Une sécurité professionnelle au service de l'automatisation des processus par la robotique

INTRODUCTION

Automation Anywhere a commencé son activité il y a 15 ans en posant une question simple : après plus de 20 ans d'investissement dans les technologies d'automatisation des processus métier, pourquoi seulement moins de 20 % des tâches sont-elles automatisées ? L'entreprise s'est rapidement penchée sur le principal défi : 85 % des systèmes d'entreprise sont dépourvus de systèmes d'API correctement définis. De ce fait, les services informatiques prennent de plus en plus de retard face aux demandes d'intégration émanant des unités d'exploitation.

L'automatisation des processus par la robotique est née avec la vision de donner aux utilisateurs professionnels les moyens de créer des robots logiciels qui pourraient interagir avec les systèmes d'entreprise de la même manière que les humains. La RPA permet à tout utilisateur professionnel de comprendre les macros Excel pour enregistrer les étapes utilisées dans des tâches répétitives et de les transformer en script facile à comprendre pour les robots. Les robots RPA peuvent se connecter aux applications d'entreprise à l'aide d'informations d'identification, tout comme les humains, et automatiser des tâches impliquant n'importe quelle application d'entreprise, même celles d'ancienne génération dépourvues d'API. Traitement des demandes d'indemnisation ou de prêt, rapprochement des comptes, génération et envoi de factures et création de rapports ne sont que quelques exemples des automatisations possibles couvrant différentes disciplines métier.

On perçoit facilement les avantages que peut offrir la RPA, qu'il s'agisse des gains de temps substantiels, des importantes économies de coûts, de l'amélioration de la satisfaction des clients et de l'état d'esprit du personnel, ou encore de la possibilité de prendre une longueur d'avance décisive sur la concurrence. Néanmoins, les concrétiser entièrement exige une solution qui soit à la hauteur des besoins de l'entreprise.

Fiabilité à toute épreuve, évolutivité et ensemble complet de fonctionnalités permettant d'optimiser l'applicabilité et la facilité d'utilisation comptent parmi les critères de base de l'automatisation. Toutefois, ces éléments ne suffisent pas pour répondre à l'exigence la plus cruciale des entreprises : une sécurité de bout en bout. Le fonctionnement d'une entreprise requiert une architecture de sécurité robuste dotée de fonctionnalités permettant une prise en charge complète de ces principes fondamentaux que sont notamment le moindre privilège et la séparation des responsabilités, ainsi que la protection de bout en bout des applications essentielles et des données sensibles concernées.

Ce rapport fournit une présentation sur la sécurité pour entreprises conforme aux normes les plus rigoureuses du secteur, telle qu'elle est mise en œuvre par la plateforme de force de travail numérique leader du marché, Automation Anywhere Enterprise.

On perçoit facilement les avantages que peut offrir la RPA, qu'il s'agisse des gains de temps substantiels, des importantes économies de coûts, de l'amélioration de la satisfaction des clients et de l'état d'esprit du personnel, ou encore de la possibilité de prendre une longueur d'avance décisive sur la concurrence. Néanmoins, les concrétiser entièrement exige une solution qui soit à la hauteur des besoins de l'entreprise.

ARCHITECTURE ET OPÉRATIONS

Comprendre les contrôles de sécurité nécessaires pour réaliser une implémentation RPA répondant aux besoins de l'entreprise exige de bien connaître les composants de la solution et leur fonctionnement.

Composants de base

Comme le montre la figure 1, les composants architecturaux d'Automation Anywhere Enterprise sont la salle de contrôle (Control Room), les créateurs de robots (Bot Creator) et les exécuteurs de robots (Bot Runner).

Control Room

La Control Room constitue le cerveau de l'environnement d'automatisation. Ce système de gestion basé sur un serveur Windows et doté d'une base de données complète fournit une vue unifiée pour l'administration système globale. C'est également à la Control Room que les opérateurs RPA accèdent pour organiser la force de travail numérique, c'est-à-dire pour planifier, déployer, exécuter, surveiller et gérer les tâches des robots de l'entreprise. De plus, des fonctions intégrées de contrôle des versions (serveur Apache Subversion) permettent la collaboration entre plusieurs utilisateurs, tout en appliquant les meilleures pratiques de gestion des changements et en établissant un référentiel centralisé de robots prêts pour la production.

Bot Creator

Le Bot Creator sert à concevoir les robots. Le client Bot Creator est une application de bureau Windows s'exécutant sur un poste de travail ou une machine virtuelle, utilisée par des experts des processus métier pour créer et tester leurs automatisations. Les robots sont créés au moyen de Task Editor, tandis que leurs tests (à l'aide d'instances d'applications et de données de test locales hors production) sont réalisés par la fonction Player. Après avoir passé avec succès les tests (de performances, d'intégrité des données, de sécurité, etc.), les robots sont intégrés au référentiel de la Control Room et deviennent disponibles pour être déployés dans l'environnement de production.

Bot Runner

Le Bot Runner assure la mise en service des robots. Utilisant le même code d'application que le Bot Creator, mais avec une clé de licence différente, le Bot Runner utilise également la fonction Player pour exécuter les robots dans l'environnement de production. Pour ce faire, il emploie des instances de production de l'application cible et des magasins de données de production. En réalité, les Bot Runner sont uniquement en mesure d'exécuter les robots, car ils n'ont pas accès aux fonctions de création et d'édition. Leur regroupement est également pris en charge pour permettre des opérations à grande échelle hautement fiables.

