FAQ Sage Intacct

Gouvernance et cybersécurité

Comment nous protégeons vos données et maintenons l'intégrité et la continuité des systèmes critiques

Ce guide explique comment la cybersécurité et la gouvernance de Sage Intacct fonctionnent pour assurer la sureté et la fiabilité de votre système financier. Lorsque vous travaillez avec Sage Intacct, vous nous confiez le traitement d'informations financières confidentielles et sensibles en toute sécurité. Votre réputation repose sur notre capacité à les protéger de manière exhaustive. Nous prenons cette responsabilité au sérieux, et la sécurité est une priorité absolue pour Sage Intacct, comme pour tous nos clients.

Sage Intacct est construit nativement dans le cloud et déployé pour nos clients mondiaux sur AWS, fournissant des services fiables, sécurisés et évolutifs auxquels font confiance des millions de clients dans le monde entier.

AWS est le leader du secteur en tant que référentiel de confiance pour les données des clients, avec des programmes de sécurité et de confidentialité de classe mondiale. Toutes les données des clients de Sage Intacct FR sont stockées et traitées dans le cloud.

Il fournit une infrastructure sécurisée et des outils flexibles qui vous aident, ainsi que nous, à nous conformer aux réglementations mondiales en matière de confidentialité et de protection des données. Son modèle de sécurité des données complet et flexible sécurise les données à tous les niveaux, y compris la sécurité de l'infrastructure, du réseau, de l'application et de la base de données.

Comment utiliser ce guide

Nous avons rédigé ce document pour répondre plus en détail à d'importantes questions sur la sécurité et la gouvernance, couvrant la politique, la conformité et les mesures de contrôle techniques et organisationnelles spécifiques. Si vous avez besoin de plus d'informations sur n'importe quel aspect de Sage Intacct, veuillez vous adresser à votre gestionnaire de compte.

Modèle de responsabilité partagée en matière de sécurité

Sage contrôle et gère le développement sécurisé de notre logiciel, y compris toutes les mises à jour et les correctifs, la gestion des changements et la gestion des incidents directement liés à notre application.

AWS est responsable de la gestion de la plateforme sur laquelle l’application Sage Intacct est hébergée, y compris tous les systèmes d'exploitation, les bases de données, l'infrastructure réseau, la surveillance de la sécurité et la sécurité physique des centres de données.

Les clients de Sage Intacct doivent s'assurer qu'ils configurent et surveillent leurs autorisations, la gestion des identités, les contrôles d'accès et les privilèges, en utilisant la fonctionnalité fournie par la plateforme et notre application.

Table des matières

Gestion de la sécurité des informations....4

Cybersécurité des tiers....7

Comment nous sécurisons vos données....8

Développement sécurisé de l'application....11

Sécurité des centres de traitement....13

Continuité et reprise d'activité....13

Gestion des risques et incidents....15

Protection des données, respect de la vie privé et conformité....18

Gestion de la sécurité des informations

Sage a-t-il mis en place un programme de gouvernance de la sécurité ?
Oui. Nous prenons très au sérieux la sécurité des données de nos clients. Nous savons à quel point il est important de préserver la sécurité de ces données, c'est pourquoi nous avons mis en place un ensemble de mesures de protection, basées sur les meilleures pratiques reconnues dans l'industrie. De plus amples informations sont disponibles ici : https://www.sage.com/fr-fr/legal

Sage Intacct conserve ses dernières directives en ligne, accessibles au public via le Programme de sécurité de l'information.

https://www.sageintacct.com/information-security-management-program

Quelles sont les politiques de sécurité de Sage ?
Les politiques de Sage sont publiées et accessibles à tous les employés sur notre Intranet. Elles s'appuient sur des normes et des procédures basées sur des standards de cybersécurité de premier plan tels que la norme ISO 27001. Elles couvrent la sécurité de l'information, l'utilisation acceptable des systèmes et applications Sage, le développement de logiciels sécurisés, la classification de l'information et le traitement des données.

Quelles certifications de sécurité l'application Sage Intacct détient-elle ?
Sage effectue divers types d'audits internes et de tiers pour valider la conformité de toutes les activités principales liées à la fourniture opérationnelle de notre système de gestion financière global et sécurisé dans le nuage.

- SSAE 18 SOC 1 Type II
- SOC 2 Type II
- ISAE 3402 / ISAE 3000
- PCI-DCC Level 1 (US)
- HIPAA (US)
- GDPR (UK & EU)

L'application Sage Intacct est déployée sur la plateforme cloud AWS, qui dispose des certifications suivantes :

- ISO 9001 / 27001 / 27017
- SOC 1 / 2 / 3
- NIST Cybersecurity Framework
- Cyber Essentials Plus

Vous trouverez plus d'informations sur le site conformité d'AWS :
https://aws.amazon.com/compliance/programs

Sage dispose-t-elle d'une équipe dédiée à la cybersécurité ?
Sage dispose d'un responsable mondial de la sécurité de l'information (EVP CISO) qui rend compte

directement au conseil d'administration de Sage et qui dirige une équipe de sécurité mondiale spécialisée travaillant dans l'ensemble de l'entreprise. Les fonctions de l'équipe couvrent la sécurité et l'architecture des produits, la conformité, l'ingénierie de la sécurité, les opérations de cyberdéfense, la continuité des activités et la réponse aux crises. Sage dispose également d'une équipe mondiale de gestion des risques et de la conformité qui supervise tous les risques commerciaux.

