Security & Cloud Operations for Automation Anywhere Enterprise Cloud

SECURITY & CLOUD OPERATIONS FOR AUTOMATION ANYWHERE ENTERPRISE CLOUD

Automation Anywhere customers can now reap the full benefits and flexibility of running automation in a secure public cloud infrastructure with our new Enterprise Cloud solution. This provides a full suite of options to our Enterprise customers to run automation on premise and over the public cloud. The new Enterprise Cloud solution comprises an integrated Control Room and BOT creation service hosted on our Enterprise Cloud and the ability to deploy and run cloud-connected BOT Runner nodes on the customer's infrastructure via a secure and encrypted channel. Our Enterprise Cloud solution provides the same functionality as the Enterprise Edition solution deployed by the customer on their infrastructure but is, instead, deployed and operated by the Automation Anywhere cloud operations team. This ensures that customers can rely on our cloud operations team to monitor and scale the supporting cloud infrastructure on demand. Customers can now benefit from multi-node, high availability infrastructure that powers SLA-driven performance and business continuity, even when there are dramatic swings in automation workloads.

Automation Anywhere takes data security, trust, and integrity of our customers' data and processes very seriously. Our cloud solution is going through a stringent SOC 2 Type 1 compliance process to ensure the highest level of security and compliance. We have put a robust, secure operations service in place to ensure our customer data is secure. This document covers the cloud service architecture, data security and operational measures, physical controls, and compliance certifications for our hosted service that delivers intelligent automation in the cloud.

AUTOMATION ANYWHERE ENTERPRISE CLOUD DEPLOYMENT ARCHITECTURE

Enterprise Edition RPA services are deployed in the cloud via a multitenant architecture. Each customer tenant will be set up in its own set of containers for the core RPA components; tenant isolation means each tenant has their own pod with a set of containers for a Control Room in a their own private network. A different database is created on a relational data base storage instance per tenant and a different directory mount is created per tenant on a common file system.

The microservices architecture uses containers for structuring applications as a collection of services. All Control Room instances for Kubernetes worker nodes, IQ Bot instances and datastores are inside a private network on private subnets with no direct access to the internet. The MSSQL database & Elastic Search cluster for logging use encryption at rest and are on a private network with no access from the internet.

For IQ Bot, we need to create a unique database instance, cloud storage and a cluster of Virtual Machine's for each customer.