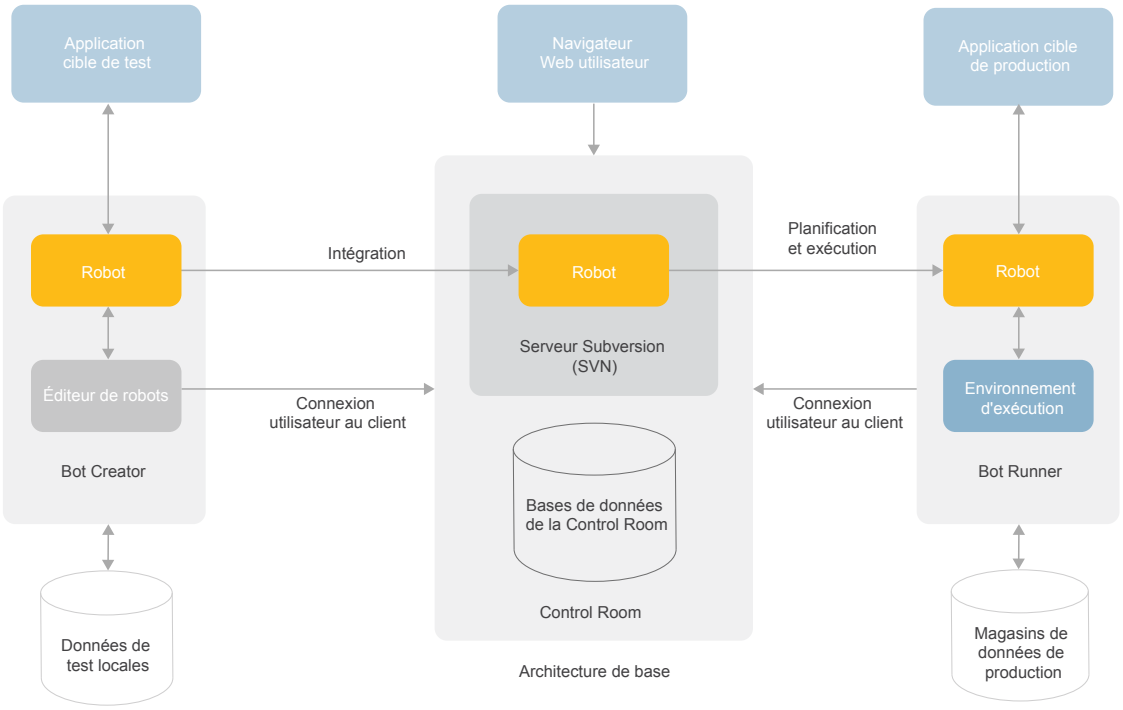


Figure 1 : architecture de base d'Automation Anywhere Enterprise

Composants supplémentaires pour les grandes entreprises

Puisqu'il s'agit d'opérations à grande échelle, deux autres solutions RPA importantes se révèlent pertinentes pour les déploiements adaptés aux grandes entreprises : l'évolutivité à la demande et Bot Insight.

Évolutivité à la demande

Tirant parti du cloud public Amazon Web Services (AWS), Automation Anywhere Enterprise fournit un système RPA en tant que service efficace, avec toutes les fonctionnalités d'accompagnement, notamment l'élasticité des ressources (ajout/suppression), l'emploi de compteurs d'utilisation, l'évolutivité horizontale illimitée, ainsi que la journalisation d'audit et la surveillance en continu de l'infrastructure d'exécution de robots. Il en résulte une haute disponibilité multinœuds conforme à la continuité d'activité et aux performances du SLA, même en cas de fluctuations radicales de la charge de travail d'automatisation.

Bot Insight

Sous-système entièrement intégré au sein de la Control Room, Bot Insight effectue l'analyse en temps quasi réel des opérations des robots et des données des processus métier. Au moyen d'algorithmes avancés spécifiques à chaque robot, il génère automatiquement des tableaux de bord personnalisables. Le niveau de détail fourni par Bot Insight sur la base de journaux d'événements ultraprécis relatifs aux opérations des robots permet l'émission d'alertes nuancées, l'exécution de découvertes ad hoc, des analyses détaillées interactives, des analyses chronologiques et une visibilité complète sur les processus opérationnels/métier. En outre, toutes les données peuvent être exportées vers des journaux de gestion des événements et des informations de sécurité (SIEM) pour analyse, enquête et création de rapports ultérieures.

Les robots en action : deux types d'automatisations

Un dernier point doit être clarifié avant de plonger au cœur des fonctionnalités de sécurité de haut niveau offertes par Automation Anywhere Enterprise : les deux types fondamentaux d'automatisations, à savoir assistée et non assistée.

Une automatisation est dite assistée lorsqu'elle implique que l'utilisateur est connecté au Bot Runner pour observer cette exécution et/ou y participer activement. La présence de l'utilisateur peut être nécessaire du fait que le robot assure une fonction utilitaire qui aide celui-ci dans son travail ou effectue des tâches par lots exigeant régulièrement une intervention ou des instructions en contexte de sa part. Les automatisations assistées sont également appelées automatisations en front office.

Comme leur nom l'indique, les automatisations non assistées fonctionnent sans nécessiter d'interaction de la part d'un opérateur ou d'un utilisateur professionnel. Elles sont généralement exécutées par un opérateur aux connaissances limitées ou inexistantes concernant le robot, l'application automatisée ou l'objet de l'automatisation. L'opérateur, en collaboration avec l'unité opérationnelle, définit un planning d'exécution des robots sur les Bot Runner. Pendant que les robots sont en cours d'exécution, il en surveille les aspects opérationnels, tels que l'utilisation du processeur, de la mémoire et du stockage, pour s'assurer de l'absence d'erreurs ou d'exceptions. Les tableaux de bord de la Control Room affichent tous les détails opérationnels des robots en cours d'exécution.

UNE SÉCURITÉ PERFORMANTE POUR LA RPA GRÂCE À L'IDENTIFICATION ET À L'AUTHENTIFICATION À PLUSIEURS NIVEAUX

Un principe fondamental de l'architecture de sécurité d'Automation Anywhere Enterprise est qu'aucun accès ni aucune action ne sont accordés sans l'autorisation préalable de l'entité impliquée. Cela s'applique aux êtres humains comme aux robots. Pour comprendre l'autorisation liée à la RPA, il faut d'abord comprendre le processus d'authentification pour les automatisations assistées et non assistées.

QUI EST QUI ? LES AUTHENTIFICATIONS COURANTES EN ENTREPRISE

L'utilisation d'informations d'identification et de profils d'utilisateur peut comporter plusieurs niveaux. Prenons l'exemple d'un scénario d'authentification simple en entreprise (voir la figure 2). Une utilisatrice professionnelle nommée Alice s'authentifie sur son poste de travail Windows. Elle se connecte ensuite à une application exécutée à distance, en s'authentifiant à l'aide d'un identifiant Active Directory de domaine Windows ou peut-être de Kerberos à condition que son poste de travail dispose d'un ticket valable. Dans ce scénario, la chaîne d'authentification implique une seule personne et ses informations d'identification.

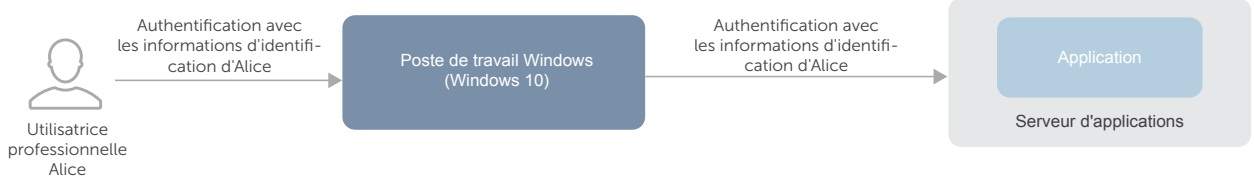


Figure 2 : authentification type en entreprise

Intéressons-nous à présent au scénario d'automatisation assistée illustré dans la figure 3. Dans ce cas-ci, l'utilisateur (Louis) teste un robot ou exécute une automatisation assistée au cours de sa journée de travail habituelle. À l'étape 1, il s'authentifie auprès du poste de travail d'exécution de robots avec ses informations d'identification personnelles (tout comme Alice dans le scénario précédent).
À l'étape 2, il lance le client Automation Anywhere Enterprise et saisit son ID utilisateur et son mot de passe d'accès à la Control Room, ce qui entraîne l'authentification du logiciel client auprès de cette dernière. À l'étape 3, il exécute le robot, qui, à son tour, accède à une application exigeant une authentification. Deux cas de figure sont alors possibles. Les informations d'identification utilisées par le robot lors de cette étape peuvent être stockées dans le coffre d'accréditation (Credential Vault) de l'entreprise et extraites par le robot pendant l'exécution. Ou alors, il peut y avoir une authentification pass-through avec les informations d'identification personnelles de Louis (basée sur le fait que Louis s'est authentifié auprès du domaine et qu'il possède un ticket Kerberos, ou sur l'utilisation d'une authentification unique). Dans les deux cas, trois niveaux d'identification et d'authentification sont appliqués.

