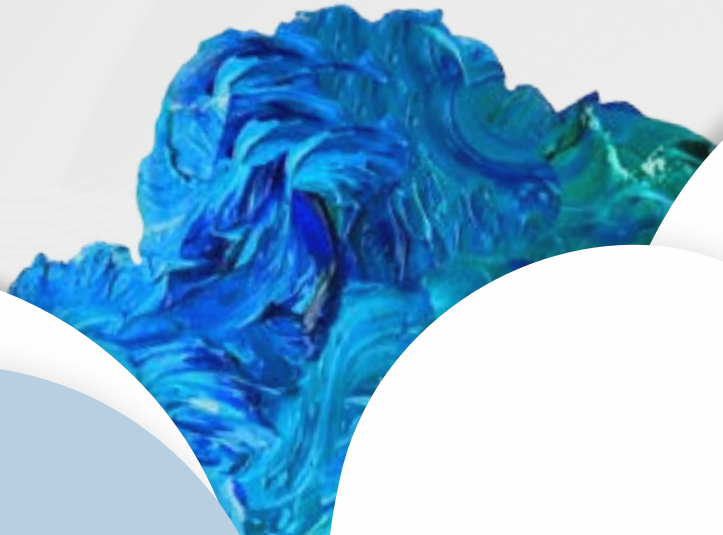
AUTOMATION ANYWHERE

Automation 360™ Cloud Security and Data Privacy



VERSION 1

Table of Contents

Introduction

The adoption of cloud is transforming the way companies of all sizes are scaling services to fulfill customer expectations. As Robotic Process Automation (RPA) in the cloud accelerates in demand and adoption, providing a platform that is secure and ensures data privacy compliance is a core business requirement, and Automation Anywhere is committed to achieving and maintaining the trust of our customers.

Automation 360™ Cloud is an end-to-end, cloud-native, intelligent automation platform provided by Automation Anywhere. The platform is offered in the three deployment models that customers can choose from Pure Cloud, Cloud-Enabled, and On-Premises.

Pure Cloud—In addition to this cloud model lowering the total cost of ownership (TCO) and enabling faster scaling, customers benefit from a SaaS experience that is secure and always up to date with the fully hosted and managed Automation 360 Cloud. Log in and automate. It is as simple as that.

Cloud-Enabled—This option is ideal for organizations looking to transition to the cloud for the first time, or those with on-premises data requirements to leverage a hybrid model. In the Cloud-Enabled deployment model, the core platform components and data reside on the customer's infrastructure, and management functions such as authentication, licensing, and bot scheduling occur in Automation 360 Cloud. Customers keep all data on-premises, utilizing the latest features while still leveraging key benefits of Automation 360 Cloud.

On-Premises—Customers get a fully hosted solution on their infrastructure with access to timely updates. Customers deploy on-premises with control over implementing updates and new AI capabilities. Although the model is on a cloud-native architecture and uses the same functionalities as other models, the setup, deployment, and implementation of updates are the customer's responsibility. Since the scope of this document covers security and data privacy for Automation 360 Cloud-hosted deployments, on-premises deployment will not be covered in depth.

Automation Anywhere provides comprehensive defense in depth with a multi-layered approach to security for Automation 360 Cloud. It is the industry's only cloud-native, web-based RPA service that is SOC 2 Type 2, SOC 1 Type 2, and ISO 27001 certified. Automation 360 Cloud is built on a robust security architecture that enables full support for core security principles such as identity and access management, least privileges, and separation of duties while delivering end-to-end protection for mission-critical apps, safeguarding sensitive data, and ensuring data privacy.

This document provides an overview of:

Automation 360 cloud secure operations and controls

Automation 360 data privacy

How security works in the Automation 360 Cloud deployment models

Automation Anywhere Security Certifications

Automation Anywhere is a security- and privacy-focused enterprise. This is reflected in the Automation 360 platform. This continued endeavor has resulted in achieving multiple security, business continuity, and data privacy-related certifications.