Les employés, les sous-traitants et le personnel temporaire reçoivent-ils une formation à la sécurité de l'information ?
Sage organise régulièrement des formations et des campagnes de sensibilisation à la sécurité afin d'ancrer et de renforcer une culture de la sécurité dans l'ensemble de l'entreprise. La formation est obligatoire pour tous les nouveaux employés et comprend une formation en ligne, des rafraîchissements spécifiques aux processus et des mises à jour sur les meilleures pratiques en matière de sécurité, de risque, de lutte contre la corruption et de protection de la vie privée ; elle est mise à jour chaque année ou lorsqu'un changement important se produit.

Le programme de formation comprend des méthodes d'apprentissage mixte telles que la jeu, les exercices avec aléa, les conférences avec démonstration en direct et le micro-apprentissage, afin de garantir que la culture de la sécurité est profondément ancrée dans nos pratiques de travail quotidiennes.

Certaines fonctions, telles que les ingénieurs produits, bénéficient d'une formation annuelle obligatoire supplémentaire sur les meilleures pratiques en matière de développement de logiciels sécurisés.

Nous avons également mis en place un programme de champions de la sécurité au sein de l'ingénierie des produits. Les champions de la sécurité travaillent en étroite collaboration avec notre équipe mondiale de sécurité des applications pour garantir la sécurité de nos logiciels et la protection de vos données. Notre fournisseur de plateforme AWS veille à ce que tous les employés qui gèrent l'environnement en contact avec les clients suivent les programmes de certification et de formation d'AWS.

Comment les contrats des fournisseurs (employés, sous-traitants ou fournisseurs tiers) définissent-ils les responsabilités en matière de sécurité de l'information ?
Nous informons nos employés et nos sous-traitants de leurs obligations en matière de sécurité de l'information en utilisant des clauses spécifiques de confidentialité et de non-divulgation dans leurs conditions d'emploi.

Les employés doivent confirmer qu'ils acceptent les termes de notre politique d'utilisation acceptable (AUP) et les partenaires sont tenus de lire et de signer une déclaration annuelle de conformité en matière de sécurité.

Quelles sont les procédures de sélection des candidats mises en place ?
Nous vérifions l'identité et le droit de travailler en prenant des copies des passeports, des permis de conduire et de tout autre document pertinent. Nous prenons plusieurs références indépendantes en matière d'emploi et procédons à des vérifications de base du casier judiciaire lorsque la loi le permet.

Notre fournisseur de plateforme AWS procède à des vérifications approfondies des antécédents de ses employés qui travaillent avec des systèmes internes sécurisés. Les employés autorisés suivent une formation, un accompagnement et un mentorat avant de se voir accorder l'accès. Cet accès est revu tous les trimestres et mis à jour si nécessaire.

Chaque employé qui gère l'environnement en contact avec les clients suit une certification et une

formation supplémentaires.

Cybersécurité des tiers

Sage s'associe-t-il, externalise-t-il ou sous-traite-t-il une partie du service ?
Nous travaillons avec plusieurs partenaires complémentaires qui sont alignés sur les exigences des politiques de sécurité et de gouvernance de Sage. Notre principal sous-traitant est notre fournisseur de plateforme, AWS, et Cloudflare est également utilisé pour la performance et la sécurité du web. Nous pouvons confirmer tous nos sous-traitants sur demande.

Quels sont les services fournis par AWS pour Sage Intacct ?
La plateforme AWS est un service entièrement géré, basé sur le cloud, ce qui signifie que l'installation, la maintenance, les mises à niveau, les correctifs et la surveillance des serveurs physiques, des réseaux et de l'infrastructure associée sont tous fournis par AWS. En outre, nous pouvons tirer pleinement parti des multiples couches de contrôles de sécurité et des fonctionnalités fournies par AWS, ce qui permet à nos clients de bénéficier de notre utilisation de fonctions telles que l'informatique élastique, les services de stockage et les services de surveillance.

D'autres services critiques, tels que la sécurisation de l'accès aux centres de données où vos données sont stockées et traitées, la protection de vos données contre les accès non autorisés et la résilience pour assurer une haute disponibilité, sont inclus dans l'environnement dans lequel l'application Sage Intacct est construite.

Comment vous assurez-vous que vos fournisseurs respectent vos normes de sécurité ?
Nous appliquons un processus solide d'assurance de la sécurité et de diligence raisonnable pour l'évaluation des risques et l'approbation des fournisseurs. AWS nous fournit régulièrement des preuves de leur conformité continue avec les cadres et les normes de sécurité de pointe du secteur. Pour en savoir plus : https://aws.amazon.com/compliance/programs

Nous contrôlons les performances d'AWS au moyen de rapports d'audit réguliers et de réunions de gestion de l'examen des fournisseurs. Les rapports de conformité en matière de sécurité peuvent être mis à disposition sur demande, après signature d'un accord de confidentialité.

Qu'est-ce qui est inclus dans vos contrats avec les fournisseurs ?
Il existe des clauses requises par la législation française en matière de lutte contre la corruption, d'esclavage moderne, de fiscalité, de traitement des données, de sécurité, de confidentialité et de protection des données.

Comment nous sécurisons vos données

Comment assurez-vous la sécurité du réseau ?
L'application Sage Intacct est hébergée sur la plateforme AWS qui est accessible via l'Internet public.

Sage Intacct est servie à 100 % par HTTPS, avec des connexions sécurisées par les dernières versions de TLS, les anciennes versions étant désactivées. Toutes les données envoyées vers ou depuis Sage Intacct sont chiffrées en transit avec des clés de longueur minimales de 2048bits.

