Sécurité de Smartsheet

Présentation approfondie des fonctionnalités, pratiques et protections offertes par Smartsheet en matière de sécurité

Résumé

Chez Smartsheet, nous sommes conscients que toute plateforme de logiciel en tant que service (SaaS) destinée aux professionnels se doit de disposer de multiples niveaux de défense ainsi que d'une myriade de protections et contrôles informatiques pour assurer la sécurité des données sensibles de l'entreprise. Ces solutions doivent également être flexibles, et capables de s'intégrer dans les systèmes et les processus de sécurité des données existants.

Ce livre blanc présente les fonctionnalités, les protections et les pratiques de Smartsheet en matière de sécurité et de gouvernance. Nous nous intéresserons en premier lieu aux fonctionnalités contrôlées par le client que Smartsheet recommande de mettre en œuvre afin de garantir un environnement de travail sécurisé, conforme et bien gouverné en toutes circonstances. Veuillez noter que ce livre blanc s'intéresse uniquement aux fonctionnalités de sécurité généralement disponibles.

Présentation

Afin de renforcer la sécurité de votre organisation, nous recommandons la mise en place de contrôles dans trois domaines clés : la gestion des identités et des accès, la gouvernance des données et la configuration globale des comptes. En complément, ce document présente des informations générales concernant les pratiques de sécurité, de confidentialité et de conformité de Smartsheet.

- **La gestion des identités et des accès** consiste en premier lieu à contrôler la façon dont vos utilisateurs accèdent à Smartsheet. Vous avez ainsi la garantie que le rôle et l'identité de chaque utilisateur de la plateforme correspondent à votre structure ainsi qu'à vos politiques organisationnelles. Nous expliquerons également comment sécuriser la plateforme tout en collaborant avec des utilisateurs extérieurs en adaptant vos préférences de sécurité.

- **La gouvernance des données** concerne aussi bien l'utilisateur que l'organisation tout entière. Smartsheet applique par défaut le principe de moindre privilège pour les utilisateurs et met à votre disposition des contrôles supplémentaires pour mieux contrôler la visibilité. Ainsi, les utilisateurs n'accèdent qu'aux données dont ils ont besoin, quand ils en ont besoin. Au niveau de l'organisation, nous examinerons des mécanismes simples (partage sécurisé, rapports d'utilisateurs, etc.) ainsi que des capacités avancées disponibles en option (p. ex., les politiques de sortie des données).

- **La configuration globale des comptes** vous permet de personnaliser l'aspect de votre environnement Smartsheet afin qu'il corresponde à la charte graphique de votre organisation. Même une simple confirmation visuelle que vos utilisateurs se trouvent dans l'environnement sécurisé de votre organisation peut renforcer la sécurité. Assurez la cohérence en verrouillant les éléments de personnalisation. Ainsi, chaque ressource créée s'harmonise avec votre marque.

- **Les pratiques de sécurité, de confidentialité et de conformité** concernent les actions ainsi que les protections mises en place par Smartsheet en dehors de la plateforme afin de sécuriser les données des clients. Smartsheet déploie une stratégie de protection avancée parmi les meilleures de l'industrie, en associant des individus, des processus et des technologies qui renforcent aussi bien la confidentialité, l'intégrité que la disponibilité des environnements et ressources Smartsheet.

Table des matières

Gestion des identités

La gestion de l'identité d'un utilisateur utilisant Smartsheet — et donc de son accès au système — est tout aussi importante que la gestion des données dans la plateforme.

En déployant Smartsheet, il vous sera rapidement proposé de choisir une méthode d'authentification. Smartsheet propose différentes options : e-mail et mot de passe ou méthodes d'authentification unique (SSO) offertes par Google, Microsoft, Apple et les fournisseurs d'identité SAML 2.0.

Vous pouvez sélectionner une ou plusieurs méthodes pour votre organisation, bien que nous recommandions de mettre en place une seule méthode d'authentification SSO pour tous les utilisateurs et de désactiver les autres options. Nous conseillons également d'ajouter une couche de sécurité en mettant en place l'authentification multifacteur (MFA) lorsque vous configurez l'authentification unique.

Smartsheet dispose d'un ensemble performant d'API REST. L'API utilisé par Smartsheet se base sur le protocole OAuth 2.0 pour ses besoins d'authentification et d'autorisation. Un en-tête HTTP comprenant un jeton d'accès est nécessaire pour procéder à l'authentification de chaque demande. Pour plus de sécurité, les bonnes pratiques veulent que vous utilisiez le protocole OAuth 2.0 pour toute intégration.

Gestion des accès

La gestion des utilisateurs et de leur accès est une fonction administrative essentielle, qui peut avoir un impact aussi bien sur la sécurité que sur l'adoption de Smartsheet par votre organisation. Les organisations doivent maintenir un équilibre délicat, en encourageant la collaboration tout en gérant les risques liés à la décentralisation croissante des données et des équipes. Pour y parvenir, Smartsheet propose trois modèles de gouvernance distincts qui correspondent aux principales façons dont nos clients souhaitent gérer l'application.

