Sage Intacct

Programme de management de la cybersécurité

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

Objectif

Bien que l'architecture SaaS de Sage Intacct permette flexibilité et évolutivité, la sécurité des données sensibles de nos clients est un élément central de notre philosophie. Ce document illustre et explique l'architecture, les contrôles et les pratiques de sécurité de Sage Intacct pour tous les environnements de production de Sage Intacct core ERP.

Personnel et gestion de la sécurité

Sage emploie des professionnels de la sécurité de l'information dévoués, expérimentés et certifiés (CISSP) qui ont la responsabilité de développer et de diriger le programme de sécurité de Sage Intacct. Ce programme englobe la sécurité physique et logique de l'application et de l'infrastructure Sage Intacct, ainsi que des systèmes informatiques internes de Sage Intacct.

Politiques et processus de sécurité

Sage maintient une série de politiques et de procédures pertinentes liées à la sécurité. Les mises à jour des politiques et procédures sont effectuées au moins une fois par an avec les approbations et les contrôles de documentation appropriés. Voici une liste des politiques :

Nom	Périmètre
Politique d'utilisation acceptable	Politique générale de sécurité couvrant les sujets suivants : • Propriété des données informatiques de Sage Intacct et droits de propriété intellectuelle • Protection des données • Utilisation personnelle • Représentation publique de Sage Intacct • Applications interdites • Utilisation inappropriée • Anti-virus et correctifs • Appareils mobiles • Mots de passe et informations d'identification de l'utilisateur • Accès à distance • Technologie "Push" • Conformité (i.e. PCI, HIPAA, GDPR) • Courrier électronique • Outils de compromission de la sécurité

	• Transfert électronique ou stockage d'informations confidentielles de l'entreprise
Standards de configuration systèmes et réseaux	Les normes de configuration doivent être maintenues pour toutes les ressources/applications critiques, conformément aux normes de référence définies par l'industrie et les organisations gouvernemtales.
Politique et procédures de sauvegarde système	Spécifie la fréquence des sauvegardes, les données qui sont sauvegardées, l'emplacement et le déplacement sécurisé des données de sauvegarde et les exigences en matière de tests réguliers.
Politique et procédures d'analyse des vulnérabilités et de la gestion des menaces	Détermine la responsabilité, l'étendue et la fréquence des audits et des évaluations des vulnérabilités.
Politique de sécurité des applications	Politique et normes, basées sur l'OWASP et d'autres bonnes pratiques générales, pour le développement sécurisé d'applications.
Contrôle des changements / Gestion des problèmes	Définit les exigences en matière de gestion du changement et le processus de gestion du changement pour l'infrastructure technique, l'ingénierie et les opérations.
Évaluation interne de la vulnérabilité des systèmes, des applications et des réseaux	Définit l'autorité et la portée des évaluations internes et des tests de pénétration de nos applications, de notre réseau et de notre infrastructure.
Gestion des médias	Définit les exigences permettant de s'assurer que les données sensibles et les données clients de Sage Intacct sont définitivement supprimées des supports avant leur élimination, leur maintenance ou leur réutilisation.
Document sur le processus de développement et de cycle de vie des systèmes (SDLC)	Comprend la planification, la conception, la construction, les tests de sécurité et autres et la livraison de divers composants de notre application.
Plan de continuité des activités (PCA) et plan de reprise d'activité (PRA)	Exigences et processus à suivre en cas de sinistre ou d'autre événement obligeant Sage Intacct à assurer la continuité des activités afin de respecter les accords de niveau de service.
Mots de passe	Politique et normes relatives à la création, à l'administration et à la gestion des mots de passe, à la protection de ces mots de passe et à la fréquence des changements de mots de passe.
Dispositifs mobiles	Décrit la politique de sécurité concernant les dispositifs mobiles portables.
Fin de contrat	Régit les mesures à prendre en cas de cessation volontaire ou involontaire de l'emploi ou de toute autre affiliation à Sage Intacct.
Accès aux installations	Fournit des exigences de sécurité physique pour l'accès aux installations de Sage.
Classification des informations	Conseils relatifs à la classification des actifs immatériels de Sage

	Intacct
Antivirus et gestion des correctifs	Décrit les exigences en matière de protection des postes de travail et serveurs (c'est-à-dire l'antivirus et les correctifs de sécurité des logiciels).
Sensibilisation à la sécurité	Définit les exigences relatives au programme de sensibilisation et de formation à la sécurité de l'information de Sage.
Politique de protection de la vie privée	Définit les règles en conformité avec la réglementation RGPD.