SOC 1 Type 2

The SOC 1 Type 2 audit is an annual certification that attests Automation Anywhere has the proper internal controls and processes regarding security and availability to ensure that customer data is kept safe.

SOC 2 Type 2

The SOC 2 Type 2 certification shows that Automation Anywhere adheres to the best security and compliance practices related to availability, confidentiality, processing integrity, security, and privacy and has sustained that for one year after achieving the SOC 2 Type 1 certification.

ISO 27001

Automation 360 Cloud service was awarded the ISO 27001 certification upon the successful completion of an independent audit that demonstrated the confidentiality, integrity, and availability standards for information assets.

ISO 22301

The ISO 22301:2019 "Security and Resilience—Business Continuity Management Systems" certification covers how well Automation Anywhere is ready to respond and recover in the case of an emergency or disaster.

Cloud Security Alliance Attestation

The Security Trust Assurance and Risk (STAR) registry founded by Cloud Security Alliance recognizes and documents the security and privacy controls put in place by organizations in the cloud computing space. Automation Anywhere is the only provider of Enterprise RPA listed in the registry. For more details, please visit the STAR Registry.

HITRUST CSF

The HITRUST Common Security Framework (CSF) is built on a set of security controls mapped to various nationally and internationally recognized security and privacy-related frameworks such as HIPAA, PCI, ISO, etc. By getting HITRUST CSF certification, Automation 360 becomes the only cloud-native RPA solution in the market to demonstrate healthcare-specific security and privacy controls to help customers deliver on their regulatory compliance.

Automation 360 Cloud Secure Operations and Controls

Automation 360 Cloud services are secured based on industry standards and frameworks such as NIST Cybersecurity Framework, Cloud Security Alliance (CSA) controls, AWS Cloud Adaption Framework, Center for Information Security (CIS) baselines, and others. This section describes the physical, logical, and administrative controls Automation Anywhere employs to secure Automation 360 Cloud, including alignment with customers' associated security practices.

As part of the cloud security framework, there are a few key security areas required to protect the cloud service. They include:

- Security program management
- Asset management
- Access management
- Physical and environmental security (access control, availability control)
- Application and development
- Secure operations
- Incident management
- Vendor management
- Business continuity and disaster recovery

Security Program Management

Security Ownership: Automation Anywhere maintains an IT InfoSec, data privacy, and Cloud SecOps team who advise the cloud operations team and manage security certifications and data privacy controls. All such team members complete security and privacy training on an annual basis.

Security Roles and Responsibilities: Automation Anywhere CloudOps and Cloud SecOps personnel with access to customer content are subject to strict confidentiality obligations. Automation 360 service security policies: Automation Anywhere maintains security and safety principles established and approved by Automation Anywhere executive management. Policies provide security requirements in a clear and concise manner. Standards define the process or methodology of meeting policy requirements.

Automation 360 Service Risk Management: Automation Anywhere performs assessments of key areas of risk associated with cloud services, including, by way of example only and as applicable, privacy risk assessments, open-source reviews, and export control analysis.

Asset Management

Asset Inventory: Automation Anywhere-managed systems and services are used to deliver the Automation 360 Cloud. Identified system owners are responsible for maintaining and updating the inventory as needed.

Asset and Data Handling: Automation Anywhere identifies and classifies customer content to ensure access is appropriately restricted. Automation Anywhere personnel must obtain customer authorization before remotely accessing customer content.

Access Management

Access Policy: Automation Anywhere maintains a record of background checks and security privileges of CloudOps and Cloud SecOps individuals having access to customer content and follows the principle of least privilege.

Access Authorization: Automation Anywhere maintains and updates a record of CloudOps and Cloud SecOps personnel authorized to access Automation Anywhere systems that contain customer content. New access to systems is reviewed and approved by management before being granted. Automation Anywhere performs regular reviews of user accounts and assigned permissions for key systems. Automation Anywhere identifies personnel who may grant, alter, or cancel authorized access to data and resources. Automation Anywhere ensures that where more than one individual has access to systems containing customer content, the individuals have separate identifiers/log-ins.