Cette triple authentification est également utilisée dans le scénario d'automatisation non assistée illustré dans la figure 4, mais avec quelques changements. Dans ce cas, l'opérateur RPA (nommé Charles) commence par s'authentifier auprès de la Control Room afin de pouvoir sélectionner un robot à exécuter, soit de manière immédiate, soit au moment défini dans le planning.

À l'étape 2, lorsque l'exécution du robot débute, la Control Room lance une connexion automatique au poste de travail du Bot Runner avec les informations d'identification personnelles de ce dernier. Après que le robot est téléchargé vers la fonction Player locale (étape 3) et commence à s'exécuter, il s'authentifie auprès de l'application cible avec les informations d'identification personnelles de l'utilisateur de l'application de robots (étape 4). Tout comme dans le scénario d'automatisation assistée, ces informations d'identification peuvent être extraites du Credential Vault ou être celles de l'utilisateur du Bot Runner (pass-through d'authentification).

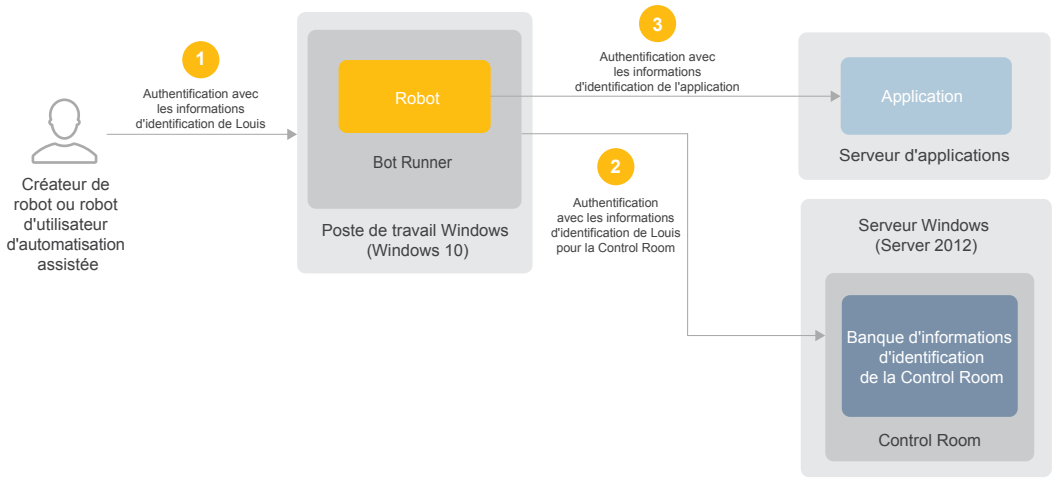


Figure 3 : processus d'authentification du scénario d'automatisation assistée

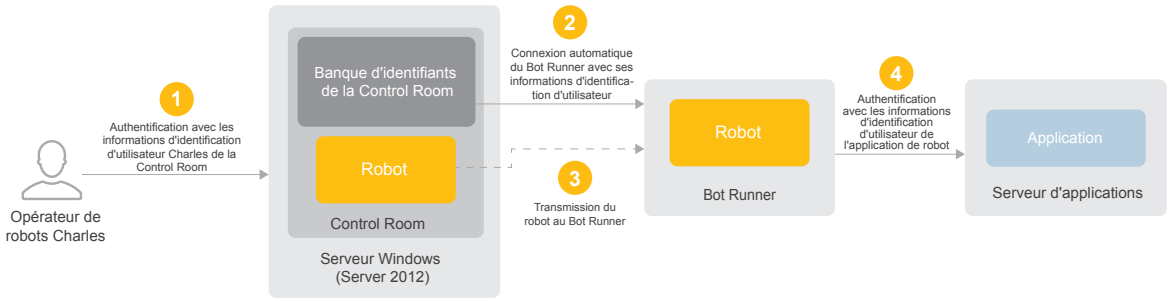


Figure 4 : processus d'authentification du scénario d'automatisation non assistée

Options d'authentification et intégrations IAM

Les options prises en charge pour l'authentification auprès de la Control Room incluent Active Directory avec LDAP, Active Directory avec Kerberos et l'authentification locale à l'aide du Credential Vault intégré (abordée dans une section ultérieure).

D'autres options de gestion des identités et des accès sont disponibles pour les déploiements en entreprise, notamment :

+ Prise en charge de l'authentification unique via SAML 2.0
+ Intégration à des solutions de fournisseurs tiers pour la gestion des informations d'identification/accès avec privilèges (par ex., CyberArk)

CONTRÔLE INTÉGRAL DE L'ACCÈS EN FONCTION DES RÔLES

L'authentification réussie ne constitue que le premier niveau du contrôle d'accès obligatoire tel qu'il est mis en œuvre et permis par l'architecture de sécurité Automation Anywhere Enterprise. L'autorisation est tout aussi importante, surtout en matière de respect de ces principes de base que sont le moindre privilège et la séparation des responsabilités. L'autorisation dans Automation Anywhere est configurée à l'aide du contrôle d'accès ultraprécis en fonction du rôle (ou RBAC).

Pour illustrer le RBAC, nous allons définir quelques rôles distincts. Les rôles que vous utilisez lors de votre déploiement peuvent être légèrement différents et il est possible que vous ayez des rôles supplémentaires. Il existe cinq rôles distincts (voir tableau 1) à prendre en compte dans l'architecture de base et pour les principales fonctions de la plateforme RPA. Les créateurs de robots utilisent le client Bot Creator pour extraire la logique métier et créer les automatisations correspondantes. Ils travaillent avec des applications de test et des ensembles de données pour éviter que les systèmes de production ne subissent d'impact au cours de la phase de développement. Un robot passera généralement par de nombreuses itérations et versions différentes, non seulement durant la phase de développement initiale, mais aussi à chaque mise à jour des processus métier associés et/ou de l'application cible. Les testeurs de robots ont eux aussi recours au client Bot Creator pour tester les performances, l'intégrité des données et la sécurité des robots, s'assurant que chacun d'eux exécute les tâches qu'il est censé accomplir et de façon sûre. Ils interviennent en tant que deuxième phase d'autorisation du robot, avant que celui-ci ne puisse s'exécuter avec les applications et données de production.

