

LIVRE BLANC

Gestion des données privées



SOMMAIRE

GESTION DES DONNÉES PRIVÉES	3
PRINCIPES	3
MISSION	3
GESTION DES DONNÉES PRIVÉES	4
Conditions préalables	4
SÉCURITÉ DES DONNÉES	5
Architecture	5
Exemple de flux	6
Gestion des données	7
Inventaire et classification	7
Données : retour, destruction et mise au rebut	7
Chiffrement en transit	8
Chiffrement au repos	8
Collecte de métadonnées	8
DÉPLOIEMENT	9
Séparation des tâches	9
Correctif	9
Gestion des vulnérabilités	9
Composants tiers	9
GESTION DES IDENTITÉS ET DES ACCÈS	10
Exigences	10
GESTION DES INFORMATIONS D'IDENTIFICATION	10
AUDIT	10



Gestion des données privées

Le document suivant fournit un aperçu des contrôles de sécurité, de l'architecture et des pratiques de gouvernance utilisés pour sécuriser un plan de données privé Alteryx Analytics Cloud Platform. Il s'agit d'un cluster de traitement des données que les clients peuvent exécuter sur leur propre infrastructure pour conserver les charges de travail de données sur leurs propres réseaux.

Principes

Alteryx rend l'analytique accessible à tous grâce à sa plateforme d'analytique cloud de pointe. Alteryx permet d'automatiser facilement et de bout en bout les processus d'ingénierie des données, d'analytique, de reporting, de machine learning et de Data Science afin de démocratiser l'analytique à grande échelle, pour de nombreux cas d'usage. Notre plateforme Alteryx Analytics Cloud s'appuie sur un programme de sécurité de l'information robuste et complet, basé sur une philosophie de défense approfondie et une approche sécurisée par défaut. Ce programme est conçu pour protéger notre plateforme et les données de nos clients contre les menaces potentielles, et pour garantir l'intégrité et la fiabilité de nos solutions. En déployant ces mesures de sécurité, nous aidons nos clients à garder l'esprit tranquille en utilisant une plateforme de confiance pour leurs besoins en matière d'analytique des données et pour accélérer leur transformation digitale.

En faisant appel à des experts de la sécurité de l'information, d'Internet, des réseaux et des applications, Alteryx démontre son engagement pour la protection continue de ses systèmes de défense, la garantie de processus d'examen de la sécurité cohérents, la sécurisation de son infrastructure et le respect de nos politiques de sécurité. La sécurité est intégrée à nos produits et opérations.

Nous pensons que lorsque des produits conçus dans des environnements sécurisés contribuent à bâtir un monde plus sûr pour travailler, et nos clients bénéficient directement de ces protections. La sécurité et la protection des données font partie de nos principaux critères de conception.

Mission

Chez Alteryx, nous veillons à appliquer les normes de sécurité et de transparence les plus strictes. Nous nous engageons à garder une longueur d'avance en matière de sécurité dans un contexte en constante évolution, et à déployer les normes et meilleures pratiques les plus à jour pour protéger les données de nos clients. Nos mesures de sécurité exhaustives sont conçues pour empêcher la destruction accidentelle ou illégale, la perte, l'altération, la divulgation non autorisée ou l'accès non autorisé aux données.

Ce livre blanc présente nos pratiques de sécurité sur la plateforme Alteryx Analytics Cloud lorsqu'elle est configurée pour le traitement des données privées et démontre notre engagement à garantir l'intégrité et la fiabilité de nos produits, de notre environnement et de nos données. Pour plus d'informations sur nos programmes globaux de sécurité et de confidentialité, rendez-vous sur alteryx.com/fr/trust. Nous avons hâte de travailler avec vous et de vous aider à atteindre vos objectifs métier tout en garantissant la protection de vos données.

Gestion des données privées

La gestion des données privées s'applique à l'ensemble de l'architecture d'Alteryx Analytics Cloud Platform, qui offre une plus grande flexibilité en matière de traitement et de stockage des données. En d'autres termes, les parties de la plateforme qui gèrent les données internes du client sont déployées de manière à donner au client un contrôle total sur l'emplacement de stockage et de traitement de ses données. Nous tirons parti des meilleures pratiques du secteur pour mettre en place des contrôles de sécurité complets et approfondis afin de vous donner confiance et de respecter les obligations de conformité.