Least Privilege: Automation Anywhere restricts access to customer content to only those individuals with customer authorization to perform their support and troubleshooting job function.

Integrity and Confidentiality: Automation Anywhere requires that all support, CloudOps, and Cloud SecOps involved in delivering the Automation 360 Cloud secure computers and data when left unattended and that passwords remain unintelligible throughout their lifecycle.

Authentication: Automation Anywhere uses industry-standard practices to identify and authenticate CloudOps and Cloud SecOps personnel accessing information systems. Where authentication mechanisms are based on passwords, we follow industry-standard practices for password handling and management, including:

- Passwords are renewed regularly, as dictated by system requirements and Automation Anywhere standards.
- Passwords must meet length and complexity requirements, including a minimum length of eight characters.
- Personnel are prohibited from sharing passwords.
- Deactivated or expired identifiers are not granted to other individuals.

Automation Anywhere maintains procedures to deactivate passwords that have been corrupted or inadvertently disclosed. Automation Anywhere monitors security risks through, including but not limited to, penetration testing, vulnerability assessments, etc.

Physical and Environmental Security (Access Control, Availability Control)

Physical Access to Automation Anywhere Facilities: Automation Anywhere limits facilities access to authorized individuals. ID badges are required for employees, contractors, and guests and must be visible at all times when in the facility. Automation Anywhere monitors facility entry points using various methods, including security guards, intrusion detection, and CCTV cameras.

Onboarding: New employees and contractors are required to sign a confidentiality agreement prior to starting with us, and subsequently, during the onboarding process, security awareness courses are delivered to these new hires.

Hosted Data Centers: Automation Anywhere uses public cloud services to provide a global presence for Automation 360 Cloud. Geo presence is maintained in the following regions and countries: US, EU, Brazil, Japan, India, Singapore, Australia, South Africa, and Bahrain. No physical data center facilities are used.

Application and Development

Security System Development and Maintenance: A secure software development life cycle (SDLC) is set up by employing tools and techniques to the existing development process. At each step in the software development lifecycle process, checks and certifications are performed by distinct administrators with different roles and privileges. Strict separation of duties and multi-layer controls are built in by design to ensure the software development pipeline is reliable, scalable, efficient, secure, and compliant.

Cloud security is managed and monitored by a specialized security engineering team, responsible for design review, threat modeling, manual code review and spot checks, and ongoing penetration testing.

We have internal and external security testing programs. Internal testing spans planning, development, and testing phases, with each test building on previous work. We have an established approach to static and dynamic code analysis at both the development and testing phases. External testing is done on production and is built around the concept of "ongoing assurance."

Open-Source Management: Automation Anywhere uses a software-based system for managing open-source reviews and approvals. In addition, Automation Anywhere conducts periodic scans and audits of its software products to confirm open-source compliance.

Change Management: Automation Anywhere maintains change control procedures that address security requirements of information systems, testing, acceptance of testing, and security around the use of test data. Software and configuration changes are managed and tracked using standard ticketing systems.

Secure Operations

Loss Prevention: Automation 360 leverages data loss prevention (DLP) techniques and tools that are cloud-specific. A combination of tools that monitor, detect, correlate, and remediate events is deployed. These tools integrate with security information and event management (SIEM) and log analytics to detect intrusion and data exfiltration.

Malicious Software: Automation Anywhere uses anti-virus software, anti-malware software, and other controls to avoid malicious software gaining unauthorized access to customer data.

Network Segregation and Access: Automation Anywhere implements mechanisms designed to enforce internal access management policies and standards across services, including network controls covering access to customer data. These include, as appropriate: configuring an intermediate untrusted zone between the internet and the internal network that includes a security mechanism to restrict access and unauthorized traffic.

Automation Anywhere practices a layered approach to network segregation with controls at each layer. The public subnet(s) shields the internal private subnet(s) from direct internet access. Sensitive data and/or other information assets are deployed on the internal private subnets only, where there is no direct access to the internet. The only access to those assets is from select authorized hosts, restricted by network layer access control lists (ACLs), virtual private cloud (VPC) routing, and firewall rules as relevant. Within the private subnet, lateral propagation is also restricted based on business needs. We control access to our sensitive networks on a need-basis only. All staff connectivity for backend privileged administrators requires connection to the bastion hosts as the first layer using device certificates, multi-factor authentication, and proxies or VPNs.

