Automation Anywhere 클라우드
고객 데이터의 개인정보 보호가 최우선

Automation Anywhere® 클라우드 포트폴리오는 호스팅된 서비스 제공 플랫폼입니다. 클라우드 포트폴리오에는 클라우드에서 호스팅된 통합 Control Room과 봇 생성 기능이 있으며, 고객의 인프라에서 클라우드에 연결된 Bot Runner 노드를 실행할 수 있는 기능도 포함되어 있습니다. IQ Bot™과 같은 추가 제품도 클라우드에서 호스팅할 수 있습니다.

클라우드 솔루션은 데이터 프라이버시를 보장하도록 설계되었으며 GDPR과 기타 데이터 프라이버시 원칙 및 지침에 따라 운영됩니다.

데이터 보안

배포 아키텍처는 고객의 데이터와 인프라를 보호하기 위해 "개인정보 보호 최우선" 접근 방식을 채택하고 있습니다.

고객 네트워크 상의 Bot Runner와 클라우드에 위치한 Control Room 사이의 데이터 연결은 암호화되어 처리됩니다. 전송 중인 데이터를 암호화하는 데는 HTTPS 및 TLS 1.2와 같은 보안 암호화 프로토콜이 사용됩니다. 클라우드에 저장된 데이터의 경우, 유휴 시 데이터 암호화(예: AES 256비트 암호화)가 사용됩니다.

클라우드 솔루션이 배포되는 클라우드 운영 환경을 다루는 전체 보안 정책, 암호화 기술 및 운영 환경의 네트워크 보안에 대한 내용은 클라우드 보안 운영 가이드(<URL 삽입>)에 설명되어 있습니다.

데이터 수집

배포 모델에는 고객이 클라우드 상의 Control Room에서 봇을 구축하고 봇 배포를 관리하는 작업이 포함되어 있습니다. 봇이 구축되면 사용자의 자체 컴퓨팅 인프라에서 실행할 목적으로 테스트를 수행한 후 배포하게 됩니다.

아래 표는 Automation Anywhere 클라우드 포트폴리오에서 수집하는 데이터를 보여줍니다. 이 표는 사람을 식별하는 데 사용할 수 있는 데이터에 관한 지침을 제공합니다.

데이터 항목	데이터 범주	설명
사용자 이름	개인	이메일, 성명, 선호 이름, 표준 시간대, 마지막 로그인, 비밀번호, 질문 세트, AD 도메인
사용자 비밀번호	개인	
비밀번호 보안 키	개인	자격증명 보관 비밀번호 보안 키
Bot Runner 장치 액세스	개인	장치 사용자 이름 및 액세스 자격증명
역할 정의	개인	관리자, 크리에이터 등
사용자, 장치, 리소스에 매핑된 역할	개인	사용자 역할
봇 장치 IP / FQDN	개인	장치 IP 주소 또는 FQDN를 통해 사용자를 추적할 수 있음
봇 정의(리포지터리)	메타데이터	봇 정의의 일부로 저장된 데이터
봇 애플리케이션 자격증명	개인	애플리케이션 사용자, URL, 공개 키, 라우팅 이름
Control Room 봇 일정	메타데이터	봇 관리나 봇 실행 시기 및 위치
WLM 워크플로 정의	메타데이터	봇 실행 시기, 위치 및 순서
감사 로그	개인	포함될 수 있는 식별자: 장치 메시지 로그, 배포 메시지 로그, 이메일 메시지 로그, 작업 실행 로그 (예: 시작/종료 시간, 사용자 ID, 일정, 자동화 이름, 배포 ID, 장치 이름, 봇 이름, 사용자 이름), 사용자 관리 편집 로그, 자격증명 보관 메시지 로그, 서버 및 데이터베이스 변경 로그
오류 로그	개인	식별자가 포함될 수 있음
운영 분석	메타데이터	서비스 상태
사용 데이터	메타데이터	기능 사용, 활성화된 라이선스, 개인/사용자 데이터 식별자 없이 집계됨. IQ Bot이 대상인 경우: 사용자 학습 인스턴스, 도메인, 운영 통계, 유효성 검사 변경 사항, 업로드 문서 및 추출 결과
사용 데이터	개인/ 메타데이터	사용자 학습 인스턴스, 도메인, 운영 통계, 유효성 검사 변경 사항, 사용자 업로드 문서 및 추출 결과

데이터 활용

운영 및 지원

클라우드 운영 시 서비스 SLA(<여기에 링크>)에 따른 서비스의 운영, 확장 및 지원을 수행하기 위해 배포 시스템과 운영 성능을 모니터링하게 됩니다. Automation Anywhere는 일반적으로 위에 열거된 고객 데이터를 볼 수 없습니다.