Pour ce faire, nous créons plusieurs plans, que nous appelons le plan de contrôle, ou la partie de l'architecture qui réside dans l'infrastructure d'Alteryx, et le plan de données, qui réside dans votre infrastructure cloud. Le plan de contrôle est responsable des interactions de l'interface utilisateur, des capacités de déploiement, de la surveillance, du stockage des métadonnées des applications et de la communication. Le plan de données est chargé d'établir des connexions aux sources de données, de traiter les données et de stocker les jeux de données téléchargés ainsi que les échantillons de données au repos.

Les moteurs d'exécution SQL ou de stockage de données tiers tels que Snowflake, Databricks ou BigQuery sont classés dans le plan de données (où le contenu client est stocké et traité), mais ce n'est pas le sujet principal de ce document.

Conditions préalables

La prise en charge du déploiement de l'infrastructure du plan de données nécessite la création d'un compte cloud avec un VPC (Virtual Private Cloud) dans la région de votre choix. Une connectivité est également requise entre l'infrastructure du plan de données et tout autre environnement nécessaire au traitement de tous les cas d'usage des charges de travail. Il est possible de déployer l'infrastructure du plan de données dans un environnement Amazon Web Services (AWS).



Sécurité des données

Alteryx a pris soin de garantir la sécurité et l'intégrité des données, quel que soit leur emplacement ou leur lieu de transmission dans l'infrastructure de la plateforme Alteryx Analytics Cloud. Alteryx classe les données en deux catégories principales : le contenu client et les métadonnées des applications. Le contenu client appartient à celui-ci et désigne les données qui sont fusionnées, transformées, analysées ou traitées. Les métadonnées des applications sont les données qu'Alteryx utilise pour traiter correctement le contenu client selon ses instructions.

Architecture

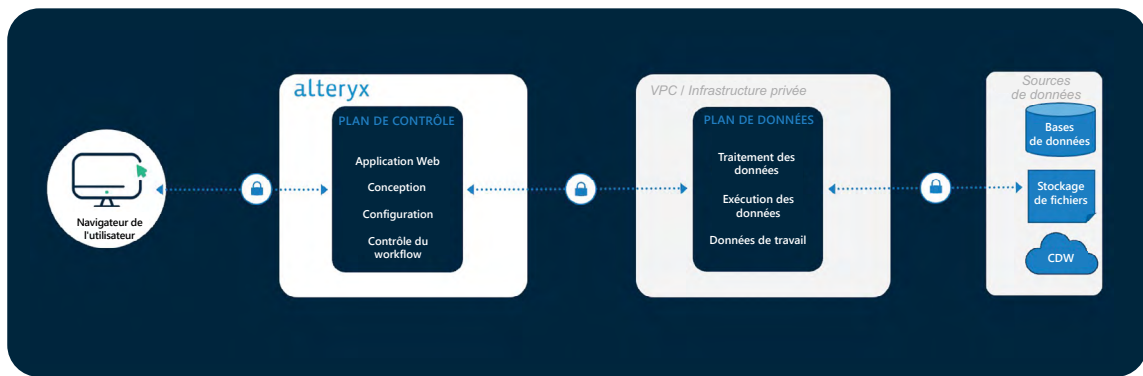
La séparation du plan de données de l'environnement Alteryx et des autres environnements client permet d'empêcher l'amalgame des données et prévient toute fuite entre les locataires.

Cette approche de la conception du réseau sépare le plan de contrôle, qui est responsable des décisions de routage et de transfert, du plan de données, qui est responsable du transfert des paquets de données. Cette séparation contribue à améliorer la sécurité du réseau en isolant le plan de contrôle des attaques externes et en empêchant les cybercriminels d'accéder aux informations de routage sensibles. En outre, ce type d'architecture permet d'utiliser différents contrôles et mesures de sécurité sur les plans de contrôle et de données, ce qui renforce encore la sécurité.

Les flux de communication dans le système sont séparés, de sorte que les messages relatifs au contrôle sont dirigés vers l'infrastructure de gestion des données privées, et que les messages de retour contiennent uniquement des métadonnées sur les actions demandées et des échantillons de données à des fins d'affichage. Les échantillons de données ne sont ni mis en cache ni stockés de manière centralisée. La communication réseau sur réseau public est chiffrée avec le protocole TLS 1.3 ou version ultérieure. C'est également vrai pour la connexion entre le plan de données privé et la source de données si la communication est prise en charge par la source de données.



*Tout au long de ce document, le terme « données » désigne le contenu client, sauf indication contraire.

