E-BOOK

Sécurité du cloud et confidentialité des données d'Automation 360™

AUTOMATION ANYWHERE

Table des matières

Introduction

Automation 360™ est une plateforme d'automatisation intelligente de bout en bout native du cloud fournie par Automation Anywhere. La plateforme est proposée dans les trois modèles de déploiement que les clients peuvent choisir : dans le cloud ou sur site.

Cloud

En plus de ce modèle cloud qui réduit le coût total de possession (TCO) et permet une mise à l'échelle plus rapide, les clients bénéficient d'une expérience SaaS sécurisée et toujours à jour grâce à l'hébergement et à la gestion complète d'Automation 360 Cloud. Connectez-vous et automatisez : c'est aussi simple que ça.

Sur site

Les clients bénéficient d'une solution entièrement hébergée sur leur infrastructure et d'un accès à des mises à jour régulières. Le déploiement sur site permet aux clients de contrôler la mise en œuvre des mises à jour et des nouvelles capacités d'IA. Bien que ce modèle repose sur une architecture native du cloud et utilise les mêmes fonctionnalités que les autres modèles, l'installation, le déploiement et la mise en œuvre des mises à jour relèvent de la responsabilité du client. Étant donné que ce document porte sur la sécurité et la confidentialité des données pour les déploiements d'Automation 360 dans le cloud, les déploiements sur site ne seront pas abordés plus en détail.

Automation Anywhere fournit une défense en profondeur complète avec une approche multicouche de la sécurité pour Automation 360 Cloud. Ce service est le seul service d'automatisation basé sur le Web et natif du cloud qui soit certifié SOC 2 Type 2, SOC 1 Type 2, ISO 27001 et HITRUST.

Automation 360 Cloud s'appuie sur une architecture de sécurité robuste qui permet une prise en charge complète des principes de sécurité fondamentaux tels que la gestion des identités et des accès, les moindres privilèges et la séparation des fonctions, tout en offrant une protection de bout en bout pour les applications essentielles, en sauvegardant les données sensibles et en garantissant le respect de la confidentialité des données.

Ce document fournit une vue d'ensemble des éléments suivants :

Certifications de sécurité d'Automation Anywhere

Automation Anywhere est une entreprise axée sur la sécurité et la protection de la vie privée. Cela se reflète dans la plateforme Automation 360. Ces efforts continus ont permis d'obtenir de nombreuses certifications en matière de sécurité, de continuité d'activité et de confidentialité des données.

SOC 1 Type 2

L'audit SOC 1 Type 2 est une certification annuelle qui atteste qu'Automation Anywhere dispose des contrôles internes et des processus appropriés en matière de sécurité et de disponibilité afin de garantir la sécurité des données client.

SOC 2 Type 2

La certification SOC 2 Type 2 montre qu'Automation Anywhere adhère aux bonnes pratiques de sécurité et de conformité en matière de disponibilité, de confidentialité, d'intégrité du traitement, de sécurité et de respect de la vie privée et qu'elle a maintenu ce niveau pendant un an après avoir obtenu la certification SOC 2 Type 1.

ISO 27001

Le service d'Automation 360 Cloud est certifié ISO 27001 suite à un audit indépendant qui a attesté du respect des normes de confidentialité, de l'intégrité et de la disponibilité des actifs informationnels.

ISO 22301

La certification ISO 22301:2019 « Sécurité et résilience - Systèmes de management de la continuité d'activité » porte sur le niveau de préparation d'Automation Anywhere à réagir et à se rétablir en cas d'urgence ou de catastrophe.

Attestation de la Cloud Security Alliance

Le registre STAR v.4.0.2 (Security Trust Assurance and Risk), créé par la Cloud Security Alliance, identifie et documente les contrôles de sécurité et de confidentialité mis en place par les organisations dans le domaine de l'informatique dématérialisée. Automation Anywhere est le seul fournisseur d'Enterprise RPA figurant dans le registre. Pour plus de détails, veuillez consulter le STAR Registry.

HITRUST CSF

Le cadre de sécurité commun (CSF) HITRUST est construit sur un ensemble de contrôles de sécurité adaptés à divers cadres de sécurité et de confidentialité reconnus au niveau national et international, tels que HIPAA, PCI, ISO, etc. En obtenant la certification HITRUST CSF, Automation 360 devient la seule solution d'automatisation native du cloud du marché à garantir des contrôles de sécurité et de confidentialité spécifiques au secteur de la santé qui permettent à ses clients de se conformer aux réglementations en vigueur.

Pour plus d'informations, veuillez consulter le site automationanywhere.com/solutions/rpa-security

Opérations et contrôles sécurisés d'Automation 360 Cloud

Les services d'Automation 360 Cloud sont sécurisés sur la base de normes et de cadres du secteur tels que le NIST Cybersecurity Framework, les contrôles de la Cloud Security Alliance (CSA), le Framework d'adoption du Cloud AWS, les lignes de référence du Center for Information Security (CIS), et bien d'autres encore. Cette section décrit les contrôles physiques, logiques et administratifs auxquels qu'Automation Anywhere fait appel pour sécuriser Automation 360 Cloud, notamment l'alignement avec les pratiques de sécurité associées de ses clients.

Dans le cadre de la sécurité du cloud, certains domaines clés de la sécurité sont indispensables en vue de protéger le service cloud. Ils comprennent ce qui suit :

- Gestion du programme de sécurité
- Gestion d'actifs
- Gestion de l'accès
- Sécurité matérielle et des environnements (contrôle d'accès, contrôle de disponibilité)
- Application et développement
- Opérations sécurisées
- Gestion des incidents
- Gestion des fournisseurs
- Continuité d'activité et reprise après sinistre

Gestion du programme de sécurité

Prise en main de la sécurité Automation Anywhere assure la sécurité informatique, la confidentialité des données et les fonctions SecOps qui guident les équipes chargées des opérations du cloud et gère les certifications de sécurité ainsi que les contrôles de confidentialité des données. Tous les membres de cette équipe suivent une formation annuelle sur la sécurité et la protection de la vie privée.

Rôles et responsabilités en matière de sécurité Le personnel CloudOps et Cloud SecOps d'Automation Anywhere sont soumis à des obligations de confidentialité très strictes et aux politiques relatives à la sécurité des services d'Automation 360 : Automation Anywhere applique les principes de protection et de sécurité établis et approuvés par sa direction. Les politiques stipulent les exigences de sécurité de façon claire et concise. Les normes définissent le processus ou la méthodologie à utiliser pour respecter les exigences énoncées dans les politiques.

Gestion des risques liés aux services d'Automation 360 Automation Anywhere effectue des évaluations des principaux domaines de risque associés aux services cloud, y compris (à titre d'exemple seulement et selon les cas) des évaluations des risques pour la confidentialité, des vérifications du code open source et des analyses de contrôles d'exportations.