Operational Monitoring: Automation Anywhere's CloudOps team monitors infrastructure CPU, memory, and application logs 24x7 to operate and maintain the Automation 360 Cloud. This may include monitoring the performance, stability, usage, and security of the services and related components. The Control Room environments are monitored for resource capacity to ensure customers' multitenant environments have sufficient spare resources and capacity as their bot creation and operational loads increase.

Usage Telemetry: Automation Anywhere operations team does not access a customer's Control Room environment or have visibility into a customer's business data unless directed to perform diagnostics as part of a support case. Automation Anywhere does securely collect telemetry data on feature usage to help improve the service, for example, to automatically guide users in navigating the features. This telemetry does not include any personally identifiable information (PII) or business data of the customer.

Security Monitoring: Automation Anywhere has deployed multiple layers of security log, event, and threat monitoring and detection in the environment. This consists of public cloud platform, audit trail and control plane logs, IAM logs, endpoint and container security logs, operating system logs, and other third-party security logs aggregated, correlated, and monitored for round-the-clock security monitoring. Automation Anywhere security operations use AIOps monitoring techniques to automatically baseline performance and auto-detect any unusual behavior which may indicate a bad actor. The anomaly would be investigated, and the container service removed if required.

Incident Management

Incident Response: Automation Anywhere maintains an incident response program designed to analyze, contain, eradicate, and recover from security and safety incidents impacting Automation Anywhere managed networks and/or systems or customer data.

Incident Notification: If Automation Anywhere determines that customer data within its control has been subject to a security incident, the customer will be notified under and according to applicable law.

Incident Post-Mortem: Automation Anywhere runs a post-mortem after an incident has occurred to analyze and improve tools and processes to mitigate future occurrences.

Vendor Management

Onboarding: Automation Anywhere performs security assessments of service providers who provide service components that store and process customer data. Automation Anywhere requires service providers connected with the services to comply with the level of security in this section that applies to the services they provide.

Off-boarding: Upon termination of a supplier relationship, the service provider is required to return all customer content in its possession or to certify that all customer content has been securely destroyed.

Business Continuity and Disaster Recovery

Business Continuity: Automation Anywhere maintains emergency and contingency plans and has ISO 22301 BCMS certification.

High Availability: Each regional data center presence Is designed with application-level high availability and highly available public cloud services across the region. Automation 360 Cloud follows industry standards best practices with a cloud uptime SLA of 99.9%.

Disaster Recovery: Backups are taken and maintained in an encrypted format to restore the service in the case of a disaster. Backups are taken every 6 hours to another region (except Australia, where backups are kept in the country). If a disaster is declared for the primary region, a secondary region is instantiated for all tenants using the backup taken every 6 hours. The current objectives for this recovery are:

- RTO (Recovery Time Objective): Time to get a new region up and running with the last backup data restored = 6 hours.
- RPO (Recovery Point Objective): The maximum duration for data loss during a restore = 6 hours.

AUTOMATION 360 DATA PRIVACY

Automation Anywhere adopts a "privacy-first" approach for the protection of customers' data and infrastructure. There are three types of data processed in the Automation 360 Cloud.

Operational Data: This includes status and log information that aids in running the automations such as error logs, audit logs, device connectivity stats, and operational dashboards.

Business Data: This is data used in operating a business and that is being passed between systems as part of the bot automation such as customers' client data, invoice numbers, or images of PoS. An example is the data uploaded to the cloud for processing document systems like IQ Bot™.

Personal Data: This is any data that could be used to identify an individual and is governed by laws such as GDPR and CCPA. Examples of such personal information include, but are not limited to, individual names, telephone numbers, email addresses, job titles, and contact information contained in invoices or emails.

Data Collection

The deployment model involves customers building their bots and managing the bot deployments from the Control Room in the cloud. Once the bots are built, they are tested and deployed to execute on the users' compute infrastructure.

