passer d'une approche réactive à une approche proactive. Pour ce faire, nous nous sommes concentrés sur la création de solutions qui intègrent directement les éléments suivants dans la couche de protection, de gestion et de contrôle des données de notre plateforme :

- **Restauration** : nous rétablissons la situation rapidement en cas de panne, empêchons les suppressions accidentelles et limitons les pertes de données afin que les équipes puissent reprendre leur travail dans les meilleures conditions.
- **Sécurité** : des contrôles au niveau de la plateforme appliquent une authentification et des autorisations strictes, le chiffrement et la prise en charge

de plusieurs régions, tout en permettant aux organisations d'ajouter et d'appliquer des contrôles supplémentaires à leurs données.
- **Confidentialité et conformité** : protégez les données personnelles et mettez en place les contrôles nécessaires pour respecter vos obligations réglementaires.
- **Gestion des identités et des accès** : réduisez le risque d'accès non autorisé aux données grâce à des contrôles architecturaux associés aux fonctionnalités des clients.

Récupération de données

Comme indiqué dans la section précédente, notre infrastructure nous permet de rétablir la situation en cas de défaillances au niveau de l'infrastructure. Néanmoins, d'autres types de pannes peuvent survenir et avoir un impact significatif sur votre activité, à la fois en termes de chiffre d'affaires et de perte de productivité des équipes.

Selon le rapport annuel de l'Uptime Institute, les erreurs humaines ont joué un rôle dans environ 60 à 80 % des pannes liées à un manque de personnel ou à un manque de formation. Il vous faut une solution pour limiter ce risque.

Ce que fait Atlassian : empêcher les suppressions accidentelles

Nous avons intégré des garde-fous à l'architecture cloud afin d'empêcher toute suppression accidentelle d'un produit et des données correspondantes. La suppression différée d'un produit agit comme un filet de sécurité. Ainsi, au lieu d'être entièrement supprimé, le produit est suspendu, et vous n'y avez plus accès, ou seulement de manière limitée, pendant un certain temps. Cela nous permet de rétablir rapidement le fonctionnement de vos produits afin de limiter l'impact sur vos équipes. À l'avenir, nous proposerons des fonctionnalités de suppression « en douceur » qui empêcheront certains types de suppressions et fourniront plusieurs couches de protection pour éviter les erreurs.

Ce que vous faites : permettre à votre organisation de réduire les pertes de données

Il est impératif d'effectuer vos propres sauvegardes régulièrement pour garantir :

- **la continuité de l'activité** : votre équipe informatique doit être en mesure de restaurer les données (projets Jira ou espaces Confluence, par exemple) en cas de suppression accidentelle ou d'annuler les changements apportés ;
- **la conformité aux réglementations** : les politiques ou les exigences réglementaires de votre organisation, que vous devez respecter, peuvent vous imposer d'effectuer vos propres sauvegardes de données pour être en conformité ;
- **la collecte de preuves historiques en cas de litige** : en cas de litige, les sauvegardes peuvent être utilisées pour montrer l'évolution de votre environnement.

Notre solution prête à l'emploi appelée « gestionnaire de sauvegardes » vous permet d'effectuer ces sauvegardes au format XML (exportation), que vous pouvez utiliser pour récupérer vos données (importation) dans votre environnement.

Outre le gestionnaire de sauvegardes, nous avons développé une plateforme qui permettra aux clients disposant de très grands ensembles de données d'exporter des données de manière plus rapide et plus fiable. En outre, nous développons de nouvelles fonctionnalités qui seront intégrées à l'administration Atlassian (admin.atlassian.com) et qui vous permettront de sauvegarder et de restaurer facilement toutes vos données chaque fois que vous en avez besoin. Dans le cadre de ce travail, nous avons récemment lancé une interface de ligne de commande qui vous permet de sauvegarder et de restaurer des données de manière plus précise et plus fiable que jamais !

Principaux avantages

Ce que fait Atlassian **:**

- Intégrer des dispositifs de protection à la plateforme Atlassian afin de limiter les risques de suppression accidentelle d'un produit.

Ce que vous faites :

- Utiliser le gestionnaire de sauvegardes ou l'interface de ligne de commande de sauvegarde pour récupérer vos données de manière fiable chaque fois que vous en avez besoin.

Sécurité des données

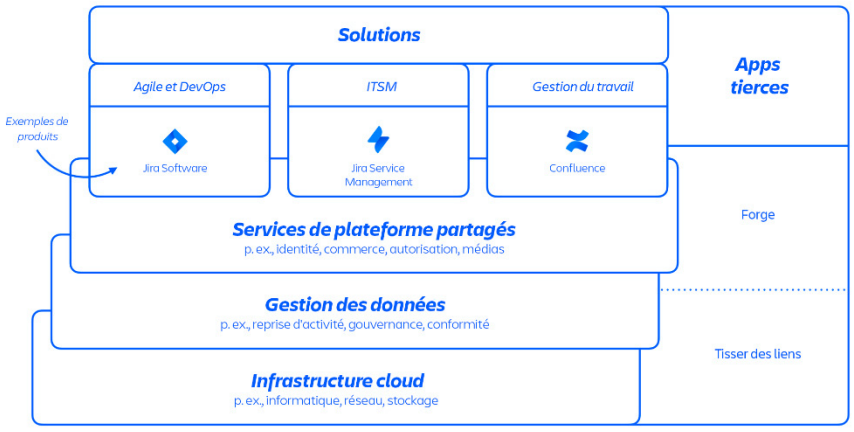
Le National Institute of Standards and Technology (NIST) définit la sécurité des données comme suit :

Le processus qui consiste à préserver la confidentialité, l'intégrité et la disponibilité des données d'une organisation conformément à sa stratégie en matière de risques. Les entreprises doivent mettre en place une architecture de sécurité et un plan de réponse avant qu'un incident ne se produise.

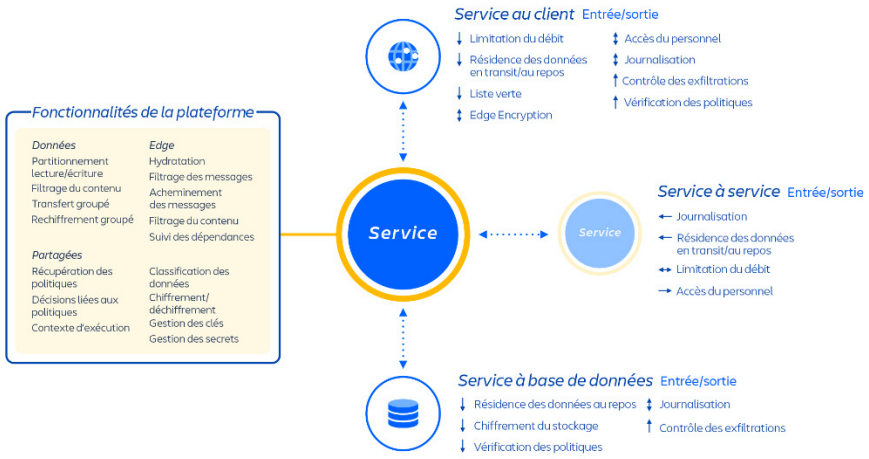
Ce que fait Atlassian : gérer un environnement multilocataire en toute sécurité

Grâce à l'architecture AWS, nous hébergeons plusieurs services de plateforme et de produits utilisés sur l'ensemble de nos solutions. Ces services incluent les fonctionnalités de la plateforme qui sont partagées et utilisées par plusieurs produits Atlassian (comme Media,

Identity et Commerce), des expériences comme notre éditeur, ainsi que des fonctionnalités spécifiques des produits, notamment le service Jira Issue et Confluence Analytics.
Les développeurs Atlassian fournissent ces services via une Platform as a Service (PaaS) développée en interne, appelée Micros, qui orchestre automatiquement le déploiement des services partagés, de l'infrastructure, des magasins de données et de leurs capacités de gestion, y compris les exigences de contrôle de la sécurité et de la conformité.

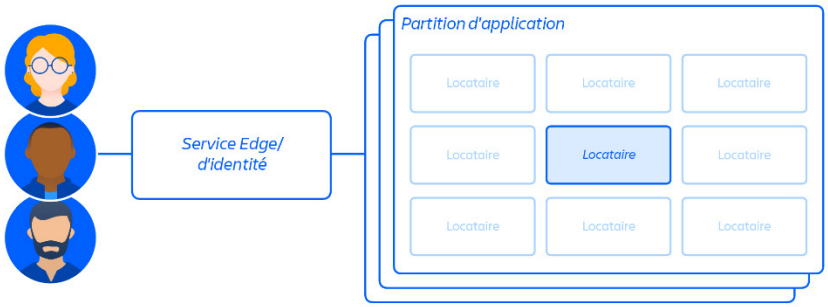


Les produits Atlassian se composent de plusieurs services conteneurisés déployés sur AWS à l'aide de Micros. Ils utilisent les fonctionnalités de base de la plateforme, notamment le réseau, le stockage de données, l'observabilité et l'analyse. Ces microservices sont conçus à l'aide de stacks techniques approuvées et standardisées au niveau de la plateforme.



En plus de cette infrastructure, nous avons créé une architecture de microservices multilocataire ainsi qu'une plateforme partagée qui prend en charge nos produits. Dans une architecture multilocataire, un seul et même service dessert plusieurs clients. Chaque partition

(généralement un conteneur) contient les données de plusieurs locataires, mais les données de chaque locataire sont isolées et inaccessibles aux autres locataires.



Ce que fait Atlassian : faire évoluer les services tout en maintenant l'isolement logique des données

Bien que nos clients partagent une infrastructure commune basée sur le cloud lorsqu'ils utilisent nos produits cloud, nous avons mis en place des mesures pour nous assurer qu'ils sont logiquement isolés afin que les actions d'un client ne puissent compromettre les données ou les services d'autres clients.