Gestion d'actifs

Inventaire des actifs Les systèmes et services gérés par Automation Anywhere sont utilisés pour fournir Automation 360 Cloud. Les propriétaires de systèmes identifiés sont responsables de la tenue et de la mise à jour de l'inventaire le cas échéant.

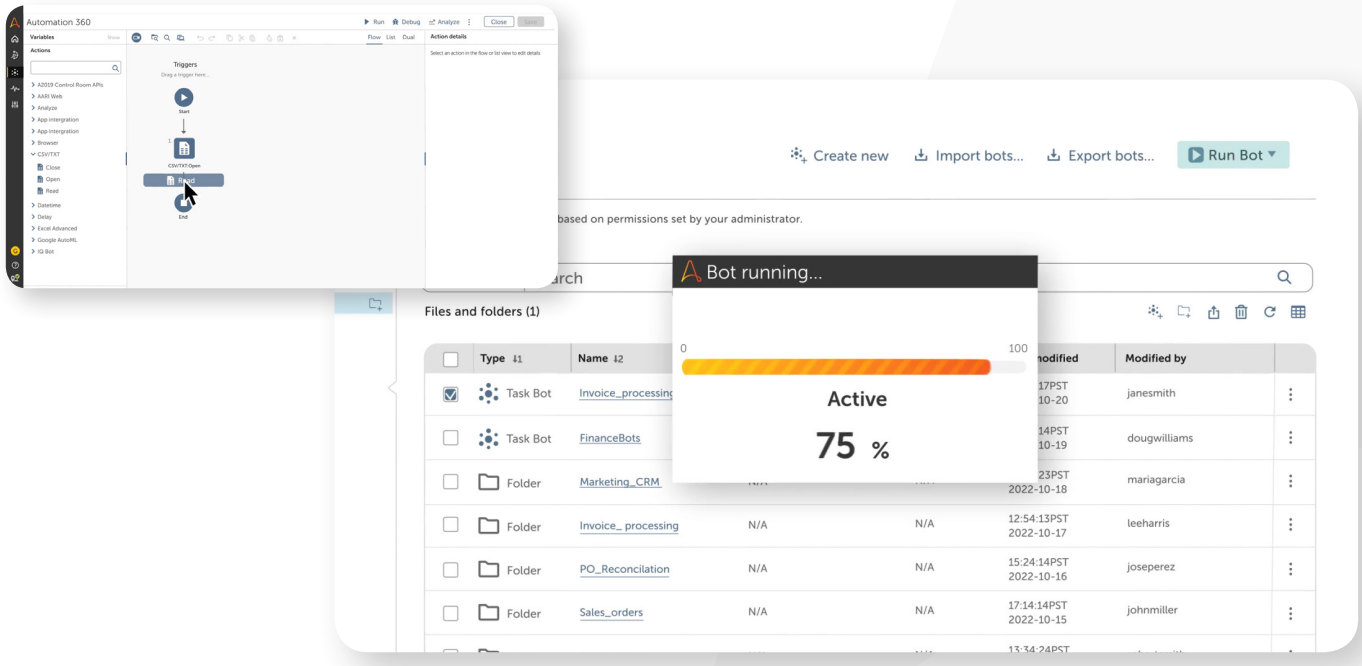
Gestion des actifs et des données Automation Anywhere identifie et classe le contenu client pour s'assurer que l'accès à celui-ci est dûment restreint.

Gestion de l'accès

Politique d'accès Automation Anywhere tient un registre des vérifications en amont et des privilèges de sécurité des membres des équipes CloudOps et Cloud SecOps ayant accès au contenu client et applique le principe du moindre privilège.

Autorisations d'accès Automation Anywhere tient et met à jour un registre des membres des équipes CloudOps et Cloud SecOps autorisés à accéder aux systèmes Automation Anywhere renfermant du contenu client. Avant qu'un nouvel accès soit accordé aux systèmes, celui-ci fait l'objet d'une procédure d'examen et d'approbation par la direction. Automation Anywhere vérifie régulièrement les comptes d'utilisateur et les autorisations attribuées sur les systèmes importants. Automation Anywhere identifie les personnes qui peuvent accorder l'accès aux données et aux ressources, le modifier ou le révoquer. Automation Anywhere s'assure que, lorsque plusieurs personnes ont accès à des systèmes hébergeant du contenu client, celles-ci disposent d'identifiants/d'informations de connexion distincts.

Moindre privilège Automation Anywhere restreint l'accès au contenu client aux seules personnes autorisées par ce dernier à exercer leur fonction d'assistance et de dépannage.