Modèles de gouvernance Smartsheet

La première approche consiste en un modèle décentralisé, ou fédéré, qui permet aux différentes unités commerciales de contrôler directement leurs achats et leurs forfaits. Dans ce modèle, le service informatique ne s'occupe généralement pas des questions administratives. Chaque service décide de la facturation des forfaits, de la gouvernance et de la gestion des utilisateurs. Ce modèle convient généralement aux entreprises qui commencent leur parcours Smartsheet.

Notre deuxième approche est un modèle centralisé, ou consolidé, où les forfaits Smartsheet sont tous regroupés au sein d'un seul abonnement régi par le service informatique. Cela permet la maîtrise directe des dépenses, de la gestion des utilisateurs et des contrôles de sécurité. Ce modèle convient particulièrement aux équipes informatiques qui souhaitent surveiller de près chaque aspect de leur expérience Smartsheet.

Enfin, notre modèle partagé, ou hybride, vise à proposer une approche intermédiaire : le service informatique contrôle les paramètres qui s'appliquent à toute l'organisation par le biais du Gestionnaire de forfaits Entreprise. Les administrateurs système de l'entreprise, quant à eux, s'occupent directement de la gestion des licences et des utilisateurs. La facturation est également répartie par forfait, et donc par service. Dans ce modèle, les dépenses Smartsheet sont intégrées dans le budget de chaque service au lieu d'être facturées de manière centralisée au service informatique.

Pour une sécurité maximale, Smartsheet recommande les forfaits partagés ou centralisés, qui favorisent des contrôles informatiques plus directs sur vos forfaits.

Administration des utilisateurs

Si plusieurs équipes de votre entreprise adoptent Smartsheet de manière indépendante pour répondre à leurs besoins, vous pouvez créer des forfaits multiples et distincts. Les fusions-acquisitions sont l'une des raisons qui conduisent à la création d'un environnement avec plusieurs forfaits Smartsheet.

Pour gérer les utilisateurs de ces forfaits à l'aide du modèle décentralisé, nous recommandons d'activer la découverte des comptes pour chacun de ces forfaits. Lorsque de nouveaux utilisateurs utilisent Smartsheet, cela leur permet, à eux ainsi qu'à toute personne rattachée au domaine de votre organisation, de visualiser la liste des forfaits Smartsheet associés à votre entreprise. Vous disposez ainsi d'une base centralisée pour demander à rejoindre l'un des forfaits existants plutôt que de souscrire à un nouveau forfait. Ces demandes sont automatiquement envoyées à vos administrateurs système (par le biais du centre d'administration de Smartsheet) pour examen et approbation.

Si vous disposez de multiples forfaits séparés et souhaitez gérer les utilisateurs à l'aide du modèle centralisé, vous devrez peut-être consolider les comptes. Remarque : les clients disposant de fonctionnalités avancées telles que Dynamic View, des connecteurs, ou Control Center doivent collaborer avec l'assistance Smartsheet pour être accompagnés dans certains aspects de la consolidation.

Si vous utilisez le modèle partagé et le Gestionnaire de forfaits Entreprise, une bonne pratique veut que vous regroupiez les forfaits par services/équipes/centres de coûts. Cela vous permet de définir une politique d'affectation automatique des utilisateurs au forfait pertinent en fonction de leur appartenance à l'une de ces entités.

Gestion des utilisateurs

Smartsheet comprend qu'ajouter un utilisateur à la fois n'est pas toujours adapté lorsque l'adoption s'étend à des dizaines, des centaines, voire des milliers d'utilisateurs. Ainsi, lors de vos débuts sur la plateforme, nous recommandons d'utiliser la fonctionnalité d'importation massive d'utilisateurs dans notre centre d'administration, afin d'ajouter en toute simplicité jusqu'à mille utilisateurs à la fois à votre organisation Smartsheet. Vous pouvez également utiliser l'actualisation en masse pour modifier les rôles des utilisateurs existants.

Les fusions-acquisitions entraînent généralement un repositionnement de marque, et les utilisateurs se voient attribuer de nouvelles adresses e-mail. La fusion des utilisateurs permet la mise à jour massive de l'adresse e-mail principale des utilisateurs tout en supprimant les comptes doublons.

Un forfait Smartsheet consolidé permet d'utiliser deux autres fonctionnalités afin de rationaliser et d'automatiser la gestion des utilisateurs :

- La fonction Provisionnement automatique des utilisateurs (UAP) automatise le processus d'ajout d'utilisateurs à un compte Entreprise. Lorsque les utilisateurs se connectent ou créent un compte Smartsheet avec l'adresse e-mail de leur entreprise, ils sont automatiquement ajoutés à votre compte. Vous pouvez également choisir d'attribuer une licence à ces utilisateurs ou de les faire rejoindre le compte automatiquement en tant que collaborateurs sans licence (forfait gratuit).

    - Si vous avez opté pour notre modèle consolidé, nous recommandons d'activer la fonction UAP afin que le personnel puisse automatiquement rejoindre le compte central contrôlé par le service informatique.

    - Si vous utilisez notre modèle partagé (et que votre organisation consigne les données liées au service et au centre de coût pour votre liste d'utilisateurs), nous conseillons là encore d'activer la fonction UAP. Ces données peuvent être importées afin d'associer automatiquement les utilisateurs avec le forfait adéquat lorsqu'ils demandent une licence. Cette fonction permet également d'automatiser le déplacement des utilisateurs sans licence entre les forfaits.