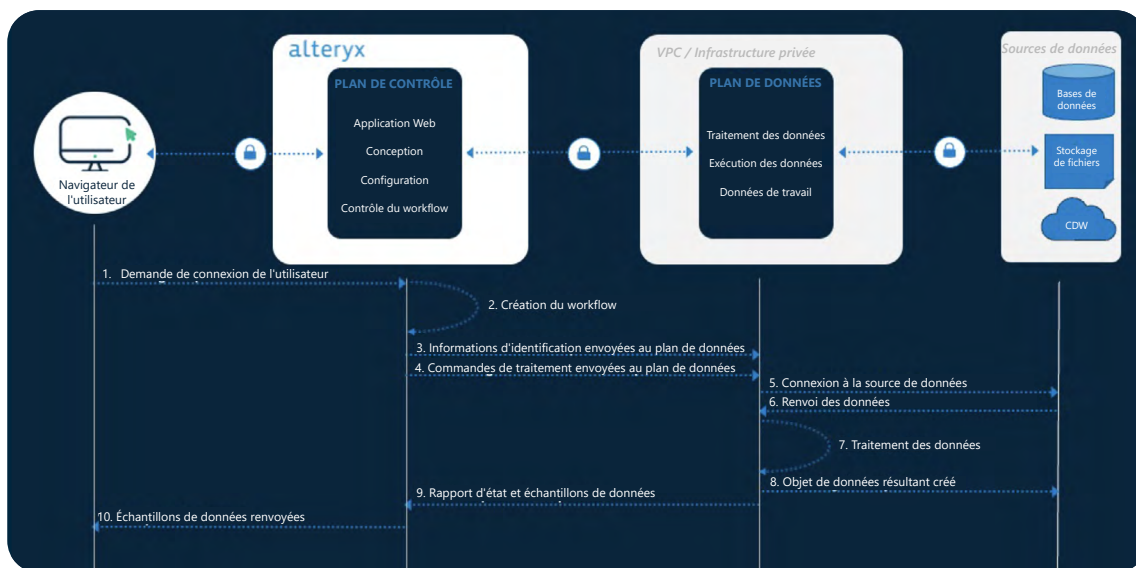


Exemple de flux

Supposons que vous soyez ingénieur de données et que vous souhaitiez récupérer des enregistrements d'une base de données sur le cloud, normaliser les données dans un jeu de données et stocker les enregistrements résultants dans un compartiment S3.

Dans cet exemple, on suppose qu'un espace de travail est configuré avec une intégration d'authentification unique, qu'un plan de données a été déployé dans votre environnement et que la configuration des informations d'identification de base de données et des rôles IAM nécessaires a déjà été effectuée.

1. Le flux commence lorsque vous vous connectez au portail Alteryx à l'aide de votre fournisseur d'identité pour l'authentification unique. Il est également possible d'utiliser l'authentification native dans les cas où aucun fournisseur d'identité externe n'est disponible.
2. Vous utilisez ensuite une connexion de base de données configurée dans le cadre de votre workflow et créez une transformation des données résultantes à stocker dans un compartiment S3 configuré.
3. Les informations d'identification configurées pour la base de données sont chiffrées par enveloppe et envoyées au plan de données pour qu'il se connecte à la source de données.
4. Les commandes de traitement basées sur la conception du workflow sont également envoyées au plan de données.
5. Le plan de données déchiffre les informations d'identification à l'aide de clés stockées en tant que secrets (également à l'aide du chiffrement d'enveloppe) et lance la connexion pour interroger les données.
6. Les résultats des données sont envoyés au plan de données pour traitement.
7. Le plan de données privé traite les données en fonction du workflow.
8. Le plan de données privé utilise ensuite les informations d'identification IAM récupérées avec un rôle IAM pour créer un objet dans le compartiment S3 avec les données résultantes.
9. Le plan de données renvoie l'état et les échantillons de données au plan de contrôle.
10. Les échantillons de données sont ensuite retransmis à votre navigateur.



Gestion des données

Chez Alteryx, nous avons mis en œuvre un ensemble de règles et de pratiques standard pour l'inventaire, la classification, la conservation et le stockage des données qui s'appliquent à notre architecture globale Analytics Cloud Platform et au déploiement d'environnements de traitement des données privées. Cela permet de garantir que les données sont facilement accessibles et peuvent être récupérées rapidement lorsque cela est nécessaire, et de les protéger contre tout accès non autorisé ou toute altération. Notre engagement en faveur de la normalisation nous permet d'offrir à nos clients une expérience cohérente et fiable lors de l'utilisation de nos environnements Analytics Cloud Platform et de garantir que leurs données sont correctement protégées et gérées.

Inventaire et classification

Des règles concernant le balisage approprié des données collectées en fonction de leur niveau de sensibilité sont en place pour garantir que les données sont correctement suivies et conservées.