Après qu'un robot a passé les tests et l'évaluation de sécurité, le promoteur de robots collabore avec les créateurs ou testeurs de robots pour désigner la version du robot à utiliser en production. Cette version sera la seule à être visible à l'opérateur de robots, chargé de coordonner la planification et l'exécution du robot avec la ou les unités opérationnelles. Cet opérateur est également responsable de la surveillance des performances du robot au sein de la Control Room, et notamment de la résolution des problèmes d'exécution susceptibles de se produire. Enfin, l'administration globale de la plateforme, y compris la configuration des composants, des interfaces et de tous les rôles/autorisations, incombe à l'administrateur RPA.

Séparation avancée des responsabilités

Cette série de rôles constitue un point de départ du contrôle d'accès basé sur les rôles (RBAC). Néanmoins, il est possible de renforcer la séparation des responsabilités au sein de la plateforme Automation Anywhere Enterprise. Au moyen de l'assistant de création de rôles, les administrateurs peuvent aisément définir des rôles personnalisés, en attribuant des privilèges/autorisations pour l'ensemble des objets et fonctions de la Control Room. Parmi ceux-ci, citons la gestion des utilisateurs, les licences, Credential Vault, les ensembles de Bot Runner, les plannings des robots, les opérations des robots/tableaux de bord et les journaux d'audit. À mesure que chaque privilège est sélectionné, l'assistant ajoute dynamiquement des étapes pour les privilèges subordonnés/dérivés.

Par exemple, lorsque les privilèges BOTS (ROBOTS) > View my bots (Afficher mes robots) > Run my bots (Exécuter mes robots) sont sélectionnés (voir figure 5), le flux de travail ajoute une étape précisant les dossiers de robots spécifiques (et donc les ensembles de robots) auxquels l'accès est accordé. L'avantage est qu'il est possible de définir des rôles très représentatifs, avec des contrôles d'accès extrêmement précis et suffisants pour répondre aux besoins des environnements les plus exigeants (notamment en matière de sécurité) et soumis à des réglementations de conformité très strictes.

Rôle	Description
Administrateur RPA	Responsable de l'administration du système (configuration des composants, des rôles et des interfaces)
Concepteur de robots	Expert des processus métier qui crée les robots à l'aide de l'éditeur de tâches et effectue les tests fonctionnels de base
Testeur de robots	Testeur chargé de l'assurance qualité qui vérifie la précision fonctionnelle, les performances et la sécurité des robots
Promoteur de robots	Administrateur responsable de l'approbation des robots et de leur transition entre les phases de développement, de test et de production
Opérateur RPA	Opérateur chargé de la planification, de l'exécution et de la surveillance des performances des robots

Tableau 1 : principaux rôles RPA dans Automation Anywhere Enterprise

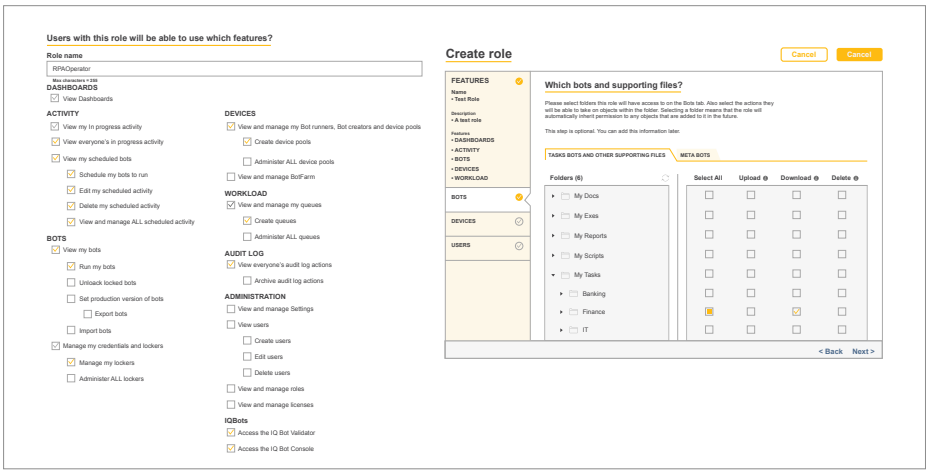


Figure 5 : création des rôles avec système d'autorisation ultraprécis

Plans de contrôle indépendants

Outre les fonctionnalités RBAC complètes, Automation Anywhere Enterprise assure de façon intrinsèque la séparation logique des responsabilités grâce à son architecture qui répartit minutieusement les tâches de développement des robots et d'exécution des robots.

Ainsi, les créateurs de robots peuvent uniquement charger et télécharger les robots sur le système de contrôle des versions dans la Control Room. Quant aux Bot Runner, ils sont limités à l'exécution des robots ; ils n'ont pas accès aux fonctions de création et de test des robots. Cette séparation des responsabilités mise en œuvre via l'architecture constitue un système de double autorisation conforme aux meilleures pratiques recommandées par l'Institut national des normes (National Institute of Standards), étant donné qu'elle requiert (au minimum) à la fois un développeur et un utilisateur professionnel pour permettre l'automatisation d'un processus métier.

Domaines de traitement indépendants

La mise en place de domaines de traitement indépendants (voir figure 6) est un cas d'utilisation très performant des fonctionnalités RBAC de la plateforme, en particulier pour les grandes entreprises. Dans ce contexte, le « domaine de traitement » est un ensemble d'automatisations (robots), de Bot Runner et d'utilisateurs. Elle peut être accomplie en organisant/stockant de façon stricte les robots de chaque domaine souhaité dans un dossier correspondant de la Control Room.

Exemple concret : des robots associés à des applications financières seraient placés dans un dossier Finance, alors que ceux relevant des ressources humaines seraient placés dans un dossier RH. Ensuite, les opérateurs de robots du service financier se verraient attribuer des privilèges pour les robots et Bot Runner associés aux finances uniquement, tandis que ceux du département des ressources humaines recevraient des privilèges sur les robots et les Bot Runner uniquement. Le même principe s'applique aux autres domaines de traitement/d'automatisation. (Voir la **figure 6**.)

Au final, cela renforce la séparation des responsabilités et l'isolation des applications et données associées, cette fois au niveau du domaine de traitement, chaque opérateur n'étant pas autorisé à voir ou à utiliser les robots n'appartenant pas à son propre domaine.