- L'intégration d'annuaire permet la synchronisation automatique des utilisateurs d'Azure Active Directory (AD) de Microsoft avec Smartsheet. Intégrez Smartsheet à votre automatisation existante dans Azure AD pour automatiser entièrement l'intégration et le départ des utilisateurs, afin de minimiser le risque que les utilisateurs s'attardent ou reviennent sur leurs comptes Smartsheet. Autre avantage : les attributs AD au niveau de l'utilisateur, tels que le service/centre de coût/pôle, sont inclus dans la fonction Chargeback Report (rapport de rétrofacturation) Smartsheet, qui est accessible depuis le centre d'administration et facilite la rétrofacturation interne. Une bonne pratique consiste à synchroniser tous les utilisateurs de l'annuaire avec le compte Smartsheet de votre organisation. Cela empêche les utilisateurs de créer des comptes Smartsheet supplémentaires, dits d'« informatique de l'ombre », lors de leur première connexion. Deuxième couche de défense possible : laisser la fonction UAP activée afin de parer à toute éventualité si des utilisateurs ne sont pas déjà synchronisés par le biais de l'annuaire.

Lorsqu'une personne quitte votre organisation, vous devez révoquer son accès à Smartsheet. Nous vous proposons deux méthodes pour cela. La suppression d'utilisateurs permet de les retirer, eux et les ressources qu'ils possèdent, de votre compte Smartsheet. Attention cependant : cela peut entraîner le retrait d'éléments toujours actifs, mettant ainsi potentiellement à mal les solutions qui s'appuient sur ces données. À la place, Smartsheet recommande la désactivation des utilisateurs. Dans ce cas de figure, les utilisateurs ne peuvent plus accéder à Smartsheet, mais vous avez toujours accès à leur contenu, ce qui vous épargne toute préoccupation concernant la stabilité de la solution ou les transferts de propriété.

Rôles et types d'utilisateurs dans Smartsheet

Quelle que soit votre méthode de provisionnement, vous devez attribuer des rôles Smartsheet au personnel de votre organisation.

Remarque : l'attribution d'un rôle à l'utilisateur ne lui donne pas accès aux ressources Smartsheet de votre organisation. Vous devez aussi partager directement ces ressources avec les utilisateurs concernés. Ainsi, tant les autorisations d'accès aux ressources que les rôles permettent de déterminer ce que les intervenants peuvent visualiser ou réaliser dans Smartsheet. Smartsheet propose les rôles de base suivants :

- Utilisateur sous licence : utilise des fonctionnalités sous licence, telles que la création de feuilles.

- Administrateur de groupe* : crée et gère des groupes Smartsheet.

  * Les rôles « Administrateur de groupe » ne sont attribuables qu'aux utilisateurs sous licence.

- Administrateur système : gère les utilisateurs, les paramètres de compte et les contrôles de sécurité.

Nous vous recommandons fortement d'affecter au moins deux administrateurs système à votre compte Smartsheet pour assurer la continuité du service en cas d'absence.

Les administrateurs de groupe peuvent créer des groupes Smartsheet qui permettent aux utilisateurs de partager du contenu avec le groupe plutôt qu'avec chaque membre individuellement. Ces administrateurs ne gèrent que les groupes qu'ils possèdent. Si nécessaire, n'autorisez que les intervenants de votre organisation à rejoindre le groupe pour limiter les collaborations externes.

Si vous n'affectez aucun des rôles cités ci-dessus à un utilisateur, son accès sera limité aux éléments Smartsheet partagés avec lui (feuilles, rapports, tableaux de bord ou WorkApps). Afin de créer des ressources Smartsheet, les intervenants doivent être des utilisateurs sous licence. Ils peuvent soumettre une demande de licence directement sur l'application Smartsheet. Les administrateurs système peuvent suivre et répondre aux demandes de manière individuelle ou groupée par le biais de la section dédiée à la gestion des demandes de licence du centre d'administration. Si vous avez déjà un processus établi pour la gestion des demandes de licence, tirez profit de l'écran de mise à niveau personnalisé pour rediriger les utilisateurs vers ce processus interne.

Collaborateurs externes

Tout intervenant qui n'appartient pas à votre domaine et avec qui vous partagez vos ressources Smartsheet est considéré comme un collaborateur externe. Smartsheet permet à votre organisation de travailler librement avec des collaborateurs externes de confiance sans frais supplémentaires. Pour renforcer la sécurité lorsque vous collaborez avec des tiers, nous vous conseillons de tirer parti de trois contrôles du centre d'administration :

Le partage sécurisé permet de désigner les domaines ou les adresses e-mail de confiance pour lesquels vous autorisez la collaboration externe.

Les rapports d'accès aux feuilles fournissent une liste des collaborateurs externes qui ont accès au contenu Smartsheet de votre organisation.

Révoquez l'accès aux éléments directement depuis le centre d'administration pour retirer les collaborateurs externes du contenu auxquels ils n'ont plus besoin d'accéder.

Gouvernance des données

La gouvernance efficace des données est aujourd'hui indispensable à l'entreprise. Elle garantit que les informations détenues par l'organisation sont créées, utilisées, partagées et protégées conformément aux réglementations applicables, aux politiques de l'entreprise et aux bonnes pratiques du secteur.