Formation / Sensibilisation

Sage exige que tous les employés aient suivi une formation périodique sur la sécurité au cours des douze (12) mois précédents. Cette formation à la sécurité comprend, sans s'y limiter : l'utilisation acceptable, l'ingénierie sociale, la sécurité du personnel, la protection des données, PCI, HIPAA, RGPD, et la réponse aux incidents. Les développeurs d'applications et les ingénieurs de Sage Intacct reçoivent une formation supplémentaire en sécurité liée au développement d'applications pour inclure (au minimum) les dix principaux risques de sécurité décrits par l'Open Web Application Security Project (OWASP Top 10). Outre la formation formelle à la sécurité, les employés sont sensibilisés à la sécurité lors de l'orientation des nouveaux embauchés et tout au long de l'année par le biais de rappels par courrier électronique et d'affiches/moniteurs.

Réponse aux incidents de sécurité

Sage maintient un plan de réponse aux incidents de sécurité, qui détaille les procédures à suivre en cas d'accès non autorisé réel ou raisonnablement soupçonné ou d'utilisation de Sage Intacct ou des données des clients, y compris, mais sans s'y limiter, la divulgation, le vol ou la manipulation des données qui ont le potentiel de causer un préjudice aux systèmes Sage, aux données ou à la marque Sage Intacct. Notre processus de réponse aux incidents est testé au moins une fois par an et répond aux exigences spécifiques liées à PCI, HIPAA, et GDPR, CCPA et autres réglementations et exigences en matière de sécurité et de confidentialité.

Analyse des journaux

Pour les applications et les systèmes associés à l'accès, au traitement, au stockage, à la communication et/ou à la transmission des données de Sage, Sage Intacct génère des journaux d'audit détaillant l'utilisation, l'accès, la divulgation, le vol, la manipulation et la reproduction. Les journaux d'audit liés à la sécurité sont générés et examinés régulièrement pour détecter des indicateurs de compromission ou d'autres activités suspectes pertinentes. Les journaux sont conservés pendant au moins un an. Si l'examen des journaux d'audit révèle des preuves raisonnables d'un incident de sécurité, des mesures appropriées sont prises conformément au plan d'intervention en cas d'incident de sécurité.

Audit et conformité

Sage effectue divers types d'audits internes et de tiers pour valider la conformité aux exigences applicables. À l'issue de chaque audit, un rapport écrit des conclusions et des recommandations est créé et conservé dans un répertoire central sécurisé. Dans le cas où une non-conformité, une déficience ou une autre constatation est découverte au cours d'un audit, Sage évalue, priorise, atténue ou identifie rapidement les contrôles compensatoires appropriés. Les environnements de production de Sage Intacct en Europe sont inclus dans le champ d'application des certifications et des audits énumérés ci-dessous.

✓ SSAE 18 SOC 1 Type II

Sage maintient une certification SSAE 18 SOC 1Type II d'un cabinet d'audit tiers réputé et indépendant. Nous menons cette activité deux fois par an pour répondre aux exigences des clients en matière de rapports. Le rapport contrôlé est disponible sous NDA pour les parties concernées (y compris les clients et les clients potentiels) sur demande.

✓ SOC 2 Type II

Sage maintient une certification SOC 2 Type II d'un cabinet d'audit tiers réputé et indépendant. Nous menons cette activité une fois par an. Le rapport contrôlé est disponible sous NDA pour les parties concernées (y compris les clients et les clients potentiels) sur demande.

✓ ISAE 3402 / ISAE 3000

La norme internationale sur les missions d'assurance (ISAE) 3402 et 3000 sont des normes d'assurance internationales, qui correspondent respectivement à SSAE 18 et SOC 2. Sage Intacct maintient une certification ISAE 3402 et ISAE 3000 d'un cabinet d'audit tiers réputé et indépendant. Les rapports contrôlés sont disponibles sous NDA pour les parties concernées (y compris les clients et les clients potentiels) sur demande.

✓ PCI-DCC Niveau 1

Sage maintient un statut PCI de niveau 1, qui comprend un audit complet par un évaluateur de sécurité qualifié (QSA), qui émet un rapport de conformité (RoC) et deux attestations à la fois en tant que commerçant et fournisseur de services. Nos attestations de conformité (AoC) sont disponibles sous NDA pour les parties concernées (y compris les clients et les clients potentiels) sur demande.

