



Security Overview

UiPath Platform

December 2025

Contents

1. Introduction	4
2. Flexible deployment options.....	5
3. UiPath Trust Culture	8
Security Framework.....	8
UiPath Security Management Team	11
HR Security	11
Risk management	12
Vendor Risk Management.....	12
External - Internal Audit.....	12
Secure Software Development Life Cycle (SDLC)	13
4. Security Responsibilities	14
Data Management Roles and Responsibilities	14
Shared Responsibility Model	15
5. Infrastructure Security	16
Service-Design Principles and Architecture.....	16
On-premises models.....	16
Cloud models	19
Data Flows.....	22
Physical Security	25
Network Security	25
6. Operational Security	27
Release Cycle and Security Updates	27
Vulnerability Management and Penetration Testing	29
Common Vulnerability Mitigations in Automation Suite	31
Production Environment Access Controls	32
Availability and Disaster Recovery	32
Backup and Restoration	34
Operational Monitoring	34
Incident Management.....	35

7. Application Security	38
User Authentication	38
Login Consent Configuration	39
Authorization and Centralized Access Management.....	39
Credential Stores	40
Logs	41
Encryption.....	41
API Security	43
8. AI Features and Integrations in UiPath.....	45
Securing AI Integrations in UiPath	47
Agentic Security	49
9. Data Governance and Privacy	53
Data Residency.....	53
Data Isolation	54
Data Retention and Destruction.....	55
Data Classification	55
Telemetry Data Collection.....	56
10. Compliance	58
11. Third Party Security Integrations.....	60
12. Conclusion	61
13. Appendices	63
Appendix 1: UiPath Robots — Guidance for Handling Multi-Factor Authentication.....	63
Appendix 2: UiPath Automation Cloud — Security Configuration Guide	66
Appendix 3: UiPath Automation Suite — Security Configuration Guide	69

1. Introduction

Embracing cutting-edge AI-powered automation, fueled by robotic process automation (RPA), Agents, Generative AI and allied technologies such as machine learning and natural language processing, become pivotal in propelling successful business transformation. UiPath products deliver enterprise-wide agentic automation benefits, residing in an open, extensible architecture designed for truly smart, highly scalable automation. The UiPath Platform offers everything you need to automate end-to-end — from discovering the best automation opportunities to measuring ROI, building, deploying, and executing robotic workflows and agents — and everything in between, all within a centrally managed, fully governed, secure platform that continues to scale.



The UiPath Platform, an AI-powered, holistic, and seamlessly integrated solution, not only meets but surpasses the prerequisites of the automation lifecycle at enterprise scale. From inception and development to seamless deployment and governance, the comprehensive UiPath Platform empowers organizations to harness automation’s true potential.

The security of all data associated with your automation projects is of the utmost importance to UiPath, whether you choose SaaS deployment or alternative options such as on-premises installation or deployment to a 3rd party cloud. In this white paper, we focus on the various security capabilities in the platform along with security, privacy, and compliance practices followed by UiPath.

2. Flexible deployment options

UiPath follows the principle of cloud-first customer choice, enabling customers to deploy the platform based on their policies and preferences. UiPath offers different deployment models, which present distinct approaches - each model catering to different organizational needs and preferences. These deployment options can be categorized as:

1. **Self-Hosted Options:** UiPath Automation Suite and Standalone deployment of UiPath products are self-hosted options, supporting installation on customer premises or on customer cloud.
2. **Software-as-a-service (SaaS) Option:** UiPath Automation Cloud and UiPath Automation Cloud Public Sector are the SaaS deployment models hosted by UiPath.

