Automation Anywhere, Inc.

Type 2 SOC 3

2023

SOC 3 FOR SERVICE ORGANIZATIONS REPORT

November 1, 2022 to October 31, 2023

Table of Contents

SECTION 1

ASSERTION OF AUTOMATION ANYWHERE, INC. MANAGEMENT

ASSERTION OF AUTOMATION ANYWHERE, INC. MANAGEMENT

November 30, 2023

We are responsible for designing, implementing, operating, and maintaining effective controls within Automation Anywhere, Inc.'s ('Automation Anywhere' or 'the Company') Automation 360 Cloud and Process Discovery Cloud Services System throughout the period November 1, 2022 to October 31, 2023, to provide reasonable assurance that Automation Anywhere's service commitments and system requirements were achieved based on the trust services criteria relevant to Security, Availability, and Confidentiality (applicable trust services criteria) set forth in TSP section 100, *2017 Trust Services Criteria for Security, Availability, Processing Integrity, Confidentiality, and Privacy* in AICPA, *Trust Services Criteria*. Our description of the boundaries of the system is presented below in "Automation Anywhere, Inc.'s Description of Its Automation 360 Cloud and Process Discovery Cloud Services System throughout the period November 1, 2022 to October 31, 2023" and identifies the aspects of the system covered by our assertion.

We have performed an evaluation of the effectiveness of the controls within the system throughout the period November 1, 2022 to October 31, 2023, to provide reasonable assurance that Automation Anywhere's service commitments and system requirements were achieved based on the trust services criteria. Automation Anywhere's objectives for the system in applying the applicable trust services criteria are embodied in its service commitments and system requirements relevant to the applicable trust services criteria. The principal service commitments and system requirements related to the applicable trust services criteria are presented in "Automation Anywhere, Inc.'s Description of Its Automation 360 Cloud and Process Discovery Cloud Services System throughout the period November 1, 2022 to October 31, 2023".

Automation Anywhere uses Amazon Web Services ('AWS') and Google Cloud Platform ('GCP') to provide cloud hosting services (collectively, the 'subservice organizations'). The description indicates that complementary subservice organization controls that are suitably designed and operating effectively are necessary, along with controls at Automation Anywhere, to achieve Automation Anywhere's service commitments and system requirements based on the applicable trust services criteria. The description presents Automation Anywhere's controls, the applicable trust services criteria, and the types of complementary subservice organization controls assumed in the design of Automation Anywhere's controls. The description does not disclose the actual controls at the subservice organizations.

The description indicates that complementary user entity controls that are suitably designed and operating effectively are necessary to achieve Automation Anywhere's service commitments and system requirements based on the applicable trust services criteria. The description presents the applicable trust services criteria and the complementary user entity controls assumed in the design of Automation Anywhere's controls.

There are inherent limitations in any system of internal control, including the possibility of human error and the circumvention of controls. Because of these inherent limitations, a service organization may achieve reasonable, but not absolute, assurance that its service commitments and system requirements are achieved.

We assert that the controls within the system were effective throughout the period November 1, 2022 to October 31, 2023 to provide reasonable assurance that Automation Anywhere's service commitments and system requirements were achieved based on the applicable trust services criteria, if complementary subservice organization controls and complementary user entity controls assumed in the design of Automation Anywhere's controls operated effectively throughout that period.

Prince Kohli

Prince Kohli
Chief Technology Officer
Automation Anywhere, Inc.

SECTION 2

INDEPENDENT SERVICE AUDITOR'S REPORT

INDEPENDENT SERVICE AUDITOR'S REPORT

To: Automation Anywhere, Inc.

Scope

We have examined Automation Anywhere's accompanying assertion titled "Assertion of Automation Anywhere, Inc. Management" (assertion) that the controls within Automation Anywhere's Automation 360 Cloud and Process Discovery Cloud Services System were effective throughout the period November 1, 2022 to October 31, 2023, to provide reasonable assurance that Automation Anywhere's service commitments and system requirements were achieved based on the trust services criteria relevant to Security, Availability, and Confidentiality (applicable trust services criteria) set forth in TSP section 100, *2017 Trust Services Criteria for Security, Availability, Processing Integrity, Confidentiality, and Privacy* in AICPA *Trust Services Criteria*.

Automation Anywhere uses AWS and GCP to provide cloud hosting services. The description indicates that complementary subservice organization controls that are suitably designed and operating effectively are necessary, along with controls at Automation Anywhere, to achieve Automation Anywhere's service commitments and system requirements based on the applicable trust services criteria. The description presents Automation Anywhere's controls, the applicable trust services criteria, and the types of complementary subservice organization controls assumed in the design of Automation Anywhere's controls. The description does not disclose the actual controls at the subservice organizations. Our examination did not include the services provided by the subservice organizations, and we have not evaluated the suitability of the design or operating effectiveness of such complementary subservice organization controls.

The description indicates that complementary user entity controls that are suitably designed and operating effectively are necessary, along with controls at Automation Anywhere, to achieve Automation Anywhere's service commitments and system requirements based on the applicable trust services criteria. The description presents Automation Anywhere's controls, the applicable trust services criteria, and the complementary user entity controls assumed in the design of Automation Anywhere's controls. Our examination did not include such complementary user entity controls and we have not evaluated the suitability of the design or operating effectiveness of such controls.

Service Organization's Responsibilities

Automation Anywhere is responsible for its service commitments and system requirements and for designing, implementing, and operating effective controls within the system to provide reasonable assurance that Automation Anywhere's service commitments and system requirements were achieved. Automation Anywhere has also provided the accompanying assertion (Automation Anywhere assertion) about the effectiveness of controls within the system. When preparing its assertion, Automation Anywhere is responsible for selecting, and identifying in its assertion, the applicable trust services criteria and for having a reasonable basis for its assertion by performing an assessment of the effectiveness of the controls within the system.

Service Auditor's Responsibilities

Our responsibility is to express an opinion, based on our examination, on management's assertion that controls within the system were effective throughout the period to provide reasonable assurance that the service organization's service commitments and system requirements were achieved based on the applicable trust services criteria. Our examination was conducted in accordance with attestation standards established by the AICPA. Those standards require that we plan and perform our examination to obtain reasonable assurance about whether management's assertion is fairly stated, in all material respects. We believe that the evidence we obtained is sufficient and appropriate to provide a reasonable basis for our opinion.

Our examination included:

- Obtaining an understanding of the system and the service organization's service commitments and system requirements
- Assessing the risks that the description is not presented in accordance with the description criteria and that controls were not suitably designed or did not operate effectively
- Performing procedures to obtain evidence about whether controls stated in the description were suitably designed to provide reasonable assurance that the service organization achieved its service commitments and system requirements based on the applicable trust services criteria

Our examination also included performing such other procedures as we considered necessary in the circumstances.

Independence and Ethical Responsibilities

We are required to be independent and to meet our other ethical responsibilities in accordance with relevant ethical requirements relating to the examination engagement.

Inherent Limitations

There are inherent limitations in the effectiveness of any system of internal control, including the possibility of human error and the circumvention of controls.

Because of their nature, controls may not always operate effectively to provide reasonable assurance that the service organization's service commitments and system requirements are achieved based on the applicable trust services criteria. Also, the projection to the future of any conclusions about the suitability of the design and operating effectiveness of controls is subject to the risk that controls may become inadequate because of changes in conditions or that the degree of compliance with the policies or procedures may deteriorate.