✓ HIPAA

Le produit Sage Intacct est certifié pour répondre aux exigences de la loi américaine sur la portabilité et la responsabilité de l'assurance maladie.

✓ RGPD / GDPR

Le produit Sage Intacct répond aux exigences du règlement général sur la protection des données (GDPR).

✓ ISO27001

Sage maintient une certification ISO27001 de l’application Sage Intacct, qui est une norme internationale qui définit les exigences d'un système de gestion de la sécurité de l'information (SGSI). Un SGSI est un ensemble de politiques, de procédures, de processus et de systèmes qui gèrent les risques liés à l'information, tels que les cyberattaques, les piratages, les fuites de données ou le vol.

Évaluation des risques et tests d’intrusion

Sage Intacct effectue régulièrement des évaluations des risques et des tests d’intrusion internes et externes par des tiers sur les applications, systèmes et infrastructures de données associés à l'accès, au traitement, au stockage, à la communication et/ou à la transmission des données des clients ou des données sensibles. Un rapport de synthèse indépendant est mis à la disposition des parties concernées (y compris les clients et les clients potentiels) sur demande, sous couvert d'un accord de confidentialité.

Gestion des fournisseurs

Sage Intacct a développé et mis en œuvre un programme visant à évaluer les fournisseurs et partenaires tiers pertinents avant de s'engager dans une relation commerciale et régulièrement par la suite. Notre programme de gestion des fournisseurs adopte une approche basée sur le risque pour évaluer la maturité de la sécurité, la conformité et les caractéristiques et fonctionnalités de sécurité disponibles pour Sage Intacct.

Prévention de la perte de données

Sage Intacct a mis en œuvre une variété de processus et de technologies pour identifier et gérer les événements de perte de données dans les principales applications commerciales internes de Sage Intacct, telles que le courrier électronique d'entreprise et les outils de collaboration sanctionnés.

Réputation numérique / Surveillance de l'intelligence

Sage a déployé une technologie et des processus pour détecter et remédier aux menaces contre l'organisation et ses employés sur les plateformes sociales, mobiles, numériques et de collaboration pour inclure les ressources commerciales ainsi que celles du "dark web".

Transfert de données Sage Intacct

La manipulation et le transfert des données des clients, tant électroniques que sur papier, y compris, mais sans s'y limiter, le transport hors site à des fins de stockage ou de sauvegarde, sont effectués en utilisant des méthodes appropriées à la sensibilité et à la criticité des données. Le processus de traitement et de transport physique des données des clients est documenté et revu régulièrement.

Protection des données

Sage s'engage à respecter les lois sur la protection des données qui s'appliquent à notre activité et à nos opérations. Nous avons mis en place de nombreuses mesures techniques et administratives pour la protection et la sécurité de vos données et nous sommes transparents sur la façon dont nous traitons les données. Notre politique de confidentialité des produits peut être consultée à l'adresse suivante : Politique de confidentialité.

Contrôle d'accès

Tous les employés de Sage doivent disposer d'identifiants et de mots de passe valides pour accéder au réseau d'entreprise Sage, aux applications internes et basées sur SaaS depuis le bureau et/ou à distance via un réseau privé virtuel. En plus du nom d'utilisateur et du mot de passe, l'authentification multifactorielle est requise pour l'accès aux systèmes critiques de l'entreprise. Les identifiants d'utilisateur sont utilisés pour restreindre les privilèges du système en fonction des tâches professionnelles, des responsabilités du projet et d'autres activités commerciales pertinentes. Les politiques de Sage exigent que les utilisateurs se conforment aux politiques du système d'exploitation du réseau en ce qui concerne les identifiants et les mots de passe. Dans la mesure du possible, les mots de passe doivent comporter un nombre minimum de caractères et expirer à intervalles réguliers. Les mots de passe doivent être complexes et comporter une combinaison de chiffres, de lettres et de caractères spéciaux. En outre, si l'utilisateur tente de se connecter en utilisant un mot de passe incorrect plus d'un certain nombre de fois, il sera exclu du système pendant une durée déterminée ou jusqu'à ce que le mot de passe soit réinitialisé manuellement par un administrateur.