Données : retour, destruction et mise au rebut

Chez Alteryx, nous avons mis en œuvre un ensemble complet de règles et de procédures pour la mise au rebut de biens matériels et incorporels, y compris des données. Ces règles sont conçues pour garantir que les données sont suivies, examinées, conservées et mises au rebut conformément à leur sensibilité et aux périodes de conservation définies. Cela signifie que les données ne sont conservées que pendant la période requise par les obligations légales et contractuelles applicables, après quoi elles sont mises au rebut de façon sécurisée. En suivant ces règles, nous pouvons garantir que le contenu des clients est correctement géré et protégé tout au long de son cycle de vie. Cela permet de préserver la sécurité et l'intégrité des données, et d'éviter les violations potentielles ou les accès non autorisés. Notre engagement en faveur de la mise au rebut sécurisée des données aide nos clients à garder l'esprit tranquille, avec l'assurance que leurs données sont traitées de manière responsable et sécurisée.

Chiffrement en transit

Pour garantir la sécurité des données en transit dans les systèmes Alteryx, y compris l'infrastructure de traitement des données privées déployée dans l'environnement du client, nous utilisons TLS (Transport Layer Security) version 1.3 ou ultérieure.

Ce protocole de chiffrement permet d'empêcher tout accès non autorisé aux données lorsqu'elles sont transmises entre différents composants du système. En outre, la communication entre le plan de contrôle et le plan de données et la communication entre clusters sont toutes deux chiffrées pour une protection renforcée du contenu client. Ces mesures garantissent la sécurité des données lorsqu'elles sont transmises dans le système Alteryx et préviennent les vulnérabilités ou les violations potentielles. Avec le déploiement du chiffrement en transit, nos clients restent sereins, avec l'assurance que leurs données sont protégées et sécurisées.

Chiffrement au repos

Les données stockées dans un espace de travail sont chiffrées au repos par défaut à l'aide de chiffrements par blocs AES (Advanced Encryption Standard) 256 bits et de services cloud natifs pour la gestion des clés, la gestion des versions et la rotation.

- Les secrets du cluster de plans de données sont chiffrés à l'aide d'un chiffrement par enveloppe distinct de celui des charges de travail prises en charge par les clés gérées par le client.
- Les clients peuvent utiliser des compartiments de stockage et des bases de données chiffrés comme sources de données.

Les sources de données client en dehors de l'espace de travail respectent la règle de

chiffrement sous-jacente pour cette source de données. Par exemple, si un client se connecte à un compartiment S3 en tant que source de données externe, tous les fichiers qu'il contient suivront la règle définie par le client.

Collecte de métadonnées

Un ensemble de données dédié à la surveillance des applications est collecté à partir de l'environnement de traitement des données privées pour surveiller et maintenir la stabilité opérationnelle du système. Ces métadonnées sont un petit échantillon des données globales du workflow. Elles sont soigneusement regroupées, masquées, puis utilisées pour fournir des insights précieux sur les performances du système. Cela permet de s'assurer que l'environnement de traitement des données privées fonctionne correctement et efficacement, et permet une identification et une résolution proactives des problématiques ou goulots d'étranglement potentiels.

En surveillant et en analysant régulièrement les métadonnées, Alteryx garantit la stabilité et la fiabilité des environnements de ses clients, tout en nous permettant de prendre des décisions éclairées sur la façon d'optimiser et d'améliorer leurs performances.

Alteryx collecte également un ensemble de données d'utilisation de l'application via le navigateur sur les interactions des utilisateurs finaux avec l'application. Tout comme les données de surveillance, ces données d'utilisation sont également regroupées et masquées. Alteryx analyse ces métadonnées pour mieux comprendre la façon dont les utilisateurs finaux interagissent avec l'application, l'utilisation des fonctionnalités et les opportunités d'amélioration de l'expérience de l'utilisateur final.

Déploiement

Séparation des tâches

Alteryx crée l'infrastructure nécessaire pour exécuter la gestion du plan de données au sein du compte cloud d'un client. Aucune infrastructure existante, telle que le réseau et le stockage, n'est modifiée au cours de ce processus. Toute l'infrastructure nécessaire créée au cours du déploiement complète toute infrastructure existante et aucune modification n'est apportée aux règles de gouvernance dans l'environnement.