Opinion

In our opinion, management's assertion that the controls within Automation Anywhere's Automation 360 Cloud and Process Discovery Cloud Services System were suitably designed and operating effectively throughout the period November 1, 2022 to October 31, 2023, to provide reasonable assurance that Automation Anywhere's service commitments and system requirements were achieved based on the applicable trust services criteria is fairly stated, in all material respects, if complementary subservice organization controls and complementary user entity controls assumed in the design of Automation Anywhere's controls operated effectively throughout that period.

The SOC logo for Service Organizations on Automation Anywhere's website constitutes a symbolic representation of the contents of this report and is not intended, nor should it be construed, to provide any additional assurance.

Restricted Use

This report, is intended solely for the information and use of Automation Anywhere, user entities of Automation Anywhere's Automation 360 Cloud and Process Discovery Cloud Services during some or all of the period November 1, 2022 to October 31, 2023, business partners of Automation Anywhere subject to risks arising from interactions with the Automation 360 Cloud and Process Discovery Cloud Services, and those who have sufficient knowledge and understanding of the complementary subservice organization controls and complementary user entity controls and how those controls interact with the controls at the service organization to achieve the service organization's service commitments and system requirements.

This report is not intended to be, and should not be, used by anyone other than these specified parties.

A-LIGN ASSURANCE

Tampa, Florida
November 30, 2023

SECTION 3

AUTOMATION ANYWHERE, INC.'S DESCRIPTION OF ITS AUTOMATION 360 CLOUD AND PROCESS DISCOVERY CLOUD SERVICES SYSTEM THROUGHOUT THE PERIOD NOVEMBER 1, 2022 TO OCTOBER 31, 2023

OVERVIEW OF OPERATIONS

Company Background

Automation Anywhere's goal is to enable companies to operate with unprecedented productivity and efficiency by automating any part of the enterprise that can be automated with their intelligent and intuitive robotic process automation platform.

The company's vision is to take the robot out of the human. To liberate employees from mundane, repetitive tasks, allowing the employee to spend more time using their intellect and creativity to solve higher order business challenges. Automation Anywhere envisions a world where every employee will be empowered to be more productive and to drive more innovation, with all manual and routine tasks automated.

Automation 360 Cloud is a cloud-native intelligent automation platform, enabling companies to transcend front- and back-office silos and systems, both Software as a Service (SaaS) and legacy. Automation Co-Pilot is the digital assistant that simplifies automation so anyone can automate their business processes. At the beginning of 2022 AAI, acquired FortressIQ a meta-learning company that offers cognitive process intelligence using ethical artificial intelligence (IA). The Process Discovery Cloud cognitive automation Software-as-a-Service platform provides analytical tools to examine business processes by capturing video from customer workflows. Automation Anywhere's Process Discovery Cloud Services System "learns" the internal operations of businesses through imitation learning, in which technical operations are observed in real time. This compliments the Automation 360 suite and eventually will be fully integrated into it.

Description of Services Provided

Automation Anywhere's Automation 360 and Process Discovery Cloud Service Systems are cloud based and are hosted on either Amazon Web Services (AWS) or Google Cloud Platform (GCP). Production locations are throughout the world. Each Production system availability zone has a different availability zone for its disaster recovery site. A multi-tenant instance in one zone has no contact with a production instance located in a different zone (i.e., A Canadian assigned tenant has no access or processing in a US or EU zone.) All production systems in each zone are identical and run on the same release version.

Automation 360

The Automation 360 application comprises of integrated Control Room with bot (short for robot) creation capabilities hosted on the Automation 360 Cloud. It has the ability to run cloud connected Bot Agent nodes on the customer's infrastructure via a secure and encrypted channel. The Automation 360 provides the same functionality as Automation 360 software deployed by the customer on their infrastructure but is deployed and operated by Automation Anywhere's Cloud Operations team. The cloud hosted Automation 360 allows Automation Anywhere to continually monitor and scale the supporting infrastructure for the customer. This provides multi-node high availability that powers Service Level Agreement (SLA)-driven performance and business continuity, even when there are dramatic swings in automation workload.

Process Discovery

Automation Anywhere's Process Discovery Cloud Services is a meta-learning platform that offers cognitive process intelligence using ethical artificial intelligence (AI). The cognitive automation SaaS platform provides analytical tools to examine business processes by capturing video from customer workflows. The primary technologies used to implement the organization's services include computer vision, Kubernetes, machine learning, and AI. These tools learn about the internal operations of businesses through imitation learning, in which technical operations are observed in real time.

Virtual Process Analyst

The Virtual Process Analyst application is deployed on customers' end users' computers to record, upload, and analyze existing workflow processes. It uses AI to discover, document, and analyze an organization's business processes, producing process documentation. After observing operations, the Virtual Process Analyst assesses and analyzes the information to provide insight to customers. The resulting analysis allows customers to view a summary and/or details of the processes and make informed business decisions about how those processes are working.

Automation Anywhere's Process Discovery Cloud Services System uses imitation learning, few-shot detection, computer vision, natural language understanding, and replication learning to train its AI to adapt to each customer's environment, allowing integration and compatibility with legacy systems, custom applications, thin-or-thick clients, and green screens.

Principal Service Commitments and System Requirements

System Design

Automation Anywhere designs its systems to meet its regulatory and contractual commitments. These commitments are based on the services that AAI provides to its clients, the laws and regulations that govern the provision of those services, and the financial, operational, and compliance requirements that Automation Anywhere has established for its Services. Automation Anywhere establishes operational requirements in its system design that support the achievement of its regulatory and contractual commitments. These requirements are communicated in Automation Anywhere's information system policies, standards, and procedures, system design documentation, and contracts with clients.

Contractual Commitments

Automation Anywhere provides deployment, availability and organizational security controls employed in connection with the subscriptions for the Automation 360 Cloud and the Process Discovery Cloud. AAI employs standardized MSA which contains provisions for SLAs. Any alterations to the MSA are codified by AAI in-house legal department. All clients sign a non-disclosure agreement.

Service Delivery Process

The deployment model for Automation 360 Cloud involves customers building their bots and managing the bot deployments from the control room on Automation 360 Cloud. Once the bots are built, they are tested and run on the users' own compute infrastructure. Automation Anywhere's service commitment for Automation 360 Cloud is to maintain at least 99.9% monthly uptime on user browser access to the Automation 360 control room in a specified region.

Customers that purchase Automation Anywhere's Process Discovery Cloud Services are responsible for the installation of the Process Discovery Cloud Services agents/sensors in their environment.

Afterwards, AAI will provide access to AAI's online learning management (LMS) tool which provides training on Automation Anywhere's Automation 360 or the Process Discovery Cloud Services Systems product installation and use.

Components of the System

Infrastructure - A360

The in-scope system and supporting infrastructure is hosted by commercial Cloud Service Providers (CSP) AWS and GCP. As such, the CSP's are responsible for the physical infrastructure of the in-scope services.

AAI production environments are hosted is the following CSP regions:

AWS

us-west-2, us-west-1, ap-northeast-1, sa-east-1, me-south-1, eu-west-1, ap-southeast-1, ap-south-1, ap-southeast-2, us-east-1, af-south-1, us-gov-west-1.

GCP

us-central1, europe-west4, europe-west2, northamerica-northeast1, australia-southeast1.