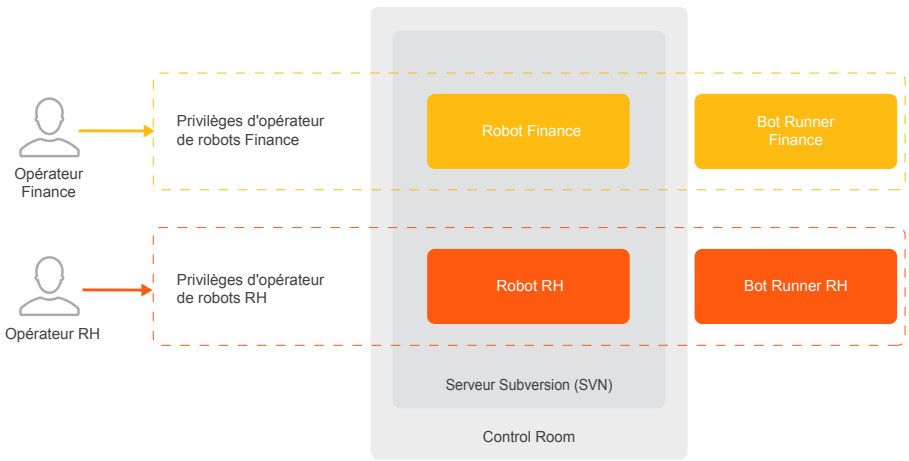


Figure 6 : prise en charge des domaines de traitement indépendants

PROTECTION DES DONNÉES DE BOUT EN BOUT

L'authentification à plusieurs niveaux et le contrôle d'accès ultraprécis sont essentiels pour garantir que l'environnement soit strictement contrôlé. De même, la protection des données de bout en bout est une condition sine qua non pour préserver la confidentialité et l'intégrité des processus essentiels pour l'entreprise, ainsi que de ses données sensibles et informations secrètes associées (telles que les informations d'identification).

La plateforme Automation Anywhere Enterprise répond à ce besoin en offrant un Credential Vault intégré de même qu'un ensemble complet de mesures de sécurité qui protègent les données inactives et en transit, mais aussi les données en cours d'utilisation sur les systèmes individuels.

Clés de cryptage et Credential Vault

La **figure 7** montre les principales clés de cryptage utilisées par la plateforme, ainsi que leur relation avec le Credential Vault. Toutes les opérations de cryptage sont effectuées à l'aide de modules cryptographiques validés FIPS 140-2 de niveau 1.

Durant l'installation (partie gauche de la **figure 7**), le système génère une paire de clés publique/privée RSA 2 048 bits et une clé AES 256 bits. La clé privée de la paire RSA 2 048 bits est appelée clé principale, et la clé AES 256 bits, clé de données. La clé principale est fournie à l'administrateur qui effectue l'installation, lequel doit la conserver de façon sécurisée dans un emplacement protégé physiquement externe au système. La clé publique est utilisée pour crypter la clé de données. Ensuite, la clé publique et la clé de données cryptée sont toutes deux stockées dans la base de données.

Au démarrage ou au redémarrage de la Control Room (partie droite de la **figure 7**), l'administrateur est invité à fournir la clé principale. La clé de données cryptée est ensuite extraite de la base de données, décryptée à l'aide de la clé principale, après quoi elle est prête à être utilisée. Chaque fois que le système stocke et extrait des données dans le Credential Vault, la clé de données est utilisée pour les crypter et les décrypter.

Le Credential Vault sert à stocker toutes les informations d'identification gérées par le système et les données de configuration système essentielles. Il permet également de conserver d'autres données sensibles (par ex., paires nom-valeur) utilisées dans les automatisations de l'entreprise. Les créateurs de robots peuvent ainsi éviter cette pratique contraire à la sécurité qui consiste à coder en dur, directement au sein de leurs automatisations, les informations d'identification et autres données/éléments sensibles. Dans le Credential Vault, les données sont organisées par casiers. Ils permettent d'attribuer des données d'identification cryptées pour chaque utilisateur, protégées par des privilèges et des rôles, dans le cadre des fonctionnalités RBAC d'Automation Anywhere. Chaque casier peut être assigné à un utilisateur ou rôle seul pour limiter l'accès à ce casier seulement à des utilisateurs RPA spécifiques.

Protection des données inactives

En plus de crypter les informations d'identification locales et les données d'exécution utilisées par les robots, le Credential Vault stocke de façon sécurisée les paramètres de configuration sensibles et les informations des services de messagerie électronique et de contrôle de version intégral.

Protection des données en transit

Tous les services réseau exécutés sur les clients et dans la Control Room font appel à TLS (Transport Layer Security) 1.2 pour garantir la sécurité et l'intégrité des données pendant leur transfert entre composants.

Les informations d'identification utilisées pour l'authentification des Bot Creator/Runner auprès de la Control Room sont cryptées avant d'être envoyées via une connexion sécurisée au moyen de TLS. Non seulement ce niveau de cryptage supplémentaire protège contre les incidents liés à la pile réseau (par exemple, la faille Heartbleed), mais il prévient également la divulgation d'informations d'identification dans les implémentations où le point de terminaison de la connexion TLS au niveau de la couche externe est un équilibreur de charge front-end.

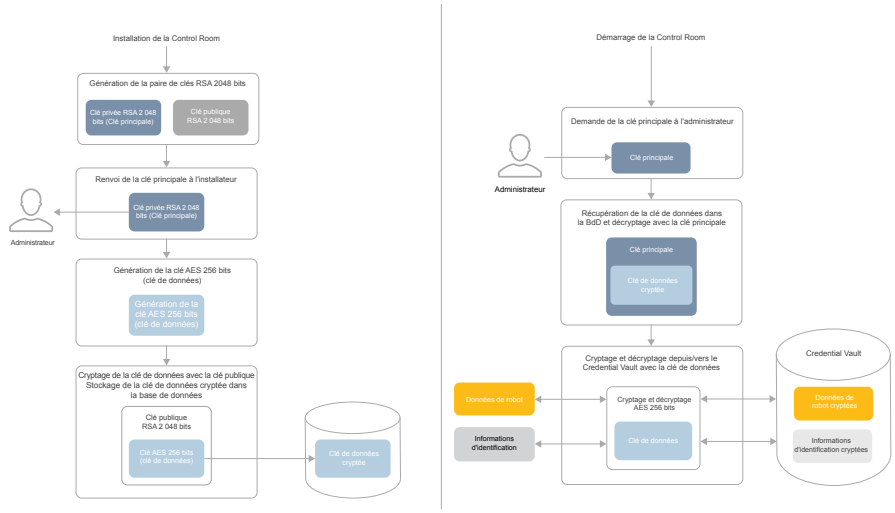


Figure 7 : architecture de cryptage d'Automation Anywhere Enterprise

Protection des données en cours d'utilisation

La sécurité à l'exécution commence par la protection distribuée des informations d'identification. Plus précisément, il n'existe pas de stockage local pour ces informations sur les Bot Runner. En fait, les informations d'identification et autres données extraites dynamiquement à partir du Credential Vault afin d'être utilisées au sein des automatisations sont uniquement conservées au format crypté dans une mémoire volatile. Elles sont ensuite effacées une fois l'exécution du robot associé terminée.