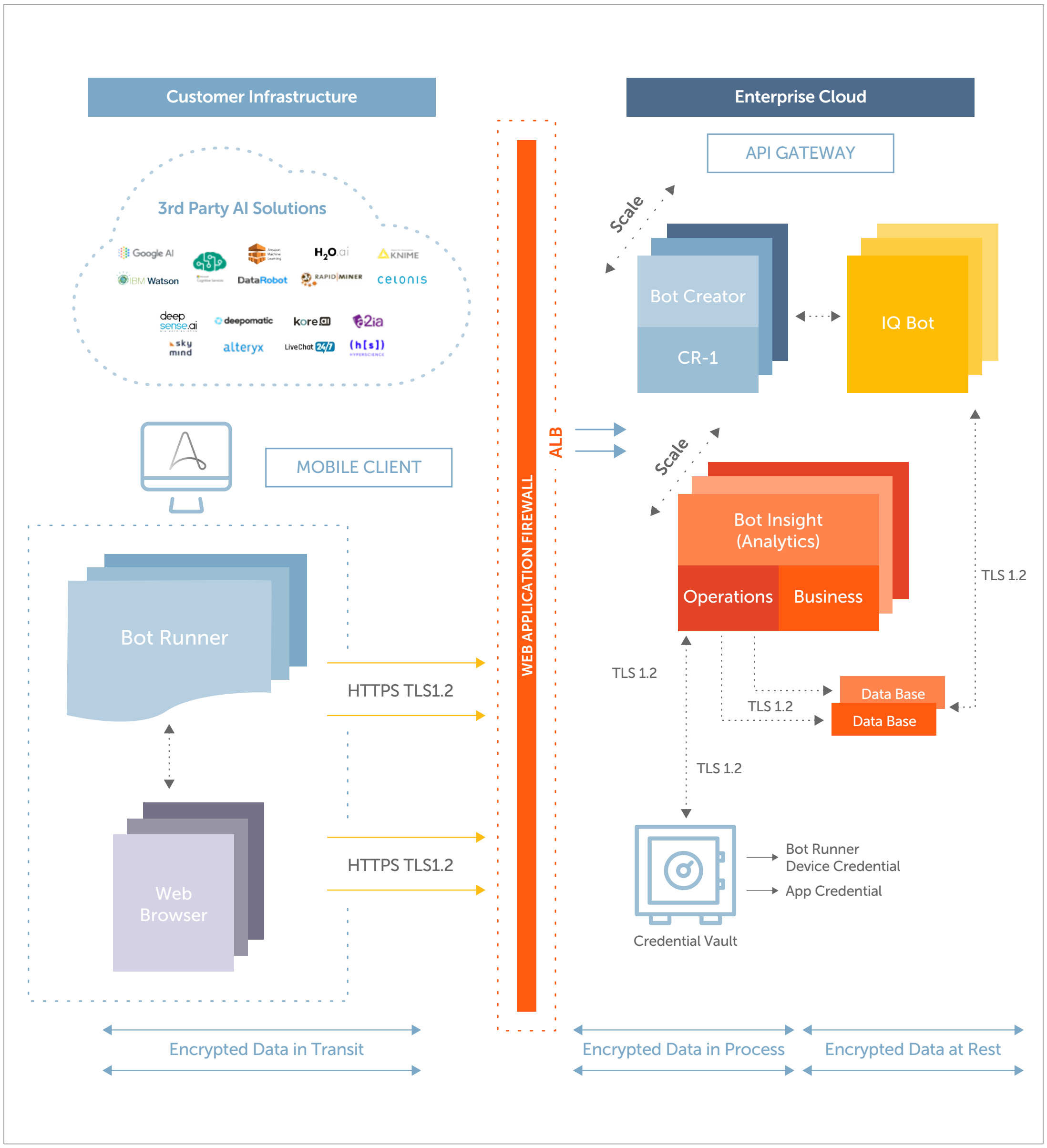

FIGURE 1. AUTOMATION ANYWHERE ENTERPRISE CLOUD SOLUTION ARCHITECTURE

Data Encryption: All traffic to/from users (BotRunners) residing on the customer's network is encrypted using HTTPS + SSL / TLS 1.2 (port 443) to talk to the intelligent automation cloud. All sessions are started by the customer by initiating an outbound session from the customer's network to the cloud.

Access to the Enterprise Control Room and IQ Bot on the Enterprise Cloud is only via HTTPS on port 443 via Application Load Balancers (ALBs). The Bot runners/agents initiate web socket connections into the cloud-hosted Control Room. The connection is resilient, and connections are re-established automatically in the event of any loss of connectivity. Any loss of connectivity does not impact any running bots.

In addition to encrypting data in transit, local credentials, uploaded documents and selected runtime data used by bots are encrypted when that data is at rest via AES-256 encryption.

Separation of Duties: Extensive separation of duties is supported to restrict access to a single individual to prevent fraud or manual errors. Only authorized personnel have limited access to individual tasks, providing protection to business and driving internal controls using the Automation Anywhere cloud platform. Using the role creation wizard, administrators can easily define user privileges including custom roles, setting permissions that account for the full suite of Control Room, IQ Bot objects and functions including user management, licensing, Credential Vault, sets of Bot Runners, bot schedules, bot operations/dashboards, and audit logs.

Authentication and Authorization: Access control is mandated and enforced by the Automation Anywhere enterprise security architecture. Once a user is authenticated, authorization to resources adhering to the core principles of least privileges and separation of duties is performed. Authorization to perform actions within the Automation Anywhere enterprise security architecture is configured with fine-grained Role Based Access Control (RBAC). The responsibility for overall administration of the platform – including configuring components, interfaces, and all roles/permissions administration – resides with the RPA system administrator.

Automation Anywhere will maintain proper controls for requesting, approving, revoking, and revalidating our cloud operations staff's access to our cloud infrastructure. Only employees with clear business needs have access to cloud infrastructure, databases, and applications. All access requests are approved based on individual role-based accesses and reviewed on a regular basis to validate the continued business need.

Initial Configuration and Access: Upon purchase, the customer's primary administrator will be sent an e-mail containing their access URL, username and initial password so they can log in securely and begin using the enterprise Control Room.

