Seguridad de calidad empresarial para la automatización robótica de procesos

INTRODUCCIÓN

Automation Anywhere comenzó hace 15 años con una simple pregunta: ¿Por qué, después de más de 20 años de inversión en tecnologías de automatización de los procesos de negocios, se ha automatizado menos del 20 % de las tareas que se podrían haber automatizado? Rápidamente se centraron en el desafío principal: el 85 % de los sistemas empresariales carecen de interfaces de programación de aplicaciones (API) bien definidas, lo que resulta en un creciente aumento de trabajo pendiente de IT en cuanto a solicitudes de integración por parte de las líneas de negocio.

La automatización robótica de procesos (RPA) nació con la visión de otorgar a los usuarios comerciales la posibilidad de crear bots de software que puedan interactuar con los sistemas empresariales tal como lo hacen los humanos. La RPA permite a cualquier usuario comercial con conocimientos de macros de Excel registrar los pasos utilizados en tareas repetitivas y convertirlos en un script fácil de entender para bots. Los bots de RPA pueden iniciar sesión en las aplicaciones empresariales por medio de credenciales, igual que los humanos, y automatizar las tareas que involucran cualquier aplicación empresarial, incluidas las aplicaciones heredadas sin API. El procesamiento de reclamos, el procesamiento de préstamos, las conciliaciones de cuentas, la creación o envío de facturas y la generación de informes son solo algunos ejemplos de las automatizaciones posibles que se extienden a través de las diferentes disciplinas empresariales.

Es fácil ver el potencial de los ahorros sustanciales en tiempo y costos, la mejora en la satisfacción del cliente, el aumento en la moral de los empleados y la habilidad de construir una ventaja imponente por encima de los competidores mediante el uso de la RPA. Sin embargo, la obtención completa de estas ganancias depende de si se cuenta con una solución de calidad empresarial.

Algunos de los criterios esenciales básicos de la automatización son proveer confiabilidad sólida y absoluta, escalabilidad y una gama amplia de funciones determinadas para maximizar la aplicabilidad y la utilidad. Pero estos elementos no cubren el requisito fundamental de las empresas: la seguridad integral. Es esencial contar con una arquitectura de seguridad sólida con funciones que permitan el soporte completo para los principios fundamentales, tales como privilegios menores y la separación de tareas durante la entrega de protección integral para las aplicaciones cruciales y los datos confidenciales involucrados.

En este artículo, se presenta una descripción general sobre el estándar más alto de la industria en cuanto a la seguridad de calidad empresarial tal como se demuestra en la plataforma de fuerza de trabajo digital líder del mercado, Automation Anywhere Enterprise.

Es fácil ver el potencial de los ahorros sustanciales en tiempo y costos, la mejora en la satisfacción del cliente, el aumento en la moral de los empleados y la habilidad de construir una ventaja imponente por encima de los competidores mediante el uso de la RPA. Sin embargo, la obtención completa de estas ganancias depende de si se cuenta con una solución de calidad empresarial.

ARQUITECTURA Y OPERACIONES

Comprender los controles de seguridad que se necesitan para la implementación de RPA de calidad empresarial depende de la compresión de los componentes que constituyen la solución y las operaciones.

Componentes básicos

Tal como se muestra en la Figura 1, los componentes arquitectónicos básicos de Automation Anywhere Enterprise son Control Room, Bot Creators y Bot Runners.

Control Room

Control Room cumple la función de cerebro del entorno de automatización. Es un sistema de gestión Windows basado en servidores, con una base de datos integral, que proporciona una visión unificada para el sistema de administración en general. Control Room es también el lugar donde los operadores de la RPA organizan la fuerza de trabajo digital; en otras palabras, programan, implementan, ejecutan, supervisan y administran las operaciones de los bots de la organización. Además, las funciones de control de versiones integradas (Apache Subversion Server) facilitan la colaboración de múltiples usuarios mientras que ejecutan las mejores prácticas de gestión de cambio y establecen un depósito centralizado de los bots listos para la producción.

Bot Creator

Bot Creator se utiliza para crear bots. Es una aplicación de escritorio de Windows que funciona en un hardware de estación de trabajo o en una máquina virtual. Los expertos en procesos empresariales utilizan Bot Creator Client para crear y evaluar las automatizaciones. Los bots se crean mediante el uso del editor de tarea, mientras que las pruebas de bots, que utilizan datos de pruebas locales no productivas e instancias de aplicaciones, se facilitan mediante la función de jugador. Luego de las pruebas exitosas (p. ej., de rendimiento, integridad de los datos y seguridad), los bots se registran en el depósito de Control Room y quedan disponibles para implementarse en la producción.

Bot Runner

Bot Runner pone en funcionamiento a los bots. Por medio del mismo código de aplicación que Bot Creator Client, pero con una clave de licencia diferente, Bot Runner utiliza la función de jugador para ejecutar a los bots en el entorno de producción; es decir, utiliza las instancias de producción de la aplicación de destino y de los almacenes de datos de producción. De hecho, poner en funcionamiento a los bots es todo lo que pueden hacer las instancias de Bot Runner, ya que las funciones de creación y edición no están disponibles para ellos. Para operaciones altamente confiables y de gran escala, también se admiten combinaciones de Bot Runners.