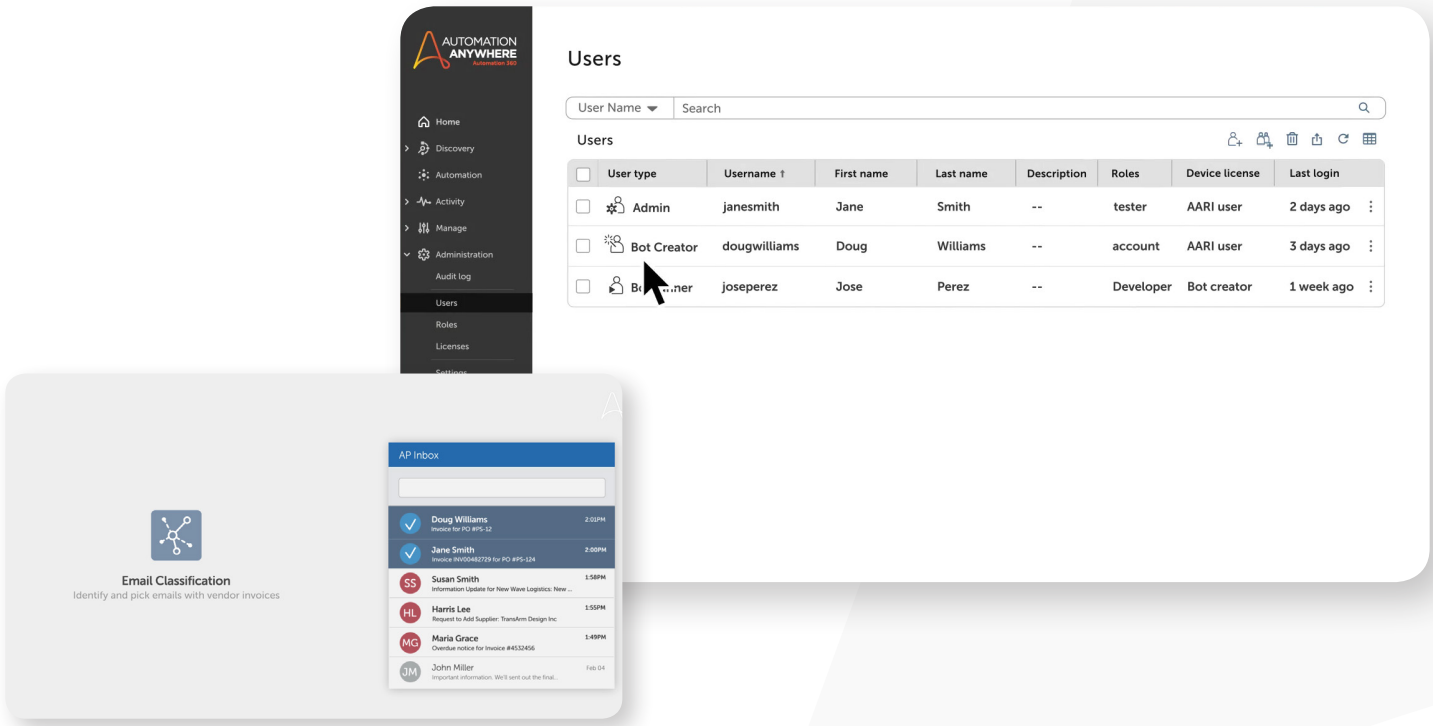


Intégrité et confidentialité Automation Anywhere exige que tous les services d'assistance, de CloudOps et de Cloud SecOps impliqués dans la fourniture d'Automation 360 Cloud sécurisent les ordinateurs et les données lorsqu'ils sont laissés sans surveillance et que les mots de passe restent inintelligibles tout au long de leur cycle de vie.

Authentification Automation Anywhere utilise des pratiques standard du secteur pour identifier et authentifier le personnel CloudOps et Cloud SecOps accédant aux systèmes d'information. Lorsque les mécanismes d'authentification sont basés sur des mots de passe, les pratiques sectorielles standard sont appliquées pour le traitement et la gestion des mots de passe, notamment les suivantes :

- Les mots de passe doivent être renouvelés régulièrement, conformément aux exigences système et aux règles d'Automation Anywhere.
- Les mots de passe doivent répondre aux exigences en termes de longueur et de complexité ; par exemple, ils doivent être composés d'au minimum huit caractères.
- Il est interdit au personnel de partager les mots de passe.
- Les identifiants désactivés ou expirés ne peuvent pas être attribués à d'autres personnes.

Automation Anywhere prévoit des procédures de désactivation des mots de passe qui ont été corrompus ou divulgués par inadvertance. En outre, Automation Anywhere surveille les risques de sécurité au moyen de différentes mesures, telles que les tests d'intrusion, les évaluations de vulnérabilités, etc.



Sécurité matérielle et des environnements (contrôle d'accès, contrôle de disponibilité)

Accès physique aux installations d'Automation Anywhere Automation Anywhere limite l'accès aux installations au personnel autorisé. Les employés, sous-traitants et invités doivent disposer de badges d'identité et, lorsqu'ils se trouvent dans les locaux, ces badges doivent être constamment visibles. Automation Anywhere fait appel à diverses méthodes de surveillance des points d'entrée des installations, notamment la présence d'agents de sécurité, la détection des intrusions et des caméras de vidéosurveillance.

Intégration Avant de commencer à travailler chez Automation Anywhere, les nouveaux membres du personnel et sous-traitants sont tenus de signer un accord de confidentialité. Par la suite, pendant le processus d'intégration, des cours de sensibilisation à la sécurité sont dispensés à ces nouvelles recrues.

Centres de données hébergés Automation Anywhere utilise des services de cloud public afin de garantir à Automation 360 Cloud une présence mondiale. La présence géographique est maintenue dans les régions et pays suivants : États-Unis, Canada, UE, Brésil, Japon, Inde, Singapour, Australie, Afrique du Sud et Bahreïn. Aucun centre de données physique n'est utilisé.

Application et développement

Développement et maintenance de systèmes de sécurité Un cycle de développement logiciel sécurisé (SDLC) est créé en employant des outils et des techniques dans le processus de développement existant. À chaque étape du processus de cycle de développement logiciel, des vérifications et validations sont effectuées par des administrateurs distincts dont les rôles et privilèges diffèrent. La séparation stricte des responsabilités et les contrôles à plusieurs niveaux sont intégrés dès la conception, pour garantir un pipeline de développement logiciel à la fois fiable, évolutif, efficace, sécurisé et conforme.

La sécurité du cloud est gérée et surveillée par une équipe spécialisée en génie de la sécurité, responsable de l'examen de la conception, de la modélisation des menaces, de la validation manuelle du code et des vérifications ponctuelles, ainsi que des tests d'intrusion réguliers.

Nous disposons de programmes de tests de sécurité internes et externes. Les tests internes couvrent les phases de planification, de développement et de test, et chacun d'entre eux s'appuie sur les tâches réalisées précédemment. Nous mettons en œuvre une approche qui a fait ses preuves pour l'analyse du code statique et dynamique, à la fois lors des phases de développement et de test. Les tests externes sont menés en environnement de production et s'articulent autour du concept de « garantie continue de résultat ».

Gestion de l'open-source Automation Anywhere recourt à un système logiciel pour gérer les contrôles et approbations du code open source. En outre, Automation Anywhere effectue des analyses et des audits périodiques de ses produits logiciels pour vérifier la conformité du code open source.

Gestion des changements Automation Anywhere applique des procédures de contrôle des changements qui répondent aux exigences de sécurité pour les systèmes d'information, les tests, l'acceptation des tests et la sécurité relative à l'utilisation des données de test. La gestion et le suivi des modifications des logiciels et de la configuration s'effectuent à l'aide de systèmes de tickets standard.

Opérations sécurisées

Prévention des pertes Automation 360 exploite des techniques et des outils de protection contre la perte de données (DLP) spécifiques au cloud. Une combinaison d'outils qui surveillent, détectent, mettent en corrélation et corrigent les événements est déployée. Ces outils s'intègrent à la gestion des informations et des événements de sécurité (SIEM) ainsi qu'à l'analyse des journaux pour détecter les intrusions et l'extraction de données.

Logiciels malveillants Automation Anywhere utilise des logiciels antivirus, des logiciels anti-malware et d'autres contrôles pour éviter que des logiciels malveillants n'obtiennent un accès non autorisé aux données des clients.

Séparation et accès au réseau Automation Anywhere met en œuvre des mécanismes conçus pour appliquer les politiques et les normes internes de gestion de l'accès dans l'ensemble des services, y compris les contrôles réseau couvrant l'accès aux données client. Selon le cas, il peut ainsi s'agir de configurer une zone intermédiaire non approuvée entre l'internet et le réseau interne avec un mécanisme de sécurité afin de restreindre l'accès et le trafic non autorisé.