Secure Cloud Access: Access to the cloud infrastructure is protected through the use of Virtual Private Cloud (VPC) routing, firewall rules, and application firewalls. Intelligent threat detection is enabled for each region to inspect DNS logs and network flow logs into and within the tenant's private network. Access is protected with WAF, which is set up for OWASP top 10 on all load balancers for each tenant.

DNS: Whitelist their <customername>.my.automationanywhere.digital domain

Compliance: AAI is working towards SOC2 type 1 and ISO27001 compliance.

API: Automation Anywhere provides APIs for integrating with third-party automation for secure authentication and orchestration of bot lifecycle management.

Cloud Operations is only accessible for operations. Each environment, production, staging, and development is set up using a different AWS account for each. To ensure secure access of system information, RBAC is used to restrict access, so only authorized operations personnel will have access to production and staging environments.

AUTOMATION ANYWHERE ENTERPRISE CLOUD OPERATIONS

This security operations description covers the technical and organizational measures employed in connection with delivering the Automation Anywhere Enterprise Cloud solution.

AUTOMATION ANYWHERE SECURITY CONTROLS

This section describes the physical, logical, and administrative controls Automation Anywhere employs to secure the Enterprise Cloud solution and customer's associated security practices. Automation Anywhere is working towards SOC2 type 1 certification as the baseline for its services security program.

Automation Anywhere reserves the right to modify the controls specified herein provided that the controls employed during a term of service for which the customer has paid remain protective of customer content on the effective date of such term.

Area	Control(s)
Security Program Management	**Security Ownership:** Automation Anywhere maintains an IT Infosec and data privacy 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 personnel with access to customer content are subject to confidentiality obligations. **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.

Area	Control(s)
Security Program Management	**Product 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 maintains an inventory of Automation Anywhere-managed systems and services used to deliver the services. 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 imposes restrictions on printing customer content and disposing of printed materials that contain customer content. Automation Anywhere personnel must obtain authorization prior to storing customer content on portable devices, remotely accessing customer content, or processing customer content outside facilities managed by Automation Anywhere or its service providers.
Access Management	**Access Policy:** Automation Anywhere maintains a record of background checks and security privileges of individuals having access to customer content and follows the principle of least-privilege. **Access Authorization:** Automation Anywhere maintains and updates a record of personnel authorized to access Automation Anywhere systems that contain customer content. New access to systems is reviewed and approved by management prior to being granted. Automation Anywhere performs regular reviews of user accounts and assigned permissions for key systems. Automation Anywhere identifies those 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 who require such access to perform their job function.

Area	Control(s)
Access Management	**Integrity and Confidentiality:** Automation Anywhere requires that users secure computers and data while unattended, and that passwords remain unintelligible throughout their lifecycle. **Authentication:** Automation Anywhere uses industry-standard practices to identify and authenticate users 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 8 characters. • Personnel are prohibited from sharing passwords. • De-activated 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.
Loss Prevention	**Malicious Software:** Automation Anywhere uses anti-virus software, anti-malware software, and other controls to avoid malicious software gaining unauthorized access to customer content, including malicious software originating from public networks.
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.

Area	Control(s)
Physical and Environmental Security (Access Control, Availability Control)	**Hosted Data Centers:** When Automation Anywhere uses third-party co-located data centers for provision of the services, Automation Anywhere requires that the service provider meets or exceeds the physical and environmental security requirements of Automation Anywhere-managed facilities. Minimum security requirements include, but are not limited to: • Physical access restrictions and safeguards (authentication,logs, monitoring, etc.) • Adequate separation of environments • Fire suppression, detection, and prevention mechanisms • Climate control systems (temperature, humidity, etc.) **Cloud Computing:** When Automation Anywhere uses public cloud infrastructure, Automation Anywhere contracts with the public cloud providers to provide physical access control to their hosted data centers.
Application and Development	**Security System Development & Maintenance:** In order to prevent rogue and unauthorized bots, a secure SDLC is set up by adding security-related activities to an existing development process. At each step in the bot 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 digital workforce is reliable, scalable, efficient, secure, and compliant. This process 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 both 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.