Nos points d'extrémité d'API et d'application sont uniquement accessibles en TLS/SSL et obtiennent la note "A" lors des tests de SSL Labs. Cela signifie que nous n'utilisons que des suites de chiffrement fortes.

Pour protéger le périmètre de l'environnement, AWS utilise des routeurs de périphérie, des pare-feu dynamiques et des systèmes de détection d'intrusion (IDS). Seul le trafic réseau approuvé passe par les pare-feu du périmètre.

L'environnement de l'application est entièrement sécurisé par rapport à Internet et seuls les services requis sont autorisés.

Comment réagissez-vous aux alertes la sécurité ?
AWS dispose d'équipes de réponse aux incidents de sécurité informatique (CSIRT) dédiées, disponibles 24 heures sur 24 et 7 jours sur 7.

Elles supervisent et répondent immédiatement aux informations provenant des principaux outils de sécurité réseau, notamment les systèmes de détection d'intrusion, la gestion des événements de sécurité, la surveillance des menaces par des autorités tierces et la surveillance du périmètre.

Par ailleurs, Sage dispose de sa propre équipe de cyberdéfense et nous avons armé un SOC permettant d’assurer une détection et réponse aux incidents 24h sur 24, 7j sur 7.

Comment se protéger contre les logiciels malveillants ?
Pour protéger les actifs tels que les ordinateurs portables et les systèmes de messagerie, Sage a mis en place une série de contrôles techniques pour se prémunir contre les logiciels malveillants et leurs effets. Une approche de défense en profondeur par couches est utilisée en combinaison avec un programme de sensibilisation des utilisateurs.

Les appareils des employés sont protégés par une suite de systèmes de protection des points d'extrémité de l'entreprise gérés par notre équipe CDO (Cyber Defence Operations) 24 heures sur 24 et 7 jours sur 7, avec une surveillance, des alertes et des rapports en temps réel.

Nos systèmes de messagerie électronique sont dotés d'une protection technologique à plusieurs niveaux, déployée de manière appropriée, tant pour les messages entrants que pour les messages sortants. Nous menons régulièrement des programmes d'éducation et de formation pour tester l'efficacité de nos campagnes de sécurité, notamment contre les logiciels malveillants et les attaques par hameçonnage.

Où stockez-vous les données des clients ?
Toutes les données sont stockées et traitées dans les infrastructures AWS et non dans les locaux de Sage. Actuellement, le centre principal se trouve en Irlande et le centre de secours pour la continuité des activités se trouve à Frankfort.

Pour nous conformer aux lois sur la protection des données, nous avons mis en place des accords (avec des garanties supplémentaires le cas échéant) pour permettre des flux de données qui identifient le centre de données correct pour les informations sur les clients, lorsque les utilisateurs accèdent aux données à partir d'autres sites.

Quel niveau de chiffrement des données utilisez-vous ?
Toutes les données envoyées vers ou depuis Sage Intacct sont chiffrées en transit à l'aide d'un algorithme symétrique muni d'une clé de 256 bits, et des clés aymétriques de 2048 bits pour l'échange de la clé symétrique.

Lorsque le chiffrement au repos est exigé par la loi ou la réglementation, nos données de production et nos sauvegardes peuvent être chiffrées au repos à l'aide d'un algorithme par bloc AES-256.

Dans Sage Intacct, les données des clients ne sont pas actuellement chiffrées par défaut, en raison de la force des contrôles de sécurité physiques et numériques. Ceci est entièrement conforme aux normes de sécurité internationales et aux directives telles que l'ACC, le GDPR et l'ICO. Toutefois, si les clients souhaitent chiffrer des données sensibles, nous pouvons les aider à le faire.

Tous les ordinateurs portables de Sage sont protégés par un chiffrement complet du disque et une suite d'outils de protection des points finaux protège nos appareils contre de multiples menaces de sécurité.

Qui a accès aux données des clients ?
Seuls les employés qui ont besoin d'accéder aux systèmes de traitement et de stockage des données des clients ont accès aux données des clients, afin de fournir le service que nous avons contracté. Les employés autorisés suivent une formation, un accompagnement et un mentorat avant d'être autorisés à accéder aux données.

Les autorisations sont régulièrement réexaminées en appliquant le principe du moindre privilège. Les employés des opérations techniques d'AWS doivent s'authentifier pour accéder aux systèmes de production et les gérer. Il n'y a pas de fonction copier-coller dans l'environnement hébergé.

Autorisez-vous l'accès à distance ?
Il n'y a pas d'accès à distance à la plateforme backend. Tout accès se fait via le portail web.

Quel type d'authentification utilisez-vous ?
Nous avons des politiques de mots de passe forts et une authentification multi-facteurs sur AWS et Sage Intacct pour s'assurer que l'accès aux services cloud est protégé. Nous appliquons MFA dans le système d'administration de Sage Intacct pour chaque employé de Sage. Nous utilisons une authentification de haute assurance pour les ressources sécurisées, qui demande également une vérification de l'identité.

Qu'en est-il des données stockées sur un appareil mobile ou un ordinateur portable ?
Toutes les données que vous partagez avec nous dans le cadre de la mise en œuvre de votre service seront enregistrées, puis supprimées en toute sécurité selon les meilleures pratiques du secteur une fois que l'application aura été mise en service.