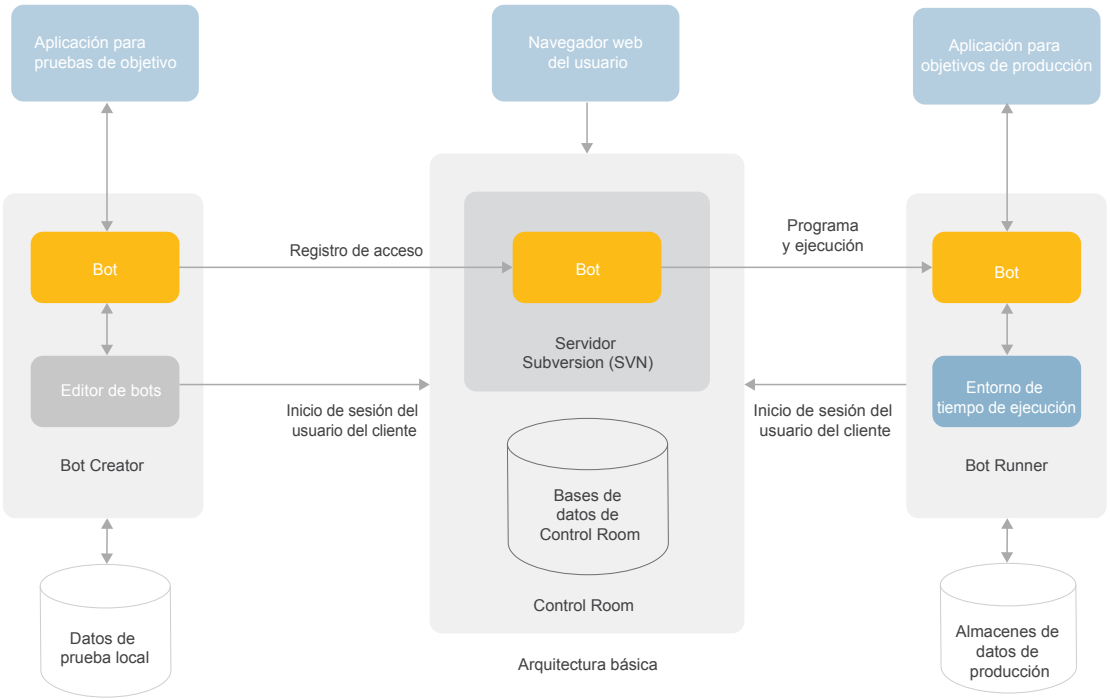


Figura 1: Arquitectura básica de Automation Anywhere Enterprise

Componentes adicionales de calidad empresarial

Al considerar operaciones de gran escala, surgen dos soluciones de RPA importantes para las organizaciones que buscan implementaciones de nivel empresarial: escalamiento a demanda y Bot Insight.

Escalamiento a demanda

Gracias a la nube pública de Amazon Web Services (AWS), Automation Anywhere Enterprise ofrece de manera eficaz la RPA como servicio, con todas las capacidades del asistente, que incluyen refuerzo o disminución flexible, medición basada en el uso, escalabilidad horizontal ilimitada, supervisión continua y registro de auditorías de la infraestructura de Bot Runner. Como resultado, se obtiene una alta disponibilidad de varios nodos que alimenta el rendimiento basado en acuerdos de nivel de servicio (SLA) y la continuidad del negocio, aun cuando existen fluctuaciones drásticas en la carga de trabajo de automatización.

Bot Insight

Bot Insight, un subsistema completamente integrado dentro de Control Room, lleva a cabo análisis casi en tiempo real de las operaciones de los bots y de los datos de los procesos empresariales. Bot Insight genera automáticamente paneles personalizables mediante el uso de algoritmos específicos para cada bot. El nivel de detalle que Bot Insight proporciona, basado en el registro de incidencias detallado de las operaciones de los bots, permite enviar alertas sutiles, hacer descubrimientos ad hoc, hacer análisis en profundidad interactivos, series temporales de análisis y tener una visión completa de los procesos operacionales o empresariales. Además, todos los datos se pueden exportar a un Sistema de gestión de eventos e información de seguridad (SIEM) para guardar los registros a fin de realizar análisis, investigaciones e informes adicionales.

Bots en acción: existen dos tipos de automatización

Antes de comenzar con las capacidades de seguridad de alto nivel de Automation Anywhere Entrerprise, es necesario aclarar que existen dos tipos básicos de automatización: surpervisada y no supervisada.

La automatización supervisada es aquella en la que el usuario está registrado en la máquina de Bot Runner para observar o ayudar de manera activa en la ejecución del bot. Las razones para tener a un usuario presente se pueden deber a que el bot cumple una función de utilidad que ayuda en el trabajo o que el bot realiza un trabajo de tipo en lotes que requiere un aporte periódico o una dirección circunstancial por parte de un usuario. A las automatizaciones supervisadas también se las conoce como automatizaciones de servicio al cliente.

Las automatizaciones no supervisadas, como su nombre lo indica, funcionan sin la necesidad de contar con la interacción del usuario u operador empresarial. Las automatizaciones no supervisadas, por lo general, se ejecutan por medio de un operador que tiene poco o nada de conocimiento del bot, de la aplicación que se está automatizando o del propósito de la automatización. El operador, junto con la unidad de negocio, programa los bots para que funcionen por medio de Bot Runners. Durante la ejecución, el operador monitorea los aspectos operacionales de los bots en funcionamiento, tales como el CPU, la memoria y el uso del almacenamiento para asegurarse de que los bots se estén ejecutando sin errores ni excepciones. Los paneles de Control Room muestran todos los detalles operacionales de los bots mientras están en funcionamiento.

IDENTIFICACIÓN Y AUTENTICACIÓN DE SEGURIDAD DE RPA EMPRESARIAL MULTICAPA

Un principio fundamental de la arquitectura de seguridad de Automation Anywhere Enterprise es que no se permite el acceso ni acciones sin la autorización previa de la entidad involucrada. Esto aplica tanto para los humanos como para los bots. Para entender la autorización en la RPA uno debe primero entender el proceso de autenticación para las automatizaciones supervisadas y no supervisadas.

QUIÉN ES QUIÉN: AUTENTICACIONES EMPRESARIALES TÍPICAS

Tanto las credenciales como las personas pueden ser multicapa. Considere un escenario de autenticación empresarial simple (vea la Figura 2). Un usuario de la empresa, Alice, se autentica en su estación de trabajo de Windows. Luego, Alice inicia sesión en una aplicación que se está ejecutando de manera remota. Lo hace mediante la autenticación de Active Directory de dominio de Windows o tal vez por medio de Kerberos instalado en su estación de trabajo y con un ticket válido. En este escenario, la cadena de autenticación involucra a una sola persona y sus credenciales.