Automation Anywhere pratique une approche par couche de la séparation du réseau, avec des contrôles à chaque couche. Le(s) sous-réseau(x) public(s) protège(nt) le(s) sous-réseau(x) privé(s) interne(s) de l'accès direct à l'internet. Les données sensibles et/ou autres actifs informationnels sont déployés uniquement sur les sous-réseaux privés internes, sur lesquels aucun accès direct à l'internet n'est possible. L'accès à ces actifs se fait uniquement à partir de certains hôtes autorisés, limités par des listes de contrôle d'accès (ACL) au niveau du réseau, par le routage de clouds privés virtuels (VPC) et par des règles de pare-feu, le cas échéant. À l'intérieur du sous-réseau privé, la propagation latérale est également limitée en fonction des besoins de l'entreprise. Nous contrôlons l'accès à nos réseaux sensibles selon le principe de l'accès régi par les besoins. Les administrateurs privilégiés du backend doivent se connecter aux hôtes du bastion en tant que première couche en utilisant des certificats d'appareil, une authentification multifacteur et des proxys ou des VPN.

Surveillance opérationnelle L'équipe chargée du CloudOps d'Automation Anywhere surveille le processeur de l'infrastructure, la mémoire et les journaux d'application 24 h/24 et 7 j/7 afin d'exploiter et de maintenir Automation 360 Cloud. Cela peut notamment servir à surveiller les performances, la stabilité, l'utilisation et la sécurité des services et des composants connexes. Les environnements de la Control Room font l'objet d'un contrôle de la capacité des ressources afin de garantir que les environnements multilocataires des clients disposent de suffisamment de ressources et de capacités de réserve à mesure que la création de robots et les charges opérationnelles augmentent.

Télémétrie d'utilisation L'équipe chargée des opérations d'Automation Anywhere ne peut accéder à l'environnement de la Control Room d'un client ni avoir une visibilité sur les données commerciales d'un client, à moins qu'il ne lui soit demandé d'effectuer des diagnostics dans le cadre d'un cas de support. Automation Anywhere collecte en toute sécurité des données télémétriques sur l'utilisation des fonctionnalités afin d'améliorer le service, afin, par exemple, d'aider automatiquement les utilisateurs à utiliser les fonctionnalités. Cette télémétrie ne comprend pas d'informations personnelles identifiables (PII) ou de données commerciales du client.

Surveillance de la sécurité Automation Anywhere a déployé plusieurs couches de surveillance et de détection des journaux de sécurité, des événements et des menaces dans l'environnement. Celles-ci se composent de la plateforme cloud public, de la piste d'audit et des journaux du plan de contrôle, des journaux IAM, des journaux de sécurité des terminaisons et des conteneurs, des journaux du système d'exploitation et d'autres journaux de sécurité de tiers agrégés, corrélés et surveillés pour une surveillance de la sécurité 24 h/24. L'équipe chargée des opérations de sécurité d'Automation Anywhere utilise les techniques de surveillance AIOps pour évaluer automatiquement les performances et détecter automatiquement tout comportement inhabituel susceptible d'indiquer la présence d'un acteur malveillant. L'anomalie sera examinée et le service de conteneurs sera supprimé si nécessaire.

Gestion des incidents

Réponse aux incidents Automation Anywhere met en œuvre un programme de réponse aux incidents conçu pour analyser, contenir, éliminer et surmonter les incidents de sécurité ayant un impact sur les réseaux ou les systèmes gérés d'Automation Anywhere ou les données client.

Notification des incidents Si Automation Anywhere détermine que les données client sous son contrôle ont fait l'objet d'un incident de sécurité, le client en sera informé en vertu et selon la loi applicable.

Incident post-mortem Automation Anywhere effectue une étude post-mortem après un incident afin d'analyser et d'améliorer les outils et les processus en vue d'atténuer les risques à l'avenir.

Gestion des fournisseurs

Intégration Automation Anywhere évalue la sécurité des prestataires de services qui fournissent des composants de services qui stockent et traitent les données des clients. Automation Anywhere exige que les prestataires connectés aux services respectent les exigences en termes de niveau de sécurité énoncées dans cette section qui s'applique aux services qu'ils fournissent.

Gestion des départs Lorsque la relation avec un prestataire de services prend fin, celui-ci est tenu de retourner tout le contenu client en sa possession ou de certifier que tout ce contenu a été détruit de façon sécurisée.

Activités

Continuité de l'entreprise Automation Anywhere dispose de plans d'urgence et de secours et a obtenu la certification ISO 22301 BCMS.

Haute disponibilité Chaque centre de données régional est conçu pour assurer une haute disponibilité au niveau des applications et des services cloud publics hautement disponibles dans toute la région. Automation 360 Cloud suit les bonnes pratiques du secteur avec un SLA de durée de fonctionnement de 99,9 %.

Reprise après sinistre Des sauvegardes sont effectuées et conservées dans un format chiffré afin de restaurer le service en cas de catastrophe. Les sauvegardes sont effectuées toutes les 4 heures dans une autre région (sauf en Australie et au Canada où les sauvegardes sont conservées dans le pays). Si un sinistre est déclaré pour la région principale, une région secondaire est instanciée pour tous les locataires à l'aide de la sauvegarde effectuée toutes les 4 heures. Les objectifs actuels de cette reprise sont les suivants :

- RTO (Recovery Time Objective, Objectif de temps de récupération) : temps nécessaire pour mettre en place une nouvelle région avec les dernières données de sauvegarde restaurées = 4 heures
- RPO (Recovery Point Objective, Objectif de point de récupération) : durée maximale de perte de données pendant
  une restauration = 4 heures

Confidentialité des données d'Automation 360

Automation Anywhere adopte une approche de « priorité à la confidentialité » en ce qui concerne la protection des données et l'infrastructure des clients. Il existe trois types de données traitées dans Automation 360 Cloud.

Données opérationnelles Il s'agit des données qui comprennent des informations sur l'état et les journaux qui facilitent l'exécution des automatisations, telles que les journaux d'erreurs, les journaux d'audit, les statistiques sur la connectivité des appareils et les tableaux de bord opérationnels.

Données commerciales Il s'agit des données, telles que les données relatives aux clients, les numéros de factures ou les images des points de vente, qui sont utilisées dans le cadre du fonctionnement d'une entreprise et passent d'un système à l'autre dans le cadre de l'automatisation des robots. Par exemple, les données chargées dans le cloud pour le traitement de systèmes de documents tels que Document Automation.

Données à caractère personnel Il s'agit de toutes les données qui pourraient être utilisées pour identifier un individu et qui sont régies par des lois telles que le **Règlement général sur la protection des données (RGPD)** et la CCPA. Ces informations personnelles incluent, sans toutefois s'y limiter, les noms de personnes, les numéros de téléphone, les adresses e-mail, les intitulés de poste et les coordonnées contenus dans les factures ou les e-mails.