En tant que responsable du traitement des données, le client déterminera les enregistrements de données nécessaires et approuvera ce processus si nécessaire. Nous effaçons de manière sécurisée tous les appareils Sage avant de les mettre au rebut et nous obtenons des certificats de destruction.

Quelle est votre politique en matière de noms d'utilisateur et de mots de passe ?
Sage vous donne un nom d'utilisateur et un mot de passe uniques, ainsi que des politiques de mot de passe strictes. Nous pouvons vous aider à configurer vos paramètres de sécurité pour répondre à vos propres exigences en matière de politique de sécurité.

Sage Intacct prend en charge l'authentification unique (SSO). Notre site d'assistance contient des informations sur la configuration SAML. Vous pouvez configurer le SSO en utilisant votre fournisseur d'identité SSO existant s'il prend en charge le protocole SAML 2.0 pour l'authentification et l'autorisation des utilisateurs.

https://www.intacct.com/ia/docs/en_AU/help_ action/Administration/Sign-in/Single_sign_on/ aa-TOC-sso.htm

Microsoft propose un tutoriel montrant comment intégrer Sage Intacct à Azure Active Directory :

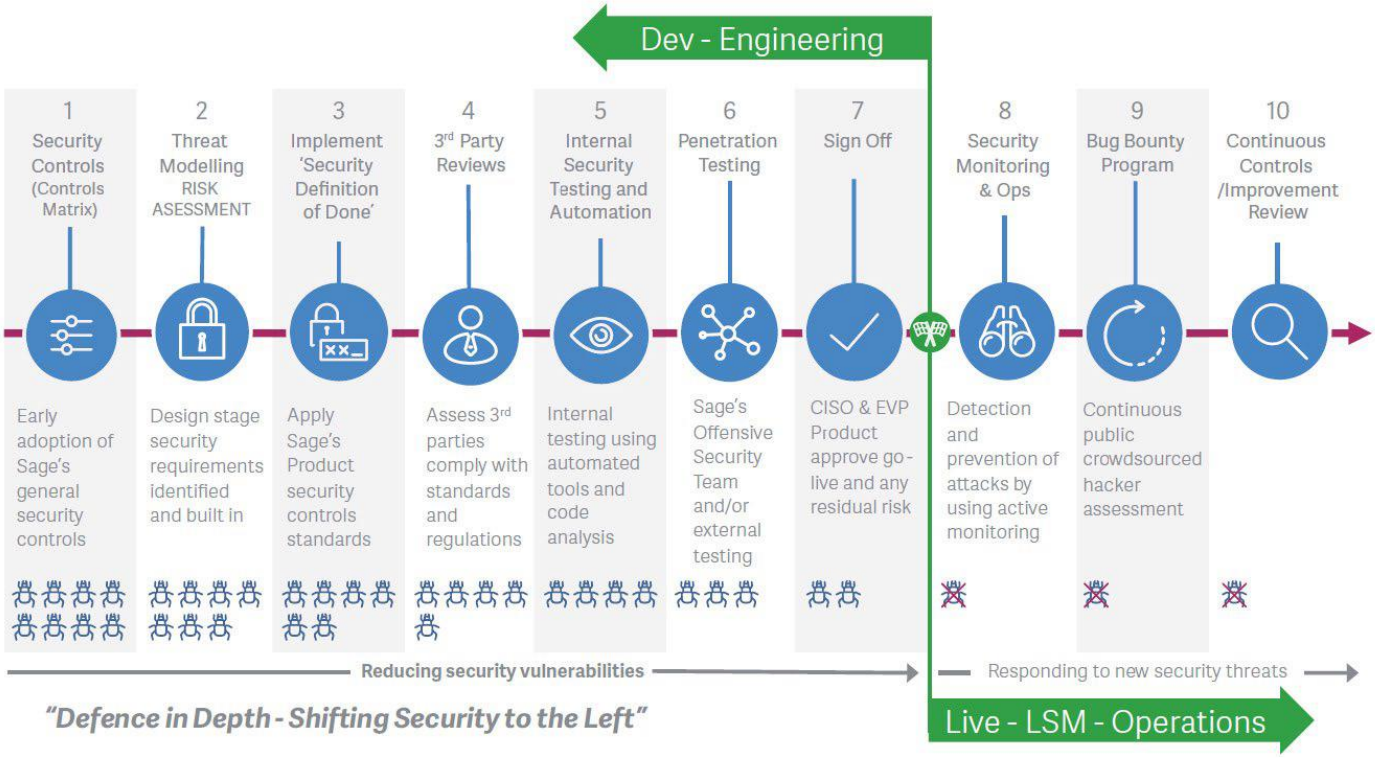
https://docs.microsoft.com/en-us/azure/active-directory/saas-apps/intacct-tutorial

Développement sécurisé de l'application

Disposez-vous d'un processus clairement défini pour le développement sécurisé de logiciels ?
Sage dispose d'un cycle de développement logiciel sécurisé (SDLC) qui permet d'effectuer des changements et de publier des versions de manière sécurisée et contrôlée. Ce cycle couvre la conception, le développement, les tests d'assurance qualité et la publication, la sécurité étant prise en compte tout au long du cycle de vie.

Sage a élaboré un ensemble de politiques, de normes et de processus de développement de logiciels sécurisés pour soutenir les équipes d'ingénieurs produits, y compris les principes de conception de l'architecture et du développement, la gestion du code source, la cryptographie, la conservation des données et les contrôles d'accès. Toute la documentation est publiée sur le portail interne des développeurs de Sage.