AAI also utilities additional regions for its disaster recovery, and non-production environments (test, staging, and development).

Infrastructure - Process Discovery

Automation Anywhere's Process Discovery Cloud Services production environments are hosted in the following GCP regions:

- us-central1
- europe-west2
- northamerica-northeast1
- australia-southeast1

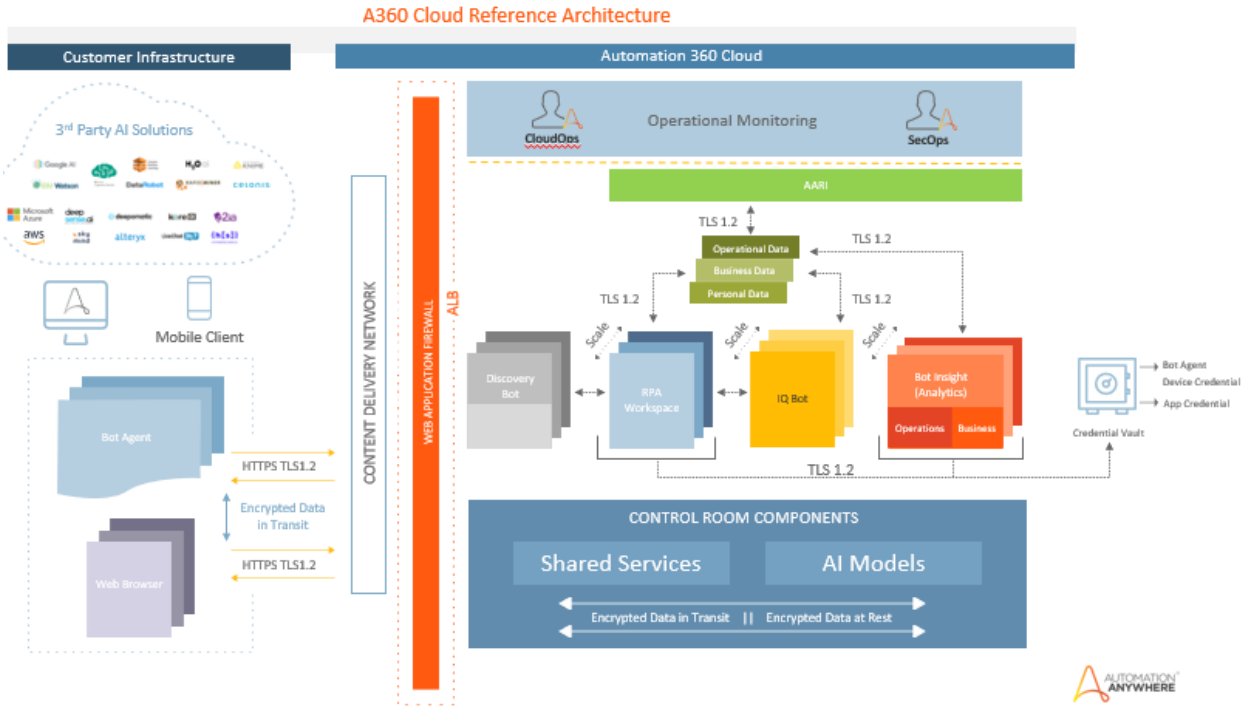
AAI also utilities additional regions for its disaster recovery, and non-production environments (test, staging, and development).

Network Architecture Diagrams

Automation Anywhere documents its network design for showing network inter- connectivity between its locations and the associated segmentation of various parts of network, including the perimeter security. To outline the topology of its network, the organization maintains and updates the network diagrams below to illustrate its internal infrastructure.

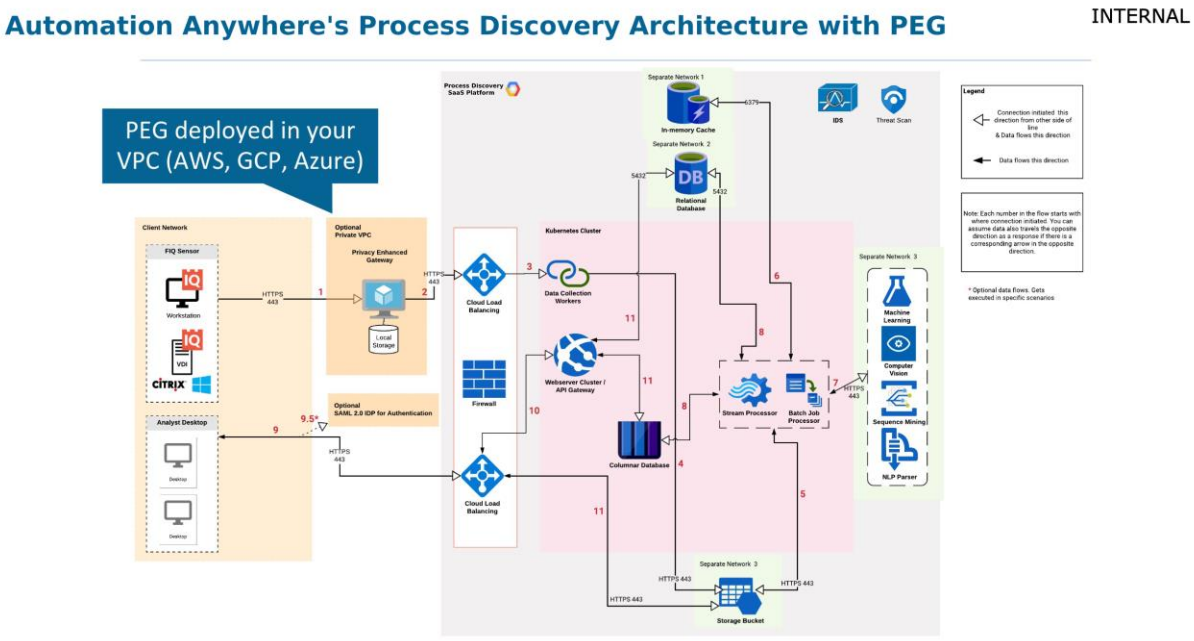
Automation 360 Cloud Network Architecture Diagram

Below is a network diagram depicting the network segmentation for a sample Cloud VPC. The public subnet segregates the services running in the internal subnet from direct connectivity from the internet using various types of technologies like firewalls, ACLs, security groups and whitelisting, depending on the type of CSP and the security requirements for that zone or service:



Process Discovery Cloud Network Architecture Diagram

Similarly, for the Process Discovery platform, the following network diagram for a sample GCP VPC demonstrates the necessary network segmentation. A redundant network is represented, with the highest zones of security identified as core, and a lower zone identified as Demilitarized Zone (DMZ). A separate segment is maintained for partner and private wide area network (WAN) interconnections.



Assets

System inventories are maintained through an asset management tool, and the entirety of the production environment is hosted on either Amazon Web Service (AWS) or Google Cloud Platform (GCP). The bulk of the servers are containers running in the Amazon Elastic Kubernetes Service (EKS) or Google Kubernetes Engine (GKE); these containers are ephemeral and can be replaced by a newer version of the container at a moment's notice. The system inventory includes virtual systems and a description of the function and use of each system. AAI cloud providers are responsible for the infrastructure for the in-scope services. AAI services do not have any subservice organizations.