L'approche d'Atlassian varie selon les applications. Pour Jira et Confluence Cloud, nous utilisons un concept appelé « contexte de locataire » pour isoler logiquement nos clients. Ce concept est implémenté à la fois dans le code applicatif et géré par ce que nous appelons un « service de contexte de locataire » (Tenant Context Service, TCS). Celui-ci permet de garantir que :

- les données de chaque client sont logiquement isolées des données au repos des autres locataires ;
- toutes les demandes traitées par Jira ou Confluence offrent une vue propre au locataire afin que les autres locataires ne soient pas impactés.

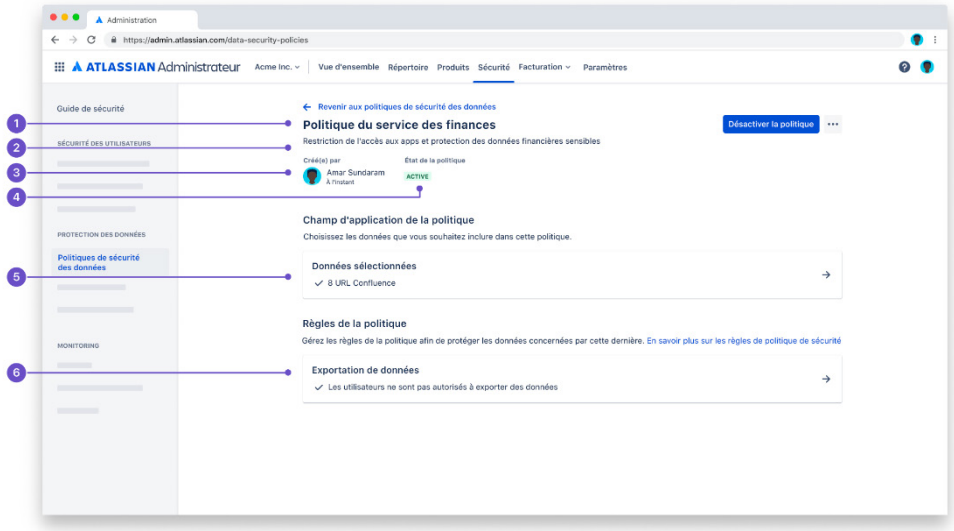
Dans les grandes lignes, le TCS stocke un contexte pour les différents locataires du client. Le contexte de chaque locataire est associé à un ID unique stocké de façon centrale par le TCS et inclut diverses métadonnées associées au locataire, comme les bases de données dans lesquelles le locataire se trouve, les licences dont il dispose, les fonctionnalités auxquelles il a accès et tout un éventail d'autres informations de configuration. Lorsqu'un client accède à Jira ou à Confluence Cloud, le TCS utilise l'identifiant du locataire pour rassembler ces métadonnées, qui sont ensuite associées à toutes les opérations effectuées par le locataire dans l'application tout au long de sa session.

Cela empêche les fuites de données entre locataires et tout autre problème, tel qu'une connexion à la mauvaise base de données, ce qui constitue une protection supplémentaire.

Ce que vous faites : implémenter la gouvernance du contenu

Nous veillons à ce que seules les personnes autorisées aient accès à vos données. Mais cela ne nous permet en aucun cas de contrôler la manière dont les utilisateurs, les applications et même les personnes extérieures à votre organisation interagissent avec votre contenu.

Nous proposerons prochainement des politiques de sécurité des données qui vous permettront d'appliquer une protection supplémentaire à vos données.



Au lieu de vous contenter d'accorder ou de supprimer des autorisations utilisateur, vous pouvez limiter les actions des utilisateurs. Par exemple, vous pouvez créer une politique pour l'un de vos sites qui interdit à vos équipes d'exporter des pages Confluence, afin de réduire le risque d'exfiltration de données ou d'autres pertes de données.

Vous pouvez définir le champ d'application de la politique, c'est-à-dire le périmètre des produits auxquels elle s'applique si vous disposez de plusieurs produits, ainsi que les règles, c'est-à-dire les contrôles de sécurité configurés dans le cadre de la politique. Pour plus d'informations, consultez notre documentation.

Protéger les données sensibles en limitant l'accès

Le chiffrement des données reste l'un des principaux mécanismes de protection des données sensibles. Il consiste à appliquer un texte chiffré autour de vos données afin que personne ne puisse les lire à moins de disposer de la clé de chiffrement.

Ce que fait Atlassian : chiffrer les données en transit et les données au repos

Concernant nos produits Cloud, Atlassian gère principalement le chiffrement dans le cadre du modèle de responsabilité partagée. Nous chiffrons vos données en transit à l'aide du protocole TLS 1.2+ avec Perfect Forward Secrecy (PFS) et vos données au repos à l'aide de l'algorithme AES-256. Nous utilisons le service AWS Key Management Service (KMS) pour gérer nos clés de chiffrement. Ainsi, seules les personnes disposant des rôles AWS et des autorisations valides peuvent accéder à ces clés et déchiffrer vos données.

Ce que vous faites : gérer les personnes autorisées à déchiffrer vos données

Votre organisation peut avoir besoin d'autres fonctionnalités de chiffrement que celles que nous proposons directement sur la plateforme Atlassian. Nous proposerons prochainement le chiffrement Bring Your Own Encryption (BYOK), qui vous permettra de générer et d'héberger des clés sur votre compte AWS via le service AWS Key Management Service (KMS). Pour rester informé, abonnez-vous à la feuille de route Cloud.

Respecter les exigences réglementaires en matière de résidence des données

Les organisations opèrent souvent dans plusieurs zones géographiques et ont besoin que leurs données soient stockées dans des lieux spécifiques afin de limiter les risques et de se protéger contre toute utilisation non autorisée de données personnelles. De par sa conception, AWS est disponible dans les régions du monde entier, ce qui nous permet d'étendre le nombre de sites sur lesquels les données de nos produits peuvent être hébergées.

Ce que vous faites : spécifier où vos données doivent résider

Par défaut, tous les produits sont hébergés sur le site mondial, qui inclut toutes nos régions AWS, mais nous proposons également la résidence des données, qui vous permet d'assigner les données concernées à un site précis. Nous proposons aujourd'hui la résidence des données aux États-Unis, en Asie-Pacifique (APAC), dans l'Union européenne (UE), en Allemagne et à Singapour. Pour mieux vous aider, nous continuons à proposer de nouvelles régions.

Comme indiqué dans la section Infrastructure, chaque région comprend plusieurs zones de disponibilité (ZD). En cas de panne de ZD dans la région à laquelle vous avez assigné vos données, vous basculerez sur une autre ZD de la même région afin de continuer à respecter vos obligations réglementaires. Nous ne proposons pas de basculement interrégional.

Dans certains cas, certaines exigences peuvent vous empêcher de stocker toutes vos données dans le cloud, mais vous souhaitez quand même permettre aux équipes, sans ces contraintes, de commencer à utiliser Atlassian Cloud. Les tunnels applicatifs constituent une passerelle sécurisée entre nos produits auto-gérés et les produits Cloud. Cela vous permet d'intégrer vos

produits Atlassian et de faire en sorte que des données et des fonctionnalités soient échangées entre eux en toute sécurité sans exposer votre réseau ni autoriser les connexions ou adresses IP entrantes.

Principaux avantages

- Ce que fait Atlassian :
  - Nous utilisons l'architecture AWS pour héberger plusieurs services de plateforme et de produits utilisés sur l'ensemble de nos solutions. Ces services sont fournis à l'aide d'un PaaS appelé Micros, qui orchestre leur déploiement. Les contrôles de sécurité et de conformité en font partie intégrante.
  - La plateforme, les produits et les solutions Atlassian utilisent une architecture de microservices multilocataire avec un isolement strict des locataires afin de rendre les données inaccessibles via le service de contexte de locataire (TCS). Chaque locataire possède un identifiant unique et des métadonnées pour se protéger contre les fuites entre locataires.
  - Nous chiffrons vos données en transit et au repos pour les protéger.
  - Nous élargissons le nombre de régions AWS prises en charge pour que vous puissiez respecter vos exigences réglementaires.
- Ce que vous faites :
  - Utiliser BYOK pour générer vos propres clés AWS et ainsi réduire le nombre de personnes susceptibles de déchiffrer vos données.
  - Utiliser des politiques de sécurité des données pour appliquer la gouvernance du contenu à vos données afin de renforcer la protection.
  - Activer la résidence des données pour héberger vos données dans des régions spécifiques afin de respecter vos exigences réglementaires.

Confidentialité et conformité

Confidentialité et conformité sont deux termes souvent utilisés de manière interchangeable.

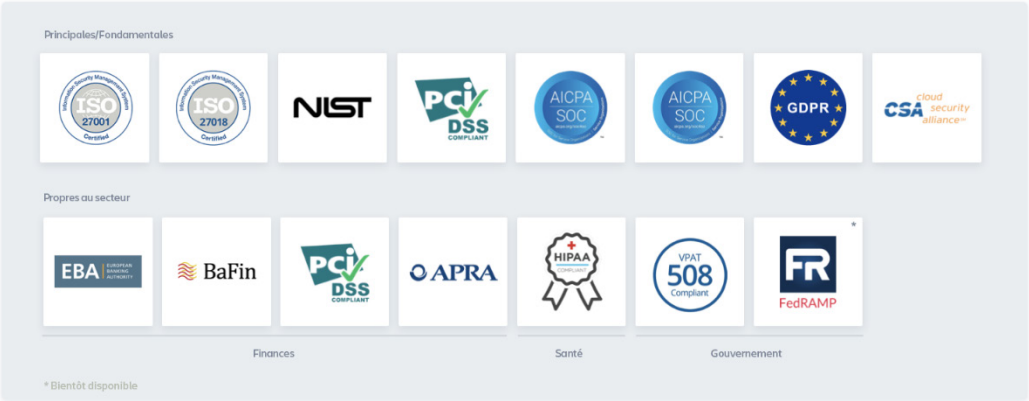
- **Confidentialité** : la confidentialité des données vise à garantir que les informations d'identification personnelle appartiennent à la personne, et que celle-ci a le droit de déterminer qui et quoi a accès à ses informations, quand et comment. Il incombe aux entreprises de respecter les exigences appropriées pour répondre à ces besoins.
- **Conformité :** la conformité désigne un ensemble de politiques, d'exigences réglementaires ou de lois qui décrivent les conditions qui doivent être remplies pour qu'un élément soit considéré comme sécurisé, fiable et privé.