	Software-as-a-Service (SaaS)			Self-Hosted Options	
	Automation Cloud	Automation Cloud Public Sector	Automation Cloud Dedicated	Automation Suite	Standalone Products
Description	In this model, the cloud native UiPath Platform is delivered as SaaS from UiPath. Within this model, no server-side installation is required. Customers can start using the solution instantly and scale infinitely.	This is a cloud-based enterprise SaaS solution tailored to the specific requirements of public sector organizations in the United States.	This is a cloud-based enterprise SaaS solution tailored to the specific requirements of large organizations that need dedicated resources while leveraging the best of SaaS releases.	In this model, the cloud native UiPath Platform is delivered as a single, containerized suite. Automation Suite supports deployment of the full UiPath Platform in the environment of customer choice, including bare-metal machines, on-premises Virtual Machine infrastructure, or cloud subscriptions to any of the major providers. Additionally, it enables you to deploy the complete platform on containerized platforms such as AKS or EKS, as well as on OpenShift - Red Hat's container orchestration platform.	In this model, UiPath Platform products are individually installed and managed in the customer environment, either on customer premises, or on a customer cloud.

Product Deployment/ Installation	Products are pre-deployed to the cloud with full governance.	Products are pre-deployed to the cloud with full governance.	Products are pre-deployed to the cloud with full governance.	Single installation file for the entire Suite with on-premises, public or private cloud deployment options. Customers can install this on-premises, Linux VM, EKS/AKS, or public cloud.	Individual installation files are available per product and each product has its own hardware and software requirements. Can be installed on the client's cloud or data centers.
---	--	--	--	---	--

Characteristics	<p>Fastest time to value, the lowest cost of ownership, and the best ROI for most UiPath customers. This is especially true in the earliest phases of the ownership cycle, where installation costs and timeframes are minimized. Ongoing management needs and costs tend to be lower over time, and new capabilities are available sooner due to frequent updates with fewer integration and installation considerations. For these reasons, we recommend Automation Cloud as the deployment choice wherever possible.</p>	<p>This model is specifically for U.S. federal customers. UiPath Automation Cloud for Public Sector holds FedRAMP Moderate compliance, confirming our adherence to the rigorous security controls mandated by the Federal Risk and Authorization Management Program.</p>	<p>As a single-tenant SaaS solution, it provides infrastructure-level isolation of your environment with flexibility on upgrades</p>	<p>This option is available for organizations who want an “Automation Cloud-like” full-platform experience but who have compelling reasons to avoid the SaaS model. As a completely self-hosted enterprise platform, Automation Suite is essentially “Automation Cloud in a box.” It is designed for organizations that choose not to adopt a SaaS-based automation strategy. Automation Suite delivers many of the integration and platform benefits of Automation Cloud, while offering complete control of the entire environment, including the infrastructure itself.</p>	<p>This option allows customers to choose where to deploy and manage each product available in this deployment option. However, note that in this option, there is limited cross-product integration and involves per-product management at the infrastructure and software level.</p>
------------------------	---	--	--	--	--

For more information on product details across deployment options and for a detailed comparison, please refer to: <https://docs.uipath.com/overview/other/latest/overview/product-availability>

3. UiPath Trust Culture

Security Framework

UiPath has implemented an information security management system (ISMS) in accordance with ISO/IEC 27001 and aligned to meet the control implementation guidance and additional control sets of ISO/IEC 27017 and ISO/IEC 27018, which requires various security-related policies and documentation, including procedures. Our ISMS is audited by an accredited ISO certification body annually for conformity with the international standard.

UiPath has ISO/IEC 27001, ISO 9001, ISO/IEC 42001, IRAP, HITRUST and Cyber Essentials Plus certifications, SOC 1®, SOC® 2 and HIPAA attestations. For the latest information, please refer to: <https://www.uipath.com/legal/trust-and-security/security>. Trust.uipath.com.