Vous trouverez ci-dessous un diagramme décrivant le cycle de vie du développement de logiciels sécurisés de Sage :



Quelle est la fréquence des mises à jour de votre produit ?
Nous avons mis en place un système d'automatisation fonctionnel et fréquemment utilisé afin de pouvoir déployer en toute sécurité et fiabilité des modifications à notre application en l'espace de quelques minutes.

Sage Intacct publie des mises à jour de ses services chaque trimestre. Ces mises à jour sont automatiques, ne nécessitent aucune action de votre part, et incluent de nouvelles fonctionnalités significatives et des améliorations du produit.

Nous publions nos notes de mise à jour ici :

https://www-p04.intacct.com/ia/docs/en_GB/releasenotes/all-release-notes.htm

Comment gérez-vous les changements en toute sécurité ?
Les mises à jour logicielles sont strictement contrôlées sur la plateforme AWS, avec des tests automatisés et des contrôles de sécurité. Les changements et les versions sont gérés par le SDLC de Sage, sont strictement contrôlés et un historique de tous les changements et approbations est enregistré dans nos systèmes de gestion des changements, de gestion des cas et de contrôle des versions.

Tous les changements apportés à l'environnement en nuage de la plateforme doivent être documentés dans le ticket de changement : résumé du risque, gravité de l'impact, étendue de l'impact, plan de vérification, plan de secours.

Sage teste-t-il ses logiciels pour détecter les failles de sécurité ?
Sage utilise une suite d'outils de sécurité d'entreprise pour les tests de sécurité des applications et la gestion des vulnérabilités, et nos normes de développement de logiciels sécurisés et de gestion des vulnérabilités techniques sont alignées sur les normes et les meilleures pratiques de l'industrie (par exemple, ISO 27001, OWASP) pour garantir que les vulnérabilités sont corrigées.

Les environnements de développement sont-ils séparés des systèmes de production ?
Les systèmes de production ne sont jamais utilisés pour le développement ou les tests.

Procédez-vous à des évaluations externes des menaces ?
Sage effectue régulièrement des évaluations des menaces et des risques de sécurité sur les systèmes d'information critiques en utilisant une méthodologie d'évaluation des risques standard de l'industrie, et la modélisation des menaces est incorporée dans la conception de l'application.

Nous pouvons vous fournir des rapports de conformité sur les résultats des tests si vous signez un accord de confidentialité. Vous pouvez également trouver toutes les informations relatives à la conformité AWS ici :

https://aws.amazon.com/compliance/

Sécurité des centres de traitement

Comment vous prémunissez-vous contre les accès non autorisés et les vols dans les centres de données ?

AWS est hébergé dans des centres de données dédiés de premier plan, situés dans des conditions optimales de sécurité et d'intervention en cas d'urgence. La sécurité physique des centres de données AWS commence au niveau du périmètre. Cette couche comprend un certain nombre de dispositifs de sécurité en fonction de l'emplacement, tels que des agents de sécurité, des clôtures, des flux de sécurité, une technologie de détection des intrusions et d'autres mesures de sécurité.

Le système AWS limite l'accès physique aux personnes qui doivent se trouver sur un site pour une raison professionnelle justifiée. Les employés et les fournisseurs qui ont besoin d'être présents dans un centre de données doivent d'abord faire une demande d'accès et fournir une justification professionnelle valable. La demande est examinée par un personnel spécialement désigné, y compris un responsable d'accès à la zone. Si l'accès est accordé, il est révoqué une fois les travaux nécessaires terminés.

Les centres d'opérations de sécurité d'AWS sont situés dans le monde entier et sont responsables de la surveillance, du triage et de l'exécution des programmes de sécurité pour nos centres de données. Ils supervisent la gestion de l'accès physique et la réponse à la détection des intrusions, tout en fournissant une assistance globale, 24 heures sur 24 et 7 jours sur 7, aux équipes de sécurité des centres de données sur site. En bref, ils soutiennent notre sécurité par des activités de surveillance continue telles que le suivi des activités d'accès, la révocation des autorisations d'accès et la disponibilité pour répondre à un incident de sécurité potentiel et l'analyser.

Comme pour les autres couches, l'accès à la couche infrastructure est limité en fonction des besoins de l'entreprise. En mettant en œuvre un examen de l'accès couche par couche, le droit d'accéder à chaque couche n'est pas accordé par défaut. L'accès à une couche particulière n'est accordé que s'il existe un besoin spécifique d'accéder à cette couche.

La couche de données est le point de protection le plus critique, car c'est la seule zone où se trouvent les données des clients. La protection commence par la restriction de l'accès et le maintien d'une séparation des privilèges pour chaque couche. En outre, des dispositifs de détection des menaces, une surveillance vidéo et des protocoles de système sont déployés, ce qui renforce la protection de cette couche.

Les supports de stockage utilisés pour conserver les données des clients sont classés par AWS comme étant critiques et traités en conséquence, comme ayant un impact élevé, tout au long de leur cycle de vie. Nous appliquons des normes rigoureuses en matière d'installation, d'entretien et de destruction des dispositifs lorsqu'ils ne sont plus utiles. Lorsqu'un dispositif de stockage a atteint la fin de sa durée de vie utile, AWS déclasse les supports en utilisant les techniques détaillées dans le document NIST 800-88. Les supports qui ont stocké les données des clients ne sont pas retirés du contrôle d'AWS tant qu'ils n'ont pas été mis hors service en toute sécurité.

Comment contrôlez-vous l'environnement des centres de données ?