En bref, la confidentialité met l'accent sur la protection des données personnelles, et la conformité est un plan qui explique sa mise en œuvre, en plus de fournir d'autres conditions de sécurité.

Ce que fait Atlassian : intégrer des contrôles réglementaires et de conformité à nos produits

Pour obtenir une certification ou une attestation de conformité, nous devons prouver que nous avons implémenté les nombreux contrôles décrits dans ces frameworks spécifiques. Les types de contrôles et la complexité de leur implémentation dépendent du secteur dans lequel ils sont implantés.

Nous prenons actuellement en charge les lois, certifications et frameworks suivants :



Chacune de nos certifications de conformité fait l'objet d'une validation indépendante par une tierce partie afin de garantir que nous répondons à toutes les exigences pertinentes.

Et l'avantage pour les organisations qui n'opèrent peut-être pas dans des secteurs fortement réglementés est qu'elles utilisent la même infrastructure avec ces contrôles avancés.

Ce que fait Atlassian : s'assurer que vos données restent privées

Il est crucial de préserver la confidentialité de vos données, et cela ne se limite pas à la mise en place de contrôles techniques. Nous nous concentrons également sur le développement de politiques et de programmes, notamment :

- Une politique de confidentialité
- Des politiques de gestion des données
- Des politiques de restriction d'accès aux données
- Un avenant sur le traitement des données

Ce que vous faites : gérer vos produits de manière conforme

Pour respecter vos obligations réglementaires, vous devez notamment utiliser vos produits de manière conforme. Nous proposons pour cela des fonctionnalités telles que la résidence des données et de la documentation. Par exemple, si vous devez respecter la loi HIPAA, nous avons créé un guide d'implémentation qui explique comment utiliser les produits Atlassian concernés conformément à cette loi.

Principaux avantages

- Ce que fait Atlassian :
  - Nous intégrons à notre infrastructure, à nos produits et à nos solutions des contrôles qui nous permettent de nous mettre en conformité sur différents frameworks, et nous nous soumettons chaque année à une validation indépendante par une tierce partie pour nous assurer de la conformité de notre fonctionnement.
  - Nous gérons notre programme de confidentialité conformément aux normes du secteur.
- Ce que vous faites :
  - Gérer vos données de manière conforme afin de respecter vos obligations réglementaires

Gestion des identités et des accès

Gartner définit la gestion des identités et des accès (IAM) comme suit :

Une discipline métier et de sécurité qui inclut de multiples technologies et processus métier visant à permettre aux bonnes personnes ou machines d'accéder aux bons actifs, au bon moment et pour les bonnes raisons, tout en évitant les accès non autorisés et les fraudes.

En bref, il s'agit de protéger vos données en veillant à ce que seuls les personnes, les appareils et les applications autorisés puissent y accéder. Malheureusement, les identifiants compromis restent l'une des principales causes de violations de données. C'est pourquoi nous avons adopté une approche partagée en matière d'IAM.

Ce que fait Atlassian : appliquer l'authentification et l'autorisation des services

Notre plateforme utilise un modèle de moindre privilège pour la gestion de l'accès aux données. Autrement dit, toutes les données ne sont accessibles qu'au seul service chargé de les enregistrer, de les traiter ou de les récupérer. Par exemple, les services multimédias, qui vous permettent de bénéficier d'une expérience cohérente de chargement et de téléchargement de fichiers sur l'ensemble de nos produits cloud, disposent d'un stockage dédié auquel aucun autre service Atlassian ne peut accéder. Tout service nécessitant un accès au contenu multimédia doit interagir avec l'API des services multimédias. Par conséquent, une authentification et une autorisation fortes au niveau de la couche de service imposent également une forte séparation des tâches et un accès aux données selon le principe du moindre privilège.

Nous utilisons des jetons web JSON (JWT) pour garantir l'autorité de signature en dehors des applications, afin que nos systèmes d'identité et le contexte du locataire soient la source de

référence. Les jetons ne peuvent être utilisés à d'autres fins que celles pour lesquelles ils sont autorisés. Lorsque vous ou un membre de votre équipe appelez un microservice ou une partition, les jetons sont transmis à votre système d'identité et validés par rapport à celui-ci. Ce processus garantit que le jeton est à jour et signé avant tout partage des données appropriées. Si l'on y ajoute l'autorisation et l'authentification requises pour accéder à ces microservices, leur périmètre est limité en cas de compromission d'un service.

Nous savons toutefois que les systèmes d'identité peuvent parfois être compromis. Pour limiter ce risque, nous utilisons deux mécanismes. Tout d'abord, le service de contexte de locataire (TCS) et les proxys d'identité sont hautement répliqués. Nous disposons d'un TCS supplémentaire pour presque tous les microservices et nous utilisons des proxys supplémentaires qui émanent de l'autorité d'identité, de sorte que des milliers de ces services sont en cours d'exécution à tout moment. En cas de comportement anormal de l'un ou de plusieurs d'entre eux, nous pouvons intervenir et résoudre le problème rapidement.

De plus, nous n'attendons pas que quelqu'un découvre une vulnérabilité dans nos produits ou notre plateforme. Nous identifions activement ces scénarios afin qu'ils vous impactent le moins possible, et nous exécutons un certain nombre de programmes de sécurité pour identifier et détecter les menaces de sécurité et pour y répondre.

Nous nous assurons que les demandes adressées à tous les microservices contiennent des métadonnées concernant le client (ou le locataire) qui demande l'accès. C'est ce que nous appelons le service de contexte de locataire (TCS). Il est directement renseigné à partir de nos systèmes de provisionnement. Lorsqu'une demande est initiée, le contexte est lu et internalisé dans le code de service en cours d'exécution, qui est utilisé pour autoriser l'utilisateur. Tous les accès au service (et donc aux données) dans Jira et Confluence nécessitent ce contexte de locataire, sinon la demande sera rejetée.

L'authentification et l'autorisation des services sont appliquées via le protocole Atlassian Service Authentication Protocol (ASAP). Une liste verte explicite détermine quels services peuvent communiquer, et des informations d'autorisation spécifient les commandes ainsi que les chemins disponibles. Cela limite tout mouvement latéral potentiel d'un service compromis.

L'authentification, l'autorisation et la sortie des services sont contrôlées par un ensemble de proxys dédiés. Ainsi, les vulnérabilités du code de l'application n'ont aucun impact sur ces contrôles. L'exécution de code arbitraire (RCE) nécessiterait de compromettre l'hôte sous-jacent et de contourner les limites du conteneur Docker, et non uniquement de pouvoir modifier la logique de l'application. Notre détection des intrusions au niveau de l'hôte signale plutôt les incohérences.

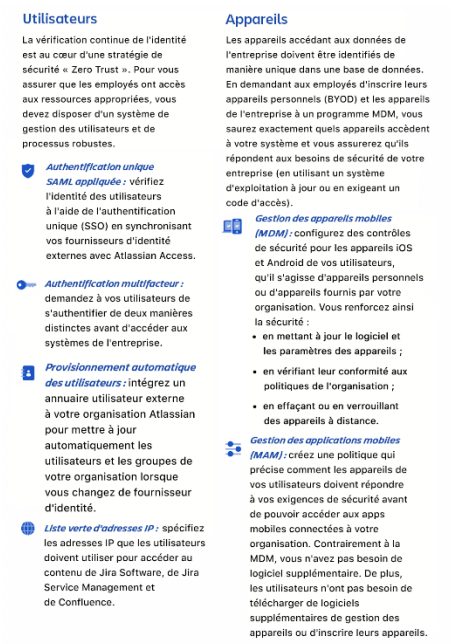
Ces proxys limitent le comportement de sortie en fonction du comportement prévu du service. Les services qui n'ont pas besoin d'émettre de webhooks ou de communiquer avec d'autres microservices ne sont pas autorisés à le faire.

Ce que vous faites : appliquer l'authentification et l'autorisation des utilisateurs et des appareils

Atlassian Access fournit aux administrateurs des fonctionnalités et des capacités IAM permettant d'appliquer la sécurité et la gouvernance à leurs utilisateurs et à leurs appareils depuis l'administration Atlassian, permettant ainsi l'implémentation d'une approche « Zero Trust ».

Utilisateurs La vérification continue de l'identité est au cœur d'une stratégie de sécurité « Zero Trust ». Pour vous assurer que les employés ont accès aux ressources appropriées, vous devez disposer d'un système de gestion des utilisateurs et de processus robustes.	• **Authentification unique SAML appliquée** : vérifiez l'identité des utilisateurs à l'aide de l'authentification unique (SSO) en synchronisant vos fournisseurs d'identité externes avec Atlassian Access. • **Authentification multifacteur** : demandez à vos utilisateurs de s'authentifier de deux manières distinctes avant d'accéder aux systèmes de l'entreprise. • **Provisionnement automatique des utilisateurs** : intégrez un annuaire utilisateur externe à votre organisation Atlassian pour mettre à jour automatiquement les utilisateurs et les groupes de votre organisation lorsque vous changez de fournisseur d'identité. • **Liste verte d'adresses IP** : spécifiez les adresses IP que les utilisateurs doivent utiliser pour accéder au contenu de Jira Software, de Jira Service Management et de Confluence. • **Sécurité des utilisateurs externes** : exigez des utilisateurs externes collaborant avec des membres de votre organisation qu'ils utilisent la validation en deux étapes ou qu'ils appliquent une fréquence de vérification (disponible prochainement).
Appareils Les appareils accédant aux données de l'entreprise doivent être identifiés de manière unique dans une base de données. Par exemple, en demandant aux employés	• **Gestion des appareils mobiles (MDM)** : configurez des contrôles de sécurité pour les appareils iOS et Android de vos utilisateurs, qu'il s'agisse d'appareils

d'inscrire leurs appareils personnels (BYOD) et les appareils de l'entreprise à un programme MDM, vous saurez exactement quels appareils accèdent à votre système et vous assurerez qu'ils répondent aux besoins de sécurité de votre entreprise (en utilisant un système d'exploitation à jour ou en exigeant un code d'accès).	personnels ou d'appareils fournis par votre organisation. Vous renforcez ainsi la sécurité : ○ en mettant à jour le logiciel et les paramètres des appareils ; ○ en vérifiant leur conformité aux politiques de l'organisation ; ○ en effaçant ou en verrouillant des appareils à distance. ● **Gestion des applications mobiles (MAM)** : créez une politique qui précise comment les appareils de vos utilisateurs doivent répondre à vos exigences de sécurité avant de pouvoir accéder aux applications mobiles connectées à votre organisation. Contrairement à la MDM, vous n'avez pas besoin de logiciel supplémentaire, et les utilisateurs n'ont pas besoin de télécharger d'autres logiciels de gestion des appareils ou d'inscrire leurs appareils.