Software

Primary software used to provide Automation Anywhere's A360 Cloud Services on AWS include the following:

Primary Software - Automation 360 Cloud on AWS		
Software	**Operating System**	**Purpose**
AWS	Not applicable (Cloud Service)	Public cloud provider provides services and infrastructure as a service (IaaS and PaaS)
AWS Account	Not applicable (Cloud Service)	Logical service subscription and isolation boundary
Cloud IAM	Not applicable (Cloud Service)	IAM service is used to provide access to cloud resources and services

Primary Software - Automation 360 Cloud on AWS		
Software	**Operating System**	**Purpose**
AWS - EKS - Elastic Kubernetes Service	Not applicable (Cloud Service)	Amazon Elastic Kubernetes Service (Amazon EKS) is a fully managed Kubernetes service
AWS - ECR - Elastic Container Registry	Not applicable (Cloud Service)	Amazon ECR is a managed AWS Docker registry service that is secure, scalable, and reliable. Amazon ECR supports private Docker repositories with resource-based permissions using AWS IAM so that specific users or Amazon EC2 instances can access repositories and images
AWS - RDS	Not applicable (Cloud Service)	Amazon Relational Database Service (Amazon RDS) makes it easy to set up, operate, and scale a relational database in the cloud
AWS - VPC	Not applicable (Cloud Service)	Amazon Virtual Private Cloud (Amazon VPC) lets you provision a logically isolated section of the AWS Cloud where you can launch AWS resources in a virtual network that you define
AWS - Internet Gateway	Not applicable (Cloud Service)	An internet gateway is a horizontally scaled, redundant, and highly available VPC component that allows communication between instances in your VPC and the internet. It therefore imposes no availability risks or bandwidth constraints on your network traffic
AWS - Network Address Translation (NAT) Gateway	Not applicable (Cloud Service)	NAT gateway enables instances in a private subnet to connect to the internet or other AWS services but prevent the internet from initiating a connection with those instances
AWS - EC2 - EKS Worker Nodes	Not applicable (Cloud Service)	Worker machines in Kubernetes are called nodes. Amazon EKS worker nodes run in your AWS account and connect to your cluster's control plane via the cluster Application Programming Interface (API) server endpoint
AWS - EC2 - Bastion Host	Linux Windows	A bastion host is a special-purpose computer designed to provide access to networked cloud resources
AWS - WAF	Not applicable (Cloud Service)	A WAF or Web Application Firewall helps protect web applications by filtering and monitoring HTTP traffic between a web application and the Internet. It typically protects web applications
AWS - EFS	Not applicable (Cloud Service)	Amazon Elastic File System (Amazon EFS) provides a simple, scalable, fully managed elastic NFS file system for use with AWS Cloud services
AWS - S3	Not applicable (Cloud Service)	Object storage services from AWS
Jenkins	Container Linux	Deployment automation tool a main component in CI/CD pipeline

Primary Software - Automation 360 Cloud on AWS		
Software	**Operating System**	**Purpose**
BitBucket	Not applicable (Cloud Service)	Bitbucket is Git repository management solution designed for professional teams
Confluence	Not applicable (Cloud Service)	Document and content management system. Design for enhanced collaboration
JIRA	Not applicable (Cloud Service)	Information Technology (IT) service management system
Lacework	Not applicable (Cloud Service)	Container security solution
AWS - Inspector	Not applicable (Cloud Service)	Vulnerability scanner
AWS - ALB/ELB	Not applicable (Cloud Service)	Load Balancer
AWS - GuardDuty	Not applicable (Cloud Service)	Threat and intrusion detection service
AWS - Route S3	Not applicable (Cloud Service)	DNS Service
AWS - Systems Manager	Not applicable (Cloud Service)	System Management Service
Amazon Secrets Manager	Not applicable (Cloud Service)	Secrets management service used to store Jira credentials for SecOp automation
Terraform	Not applicable (Cloud Service)	Terraform is a free tool from Hashicorp for building, changing, and versioning infrastructure safely and efficiently
HELM Charts	Not applicable (Cloud Service)	Helm chart is a tool for building and versioning containers
CloudFormation	Not applicable (Cloud Service)	Cloudformation is a tool for building, changing, and versioning infrastructure safely and efficiently
Amazon Certificate Manager (ACM)	Not applicable (Cloud Service)	ACM handles creating and managing public Secure Sockets Layer / Transport Layer Security (SSL/TLS) certificates for your AWS based websites and applications. You can use public certificates provided by ACM (ACM certificates) or certificates that you import into ACM. ACM certificates can secure multiple domain names and multiple names within a domain
Amazon ElasticSearch (EFK Stack)	Not applicable (Cloud Service)	Amazon Elasticsearch Service is a fully managed service that makes it easy for you to deploy, secure, and run Elasticsearch cost-effectively at scale
AWS CloudWatch	Not applicable (Cloud Service)	Observability of your AWS resources and applications on AWS and on-premises

Primary Software - Automation 360 Cloud on AWS		
Software	**Operating System**	**Purpose**
AWS Key Management Service (KMS)	Not applicable (Cloud Service)	AWS key management service is a secure and resilient service that uses hardware security modules that have been validated under FIPS 140-2
AWS Lambda	Not applicable (Cloud Service)	AWS Lambda lets you run code without provisioning or managing servers. You pay only for the compute time you consume
Palo Alto Virtual Private Network (VPN)	Not applicable (Cloud Service)	VPN Service
OKTA	Not applicable (Cloud Service)	Single Sign On (SSO)
Sumo Logic	Not applicable (Cloud Service)	Log management and SIEM service
Qualys	Not applicable (Cloud Service)	Vulnerability management service, infrastructure, and web application scanning
AWS Backup	Not applicable (Cloud Service)	Native backup service provided by AWS

Primary software used to provide Automation Anywhere's A360 Cloud Services on GCP include the following:

Primary Software - Automation 360 Cloud on GCP		
Software	**Operating System**	**Purpose**
Cloud Armor (WAF)	Not applicable (Cloud Service)	Web Application Firewall
Cloud DNS	Not applicable (Cloud Service)	GCP managed DNS Service
Cloud Key Management	Not applicable (Cloud Service)	Manages encryption keys on Google Cloud
Cloud NAT	Not applicable (Cloud Service)	Cloud NAT lets certain resources without external Internet Protocol (IP) addresses create outbound connections to the internet
Cloud Structured Query Language (SQL)	Not applicable (Cloud Service)	GCP managed SQL Database
Cloud Volumes	Not applicable (Cloud Service)	GCP managed native storage service
Digicert CA	Not applicable (Cloud Service)	Certificate Authority
ElasticSearch	Not applicable (Cloud Service)	Store, search and analyze data