Also, refer here for the Information Security Exhibit summarizing UiPath policies: <https://www.uipath.com/assets/downloads/information-security-exhibit>

List of Global Security Policies

Cyber Security Policy

UiPath has a Global Cyber Security Policy that defines the cyber security procedures and measures implemented by UiPath and its subsidiaries. This policy is designed to protect the confidentiality, integrity, and availability of the company's information assets in accordance with business objectives and applicable laws and regulations. The policy is approved by UiPath management, published, and communicated to all users, including employees, contractors, freelancers, vendors, and collaborators. It is subject to continuous monitoring and regular improvement and is reviewed annually and modified if significant changes occur. All data stored and processed by UiPath is handled according to an appropriate level of confidentiality and in compliance with relevant regulatory and contractual requirements. Cyber security roles and responsibilities are defined and communicated. The policy covers aspects such as Risk Management, Access Control, Asset Management, Data Handling, Mobile Devices and Teleworking, Human Resources Security, Cryptographic Controls, Third Party Vendor Risk Management, Physical Security, Incident Management, Business Continuity, and Awareness and training of employees.

Acceptable Use Policy

UiPath has an Acceptable Use Policy that has been approved by management and communicated to all relevant parties. It requires all employees, contractors, and third parties to respect a set of security measures when handling UiPath devices and information. The policy is maintained and periodically reviewed by an assigned owner. It is also included in employment agreements, which all employees are required to sign as part of accepting an offer at UiPath. The policy extends to the use of mobile devices and IT infrastructure network and systems components, with specific policies and procedures in place to define allowances and conditions for their usage.

Access Control Policy

UiPath has an Access Control Policy that is approved by the management and reviewed annually. This policy adheres to the principles of least privilege, need-to-know basis access, and segregation of duties. Users are only granted access to business resources that they have been specifically authorized to use in accordance with defined access control policies and processes. Access rights of all users to information are granted as appropriate for conducting their duties and removed upon resignation or termination of employment, contract or agreement, or adjusted upon a change in role. The policy is based on the ISO 27001 framework. UiPath uses Role-Based Access Control applying Zero-Trust model enforced by Top Management according to Security Policies and Procedures, HR and Local Laws.

Bring Your Own Device Policy

UiPath has a Bring Your Own Device (BYOD) policy that defines the devices and eligibility requirements for BYOD usage. This policy applies to all mobile devices owned by employees, contractors, freelancers, or any third-party representative of UiPath that have access to the corporate environment, including business information. The policy also specifies the user roles that are allowed access via a BYOD-enabled device and clarifies the systems and servers allowed for use or access on the BYOD-enabled device. In case a wipe of the device is required, the policy clearly states the expectations over the loss of non-company data.

Cryptographic Controls Policy

Our Cryptographic Controls Policy governs the procedures where encryption and cryptographic techniques are employed. In the context of UiPath Automation Cloud, users can choose who owns and manages the key used to encrypt data: UiPath or the user themselves. UiPath supports both UiPath managed keys as well as customer-managed keys. With UiPath managed keys, UiPath has internal procedures for key lifecycle management and monitoring. If a customer chooses to use a customer-managed key, then the responsibility for managing the Key Encryption Key (KEK) is with the customer. For data in transit, communication between external systems and UiPath Automation Cloud is encrypted with ECDSA_P256 encryption with a SHA256ECDSA signature, a 6-month rotation, and accepting TLS 1.2 and TLS 1.3. Communications between services in the cloud platform are RSA 2048 encryption with a SHA256RSA signature, a 90-day rotation, and accepting only TLS 1.2.

Data Retention Policy

UiPath has an internal data retention policy in accordance with the ISO/IEC 27001 standards. Personal Information is retained for no longer than necessary or required by law. UiPath follows Data Retention Policies and Procedures in line with ISO/IEC 27001 documentation, including subcontractors as part of the process. Scoped data is included in a regular data retention review. UiPath uses an internal Information Classification policy to manage all data stored by way of the Automation Cloud platform, providing guidelines on handling of different categories of data, including the procedures to store, process and retain such data, access control requirements of such data, encryption and other security requirements.