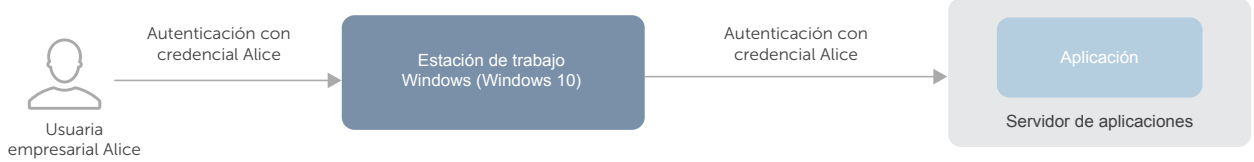


Figura 2: Autenticación empresarial típica

Ahora, considere un escenario de autenticación supervisada como se ejemplifica en la Figura 3. En este caso, el usuario, Bob, le está realizando pruebas a un bot o bien está llevando a cabo una automatización supervisada como parte de un día típico de trabajo. En el paso 1, él se autentica en la estación de trabajo del Bot Runner mediante sus credenciales personales (igual que en el escenario de Alice que se mencionó anteriormente). En el paso 2, él ejecuta el cliente de Automation Anywhere Enterprise e ingresa su identificación de usuario de Control Room y contraseña; de esta manera, autentica el software del cliente con Control Room. En el paso 3, pone en funcionamiento al bot que, a su vez, accede a la aplicación que requiere autenticación. Las credenciales que utiliza el bot en este paso pueden estar almacenadas en Credential Vault empresariales y el bot las puede recuperar durante el tiempo de ejecución, o bien, puede haber una transmisión de las credenciales personales de Bob (basada en el hecho de que Bob tiene una autenticación de dominio y un ticket de Kerberos o basada en cualquier inicio de sesión único que se utilice). En cualquiera de los casos, el resultado es un proceso de identificación y autenticación de tres capas en total.

También se utilizan tres capas de autenticación en el escenario de automatizaciones no supervisadas que se describe en la Figura 4, no obstante, con algunos cambios. En este caso, el usuario, un operador de RPA llamado Charles, comienza con la autenticación en Control Room para poder seleccionar un bot para poner en funcionamiento, ya sea de manera inmediata o a una hora programada.

En el paso 2, cuando comienza la hora de ejecución del bot, Control Room comienza un inicio de sesión automático en la estación de trabajo de Bot Runner, mediante el uso de la credencial del usuario de Bot Runner. Luego de que el bot se descarga en la función de jugador local (paso 3) y se empieza a ejecutar, se autentica en la aplicación de destino mediante el uso de la credencial del usuario de la aplicación bot (paso 4). Igual que en el caso del escenario de automatización surpervisada, la credencial del usuario de la aplicación bot puede ser una que se recuperó de Credential Vault o una que se transfirió de la credencial del usuario de Bot Ruuner.

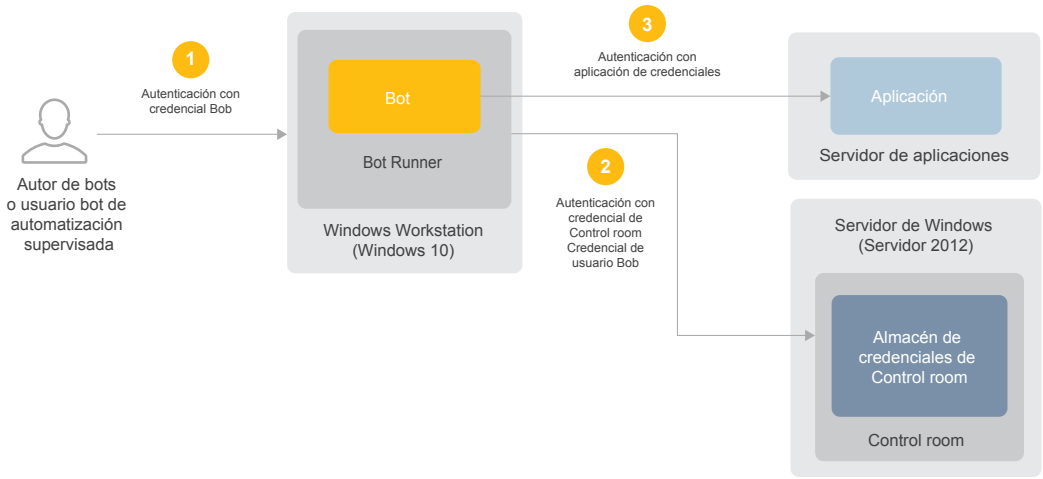


Figura 3: Proceso de autenticación en un escenario de automatización surpervisada

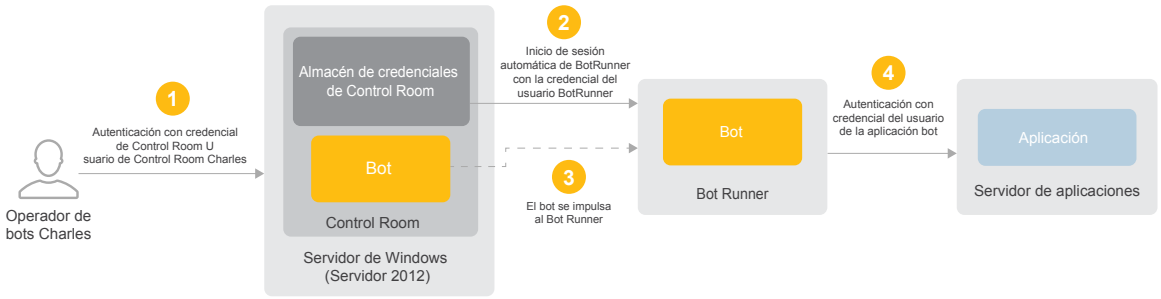


Figura 4: Proceso de autenticación en un escenario de automatización no supervisada

Opciones de autenticación e integraciones de Administración de identidad y acceso

Las opciones admitidas para la autenticación de Control Room incluyen Active Directory mediante el protocolo simplificado de acceso a directorios (LDAP), Active Directory mediante Kerberos y autenticación local mediante Credential Vault integrada (que se desarrolla en una sección posterior).

Otras opciones de administración de identidad y acceso disponibles para las implementaciones empresariales son las siguientes:

+ Soporte para SAML 2.0 basado en inicio de sesión único
+ Integración con soluciones de administración para accesos o credenciales privilegiados de terceros (p. ej. CyberArk)

CONTROL DE ACCESO BASADO EN ROLES COMPLETO

La autenticación exitosa es solo el primer nivel de la implementación del control de acceso obligatorio ofrecido por la arquitectura de seguridad de Automation Anywhere Enterprise. Igualmente importante es la autorización, especialmente cuando se trata de adherirse a los principios básicos de privilegios menores y separación de tareas. La autorización dentro de Automation Anywhere se configura con el control de acceso basado en roles o RBAC detallado.