문제 해결을 위해 지원 서비스에서 액세스해야 하는 경우, 고객이 적절한 승인을 한 경우에만 지원 담당자가 액세스하게 됩니다.

제품 개선을 위해 Automation Anywhere는 다음 사항을 진행합니다.

- 기능 사용 데이터를 분석하여 제품을 개선합니다(예: 원격 측정기를 추가하여 기능 사용량에 대한 운영 가시성을 제공). 이를 통해 Automation Anywhere는 우선순위를 정하여 제품을 개선하게 됩니다. 다음은 관련된 예시입니다.
  - Excel의 명령어 사용 빈도를 검토하여 향후 릴리스에 추가할 명령어의 우선순위 결정
  - 운영 모범사례 추천 제공
  - 업데이트, 보안 및 문제 해결에 사용되는 지원 서비스 제공
  - 제품 개인화 및 추천 제공
  - IQ Bot의 경우, AI 러닝 기술의 품질 향상에 고객 데이터가 사용됨

Automation Anywhere의 데이터 프라이버시 정책에 관한 자세한 내용은 다음을 참조하십시오. https://www.automationanywhere.co.kr/privacy

구독 종료 후 데이터 보존

Automation Anywhere는 고객이 구독을 종료한 후 30일 동안 고객 데이터, 구성(봇), IQ Bot 데이터 및 대부분의 로그를 보관합니다. 일부 로그는 고객이 구독을 종료한 후 최대 180일까지 보관될 수 있습니다.

데이터 처리 부록 및 데이터 보존 정책에 관한 자세한 내용은 다음을 참조하십시오. https://www.automationanywhere.com/support/DPA.pdf

데이터 보호

Automation Anywhere는 데이터 보호를 위해 설계 단계에서 구성할 수 있거나 자동으로 제공되는 포괄적인 보안 기능 세트를 갖추고 있습니다. 다른 모든 엔터프라이즈 애플리케이션과 마찬가지로, 보안 제어를 일관되고 적절하게 활용하는 것은 해당 엔터프라이즈 애플리케이션을 사용하는 조직에 달려 있습니다. 사용자 권한 부여 업무는 IT 관리자가 수행하며, IT 관리자는 권한이 있는 사람만 액세스할 수 있도록 제어를 구현해야 합니다.

데이터 소유자는 업무상 권한이 있는 사람만 해당 서비스에 액세스할 수 있게 해야 합니다. 액세스 권한이 있는 기업 사용자에게는 역할 기반 액세스 제어(RBAC)를 통해 세분화된 사용 권한을 부여할 수 있습니다. RBAC 모델은 운영 시 이중 제어 및 업무 분장을 보장해 줍니다. 자격증명, 봇, Bot Runner, Bot Creator, 봇 일정, IQ Bot 학습 인스턴스, 감사 로그 액세스, 워크로드 관리 대기열, 풀 등을 비롯한 제품 운영의 모든 측면에 대해 권한을 구현할 수 있습니다.

Automation Anywhere는 플랫폼 내에서 모든 사용자 활동을 감사할 수 있는 완벽한 감사 기능을 통해 운영 담당자가 수행한 모든 액세스와 동작에 관한 기록을 제공합니다. 감사는 NIST AC-6에 정의된 모범사례를 준수하도록 권한 여부와 상관없이 모든 역할에 대해 수행되도록 자동화되어 있습니다.

봇은 고객 비즈니스 전문가가 개발한 소프트웨어 프로그램이므로 그에 맞춰 고객이 최신 필수 SDLC(보안 소프트웨어 개발 수명 주기) 프로세스를 구현해야 합니다. 이를 위해 Automation Anywhere는 위에서 설명한 대로 개별 배포와 RBAC를 조합하여 개발, 테스트 및 프로덕션 환경의 분리를 지원하고 있습니다.