Cette couche est consacrée aux considérations environnementales, depuis la sélection du site et la construction jusqu'à l'exploitation et la durabilité. AWS choisit soigneusement l'emplacement de ses centres de données afin d'atténuer les risques environnementaux, tels que les inondations, les conditions météorologiques extrêmes et l'activité sismique.

AWS se prépare de manière proactive aux menaces environnementales potentielles, telles que les catastrophes naturelles et les incendies. L'installation de capteurs automatiques et d'équipements réactifs est l'un des moyens utilisés pour protéger les centres de données. Les dispositifs de détection de l'eau peuvent alerter les employés en cas de problème, tandis que des pompes automatiques s'efforcent d'évacuer le liquide et de prévenir les dommages. De même, les équipements automatiques de détection et d'extinction des incendies réduisent les risques et peuvent avertir les employés d'AWS et les pompiers en cas de problème.

Outre la prise en compte des risques environnementaux, des considérations relatives au développement durable sont également intégrées dans la conception du centre de données. AWS s'est engagé à long terme à utiliser 100 % d'énergie renouvelable. Lorsque les entreprises passent d'une infrastructure sur site au cloud AWS, elles réduisent généralement leurs émissions de carbone de 88 %, car nos centres de données peuvent offrir des économies d'échelle sur le plan environnemental. Les organisations utilisent généralement 77 % de serveurs en moins, 84 % d'énergie en moins et exploitent un mélange d'énergie solaire et éolienne 28 % plus propre dans le nuage AWS que dans leurs propres centres de données. Pour en savoir plus sur nos initiatives en matière de développement durable et suivre nos progrès, consultez le site https://sustainability.aboutamazon.co.uk/environment/the-cloud.

Continuité et reprise d’activité

Comment assurez-vous la disponibilité du service Sage Intacct ?

L'application Sage Intacct étant hébergée sur AWS, Sage peut tirer parti des capacités de continuité des activités et de gestion des sinistres offertes par la plateforme pour s'assurer que le service reste disponible. De plus amples détails sur les capacités de continuité d'activité d'AWS sont disponibles ici : https://aws.amazon.com/compliance/data-center/controls/.

Le plan de continuité des activités d'AWS décrit les mesures à prendre pour éviter et réduire les perturbations de l'environnement. Il comprend des détails opérationnels sur les mesures à prendre avant, pendant et après un événement. Le plan de continuité des activités est étayé par des tests comprenant des simulations de différents scénarios. Pendant et après les tests, le SAP documente les performances des personnes et des processus, les mesures correctives et les leçons tirées de l'expérience, dans un souci d'amélioration continue.

L'eau, l'électricité, les télécommunications et la connectivité internet sont conçues de manière redondante, afin que nous puissions continuer à fonctionner en cas d'urgence. Les systèmes d'alimentation électrique sont conçus pour être entièrement redondants, de sorte qu'en cas de perturbation, des unités d'alimentation sans interruption peuvent être engagées pour certaines fonctions, tandis que des générateurs peuvent fournir une alimentation de secours pour l'ensemble de l'installation. Le personnel et les systèmes surveillent et contrôlent la température et l'humidité afin d'éviter toute surchauffe, ce qui réduit encore les risques d'interruption de service.

Comment les sauvegardes sont-elles gérées et quel est le temps de disponibilité ?

Sage Intacct adhère et maintient des mesures pour sécuriser les sauvegardes de données.

La base de données de Sage Intacct est sauvegardée et stockée sur AWS S3. En plus de S3, nous prenons également des instantanés AWS quotidiens de tous les serveurs de base de données (qui sont également stockés dans leur région AWS respective).

Avez-vous un plan de reprise d’activité ?

La combinaison de toutes ces sauvegardes nous permet de restaurer les serveurs de base de données pour différents types de défaillances (serveur unique, plaque régionale, récupération ponctuelle, etc.) et de fournir un objectif de point de restauration (RPO) ne dépassant pas 4 heures et un objectif de temps de restauration (RTO) ne dépassant pas 24 heures.

Outre les bases de données, tous les autres types de serveurs traitant les données des clients sont sauvegardés via des instantanés AWS. Il n'y a pas de sauvegardes sur bande (et elles ne sont pas nécessaires). La transmission des données se fait via des protocoles sécurisés.

Nous effectuons des efforts commercialement raisonnables pour maintenir un temps de disponibilité de 99,8 %/mois calendaire.

Disposez-vous d'un plan de continuité des activités (PCA) ?

Sage dispose d'une politique de continuité des activités documentée, soutenue par des plans de continuité des activités mondiaux, régionaux et locaux. L'équipe de gestion de crise de Sage est composée de représentants de notre comité exécutif et d'experts en matière de risques, de sécurité, de voyages, de personnel, de biens, d'informatique et de communication.

Le plan de continuité des activités d'AWS est un guide des processus opérationnels qui explique comment éviter et réduire les perturbations dues aux catastrophes naturelles, avec des étapes détaillées à suivre avant, pendant et après un événement. Afin d'atténuer les effets de l'imprévu et de s'y préparer, AWS teste régulièrement le plan de continuité des activités en organisant des exercices qui simulent différents scénarios.

Nous documentons les performances de notre personnel et de nos processus, puis nous débriefons sur les enseignements tirés et les mesures correctives éventuellement nécessaires pour améliorer notre taux de réponse. Nous sommes formés et prêts à rebondir rapidement en cas de perturbation, ce qui inclut un processus de récupération méthodique. afin de minimiser les temps d'arrêt supplémentaires dus à des erreurs.