Para ilustrar el RBAC definiremos algunos roles distintos. Los roles que utilice en su implementación pueden ser ligeramente diferentes y usted puede tener roles adicionales. Se deben distinguir cinco roles diferentes (ver Tabla 1) dentro de la arquitectura básica y las funciones principales de la plataforma de RPA. Los autores de bots utilizan Bot Creator Client para capturar la lógica empresarial y así crear las automatizaciones correspondientes. Los autores de bots trabajan con aplicaciones de prueba y conjuntos de datos para no producir un impacto en los sistemas de producción durante la etapa de desarrollo. Normalmente, un bot individual pasará por varias iteraciones y versiones diferentes, no solo durante el desarrollo inicial sino también siempre que los procesos empresariales asociados o las aplicaciones de destino se actualicen. Los evaluadores de bots también trabajan con Bot Creator Client para realizar pruebas en cuanto al desempeño, la integridad de datos y la seguridad, con el objetivo de garantizar que cada bot esté realizando las funciones para las cuales está destinado de manera segura. Los evaluadores de bots funcionan como una segunda etapa de autorización de los bots antes de que se puedan ejecutar con los datos y aplicaciones de producción.

Una vez que el bot se evaluó y que pasó por una revisión de seguridad, BotPromoter trabaja con el autor de bots o el evaluador de bots para designar la versión del bot que se debería usar en la producción. Esta es la única versión del bot que estará visible para el operador de bots, que es el que coordina junto con las unidades de negocio para organizar y poner los bots en funcionamiento. El operador de bots también es responsable de monitorear el desempeño de los bots dentro de Control Room, que incluye solucionar cualquier problema relativo al tiempo de ejecución que pueda ocurrir. Por último, la responsabilidad sobre la administración de la plataforma en general, como por ejemplo la configuración de los componentes, interfaces y todos los permisos o roles, recae en el administrador de RPA.

Separación avanzada de tareas

Este conjunto principal de roles demuestra un punto de partida básico para el Control de acceso basado en roles (RBAC), pero una separación de tareas aun mayor es posible dentro de la plataforma Automation Anywhere Enterprise. Mediante el uso del asistente para la creación de roles, los administradores pueden, de manera fácil, definir los roles personalizados y configurar los privilegios o permisos que justifican el paquete completo de los objetos y funciones de Control Room, que incluye administración de usuarios, licencias, Credential Vault, conjuntos de instancias de Bot Runner, programaciones de bots, operaciones o paneles de bots y registros de auditoría. A medida que se selecciona cada privilegio, el asistente agregará pasos de manera dinámica para los privilegios contingentes o derivados.

Por ejemplo, cuando se seleccionan los privilegios BOTS (BOTS) > View my bots (Ver mis bots) > Run My bots (Ejecutar mis bots), (ver Figura 5), el flujo de trabajo agregará un paso para indicar las carpetas de bots específicas (es decir, conjuntos de bots) para las cuales se ha permitido el acceso. El resultado neto es la capacidad de establecer roles de alta confiabilidad con controles de acceso lo suficientemente detallados para cumplir con las necesidades de los entornos más rigurosos, seguros y regulados en cuanto a cumplimiento.

Rol	Descripción
Administrador de RPA	Administrador del sistema (configura los componentes, roles, interfaces).
Diseñador de bots	Experto en procesos empresariales que diseña los bots con el editor de tareas y lleva a cabo pruebas funcionales básicas.
Evaluador de bots	Encargado de pruebas de control de calidad que revisa los bots en cuanto a la precisión operativa, desempeño y seguridad.
BotPromoter	Administrador que aprueba y mueve a los bots entre las etapas de desarrollo, pruebas y producción.
Operador de RPA	Operador que programa, ejecuta y monitorea el desempeño de los bots.

Tabla 1: Roles principales de la RPA en Automation Anywhere Enterprise

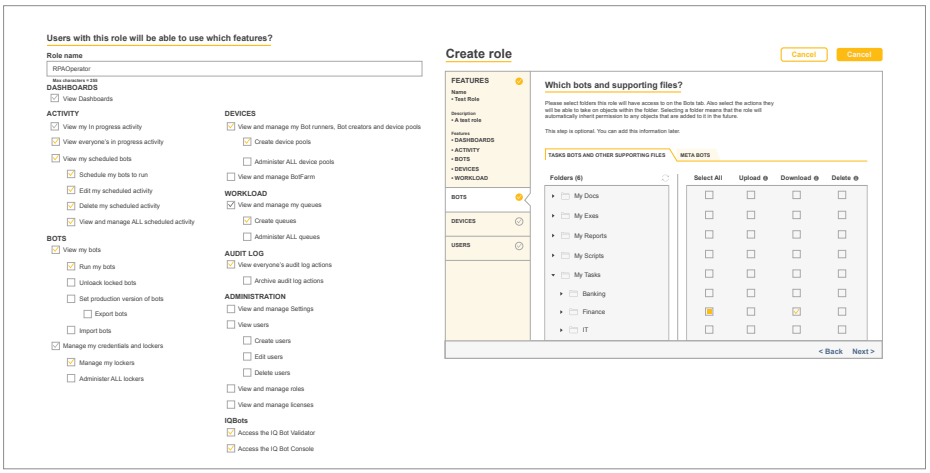


Figura 5: Creación de roles con autorización específica

Planos de control independientes

Más allá de las amplias capacidades de los RBAC, Automation Anywhere Enterprise ofrece intrínsecamente una separación lógica de tareas al emplear una arquitectura que separa de manera minuciosa las operaciones de desarrollo y ejecución de bots.

Bot Creators solo pueden subir o descargar bots desde y hacia el sistema de control de versiones dentro de Control Room. Al mismo tiempo, Bot Runners se limitan a la ejecución de los bots ya que no tienen acceso a las funciones de creación ni de pruebas. Esta separación de tareas ejecutada arquitectónicamente constituye una autorización doble acorde con las mejores prácticas del Instituto Nacional de Estándares, puesto que requiere (como mínimo) un desarrollador y un usuario empresarial para habilitar en última instancia la automatización de los procesos de negocio.

Dominios de procesamiento independientes

La creación de dominios de procesamiento independientes es un caso de uso importante para las capacidades de los RBAC de la plataforma, en especial para las empresas grandes (ver Figura 6). En este contexto, el “dominio de procesamiento” es una colección de automatizaciones (bots), bot runners y usuarios. Esto se puede lograr mediante la estricta organización o almacenamiento de los bots para cada dominio en la carpeta correspondientes dentro de Control Room.

