"Privacidad primero" en los datos del cliente con la nube de Automation Anywhere

La cartera de funciones en la nube de Automation Anywhere® es una plataforma hospedada de prestación de servicios. La cartera de funciones en la nube incluye capacidades para la creación de bots, Control Room integrada y la posibilidad de ejecutar nodos de Bot Runner conectados a la nube en la infraestructura del cliente. Los productos adicionales como IQ Bot™ también pueden hospedarse en la nube.

La oferta de la nube está diseñada para garantizar la privacidad de los datos y funciona según el Reglamento general de protección de datos (RGPD) y otros principios y lineamientos de privacidad de datos.

SEGURIDAD DE DATOS

La arquitectura de implementación adopta el enfoque "privacidad primero" para la protección de los datos y la infraestructura del cliente.

La conectividad de los datos entre Bot Runner de la red del cliente y Control Room de la nube se encuentra cifrada. Los protocolos de seguridad de cifrado como HTTPS y TLS 1.2 se utilizan para cifrar los datos en tránsito. Para los datos almacenados en la nube, se utiliza el cifrado de datos en reposo (por ejemplo, cifrado AES de 256 bits).

La estrategia de seguridad completa (como las operaciones en la nube desde donde se implementa la oferta de la nube, las tecnologías de cifrado y la seguridad de red del entorno) se describe en la Guía de operaciones de seguridad en la nube, disponible aquí <insert URL>

RECOLECCIÓN DE DATOS

El modelo de implementación requiere que los clientes creen sus propios bots y administren la implementación de bots desde Control Room de la nube. Una vez creados los bots, se prueban e implementan para su ejecución en la infraestructura de procesamiento de los usuarios.

En la tabla siguiente se describen los datos recopilados para la cartera de funciones en la nube de Automation Anywhere. La tabla brinda orientación sobre qué datos podrían utilizarse para identificar a una persona física.

Elemento de datos	Categoría de datos	Descripción
Nombre de usuario	Personal	Correo electrónico, nombre y apellido, nombre preferido, zona horaria, último inicio de sesión, contraseña, conjunto de preguntas, dominio de AD
Contraseña de usuario	Personal	
Clave de seguridad	Personal	Clave de seguridad de Credential Vault
Acceso al dispositivo Bot Runner	Personal	Nombre de usuario del dispositivo y credenciales de acceso
Definición de roles	Personal	Administrador, creador, etc.
Roles asignados a usuarios, dispositivos, recursos	Personal	Roles del usuario
IP del dispositivo bot/FQDN	Personal	Seguimiento de la dirección IP del dispositivo o el FQDN de un usuario
Definición de bot (depósito)	Metadatos	Datos almacenados como parte de la definición de bot
Credenciales de la aplicación de bot	Personal	Usuario de la aplicación, URL, clave pública, nombre de enrutamiento
Programación de bots en Control Room	Metadatos	Administración de bots; cuándo y dónde ejecutar bots
Definición de flujo de trabajo de la WLM	Metadatos	Cuándo y dónde ejecutar bots en cada secuencia
Registros de auditoría	Personal	Puede contener identificadores: registro de mensajes del dispositivo, registro de mensajes de implementación, registro de mensajes de correo electrónico, registro de ejecución de trabajo: (hora de inicio/finalización, ID de usuario, programación, nombre de automatización, ID de implementación, nombre del dispositivo, nombre del bot, nombre del usuario), registro de edición de administración del usuario, registro de mensajes de Credential Vault, registros de cambio de base de datos y servidor
Registros de errores	Personal	Puede contener identificadores
Análisis operativo	Metadatos	Estado del servicio
Datos de uso	Metadatos	Uso de características, licencias habilitadas, agregadas sin identificadores de datos personales ni de usuario. Para IQ Bot: instancias de aprendizaje de usuarios, dominios, estadísticas operativas, cambios de validación, documentos cargados y resultados de extracción.
Datos de uso	Personal/ Metadatos	Instancias de aprendizaje de usuarios, dominios, estadísticas operativas, cambios de validación, documentos cargados de usuarios y resultados de extracción.

USO DE DATOS

Operaciones y asistencia técnica

Las operaciones en la nube supervisarán los sistemas de implementación y el rendimiento operativo para operar, escalar y brindar asistencia técnica al servicio según los acuerdos de nivel de servicio (SLA) <link here>. Automation Anywhere generalmente no puede visualizar los datos del cliente enumerados anteriormente.

Cuando el servicio de asistencia técnica necesite el acceso para resolver problemas, el personal de asistencia podrá acceder únicamente con el correspondiente permiso del cliente.

Con el fin de mejorar el producto, Automation Anywhere realizará lo siguiente:

- Analizar los datos de uso de funciones para mejorar el producto, por ejemplo, agregar telemetría para proporcionar visibilidad operativa en el uso de las funciones. Esto ayudará a que Automation Anywhere priorice y agregue mejoras en el producto. Estos son algunos ejemplos específicos:
  - Revisar la frecuencia de uso de los comandos de Excel para ayudar a priorizar qué comandos agregar a futuras versiones.
  - Brindar recomendaciones de mejores prácticas operativas.
  - Proporcionar servicios de asistencia técnica que se utilicen para actualizar, proteger y solucionar problemas.
  - Personalizar productos y hacer recomendaciones.
  - Para IQ Bot, los datos del cliente se utilizarán para mejorar la calidad de las habilidades de aprendizaje de AI.