Utilisateurs

La vérification continue de l'identité est au cœur d'une stratégie de sécurité « Zero Trust ». Pour vous assurer que les employés ont accès aux ressources appropriées, vous devez disposer d'un système de gestion des utilisateurs et de processus robustes.

- ***Authentification unique SAML appliquée :*** vérifiez l'identité des utilisateurs à l'aide de l'authentification unique (SSO) en synchronisant vos fournisseurs d'identité externes avec Atlassian Access.
- ***Authentification multifacteur :*** demandez à vos utilisateurs de s'authentifier de deux manières distinctes avant d'accéder aux systèmes de l'entreprise.
- ***Provisionnement automatique des utilisateurs :*** intégrez un annuaire utilisateur externe à votre organisation Atlassian pour mettre à jour automatiquement les utilisateurs et les groupes de votre organisation lorsque vous changez de fournisseur d'identité.
- ***Liste verte d'adresses IP :*** spécifiez les adresses IP que les utilisateurs doivent utiliser pour accéder au contenu de Jira Software, de Jira Service Management et de Confluence.

Appareils

Les appareils accédant aux données de l'entreprise doivent être identifiés de manière unique dans une base de données. En demandant aux employés d'inscrire leurs appareils personnels (BYOD) et les appareils de l'entreprise à un programme MDM, vous saurez exactement quels appareils accèdent à votre système et vous assurerez qu'ils répondent aux besoins de sécurité de votre entreprise (en utilisant un système d'exploitation à jour ou en exigeant un code d'accès).

- ***Gestion des appareils mobiles (MDM) :*** configurez des contrôles de sécurité pour les appareils iOS et Android de vos utilisateurs, qu'il s'agisse d'appareils personnels ou d'appareils fournis par votre organisation. Vous renforcez ainsi la sécurité :
  - en mettant à jour le logiciel et les paramètres des appareils ;
  - en vérifiant leur conformité aux politiques de l'organisation ;
  - en effaçant ou en verrouillant des appareils à distance.
- ***Gestion des applications mobiles (MAM) :*** créez une politique qui précise comment les appareils de vos utilisateurs doivent répondre à vos exigences de sécurité avant de pouvoir accéder aux apps mobiles connectées à votre organisation. Contrairement à la MDM, vous n'avez pas besoin de logiciel supplémentaire. De plus, les utilisateurs n'ont pas besoin de télécharger de logiciels supplémentaires de gestion des appareils ou d'inscrire leurs appareils.

Section 3 : administration centralisée

En tant qu'administrateur, vous devez avoir une vue d'ensemble de tous vos produits Atlassian. Dans des environnements auto-gérés, avoir cette vue d'ensemble est assez complexe. De par leur conception, les produits auto-gérés sont isolés les uns des autres afin de rendre les données inaccessibles à d'autres instances. Cependant, vous ne disposez pas des mécanismes nécessaires pour suivre ce qui se passe dans votre environnement. Dans le cloud, vous pouvez toujours isoler vos données, si nécessaire, mais vous bénéficiez d'une expérience d'administration centralisée qui vous aidera à gérer vos produits Atlassian et à avoir une visibilité accrue pour assurer la sécurité de vos données.

Cette expérience d'administration centralisée, Atlassian Administration, repose sur la plateforme Atlassian et a été optimisée avec les éléments suivants :

- **Surveillance et rapports** : maintenez votre niveau de sécurité et votre conformité grâce à des fonctionnalités de détection des menaces et d'audit.
- **Gestion du cycle de vie des produits et de l'organisation** : gérez vos produits et votre organisation pour répondre efficacement à vos exigences.

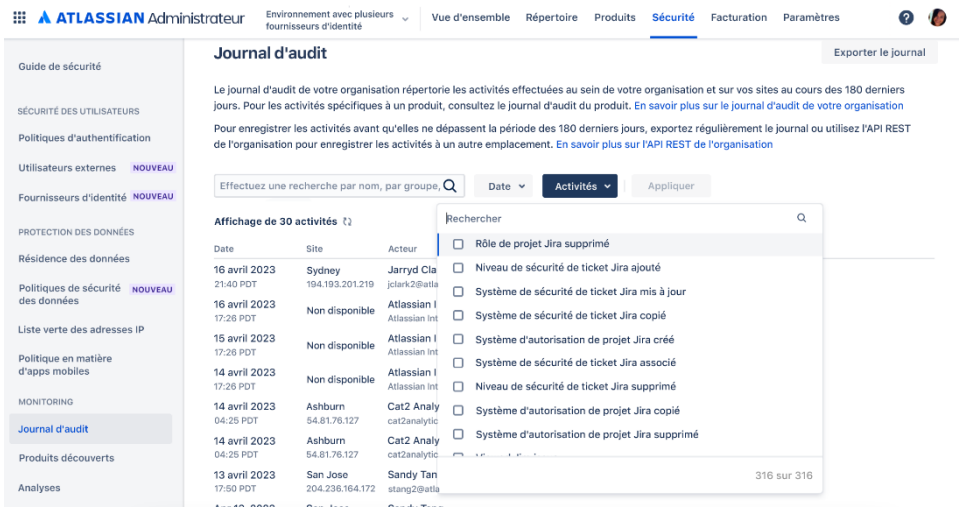
Surveillance et reporting

Obtenir de la visibilité sur votre instance peut apporter de nombreux avantages aux organisations à grande échelle, mais quelle que soit sa taille, chaque organisation peut tirer parti de l'utilisation d'outils de détection des menaces.

Les outils de détection des menaces surveillent votre réseau à la recherche d'activités malveillantes afin que votre équipe de sécurité puisse rapidement traiter le risque. La détection des menaces vous permet également de hiérarchiser les risques et d'obtenir des informations en temps réel pour réagir aux comportements suspects avant qu'ils ne deviennent un incident risqué et généralisé.

Ce que vous faites : suivre les événements qui se produisent dans votre instance

Les produits Cloud Standard et Premium contiennent des journaux d'audit qui vous permettent de suivre les principaux événements liés aux produits. Ils n'offrent toutefois pas de visibilité complète sur la sécurité de vos données sur l'ensemble de vos produits Atlassian regroupés au même endroit. Avec Atlassian Access, vous pouvez consulter les journaux d'audit de l'organisation, qui consignent des événements tels que les changements apportés à l'accès d'une personne à vos produits ou les modifications des accès administrateur. Contrairement aux journaux d'audit des produits qui dépendent de la quantité de stockage de votre offre, les journaux d'audit de l'organisation sont conservés pendant 180 jours pour vous apporter une garantie supplémentaire.



Et si votre organisation a besoin d'encore plus de granularité, avec Enterprise Cloud, vous pouvez choisir d'inclure les activités créées par les utilisateurs dans vos journaux d'audit. Cela vous permet de suivre les actions liées aux produits, à la fois pour les produits non gérés et pour les produits gérés de manière centralisée. Pour plus d'informations, consultez le billet dédié aux journaux d'audit sur la Communauté.

Ce que vous faites : surveiller les menaces

L'application de contrôles vous aidera à protéger vos données, et les utilisateurs réduiront le risque de violation de données. Néanmoins, l'élément le plus important dont vous avez besoin est la surveillance de votre environnement pour neutraliser les menaces avant qu'elles ne se transforment en incidents.

La détection des menaces renforce la surveillance de votre instance en vous permettant d'analyser rapidement les événements quotidiens et d'identifier ainsi toute activité malveillante.

L'un des nombreux avantages des solutions SaaS est qu'elles sont faciles à prendre en main. Malheureusement, cela permet également aux équipes de télécharger plus facilement de nouvelles versions de produits en dehors de la gouvernance de votre service informatique, ce qui constitue un autre point d'entrée de données potentiellement malveillantes. Grâce à la découverte automatique des produits, vous pouvez accéder facilement à ces informations depuis l'administration Atlassian et prendre des mesures immédiates.

La découverte automatique des produits effectue une analyse quotidienne pour identifier les instances créées par une personne dont l'adresse e-mail est associée au domaine de votre organisation. Un rapport vous est transmis chaque jour par e-mail. Grâce à l'administration Atlassian, vous savez qui a créé l'instance et combien d'utilisateurs l'utilisent. Vous pouvez ainsi décider si vous souhaitez que votre équipe informatique la prenne en main ou qu'elle travaille avec le propriétaire de l'instance pour l'intégrer à l'instance gérée par votre entreprise.

Vous pourrez bientôt adopter une approche basée sur le contenu pour définir la manière dont vos données peuvent être utilisées dans les produits Atlassian. Cette approche diffère d'une approche basée sur l'utilisateur, qui consiste à accorder ou à révoquer des autorisations spécifiques qui permettent à des utilisateurs ou à des applications d'effectuer certaines actions. Pour plus d'informations, consultez notre documentation.

Mais vous devez également savoir où sont stockées les données. En particulier dans les grandes entreprises, il peut être de plus en plus difficile pour les équipes de connaître les produits pris en charge par l'équipe informatique. Il n'est donc pas rare que des utilisateurs créent de nouvelles instances de produits pour travailler plus efficacement. Malheureusement, ces nouvelles instances peuvent vous exposer par inadvertance à une violation de données. Vous pourrez bientôt empêcher vos utilisateurs gérés de provisionner de nouveaux produits sans votre approbation et mettre en place un système de demandes de produit. Vous aurez non seulement un meilleur contrôle de la situation, mais également une meilleure visibilité sur vos utilisateurs.