Disposal and Destruction Policy

UiPath has an internal Disposal and Destruction policy that governs the secure disposal and destruction of data, technology equipment, and components owned by the company. UiPath leverages sub-processor agreements for cloud services that manage the data centers. Therefore, UiPath can only provide software deletion and, if requested, a certificate of destruction. Note: Data and infrastructure within the customer environment are customer responsibility.

Enterprise Change Management Policy

UiPath follows an internal Change Management policy that provides guidelines for implementing changes to the products and systems that UiPath develops, maintains, and supports. This policy is based on the ISO 27001 framework and is communicated to all employees. The policy includes changes to the production environment including network, systems, application updates, and code changes subject to the Change Control process. It also includes a procedure for addressing emergency changes, including appropriate approvals after deployment. The change management procedure requires requests, review, and approval of proposed changes. The policy also defines Application Code Lifecycle Management practices for implementing the changes that start from ticketing the change request/ features, coding, code review process, testing, and documenting the changes.

Information Classification Policy

UiPath has an internal Information Classification policy that manages all data stored via the Automation Cloud platform. This policy provides guidelines on handling different categories of data, including procedures to store, process, and retain such data. It also outlines the access control requirements of such data, encryption, and other security requirements.

Managed Devices Policy

Our Managed Devices Policy is part of the company's cybersecurity policy. It provides guidelines for the acceptable use of mobile devices within the organization. This policy applies to all mobile devices that have access to the corporate environment and business information, including smartphones and tablet computers. It also includes guidelines on the usage of approved app stores and applications.

Network and Communications Security Policy

UiPath has an established Network and Communications Security Policy. This policy is approved by management and communicated to all relevant parties. It has an owner who is responsible for its maintenance and review. The policy defines enterprise network security requirements and manages the protection of information in systems and applications. It includes security mechanisms, service levels, and management requirements of all network services, whether these services are provided in-house or outsourced. The policy also establishes controls to safeguard the confidentiality and integrity of data passing over the UiPath network, including authorized access to the network, management of network equipment, logging and monitoring of the network, and deploying network access control measures to restrict access of rogue devices to its networks.

Password Policy

UiPath has a comprehensive Password Policy in place to ensure the security of its systems and applications. This policy is designed to make passwords difficult to guess and resistant to automated compromise attempts. The IT department enforces password complexity rules in line with this policy, and users are responsible for maintaining the confidentiality of their passwords.

In addition, UiPath follows the password policies and procedures from the ISO/IEC 27001 documentation.

Physical Security Policy

Our Physical Protection policy governs the company's facilities and is reviewed at least once annually. The policy includes measures designed to prevent unauthorized physical access or damage caused by physical and environmental threats to UiPath employees, premises, system and network devices, and information. The level of security measures, policies, and procedures implemented commensurate with the legal, regulatory, or contractual requirements associated with each facility.

Security and Privacy Incident Management Policy

The Security and Privacy Incident Management Policy at UiPath is designed to detect and report unauthorized acquisition, use, or disclosure of client-scoped data. All UiPath users, including employees, contractors, and third parties, are required to report privacy incidents and events using the UiPath Incident Management and Reporting System. This policy also governs the management of such issues.

UiPath has an internal Incident Management Program that defines how incidents are documented, categorized, resolved, and reported. The Incident Response process addresses incidents related to security, availability, confidentiality, and other product issues.

UiPath also enforces and follows Incident Management Policies and Procedures covering sections like: Identifying and Reporting Information Security and Privacy Events, Roles and Responsibilities, Incident Classification, Response to Security Incidents and Post-incident Response.

Supplier Information Security Policy

The Supplier Information Security Policy at UiPath provides guidelines on managing non-conformity to any data confidentiality or security provision. This policy is part of our internal procedures and is enforced through the ISO 27001 Policies and Procedures. It covers sections like general requirements on Cyber Security and Data Handling, Risk Assessment, Roles and Responsibilities, Cyber Security, Privacy and Security Compliance, Legal Procurement, Procurement, Identifying and Reporting information security events, and Policy Breach Reporting.