Collecte des données

Le modèle de déploiement implique que les clients construisent leurs robots et gèrent les déploiements de robots à partir de la Control Room dans le cloud. Une fois les robots construits, ils sont testés et déployés pour exécution sur l'infrastructure informatique des utilisateurs.

Le tableau ci-après décrit les données recueillies pour le portefeuille du cloud d'Automation 360. Il donne également des indications sur les données qui pourraient éventuellement être utilisées pour identifier une personne physique.

Élément de données	Catégorie de données	Description
Nom d'utilisateur	Personnelle	Adresse e-mail, prénom et nom de famille, nom d'usage, fuseau horaire, dernière connexion, mot de passe, série de questions, domaine AD.
Mot de passe de l'utilisateur	Personnelle	
Clé de sécurité du mot de passe	Personnelle	Clé de sécurité du mot de passe du Credential Vault.
Accès à l'appareil de l'agent de robot	Personnelle	Nom d'utilisateur et informations d'identification d'accès de l'appareil.
Définitions des rôles	Personnelle	Administrateur, créateur, etc.
Rôles mappés à des utilisateurs, des appareils, des ressources	Personnelle	Rôles d'utilisateur.
FQDN/IP du robot	Personnelle	L'adresse IP ou le FQDN de l'appareil peut être relié(e) à un utilisateur.
Définition du robot (référentiel)	Opérationnelle	Données stockées comme partie intégrante de la définition du robot.

Élément de données	Catégorie de données	Description
Informations d'identification de l'application du robot	Personnelle	Utilisateur d'application, URL, clé publique, nom de routage.
Plannings des robots de la Control Room	Opérationnelle	Gestion des robots ; quand et où exécuter les robots.
Définition du flux de travail WLM	Opérationnelle	Quand et où exécuter des robots, et dans quel ordre.
Journaux d'audit	Personnelle	**Peut contenir des identificateurs :** journal des messages de l'appareil, journal des messages de déploiement, journal des e-mails, journal d'exécution des tâches : (heure de début/fin, ID d'utilisateur, horaire, nom de l'automatisation, ID de déploiement, nom du périphérique, nom du robot, nom d'utilisateur). Gestion des utilisateurs, journal des modifications, journal des messages du coffre des informations d'identification, serveur et base de données, journaux des modifications.
Journal des erreurs	Personnelle	Peut contenir des identificateurs.
Analyse opérationnelle	Opérationnelle	État du service.
Analyse marketing	Entreprises/ Personnes	Données commerciales marquées dans les processus automatisés pour être analysées par Bot Insight.
Données de traitement intelligent des documents	Entreprises/ Personnes	Documents chargés vers Document Automation pour extraction et traitement. **Pour Document Automation :** documents chargés et résultats d'extraction.
Données de traitement intelligent des documents	Opérationnelle	**Pour Document Automation :** instances d'apprentissage, domaines, statistiques opérationnelles et changements de validation des utilisateurs.
Données d'utilisation de la télémétrie	Opérationnelle	Utilisation des fonctionnalités, licences activées, agrégées sans identifiants de données personnelles/d'utilisateur.
Données sur les processus et les flux de travail	Entreprises/ Personnes	**Pour Automation Co-Pilot :** définition du flux de travail Web d'Automation Co-Pilot : description de l'exécution d'un processus (y compris, mais sans s'y limiter, le robot, les formulaires et les autres étapes nécessaires à l'exécution dudit processus). **Flux de données Web d'Automation Co-Pilot :** stocke les données générées incidemment par l'exécution du processus (y compris toutes les entrées et sorties des différentes étapes dudit processus).
Autres données	Entreprises/ Personnes	**Pour Automation Co-Pilot :** définitions de l'équipe Web d'Automation Co-Pilot : description des membres de l'équipe et des règles d'accès aux processus. **Stockage de fichiers sur le Web d'Automation Co-Pilot :** stocke les fichiers chargés dans le cadre du flux de données de la demande.

Télémétrie de l'utilisation des données

Exploitation et assistance

Les équipes chargées des opérations d'Automation 360 Cloud surveilleront les performances opérationnelles du système de déploiement afin d'exploiter, de mettre à l'échelle et d'assister le service conformément à l'accord de niveau de service (SLA) et conformément au contrat de service conclu entre Automation Anywhere et le client.

Le personnel opérationnel d'Automation Anywhere n'utilise pas les données client. Cependant lorsque les services d'assistance ont besoin d'accéder aux données réelles pour le dépannage et la résolution de problèmes techniques liés aux produits, le personnel d'Automation Anywhere est soumis aux contrôles d'accès décrits ci-dessus.

Pour améliorer le produit, Automation Anywhere :

- Analysera les données d'utilisation des fonctionnalités pour améliorer le produit, par exemple, ajouter de la télémétrie afin d'offrir une visibilité opérationnelle sur l'utilisation des fonctionnalités. Cela permettra à Automation Anywhere de prioriser et d'apporter des améliorations au produit. Voici quelques exemples :
  - Examiner la fréquence d'utilisation des commandes de l'application pour aider à déterminer les commandes à ajouter en priorité aux prochaines versions.
  - Fournir des recommandations sur les meilleures pratiques opérationnelles.
  - Fournir des services d'assistance qui seront utilisés pour la mise à jour, la sécurisation et le dépannage.
  - Personnaliser les produits et émettre des recommandations.
  - Pour Document Automation et AISense, la structure des champs des documents peut être utilisée pour améliorer la qualité des modèles d'IA pour le traitement des documents.

Pour plus d'informations sur la politique de confidentialité des données d'Automation Anywhere, veuillez consulter l'adresse suivante : automationanywhere.com/fr/legal/privacy

Rétention des données après la résiliation de l'abonnement

Automation Anywhere conservera les données client, les configurations (robots), les données de Document Automation et la plupart des journaux pendant 30 jours après la fin de l'abonnement du client. Certains journaux peuvent être conservés jusqu'à 270 jours après la fin de l'abonnement du client. Vous trouverez ici tous les détails de l'Addenda relatif au traitement des données et de la politique de rétention des données : automationanywhere.com/support/DPA.pdf

Sécurité des données

Le cloud d'Automation 360 offre à ses clients un ensemble complet de fonctions de sécurité qui sont automatiquement fournies ou qui sont configurables dès la conception pour assurer la protection des données. Comme pour toute application d'entreprise, l'utilisation cohérente et appropriée des contrôles de sécurité est à la charge de l'entreprise qui utilise l'application.

L'autorisation des utilisateurs dépend des administrateurs informatiques, qui doivent mettre en œuvre des contrôles pour s'assurer que seul le personnel autorisé y a accès.