Ces contrôles sont non seulement obligatoires, mais garantissent également l'efficacité, la confidentialité et la continuité des activités :

Au niveau de l'utilisateur, l'organisation doit disposer d'outils efficaces pour limiter la visibilité, en ne montrant que les informations pertinentes aux intervenants concernés.

Au niveau de l'organisation, l'entreprise doit être équipée des outils nécessaires à la création ainsi qu'à l'application d'une politique efficace.

Gouvernance des données au niveau de l'utilisateur

La plupart des utilisateurs connaissent bien les niveaux d'autorisation dans Smartsheet (spectateur, éditeur, administrateur et propriétaire). Les outils Dynamic View et WorkApps offrent des contrôles et une flexibilité supplémentaires, granulaires, pour disposer de fonctionnalités de gouvernance des données efficaces au niveau de l'utilisateur. Le fait de limiter l'accès au contenu pertinent permet à la fois de garantir l'efficacité du processus (puisque les utilisateurs ne s'intéressent qu'aux éléments qui requièrent leur attention) et de renforcer la sécurité, en appliquant le principe de moindre privilège par défaut de Smartsheet à une échelle plus précise.

Dynamic View

Tous les processus d'entreprise n'exigent pas une transparence totale. De nombreux processus (gestion des commandes, collaboration avec les fournisseurs, projets impliquant des équipes mixtes internes et externes) nécessitent au contraire de contrôler strictement les données partagées et leurs destinataires.

L'outil Dynamic View facilite la collaboration tout en protégeant la confidentialité. Avec Dynamic View, les propriétaires de feuilles peuvent partager de manière sélective des lignes et des champs pertinents avec des collaborateurs précis, sans leur donner pour autant accès aux feuilles liées. Les utilisateurs partagent ainsi de façon ciblée des éléments avec des fournisseurs, des équipes mixtes internes et externes, ou entre organisations, de manière à collaborer seulement sur certains champs. Chacun a accès aux informations dont il a besoin, et uniquement à celles-ci.

WorkApps

WorkApps vous permet de rationaliser votre travail et de simplifier la collaboration avec des applications intuitives construites directement depuis vos feuilles, formulaires, tableaux, rapports et plus encore. Vous pouvez adapter l'expérience de l'application aux membres de votre équipe selon le rôle de chacun, et travailler conjointement à partir des mêmes ensembles de données liés. Faites évoluer vos applications en utilisant la même sécurité multiniveau de pointe que la plateforme Smartsheet.

WorkApps vous évite d'avoir à partager les ressources liées qui composent l'application WorkApp. Vous pouvez créer une application WorkApp avec un affichage filtré des feuilles et des rapports sélectionnés, sans avoir à partager ceux-ci avec l'utilisateur final. Ce dernier n'a que la vue « WorkApp » de ces ressources.

Contrôles des politiques de gouvernance des données au niveau de l'organisation

Smartsheet permet aux administrateurs de veiller à ce que les fonctionnalités de la plateforme soient utilisées conformément aux politiques de gouvernance de l'organisation. Ces contrôles autorisent les administrateurs à mettre en place des garde-fous pour assurer une bonne gouvernance des données. Ainsi, seules les personnes ayant besoin d'interagir avec ces données sont autorisées à les traiter, et ce, de la manière autorisée.

Les administrateurs peuvent décider de la façon dont les utilisateurs pourront interagir avec certaines fonctionnalités. Les propriétaires de la feuille doivent-ils être autorisés à publier celles-ci et à créer de nouvelles automatisations ? Disposez-vous d'un système de stockage précis auquel les fichiers doivent être rattachés ? Les collaborateurs externes doivent-ils être en mesure de télécharger le contenu partagé avec eux ? Voici quelques questions que les administrateurs doivent se poser pour identifier efficacement les contrôles à mettre en place au niveau de l'organisation.

Ces contrôles de politique s'appliquent aussi au partage sécurisé. Il s'agit de l'outil idéal pour limiter le partage des données et des ressources avec certains domaines ou adresses e-mail. Comme mentionné précédemment, le partage sécurisé permet également de définir si votre organisation peut partager des éléments Smartsheet avec d'autres acteurs, tels que des fournisseurs et des partenaires.

Contrôle widget de contenu Web

Les tableaux de bord offrent la possibilité d'intégrer du contenu interactif (des vidéos, des diagrammes, des documents et plus encore). Les administrateurs peuvent activer ou désactiver cette fonctionnalité et établir une liste approuvée de domaines pris en charge pour le widget de contenu Web. Une bonne pratique consiste à limiter cette fonctionnalité aux domaines internes de l'entreprise.

Autorisations d'automatisation

Contrôlez qui reçoit l'automatisation depuis les feuilles. Les options disponibles sont Restreintes (seuls les utilisateurs partagés sur la feuille peuvent réaliser des actions) ou Non-restreintes (l'automatisation s'applique à toute adresse e-mail ou intégration tierce, comme Slack). Nous vous recommandons de vérifier ce contrôle pour vous assurer qu'il est configuré conformément au niveau de collaboration interne et externe que souhaite votre organisation.