Para obtener más información acerca de la política de privacidad de datos de Automation Anywhere, consulte: https://www.automationanywhere.com/in/privacy

Retención de datos luego de finalizar la suscripción

Automation Anywhere conservará los datos del cliente, las configuraciones (bots), los datos de IQ Bot y la mayoría de los registros durante un plazo de 30 días luego de que finalice la suscripción del cliente. Algunos registros se pueden conservar hasta un plazo de 180 días luego de que finalice la suscripción del cliente.

Los detalles completos del Anexo de procesamiento de datos y la política de retención de datos se pueden encontrar aquí: https://www.automationanywhere.com/support/DPA.pdf

PROTECCIÓN DE DATOS

Automation Anywhere cuenta con un conjunto integral de características de seguridad que se proporcionan automáticamente o que son configurables por diseño para brindar protección de datos. Al igual que con cualquier aplicación empresarial, la utilización coherente y adecuada de los controles de seguridad depende de que la organización utilice la aplicación empresarial. La autorización de los usuarios depende de los administradores de IT, que deben implementar controles para garantizar que solo el personal autorizado tenga acceso.

El propietario de los datos debe asegurarse de que solo el personal autorizado con una necesidad empresarial pueda acceder al servicio. A los usuarios corporativos con acceso se les pueden otorgar permisos detallados a través de controles de acceso basados en roles (RBAC). Los modelos de RBAC aseguran controles duales y división de tareas dentro de las operaciones. Los permisos se pueden implementar para todos los aspectos de la operación del producto, que incluyen credenciales, bots, Bot Runners, Bot Creators, programaciones de bots, instancias de aprendizaje de IQ Bot, acceso al registro de auditoría, listas de prioridad para la administración de cargas de trabajo y grupos.

Automation Anywhere brinda funciones de auditoría completa donde todas las acciones del usuario se auditan dentro de la plataforma y, de este modo, se brindan registros de todos los accesos y acciones realizadas por el personal de operaciones. La auditoría se automatiza para que todos los roles con y sin privilegios se ajusten a las mejores prácticas definidas en NIST AC-6.

Como los bots son programas de software desarrollados por expertos empresariales de clientes, los procesos seguros de ciclo de vida de desarrollo de software (SDLC) de última generación que se requieren deben ser implementados por el cliente según el caso. Con este fin, Automation Anywhere admite la división de entornos de desarrollo, pruebas y producción mediante una combinación de implementaciones independientes y de RBAC, según lo descrito anteriormente.

Seudonimización

El RGPD define específicamente a la seudonimización como una medida técnica adecuada para proteger los datos. La seudonimización transforma los datos en identificadores artificiales. Esto le da al controlador y al procesador una forma de procesar los datos de manera que ya no es posible usar los datos para identificar a una persona física sin la información adicional que se guarda por separado. La tokenización es otro enfoque que transforma los datos para que se pueda hacer referencia a ellos más adelante, pero en términos de datos tokenizados, de tal manera que no se pueden usar para identificar a una persona física.

Automation Anywhere recomienda el uso de la seudonimización de datos para entornos de desarrollo y pruebas. Para IQ Bot, los documentos e imágenes en el entorno de producción se procesarán con información real del usuario. No hay ninguna posibilidad técnica de seudonimizar estos documentos automáticamente y utilizar IQ Bot.

Conservación de datos en Control Room

Hay casos en que los datos se conservan en las bases de datos que asisten técnicamente a Control Room, en especial cuando se usa la administración de cargas de trabajo, IQ Bot y Bot Insight™ (futura versión). En todos los casos de conservación de datos en Control Room, la seudonimización y la tokenización reducen el esfuerzo del controlador y el procesador para cumplir con el RGPD. Además, cuando se habilitan los registros para la información de depuración, como el nombre de usuario (usuarios de la plataforma), estos se retendrán en los registros.

Administración de la carga de trabajo y listas de prioridad

Al utilizar la administración de la carga de trabajo (futura versión) para implementar múltiples bots en la misma automatización, los elementos de trabajo que se colocan en las listas de prioridad se almacenan en la base de datos de Control Room. A través de la interfaz de usuario de Control Room, cualquier elemento de trabajo puede consultarse, revisarse y eliminarse. Al procesar datos personales en elementos de trabajo, las listas de prioridad pueden eliminarse periódicamente.

Cualquier administrador con los privilegios apropiados (establecidos por el rol correspondiente) pueden agregar y eliminar las credenciales del usuario. Control Room brinda asistencia técnica en la consulta, revisión y eliminación de cualquier credencial en cualquier momento.

Control Room proporciona los medios para configurar y eliminar cuentas de usuario con RBAC adecuados. El administrador de la organización es responsable de proporcionar acceso adecuado a los usuarios y recursos. El administrador debe crear una política con el nivel de acceso necesario según los lineamientos de privacidad de datos corporativos y de usuario. Si un usuario individual solicita acceso o limitaciones a su información personal, debe ponerse en contacto con el administrador del cliente. Los administradores del cliente pueden eliminar las cuentas del usuario en Control Room.

Para obtener más detalles sobre las consultas de privacidad de RGPD y las copias de los datos personales, Automation Anywhere proporciona el siguiente sitio: Formulario de solicitud de derechos de acceso a los sujetos de los datos.

RESUMEN

Las ofertas actuales basadas en la nube y esenciales para la empresa se encargan de ofrecer soluciones con seguridad de acceso y privacidad de datos como consideraciones primordiales desde un principio.

La cartera de funciones en la nube de Automation Anywhere está diseñada para cumplir y superar los exigentes lineamientos operativos por una buena razón: nos preocupamos profundamente por la privacidad y seguridad del cliente en la prestación de servicios de automatización.

Para obtener más información sobre las innovadoras soluciones en la nube de Automation Anywhere, visite la página de la nube.