Buen ejemplo: aquellos bots asociados a aplicaciones de finanzas se deberán colocar en la carpeta de finanzas mientras que los asociados a RR. HH se deberán asignar a la carpeta de RR. HH. A los operadores de bots del departamento de Finanzas se les asignarán privilegios únicamente para los bots y Bot Runners de finanzas. De la misma manera, los operadores de bots de RR. HH. recibirán privilegios solo para bots y Bot Runners de RR. HH. y lo mismo sucederá para los otros dominios de procesamiento o automatización (ver **Figura 6**).

Como resultado final, se produce una separación de tareas adicional y el aislamiento de aplicaciones y datos asociados, en este caso en el nivel de dominio de procesamiento, ya que los operadores individuales no pueden ver ni operar los bots que se encuentran fuera de sus dominios establecidos.

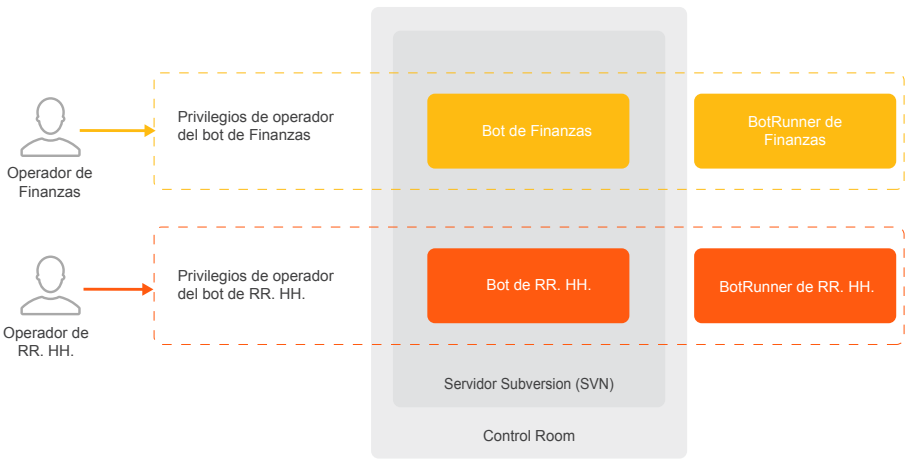


Figura 6: Asistencia técnica para dominios de procesamiento independientes

PROTECCIÓN INTEGRAL DE DATOS

La autenticación multicapa y el control de acceso específico son esenciales para conseguir un entorno estrictamente controlado. Por lo tanto, igual de importante es la protección de datos integral, ya que es necesaria para mantener la privacidad y la integridad de los procesos empresariales cruciales, de los datos confidenciales y de los secretos asociados (por ej., las credenciales).

La plataforma de Automation Anywhere Enterprise aborda esta necesidad con Credential Vault integrada y proporciona un conjunto amplio de medidas de protección que no solo protegen los datos en reposo o en tránsito sino también cuando los datos están en uso en sistemas individuales.

Claves de cifrado y Credential Vault

La **Figura 7** muestra las claves de cifrado principales que usa la plataforma, junto con su relación con Credential Vault. Todo el cifrado se realiza por medio de módulos criptográficos Nivel 1 validados por los Estándares Federales de Procesamiento de la Información (FIPS 140-2).

Durante la instalación (parte izquierda de la **Figura 7**), el sistema genera un par de claves RSA de 2048 bits públicas o privadas y una clave AES de 256 bits. A la clave privada del par RSA 2048 se la denomina clave principal y a la clave AES 256 se la denomina clave de datos. Al administrador de instalación se le entrega la clave principal para que la resguarde en un lugar físicamente seguro fuera del sistema. La clave pública se usa para cifrar la clave de datos. Luego, la clave pública y la clave de datos cifrada se almacenan en la base de datos.

Durante el arranque o reinicio de Control Room (parte derecha de la **Figura 7**), se le solicita al administrador que ingrese Master Key. La clave de datos cifrada se recupera desde la base de datos y se descifra con Master Key. De esta manera, la clave de datos queda lista para usar. A medida que el sistema almacena y recupera datos desde Credential Vault, se usa la clave de datos para cifrar y descifrar esa información.

Credential Vault se usa para almacenar todas las credenciales gestionadas del sistema y los datos de configuración del sistema fundamentales. También se puede usar para guardar cualquier otro tipo de datos confidenciales (p. ej. pares nombre-valor) que se utilizan en las automatizaciones de las empresas. Como resultado, los autores de bots pueden evitar la práctica insegura de codificar de forma rígida las credenciales y otros datos o argumentos confidenciales directamente dentro de las automatizaciones. Los datos de Credential Vault están organizados por casilleros. Los casilleros permiten la asignación de datos de credenciales cifrados por usuario, protegidos por privilegios y roles como parte de las características de los RBAC de Automation Anywhere. Cada casillero se puede asignar a un usuario o rol individual para restringir el acceso al casillero solo a usuarios específicos de RPA.

Protección de los datos en reposo

Además de cifrar las credenciales locales y los datos seleccionados en tiempo de ejecución que utilizan los bots, Credential Vault ofrece un almacenamiento seguro para los parámetros de configuración confidencial, y para los detalles pertenecientes al control de versiones integral y a los servicios de correo electrónico.

Protección de los datos en tránsito

Todos los servicios de red de los clientes y de Control Room utilizan Seguridad de la capa de transporte 1.2 (TLS, por sus siglas en inglés) para garantizar la seguridad e integridad de los datos durante el traslado entre los componentes.

Las credenciales que se utilizan para la autenticación de Bot Creator y Bot Runner a la Control Room se cifran antes de someterse a una conexión asegurada por TLS. Esta capa extra de cifrado no solo ofrece protección contra problemas de pila de red (como, por ejemplo, Heartbleed), sino que también previene la exposición de las credenciales para las implementaciones donde la capa externa de la conexión TLS finaliza en un equilibrador de carga front-end.