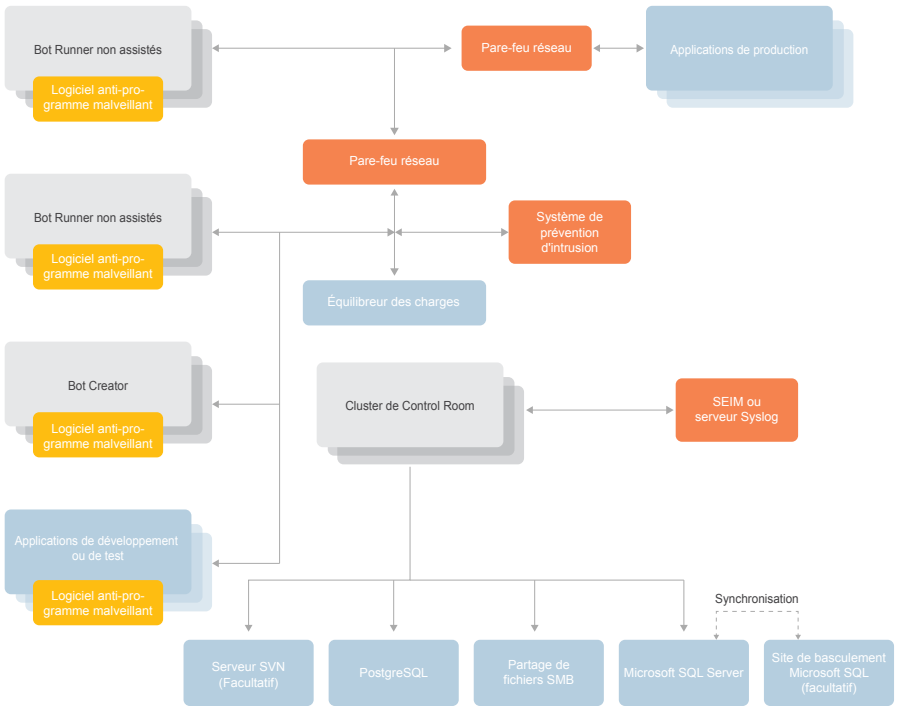
D'autres fonctionnalités et options de configuration peuvent être employées pour éviter l'accès non autorisé aux informations confidentielles (fuite de données) ou le sabotage des robots pendant leur exécution, notamment :

+ Mode furtif – Aucune fenêtre de programme n'est affichée sur l'écran local et les utilisateurs connectés ont la possibilité de désactiver la capture d'image sur les Bot Creator and Bot Runner, empêchant ainsi que les informations sensibles affichées à l'écran puissent être stockées dans les robots.
+ Verrouillage de la saisie – Il est possible de désactiver la souris et le clavier de la machine sur laquelle une automatisation s'exécute.
+ Durée limitée – Le système permet de définir un délai au terme duquel une automatisation sera interrompue si elle n'est pas arrivée au bout de son exécution.
+ Contrôle centralisé – La Control Room permet de contrôler de façon centralisée (suspendre, réactiver, arrêter) le fonctionnement d'automatisations exécutées à distance.

SÉCURISATION DU DÉPLOIEMENT RPA

L'architecture AAE se compose de l'infrastructure de bureau et de serveur standard pour les clients et de la Control Room. Cette section détaille les meilleures pratiques en matière de sécurité dans le cadre de la RPA pour les contrôles de sécurité externes qui sont mis en place dans n'importe quelle entreprise. Les pare-feu basés sur le réseau, les systèmes de détection d'intrusion, les logiciels anti-programme malveillant et les serveurs de journal externes sont tous des contrôles de sécurité standard qui sont aussi pertinents pour le déploiement RPA qu'ils le sont pour l'autre infrastructure de votre environnement. Le diagramme ci-dessous montre logiquement où ces composants sont déployés dans le déploiement RPA.

Chaque contrôle de sécurité externe est abordé en détail ci-dessous en termes de placement et de configuration. Les services réseau tels qu'Active Directory, SVN Server, PostgreSQL, SMB File Share, Microsoft SQL et les Applications de production peuvent être consultés via des pare-feu réseau ou directement, en fonction de leur placement par rapport aux composants RPA.



Contrôle d’accès basé sur le réseau - Protection de la RPA à l’aide de pare-feu

Les pare-feu basés sur le réseau et le pare-feu local basé sur le serveur sont utilisés pour protéger la Control Room ou tous les nœuds dans un cluster de Control Room lors de l’utilisation d’un déploiement groupé. Par défaut, seuls les protocoles requis sur la Control Room doivent être autorisés à partir du réseau d’entreprise. En outre, tous les protocoles de mise en cluster ne doivent être autorisés qu’entre les nœuds du cluster de la Control Room. Les pare-feu basés sur le réseau sont utilisés pour isoler les environnements RPA de développement, de test et de production du réseau d’entreprise, ainsi que les uns des autres (voir section Sécurisation du cycle de vie de développement des logiciels ci-dessous).

Pour les environnements d’automatisation non assistée, les exécuteurs de robots sont placés dans un réseau isolé distinct et protégés par un pare-feu basé sur le réseau. Les automatisations assistées sont exécutées à partir des postes de travail d’entreprise, sur lesquels est installé le client d’exécuteur de robots, et elles sont protégées par les pare-feu de périmètre d’entreprise ou les pare-feu internes protégeant l’infrastructure de bureau de l’entreprise, comme n’importe quel bureau.

Reportez-vous aux tableaux ci-dessous pour connaître les protocoles utilisés par la Control Room et le client.

3.10 List of Port Numbers

Below table lists the configurable ports used by our platform

3.10.1 Client

Port	Description	Deployment	Used for
110 995	POP3	Client	“Email Automation” command to retrieve emails from mail server.
143 993	IMAP	Client	
21	FTP/SFTP	Client	“FTP/SFTP” command
25 465 587	SMTP	Client	“Send email, Error handling” command “Email notification” feature
161	UDP	Client	“SNMP” command
22 23	Terminal Emulator	Client	“Terminal Emulator” command
4530	TCP	Client (AAProxyServer.exe)	Used by the client to communicate with plugins via TCP socket for AAE Client, Editor or Player

80	HTTP	Control Room	Web UI access (No TLS, not recommended)
443	HTTPS	Control Room	Web UI access (Recommended)
25 465 587	SMTP	Control Room	Send email when important events occur (user created, password set/reset, role changed etc.)
1433	TCP	Microsoft SQL Server	Default port used by Microsoft SQL Server
5672	TCP	Control Room	Cluster Messaging
47500-47600	TCP	Control Room	Cluster Messaging and Caching
47100-47200	TCP	Control Room	Cluster Messaging and Caching

Logiciel anti-programme malveillant - Protection de la RPA contre les virus et les logiciels malveillants

Le client AA fonctionne sur l’infrastructure de classe bureau et doit être considéré comme un bureau d’entreprise à tous égards. Les logiciels anti-programme malveillant/antivirus sont utilisés pour protéger l’environnement client contre les logiciels malveillants se présentant sous la forme de virus et de malwares.