Teleworking Policy

UiPath has a teleworking policy that enforces rules on using a VPN approved by UiPath to connect to the corporate network. All connections are over TLS 1.2+. The policy also enforces a clear-desk and clear-screen policy for remote workers. It is important to note that UiPath employees do not have any default access to customer data.

UiPath Security Management Team

UiPath has a dedicated CISO and a product security team. UiPath has established a Product Trust Management Board (PTMB), which is responsible for the security, availability, and confidentiality of UiPath cloud-based products.

UiPath has different roles and functions as part of the larger security management teams in the organization. This includes the Product Trust team, Privacy and Security Compliance team, Site Reliability Engineers (SRE), DevOps, CloudOps, quality engineers, and security champions as part of the development team. For cloud operations, UiPath employs a 24/7 Site Reliability Team that monitors security alerts and incidents.

Our security staff's security certifications include CISSP (Certified Information Systems Security Professional) and CISM (Certified Information Security Manager).

HR Security

UiPath provides and enforces annual training to its employees and contingent workers to help improve the company's cyber hygiene and protect UiPath assets.

UiPath has an Internal Training and Evaluation Platform used by UiPath personnel to access and enroll mandatory Security trainings and Quiz Tests accordingly with the Onboarding Plan, HR Policies, Local Laws and the well-known Security Awareness Trainings Best Practices.

UiPath maintains an annual internal training program to educate its employees with respect to UiPath information security and compliance-related policies. Employees are informed of the requirements for acceptable use of UiPath resources, in order mitigate the risk of unauthorized access to UiPath equipment, as well as use and modification of information assets. Training requirements and objectives include:

- Information Classification
- Privacy
- Internal Security
- Code of Conduct
- Anti-Bribery
- Anti-Harassment
- Conflict of Interests
- Customer Data (i.e., PII or CPNI) Handling and Protection
- Storage, retention, and disposal
- Notice and consent requirements
- Cross-Border Data Transfer Controls (such as a global clearance process)
- Procedures for managing Third Parties handling customer or employee PII or CPNI
- Social engineering awareness/detection
- Phishing awareness/detection
- Malware attacks (ransomware, key loggers, Trojans etc.)
- And others

UiPath mandates these trainings for employees upon hire and annually thereafter. Training completion is monitored through the training platform and reminders are sent automatically. Managers monitor to ensure that all team members complete this yearly requirement.

UiPath has implemented a background verification process for all hires via a Background Checks policy and aligned with the applicable local laws of hiring based on the regions. All employees have signed our Information Security Employee Policy and a clause on the protection of confidential information is part of the contract.

Risk management

UiPath has a risk management process in place, based on which it designs the set of security controls meant to reduce security risks to an acceptable level. The Risk Management process takes into account the cyber security objectives and is used to achieve acceptable risk levels for the company. The Risk Management process is a continual process of planning and performing risk assessments, reporting activities and mitigating risks. Risk assessments are carried out according to the approved Risk Assessment Methodology.

A Risk Assessment is conducted at least annually. The Risk Assessment Methodology is based upon the in-scope business systems, threat landscape and potential vulnerabilities. Identified risks are mitigated according to risk severity and business priorities and captured in a Risk Treatment Plan.

Vendor Risk Management

UiPath maintains a Third-Party Vendor Risk Management Program through which it assesses and manages the risks assumed by the nature of relationships with vendors and contractors that receive, store, process or host UiPath data or have access to UiPath networks and systems.

UiPath concludes data protection agreements and imposes security requirements on its vendors in order to ensure that at least the same level of confidentiality and data security is implemented by its sub-contractors as the ones applicable to UiPath. UiPath maintains the right to perform audits in order to monitor the compliance of its sub-contractors with the agreed technical and organizational measures regarding data confidentiality and security.