Comment nous renvoyer les données en cas de fin de contrat ?

Les données du client peuvent être exportées à tout moment. Nous ne supprimerons pas les données client de notre environnement de production pendant les 90 jours suivant la résiliation ou l'expiration de l'accord, et nous pourrons vous aider à exporter les données client pendant cette période à notre tarif horaire standard de conseil. Après cette période de 90 jours, nous aurons le droit de supprimer toutes les données client et n'aurons plus l'obligation de les mettre à votre disposition.

Pour de plus amples informations, veuillez consulter : https://www.sageintacct.com/customer-terms-uki/tos

Gestion des risques et incidents

Comment Sage gère-t-il les risques ?

Sage dispose d'une politique de gestion des risques documentée, détenue par l'équipe Business Integrity and Assurance, qui est responsable de la supervision de tous les risques commerciaux, avec des exigences détaillées en matière de reporting, d'enregistrement, d'évaluation et de gestion des risques dans l'ensemble de l'entreprise. En outre, Sage Intacct tient un registre des risques liés aux actifs d'information applicables au service. Des responsables des risques liés à l'information sont désignés pour s'assurer que les risques sont traités de manière appropriée et qu'ils sont transmis au Registre mondial des risques si nécessaire.

Tous les risques sont enregistrés dans l'outil Sage Governance, Risk and Compliance (Sage GRC), et tous les collègues reçoivent une formation régulière pour s'assurer qu'ils sont conscients des risques et qu'ils savent qu'il est important de les identifier, de les signaler et de les gérer.

Quelle est la procédure de gestion des incidents et de notification des violations ?

Notre processus documenté comprend des procédures de signalement, d'évaluation, de confinement et de résolution, et nous conservons un registre détaillé de tous les incidents.

Nous vérifions le processus chaque année, ou plus tôt en cas de changement important. Les incidents sont signalés aux parties prenantes et aux clients concernés (le cas échéant) en temps voulu et conformément à nos obligations légales et réglementaires.

Sage dispose d'une politique de gestion des incidents, des urgences et des crises parrainée par la direction et approuvée au niveau mondial, qui inclut la gestion des violations de données.

En cas de violation de données suspectée ou confirmée, le processus d'incident est invoqué avec le soutien supplémentaire d'experts juridiques spécialisés. Si la violation doit être notifiée à l'ANSSI, nous le ferons conformément à nos obligations légales et réglementaires.

Protection des données, respect de la vie privé et conformité

Quels types de données stockez-vous ?

C'est à vous, le client, de décider. Sage Intacct peut être configuré pour vous permettre de collecter et de contrôler vos données et de vous assurer qu'elles sont complètes, adéquates et exactes pour vos besoins.

Sage Intacct est-il un contrôleur ou un processeur de données ?

Sage Intacct agit en tant que “processeur” de données. Les clients de Sage Intacct sont les contrôleurs de données - vous déterminez les données que vous soumettez en tant qu'informations d'entreprise et personnelles.

Nous avons effectué des évaluations de l'impact sur la vie privée des produits pour nous aider à créer des fonctionnalités qui facilitent votre travail en tant que responsable du traitement des données. Notre produit est conçu pour intégrer la protection de la vie privée dès la conception.

Quels sont vos principes en matière de protection de la vie privée en tant que responsable du traitement des données des clients ?

Nous prenons la confidentialité des données très au sérieux et nous adhérons à toutes les obligations légales et réglementaires qui nous sont conférées en tant que sous-traitant. Nous agissons conformément aux instructions de votre client, telles qu'elles sont détaillées dans l'accord (qui comprend les conditions générales et l'avenant relatif à la protection des données).

Vous êtes responsable de l'exactitude, de la qualité, de l'intégrité, de la fiabilité et de la pertinence des données soumises. Vous devez respecter les lois applicables dans votre utilisation des services Sage.

Qu'en est-il des demandes d'accès et des droits similaires ?

Nous traiterons les demandes d'accès des personnes concernées conformément aux lois sur la protection des données. Dans la mesure où nous sommes un contrôleur de données, nous serons responsables du traitement de ces demandes. Lorsque nous sommes un processeur de données, nous vous aiderons, en tant que responsable du traitement, à traiter les demandes. Sage Intacct propose également une interface en libre-service qui permet aux utilisateurs d'accéder à leurs propres données. Ils peuvent accéder à leurs propres informations et les mettre à jour si nécessaire. Vous pouvez également récupérer des rapports plus complets pour répondre à des demandes d'accès formelles. Vous pouvez gérer les données à un niveau granulaire, pour effectuer des rectifications ou des demandes d'effacement.

Quelle est la juridiction compétente en matière de conformité des données ?

À des fins de sauvegarde, la réplication peut se faire vers une autre juridiction s'il n'y a pas d'installation locale de sauvegarde sécurisée disponible. Sage a conclu un contrat avec AWS qui met en place un cadre juridique approprié basé sur les règles d'entreprise contraignantes de l'UE et les clauses contractuelles standard. Tous nos contrats clients sont conformes à l'article 28 du GDPR.

Les clients peuvent configurer la fonctionnalité de sécurité de l'application Sage Intacct pour se conformer aux lois locales sur la protection des données, y compris la RGPD.

Tous les détails sont disponibles sur https://aws.amazon.com/compliance.

Comment maintenez-vous votre conformité légale et réglementaire ?