Systèmes de détection d’intrusion - Protection de la RPA contre les attaques directes

Les systèmes de détection et de prévention des intrusions (IPS) protègent le réseau d’entreprise en détectant les attaques basées sur le réseau grâce à l’analyse du trafic réseau. Comme toute autre section critique du centre de données, la plateforme RPA est protégée au point de sortie, derrière le pare-feu basé sur le réseau, par un système IPS. Le placement d’IPS dans votre réseau doit être décidé en fonction d’une convention d’entreprise et doit s’appliquer de la même manière à la plateforme RPA.

Gestion des incidents de sécurité - Protection de la RPA à l’aide de l’audit externe

Les journaux de la Control Room peuvent être transmis à un système de gestion des incidents de sécurité (SEIM) pour le stockage externe, le traitement et les alertes. L’intégration à SIEM ou à tout système de consolidation et de réduction d’audit basé sur Syslog améliore considérablement la position de sécurité et la conformité à la gouvernance. Configurez la Control Room de façon à ce qu’elle transmette les journaux d’audit au serveur de collecte Syslog approprié dans l’environnement.

VALIDATION EXTERNE DES CONTRÔLES DE SÉCURITÉ

Pour les agences fédérales, lors du déploiement d'AAE, l'un des prérequis est de répondre aux exigences en matière de contrôle de sécurité de la Loi fédérale sur la gestion de la sécurité de l'information (Federal Information Security Management Act, ou FISMA) lorsqu'AAE est déployé dans un système informatique sur site.

AAE prend en charge les fonctionnalités de sécurité qui intègrent AAE à un environnement déjà existant et conforme à la FISMA. Il prend également en charge les contrôles tels que l'authentification centralisée (par ex., Active Directory (AD), la gestion centralisée des journaux, les capacités d'analyse et de génération de rapports avec la gestion des événements et des informations de sécurité (SIEM), ainsi que le partitionnement du réseau et le contrôle d'accès au réseau avec des réseaux locaux virtuels privés (VLAN) et des pare-feu) mis en œuvre et pouvant être intégrés à AAE, le cas échéant.

AAE prend en charge la mise en œuvre des contrôles de sécurité applicables, permettant aux informaticiens de mettre à jour le SSP d'un système informatique afin de déployer et d'utiliser AAE de manière sécurisée. Pour plus de détails concernant les contrôles FISMA, se référer aux fonctionnalités et aux capacités de base d'AAE qui ont été comparées avec les contrôles sélectionnés Moderate FISMA dans NIST SP 800-53 rev. 4 et analysées en matière de compatibilité et d'impact sur les exigences de contrôle. Le cadre NIST peut être mappé à d'autres cadres tels que ceux de la loi HIPAA et de la PCI. Pour plus de détails sur les contrôles FISMA mis en œuvre dans Automation Anywhere Enterprise, consultez le livre blanc Automation Anywhere Enterprise - Through The Lense of FISMA.

PRISE EN CHARGE DU CYCLE DE VIE SDLC SÉCURISÉ

Il est possible d'optimiser les contrôles et les mesures de protection mis en place dans l'environnement d'automatisation. Pour ce faire, le scénario de déploiement de base décrit précédemment peut être « étendu » pour mieux respecter les meilleures pratiques du cycle de vie sécurisé du développement d'un logiciel (SDLC), telles que celles prescrites par la loi FISMA, le programme FedRamp et la norme PCI DSS. Le modèle de déploiement avancé résultant est composé de trois zones RPA distinctes, qui contrôlent respectivement le développement, les tests d'acceptation utilisateur (UAT) et la production (voir la figure 8). Chaque zone est séparée (isolée) logiquement et contient des groupes d'utilisateurs différents dotés de rôles et de privilèges distincts. Les lignes verticales en pointillés représentent la segmentation réseau et les pare-feu.

Comme dans le modèle de déploiement de base, le cycle de vie d'un robot débute par le développement. Lorsque les créateurs de robots sont satisfaits du robot, les promoteurs de robots UAT le transfèrent du référentiel de gestion des versions (SVN), appartenant à la zone de développement, vers le référentiel UAT. La zone UAT est exclusivement réservée aux tests des robots concernant leur précision, leurs performances et leur sécurité. Lorsqu'un robot réussit les tests d'acceptation, un promoteur de robots de production le transfère vers la zone de production. À ce stade, il obtient le statut de robot de production et devient disponible aux opérateurs RPA qui peuvent ainsi l'utiliser avec les applications de production. À chaque étape du processus, 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 une force de travail numérique à la fois fiable, évolutive, efficace, sécurisée et conforme.

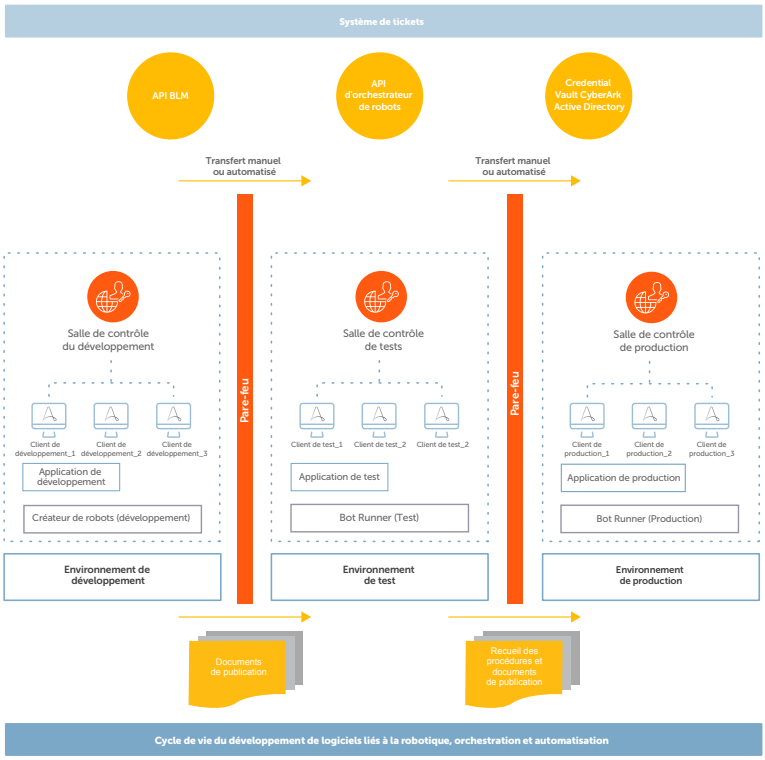


Figure 8 : modèle de déploiement avancé pour un cycle SDLC intégral

JOURNALISATION ET SURVEILLANCE

Des fonctions complètes de journaux d'audit, de surveillance et de création de rapports constituent des éléments essentiels de l'architecture de sécurité de toute solution informatique digne de ce nom. Automation Anywhere Enterprise ne fait pas exception à la règle.