Processus de justification et d'autorisation d'accès

Les procédures d'autorisation d'accès sont conformes aux normes suivantes :

- Sage a mis en place un processus conçu pour limiter l'accès aux données des clients au seul personnel autorisé ayant un besoin professionnel pour remplir ses obligations envers les clients.
- Chaque autorisation est approuvée par la direction compétente de Sage. L'autorisation et l'approbation du responsable sont documentées et conservées.
- Sage a mis en place un processus qui supprimera rapidement tout accès pour les employés qui quittent l'entreprise ou changent de poste au sein de l'entreprise et n'ont plus besoin d'accès.
- Une revérification annuelle des personnes ayant accès aux systèmes qui hébergent l’application Sage Intacct ou les données des clients de Sage Intacct est effectuée pour vérifier qu'il n'existe pas de comptes malveillants, obsolètes ou inconnus.
- Sage surveille les comptes utilisés pour la maintenance à distance afin de vérifier qu'ils ne sont activés que pendant la durée nécessaire.

Surveillance des systèmes et des applications

Sage utilise une variété de services de surveillance pour contrôler l'activité du système dans les systèmes de production et d'entreprise. Ces mévanismes suivent et surveillent l'activité des serveurs et des utilisateurs sur les serveurs du réseau Sage, y compris les paramètres de sécurité, la surveillance des

systèmes, l'activité d'accès à distance, la capacité du serveur et les activités liées aux événements du serveur. Les administrateurs système et le personnel de sécurité sont chargés d'examiner les activités surveillées à intervalles réguliers, ainsi que de surveiller les journaux du pare-feu et d'autres activités d'administration du système et du réseau. Les événements sont enregistrés sur un serveur central de journalisation, corrélés au sein d'un SIEM et affichés sur une console, et les alertes pertinentes sont envoyées au personnel chargé des opérations et de la sécurité de Sage.

Chiffrement et gestion des clés

Sage assure la protection des données des clients grâce à une combinaison de contrôles d'accès et de chiffrement.

Le chiffrement est nécessaire si :

- Les données du client sont transmises sur des réseaux publics.
- L'utilisation du chifrrement est exigée par la loi ou la réglementation (par exemple PCI).
- Sage détermine que le chiffrement est nécessaire pour protéger les données des clients.

Lorsque les données sont transmises sur des réseaux publics ou sur des réseaux sans fil privés ou publics, les dispositions suivantes s'appliquent comme indiqué :

- Utilisation d'une cryptographie forte et de techniques de chiffrement (au moins 128 bits) telles que Secure Sockets Layer (SSL/TLS) ou Internet Protocol Security (IPSEC) pour protéger les données sensibles.
- Pour les réseaux sans fil transmettant des données clients, les transmissions sont chiffrées à l'aide de la technologie Wi-Fi Protected Access (WPA) si elle est compatible avec cette technologie, sinon à l'aide de VPN ou de TLS à 128 bits.

Lorsque le chiffrement au repos est exigé par la loi ou la réglementation, ou lorsque Sage détermine que le chiffrement est nécessaire, les mesures suivantes sont mises en œuvre :

- Les données sensibles des clients sont rendues illisibles partout où elles sont stockées (au repos), en utilisant l'une des approches suivantes en fonction des circonstances :
    - Hachures à sens unique (index hachés) telles que SHA256
    - Troncature
    - Cryptographie forte, telle que Triple-DES 128 bits ou AES 256 bits avec les processus et procédures de gestion des clés associés.
- L'accès aux clés est limité au plus petit nombre de personnes possible
- Les clés sont stockées dans le plus petit nombre d'endroits possible en utilisant des mesures conçues pour empêcher toute divulgation non autorisée
- La prévention de la substitution non autorisée des clés
- Le remplacement des clés compromises connues ou présumées

Sécurité des applications

Sage a établi des directives et des processus dans le but d'architecturer, de développer et de maintenir la plateforme et les applications Sage Intacct exemptes de vulnérabilités en matière de sécurité. La sécurité est intégrée dans notre processus de cycle de vie de développement logiciel axé sur l'agilité. Des évaluations internes et tierces régulières sont effectuées, et nous sommes constamment à l'affût des menaces et vulnérabilités nouvelles et émergentes qui pourraient avoir un impact sur l'application Sage Intacct.