Correctif

Les clusters du plan de données sont régulièrement mis à jour avec des images corrigées en fonction de la sécurité. L'application de correctifs sur les composants du plan de données s'effectue à l'aide d'un flux de distribution continu, qui garantit que les mises à jour sont déployées rapidement et de manière transparente sur le système. Ce processus commence lorsque des mises à jour sont envoyées aux référentiels Alteryx qui contiennent des images ayant subi des tests et des vérifications approfondis. Lorsqu'une nouvelle mise à jour est disponible, elle déclenche un déploiement vers le plan de données privé, qui installe la mise à jour et garantit que le plan de données reste à jour et sécurisé. Ce flux de distribution continu permet d'appliquer des correctifs efficaces au plan de données, d'éviter les failles de sécurité, et de préserver la stabilité et la fiabilité du système. En mettant en œuvre ce processus, Alteryx s'assure que le plan de données est toujours à jour et protégé contre les menaces potentielles.

Gestion des vulnérabilités

Les images de charge de travail déployées utilisent les mêmes pratiques sécurisées de cycle de vie de développement logiciel (SDLC) que celles que nous utilisons dans toute l'entreprise. Les conteneurs commencent avec des images de base renforcées et sont analysés pour détecter toute vulnérabilité potentielle.

Pour plus d'informations sur nos pratiques SDLC ou notre programme de sécurité, rendez-vous sur alteryx.com/fr/trust.

Chez Alteryx, la surveillance inclut l'analyse statique, dynamique, de la composition logicielle, du code d'infrastructure et de la vulnérabilité des images.

L'application de correctifs de sécurité aux images de charge de travail est déterminée par l'importance de toutes les vulnérabilités potentielles qui peuvent exister, et le processus suit la politique de vulnérabilité d'Alteryx. En général, les images sont envoyées à l'aide de mises à jour continues au sein du cluster.

Les services cloud utilisés dans le plan de données privé sont corrigés en fonction des planifications définies par AWS.

Composants tiers

La section suivante décrit les images de charges de travail tierces utilisées pour les opérations dans le plan de données. Les images utilisées par le fournisseur sont toujours corrigées avec les dernières mises à jour de sécurité.

COMPOSANT	UTILISATION
ArgoCD	Gestion des charges de travail des clusters
DataDog	Relaie les mesures et la télémétrie du cluster
Teleport	Connexions à distance pour l'assistance

Gestion des identités et des accès

Exigences

La plateforme Alteryx Analytics Cloud s'intègre avec AWS IAM avec un modèle de moindre privilège pour que les services et les utilisateurs obtiennent l'accès approprié. Un compte IAM (Identity and Access Management) et un rôle associé doté de l'ensemble d'autorisations requis doivent être fournis à Alteryx par le client pour prendre en charge le déploiement initial.

Ce compte et ce rôle sont utilisés à des fins de déploiement initial et pour toute modification requise de l'infrastructure du plan de données nécessaire à Alteryx. Des scripts de configuration sont disponibles pour la création automatique des autorisations nécessaires.

Gestion des informations d'identification

Les connexions à différents systèmes pour la création de jeux de données sont initiées uniquement par le plan de données. Les informations d'identification sont stockées à l'aide du chiffrement par enveloppe. Une clé de chiffrement des données (DEK) est utilisée pour chiffrer les informations d'identification, tandis qu'une clé de chiffrement (KEK) est utilisée pour chiffrer la clé. Ce chiffrement est utilisé à la fois pour le stockage et pendant le transit.

Le plan de données s'intègre aux services de gestion des identités et des accès natifs dans le cloud pour utiliser les rôles d'accès aux données sans avoir à stocker les informations d'identification dans l'environnement.

Audit

Comme le plan de données s'exécute dans votre environnement, la gouvernance et la configuration de la journalisation que vous avez appliquée sont elles aussi appliquées au plan de données. Les événements qui se produisent, tels que les modifications de l'infrastructure et l'accès au compte, sont consignés et consultables en fonction de votre stratégie de journalisation.





alteryx

L'analytique pour tous les employés, systèmes et décisions. Accélérez votre parcours d'analytique avec la plateforme Alteryx Analytics Cloud.

C'est parti

La plateforme Alteryx Analytics Cloud vous permet de résoudre vos problématiques métier les plus complexes grâce à l'analytique puissante et facile à utiliser sur une même plateforme. Partagez rapidement vos workflows dans le cloud, en local et sur site. Obtenez rapidement des insights grâce à l'analytique cloud native, accessible dans votre navigateur. Découvrez des intégrations fluides et prêtes à l'emploi avec les applications modernes de l'écosystème cloud. Utilisez la plateforme Alteryx Analytics Cloud pour faire émerger des signaux cachés et vous concentrer sur ce qui compte grâce aux insights automatisés basés sur l'IA, et changez la donne grâce aux recommandations intégrées et aux meilleures pratiques de la Communauté Alteryx.

alteryx.com/fr