Le propriétaire autorisé des données peut limiter l'accès au service aux seules personnes autorisées en ayant besoin pour des raisons professionnelles. Les utilisateurs professionnels disposant d'un accès peuvent recevoir des autorisations précises provenant de la Control Room via des contrôles d'accès en fonction des rôles (RBAC). Les modèles RBAC permettent un double contrôle et une séparation des tâches au sein des opérations. Des autorisations peuvent être appliquées à tous les aspects du fonctionnement du produit, y compris les informations d'identification, les robots, les Bot Runners, les Bot Creators, les planifications de robots, les instances d'apprentissage de Document Automation, l'accès au journal d'audit, les files d'attente de gestion de la charge de travail et les pools.

Le cloud d'Automation 360 fournit des fonctions d'audit complètes où toutes les actions des utilisateurs sont vérifiées au sein de la plateforme, avec des enregistrements de tous les accès et de l'ensemble des mesures prises par le personnel exploitant. Un audit est automatisé pour tous les rôles privilégiés et non privilégiés afin de se conformer aux bonnes pratiques définies dans la norme NIST AC-6.

Dans la mesure où les robots sont des programmes logiciels développés par les experts commerciaux du client, des processus SDLC sécurisés de pointe doivent être mis en œuvre par le client à cet effet. À cette fin, Automation Anywhere prend en charge la séparation des environnements de développement, de test et de production via une combinaison de déploiements séparés et du système RBAC, décrit ci-dessus.

Chiffrement

Le service utilise des technologies de chiffrement standard du secteur pour garantir que les données des clients sont chiffrées entre le réseau du client et le service d'Automation 360 Cloud. Tout le trafic vers/depuis les utilisateurs est chiffré en utilisant HTTPS + SSL / TLS 1.2 (port 443) pour communiquer avec l'environnement d'Automation 360 Cloud. Toutes les données stockées dans le service, c'est-à-dire les données au repos, sont chiffrées à l'aide de l'algorithme AES-256.

Confidentialité des données

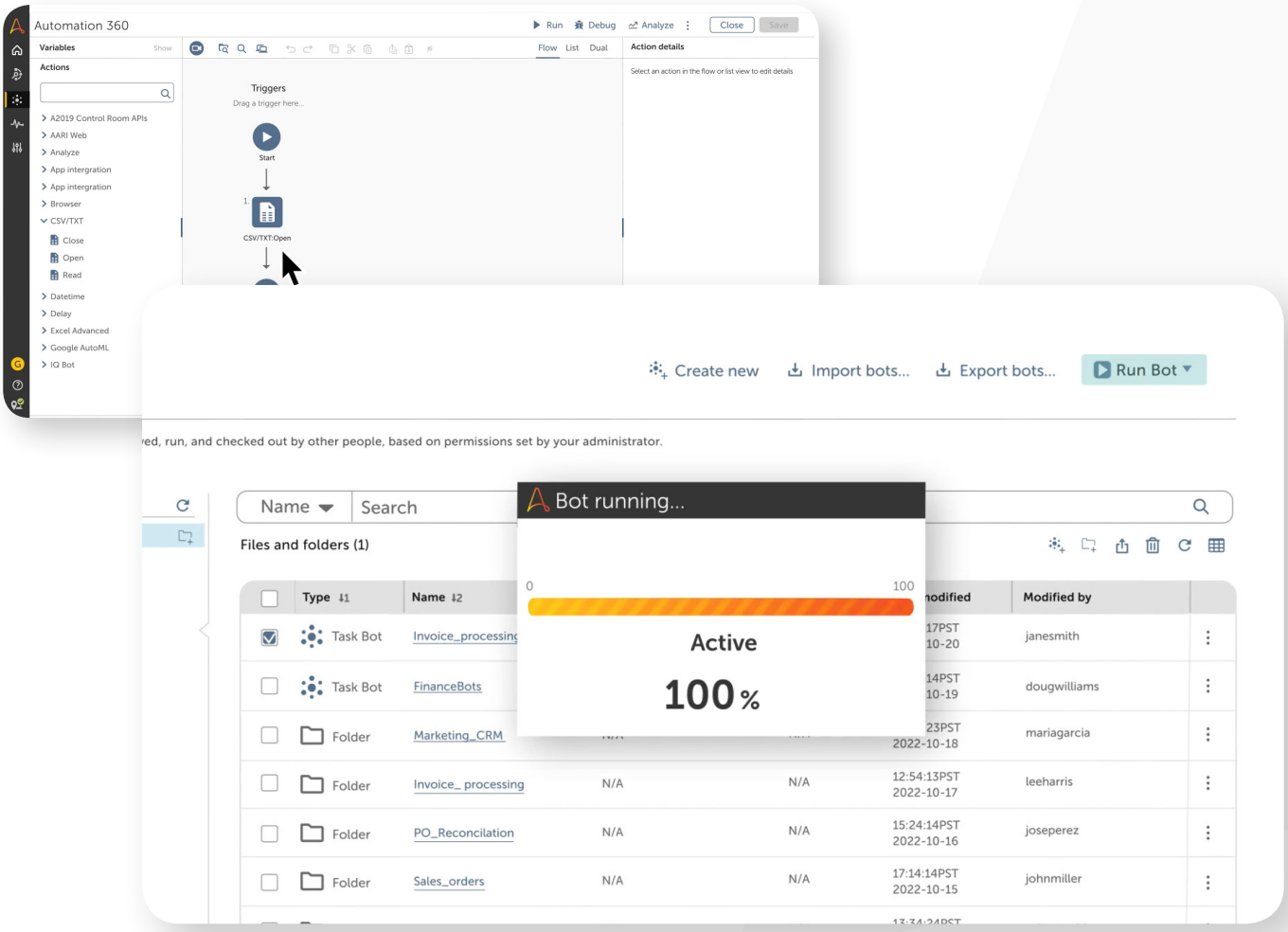
Automation Anywhere adopte une approche de priorité à la confidentialité des données pour le développement de ses produits. Chaque produit est conçu pour répondre aux exigences de nos clients internationaux en matière de réglementation des données et de protection de la vie privée, y compris en ce qui concerne les réglementations nationales visant à protéger la confidentialité des données. La California Consumer Privacy Act (CCPA) et le RGPD sont des exemples de réglementation qui dictent la manière de traiter les données à caractère personnel sensibles et de s'assurer que les informations ne sont pas exposées à des parties non autorisées.

Le RGPD prévoit différentes responsabilités lorsqu'il s'agit de traiter des données. Le responsable du traitement des données est une entité qui détermine pourquoi et comment les données sont traitées. Un sous-traitant des données effectue le traitement des données pour le compte du responsable du traitement. Le rôle d'Automation Anywhere est celui d'un sous-traitant des données, tandis que le client est le responsable du traitement des données et contrôle toujours les données commerciales, opérationnelles et personnelles.