Tous les types de travailleurs responsables du développement ou de la maintenance du code sont tenus de :

- Se conformer aux normes de codage sécurisé de Sage Intacct
- Remédier à tout problème de sécurité de l'application découvert en temps opportun
- Suivre une formation et une sensibilisation à la sécurité des applications. Les domaines d'intérêt sont basés sur le Top 10 de l'OWASP et peuvent inclure :
    - Les failles d'injection
    - Authentification et gestion des sessions
    - Les scripts intersites
    - Références directes d'objets non sécurisées
    - Mauvaises configurations de sécurité
    - Exposition de données sensibles
    - Contrôle d'accès
    - Falsification des requêtes intersites
    - Utilisation de composants présentant des vulnérabilités connues
    - Redirections et transferts non validés

Sécurité du réseau et de l'hôte

Sage déploie des capacités raisonnables et efficaces de détection d'intrusion dans le réseau, des pare-feux et une protection antivirus de qualité reconnue. Les systèmes d'exploitation et les applications associés aux données des clients de Sage et aux données sensibles de Sage Intacct sont corrigés dans un délai commercialement raisonnable après que Sage ait eu connaissance de toute vulnérabilité de sécurité ou de la publication de correctifs par les fournisseurs. Sage prend des précautions conçues pour protéger le logiciel, les systèmes ou les réseaux qui peuvent interagir avec les systèmes de Sage Intacct, les réseaux ou toutes les données des clients de Sage Intacct afin qu'ils ne soient pas infectés par des virus informatiques, des logiciels malveillants, des programmes non autorisés ou d'autres composants nuisibles.

✓ **Détection d'intrusion**

Sage met en œuvre un programme de détection d'intrusion comprenant la détection des intrusions dans le réseau, l'analyse des journaux et la surveillance de l'intégrité des données, afin de contrôler tout le trafic réseau associé à l'accès, au traitement, au stockage, à la communication et/ou à la transmission des données des clients de Sage Intacct. Le personnel de Sage est alerté, analyse et, si nécessaire, prend des mesures sur tout indicateur suspect de compromission et maintient à jour tous les moteurs de détection et de prévention des intrusions.

✓ **Pare-feu**

Sage déploie des pare-feux d'inspection de sessions à différents endroits de son infrastructure. Sage Intacct a établi des normes de configuration de pare-feu qui comprennent :

- Une politique de refus par défaut, exigeant uniquement des ports et des protocoles autorisés
- Un processus formel d'approbation et de test de toutes les connexions au réseau externe et de tous les changements apportés à la configuration du pare-feu.
- Des audits réguliers de nos configurations de pare-feu

✓ **Gestion des correctifs et des vulnérabilités**

Sage a mis en place des processus pour :

- Mettre à jour tous les composants du système et les logiciels avec les derniers correctifs de sécurité fournis par le fournisseur.
- Identifier les vulnérabilités de sécurité récemment découvertes (par le biais d'un abonnement à des services d'alerte).
- Mettre à jour les normes pour traiter les vulnérabilités nouvellement découvertes.

✓ **Antivirus**

Sage maintient un logiciel antivirus de qualité reconnue pour se protéger des virus, des vers et d'autres codes malveillants. Un logiciel de détection des virus (lorsqu'il est disponible) est installé et maintenu sur tous les systèmes, y compris ceux qui accèdent, stockent ou traitent les données des clients de Sage Intacct ou d'autres informations sensibles identifiées. Une fois installé, le logiciel antivirus ne doit pas être désactivé. Les logiciels antivirus sont régulièrement mis à jour avec des signatures de virus afin de localiser et/ou de protéger contre les nouveaux virus ou codes malveillants.

✓ **Durcissement du système**

Sage suit les pratiques de l'industrie en ce qui concerne le durcissement du système d'expoitation et de ses composants sur les systèmes hébergeant les données des clients de Sage Intacct, y compris :

- Suppression des fonctionnalités inutiles du système, y compris les scripts, les pilotes, les caractéristiques, les sous-systèmes et les systèmes de fichiers.
- Désactivation des services et protocoles inutiles et non sécurisés.
- Configurations des paramètres de sécurité du système conformément aux meilleures pratiques de l'industrie (NIST, ANSSI, GCHQ).
- Modification des paramètres par défaut fournis par le fournisseur avant que le système ne soit mis en service sur le réseau.