Contrôles des pièces jointes

Déterminez si les membres bénéficiant du forfait sont autorisés à charger des fichiers stockés sur leur ordinateur, en joignant un lien vers un site (URL), ou à partir d'un service de stockage en ligne tiers tel que Google Drive, OneDrive, Box, Dropbox, Evernote ou Egnyte. Pour empêcher la collecte de données provenant de sources non reconnues, autorisez uniquement les fournisseurs de pièces jointes dont l'utilisation est conforme aux politiques internes de votre organisation.

Contrôles de publication

La publication d'une feuille, d'un rapport ou d'un tableau de bord génère une URL unique à laquelle quiconque peut accéder sans avoir à se connecter à Smartsheet, ainsi qu'un code iframe que vous pouvez intégrer dans le code source d'un site Web pour afficher la feuille ou le rapport.

Vous pouvez désactiver la publication de feuilles, de rapports, de tableaux de bord et d'iCalendar. Dans ce cas, la touche Publier n'apparaît plus sur la ressource Smartsheet. Vous pouvez également restreindre l'accès aux éléments publiés aux personnes appartenant à votre organisation Smartsheet. D'après nos observations, les clients soucieux des questions de sécurité autorisent généralement la publication, mais limitent l'accès aux éléments publiés aux personnes rattachées à leur compte.

Partage sécurisé

Utilisez cette fonctionnalité pour restreindre le partage par domaine ou par adresse e-mail (pour vous assurer que les feuilles ne sont partagées qu'avec les personnes ayant une adresse e-mail de l'entreprise, par exemple). Smartsheet recommande fortement de mettre en place le partage sécurisé pour contrôler la collaboration externe. Pour simplifier la mise à jour et la maintenance de votre liste de partage sécurisé, nous conseillons également de collecter toutes les demandes d'actualisation à l'aide d'un formulaire en ligne Smartsheet.

Contrôles pour l'envoi de formulaires hors ligne

Lorsque vous utilisez l'application mobile, Smartsheet autorise automatiquement la soumission hors ligne des formulaires. Cela permet de répondre aux besoins des utilisateurs qui n'ont pas une connexion stable, par exemple sur un chantier de construction. Ce contrôle permet aux administrateurs de désactiver (ou de réactiver) les soumissions de formulaires hors ligne, afin de définir si un utilisateur peut lancer l'application mobile sans connexion pour soumettre des formulaires.

Contrôles pour l'intégration des services de communication

Smartsheet prend en charge les services de communication que sont Google Chat, Microsoft Teams, Slack et Cisco Webex. Les administrateurs de compte peuvent activer un ou plusieurs services, selon leur choix.

Journalisation et génération de rapports

Vous pouvez télécharger des rapports ciblant différents aspects de l'utilisation de Smartsheet par votre organisation. Vous bénéficiez ainsi d'une visibilité continue sur l'utilisation, les utilisateurs, le contenu, la facturation et l'accès à Smartsheet :

Rapport sur les accès à la feuille

Cette fonctionnalité génère un fichier Excel qui répertorie l'ensemble des feuilles, des rapports et des tableaux de bord que possèdent les utilisateurs sous licence du compte, ainsi que le nom de l'espace de travail où sont sauvegardés ces éléments (le cas échéant), les collaborateurs avec qui chaque feuille est partagée, ainsi que l'horodatage de chaque modification. Nous recommandons de consulter régulièrement ce rapport afin de vérifier la liste des collaborateurs externes ayant accès aux ressources appartenant aux membres de votre organisation.

Rapport sur les éléments publiés

Cette fonctionnalité génère un fichier Excel qui répertorie tous les éléments publiés. Cette solution est idéale pour assurer la sécurité des données ou le suivi des personnes qui ont publié des éléments précis. Utilisez ce rapport pour adapter la configuration du contrôle de publication en fonction des besoins.

Rapport de la liste des utilisateurs

Cette fonctionnalité génère un fichier Excel qui répertorie tous les membres associés au compte (aussi bien les membres invités qu'actifs), la date et l'heure auxquelles ils ont rejoint le compte, leurs niveaux d'accès (administrateur système, administrateur de groupe, etc.), le nombre de feuilles qu'ils possèdent ainsi que la date et l'heure de leur dernière connexion à Smartsheet.

Rapport sur l'historique de connexion

Les administrateurs système des comptes multi-utilisateurs peuvent passer par le centre d'administration pour recevoir par e-mail un fichier Excel répertoriant l'historique des connexions récentes.

Rapport de rétrofacturation

Les clients qui recourent à l'intégration d'annuaire peuvent utiliser les rapports de rétrofacturation, disponibles dans le centre d'administration, pour faciliter la rétrofacturation interne. Cette fonctionnalité permet d'ajouter des colonnes pôle, service et centre de coûts au rapport existant généré lorsque les clients téléchargent leur liste d'utilisateurs. Elle fournit ainsi les données nécessaires pour créer un rapport de rétrofacturation interne.

Pour un suivi granulaire des actions de l'utilisateur au niveau de la feuille, du tableau de bord et de la cellule, vous pouvez consulter le journal d'activité, l'historique de la cellule et les colonnes systèmes.

- **Journal d'activité :** affiche une piste d'audit de toutes les modifications apportées à une ressource, de leur auteur et du moment où elles ont été réalisées. Il s'agit de modifications telles que la suppression d'une ligne (avec les données supprimées), les personnes qui ont consulté l'élément et les modifications des autorisations de partage.