Area	Control(s)
Application and Development	**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	**Network Design:** Automation Anywhere implements mechanisms designed to enforce access management policies and standards across services, including network controls over access to customer content. 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. We practice a layered approach to network access with controls at each layer of the stack. We control access to our sensitive networks through the use of Virtual Private Cloud (VPC) routing, firewall rules, encryption technologies, and need-basis access. Staff connectivity requires device certificates, multi-factor authentication, and use of proxies for sensitive network access. **Event Logging:** In certain services, Automation Anywhere collects logs in order to operate Enterprise Cloud solution. Logs may include access ID, time, authorization granted or denied status, diagnostic data such as trace and crash files, and other relevant activity. Logs are used: (i) for providing, securing, managing, measuring, and improving the services and associated analytics, (ii) as directed or instructed by the customer and its users for support purposes, and/or (iii) for compliance with Automation Anywhere policies, applicable law, regulation, or governmental request. This may include monitoring the performance, stability, usage and security of the services and related components. The customer may not block or interfere with this monitoring. Automation Anywhere may supplement logs with information collected from third parties for the purposes specified above.

Area	Control(s)
Incident Management	**Incident Response:** Automation Anywhere maintains an incident response program designed to contain, analyze, remediate, and communicate security and safety incidents impacting Automation Anywhere managed networks and/or systems or customer content. **Incident Notification:** If Automation Anywhere determines that customer content within its control has been subject to a security incident, the customer will be notified under and pursuant to applicable law. **Incident Recording:** Automation Anywhere maintains a record of known security incidents with a description of the incident, the time period, the consequences of the incident, the name of the reporter, to whom the incident was reported, and the procedure for recovering data and services as applicable.
Vendor Management	**Onboarding:** Automation Anywhere performs security assessments of service providers who will have access to customer content and/or to components of the services that process customer content. Automation Anywhere requires service providers connected with the services to comply with the level of security in this section that are applicable to the services they provide. Service providers who access and subsequently transfer customer personal data that is subject to GDPR outside of the European Union do so via Privacy Shield or pursuant to the standard contractual clauses. Service providers are assessed periodically, based upon the sensitivity and risk associated with their services. **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.

Area	Control(s)
Business Continuity and Disaster Recovery	**Business Continuity:** Automation Anywhere maintains emergency and contingency plans for the infrastructure in which Automation Anywhere information systems that process customer content are hosted. **Disaster Recovery:** Backups are taken to enable data to be restored in the case of a disaster. Production data centers are designed with high availability and resilient design of network and compute infrastructure. In special scenarios, there may be an impact on the service until the service is restored. The Automation Anywhere redundant storage, backup policy and procedures for recovering data are designed to attempt to reconstruct customer content in its original or last-replicated state.
Customer Security Obligations	The customer is responsible for managing security not expressly included as part of the services. This includes limiting the access by Automation Anywhere to customer content only to what is needed for a customer to receive the service support. This includes protecting a customer's network and service components against interference, including monitoring and securing its networks and computing equipment. **Downloading customer content:** Where needed, both during the term of services and upon termination, Automation Anywhere Enterprise encrypts data in transit by default (HTTPS) and data at rest is encrypted. Further detail is provided in the product documentation for the services. The customer is responsible for using an appropriate browser.
Data Protection (Availability Control, Transmission Control)	**Failover Procedures:** Automation Anywhere implements mechanisms designed to address loss of availability of customer content, including storing copies of customer content in a different place from where the primary infrastructure processing the customer content is located. **Data Beyond Boundaries:** Automation Anywhere encrypts or enables customers to encrypt customer content that is transmitted over public networks that are part of a service.
Data Encryption	The service follows industry standard encryption technologies to ensure customer data is encrypted between the customer's network and the covered cloud service. All traffic to/from users (Bot Managers) is encrypted using HTTPS + SSL / TLS 1.2 (port 443) to talk to the intelligent automation cloud environment.

Area	Control(s)
Data Retention	The Automation Anywhere Enterprise Cloud solution will keep customer data, configs (bots), IQ Bot data, and most logs for 30 days after the customer’s subscription ends. Log files will be deleted no later than 180 days after the customer’s subscription ends.
Data Usage	Automation Anywhere does not generally have visibility into the customer data. Where support services need access into the actual data in order to troubleshoot and resolve issues, support personal will only do so with the appropriate permissions in place.
Automation Anywhere Enterprise Cloud	Automation Anywhere cloud operations will monitor the deployment system’s operational performance in order to operate, scale, and support the service in accordance with the service SLA <link here>.