Primary Software - Automation 360 Cloud on GCP		
Software	**Operating System**	**Purpose**
GCP - GKE Worker Nodes	Not applicable (Cloud Service)	Worker machines in Kubernetes are called nodes. GCP GKE worker nodes run in your GCP account and connect to your cluster's control plane via the cluster API server endpoint
GCP Compute - Bastion Host	Not applicable (Cloud Service)	A bastion host is a special-purpose computer designed to provide access to networked cloud resources
GCP projects	Not applicable (Cloud Service)	Logical service subscription and isolation
GCP Public Cloud	Not applicable (Cloud Service)	Public cloud provider provides services and infrastructure as a service (IaaS and PaaS)
Vertex AI	Not applicable (Cloud Service)	Fully managed GCP service to build, deploy, and scale machine learning (ML) models faster, with fully managed ML tools for any use case
Memorystore (Redis)	Not applicable (Cloud Service)	Scalable, secure and highly available cache memory service by GCP
GCR	Not applicable (Cloud Service)	Container Registry that Store, manage, and secure your build artifacts
GCS	Not applicable (Cloud Service)	Cloud Object Storage
GKE - Google Kubernetes Engine	Not applicable (Cloud Service)	Full automated and managed Kubernetes cluster service that put your containers on autopilot, eliminating the need to manage nodes or capacity and reducing cluster costs-with little to no cluster operations expertise required
Google Secrets Manager	Not applicable (Cloud Service)	Store API keys, passwords, certificates, and other sensitive data
Internet Routes	Not applicable (Cloud Service)	Google Cloud routes define the paths that network traffic takes from a virtual machine (VM) instance to other destinations. These destinations can be inside your Google Cloud Virtual Private Cloud (VPC) network (for example, in another VM) or outside it
Load balancer	Not applicable (Cloud Service)	Load Balancing service by GCP
VPC	Not applicable (Cloud Service)	Virtual Private Cloud (VPC) network that spans all regions and is a virtual version of a physical network
env0	Not applicable (Cloud Service)	env0 provides an automated, collaborative remote-run workflows management for cloud deployments on Terraform

Primary Software - Automation 360 Cloud on GCP		
Software	**Operating System**	**Purpose**
Ansible	Not applicable (Cloud Service)	Ansible is an open-source IT automation tool that automates provisioning, configuration management, application deployment, orchestration, and many other manual IT processes
Shoreline	Not applicable (Cloud Service)	Shoreline provides real-time automation and control for cloud operations
Cloud data transfer	Not applicable (Cloud Service)	Storage Transfer Service, Secure, low-cost services for transferring data from cloud or on-premises sources
Google Apigee API Management	Not applicable (Cloud Service)	Google Cloud's native API management tool to build, manage, and secure APIs-for any use case, environment, or scale

Primary software used to provide Automation Anywhere's Process Discovery Cloud Services include the following:

Primary Software - Process Discovery on GCP		
Software	**Operating System**	**Purpose**
Solr	Not applicable (Cloud Service)	Search Engine
Sidesiq	Not applicable (Cloud Service)	Redis based queue system
Cloud Stackdriver	Not applicable (Cloud Service)	Google's integrated monitoring, logging, and trace managed service for applications
Cloud Data Loss Prevention	Not applicable (Cloud Service)	Data Loss Prevention
Cloud IAM	Not applicable (Cloud Service)	Identity and Access Management System
Insight VM	Not applicable (Cloud Service)	Vulnerability management platform
Sysdig Cloud-Native Intelligence Platform	Not applicable (Cloud Service)	Cloud metrics platform
ESLint	Not applicable (Cloud Service)	Static code analysis tool
RuboCop	Not applicable (Cloud Service)	Static code analysis tool
Tensorflow GPU	Not applicable (Cloud Service)	Open-source software library for high performance numerical computation
Cloud Memoryshtore (Redis)	Not applicable (Cloud Service)	Memory data store service

Primary Software - Process Discovery on GCP		
Software	**Operating System**	**Purpose**
GitHub	Not applicable (Cloud Service)	Source code repository
GCP Cloud Armor	Not applicable (Cloud Service)	Web Application Firewall
GCP Cloud DNS	Not applicable (Cloud Service)	Domain Name System
GCP Cloud Key Management	Not applicable (Cloud Service)	Cloud hosted key management key systems
GCP Cloud NAT	Not applicable (Cloud Service)	NAT to isolate internal IP addresses from the Internet
GCP Cloud SQL - Postgres	Not applicable (Cloud Service)	Cloud database
GCP Cloud Volumes	Not applicable (Cloud Service)	Cloud file storage
GCP ElasticSearch	Not applicable (Cloud Service)	Distributed JSON-based search and analytics engine
GCP - GKE Worker Nodes	Not applicable (Cloud Service)	Worker machines in Kubernetes are called nodes. GCP GKE worker nodes run in your GCP account and connect to your cluster's control plane via the cluster API server endpoint
GCP Compute - Bastion Host	Linux	A bastion host is a special-purpose computer designed to provide access to networked cloud resources
GCP Projects	Not applicable (Cloud Service)	Logical service subscription and isolation boundary
GCP Google Container Registry (GCR)	Not applicable (Cloud Service)	Managed Docker Registry service
GCP Google (GCS)	Not applicable (Cloud Service)	Cloud object storage
GCP Google Kubernetes Engine (GKE)	Not applicable (Cloud Service)	Google managed Kubernetes service
GCP Google Secrets Manager	Not applicable (Cloud Service)	Secrets management service
GCP Internet Routes	Not applicable (Cloud Service)	Cloud network routing service
GCP Load balancer	Not applicable (Cloud Service)	Cloud Load Balancing
GCP Virtual Private Cloud (VPC)	Not applicable (Cloud Service)	Virtual Private Cloud (VPC)

Primary Software - Process Discovery on GCP		
Software	**Operating System**	**Purpose**
Lacework	Not applicable (Cloud Service)	Container security solution
Terraform	Not applicable	Infra as code
Jenkins	Container Linux	Deployment automation tool a main component in continuous integration/continuous delivery (CI/CD) pipeline
Ops Genie	Not applicable (Cloud Service)	IT service management system
Site 24x7 (status page)	Not applicable (Cloud Service)	Website monitoring service
HELM Charts	Not applicable	Helm chart is a tool for building and versioning containers
Sumo Logic	Not applicable (Cloud Service)	Infrastructure monitoring and Security incident & event management (SIEM) tool
DigiCert CA	Not applicable (Cloud Service)	https://www.digicert.com/tls-ssl/compare-certificates
Okta	Not applicable (Cloud Service)	Single Sign-On (SSO) and IAM

People

Automation Anywhere has a staff of approximately 2,600 employees with approximately 85 of those dedicated to the Automation Anywhere's Cloud service operations and security. Automation Anywhere staff is organized into the following key functional areas:

- Corporate: Executives, senior operations staff, and company administrative support staff, such as legal, compliance, internal audit, training, purchasing, accounting, finance, recruiting, and human resources (HR)
- Customer Success and Customer Support that provide technical assistance to Automation Anywhere's Cloud product users
- Engineering:
    - Development and quality assurance are responsible for the development (coding of enhancements), testing, and maintenance of Automation Anywhere's Cloud applications:
        - The staff receives recommendations for enhancements and issues from the customer support and customer success teams which are combined by Product into a roadmap. This team does not, by default, have access to the customer's Automation Anywhere's production system but an individual may be granted access by the customer to facilitate providing support or troubleshooting
        - The software development staff develops and maintains the custom software. The staff includes software developers, database administration, software quality assurance, and technical writers
    - Data Science Engineering analyzes data sets for patterns and are responsible for training software