The table below describes the data collected for the Automation 360 Cloud portfolio. The table provides guidance on which data could possibly be used to identify a natural person.

DATA ITEM	DATA CATEGORY	DESCRIPTION
Username	Personal	Email, first and last name, preferred name, time zone, last login, password, questions set, AD-domain
User password	Personal	
Password security key	Personal	Credential vault password security key
Bot Agent device access	Personal	Device username and access credentials
Role definitions	Personal	Admin, creator, etc.
Roles mapped to users, device, resource	Personal	User roles
Bot device IP / FQDN	Personal	Device IP address or FQDN can be tracked to a user
Bot definition (repository)	Operational	Data stored as part of the bot definition
Bot application credentials	Personal	Application user, URL, public key, routing name
Control Room bot schedules	Operational	Bot management—when and where to run bots
WLM workflow definition	Operational	When and where to run bots in which sequence
Audit logs	Personal	May contain identifiers: device message log, deployment message log, email message log, job execution log: (start/end time, user ID, schedule, automation name, deployment ID. Device name, bot name, username), User management, edit log, credential vault message log, server & data base, change logs
Errors logs	Personal	May contain identifier
Operational analytics	Operational	Service status
Business analytics	Business/ Personal	Business data tagged in automated processes for analysis by Bot Insight
Intelligent document processing data	Business/ Personal	Documents uploaded to IQ Bot for extraction and processing For IQ Bot: uploaded documents and extraction results.
Intelligent document processing data	Operational	For IQ Bot: Users learning instances, domains, operational statistics, and validation changes
Telemetry usage data	Operational	Feature usage, licenses enabled, aggregated with no personal/user data identifiers

Process and workflow data	Business/Personal	For AARI: AARI Web workflow definition: Describing how a process executes (including but not limited to bot, forms, and other steps required to execute the process) AARI Web dataflow: Stores data incidentally generated by executing the process (including all inputs and outputs from the various process steps) For Discovery Bot: Process data: This includes recordings performed by the end user about their process. The artifacts are stored in the form of JSON files, database tables (meta data e.g., application name, action name, source link), and images (snapshots of the screens while recording).
Other data	Business/Personal	For AARI: AARI Web Team definitions: Describing team membership, and process access rules AARI Web file storage: Stores files uploaded as a part of the request's dataflow.

Data Use Telemetry

Operation and Support

Automation 360 Cloud operations will monitor the deployment system's operational performance to operate, scale, and support the service according to the SLA per the service agreement between Automation Anywhere and the customer.

Automation Anywhere does not have visibility into the customer's data. Where support services need access to the actual data for troubleshooting and resolving technical product issues, Automation Anywhere support personal will only do so with the appropriate customer permissions in place.

To improve the product, Automation Anywhere will:

- Analyze feature usage data to improve the product—e.g., add telemetry to provide operational visibility into feature usage. This will help Automation Anywhere to prioritize and add improvements to the product. Examples include:
  - Review frequency of usage of application commands to help prioritize which commands to add to future releases
  - Provide operational best practices recommendations
  - Provide support services that will be used for updating, securing, and troubleshooting
  - Personalize products and make recommendations
  - For IQ Bot and AISense, the structure of document fields may be used to improve the quality of AI models for document processing

For more information about Automation Anywhere data privacy policy, please refer to:
automationanywhere.com/in/privacy

Data Retention After Subscription Termination

Automation Anywhere will keep customer data, configs (bots), IQ Bot data, and most logs for 30 days after the customer's subscription ends. Some logs may be kept for up to 180 days after the customer's subscription ends. Full details of the Data Processing Addendum and data retention policy can be found here:
automationanywhere.com/support/DPA.pdf

Data Security

Automation 360 Cloud provides customers a comprehensive set of security features that automatically provides or is configurable by design to provide data security. As with any enterprise application, the consistent and proper utilization of security controls depends upon the organization's personnel utilizing the service.

Authorization of users depends on the customer's administrators who should implement controls to ensure that only authorized personnel have access.