- **Historique de la cellule :** présente un journal des modifications effectuées au niveau de la cellule, qui précise les modifications apportées, leur auteur et le moment où elles ont été réalisées. Les utilisateurs peuvent aisément faire un copier-coller depuis l'historique de la cellule pour rétablir des informations supprimées ou modifiées par erreur.

- **Colonnes systèmes :** indiquent l'heure à laquelle chaque ligne a été modifiée pour la dernière fois et le collaborateur qui a effectué la modification.

Contrôles avancés de gouvernance des données

Smartsheet propose un certain nombre de fonctionnalités avancées qui permettent un contrôle de la gouvernance des données. Celles-ci se destinent aux clients ayant des besoins de sécurité particulièrement exigeants. Ces fonctionnalités sont proposées avec Smartsheet Advance Platinum et Smartsheet Safeguard.

Clés de chiffrement gérées par les clients

Smartsheet utilise le chiffrement afin de protéger les données des clients et d'aider ces derniers à les contrôler. Les clés de chiffrement gérées par les clients (CMEK) sont destinées aux organisations ayant des données sensibles ou réglementées qui leur imposent de gérer leurs propres clés de chiffrement. Les CMEK permettent aux entreprises d'utiliser des applications SaaS cloud tout en conservant un contrôle des données comparable à celui d'une installation sur site. Cela ajoute ainsi une couche de chiffrement gérée par le client au stockage des données Smartsheet, en accord avec les politiques avancées de sécurité et de gouvernance des données.

Remarque : pour utiliser les clés de chiffrement gérées par les clients, ces derniers doivent disposer d'un accès Amazon Web Services Key Management Service (AWS KMS). Les clés du client sont en effet générées et gérées directement sur la plateforme AWS.

Smartsheet utilise les CMEK pour chiffrer les données de votre organisation afin qu'elles restent sous votre contrôle à tout moment. Plus concrètement, Smartsheet ne stocke ni ne contrôle ces clés de chiffrement. Smartsheet doit demander et récupérer les clés auprès de votre service AWS KMS chaque fois qu'elle souhaite accéder aux données de votre feuille.

Dans la mesure où votre organisation contrôle les CMEK stockées dans le système AWS KMS, vous pouvez à tout moment révoquer l'accès de Smartsheet aux CMEK, et par conséquent, son accès à vos données. En détruisant les clés principales, ou clés KMS, dans le système AWS KMS, votre organisation supprime ses données au sein des systèmes Smartsheet. Si un tiers mal intentionné dispose d'une copie de la base de données, du code source et des clés de chiffrement cloud de Smartsheet, il ne pourra malgré tout pas lire les données chiffrées avec les CMEK.

Politiques de sortie des données

Le partage de données présente toujours un certain degré de risque. Lorsque vous partagez un contenu particulièrement sensible, il est fondamental de s'assurer que les données de votre entreprise restent dans votre compte et sous votre contrôle.

Les administrateurs système peuvent tirer profit des politiques de sortie des données afin de protéger les informations confidentielles, grâce à un contrôle granulaire de la façon dont les données sont exportées à l'intérieur et à l'extérieur de l'organisation.

En mettant en place des politiques de sortie des données, vous pouvez empêcher les collaborateurs internes et externes de réaliser les actions suivantes sur les feuilles, les rapports et les tableaux de bord :

- Enregistrer sous un nouveau nom
- Enregistrer en tant que modèle
- Envoyer en tant que pièce jointe
- Publier
- Imprimer
- Exporter

Les utilisateurs qui tentent de réaliser une action restreinte reçoivent une notification les informant que cette opération est interdite en raison de la politique de sortie des données de votre organisation.

Ces limites empêchent les collaborateurs de sauvegarder ou de partager des informations confidentielles à des fins malveillantes.

Rapports d'événements

Pour assurer la sécurité des données, de nombreuses entreprises exigent des informations continues sur la façon dont leurs applications opérationnelles, telles que Smartsheet, sont utilisées. Il est recommandé de garder une visibilité sur :

- Qui crée des feuilles
- Qui crée des espaces de travail
- Qui supprime des objets
- Qui a partagé une feuille, et avec qui

Les rapports d'événements fournissent une visibilité granulaire sur le comportement des utilisateurs et leurs activités au sein du compte Smartsheet de votre organisation. Cette fonctionnalité vous permet de surveiller les pertes de données tout en identifiant les schémas d'utilisation récurrents et anormaux, afin d'appliquer rigoureusement les politiques de sécurité et de conformité de l'entreprise.

La fonction Rapports d'événements fournit un flux de données JSON des événements d'utilisation (« Événement ») de Smartsheet au sein d'un forfait (org), auquel il est possible d'accéder par l'API Rapports d'événements. Ce service établit un rapport sur plus de 120 événements dans Smartsheet et stocke jusqu'à six mois de données dès la date d'activation du flux.

Pour bénéficier de ce flux, les données des rapports d'événements sont généralement intégrées à d'autres systèmes de sécurité qui assurent la surveillance, la notification, la création et l'application de politiques ainsi que la prévention des pertes de données (Data Loss Prevention, DLP). Ces applications sont vendues par des tiers, généralement des systèmes CASB (Cloud Access Security Broker), des outils SIEM (Security Information and Event Management), ou une association des deux systèmes. Certaines entreprises délaissent les outils tiers et développent leurs propres systèmes de suivi et d'intervention.