    - Cloud Operations administers and builds the Automation Anywhere's Cloud architecture and Service using infrastructure as code to support an automated build process within the respective CSP to deliver a consistent and secure infrastructure. They provide direct day-to-day services such as maintaining and upgrading systems, quality assurance monitoring, network support, and reporting. It also performs systems administration duties to deploy Automation Anywhere's newest SaaS application releases into production cloud
    - Cloud Security Engineering team oversees the security of all production accounts and applications. It is responsible for design and testing of cloud security architecture, infrastructure vulnerability management, monitoring and reacting to 0-day threats and advisories, identification and tracking of cloud configuration violations and administration of third-party and/or native cloud security tools
    - Cloud Security Operations Center: They are responsible for configuring and tuning of detection and prevention rules, building SIEM content, threat rules, proactively searching and hunting for threats, monitoring and triaging of alerts and events 24x7, ensuring all security incidents ate investigated, contained and recovered from, in a timely manner. They manage the security incidents reported by the customer or customer success team, investigate the reported incidents, and work with the various Automation Anywhere teams to drive resolution. Resolution of the reported incident can include changes to Automation Anywhere's application, its stack, the CSP infrastructure, or implementation of additional security controls
    - The Cloud Risk & Compliance team monitors Automation Anywhere's policies and standards for effective security practices that comply with multiple standards including ISO 27001, CSA-CCM, SOC2, HITRUST, PCI, HIPAA etc.
- IT: Provides the corporate Information Technology services that are used throughout Automation Anywhere including by the teams responsible for Automation Anywhere's Cloud Services:
    - Help desk, IT infrastructure, IT networking, IT system administration, information security, and IT operations

Data

The Automation 360 Cloud is a hosted Automation Anywhere service delivery platform upon which Automation 360 based services are offered. The Automation 360 Cloud comprises integrated Control Room and bot creation capabilities hosted on the Automation 360 Cloud with the ability to run cloud connected bot runner nodes located on the customer infrastructure. In addition, the following products are applications running on the Automation 360 Cloud - Bot Insight, and Automation Co-Pilot.

Bot Insight - Easy access to insights about your intelligent automation program in a single, friendly, interactive visual dashboard. Share insights directly from the dashboard to increase visibility and organizational buy-in. Manipulate data with flexibility in Microsoft Power BI, Tableau, or any analytics of your choice via native connectors or APIs.

Automation Co-Pilot - Automation Anywhere's RPA integrated Digital Assistant that is used by individuals to automate routine tasks and to provide information from multiple backend systems within the consolidated Co-Pilot interface.

<u>Data Collection</u>

The deployment model for Automation 360 Cloud involves customers building their bots and managing the bot deployments from the Control Room located on the Automation 360 Cloud. Once the bots are built, they are tested and run on the customers own compute infrastructure. By default, the data involved in the actual automation does not enter the Automation 360 Cloud unless specific automation functionality is used. This default configuration significantly reduces the data collected by and stored within Automation 360 Cloud.

When users use various products including Document Automation, Bot Insight, and Automation Co-Pilot additional data can be stored on the Automation 360 Cloud. This can also happen when features such as Recorder, AISense and WLM are used.

These AAI products can store customer data as part of a customer defined automation, albeit typically temporarily during the automation process defined by the customer. For example, IQ Bot use typically involves uploading images for processing. Recorder and AISense store recorded screenshots (note Secure Recording can be enabled by administrators to ensure these are not stored). Automation Co-Pilot stores data processed by attended forms. Bot Insight can be used to create dashboards made from tagged business data being processed by a bot.

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 documents using Document Automation.

The customer has control over what business data is stored on the Automation 360 Cloud. Note that the source data remains with the customer and the customer is in control of deleting the data on the Automation 360 Cloud. The customer has the principal copy of the data in their systems.

Note this business data may contain personal information related to a customer's business.

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, e-mail addresses, job titles, and contact information contained in invoices or e-mails.

The deployment model involves customers building their boots 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	E-mail, First and Last name, preferred name, time zone, last login, password, questions set, AD-domain
User password	Personal	User password
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

Data Item	Data Category	Description
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, e-mail 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 & Database Change Logs
Errors logs	Personal	May contain identifiers
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 or Document Automation for extraction and processing For IQ Bot or Document Automation: uploaded documents and extraction results
Intelligent Document Processing Data	Operational	For IQ Bot or Document Automation: 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 Automation Co-Pilot: Automation Co-Pilot Web Workflow Definition: Describing how a process executes (including but not limited to bot, forms, and other steps required to execute the process) Automation Co-Pilot Web Dataflow: Store's data incidentally generated by executing the process (including all inputs and outputs from the various process steps)
Other Data	Business / Personal	For Automation Co-Pilot: Automation Co-Pilot Web Team Definitions: Describing team membership, and process access rules Automation Co-Pilot Web File Storage: Stores files uploaded as a part of the request's dataflow

The Automation Anywhere's Process Discovery Cloud agent running on customers' workstations captures the screen of whitelisted applications as defined by the customer organization. Any sensitive data displayed on the screen of those whitelisted applications is captured and processed by Automation Anywhere's Process Discovery Cloud. All data sent to the organization from customer sites is sensitive because it is data from inside customer internal networks. The varieties of data contained in the customer data varies based upon the type of business the customer conducts and the job function of the personnel who use the computer being monitored. Data can be restricted using whitelist process and blacklist process, and also via masking software. Automation Anywhere's Process Discovery Cloud requests that customers do not send PII, such as card data.

Automation Anywhere's Process Discovery Cloud complies with numerous standards regarding data collected and storage. These include GDPR, CCPA, HIPAA, PCI, and the US ECPA, among others. The organization has provisions in policies for legal holds as requested by customers or law enforcement. All of the organization's customers require data retention to be considered in agreements and as part of due diligence. A Data Classification Policy is documented to ensure data is protected from unauthorized disclosure, use or modification, and deletion. All customer data is stored in the cloud with restricted access.

Encryption key management is governed by the Encryption and Key Management Policy. All encryption within the cardholder data environment (CDE) is either managed by Google in the applications it manages or by Google Cloud Key Management System (KMS) for encryption managed by the organization within the Google environment. Keys are required to be accessed, generated, and distributed in a secure manner, and there are minimum length requirements for generating keys. Split knowledge is required, and keys should only be accessed by approved custodians. The Application Implementation Team is the only personnel with access to the encryption keys.

Sensitive data is secured any time it must be transmitted or received via open, public networks. The agent transmitting any sensitive data that may be captured does so over at least a TLS 1.2 encrypted channel, using a proprietary API with the customer ID encoded into the data packet to direct which table to store the data into in the database. The TLS protocol provides mitigation against unauthorized alteration, unauthorized disclosure, and replay. Encryption policies and processes are based on guidance provided by the National Institute of Standards and Technology (NIST).

Processes, Policies and Procedures

Formal IT policies and standards exist that describe physical security, logical access, computer operations, change control, and data communication requirements. All teams are expected to adhere to the Automation Anywhere policies, and standards that define how services should be delivered. These are located on the Company's intranet and can be accessed by any Automation Anywhere team member.

Physical Security

The in-scope system and supporting infrastructure are hosted by cloud service providers (CSP) AWS and GCP. As such, the CSP's are responsible for the physical security controls for the in-scope systems. Refer to the 'Subservice Organizations' table below for controls managed by AWS and GCP.

Automation Anywhere Facility Security

Physical access to Automation Anywhere facilities is protected. All exterior ingress doors are restricted to users possessing an access card/Identification Document (ID) that has been assigned access to use the door. The access card/ID system uses zones to control access. Each exterior door and doors to restricted areas within the facilities are assigned to door zones. Access to zones is restricted through the use of access control lists. Employees and vendors granted access cards are assigned to roles based on their job responsibilities.