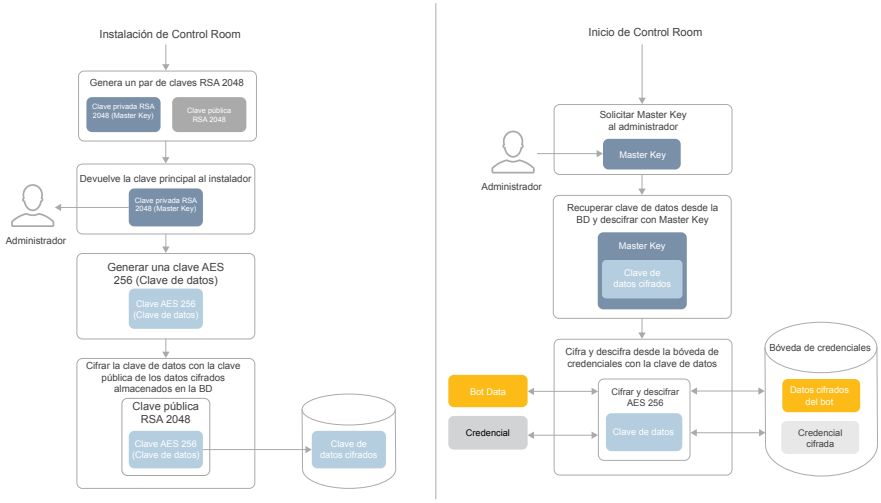


Figura 7: Arquitectura de cifrado de Automation Anywhere Enterprise

Protección de los datos en uso

La seguridad del tiempo de ejecución comienza con una protección de credenciales distribuida. Específicamente, no hay un almacenamiento local de credenciales en Bot Runners. Las credenciales y otros datos que se recuperan de manera dinámica desde Credential Vault para el uso dentro de las automatizaciones solamente se conservan en un formato cifrado en una memoria volátil y se borran una vez que el bot asociado haya finalizado con su ejecución.

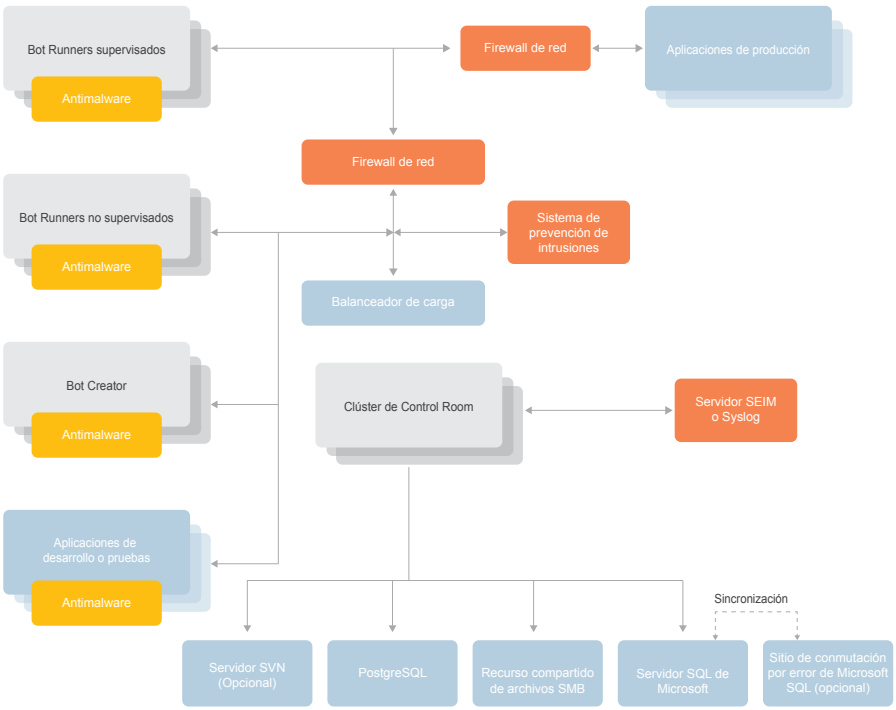
Otras funciones y opciones de configuración que se pueden utilizar para prevenir el acceso no autorizado a la información confidencial (es decir, filtración de datos) o la falsificación de bots durante el tiempo de ejecución son las siguientes:

+ Modo de sigilo: no se muestran las ventanas de los programas en la pantalla local y los usuarios conectados tienen la opción de deshabilitar la captura de imagen en Bot Creators y Bot Runners para prevenir, de esta manera, que la información confidencial que aparece en la pantalla se almacene en los bots.
+ Bloqueo de entrada: función para deshabilitar el mouse y el teclado de la máquina en la que se está ejecutando una automatización.
+ Límite de tiempo: función para configurar un límite de tiempo luego de que la automatización finalice, si es que no ha terminado con la ejecución.
+ Control central: función para controlar de manera centralizada (p. ej. pausar, reanudar, detener) la operación de las automatizaciones que se están ejecutando de manera remota desde adentro de Control Room.

ASEGURAR LA IMPLEMENTACIÓN DE LA RPA

La arquitectura de AAE consta de un escritorio estándar e infraestructura de servidor para las instancias de clientes y ControlRoom. En esta sección se describen las mejores prácticas de seguridad de RPA en relación con controles de seguridad externos que existen en cualquier empresa. Los firewalls basados en la red, los sistemas de detección de intrusiones, el antimalware y los servidores de registro externos son controles de seguridad estándar tan pertinentes para la implementación de RPA como para el resto de la infraestructura de su entorno. El siguiente diagrama muestra de manera lógica dónde se implementan estos componentes en la implementación de RPA.

Todos los controles de seguridad externos se describen en detalle en las siguientes secciones, en cuanto a su ubicación y configuración. Se puede acceder a los servicios de red de asistencia técnica, como Active Directory, SVN Server, PostgreSQL, SMB File Share, Microsoft SQL y aplicaciones de producción por medio de firewalls de red o directamente, según su ubicación en relación con los componentes de RPA.



Control de acceso basado en la red: proteger la RPA con firewalls

Los firewalls basados en la red y el firewall basado en el servidor local se utilizan para proteger Control Room o todos los nodos de un clúster de Control Room cuando se utiliza una implementación en clúster. De forma predeterminada, solo se deben permitir los protocolos necesarios en Control Room desde la red corporativa. Además, todos los protocolos de clúster se deben permitir únicamente entre los nodos del clúster de Control Room. Los firewalls basados en la red se utilizan para aislar los entornos de desarrollo, pruebas y producción de RPA entre sí y de la red corporativa (consulte la sección Ciclo de vida útil de desarrollo seguro de software).

Para los entornos de automatización no supervisados, las instancias de bot runners se ubican en una red aislada específica y están protegidos por un firewall basado en la red. Las automatizaciones supervisadas se ejecutan desde estaciones de trabajo corporativas con bot runner client instalado y están protegidas por medio de los firewalls corporativos perimetrales o firewalls internos que protegen la infraestructura de escritorio corporativa, como cualquier escritorio.