Cas de figure types pour les rapports d'événements :

- Prévention des pertes de données
- Traitement des informations personnellement identifiables (PII)
- Gouvernance des données
- Informations sur la collaboration

Contrôles de conservation des données

Plus votre organisation place du contenu sur une application SaaS, plus le risque pris est grand.

Les contrôles de conservation des données de Smartsheet permettent aux organisations de créer une politique qui détermine quand le contenu doit être supprimé, en fonction des critères qu'elles choisissent d'appliquer.

Ces politiques se basent par exemple sur la date de création ou de dernière modification d'une feuille. Votre instance Smartsheet présente donc uniquement du contenu récent ou actif, ce qui limite votre profil de risque.

Configuration globale des comptes

La sécurité du compte ne passe pas uniquement par des fonctionnalités techniques telles que le chiffrement des données, la classification ou les options d'authentification. Parfois, la sécurité peut se résumer à inclure le logo de votre organisation sur chaque élément qui lui appartient.

Les contrôles de configuration globale des comptes vous permettent de mettre en place des repères visuels correspondant à votre charte graphique (et d'autres restrictions), afin que les utilisateurs sachent que les informations sont fiables.

Les administrateurs système peuvent ajouter des logos à l'ensemble de vos ressources pour que votre déploiement Smartsheet réponde aux exigences de l'organisation en matière de charte graphique. Verrouillez les éléments de personnalisation pour vous assurer que chaque nouvelle ressource répond à la même charte graphique.

Les contrôles de personnalisation et les configurations de compte Smartsheet vous permettent de configurer des écrans d'accueil personnalisés. Vous pouvez créer des écrans d'aide personnalisés avec une description expliquant par où commencer, des écrans de demande de licence pour aider les utilisateurs à vous contacter, ou bien des écrans d'accueil personnalisés et conformes à votre charte graphique qui apparaissent lorsqu'un utilisateur se connecte. Ces écrans peuvent exiger que l'utilisateur approuve les conditions générales d'utilisation avant d'accéder à plus de contenu.

L'association d'une identité visuelle cohérente et d'informations personnalisées confirme aux utilisateurs qu'ils accèdent aux outils et aux informations désirés, ce qui renforce votre sécurité.

Pratiques de sécurité, de confidentialité et de conformité Smartsheet

Fondés sur une approche holistique, les programmes de cybersécurité, de confidentialité et de protection des données de Smartsheet ont pour point de départ des politiques stratégiques de sécurité des données définies et soutenues par le comité de pilotage de la sécurité des informations (Information Security Steering Committee, ou ISSC) et par l'équipe de direction de Smartsheet. Ces politiques sont conçues afin de correspondre aux pratiques stratégiques de gestion des risques de l'organisation, de gérer et de surveiller de manière proactive les risques de sécurité, de promouvoir la sécurité grâce à la maturité des processus et à une architecture de système efficace, et de permettre aux utilisateurs de prendre des décisions judicieuses concernant les risques de sécurité grâce à des actions de formation et de sensibilisation.

Sécurité des données

Nous sécurisons notre plateforme afin de garantir la protection de vos ressources les plus précieuses : vos données. Smartsheet fait appel à des tiers pour faire auditer ses pratiques de sécurité, notamment par le biais d'une évaluation et d'une attestation SOC2 Type II ou d'évaluations de sécurité technique avec des entreprises réalisant des tests d'intrusions. Par ailleurs, le programme de gestion des vulnérabilités de Smartsheet automatise l'identification et la correction des faiblesses du réseau et du système, aussi bien dans les environnements d'entreprise que de production Smartsheet. Smartsheet utilise le chiffrement afin de sécuriser vos données et de vous aider à les contrôler. Voilà ce que vous pouvez attendre de Smartsheet : des données stockées de manière durable avec des suites cryptographiques approuvées par le NIST (National Institute of Standards and Technology), une technologie dite TLS (Transport Layer Security, ou Sécurité de la couche de transport), un chiffrement AES 256 bits au repos ainsi que le service S3 d'Amazon pour stocker et gérer les fichiers chargés.

Confidentialité

Smartsheet respecte votre confidentialité et votre droit de connaître la manière dont vos données personnelles sont collectées et utilisées. Notre déclaration de confidentialité décrit comment Smartsheet recueille, utilise et divulgue les informations personnelles ou les autres données que nous collectons sur nos sites web, dans nos applications mobiles et sur la plateforme Smartsheet.

- Nous reconnaissons le droit à la confidentialité de nos prospects, de nos clients et de nos partenaires, et respectons les réglementations internationales de confidentialité, dont le règlement général sur la protection des données (RGPD) de l'Union européenne.