Visitors check in with the receptionist or security guard stationed in the reception area. Visitors must present a valid, government-issued photo ID. The visitor's name and purpose for the visit are recorded in a visitor log and his or her visit must be escorted by an Automation Anywhere employee who is authorized to sign nonemployees into the facility.

Upon an employee's termination of employment, the HR system automatically generates an access deletion record in the event management system on the last day of employment. This record is routed to the access administrators for deletion. In addition, terminated employees turn over their access cards/IDs during their exit interview.

Access listings are generated by security and distributed to the zone owners via the event management system. Zone owners review the listings and indicate the required changes in the event management record.

Logical Access

Automation Anywhere uses a role-based security architecture and requires support users of the system to be identified and authenticated prior to accessing any CSP hosted system resources. Resources are protected through the use of native system security and add-on single sign on software products that identify and authenticate users and validate access requests against the users' authorized roles in access control lists.

All resources are managed in the asset inventory system and each asset is assigned an owner by their role. Owners are responsible for approving access to the resource and for performing quarterly reviews of access by role.

Passwords must conform to defined password standards and are enforced through parameter settings in the Automation Anywhere SSO. These settings are part of the configuration standards and force users to change passwords at a defined interval, have complex passwords, and support account lockout for failed login attempts.

Upon hire, Automation Anywhere employees are assigned to a position in the HR management system. One week prior to the employees' start date, the HR management system creates a report of employee user IDs to be created and default system access that is to be granted. The report is then used by the IT help desk to create user IDs and associated application access based upon pre-defined rules. Access rules have been pre-defined based on defined user roles. The system generated list includes employees with position changes and the associated roles to be changed within the access rules.

On a quarterly basis, logical access rules for each role with access to the CSP are reviewed by the respective team leadership and the results are documented within the respective ticket tracking system. In evaluating role access, respective team leaders consider job duties requiring segregation, risks associated with access, and validating that all access changes (addition, change, deletion) are properly documented. Completed rules are reviewed and approved by the Chief Technology Officer (CTO) organization. As part of this process, the CTO organization reviews access by privileged roles and requests modifications based on this review. Physical and VPN access reviews are conducted at least quarterly.

The HR system generates a request for terminated employees when a termination event occurs. This event is used by the IT help desk to delete employee access through the use of a bot that runs on a daily basis. On an annual basis, HR runs a list of active employees. The IT help desk uses this list to suspend user IDs and delete all access roles from IDs belonging to terminated employees.

Customer users access Automation 360 Cloud and Process Discovery Cloud services through the Internet using TLS functionality of their web-browser to ensure that the information is encrypted while transmitted over the Internet. They must supply a valid user ID and password to gain access to their hosted cloud tenant resources.

Computer Operations - Backups

Customer data is backed up and monitored by Automation Cloud Operations (CloudOps) personnel for completion and exceptions. In the event of an exception, CloudOps personnel perform troubleshooting to identify the root cause and then rerun the backup job immediately or as part of the next scheduled backup job depending on customer indicated preference within the documented work instructions.

CSP native services are used for creating backups.

This section explains where all of the cloud service data resides as well as where it is backed up. This information is used to locate and restore data in the event of a disaster:

Data	Cloud Service	Data Type	Backup Frequency	Backup Location
MSSQL Database	AWS RDS	SQL database for application	Every 4 hours	AWS RDS to another region
ElasticSearch (ES)	AWS ES	Audit and server logs	Every 4 hours	AWS S3 to another region
Filesystem	AWS Encrypting File System (EFS)	Control room system files	Every 4 hours	AWS EFS to another region
MSSQL Database	GCP SQL	SQL database for application	Every 4 hours	GCP SQL to another region
Balanced Persistent Disk	GCP Storage	Control room system files	Every 4 hours	GCP Storage to another region
Standard Storage	GCP Storage	Audit and server logs	Every 4 hours	GCP Storage to another region

Business Continuity Program

The Business Continuity Program for the Automation Anywhere's Process Discovery Cloud product consists of a program based on cloud-based platforms as a service technologies and containerized deployments to ensure operational resiliency. A Business Continuity Policy and Plan is documented and includes formal strategies that are communicated within the Business Continuity Policy. Tests of the Business Continuity Program are performed at least on an annual basis. Lessons learned and improvements are documented and applied.

Computer Operations - Availability

Incident response policies and procedures are in place to guide personnel in reporting and responding to incidents.

Automation Anywhere monitors the capacity utilization of all Automation 360 Cloud and Process Discovery components within the company's hosted computing infrastructure and customer application load to ensure that service delivery matches or exceeds SLAs.

Automation Anywhere evaluates the need for additional infrastructure capacity in response to growth of existing customers and/or the addition of new customers. Infrastructure capacity monitoring includes, but is not limited to, the following infrastructure:

- Compute
- Memory
- Storage
- Network bandwidth

Vulnerability Management

The primary purpose of the vulnerability management is to ensure that all identified vulnerabilities in the AAI managed Cloud Service environment at the application (AAI Custom Code and Open-Source Software), container operating system (Docker & Kubernetes), host operating system and network & Internet layer will be protected from exposure and exploitation by attackers.

For ease of implementation, the vulnerability management operating procedures are divided into the following key phases:

- Preparation & Discovery Phase
- Scanning & Prioritization Phase
- Remediation Phase
- Validation and Closure Phase

Patch Management

The goal of Patch Management is to keep the components that form of the IT infrastructure (hardware, software, and services) up to date with the latest fixes and functionality through updates. Patch management is an important part of keeping the components of the IT infrastructure available to the end user.

For ease of implementation, the operating procedures are divided into the following key areas:

- Information systems and equipment to be patched
- Obtaining patch/update information
- Identification and testing of required patches/updates
- Deployment of patches/updates
- Rollback of patches/updates if required

Change Control

Automation Anywhere maintains an SDLC that the development and test team have to follow:

Every release goes through various gates before going into production. Essentially the release goes from Development to Quality Assurance (QA) to Stage to Production with checks / tests at every stage before it gets promoted. Customer data is not used for any non-production environment - test data generated by the QA team is used to simulate tenant data in all environments outside of production.

A ticketing system is utilized to ensure adherence to the change control procedures for changes in the application and implementation of new changes. QA testing and User Acceptance Testing (UAT) results are documented and maintained with the associated change request. Development and testing are performed in an environment that is logically separated from the production environment using test data. Management approves changes prior to migration to the production environment and documents those approvals within the ticketing system.

Version control software is utilized to maintain source code versions and migrate source code through the development process to the production environment. The version control software maintains a history of code changes to support rollback capabilities and tracks changes made to individual developers.

Penetration Testing

Penetration testing is conducted to measure the security posture of a target system or environment. The third-party vendor uses an accepted industry standard penetration testing methodology specified by Automation Anywhere. The third-party vendor's approach begins with a vulnerability analysis of the target system to determine what vulnerabilities exist on the system that can potentially be exploited via the penetration test, simulating a disgruntled or disaffected insider or an attacker that has obtained internal access to the network. Once vulnerabilities are identified, the third-party vendor attempts to exploit the vulnerabilities to determine whether unauthorized access or other malicious activity is possible. Penetration testing includes network and application layer testing as well as testing of controls and processes around the networks and applications and occurs from both outside (external testing) and inside the network.