The authorized data owner can limit access to allow only authorized personnel with a business need to access the service. Corporate users with access can be granted fine-grained permissions via role-based access controls (RBAC) from the Control Room. The RBAC models enable dual-controls and separation of duties within the operations. Permissions can be implemented for all aspects of product operation, including credentials, bots, Bot Runners, Bot Creators, bot schedules, IQ Bot learning instances, audit log access, workload management queues, and pools.

Automation 360 Cloud provides full audit capabilities where all user actions are audited within the platform, providing records of all access and actions taken by operations personnel. An audit is automated for all privileged and non-privileged roles to conform to best practices defined in NIST AC-6.

As bots are software programs developed by customer business experts, state-of-the-art secure software development life cycle (SDLC) processes should be implemented by the customer accordingly. Toward this end, Automation Anywhere supports the separation of development, testing, and production environments through a combination of separate deployments and RBAC as described above.

Encryption

The service follows industry-standard encryption technologies to ensure customer data is encrypted between the customer's network and the Automation 360 Cloud service. All traffic to/from users is encrypted using HTTPS + SSL / TLS 1.2 (port 443) to talk to the Automation 360 Cloud environment. All data stored in the service, i.e., data at rest is encrypted using AES-256.

Data Privacy

Automation Anywhere takes a data privacy-first approach to product development. Every product is designed to address data regulation and privacy requirements that our global customers need to abide by, including regional regulations worldwide that are meant to protect data privacy. The General Data Protection Regulation (GDPR), California Consumer Privacy Act (CCPA) are few regulatory examples that dictate how to handle sensitive personal data and ensure that the information is not exposed to unauthorized parties.

Per the GDPR, there are different responsibilities when it comes to the handling of data. A data controller is an entity that determines the why and how the data is processed. A data processor performs the data processing on behalf of the data controller. The Automation Anywhere role is that of a data processor while the customer is the data controller and always controls the business, operational, and personal data.

Automation Anywhere employs data privacy and data security best practices for the proper handling of customer's data, including consent, notice, and regulatory obligations. More specifically, data privacy involves how data is collected, stored, used, and adheres to regulatory compliance.

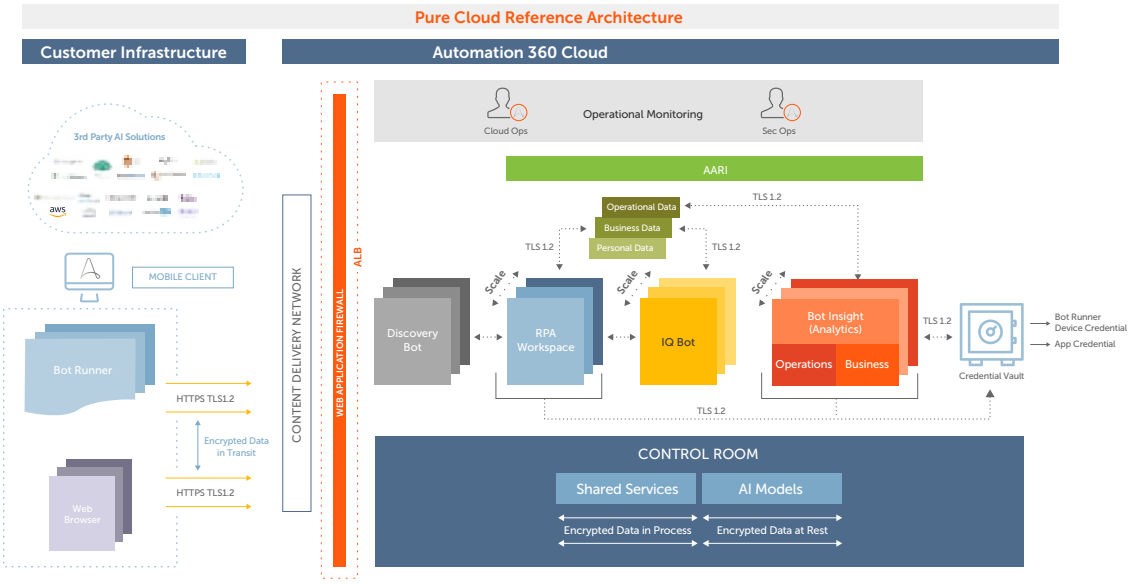
The Control Room provides the means to set up and remove user accounts with appropriate RBAC controls. The organization's administrator is responsible for providing appropriate access to users and resources. The administrator should create a policy with the required level of access as per corporate and user data privacy guidelines. If users request access or limitations to their personal information, they should contact their administrator. The customer administrators can delete the user accounts in the Control Room.