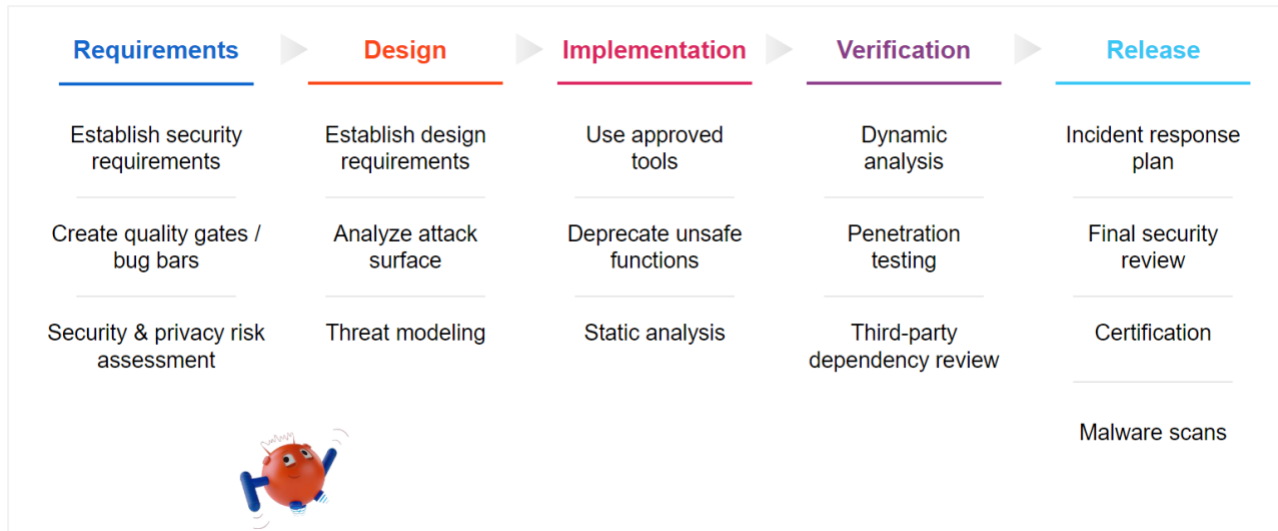
External - Internal Audit

UiPath has a structured approach to both internal and external auditing to ensure the security, availability, and confidentiality of its services. Here are some key points regarding the auditing processes at UiPath:

- **Internal Auditing:** UiPath's internal audit team conducts audits throughout the year, covering operational processes related to security, availability, and confidentiality. This includes reviewing areas where fraud could occur. The internal audit team follows documented policies and procedures, and an annual audit plan defines the audit criteria and scope for each audit. Internal audits are performed annually to ensure that internal controls are designed and operating effectively.
- **External Auditing:** UiPath is audited by external third-party entities for attestation, certification, and regulatory reasons on an annual basis. This helps UiPath support user entities in meeting various compliance and regulatory demands.
- **Subservice Organization Monitoring:** UiPath monitors critical vendors by reviewing their SOC 2® or equivalent security reports annually. This includes performing security reviews and internal performance assessments of vendors on an annual basis.

Secure Software Development Life Cycle (SDLC)

UiPath follows a Secure SDLC in developing our products. Through the SDLC, our teams include security requirements and architecture reviews alongside the functional requirements for each feature we develop. Code reviews and security assessments such as Static & Dynamic code analysis, Open-Source Software assessments & manual penetration testing are part of the process. UiPath also leverages automated tools and maintains a bug bounty program to identify vulnerabilities. Our developers are trained in secure coding practices, including OWASP guidelines, and we have a security champion watching over the lifecycle. Incident Response is also part of our Secure SDLC and handles threats that may appear over time.



UiPath ensures an agile SDLC process where developers work as a team and in sprints. All product defects and planned features are triaged together as a team. Specifications of the new feature or fix is documented along with each defect/feature in Jira, documentation is maintained in Jira as well as in Confluence, ensuring knowledge is available for everyone to see and use.