Pour les environnements sans fil, nous modifions les paramètres par défaut du fournisseur, notamment les clés WEP, le SSID par défaut, les mots de passe et les chaînes de communauté SNMP, et nous désactivons les diffusions du SSID. Nous activons la technologie Wi-Fi Protected Access (WPA) pour le chiffrement et l'authentification lorsqu'elle est compatible avec le WPA.

✓ **Routeurs et infrastructure réseau**

Sage Intacct met en œuvre les meilleures pratiques en matière de sécurisation de l'infrastructure réseau, y compris :

- L'installation des derniers correctifs de sécurité fournis par le fournisseur sur tous les dispositifs de l'infrastructure réseau (matériel et logiciel)
- Mise en place d'un processus d'identification des vulnérabilités de sécurité nouvellement découvertes
- L'audit périodique des dispositifs

Courriel

Nous limitons l'accès aux logiciels espions, aux logiciels publicitaires et au webmail en :

- Inspectant le trafic de courrier électronique sur le web à la recherche d'indicateurs d'activité suspecte
- Installant, configurant et entretenant des logiciels anti-espions et anti-malveillants
- Identifiant et en bloquant les attaques par hameçonnage pour le courrier électronique de l'entreprise
- Dispensant une formation pertinente et des avis périodiques aux travailleurs concernant les menaces liées au courrier électronique.

Sécurité physique

Sage a mis en place des mesures de sécurité physique pour contrôler l'accès physique aux bureaux, aux documents papier et aux systèmes informatiques de l'entreprise. En outre, les centres de données de Sage qui stockent ou traitent les données des clients sont conformes à la norme SOC 2 et comprennent les contrôles suivants :

- Accès par badge
- Biométrie
- Pièges à homme (sas bloquants)
- Vidéosurveillance
- Sécurité 24x7
- Contrôles environnementaux rigoureux

Continuité des activités et reprise après sinistre

✓ **Récupération des données**

Sage a la capacité de récupérer les données en cas de sinistre ou à des fins de continuité des activités. Sage maintient un processus de récupération des données, couvrant les procédures de sauvegarde et de restauration des données des clients de Sage Intacct. Pour les données des clients, nos accords de niveau de service incluent à la fois un objectif de point de restauration (RPO) de 4 heures maximum et un objectif de temps de restauration (RTO) de 24 heures maximum.

✓ **Sauvegardes hors site**

Sage adhère et maintient des mesures pour sécuriser les données transportées hors site à des fins d'utilisation, d'hébergement, de sauvegarde et/ou de stockage. Cela inclut :

- Le stockage des supports de sauvegarde dans une installation hors site sécurisée, qui peut être soit une tierce partie alternative, soit une installation de stockage commerciale.
- Le maintien d'un contrôle strict sur la distribution interne ou externe de toutes les sauvegardes de médias qui contiennent des données de clients Sage Intacct.
- Transmission des données via des protocoles sécurisés

Suppression des données et assainissement du matériel

Sage procède à l'assainissement des supports contenant des données Sage Intacct ou des données clients. Les données sont éliminées en utilisant l'une des trois méthodes suivantes :

- Écrasement - Le processus logiciel qui remplace les données précédemment stockées sur les supports de stockage magnétiques par un ensemble prédéterminé de données sans signification, ce qui rend les données irrécupérables.
- Démagnétisation - Exposition du support à des champs magnétiques puissants pour en détruire le contenu. Cette méthode permet d'éliminer toutes les données encore présentes sur le support.
- Destruction physique - Il s'agit du déchiquetage ou de toute autre méthode de destruction physique, y compris les extrêmes de force physique et de température. La destruction physique est effectuée de manière à empêcher toute utilisation ultérieure du support.
- Destructio des clés de chiffrement – Le machines virtuelles de l’infrastructure Sage Intacct sont par défaut entièrement chiffrées. La suppression de la clé de chiffrement des partitions virtuelles empêche tout visualisation ou utilisation des données client en clair (déchiffrées).