For more detail regarding GDPR data privacy inquiries and copies of the personal data, Automation Anywhere provides the following site Data Subject Access Rights Request Form.

SECURITY & DATA PRIVACY IN AUTOMATION 360 DEPLOYMENT MODELS

Automation Anywhere offers three deployment models: Pure Cloud, Cloud-Enabled, and On-Premises with select updates via cloud. In this section, we will cover the secure architecture for the Pure Cloud and Cloud-Enabled deployment models and security operational responsibilities.

Pure Cloud



Pure Cloud includes several integrated RPA services consisting of the Control Room, data storage, RPA Workspace, credential vault, Bot Insight, Discovery Bot, AARI, and IQ Bot. To learn more about the Automation 360 platform capabilities and individual Automation 360 products, visit automationanywhere.com.

Summary of Pure Cloud Security & Data Privacy Responsibilities

ATTRIBUTE	RESPONSIBLE PARTY
Cloud security NIST 800-53 framework	Security managed by Automation 360 cloud operations
Business continuity /Disaster recovery	Managed by Automation 360 cloud operations
High availability	Managed by Automation 360 cloud operations
Business data localization	Managed by Automation 360 cloud operations
Business data privacy	Managed by Automation 360 cloud operations

Table 1—Customer and Automation Anywhere covered service and responsibility matrix for the Pure Cloud deployment model.

In the Pure Cloud deployment model, the Automation 360 Cloud operations team manages and operates the core services, including the Control Room, RPA Workspace, Discovery Bot, AARI, IQ Bot, and Bot Insight. With the Pure Cloud deployment model, Automation Anywhere is the SaaS provider and responsible for the high availability (HA), business continuity (BC)/disaster recovery (DR), operations policy, and procedures.

Automation 360 Cloud is deployed as a high availability service across all supported regions specified by Automation Anywhere (this pertains to our Pure Cloud deployment offering). For disaster situations, backups are taken every 6 hours to another region (except Australia, where backups are kept in country). If a disaster is declared for the primary region, then a secondary region is instantiated for all tenants using the backup taken every 6 hours. The current objectives for this recovery are:

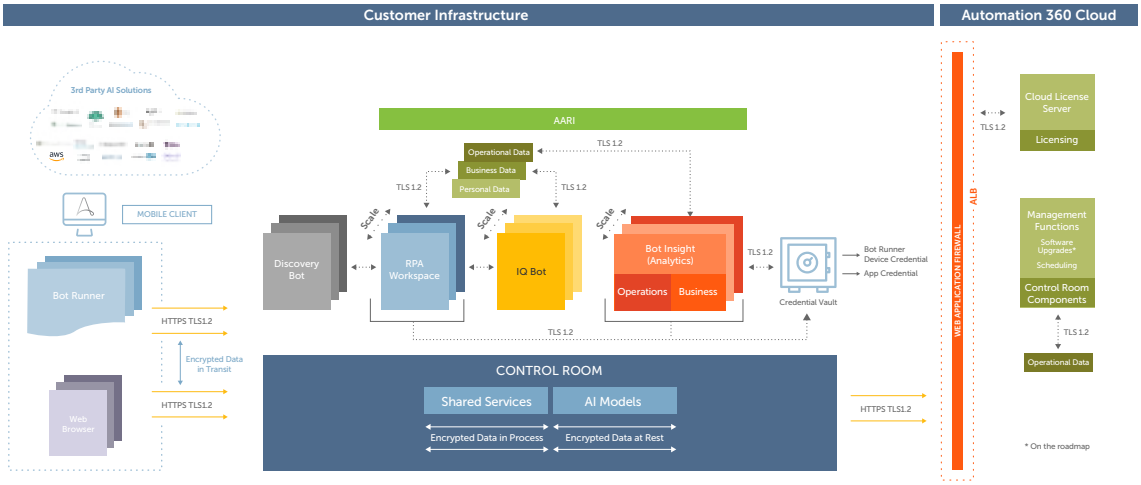
1. Recovery Time Objective (RTO)—Time to get a new region up and running with the last backup data restored = 6 hours.
2. Recovery Point Objective (RPO)—The maximum duration for data loss during a restore = 6 hours.