Il est également important de savoir ce que font les utilisateurs dans vos produits Atlassian. Vous-même ou un membre de votre équipe êtes peut-être un expert en sécurité, mais ce n'est pas le cas de tout le monde, et cela peut vous exposer involontairement à des risques supplémentaires.

- **Informations sur l'organisation et l'administration** : suivez les utilisateurs actifs qui ont consulté une page, le nombre d'utilisateurs actifs et inactifs, et découvrez combien d'utilisateurs gérés sont soumis à la validation en deux étapes par rapport aux utilisateurs non gérés qui ont accès à vos produits.
- **Intégration CASB** : connectez-vous au logiciel CASB McAfee MVISION Cloud pour bénéficier d'une surveillance automatique de la sécurité et d'analyses comportementales via votre tableau de bord McAfee MVISION Cloud.

En outre, nous avons lancé Beacon, qui fournit encore plus de fonctionnalités de détection des menaces. Avec Beacon (actuellement en version bêta), vous pouvez :

- **Détecter** : recevez des alertes automatiques en cas d'activité inhabituelle sur vos produits Atlassian afin de détecter les menaces.
- **Enquêter** : collectez des informations détaillées qui vous permettront d'évaluer la crédibilité d'une menace.
- **Réagir** : maîtrisez les menaces grâce aux informations relatives aux alertes, au suivi de l'état et au transfert SIEM pour une gestion fluide des alertes.

Pour plus d'informations, contactez-nous.

Principaux avantages

- Les journaux d'audit fournissent des informations détaillées sur les événements qui surviennent au sein de votre instance. Si votre organisation effectue des enregistrements plus avancés, Cloud Enterprise suit également les activités générées

par les utilisateurs. Ces journaux d'audit peuvent être utilisés pour maintenir la sécurité de votre instance et prouver sa conformité.
- Utilisez la découverte automatique des produits pour rester informé lorsqu'un membre de votre organisation crée une nouvelle instance afin de maintenir votre niveau de sécurité.
- Vous pourrez bientôt empêcher les utilisateurs de créer une nouvelle instance en mettant en place un système de demandes de produit.
- Beacon est une fonctionnalité de détection intelligente des menaces conçue pour les produits Atlassian.

Gestion du cycle de vie des produits et de l'organisation

Les produits Atlassian Cloud sont associés à une organisation Atlassian. Cela vous permet de savoir quelles instances appartiennent à votre organisation. En particulier lorsque vous faites évoluer votre organisation, vous avez besoin de flexibilité pour répondre à vos exigences de sécurité.

Ce que vous faites : structurer vos données en fonction des exigences en matière de données

Lorsque vous développez votre activité, vous devez finalement prendre une décision, qui consiste à déterminer si la manière dont vous avez structuré vos produits Atlassian vous donnera la flexibilité nécessaire pour développer votre activité tout en maintenant le bon niveau de supervision. Les instances illimitées offrent cette flexibilité aux entreprises.

Voici quelques exemples courants de la manière dont des organisations comme la vôtre ont configuré des environnements multi-instances :

Gouvernance et services distincts	Donnez de l'autonomie à vos équipes en créant des sites pour chacune de vos unités opérationnelles (BU). Cela permet aux équipes de personnaliser leurs sites. Elles peuvent par exemple appliquer des workflows et des apps personnalisés sans impacter les autres équipes.
Développement à travers les acquisitions et la collaboration avec des parties prenantes externes	De nouvelles équipes peuvent rejoindre votre organisation par le biais de fusions ou d'acquisitions, et vous pouvez continuer à gérer ces équipes séparément. Vous pouvez donner à ces équipes leur propre site tout en les gérant de manière centralisée.

Propriété intellectuelle très sensible	Certaines de vos équipes ont accès à des données sensibles ou propriétaires. Vous pouvez créer des sites distincts pour ces équipes et en limiter l'accès afin de maintenir un niveau de sécurité approprié.
Isolement des données pour les équipes dispersées géographiquement	De nombreuses organisations ont des équipes dans le monde entier, ce qui leur permet de créer différents sites pour des zones géographiques spécifiques. Vous pouvez par exemple vouloir créer un site distinct pour aider vos équipes de la zone EMEA à respecter des exigences réglementaires strictes. Créez des sites distincts pour respecter vos exigences en matière de confidentialité des données. Par exemple, si certaines données doivent être stockées dans une région spécifique, vous pouvez créer un site distinct et y assigner les données concernées.

Consultez notre eBook pour en savoir plus sur les instances illimitées.

Principaux avantages

- Les instances illimitées permettent aux organisations de répondre à des cas d'usage complexes, tels que la protection des données très sensibles.
- Chaque instance peut être entièrement personnalisée via l'administration Atlassian pour répondre à vos spécifications sans affecter les autres instances associées à votre organisation. Par exemple, vous pouvez assigner les données de votre instance à différentes régions en fonction de vos obligations réglementaires.

Section 4 : Atlassian Marketplace

L'Atlassian Marketplace compte plus de 5 300 apps et intégrations, dont plus de la moitié étendent et personnalisent les produits Atlassian Cloud. Bien qu'Atlassian propose quelques apps sur le Marketplace, la majorité d'entre elles sont créées et gérées par des Marketplace Partners tiers

Sécurité des données du Marketplace

Atlassian s'efforce d'aider les Marketplace Partners à créer des apps Cloud sécurisées et fiables qui répondent à vos besoins en matière de conformité. Pour ce faire, nous mettons en place des exigences et des programmes de sécurité.

Ce que fait Atlassian : exigences en matière de sécurité et application

Les app du Marketplace étant créées et gérées par des partenaires tiers, l'approche d'Atlassian en matière de sécurité du Marketplace consiste à définir des exigences de sécurité et à prendre des mesures, comme expliqué plus en détail dans la section suivante. Plus précisément, notre approche comprend les éléments suivants :

- Exigences de sécurité clairement définies (et régulièrement mises à jour) pour les apps Cloud
- Analyse et signalement continus des exigences de sécurité manquantes ou des vulnérabilités
- Planification d'actions visant à protéger les clients si nécessaire

Exigences de sécurité d'Atlassian Cloud en matière d'apps

Alors que des directives sont établies afin d'améliorer la sécurité des apps Server et Data Center, chaque Marketplace Partner doit s'engager à respecter les exigences de sécurité définies par Atlassian lorsqu'il publie une app cloud sur le Marketplace. Ces exigences sont divisées en plusieurs catégories :

Authentification et autorisation	Les apps doivent authentifier et autoriser chaque demande sur tous les terminaux exposés.
Protection des données	Chaque fois qu'une app stocke des données des utilisateurs finaux* en dehors des systèmes Atlassian, elle doit prendre certaines mesures pour protéger ces données, notamment : • garantir le chiffrement complet du disque au repos ; • utiliser le protocole TLS 1.2 (ou version ultérieure) pour chiffrer l'ensemble du trafic et activer le HSTS avec une durée minimale d'un an ; • stocker et gérer les secrets en toute sécurité (jetons OAuth, sharedSecret, clés d'API, etc.).
Sécurité des apps	Les partenaires doivent prendre des mesures pour protéger les données de leurs clients contre les menaces de sécurité. Ces mesures comprennent : • la gestion et la configuration en toute sécurité des domaines sur lesquels l'app est hébergée ; • la validation et le nettoyage de toutes les données non fiables et le traitement de toutes les entrées des utilisateurs comme dangereuses afin de limiter les vulnérabilités liées aux entrées ;

	• le refus d'utiliser toute version de bibliothèque et de dépendance tierces présentant des vulnérabilités critiques ou graves connues.
Confidentialité	Les apps ne doivent en aucun cas collecter ni stocker les identifiants des utilisateurs Atlassian, comme les mots de passe ou les jetons d'API.
Gestion des vulnérabilités	Les partenaires doivent fournir les coordonnées de leur contact de sécurité et participer au programme de gestion des vulnérabilités d'Atlassian. Si Atlassian ou un chercheur en sécurité découvre un problème de sécurité dans une app, l'équipe de sécurité d'Atlassian doit pouvoir contacter le partenaire.
* Les données des utilisateurs finaux désignent toute donnée, tout contenu ou toute information concernant un utilisateur final auxquels vous ou votre app accédez, ou que vous collectez ou traitez dans le cadre de l'utilisation de l'Atlassian Marketplace.	

Ces exigences s'appliquent à toutes les apps Cloud conformément au contrat pour les Marketplace Partners d'Atlassian.

Analyses, tests et sensibilisation

Ce travail ne s'arrête pas une fois les apps créées et publiées sur le Marketplace. Afin de promouvoir la sécurité continue de toutes les apps Cloud, Atlassian a mis en place plusieurs stratégies pour identifier et gérer les problèmes et les vulnérabilités liés à la sécurité.

Ecoscanner

La plateforme Ecoscanner analyse quotidiennement l'ensemble des apps Cloud du Marketplace à la recherche de vulnérabilités et d'écarts par rapport aux exigences de sécurité.