Dans l'ensemble de la plateforme, des détails sur les événements (qui, quoi, quand, où et quel impact) sont automatiquement capturés pour plus de 60 types d'actions d'utilisateur/d'entité. Ces événements incluent notamment la création, la modification, l'activation, la désactivation et la suppression d'utilisateurs, de robots et de Bot Creator et Bot Runner. La non-répudiation est assurée grâce à la combinaison de la capture automatique des informations, de l'association de chaque activité à une entité spécifique et d'une politique en lecture seule par défaut. La fonction RBAC peut également être utilisée pour contrôler de façon stricte les rôles bénéficiant d'une visibilité sur les journaux d'audit en premier lieu.

En ce qui concerne la surveillance, les rapports et les tableaux de bord automatisés sont accessibles dans la Control Room et peuvent être personnalisés de façon à identifier et à signaler les activités anormales (ou toute autre information jugée intéressante par l'équipe d'automatisation ou de sécurité). De plus, la possibilité d'exporter les journaux permet aux entreprises de tirer parti d'autres outils d'infrastructure d'analyse, de création de rapports et d'enquête/de réponse en cas d'incident déjà en place, tels que la gestion des événements et des informations de sécurité (SIEM), l'analyse du comportement des utilisateurs et des entités (UEBA) et les analyses avancées.

LES PLUS POUR FAVORISER LA SÉCURITÉ ET LA RÉSILIENCE DE L'ENTREPRISE

Pour soutenir la réalisation des objectifs de sécurité et de résilience des entreprises, Automation Anywhere Enterprise va encore plus loin, notamment avec :

+ Une architecture de composants distribuée (et flexible) capable de s'adapter de façon transparente aux processus et à l'infrastructure de haute disponibilité/reprise après sinistre (HA/DR) existante de l'entreprise
+ Un système de contrôle intégral des versions (Apache Subversion) qui, associé aux fonctionnalités RBAC complètes de la plateforme, est capable d'implémenter et d'appliquer une politique et des processus de gestion des changements très rigoureux
+ Des outils tels que les cadres Hibernate et ReactJS, utilisés lors du développement du code de la plateforme, qui contribuent à éliminer la vulnérabilité aux attaques courantes, par exemple celles basées sur l'injection de code SQL ou des scripts intersites (XSS)
+ Un protocole/plan de sécurité pour le développement de code nécessitant des analyses en continu à l'aide de plusieurs outils et sur plusieurs niveaux pour détecter et corriger les vulnérabilités logicielles

Pour plus de détails sur ces fonctions et les nombreux autres contrôles, mesures de protection et fonctionnalités de sécurité intégrés à Automation Anywhere Enterprise, consultez : https://www.automationanywhere.com/images/Enterprise-Architecture.pdf

AUTOMATISATION DES API

Alors que le déploiement de robots se développe de façon exponentielle, il apporte son lot de nouveaux défis en matière d'authentification sécurisée à grande échelle et de gestion du cycle de vie opérationnel des robots. Il est nécessaire de réduire le temps de déploiement et d'éliminer les erreurs humaines. Automation Anywhere propose des API qui s'intègrent aux automatisations de tiers pour l'authentification sécurisée et l'orchestration de la gestion du cycle de vie des robots. Cette section décrira les API procurant les capacités mentionnées ci-dessus.

Credential Vault - API

Le Credential Vault d'Automation Anywhere est utilisé pour le stockage crypté des informations d'identification, lesquelles sont utilisées par une automatisation (robot), pour s'authentifier de manière sécurisée. Les API du Credential Vault peuvent être utilisées pour la synchronisation des informations d'identification avec les systèmes externes de gestion des identités et des accès (Identity Access Management, ou IAM) via un programme d'orchestrateur, des scénarios délicats où le robot se voit attribuer un mot de passe dans certaines circonstances et qui change après chaque utilisation, la gestion externe des informations d'identification via un programme d'orchestrateur externe.

API de déploiement de robots

L'API de déploiement de robots permet aux applications externes de lancer un flux de travail d'automatisation sur un Bot Runner. Lorsqu'un robot peut être lancé via l'API, dans un cadre sécurisé, les robots qui exécutent des fonctions liées à la sécurité peuvent être orchestrés par une application externe. Par exemple, une solution SIEM peut déclencher une alerte qui lance un robot pour effectuer la collecte de données sur le système indiqué par l'alerte. Cette collecte de données peut être le déchargement de tables de processus en cours d'exécution, d'instantanés de sommes de contrôle de fichiers, de l'utilisation des ressources et d'utilisateurs actuellement connectés.

API de gestion du cycle de vie des robots

L'API de Gestion du cycle de vie des robots (Bot Lifecycle Management, ou BLM) permet à une application externe d'orchestration d'automatiser le processus de déplacement de robots d'une Control Room à une autre. Il s'agit d'un point important pour les entreprises qui utilisent le cycle de vie SDLC sécurisé. Pour plus d'informations, consultez la section concernant SDLC. Le processus SDLC peut être automatisé en intégrant des systèmes de tickets tels que Jira ou Zendesk pour déclencher le développement, les tests, l'évaluation de la sécurité et la promotion pour la production des robots. Un processus SDLC automatisé offre un recueil des procédures pour la création de robots, de manière à garantir que chaque robot en production exécute ce pour quoi il a été conçu, avec un processus auditable qui fournit tous les contrôles de gouvernance dont votre organisation a besoin.

CONCLUSION

L'automatisation des processus par la robotique s'annonce très prometteuse pour les entreprises modernes désireuses de réduire leurs coûts opérationnels, d'améliorer la satisfaction des clients et de prendre une longueur d'avance sur la concurrence. Plateforme leader du marché pour une force de travail numérique, Automation Anywhere Enterprise les aide à tirer le meilleur parti de ces avantages et d'autres encore. Comment ? En offrant non seulement la fiabilité, l'évolutivité et la simplicité d'utilisation nécessaires pour réussir, mais également la sécurité adaptée aux grandes entreprises indispensable pour préserver la confidentialité, l'intégrité et la disponibilité de tout l'environnement d'automatisation.

Pour en savoir plus sur Automation Anywhere Enterprise, consultez notre site à l'adresse : https://www.automationanywhere.com/products/enterprise