La sécurité et la confidentialité des données chez Workday

Introduction

Face à la digitalisation croissante de l'entreprise, la sécurité et la protection des données des clients et collaborateurs et de la propriété intellectuelle constituent la priorité n°1 des responsables informatiques. Compte tenu des menaces de plus en plus sophistiquées qui pèsent sur la sécurité des entreprises, il est par ailleurs essentiel de garantir une sécurité et une confidentialité des données optimales dans tous les aspects de service. Voici donc une présentation des pratiques de Workday en matière de sécurité et de confidentialité des données à l'intention des responsables informatiques.

Conformité réglementaire et certifications

Workday et ses clients doivent respecter un certain nombre de réglementations internationales sur la protection de la vie privée. Les principes communs à l'ensemble des pays concernés portent sur la notification, le choix, l'accès, l'utilisation, la divulgation et la sécurité des données. Notre application est conçue pour vous permettre de réaliser des configurations adaptées, conformément à la législation spécifique de votre pays.

Par ailleurs, Workday assure le respect des réglementations internationales sur la protection de la vie privée à travers la mise en œuvre d'un programme complet de sécurité de l'information sous forme écrite, qui prévoit des mesures techniques et organisationnelles visant à protéger les données des clients contre tout accès et toute utilisation ou divulgation non autorisés.

Audits externes : rapports SOC 1 et SOC 2

Les opérations, les règles et les procédures de Workday sont régulièrement auditées afin de s'assurer que les normes attendues des fournisseurs de services sont bien respectées, voire dépassées, par l'entreprise. Workday publie un rapport SOC 1 (Service Organization Controls 1) de Type II. Remplaçant le rapport SAS 70, ce rapport est établi conformément aux normes SSAE 18 (Statement on Standards for Attestation Engagements No. 18) et ISAE 3402 (International Standard on Assurance Engagements No. 3402).

Grâce à ce rapport qui s'appuie sur deux normes, les entreprises du monde entier ont la garantie que les fournisseurs de services comme Workday ont mis en place les contrôles appropriés. Ce rapport s'adresse aux clients ou prospects qui doivent comprendre quels contrôles internes ont été effectués sur les activités stratégiques externalisées ayant un impact sur leurs états financiers (conformité à la loi Sarbanes-Oxley). Le champ d'application du rapport SOC 1 est limité aux systèmes de production de Workday et l'audit SOC 1 est réalisé tous les six mois par un auditeur tiers indépendant. Le rapport est mis à la disposition des clients et prospects dès sa parution.

Workday publie également un rapport SOC 2 (Service Organization Controls 2) de Type II. Le rapport SOC 2 de Workday porte sur l'ensemble des principes et critères des services de confiance (sécurité, disponibilité, confidentialité, intégrité du traitement et vie privée). Son champ d'application couvre tout système Workday contenant des données ayant été soumises par le client à Workday Services. Ce rapport s'adresse aux clients ou prospects qui souhaitent comprendre le fonctionnement des contrôles de sécurité internes de Workday. L'audit SOC 2 est réalisé une fois par an par un auditeur tiers indépendant et mis à la disposition des clients et prospects dès sa parution.

Les audits SOC 1 et SOC 2 valident les dispositifs de protection physiques et environnementaux de Workday applicables aux data centers de production, aux procédures de sauvegarde et de reprise, aux processus de développement logiciel et aux contrôles de sécurité logiques.

Certifications ISO 27001, 27017 et 27018

La norme ISO 27001 est une norme de sécurité de l'information initialement publiée en 2005 par l'Organisation internationale de normalisation (ISO) et la Commission électrotechnique internationale (CEI). La norme ISO 27001:2013 a été publiée en septembre 2013 et remplace la norme initiale de 2005. La norme ISO 27001 est une approche de la sécurité standardisée et mondialement reconnue qui spécifie les exigences relatives à un système de management de la sécurité de l'information (SMSI) dans le contexte d'une organisation.

La norme ISO 27017, publiée en 2015, est une norme complémentaire à la norme ISO 27001. Elle prévoit des contrôles et donne des conseils de mise en œuvre pour la sécurité de l'information qui s'appliquent à la fourniture et à l'utilisation de services Cloud.

La norme ISO 27018 est une norme complémentaire publiée par l'ISO/CEI en 2014. Elle contient les directives applicables aux fournisseurs de services Cloud qui traitent des données personnelles.