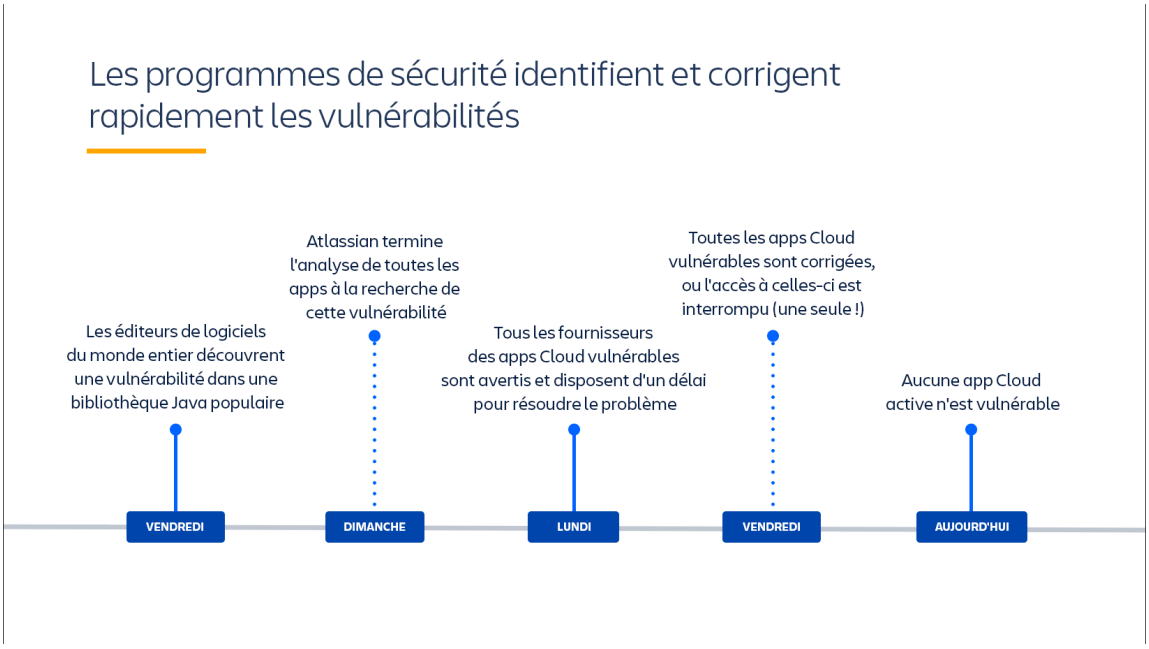
Dans le cadre de la plateforme Ecoscanner, Atlassian propose huit outils de vérification de conformité aux exigences clés, dont six sont disponibles sous forme d'outils open source que les partenaires peuvent utiliser pour analyser leurs apps et ainsi s'assurer en amont que les nouvelles versions respectent ces exigences.

Vous pouvez consulter la documentation d'Ecoscanner pour les développeurs ici pour en savoir plus sur les exigences spécifiques couvertes.

Outils d'analyse de vulnérabilités de logiciels tiers

Nous utilisons également des outils d'analyse pour identifier les vulnérabilités liées à des logiciels tiers. L'open source est puissant, et presque tous les développeurs du monde s'appuient sur des bibliothèques open source pour leurs apps. Mais ces bibliothèques

présentent parfois des vulnérabilités qui ont un impact sur un large éventail d'entreprises technologiques, mais aussi d'apps.



Nous analysons en continu les apps créées sur la plateforme Forge d'Atlassian pour détecter les vulnérabilités critiques ou graves de bibliothèques tierces.

En cas de vulnérabilité « Zero Day » ayant un impact significatif (par exemple, les récentes vulnérabilités découvertes dans log4j ou OpenSSL), Atlassian cherche à savoir si cette vulnérabilité peut être détectée dans toutes les apps Cloud du Marketplace, y compris celles qui ne sont pas basées sur notre plateforme Forge. Si possible, nous utilisons des outils d'analyse pour découvrir la vulnérabilité dans les apps du Marketplace, et nous travaillons avec des partenaires pour nous assurer qu'elle est corrigée rapidement. Si les vulnérabilités ne sont pas corrigées dans des délais raisonnables, nous prenons des mesures pour protéger nos clients.

Exemple : Apache Log4j

Pour citer un exemple, nos programmes, nos fonctionnalités d'analyse et nos mécanismes de reporting ont été mis à l'épreuve en décembre 2021 lorsque les vulnérabilités d'exécution de code arbitraire (RCE) dans Apache Log4j ont été rendues publiques. Atlassian a rapidement réagi en limitant la vulnérabilité pour tous les produits Atlassian Cloud.

De plus, l'équipe Atlassian chargée de la sécurité des apps a pu analyser l'ensemble de notre écosystème et identifier les apps vulnérables, signaler ces vulnérabilités et les corriger le plus rapidement possible en collaborant avec les développeurs respectifs. Après environ une semaine, Atlassian a pu confirmer qu'aucune app Cloud ne présentait de vulnérabilités

telles que celles de Log4j, et que toutes les apps Server/Data Center avaient reçu des correctifs ou avaient été retirées de notre Marketplace.

Signalement externe de bugs de sécurité

Outre nos exigences de sécurité et nos stratégies de découverte des vulnérabilités, les Marketplace Partners, les clients ou toute personne extérieure à Atlassian peuvent également signaler des problèmes de sécurité au niveau d'apps tierces via le projet Jira Atlassian Marketplace Security (AMS).

Les vulnérabilités, quel que soit le moyen par lequel elles sont détectées (notamment Bug Bounty, les outils d'analyse, les évaluations de sécurité et les rapports externes), sont transmises à AMS, puis suivies par l'équipe de sécurité d'Atlassian à des fins de remédiation.

*** Programme facultatif : Marketplace Bug Bounty**

Les partenaires peuvent adhérer au programme Marketplace Bug Bounty d'Atlassian, qui leur permet d'accéder à une communauté de chercheurs en cybersécurité qualifiés qui testent constamment leurs apps et signalent les vulnérabilités qu'ils découvrent.

Astuce : vous pouvez identifier les apps participant au programme Bug Bounty grâce aux badges Marketplace suivants :

- Le badge « Participant au programme Cloud Security », qui indique que l'app participe au programme Bug Bounty
- Le badge « Cloud Fortified », qui signifie que l'application participe au programme Bug Bounty et que des mesures supplémentaires ont été prises pour améliorer sa sécurité et sa fiabilité. Les apps Cloud Fortified offrent également un support aux clients 24 heures sur 24, 5 jours sur 7

  « En donnant la priorité à la sécurité et en participant activement à des initiatives telles que les programmes Bug Bounty et Cloud Fortified d'Atlassian, nous protégeons non seulement les précieuses données de nos utilisateurs, mais nous renforçons également la confiance et la crédibilité auprès de nos clients. Notre engagement en matière de sécurité est sans faille, et nous continuerons à travailler avec diligence pour fournir à nos utilisateurs les apps les plus sécurisées et les plus fiables possible. » — John Whittaker, vice-président de SmartBear, Platinum Marketplace Partner

Résolution des tickets liés à la sécurité

Les stratégies abordées jusqu'à présent sont en place pour aider Atlassian à identifier et à suivre les risques de sécurité potentiels sur le Marketplace. Mais bien entendu, la découverte des vulnérabilités n'est que le premier volet de la stratégie visant à protéger les clients grâce à des apps.

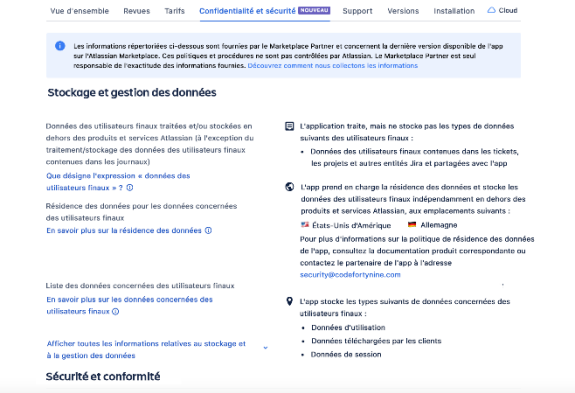
Si une vulnérabilité est découverte, toutes les apps sont soumises à la politique de correction des bugs de sécurité pour les apps du Marketplace, qui indique les dates limites pour la remédiation aux bugs liés à la sécurité découverts dans les apps du Marketplace. Lorsque nous découvrons qu'une app ne répond pas aux exigences de sécurité, nous en informons les Marketplace Partners et leur donnons un délai pour résoudre le problème. Si les apps ne respectent pas ces délais, Atlassian prendra les mesures qui s'imposent.

Pour les problèmes critiques ou les problèmes qui ne sont pas résolus passé un certain temps, Atlassian pourra notamment procéder au retrait des badges de sécurité et masquer l'app sur le Marketplace. Les apps qui enfreignent notre politique de correction des bugs de sécurité des apps du Marketplace sont répertoriées publiquement sur notre page dédiée à la transparence sur la sécurité des apps (en anglais). Dans les situations les plus graves, Atlassian pourra même suspendre une app afin de protéger les données client.

En bref, nous souhaitons transmettre aux Marketplace Partners un message clair : il est essentiel de garantir la sécurité de votre app. Si une app ne répond pas à nos exigences de sécurité, nous le découvrirons et nous prendrons les mesures qui s'imposent.

Ce que vous faites : faire preuve de vigilance et signaler tout problème

Atlassian a mis en place des processus pour soutenir ses partenaires. Mais vous avez également un rôle à jouer. Consultez les informations de confidentialité et de sécurité d'une app avant de l'installer. Ces informations sont accessibles via l'onglet Confidentialité et sécurité de l'app sur l'Atlassian Marketplace.



Sachez également que les apps qui enfreignent la politique de correction des bugs de sécurité pour les apps du Marketplace d'Atlassian seront répertoriées sur la page dédiée à la transparence sur la sécurité des apps (en anglais). Si l'une de vos apps figure sur cette page, contactez directement le Marketplace Partner pour mieux comprendre la nature de l'infraction.

Enfin, souvenez-vous que vous pouvez également tirer parti des systèmes de signalement de vulnérabilités d'Atlassian. Si vous constatez un problème dans une app, vous pouvez créer un ticket de type faille de sécurité dans AMS pour en informer Atlassian.