Gestion des changements

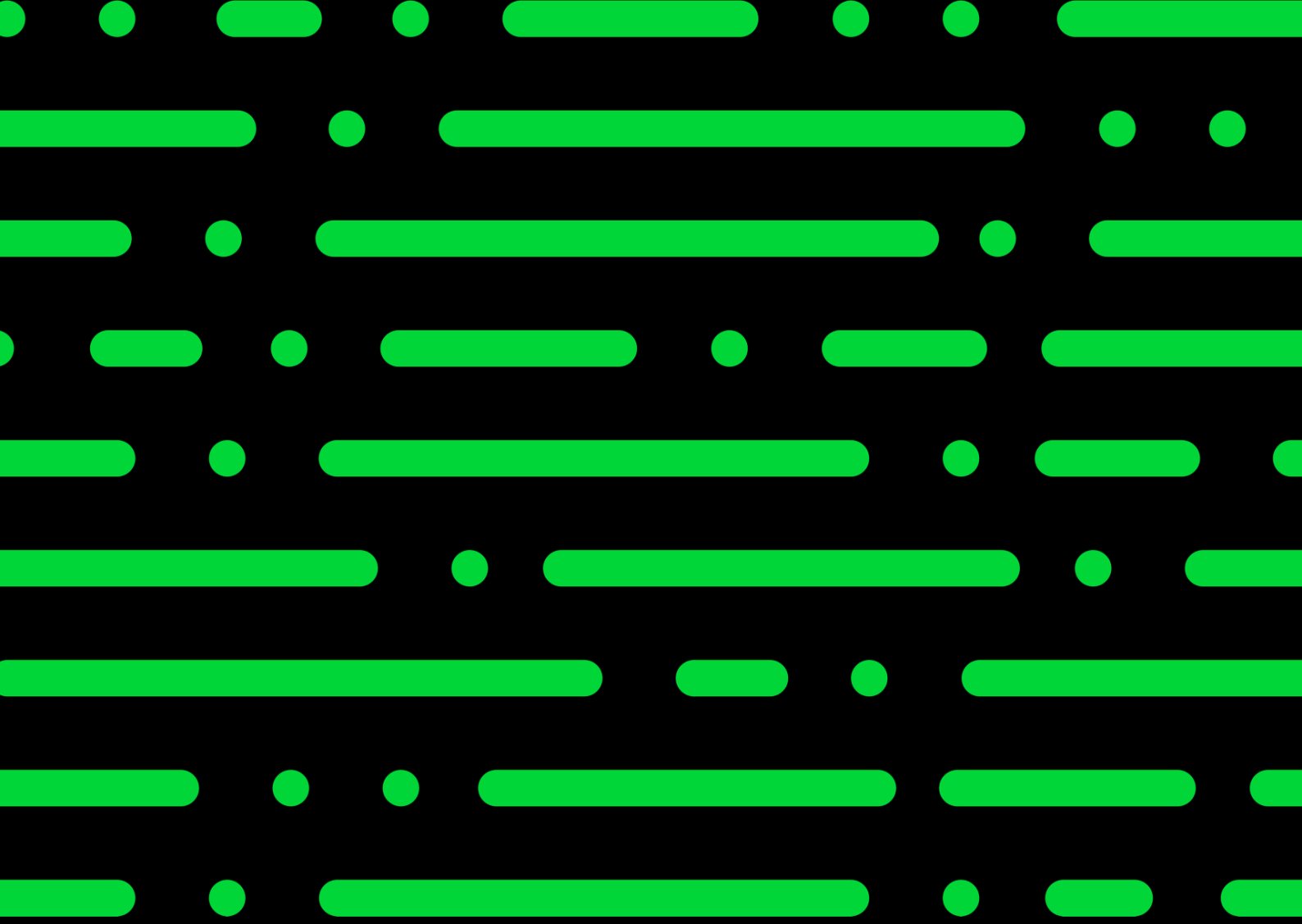
Les modifications apportées aux ressources immatérielles sont gérées et exécutées conformément à un processus défini de gestion des tickets et des changements. Ce processus nous permet d'examiner, d'autoriser, de tester, de documenter et de mettre en œuvre/publier les changements proposés de manière contrôlée, et de surveiller l'état de chaque changement proposé.

Les applications qui transmettent, traitent ou stockent les données des clients de Sage Intacct s'appuient

sur une méthodologie de cycle de vie du développement du système (SDLC) qui encourage la sécurité en tant que fonction intégrée.

Le SDLC comprend, entre autres, les éléments suivants

- Tests de sécurité et analyse du code source des changements de configuration du système et du logiciel
- Des environnements de développement/test et de production distincts
- Séparation des tâches entre les environnements de développement/test et de production
- La suppression des données et des comptes de test avant que les systèmes de production ne deviennent actifs
- Documentation de l'impact
- Approbation de la direction



sage.com
0191 479 5911

Sage