Workday est certifié ISO 27001 depuis septembre 2010, ISO 27018 depuis octobre 2015 et ISO 27017 depuis novembre 2017. La certification est obtenue après évaluation de la conformité de Workday à la norme ISO concernée par un organisme indépendant. La certification ISO est renouvelée tous les 3 ans mais pour la conserver, l'entreprise doit faire l'objet d'audits de surveillance annuels. Ces certifications ISO témoignent de notre engagement envers la confidentialité et la sécurité des données et démontrent l'efficacité de nos contrôles. Les certificats ISO et la Déclaration d'Applicabilité du SMSI sont librement consultables par nos clients sur notre site Web.

Transferts de données transfrontaliers

Des lois strictes sur la protection des données régissent le transfert de données personnelles de l'Espace économique européen (EEE) vers les Etats-Unis. Afin de répondre à ces exigences pour nos clients exerçant leurs activités dans l'EEE, nous avons intégré les clauses contractuelles types approuvées par la Commission européenne, également appelées « Contrat type », dans notre Accord de protection des données. Ce Contrat type crée un mécanisme contractuel visant à garantir le niveau de protection adéquat requis pour autoriser le transfert de données personnelles de l'EEE vers un pays tiers.

Workday est également autocertifié pour le bouclier de protection des données (Privacy Shield) UE-Etats-Unis et le bouclier de protection des données Suisse-Etats-Unis. Le bouclier de protection des données remplace le régime de la sphère de sécurité (Safe Harbor Framework) et vise à répondre spécifiquement aux problèmes identifiés par la Cour de justice de l'Union européenne dans sa décision invalidant le régime de la sphère de sécurité. Workday est enregistré comme participant « actif » au bouclier de protection des données. TRUSTe est la méthode de vérification par un tiers utilisée par Workday dans le cadre du bouclier de protection des données.

Pour en savoir plus sur le programme Privacy Shield du Département du Commerce américain, rendez-vous sur http://www.privacyshield.gov. Pour en savoir plus sur les Clauses contractuelles types, rendez-vous sur https://ec.europa.eu/info/law/law-topic/data-protection_fr.

Pour plus d'informations sur l'engagement de Workday envers la protection des données de nos clients et sur notre programme de protection des données, consultez la fiche « Workday's Robust Privacy Program ».

Règlement général sur la protection des données

Le Règlement général sur la protection des données (RGPD) est une réglementation de l'Union européenne (UE) qui abroge et remplace la directive 95/46/CE sur la protection des données ainsi que la législation de mise en œuvre des Etats membres. Entré en vigueur dans les 28 Etats membres de l'UE le 25 mai 2018, ce règlement simplifie et harmonise la législation existante sur la protection des données dans tous les Etats membres de l'UE. Le RGPD s'applique aux entreprises établies sur le territoire de l'Union européenne ainsi qu'à toutes les entreprises, quel que soit leur lieu d'établissement, qui traitent ou conservent les données à caractère personnel de citoyens de l'UE.

Workday est un sous-traitant au sens du RGPD. Après avoir étudié en détail les exigences du RGPD, Workday a mis en œuvre de nombreuses procédures de confidentialité et de sécurité afin de garantir le respect du RGPD en tant que sous-traitant dès l'entrée en vigueur du règlement. Ces procédures prévoient :

- La formation des collaborateurs aux procédures de sécurité et de confidentialité des données
- La réalisation d'analyses d'impact relatives à la protection des données
- La mise à la disposition de nos clients de méthodes de transfert de données suffisantes
- La tenue de registres pour les activités de traitement
- La mise à la disposition de nos clients de dispositifs de protection des données et de conformité configurables

Les concepts de Privacy by design et de protection des données par défaut sont profondément ancrés dans les Services Workday. Pleinement conscient de l'importance stratégique du RGPD pour nos clients internationaux, Workday suit en permanence les nouvelles directives publiées par les autorités de contrôle de l'UE concernant le RGPD afin de s'assurer que notre programme de conformité reste à jour.