Consulte las tablas que aparecen a continuación para conocer los protocolos que utilizan Control Room y 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

Antimalware: proteger la RPA contra virus y malware

El cliente de AA se ejecuta en la infraestructura de escritorio y se debe considerar como un escritorio corporativo en todos los aspectos. El software antimalware o antivirus se utiliza para proteger el entorno del cliente contra el software dañino en forma de virus y malware.

Sistemas de detección de intrusiones: proteger la RPA contra ataques directos

Los sistemas de detección y prevención de intrusiones (IPS) protegen la red corporativa mediante la detección de ataques basados en la red mediante el análisis del tráfico de red. Al igual que cualquier otra sección esencial del centro de datos, la plataforma de RPA se protege en el punto de salida, detrás del firewall basado en la red, con un sistema IPS. La colocación del sistema IPS en su red se debe considerar según la convención corporativa y se debe aplicar por igual a la plataforma de RPA.

Gestión de incidentes de seguridad: proteger la RPA con auditoría externa

Los registros de Control Room se pueden reenviar al SIEM para almacenamiento, procesamiento y alertas externos. La integración con el SIEM o cualquier sistema de consolidación y reducción de auditoría basado en Syslog mejora en gran medida la seguridad y el cumplimiento de los controles de gobernanza. Configure Control Room para reenviar los registros de auditoría al servidor de recopilación de Syslog correspondiente en el entorno.

VALIDACIÓN EXTERNA DE LOS CONTROLES DE SEGURIDAD

Las agencias federales deben cumplir con los requisitos de seguridad de la Ley FISMA para implementar AAE en un sistema de IT local.

AAE admite características de seguridad que integran AAE con un entorno ya existente que cumple con la Ley FISMA y esos controles de asistencia como la autenticación centralizada (p. ej., Active Directory [AD], capacidades centralizadas de gestión de registros, análisis y generación de informes a través de un SIEM, y la partición de red y el control de acceso a la red a través de redes de área local virtual [VLAN] y firewalls) están implementados y pueden integrarse con AAE cuando corresponda. .

AAE admite la implementación de controles de seguridad aplicables, lo que permite a los profesionales de IT actualizar el SSP de un sistema de IT para abordar la implementación y el uso seguros de AAE. Para obtener más detalles sobre los controles de la Ley FISMA, consulte las características y capacidades principales de AAE, donde se compararon con los controles seleccionados moderados de la Ley FISMA de NIST SP 800-53 rev. 4 y se analizaron para comprobar si afectan o respaldan los requisitos de control. El marco de trabajo de NIST se puede asignar a otros marcos de trabajo como la Ley de Portabilidad y Responsabilidad de Seguros de Salud (HIPAA) y la Industria de Tarjeta de Pago (PCI). Consulte el informe de Automation Anywhere Enterprise: Through The Lense of FISMA (A través del lente de la Ley FISMA) para obtener más detalles sobre los controles de la Ley FISMA que se implementan en Automation Anywhere Enterprise.

ASISTENCIA TÉCNICA PARA EL CICLO DE VIDA ÚTIL DE DESARROLLO DE SOFTWARE SEGURO (SDLC)

Para maximizar los controles y las medidas de protección que se encuentran en el entorno de automatización, se puede “ampliar” el escenario básico de implementación que se describió anteriormente para cumplir aún más con las mejores prácticas del SDLC, tales como las requeridas por la Ley de Administración de Seguridad de Información Federal (FISMA), el Programa Federal de Administración de Riesgos y Autorizaciones (FedRamp) y el Estándar de Seguridad de Datos de la Industria de Pagos con Tarjeta (PCI DSS). El modelo de implementación avanzado resultante ofrece tres zonas de RPA distintas: desarrollo, pruebas de aceptación de usuario (UAT) y producción (ver Figura 8). Cada zona está separada de manera lógica (aislada) con diferentes grupos de usuarios que tienen asignados distintos roles y privilegios. Las líneas discontinuas verticales representan la segmentación de las redes y los firewalls.

Al igual que en el modelo de implementación básica, el ciclo de vida útil de los bots comienza en la etapa de desarrollo. Una vez que los autores de bots están conformes con los bots, BotPromoters de UAT transfieren los bots desde el depósito de la versión de desarrollo (SVN) hacia el depósito de UAT. La finalidad exclusiva de la zona de UAT es evaluar los bots para garantizar precisión, buen desempeño y seguridad. Luego de que los bots pasan las pruebas de aceptación, un BotPromoter de producción los transfiere a la zona de producción. En este punto, alcanzan el estado de producción y quedan disponibles para que los operadores de RPA los utilicen con aplicaciones de producción. En cada etapa del proceso, diferentes administradores, con distintos roles y privilegios, llevan a cabo revisiones y certificaciones. La estricta separación de tareas y los controles multicapa están integrados en el diseño para garantizar que la fuerza de trabajo digital sea confiable, escalable, segura y conforme.

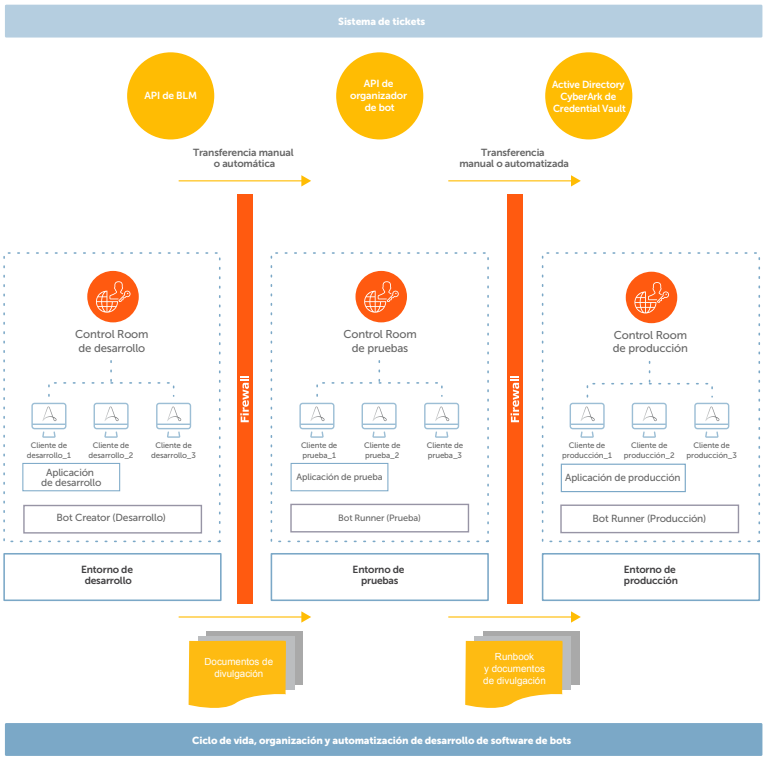


Figura 8: Modelo de implementación avanzado para el SDLC total

INICIO DE SESIÓN Y SUPERVISIÓN

Las capacidades exhaustivas de registro de auditoría, supervisión y presentación de informes son componentes esenciales de la arquitectura de seguridad para cualquier solución destacada de IT. Automation Anywhere Enterprise no es la excepción.