4. Security Responsibilities

Data Management Roles and Responsibilities

UiPath considers privacy an essential part of the business. This is why we commit to applying one of the strictest privacy standards, the European General Data Protection Regulation (GDPR), with respect to all our products. In order to satisfy the customer's different privacy compliance needs, UiPath offers both on-premises and cloud software.

With the on-premises software, the customer can use the UiPath Platform fully on its infrastructure, without any data going outside the customer's environment. In this deployment type, the customer is both the data controller and data processor. UiPath does not store, process, or transmit any data by way of the on-premises software. UiPath provides security features and capabilities as part of the product which customers can leverage to ensure secure data handling.

For the scope of UiPath Automation Cloud (SaaS services), GDPR compliance is a shared responsibility between UiPath and the customer. The customer is the data controller and UiPath is the data processor. UiPath in its capacity as a data processor seeks to comply with applicable laws and regulations in the jurisdictions where UiPath operates and where UiPath services are offered. However, UiPath has no knowledge of customer data stored in the cloud. UiPath has no visibility of the conditions under which the data was collected by the customer, whether appropriate permission was obtained, or if it is being used in accordance with those conditions. In its capacity as a data controller, the customer is responsible for collecting, handling, maintaining and governing personal information input by the customer when using UiPath cloud products in accordance with GDPR and the customer's own internal policies and procedures. This includes, but is not limited to securing, maintaining, and logging the customer's tenant in the UiPath cloud. Also, the customer is responsible for the design, development, deployment, use and behavior of any automation that the customer chooses to build either in the UiPath cloud or on the customer's own premises. Regardless of how customers classify data that is stored in their tenant, UiPath treats customer data as confidential data and ensures that it is protected with the highest standards. In its capacity as a data processor, UiPath has implemented appropriate technical and organizational measures (TOMs) required by GDPR, including but not limited to encryption of data in transit and data at rest. UiPath has also implemented privacy by design and default in its software development practices. All of this is reflected in the contract and data processing agreement between UiPath and the customer.

Please consider the additional context regarding our SaaS service:

- UiPath does not provide managed services or business process outsourcing to any customer.
- UiPath plays no role in the customer's day-to-day IT operations or business operations.
- The UiPath cloud is not a recordkeeping system of any kind, and it does not replace any of the customer's existing systems of record.
- The UiPath cloud has no inherent capacity for transaction processing (e.g., payment processing, etc.)
- The UiPath cloud is commercially available, multi-tenant, self-service SaaS. The emphasis is on "self-service" in that the customer is responsible for establishing and properly configuring its tenancy in the UiPath cloud.
- The UiPath cloud represents a suite of tools the customer uses to build the automations of its own choosing. Keep in mind that UiPath just sells the tools. The customer builds the automations of their own choosing.
- The customer is responsible for the design, development, testing, use and behavior of any automation that the customer chooses to build.
- If the customer properly designs its cloud automations, then the outputs from these automations get returned to the customer's existing system(s) of record and are not stored in the UiPath cloud.

- The customer is responsible for its own data governance, including data minimization with respect to its use of the UiPath cloud. That is, the customer and its privacy and security people must understand all dataflows, including where data is and is not stored and why.
- UiPath does not have standing access to the customer's tenancy or data in the UiPath cloud. Further, we do not have knowledge of the customer's automations in the UiPath cloud.

For customers choosing to leverage UiPath cloud services, UiPath concludes Data Processing Agreement (DPA). This will be drafted in accordance with the GDPR and will contain rules regarding personal data management, incident management, DPIAs, data subjects' rights, etc. Standard DPA is available here for reference: <https://www.uipath.com/assets/downloads/dpa-cloud>

Shared Responsibility Model

A Shared Responsibility Model clearly helps to articulate the scope of each stakeholder and the responsibilities within their scope. It also helps to call out key differences between Customer and UiPath's role in designing, developing and maintaining end-to-end security and privacy measures to keep customer data secure. We are using this shared responsibility guidance to help UiPath customers to understand their own responsibilities based on the adopted deployment model and provide clear boundaries between customer and UiPath for both on-premises and cloud products. There could be overlapping responsibilities shared by two or more parties based on the area of responsibility and deployment type.