Sécurité des données

Sécurité physique

Les systèmes de production de Workday sont hébergés dans des data centers de pointe conçus pour accueillir les systèmes informatiques sensibles avec des sous-systèmes redondants et dans des zones de sécurité compartimentées. Les data centers de Workday appliquent les mesures de sécurité physique les plus strictes :

- Plusieurs niveaux d'authentification sont requis avant d'obtenir l'accès à la zone des serveurs
- Les zones sensibles nécessitent une authentification biométrique en 2 facteurs
- Des systèmes de vidéo-surveillance sont installés aux points d'entrée internes et externes les plus critiques
- Du personnel de sécurité assure la surveillance des data centers 24 h/24, 7 j/7
- Les tentatives d'accès non autorisées sont consignées et surveillées par les équipes de sécurité du data center

Tous les accès physiques aux data centers sont extrêmement limités et strictement réglementés. L'exploitation des données par Workday respecte les meilleures pratiques en matière de sécurité, notamment grâce à des serveurs protégés par un accès limité et des fenêtres de maintenance programmées régulièrement.

Ségrégation des données

Workday est une application SaaS (Software as a Service) multi-tenant.

L'architecture multi-tenant est une fonctionnalité majeure de Workday qui permet à plusieurs clients de partager une même instance physique du système Workday tout en isolant les données applicatives de chaque client. Workday utilise pour cela son serveur de gestion des objets, Workday Object Management Server (OMS). Chaque code utilisateur est associé à un seul client (tenant) qui lui-même accède à l'application Workday.

Toutes les instances des objets d'application (par exemple une organisation ou un collaborateur) sont propres à un client, de sorte que chaque fois qu'un nouvel objet est créé, il est irrévocablement lié au client. Le système Workday gère automatiquement ces liens et limite l'accès à chaque objet, d'après le code utilisateur et le client. Lorsqu'un utilisateur demande des données, le système applique automatiquement un filtre pour garantir qu'il ne récupère que les informations correspondant au client.

Chiffrement des données stockées (sécurité de la base de données)

Workday chiffre tous les attributs des données client dans l'application avant de les stocker dans la base de données. C'est l'une des caractéristiques fondamentales de la conception technologique de Workday. Workday s'appuie sur l'algorithme AES (Advanced Encryption Standard) avec une clé de 256 bits. Le système Workday peut effectuer ce chiffrement car il s'appuie sur une application « in-memory » orientée objet et non pas sur une application SGBDR basée sur des disques. Les métadonnées Workday sont interprétées par l'OMS Workday et stockées en mémoire. Toutes les insertions, mises à jour et suppressions de données sont enregistrées dans un espace persistant au sein d'une base de données MySQL. Grâce à cette architecture unique, Workday n'a besoin que de quelques dizaines de tables de base de données. A l'inverse, une application basée sur une SGBDR nécessite des dizaines de milliers de tables, ce qui rend impossible le chiffrement de toute la base de données car l'impact sur la performance serait trop dommageable.

Chiffrement des données en transit (sécurité réseau)

Les utilisateurs accèdent à Workday via Internet. Cet accès est protégé par le protocole TLS (Transport Layer Security). Le trafic est ainsi protégé contre les indiscrétions, le piratage ou la falsification des messages.

Workday a également mis en place des procédures de sécurité proactives comme la défense du périmètre et les systèmes de prévention des intrusions sur le réseau. Des évaluations de la vulnérabilité et des tests de pénétration de l'infrastructure du réseau Workday sont également effectués régulièrement, à la fois par des ressources internes Workday et des fournisseurs tiers.

Sauvegarde des données

La base de données de production principale de Workday est dupliquée en temps réel vers une base de données secondaire gérée dans un data center hors site. Une sauvegarde complète est réalisée chaque jour à partir de cette base de données secondaire. Conformément à la politique de Workday en matière de bases de données, des sauvegardes des bases de données sont réalisées et les transactions sont consignées dans un journal afin de pouvoir restaurer une base de données en limitant le taux de perte des transactions validées à un niveau commercialement acceptable. Un journal de transactions est conservé jusqu'à ce que 2 sauvegardes des données soient réalisées après la dernière entrée dans le journal de transactions. Les sauvegardes des bases de données de systèmes qui implémentent des interfaces doivent être disponibles aussi longtemps que nécessaire pour le bon fonctionnement des systèmes d'interfaçage. Cette période est variable selon les systèmes. Les sauvegardes des bases de données et les journaux de transactions sont chiffrés pour toutes les bases de données contenant des données client.

Reprise après sinistre

Workday garantit la conformité de ses services avec son contrat de niveau de service standard (SLA). Le contrat de niveau de service inclut un Plan de reprise après sinistre du service de production Workday qui prévoit une durée maximale d'interruption admissible de 12 heures et une perte de données maximale admissible d'une heure. La durée maximale d'interruption admissible correspond à la durée maximale pouvant s'écouler entre l'interruption du service de production Workday et la reprise du service. La perte de données maximale admissible correspond à la quantité de données pouvant être perdues suite à l'interruption du service de production Workday, exprimée sous la forme d'une durée avant la panne.