Automation Anywhere adopte les bonnes pratiques en matière de confidentialité et de sécurité des données pour le traitement adéquat des données des clients, en particulier en ce qui concerne le consentement, les mentions et les exigences réglementaires. La confidentialité des données concerne plus particulièrement la manière dont les données sont collectées, stockées et utilisées, ainsi que le respect de la conformité réglementaire.

La Control Room permet de configurer et de supprimer des comptes d'utilisateurs grâce aux contrôles RBAC appropriés. L'administrateur de l'entreprise est chargé de fournir un accès approprié aux utilisateurs et aux ressources. L'administrateur doit créer une stratégie avec le niveau d'accès requis conformément aux directives sur la confidentialité des données utilisateur et d'entreprise. Si les utilisateurs souhaitent accéder à leurs informations personnelles ou en limiter l'accès, ils doivent contacter leur administrateur. Les administrateurs du client peuvent supprimer les comptes de l'utilisateur depuis la Control Room.

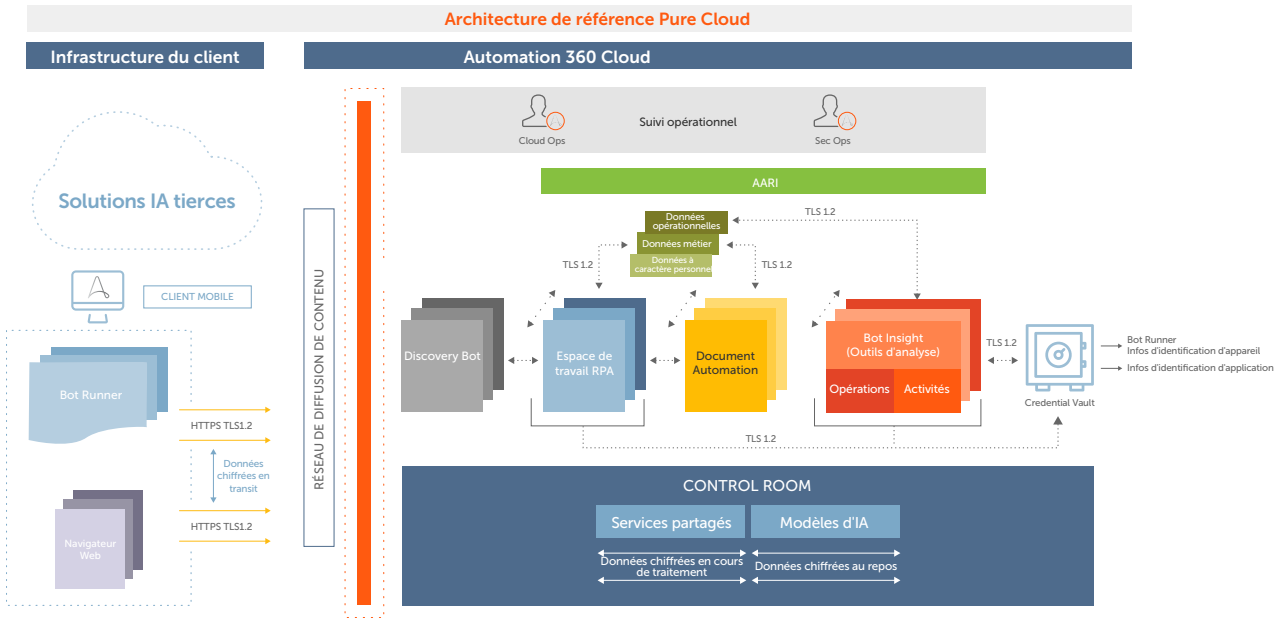
Pour en savoir plus sur les demandes de renseignements sur la confidentialité des données dans le cadre du RGPD et sur les copies des données à caractère personnel, Automation Anywhere vous invite à vous rendre sur le site suivant : Formulaire de demande d'accès aux données.



Sécurité et confidentialité des données dans les modèles de déploiement d'Automation 360

Automation Anywhere propose trois modèles de déploiement : compatible avec le cloud et sur site, avec certaines mises à jour via le cloud. Dans cette section, nous aborderons l'architecture sécurisée pour les modèles de déploiement activé pour le cloud et les responsabilités opérationnelles en matière de sécurité.

Automation 360 Cloud



Pure Cloud comprend plusieurs services RPA intégrés composés de la Control Room, du stockage des données, d'Automation Workspace, de Credential Vault, de Bot Insight, de Process Discovery, d'Automation Co-Pilot et de Document Automation. Pour en savoir plus sur les capacités de la plateforme Automation 360 et sur les différents produits d'Automation 360, visitez automationanywhere.com.

Résumé des responsabilités de Pure Cloud en matière de sécurité et de confidentialité des données	
Attribut	Partie responsable
Cadre NIST 800-53 concernant la sécurité du cloud	Sécurité gérée par Automation 360 Opérations dans le cloud.
Continuité d'activité/Reprise après sinistre	Géré par les opérations Automation 360 Cloud.
Haute disponibilité	Géré par les opérations Automation 360 Cloud.
Localisation des données commerciales	Géré par les opérations Automation 360 Cloud
Protection des données d'entreprise	Géré par les opérations Automation 360 Cloud

Tableau 1-Matrice des services et des responsabilités couverts par le client et Automation Anywhere pour le modèle de déploiement

Dans le modèle de déploiement Pure Cloud, l'équipe d'exploitation d'Automation 360 Cloud gère et exploite les services de base, notamment la Control Room, Automation Workspace, Process Discovery, Automation Co-Pilot, Document Automation et Bot Insight. Dans le cadre du modèle de déploiement Pure Cloud, Automation Anywhere joue le rôle de fournisseur SaaS et est responsable de la haute disponibilité (HA), de la continuité d'activité (BC)/reprise après sinistre (DR), de la politique d'exploitation et des procédures.