Vulnerability scanning is performed by the Security Team at least monthly by using vulnerability scanning tools i.e., Veracode, Black Duck, Snyk and Wiz, or CSP provided tools as per Automation Anywhere policy. SecOps uses industry standard scanning technologies and a formal methodology specified by Automation Anywhere. These technologies are customized to test the organization's infrastructure and software in an efficient manner while minimizing the potential risks associated with active scanning. Retests and on-demand scans are performed on an as-needed basis. Scans are performed during non-peak windows. Scanning is performed with approved scanning templates and with bandwidth-throttling options enabled. Tools requiring installation in the Automation Anywhere system are implemented through the Change Management process.

Authorized employees may access the system from the Internet using leading VPN technology. Employees are authenticated using a token-based multi-factor authentication (MFA) system.

Boundaries of the System

The scope of this report includes the Automation 360 Cloud and Process Discovery Cloud Services System. Automation Anywhere's corporate headquarters is located in San Jose, California USA with additional offices in Bengaluru and Vadodara, India.

Automation 360 Cloud is hosted by AWS and GCP and Process Discovery Cloud is hosted by GCP. The scope of this report does not include the cloud hosting services provided by AWS or GCP at their facilities.

Changes to the System in the Last 12 Months

No significant system changes have occurred to the services provided to user entities in the 12 months preceding the end of the review period.

Incidents in the Last 12 Months

No significant security incidents have occurred to the services provided to user entities in the 12 months preceding the end of the review period.

Criteria Not Applicable to the System

All Common / Security, Availability, and Confidentiality criteria were applicable to the Automation 360 Cloud and Process Discovery Cloud Services System.

Subservice Organizations

This report does not include the cloud hosting services provided by AWS or GCP at multiple facilities around the world.

Subservice Description of Services

AWS provides cloud hosting services for Automation Anywhere's Automation 360 Cloud Services, including AWS EC2, AWS RDS, AWS IAM and other monitoring systems.

GCP provides cloud hosting services for Automation Anywhere's Process Discovery Cloud, including Kubernetes, Cloud SQL, Cloud IAM and other monitoring systems.

Complementary Subservice Organization Controls

Automation Anywhere's services are designed with the assumption that certain controls will be implemented by subservice organizations. Such controls are called complementary subservice organization controls. It is not feasible for all of the trust services criteria related to Automation Anywhere's services to be solely achieved by Automation Anywhere control procedures. Accordingly, subservice organizations, in conjunction with the services, should establish their own internal controls or procedures to complement those of Automation Anywhere.

The following subservice organization controls are implemented by AWS and GCP to provide additional assurance that the trust services criteria described within this report are met:

Subservice Organization - AWS		
Category	**Criteria**	**Control**
Common Criteria / Security	CC6.4	Physical access to data centers is approved by an authorized individual.
		Physical access is revoked within 24 hours of the employee or vendor record being deactivated.
		Physical access to data centers is reviewed on a quarterly basis by appropriate personnel.
		Physical access points to server locations are recorded by closed circuit television camera (CCTV). Images are retained for 90 days, unless limited by legal or contractual obligations.
		Physical access points to server locations are managed by electronic access control devices.
		Electronic Intrusion Detection Systems (IDSs) are installed within data server locations to monitor, detect, and automatically alert appropriate personnel of security incidents.
Availability	A1.2	Uninterruptible Power Supply (UPS) units provide backup power in the event of an electrical failure in CSP-owned data centers.
		CSP-owned data centers are protected by fire detection and suppression systems.
		CSP-owned data centers are air conditioned to maintain appropriate atmospheric conditions. Personnel and systems monitor and control air temperature and humidity at appropriate levels.
		CSP-owned data centers have generators to provide backup power in case of electrical failure.

Subservice Organization - AWS		
Category	**Criteria**	**Control**
		Contracts are in place with third-party colocation service providers which include provisions to provide fire suppression systems, air conditioning to maintain appropriate atmospheric conditions, Uninterruptible Power Supply (UPS) units, and redundant power supplies.

Subservice Organization - GCP		
Category	**Criteria**	**Control**
Common Criteria / Security	CC6.1, CC6.3	Deviations from pre-defined operating system (OS) configurations running on production machines are detected and corrected.
		The organization has established guidelines for governing the installation of software on organization-owned assets.
		Access to corporate network, production machines, network devices, and support tools requires a unique ID, password, and/or machine certificate.
	CC6.4, CC7.2	Data center server floors network rooms and security systems are physically isolated from public spaces and/or delivery areas.
		Access to sensitive data center zones requires approval form authorized personnel and is controlled via badge access readers, biometric identification mechanism, and/or physical locks.
		Data center perimeters are defined and secured via physical barriers.
		Access lists to high security areas in data centers are reviewed on a periodic basis and inappropriate access is removed in a timely manner.
		Visitors to data center facilities must gain approval from authorized personnel, have their identity verified at the perimeter, and remain with an escort for the duration of the visit.
		Security measures utilized in data centers are assessed annually and the results are reviewed by executive management.
		Data centers are continuously staffed and monitored by security personnel through the use of real time video surveillance and/or alerts generated by security systems.
	CC8.1	The organization has developed policies and procedures governing the secure development lifecycle.
		A standard image is utilized for the installation and maintenance of each production server.
		Operating system changes are reviewed and approved by a separate technical resource before moving into production.
		Changes to the organization's systems are tested before being deployed.

Subservice Organization - GCP		
Category	**Criteria**	**Control**
		The organization uses a version control system, to manage source code, documentation, release labeling, and other functions. Access to the system must be approved.

Automation Anywhere management, along with the subservice organization, define the scope and responsibility of the controls necessary to meet all the relevant trust services criteria through written contracts, such as SLAs. In addition, Automation Anywhere performs monitoring of the subservice organization controls, including the following procedures:

- Reviewing attestation reports over services provided by vendors and subservice organization
- Monitoring external communications, such as customer complaints relevant to the services by the subservice organization

COMPLEMENTARY USER ENTITY CONTROLS

Automation Anywhere's services are designed with the assumption that certain controls will be implemented by user entities. Such controls are called complementary user entity controls. It is not feasible for all Trust Services Criteria related to Automation Anywhere's services to be solely achieved by Automation Anywhere control procedures. Accordingly, user entities, in conjunction with the services, should establish their own internal controls or procedures to complement those of Automation Anywhere's.

The following complementary user entity controls should be implemented by user entities to provide additional assurance that the Trust Services Criteria described within this report are met. As these items represent only a part of the control considerations that might be pertinent at the user entities' locations, user entities' auditors should exercise judgment in selecting and reviewing these complementary user entity controls.

1. User entities are responsible for understanding and complying with their contractual obligations to Automation Anywhere.
2. User entities are responsible for notifying Automation Anywhere of changes made to technical or administrative contact information.
3. User entities are responsible for maintaining their own systems of record.
4. User entities are responsible for ensuring the supervision, management, and control of the use of Automation Anywhere services by their personnel.
5. User entities are responsible for developing their own disaster recovery and business continuity plans that address the inability to access or utilize Automation Anywhere services.
6. User entities are responsible for providing Automation Anywhere with a list of approvers for security and system configuration changes for data transmission.
7. User entities are responsible for immediately notifying Automation Anywhere of any actual or suspected information security breaches, including compromised user accounts, including those used for integrations and secure file transfers.
8. User entities are responsible for provisioning and de-provisioning access to their environments.
9. User entities are responsible for installing the free Privacy Enhanced Gateway in their environment, configuring that gateway, and monitoring the gateway to ensure it continues to meet their requirements.