Pour s'assurer que le contrat de niveau de service est respecté, Workday tient à jour un environnement de reprise après sinistre avec duplication complète de l'environnement de production. Dans le cas d'une interruption imprévue, si l'estimation de la durée de l'interruption est supérieure à une durée prédéfinie, Workday exécute son Plan de reprise après sinistre. Le Plan de reprise après sinistre est testé au minimum tous les 6 mois.

Un seul modèle de sécurité

A la différence des systèmes ERP traditionnels, Workday applique un seul modèle de sécurité. Il s'applique à l'accès utilisateur, à l'intégration système, au reporting, aux appareils mobiles et à l'accès des équipes IT. Tous les utilisateurs doivent se connecter et s'identifier via le modèle de sécurité Workday. Ce n'est pas le cas des systèmes ERP traditionnels, qui incluent généralement une couche de sécurité au niveau applicatif que les équipes IT et les administrateurs de base de données peuvent contourner pour accéder aux données directement au niveau de la base de données. Avec Workday, ce n'est pas possible. Workday est un système « in-memory » orienté objet doté d'un entrepôt de données persistant et chiffré. Par conséquent, tous les événements et toutes les modifications d'accès sont suivis et audités. Ce modèle de sécurité d'une fiabilité inédite, combiné à la capacité de dater et d'auditer automatiquement toutes les mises à jour de données, permet de réduire le temps et les coûts associés à la gouvernance et la mise en conformité et, de façon générale, de limiter les risques liés à la sécurité.

Authentification

La sécurité Workday est gérée par rôles. Elle prend en charge le protocole SAML d'authentification unique et l'authentification par certificat X.509 pour les utilisateurs et les intégrations de services Web. Workday permet à ses clients de configurer des exigences d'authentification différentes en fonction des catégories d'utilisateurs.

Dans les cas où les entreprises souhaiteraient proposer plusieurs types d'authentification à leurs collaborateurs en raison de différences géographiques et/ou organisationnelles, Workday permet aussi aux utilisateurs de sélectionner le type d'authentification le mieux adapté.

Prise en charge de l'authentification unique

Alors que le protocole LDAP prend en charge une solution avec un nom d'utilisateur et un mot de passe unifiés, le protocole SAML va plus loin en offrant un environnement d'entreprise à authentification unique (SSO). Le protocole SAML offre une authentification unique et transparente entre la solution interne de gestion des identités et des accès (IAP) et Workday.

Connexion native Workday

Pour les clients qui souhaitent utiliser la connexion native, Workday stocke leur mot de passe Workday uniquement sous forme de hachage sécurisé, plutôt que le mot de passe lui-même. Les échecs de connexion, ainsi que les connexions et déconnexions réussies, sont consignés à des fins d'audit. Les sessions au cours desquelles l'utilisateur est inactif expirent automatiquement après une durée définie que le client peut configurer en fonction de l'utilisateur. Les règles du mot de passe, configurables par le client, définissent une longueur, un niveau de complexité et un délai d'expiration.

Authentification multifacteur

Workday fournit une authentification multifacteur et recommande aux clients de l'utiliser. Workday permet à ses clients de fournir toute application d'authentification reposant sur l'algorithme TOTP (Time-Based One-Time Passcode - mot de passe à usage unique et durée définie). Avec cette configuration, les clients peuvent facilement intégrer des fournisseurs d'authentification multifacteur avec la connexion native Workday. Workday permet aussi aux utilisateurs finaux des clients de recevoir un mot de passe à usage unique via un mécanisme de passerelle e-mail-SMS. Enfin, Workday prend en charge les questions secrètes comme moyen supplémentaire de prouver l'identité d'un utilisateur.

Appareils de confiance

Workday offre aux clients et à leurs utilisateurs finaux la possibilité d'inscrire leurs appareils comme étant dignes de confiance pour accéder à leur client Workday. Les utilisateurs finaux reçoivent une notification lorsque des appareils non reconnus tentent d'accéder à leur compte. Ils peuvent aussi supprimer les appareils qu'ils ne considèrent plus dignes de confiance. Une liste des appareils dignes de confiance est fournie aux administrateurs à des fins de surveillance. Pour configurer cette fonction, les administrateurs doivent l'activer pour leur client et les utilisateurs finaux doivent accepter le suivi de leurs appareils dignes de confiance à l'aide d'un cookie de navigation.