Automation 360 Cloud est déployé en tant que service de haute disponibilité dans toutes les régions spécifiées par Automation Anywhere (ceci concerne notre offre de déploiement Pure Cloud). En cas de catastrophe, des sauvegardes sont effectuées toutes les 4 heures dans une autre région (sauf en Australie où les sauvegardes sont conservées dans le pays). Si un sinistre est déclaré pour la région principale, une région secondaire est instanciée pour tous les locataires à l'aide de la sauvegarde effectuée toutes les 4 heures. Les objectifs actuels de cette reprise sont les suivants :

1. Objectif de temps de récupération (RTO) : temps nécessaire pour mettre en place une nouvelle région avec les dernières données de sauvegarde restaurées = 4 heures.
2. Objectif de point de récupération (RPO) : durée maximale de perte de données pendant une restauration = 4 heures

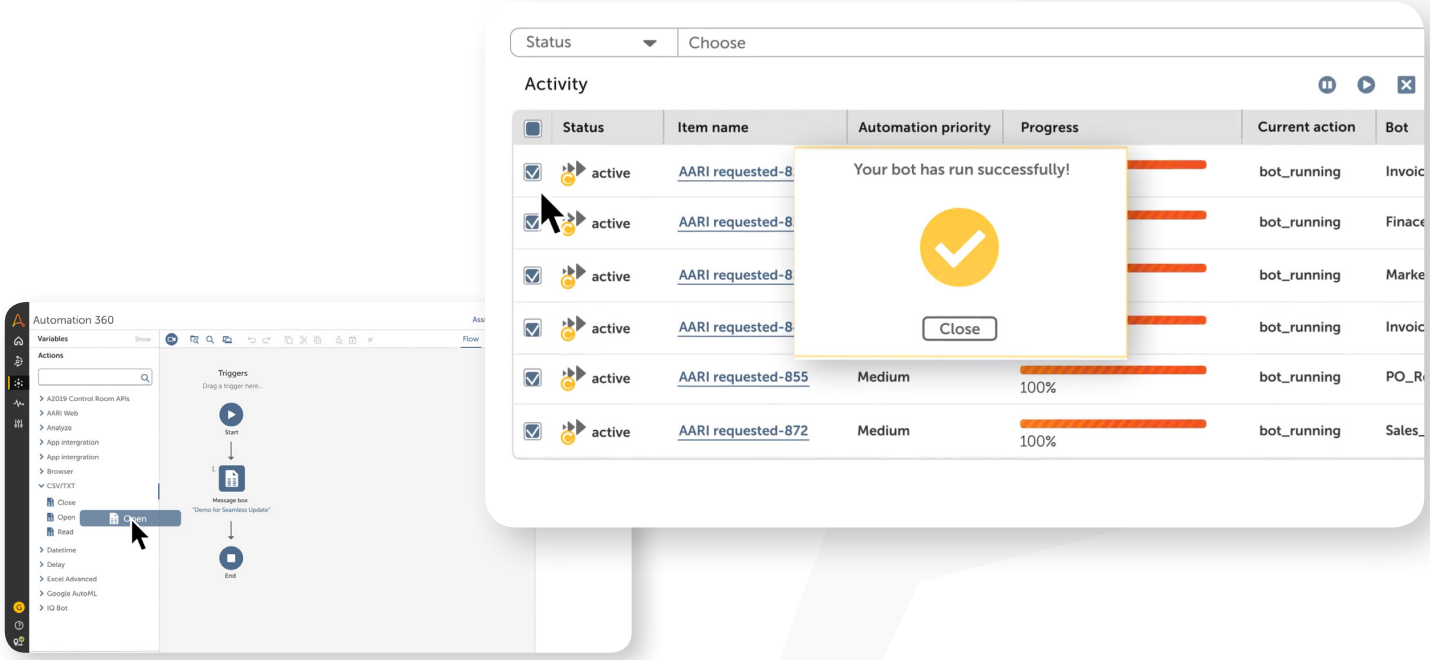
Automation 360 Cloud héberge la plateforme Automation 360 et les applications associées telles qu'Automation Workspace, Process Discovery, Automation Co-Pilot, Document Automation et Bot Insight. Les données opérationnelles et commerciales de ces produits peuvent physiquement résider dans Automation 360 Cloud. L'agent de robot qui exécute les robots et tous les systèmes et données auxquels le robot accède résident physiquement sur l'infrastructure du client, qui est gérée et exploitée par ce dernier.

Considérations du client pour le déploiement d'Automation 360 Cloud

En déployant Pure Cloud, les clients peuvent profiter de l'architecture de sécurité robuste d'Automation 360 Cloud. Dans le cadre d'une utilisation normale, le client accepte que ses informations confidentielles soient temporairement présentes dans Automation 360 Cloud dans le cadre de l'automatisation des processus.

Au cas où les processus automatisés sont susceptibles d'impliquer la manipulation de données sensibles ou réglementées stockées dans des systèmes sur l'infrastructure du client, et qu'il est exigé que ces données ne soient pas traitées ou stockées avec Automation 360 Cloud, les clients peuvent toujours développer des robots sur le cloud en utilisant des données de test qui ne sont pas soumises à ces contrôles. Les robots sont ensuite déployés dans l'infrastructure du client et l'automatisation des processus s'effectue à partir des données réglementées. Cette approche limite l'utilisation par le client de certains produits hébergés dans Automation 360 Cloud, tout en garantissant qu'aucune donnée sensible n'est envoyée à Automation 360 Cloud. Ces limitations incluent l'utilisation de la gestion de la charge de travail (WLM), les tableaux de bord de Bot Insight, Automation Co-Pilot et Process Discovery. Veuillez noter que les spécifications du compte d'utilisateur RPA et les informations d'identification sont stockées dans le cloud et sont régies par les lois sur la confidentialité des données, qu'Automation 360 Cloud est en mesure d'appliquer.

Toutes les données opérationnelles, commerciales et personnelles du client résident physiquement dans les locaux du client. Automation 360 Cloud offre des fonctions de gestion qui incluent les mises à niveau logicielles, l'authentification utilisateur via SAML 2.0, l'octroi de licences et la livraison de packages de commande. Grâce à cette solution, toutes les données client résident physiquement sur l'infrastructure du client, qui a ainsi le contrôle total de la gestion de ses données. Les services, tels que les mises à niveau logicielles et les licences hébergées sur Automation 360 Cloud, offrent une activation et une adoption rapides, ainsi qu'une maintenance plus efficace.



Ressources supplémentaires sur la sécurité du cloud

- Page Web d'Automation 360
- Page Web d'Automation 360 sur la sécurité
- Politique de confidentialité
- Architecture de sécurité
- Cloud Alliance

À propos d'Automation Anywhere
Automation Anywhere met son savoir-faire au service de tous ceux dont les idées, la réflexion et l'engagement font toute la différence. Nous proposons la plateforme de force de travail numérique la plus sophistiquée au monde. En automatisant les processus métier et en libérant le personnel de ces tâches, nous rendons le travail plus humain.

Contactez-nous au 1-888-484-3535 ou rendez-vous sur www.AutomationAnywhere.com pour planifier une démo en direct.

Automation Anywhere www.automationanywhere.com/fr

Amérique du Nord : +1-888-484-3535 x1 | International : +1-408-834-7676 x1

@AutomationAnywh www.linkedin.com/company/automation-anywhere

AUTOMATION ANYWHERE FRANCE

3-5 Rue Saint-Georges, Paris 75009, France

contact-france@automationanywhere.com