Sage tient à jour un registre juridique et de conformité et utilise le Sage Compliance Hub pour aider les collègues à identifier les changements réglementaires ou législatifs susceptibles d'avoir un impact sur le contenu des politiques ou des procédures. Il les aide également à répondre efficacement aux risques émergents via le cadre de gestion des risques globaux de Sage.

Les équipes Sage Legal et Data Privacy offrent un soutien et des conseils d'experts à tous les collègues, et des formations régulières sont organisées pour les sensibiliser.

Qui est le délégué à la protection des données (DPO) de Sage ?

Stephen Hunt, vice-président chargé de la confidentialité et de la protection des données - contactez Stephen à l'adresse globalprivacy@sage.com.

Quelle est votre politique en matière de RGPD ?

Sage dispose d'une politique interne de protection des données applicable à tous les employés qui définit clairement nos obligations en matière de protection des données et une formation régulière de sensibilisation et de mise à jour est obligatoire. Les détails complets de notre conformité et les outils mis à la disposition des clients pour les aider à gérer leur conformité sont disponibles ici :

https://www.sage.com/fr-fr/rgpd/

Avez-vous publié des avis de confidentialité ?

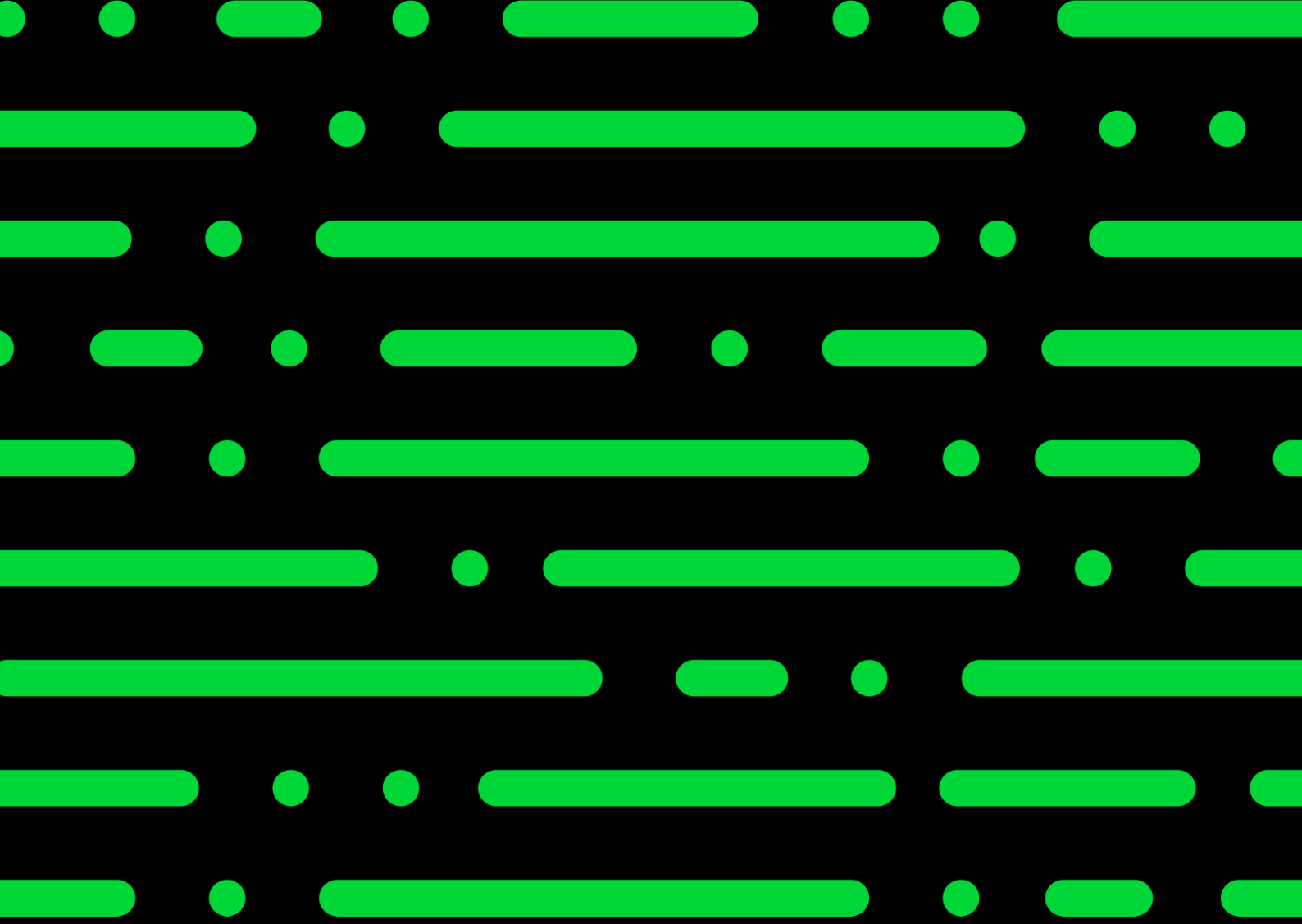
Sage Intacct est le fournisseur du produit, et l'avis de confidentialité de Sage se trouve ici : https://www.sage.com/fr-fr/informations-legales/protection-vie-privee-cookies/cookies/

Le fournisseur de la plateforme est AWS - sa politique de confidentialité se trouve à l'adresse https://aws.amazon.com/privacy.

Sage Intacct conserve ses dernières directives en ligne, accessibles au public via le Programme de sécurité

de l'information.

https://www.sageintacct.com/information-security-management-program.



sage.com
0191 479 5911

Sage