Automation 360 Cloud hosts the Automation 360 platform and associated applications such as RPA Workspace, Discovery Bot, AARI, IQ Bot, and Bot Insight. Operational data and business data from these products can physically reside on the Automation 360 Cloud. The Bot Agent for running Bots and all systems and data accessed by the bot reside physically on customer infrastructure managed and operated by the customer.

Customer Considerations for Automation 360 Pure Cloud Deployment:
With Pure Cloud deployment, customers can take advantage of the robust security architecture of the Automation 360 Cloud. Under normal usage, the customer is comfortable with their customer confidential information being present on the Automation 360 Cloud temporarily as part of automating processes.

In the case where automated processes may involve manipulation of sensitive or regulated data stored in systems on the customer's infrastructure, and it is required that this data is not processed or stored with the Automation 360 Cloud, customers can still develop bots on the cloud using test data not subject to these controls. The bots are then deployed onto the customer infrastructure, and all process automation occurs against the regulated data. This approach limits the customer's use of some Automation 360 Cloud-hosted products but ensures that none of the sensitive data is sent to the Automation 360 Cloud. The limitations are the use of workload management (WLM), Bot Insight business dashboards, AARI, and Discovery Bot. Note that the RPA user account specifications and credentials are stored on the cloud and are governed by data privacy laws, which Automation 360 Cloud supports.

Cloud-Enabled Deployment Model



In this model, the customer manages and operates the bulk of the core services, including the Control Room, bot creator, and bot runners.

Summary of Cloud-Enabled Security and Data Privacy Responsibilities

ATTRIBUTE	RESPONSIBLE PARTY
Cloud Security NIST 800-53 Framework	Shared Customer: On-site setup Automation 360 Cloud operations: Cloud components only such as licensing and scheduling
Business continuity /Disaster recovery	Shared Customer: On-site setup Automation 360 Cloud operations: Cloud components only such as licensing and scheduling
High availability	Shared Customer: On-site setup Automation 360 Cloud operations: Cloud components only such as licensing and scheduling
Business data localization	Managed and operated by the customer
Business data privacy	Managed and operated by the customer

Table 2—Customer and Automation 360 Cloud covered service and responsibility matrix for Cloud-Enabled model.

All the customer's operational, business, and personal data physically resides on the customer's premises. Automation 360 Cloud provides management functions that include software upgrades, user authentication via SAML 2.0, licensing, and command package delivery. The benefit is that all customer data physically resides on the customer's infrastructure, putting the customer in full control of managing the data. The services such as software updates, licensing hosted on the Automation 360 Cloud provide the benefits of fast activation and adoption as well as maintenance efficiencies.

Customer considerations for Automation 360 Cloud-Enabled deployment: While customers can benefit from some services and functionality in Automation 360 Cloud, the customer is responsible for the infrastructure, operations policy, and procedures related to the on-premises portion of this deployment model. High availability, business continuity, and disaster recovery are also managed by the customer. All data privacy and compliance rests with the customer. Customers should consider planning, resources, and costs associated with managing these responsibilities when choosing the Cloud-Enabled deployment model.

Additional Cloud Security Resources

- Automation 360 webpage
- Automation 360 security webpage
- Privacy Policy
- Security Architecture
- Cloud Security Alliance attestation

December 2021

AUTOMATION ANYWHERE