Principaux avantages

- Les Marketplace Partners acceptent les exigences de sécurité lorsqu'ils publient une app sur l'Atlassian Marketplace. Consultez la politique de confidentialité d'une app avant de l'installer.
- Atlassian effectue quotidiennement des analyses de sécurité personnalisées afin de s'assurer que toutes les apps Cloud répondent aux exigences de sécurité. Si des apps ne sont pas mises à jour dans les délais accordés pour respecter ces exigences, des mesures seront prises conformément à la politique de correction des bugs de sécurité pour les apps du Marketplace.
- Outre ces programmes, les partenaires peuvent adhérer à des programmes de sécurité plus avancés, tels que le programme Marketplace Bug Bounty pour la sécurité ou le programme Cloud Fortified pour la sécurité, la fiabilité et l'assistance.
- Les clients peuvent signaler des failles de sécurité dans des apps à Atlassian via la page dédiée à la transparence sur la sécurité des apps (en anglais), sur laquelle Atlassian répertorie les apps qui enfreignent la politique de correction des bugs de sécurité pour les apps du Marketplace.

Confidentialité sur le Marketplace

Ce que font Atlassian et ses partenaires : établir des obligations de confidentialité et les respecter

Outre le respect des exigences de sécurité, les apps sont tenues de fournir une politique de confidentialité qui informe les utilisateurs finaux sur :

- la manière dont un partenaire accède aux données des utilisateurs finaux, les collecte et les traite ;
- les personnes avec lesquelles une app ou un partenaire partage les données des utilisateurs finaux ; et
- le ou les pays dans lesquels les données des utilisateurs finaux seront stockées.

En dehors d'une politique de confidentialité, Atlassian demande également à ses partenaires de disposer de tous les droits et consentements, et de toutes les autorisations nécessaires de la part des utilisateurs finaux pour :

- l'accès ;
- la collecte ;
- le stockage ;
- la transmission ;
- le traitement ;

- l'utilisation ;
- la divulgation ;
- le partage ; et
- tout autre traitement

des données des utilisateurs finaux.

Ce que vous faites : vérifier les informations relatives à la confidentialité des apps

Consultez la politique de confidentialité de l'app pour en savoir plus sur la manière dont elle gère les données.

La politique de confidentialité d'une app est accessible depuis la page de l'app sur marketplace.atlassian.com. Faites défiler la page jusqu'à la section « En savoir plus ». Une rubrique « Confidentialité et sécurité » est accessible sur le côté droit. Un lien redirigeant vers la politique de confidentialité de l'app doit figurer sous la rubrique « Politique de confidentialité ». Vous pouvez également trouver ce lien dans l'onglet Confidentialité et sécurité de l'app en haut de la liste des apps, à côté de Support.

Sur la base de ces informations, vous pouvez déterminer qu'un accord de traitement des données (DPA) est nécessaire pour une app. Cet accord doit être conclu directement avec le partenaire. Un espace dédié dans la section Confidentialité de l'onglet Confidentialité et sécurité permet aux partenaires de fournir leur accord standard de traitement des données. Si cet accord ne répond pas à vos exigences (ou si le partenaire n'a fourni aucun accord), vous devrez peut-être contacter le partenaire directement.

Principaux avantages

- Les Marketplace Partners acceptent de partager publiquement leurs informations de confidentialité lorsqu'ils publient une app sur l'Atlassian Marketplace.
- Consultez la politique de confidentialité d'une app avant de l'installer.

Gestion des apps et des données

Les Marketplace Partners sont finalement responsables de la gestion de leurs activités et réaliseront des investissements stratégiques en fonction de la demande client. Au-delà des exigences d'Atlassian telles que définies dans la documentation pour les développeurs, les conditions d'utilisation pour les développeurs et le contrat pour les Marketplace Partners (en anglais), les partenaires choisissent comment créer leurs apps et les fonctionnalités qu'elles prennent en charge.

Atlassian s'efforce constamment de fournir de nouveaux outils et conseils afin que les Marketplace Partners puissent établir des priorités et créer les apps les plus sécurisées et les plus performantes possible.

Ce que font les partenaires : concevoir des apps sécurisées dès la conception

Par le biais d'une documentation, de ressources, de formations en direct et d'outils, Atlassian encourage ses partenaires à appliquer les principes de sécurité dès la conception lors de la création de leurs apps :

Accès selon le principe du moindre privilège

Les données auxquelles une app doit accéder varient selon sa fonction, mais en général, nous encourageons les partenaires à limiter l'accès aux seules informations nécessaires à son fonctionnement. Vous pouvez voir les données requises par une app en consultant la section Détails de l'intégration de la liste des apps ou en consultant l'onglet Confidentialité et sécurité de l'app.

En plus de partager ce principe avec nos partenaires, nous nous efforçons de permettre aux administrateurs de mieux contrôler les espaces ou les projets auxquels une app a accès, afin que vous puissiez limiter vous-même l'accès cette app à vos données. (Vous pouvez suivre notre avancement en ce sens dans la section Applications et extensibilité de la feuille de route Atlassian Cloud).

Réduction des sorties de données et utilisation de l'infrastructure Atlassian

Les apps avec des cas d'usage plus complexes peuvent avoir besoin de stocker ou de traiter certaines données en externe.

Les apps avec des cas d'usage plus simples, quant à elles, peuvent souvent limiter le volume de données qu'elles sont chargées de sécuriser et confient davantage à Atlassian la responsabilité de répondre aux besoins de sécurité et de conformité des clients.

Pour limiter le volume de données client quittant l'environnement d'Atlassian, les partenaires peuvent utiliser des options de stockage conçues par Atlassian pour leurs apps :

- **Stockage des données des utilisateurs finaux exclusivement dans Jira ou Confluence** : les apps dont les besoins de stockage sont réduits peuvent parfois stocker les données des utilisateurs finaux dans Jira ou Confluence, réduisant ainsi les efforts nécessaires pour sécuriser les données de manière indépendante.
- **Utilisation des fonctionnalités de stockage et de calcul gérées par Atlassian sur Forge** : les partenaires peuvent également choisir de développer des apps sur Forge, qui leur permet de stocker et de traiter des données exclusivement dans l'environnement d'Atlassian.

Pour en savoir plus sur les données des utilisateurs finaux qu'une app stocke et l'emplacement auquel elle les stocke, consultez la page de l'app sur l'Atlassian Marketplace. Depuis cette page, vous pourrez accéder à la politique de confidentialité et à la documentation de l'app, ainsi qu'à d'autres informations fournies par les partenaires.

Ce que font Atlassian et ses partenaires : récupérer les données d'app

Bien qu'Atlassian héberge une sauvegarde de l'ensemble des données stockées dans Jira, Confluence ou Forge, les Marketplace Partners sont responsables de leurs propres procédures de sauvegarde et de restauration de toutes les données stockées en dehors de l'infrastructure Atlassian.

Nous encourageons tous les Marketplace Partners à établir un plan. Contactez directement un partenaire si vous avez des questions concernant une app en particulier.

Principaux avantages

- Outre les exigences de sécurité et les obligations de confidentialité, Atlassian s'efforce constamment de fournir des outils et des conseils afin que les partenaires puissent implémenter les bonnes pratiques en matière de protection des données client.
- Pensez à consulter l'onglet Confidentialité et sécurité ainsi que la politique de confidentialité d'une app pour en savoir plus sur la façon dont elle gère les données.

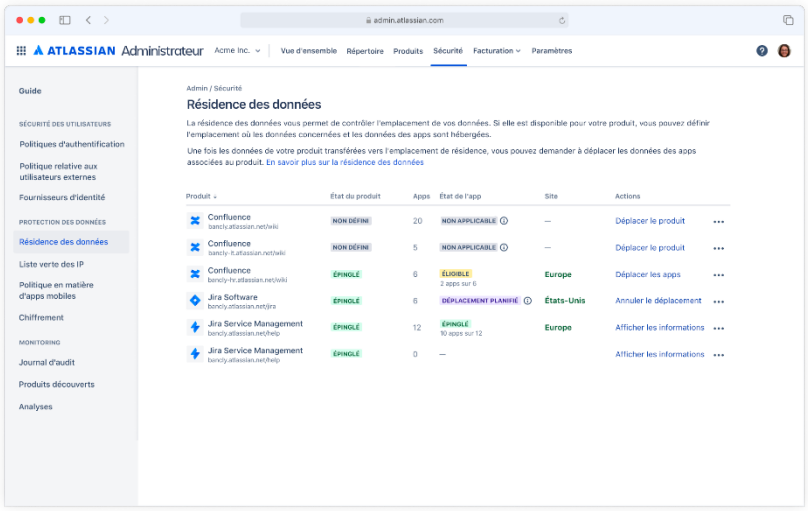
Conformité et apps du Marketplace

Si votre entreprise est soumise à des obligations légales ou à des exigences de conformité internes en matière de protection des données, il est important que les apps installées respectent également ces obligations. À cette fin, nous mettons à disposition de nos partenaires des formations et des outils pour soutenir leurs investissements dans des domaines que nous savons importants.

Ce que font Atlassian et ses partenaires : résidence des données

L'un des objectifs du partage des principes de la sécurité dès la conception est de limiter le nombre d'apps qui doivent prendre en charge la résidence des données de manière indépendante. Certaines apps stockent des données exclusivement dans le cadre des produits et services Atlassian. Ces apps ne comportant aucune donnée stockée en externe, les données concernées à votre sujet sont épinglées et suivent l'évolution régionale du produit sur lequel elles sont stockées.

Cependant, les apps qui ont besoin de stocker des données en externe doivent prendre en charge la résidence des données de manière indépendante. Les Marketplace Partners dont les apps stockent des données en dehors des systèmes Atlassian peuvent, dans la plupart des cas, investir dans l'épinglage des données dans certaines régions afin que les clients puissent répondre aux exigences de protection des données liées à la localisation ou au transport des données.
Bien que nous donnions notre propre définition des données concernées à titre d'exemple, il appartient aux partenaires de déterminer les données concernées par la gestion de la résidence des données en dehors de l'environnement Atlassian. Il est donc préférable de consulter la documentation de l'app via l'onglet Confidentialité et sécurité de la page de l'app, ou de contacter directement le partenaire pour en savoir plus. Les administrateurs de l'organisation et du site pour Jira et Confluence pourront également prochainement afficher et gérer le mode de résidence des données des apps installées dans l'administration Atlassian (admin.atlassian.com) grâce à une nouvelle expérience bêta.