Authentification progressive

Workday propose l'authentification progressive comme moyen d'authentification renforcée pour l'accès aux ressources sensibles. Les entreprises utilisant le protocole SAML comme type d'authentification peuvent renforcer la protection des données contre les accès non autorisés aux éléments jugés critiques dans le système Workday. Cela permet aux clients d'imposer un facteur d'authentification secondaire que les utilisateurs doivent saisir pour accéder à ces éléments.

Autorisations

Pour les autorisations, l'application Workday applique une stratégie de sécurité de groupe. L'application empêche tout utilisateur d'accéder directement à la base de données de production. Les groupes de sécurité fournis par Workday ou créés par le client, combinés à des stratégies de sécurité prédéfinies, autorisent ou limitent l'accès utilisateur aux fonctionnalités, aux processus de gestion, aux rapports et aux données, que l'accès se fasse en ligne ou via des services Web.

Les groupes de sécurité configurables par le client sont basés sur les utilisateurs, les rôles, les postes, les organisations, la hiérarchie de sites ou les lieux de travail. Ils peuvent être redéfinis en nouveaux groupes de sécurité qui incluent ou excluent logiquement d'autres groupes. L'accès intersystème est défini par les groupes de sécurité du système d'intégration. Les clients peuvent ajuster ces groupes et ces stratégies en fonction de leurs besoins, en paramétrant les accès aussi précisément que nécessaire pour prendre en charge les configurations complexes, y compris les implémentations à l'échelle mondiale.

Workday fournit également des groupes de sécurité qui sont mis à jour automatiquement à partir de processus de gestion tels que le recrutement et la fin de contrat. Ces groupes fournis par Workday peuvent être utilisés séparément ou en association avec d'autres groupes de sécurité fournis par Workday ou créés par le client pour définir l'accès à l'aide de règles de sécurité.

Cloud public

Workday utilise des services Cloud publics d'Amazon Web Services (AWS) pour la conservation et le traitement de contenu dans la plateforme Media Cloud de Workday. Le contenu du client est séparé logiquement de celui des autres clients. Tout le contenu du Media Cloud Workday est chiffré au repos à l'aide du chiffrement côté serveur d'AWS. Chaque objet stocké par Workday au sein d'AWS est chiffré avec l'algorithme AES et une clé de chiffrement unique de 256 bits.

Workday utilise Amazon VPC (Amazon Virtual Private Cloud - cloud virtuel privé d'Amazon), une section isolée logiquement du Cloud AWS. Toutes les communications entre les utilisateurs finaux et les data centers de Workday ou les services Amazon VPC de Workday sont chiffrées au niveau de la couche transport. De plus, toutes les communications entre les services Amazon VPC de Workday et les data centers de Workday, et inversement, sont également chiffrées. Workday utilise le protocole TLS pour chiffrer tout le trafic uniquement avec des modes de chiffrement sécurisés.

Audit permanent

Workday assure un suivi de l'ensemble des modifications des données de gestion au niveau de l'application. Ces informations d'audit de l'application constituent la base des procédures d'audit et des rapports de conformité présents dans tout le système Workday. Workday enregistre les connexions et déconnexions réussies des utilisateurs ainsi que les échecs de connexion et intègre ces informations dans les rapports d'audit de Workday. Workday utilise des mises à jour non destructrices, ce qui signifie que les données ne sont jamais écrasées et sont conservées pendant toute la durée de la relation avec le client. Cela permet aux clients d'obtenir un historique d'audit complet de grande utilité. Les fonctionnalités d'audit de Workday fournissent à un auditeur les informations requises pour retracer l'historique des modifications apportées à un objet de gestion ou à une transaction.

A propos de Workday

Workday est l'un des leaders des applications Cloud dédiées aux entreprises pour la gestion financière et la gestion des ressources humaines.

Fondé en 2005, Workday propose des solutions de gestion financière, de gestion des ressources humaines et d'analyses décisionnelles conçues pour les plus grandes entreprises, les établissements d'enseignement et les agences gouvernementales du monde entier. Des organisations de toutes tailles, des ETI aux grandes entreprises du classement *Fortune 50*, ont déjà choisi Workday.

Workday | Téléphone : +33 (0)1 84 88 34 44 | workday.com/fr