- Nous proposons un contrat de traitement des données (Data Processing Agreement, ou DPA) aux clients qui souhaitent des conditions d'utilisation particulières pour le traitement de leur contenu comprenant des informations personnelles. Si vous pensez avoir besoin d'un DPA avec Smartsheet, vous pouvez envoyer un formulaire acceptant les conditions du DPA à l'adresse smartsheet.com/legal/DPA

Gestion de l'exploitation

Nous appliquons des politiques ainsi que des procédures afin de garantir que vos données sont sécurisées et sauvegardées sur plusieurs sites géographiquement séparés. Nos équipes analysent en permanence les nouvelles menaces de sécurité et mettent en œuvre des mesures appropriées afin d'empêcher les accès non autorisés ou l'indisponibilité imprévue du service. Seuls les membres autorisés de l'équipe d'exploitation technique de Smartsheet accèdent aux systèmes et aux données de production de Smartsheet, sur la base du principe de moindre privilège et seulement pour les informations pertinentes. Smartsheet publie des informations sur l'état du système sur le site Smartsheet Status. Smartsheet prévient les clients ayant demandé à recevoir des mises à jour automatiques sur le site Smartsheet Status en cas d'incidents importants sur le système, généralement par e-mail ou par SMS.

Sécurité, continuité et redondance du centre de données

Nous collaborons avec des partenaires d'hébergement reconnus du secteur pour que vous puissiez fournir des services à votre organisation en toute confiance sur une plateforme fiable. Nous disposons d'une redondance des données sur plusieurs sites et d'un hébergement dans les locaux d'AWS. Nos installations sont examinées et certifiées SOC 1, SOC 2, ISO 27001 et FISMA. Notre suivi se fait par le biais de protocoles d'identification biométrique, d'une surveillance en continu et d'une gestion permanente de l'environnement de production. Smartsheet applique des processus et des programmes internes pour faire face aux événements perturbant la continuité des activités ainsi qu'aux scénarios de reprise après incident. Smartsheet révise et teste ces programmes chaque année avant de les transmettre au personnel concerné de l'organisation. Nos centres de données sont géographiquement isolés (environ 970 km) les uns des autres afin d'éviter qu'ils ne soient touchés simultanément en cas de catastrophe naturelle de grande ampleur.

Audits et certifications

Les audits et certifications suivants, en lien avec la sécurité et la confidentialité, concernent les principaux services d'application de Smartsheet.

- **SOC 2/SOC 3 :** Smartsheet passe chaque année un examen et un test dans le cadre du processus d'audit SOC. Les rapports d'audit externe attestent de la conception et de l'efficacité opérationnelle des contrôles internes utilisés dans l'ensemble de notre entreprise, y compris ceux liés à la sécurité, la disponibilité et la confidentialité.

- **Certification Privacy Shield (Bouclier de protection des données) UE-États-Unis et Suisse-États-Unis :** les données des clients soumises aux services concernés font l'objet d'une certification annuelle, conformément aux cadres Privacy Shield UE-États-Unis et Privacy Shield Suisse-États-Unis régis par le ministère du Commerce des États-Unis. Vous pouvez consulter la certification en cours à l'adresse privacyshield.gov/list avec le mot-clé « Smartsheet ».

- **FedRAMP (moderate) :** le programme FedRAMP Connect du Joint Authorization Board (JAB) a sélectionné Smartsheet, et a accordé la priorité à Smartsheet Gov pour la certification en fonction de la demande des administrations publiques. Smartsheet Gov est un environnement Smartsheet distinct qui dispose du statut Autorisé par FedRAMP, ce qui facilite l'utilisation de Smartsheet par le gouvernement américain pour gérer son travail tout en l'aidant à répondre à ses exigences en matière de sécurité et de conformité.

- **Loi Sarbanes-Oxley de 2002 :** en sa qualité de société cotée en Bourse, Smartsheet doit se conformer à la loi Sarbanes-Oxley (SOX) adoptée par le Congrès des États-Unis. La conformité SOX favorise la mise en place d'une équipe interne cohérente et améliore la communication entre les équipes qui se chargent des audits.

Comme l'indique notre page dédiée aux mentions légales, Smartsheet utilise l'infrastructure d'Amazon Web Services, Inc. (« AWS ») pour héberger les données client. Nous vous invitons à consulter les sites web d'AWS Security et d'AWS Compliance pour plus de renseignements sur les audits et certifications relatifs à la sécurité ainsi qu'à la confidentialité obtenus par AWS, notamment la certification ISO 27001 et les rapports SOC. Pour obtenir la liste complète de nos certifications ainsi que des livres blancs et des feuilles de données complémentaires, veuillez consulter la page Conformité du Trust Center Smartsheet.

Conclusion et ressources complémentaires

Les entreprises doivent s'appuyer dès aujourd'hui sur une plateforme de gestion du travail moderne, simple d'utilisation et sécurisée. Grâce à une volonté et à un investissement constants, nous avons conçu de A à Z la solution Smartsheet, qui offre des fonctionnalités et répond à des exigences de confidentialité des données particulièrement strictes. En plus des ressources déjà disponibles, nous développons de nouveaux dispositifs de sécurité. Pour en savoir plus sur les fonctionnalités, les programmes et les protections de Smartsheet en matière de sécurité, veuillez consulter la page smartsheet.com/trust et les ressources complémentaires suivantes :

Assistance en ligne administrateur système Smartsheet
Fonctionnalités de Smartsheet en fonction du forfait
Intégrations Smartsheet
Documentation API Smartsheet

sales@smartsheet.com
+44 (20) 39001410
smartsheet.com
/smartsheet
/company/smartsheet-com
@smartsheetplatform
/@smartsheet
/smartsheet
/smartsheet