A lo largo de la plataforma, los detalles de los eventos (quién, qué, cuándo, dónde y resultado) se capturan de manera automática para más de 60 tipos de acciones de usuarios o entidades, incluidas la creación, modificación, habilitación, inhabilitación y eliminación de usuarios, bots, Bot Creators y Bot Runners. El no repudio se logra mediante la combinación de captura automática, la vinculación de cada actividad a una identidad específica y una política predeterminada de solo lectura. El RBAC también se puede utilizar para controlar de manera estricta qué roles tienen visibilidad para los registros de auditoría en primer lugar.

Desde una perspectiva de control, los paneles e informes automatizados se encuentran accesibles dentro de Control Room y se pueden personalizar para identificar y alertar actividades anormales (o cualquier otro detalle que los equipos de automatización o seguridad consideren importante). Además, la capacidad de exportar registros admite el uso de otros análisis, informes e infraestructura de investigación o respuesta de incidentes ya existentes y en uso por las empresas, como SIEM, análisis de comportamiento de entidades y usuarios (UEBA) y herramientas de análisis avanzadas.

SEGURIDAD EMPRESARIAL ADICIONAL Y CAPACIDADES DE FORTALECIMIENTO

Automation Anywhere Enterprise también respalda la seguridad empresarial y los objetivos de fortalecimiento mediante lo siguiente:

+ Una arquitectura distribuida (y flexible) de componentes que es capaz de “adaptarse” sin problemas a la infraestructura y a los procesos de alta disponibilidad o recuperación ante desastres (AD/RD) existentes de la empresa.
+ Un sistema de control de versiones integral (Apache Subversion) que, junto con las amplias funciones de RBAC de la plataforma, es capaz de implementar y hacer cumplir una política de gestión del cambio y procesos sumamente rigurosos.
+ Herramientas tales como los marcos Hibernate y ReactJS durante el desarrollo del código de plataforma para ayudar a eliminar la vulnerabilidad a los ataques comunes (como por ejemplo, inyección de código SQL y secuencias de comandos en sitios cruzados).
+ Un plan o protocolo de seguridad para el desarrollo de códigos que requiere un escaneo constante de múltiples herramientas y capas para detectar y eliminar las vulnerabilidades del software.

Puede encontrar más detalles sobre estos y muchos otros controles, medidas de protección y capacidades de seguridad que son parte de Automation Anywhere Enterprise aquí: https://www.automationanywhere.com/images/Enterprise-Architecture.pdf

AUTOMATIZACIÓN DE API

A medida que la implementación de bots crece exponencialmente, se abren nuevos desafíos en torno a la autenticación segura a escala y la administración operativa del ciclo de vida útil de los bots. Hay una necesidad de reducir el tiempo de implementación y eliminar el error humano. Automation Anywhere proporciona API para la integración con la automatización de terceros para la autenticación segura y la organización de la administración del ciclo de vida útil de los bots. En esta sección se describen las API que proporcionan las capacidades mencionadas anteriormente.

Credential Vault: API

Credential Vault de Automation Anywhere se utiliza para el almacenamiento cifrado de credenciales que utiliza una automatización (bot) para una autenticación segura. Las API de Credential Vault se pueden utilizar para la sincronización de credenciales con sistemas externos de Administración de identidad y acceso (IAM) a través de un programa organizador, escenarios de cristal de rotura donde al bot se le asigna una contraseña en determinadas circunstancias que cambia después de cada uso, gestión externa de credenciales a través de un programa organizador externo.

API de implementación de bots

La API de implementación de bots permite que las aplicaciones externas inicien un flujo de trabajo de automatización en Bot Runner. Mientras que cualquier bot se puede iniciar a través de la API, en un contexto de seguridad, los bots que realizan funciones relacionadas con la seguridad se pueden organizar a través de una aplicación externa. Por ejemplo, un SIEM puede activar una alerta que inicia un bot para realizar la recopilación de datos desde el sistema indicado en la alerta. Se puede recopilar cualquier tipo de datos, como el volcado de tablas de proceso en ejecución, instantáneas de sumas de comprobación de archivos, la utilización de recursos y los usuarios que han iniciado sesión actualmente.

API de administración del ciclo de vida útil de los bots

La API de la administración del ciclo de vida útil de los bots (BLM) permite que una aplicación de organización externa automatice el proceso de mover bots de una Control Room a otra. Esto es importante en las empresas que utilizan el SDLC. Consulte la sección sobre el SDLC para obtener más información. El proceso de SDLC se puede automatizar al integrar sistemas de tickets como Jira o Zendesk para activar el desarrollo, las pruebas, la revisión de seguridad y la promoción a la producción de bots. Un proceso de SDLC automatizado proporciona un libro de ejecución para la creación de bots, lo que brinda una mayor seguridad de que cada bot en producción realiza la tarea para la cual fue diseñado en un proceso auditable que proporciona todos los controles de gobernanza que su organización necesita.

CONCLUSIÓN

La automatización robótica de procesos resulta muy prometedora para las empresas modernas que buscan reducir los costos operativos, mejorar la satisfacción del cliente y lograr una ventaja sobre los competidores. Como plataforma de fuerza de trabajo digital líder del mercado, Automation Anywhere Enterprise ayuda a garantizar el logro máximo de estos y otros beneficios al ofrecer no solo la confiabilidad, escalabilidad y utilidad necesarias para tener éxito, sino también la seguridad de nivel empresarial que se requiere para preservar la confidencialidad, integridad y disponibilidad de todo el entorno de automatización.

Para obtener más información sobre Automation Anywhere Enterprise, visite: https://www.automationanywhere.com/products/enterprise.