가명화(Pseudonymization)

GDPR은 데이터 보호를 위한 적절한 기술적 방안으로서 가명화를 구체적으로 언급하고 있습니다. 가명화는 데이터를 인조 식별자(artificial identifier)로 변환합니다. 가명화를 사용하면 컨트롤러 및 프로세서가 데이터를 처리할 방안이 마련되는데, 가령 별도 보관된 추가 정보 없이 더는 해당 데이터를 자연인 식별용으로 사용할 수 없게 하는 것입니다. 토큰화는 또 다른 접근 방식으로, 이는 데이터를 변환하여 향후에 참조할 수 있지만, 토큰화된 데이터 그 자체로는 자연인 식별에 사용할 수 없게 하는 방식입니다.

Automation Anywhere는 개발 및 테스트 환경에서 데이터 가명화 사용을 추천합니다. IQ Bot의 경우, 프로덕션 환경의 문서와 이미지는 실제 사용자 정보와 함께 처리됩니다. 이러한 문서를 자동으로 가명화하면서 IQ Bot을 사용하는 것은 기술적으로 불가능합니다.

Control Room에서의 데이터 잔류

Control Room을 지원하는 데이터베이스 내에 데이터가 남아있는 경우가 있습니다. 특히 워크로드 관리, IQ Bot, Bot Insight™(향후 릴리스)를 사용할 때 이런 경우가 발생합니다. Control Room에서의 데이터 잔류와 관련된 모든 사례에서 가명화와 토큰화는 GDPR을 준수하기 위한 컨트롤러 및 프로세서 엔터티의 업무를 줄여줍니다. 또한 사용자 이름(플랫폼 사용자)과 같이 디버깅 정보용으로 로그를 활성화할 경우, 해당 정보가 로그에 남게 됩니다.

워크로드 관리 및 대기열

워크로드 관리(향후 릴리스)를 사용하여 동일한 자동화를 위해 다수의 봇을 배포하는 경우, 대기열에 배치된 작업 항목은 Control Room 데이터베이스에 저장됩니다. Control Room 사용자 인터페이스를 통해 모든 작업 항목을 조회, 검토 및 삭제할 수 있습니다. 작업 항목에서 개인 데이터를 처리할 때 대기열이 주기적으로 삭제될 수 있습니다.

적절한 권한을 가지고 적정한 역할로 설정된 관리자는 사용자 자격증명을 추가 및 삭제할 수 있습니다. Control Room은 모든 자격증명의 조회, 검토 및 삭제를 언제든지 수행할 수 있도록 지원합니다.

Control Room은 적절한 RBAC 제어를 통해 사용자 계정을 설정하고 제거할 수 있는 방안을 제공합니다. 기업 내 관리자가 사용자 및 리소스에게 적절한 액세스를 제공하는 데 대한 책임을 지게 됩니다. 관리자는 회사 및 사용자 데이터 프라이버시 지침에 따라 필요한 액세스 수준이 담긴 정책을 구성해야 합니다. 개별 사용자가 자신의 개인 정보에 대한 액세스 또는 제한을 요청할 경우 고객사의 관리자에게 문의해야 합니다. 고객사의 관리자는 Control Room에서 사용자 계정을 삭제할 수 있습니다.

GDPR 데이터 프라이버시 문의와 개인 데이터 사본에 대한 자세한 내용을 제공하기 위해 Automation Anywhere에서는 데이터 주체 액세스 권한 요청 양식 사이트를 제공하고 있습니다.

요약

오늘날 클라우드를 기반으로 하는 주요 비즈니스 서비스는 처음부터 액세스 보안 및 데이터 프라이버시 보호를 가장 중요한 사항으로 고려하며 솔루션을 제공하고 있습니다.

Automation Anywhere 클라우드 포트폴리오는 까다로운 운영 지침을 충족할 뿐만 아니라 이를 넘어설 수 있도록 설계되어 있는데, 여기에는 그럴 만한 이유가 있습니다. 고객에게 자동화를 제공하는 데 있어 고객의 개인정보 보호 및 보안에 저희가 아주 깊은 관심을 가지고 있기 때문입니다.

Automation Anywhere의 획기적인 클라우드 솔루션에 관한 자세한 내용은 클라우드 페이지를 방문해 확인하실 수 있습니다.