Vérifiez l'éligibilité de votre app pour la résidence des données et planifiez les migrations de ses données sur admin.atlassian.com

Ce que font les partenaires : conformité légale

Conformément à l'accord qu'ils ont conclu avec Atlassian, les partenaires sont tenus de respecter des obligations légales dans les régions dans lesquelles ils opèrent. En outre, notre

équipe chargée de la confidentialité publie des ressources générales pour permettre aux partenaires de mieux comprendre leurs obligations légales dans certaines zones géographiques, notamment dans le cadre du RGPD.

Ce que font les partenaires : normes de conformité et certifications

La plupart des Marketplace Partners sont conscients des avantages associés au respect des normes de protection des données, et de nombreux partenaires ont investi ou investissent dans une certification.

> *Nous pensons que la protection des données des clients ne peut être que positive, purement et simplement. La sécurité guide nos décisions et la certification de notre conformité aux normes les plus élevées du secteur est une preuve de sérieux. — Julia Wester, cofondatrice de 55 Degrees et Platinum Marketplace Partner*

Pour aider les partenaires à définir leurs priorités et à mettre leur infrastructure en conformité, Atlassian fournit des suggestions et un support dans la mesure du possible.

Les partenaires qui choisissent d'utiliser le stockage hébergé par Atlassian via la plateforme Forge bénéficient des investissements d'Atlassian en matière de normes de conformité. Ces normes impliquent des efforts qui vont au-delà de l'infrastructure. C'est pourquoi la plateforme Forge d'Atlassian est conforme à la norme SOC2. Cela permet aux partenaires d'avoir une longueur d'avance pour l'obtention de la certification SOC2 lorsqu'ils s'appuient sur Forge.

Ce que vous faites : expliquer à vos partenaires ce que vous recherchez

Les partenaires réaliseront des investissements stratégiques en fonction de la demande qu'ils reçoivent de la part de clients tels que vous. Si vous êtes intéressé par une app ou si vous utilisez une app qui stocke des données de manière externe et que vous souhaitez qu'elle prenne en charge la résidence des données, informez-en le propriétaire. Des coordonnées figurent sur la page de l'app sur le Marketplace.

Principaux avantages

- Outre la définition des exigences de sécurité et des obligations en matière de confidentialité, Atlassian s'efforce constamment de fournir des outils et des conseils

afin que ses partenaires puissent répondre à vos besoins en matière de conformité.
- Consultez l'onglet Confidentialité et sécurité de la page de l'app et sa politique de confidentialité pour en savoir plus sur l'app et pour faire savoir aux partenaires que vous souhaitez qu'une app réponde à des exigences spécifiques.

Transparence et contrôle

Atlassian s'efforce de faciliter l'accès aux informations afin que vous puissiez prendre des décisions éclairées concernant les apps que vous installez dans votre environnement cloud, et pour vous permettre de mieux gérer les apps installées.

Ce que vous faites : vous assurer que les apps répondent à vos exigences avant de les installer

Vérifier les informations de confidentialité et de sécurité de l'app

Si vous êtes chargé de vous assurer que des apps répondent à vos exigences de sécurité, vous aurez besoin d'informations sur la manière dont ces apps traitent les données. De nombreux partenaires en sont conscients et s'engagent à fournir des informations qui vous aideront à évaluer leurs apps par rapport à vos exigences de sécurité.

> *Chez Appfire, nous croyons en la confiance, qui repose sur la transparence et la cohérence. Notre centre de confiance permet à nos clients d'évaluer très rapidement nos apps, car l'évaluation de sécurité peut être appliquée à toutes les apps Appfire. Notre objectif est d'apporter du confort et de renforcer la confiance afin que les clients puissent prendre leurs décisions d'achat facilement.* — Doug Kersten, directeur de la sécurité de l'information chez Appfire

Bien que de nombreux partenaires s'engagent à faire preuve de transparence, leur approche en matière de communication d'informations et de mise à disposition de ces informations à différents endroits en ligne peut varier. Par conséquent, il peut être difficile pour vous de trouver les informations dont vous avez besoin.

Consultez la page de l'app sur l'Atlassian Marketplace pour commencer votre évaluation de sécurité. Vous trouverez des informations clés fournies par les partenaires dans l'onglet Confidentialité et sécurité et dans la politique de confidentialité de l'app, ainsi que dans d'autres documents. Pour vous aider à trouver ces informations plus rapidement, nous continuons à travailler à la création d'espaces plus cohérents qui vous permettront d'en savoir plus sur la confidentialité et la sécurité d'une app.

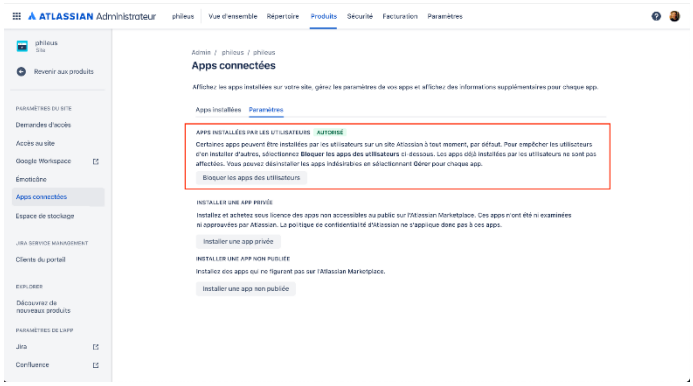
Vérifier les autorisations de l'app

Une fois que vous avez installé une app du Marketplace et que vous lui avez accordé certaines autorisations, nous ne pouvons plus empêcher l'app d'effectuer les actions autorisées, même si vous ne les approuvez pas. Nous vous recommandons de vérifier l'adéquation de l'app et de vous assurer du caractère raisonnable des autorisations demandées avant l'installation.

Ce que vous faites : gérer les apps de votre instance

Limiter les autorisations d'installation

L'installation de la grande majorité des apps Cloud est réservée aux administrateurs. Les utilisateurs finaux doivent envoyer une demande à leur administrateur s'ils souhaitent installer une app. Cependant, par défaut, les utilisateurs finaux peuvent installer et exécuter des apps OAuth 2.0 (3LO).

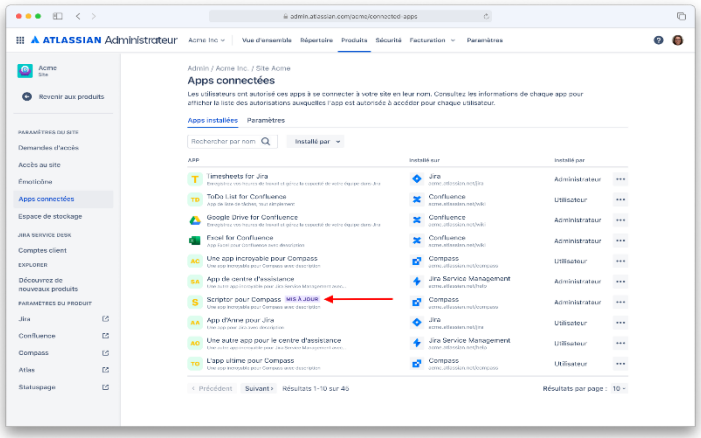


Pour mieux contrôler l'installation des apps, les administrateurs du site peuvent désactiver (ou réactiver) les fonctionnalités d'installation des apps OAuth 2.0 (3LO) pour les utilisateurs finaux via une option disponible sur admin.atlassian.com.

Bien entendu, autoriser les utilisateurs finaux à installer des apps qui les aident à travailler présente de nombreux avantages en termes de workflow. Si vous souhaitez laisser cette fonctionnalité active tout en gardant un œil sur les apps installées par les utilisateurs finaux, recherchez « Utilisateurs » dans la colonne « Installé par » et supprimez toutes les apps présentant un risque.

Rester informé des changements et maintenir les apps à jour

Les apps vérifient constamment leurs exigences de sécurité et ne cessent de renforcer leur sécurité, ce qui permet de rester à jour. Vous pouvez activer l'envoi d'alertes par e-mail sur la page d'une app sur marketplace.atlassian.com ou consulter la liste des apps installées sur admin.atlassian.com pour voir si des mises à jour sont disponibles pour ces apps.



Vérifier si des mises à jour sont disponibles pour vos apps sur admin.atlassian.com

Inscrivez-vous à « Watch App » sur marketplace.atlassian.com pour recevoir des alertes par e-mail lorsque de nouvelles versions sont disponibles

Principaux avantages

Lorsqu'il s'agit de protéger vos données lorsque vous utilisez des apps Cloud, n'oubliez pas qu'Atlassian, ses partenaires et ses clients ont tous un rôle à jouer. Atlassian continuera à :

- **améliorer le niveau de sécurité et de confidentialité sur l'ensemble de notre Marketplace Cloud** grâce à des exigences, à des formations et à des outils destinés aux partenaires ; et
- **vous apporter plus de transparence et de contrôle** pour que vous puissiez prendre des décisions éclairées lorsque vous achetez et gérez des apps.

Conclusion

La sécurité de vos données fait l'objet d'un partenariat partagé entre vous, Atlassian et vos Marketplace Partners, ou chacun assume une part de responsabilité. Cela passe par :

- l'hébergement de notre plateforme sur une infrastructure fiable et sécurisée, qui peut être rapidement rétablie en cas de panne ;
- l'intégration de contrôles de protection des données directement dans la plateforme et la fourniture de fonctionnalités avancées qui permettent aux organisations de répondre à leurs exigences métier ;
- la fourniture d'une expérience d'administration centralisée, qui permet aux administrateurs d'avoir une meilleure visibilité sur leurs produits Atlassian afin de les protéger contre des risques de sécurité ;
- la fourniture, à nos Marketplace Partners et à notre écosystème, des bons outils afin qu'ils puissent intégrer une sécurité des données robuste à leurs apps.

Pour en savoir plus sur notre approche en matière de protection des données, contactez-nous ou, si vous envisagez une migration vers le cloud, consultez notre page dédiée à l'Atlassian Migration Program pour obtenir des conseils sur la manière d'évaluer Atlassian Cloud.