 Responsibility Matrix	On Premise Products			Cloud Products		
	(C)	(U)	(A)	(C)	(U)	(A)
Data						
End Point Protection						
Identity & Access Management						
Applications						
Network Controls						
Operating System						
Physical Hosts & Network						
Physical Datacenter						

Legend

Customer (C)	
UiPath	
Azure (A)	

5. Infrastructure Security

Service-Design Principles and Architecture

UiPath products follow microservices architecture, making the services easy to scale, manage, and deploy. UiPath also supports deployment on a "module-by-module" basis or on a service-by-service basis. This modular design provides segregated deployment and less regression impact for customization and enhancement specific to functionality.

Services are designed such that they can be deployed in the cloud, on-premises, or on private clouds, giving customers the freedom to choose their deployment model. The following deployment options are available for users:

On-premises models

Standalone products and Automation Suite (our on-premises automation platform) are on-premises solutions that are meant to be installed on either your enterprise computers and servers (self-hosted), or to be deployed in a public cloud.

For both of these models, you are responsible for maintaining and scaling the infrastructure and upgrading to newer versions.

- **UiPath Automation Suite**, being a platform-type solution, establishes one single delivery and maintenance mechanism for multiple UiPath products. With Automation Suite, you can manage your on-premises UiPath Platform as one product. The suite can be deployed on Linux servers (bare-metal or virtual machines) in your data center or public cloud (Azure, AWS, or GCP), or on your Kubernetes clusters in Amazon Web Services (Elastic Kubernetes Service) or Microsoft Azure (Azure Kubernetes Service), or on your OpenShift environment. Automation Suite includes a common end user portal along with all shared suite capabilities that enable you to easily configure the integration with existing enterprise systems, such as AD, AAD, or SAML, across all products; a common experience is offered across the suite for the user, tenant, external applications, and license management. Each UiPath product that is part of Automation Suite is available as a service within the context of the automation platform.
- **Standalone products** are installed using an individual installer. For example, Orchestrator is installed using UiPathOrchestrator.msi and Studio using UiPathStudio.msi.

High-level Architecture: UiPath Automation Suite

UiPath Automation Suite follows a microservices architecture, making the services easy to scale, manage, and deploy. These services can be deployed on premises, or on private clouds, giving customers the freedom to choose their deployment model.

UiPath offers two deployment modes for UiPath Automation Suite:

Automation Suite on EKS/AKS or OpenShift	Automation Suite on Linux
 <ul style="list-style-type: none"> • Install everything once in your existing Kubernetes environment for greater control and flexibility • You know your infrastructure better – easier to manage in your K8s environment • Leverage your EKS/AKS or OpenShift, your managed cloud for storage and any third-party components you prefer • Use existing integrations from your EKS/AKS environment to easily integrate Automation Suite capabilities 	 <ul style="list-style-type: none"> • Install everything once with Kubernetes infrastructure and tools on Linux • Easier upgrades and patch management – UiPath does the validation and compatibility check • UiPath does all the heavy lifting – we provision the entire K8 stack • We have got you covered: pre-built/pre-installed integrations for third-party applications

With UiPath Automation Suite, the products, integrations, *and* management tools are all containerized and preconfigured so customers can run things smoothly and benefit from more platform capabilities without increasing overhead.

				
Single install in cloud, on-prem Linux VMs, or on bare metal servers	Portal access to all services and integrations	Host multiple organizations on one infrastructure	Supported by UiPath end-to-end	Kubernetes infrastructure and tools embedded, or deploy on your current AKS/EKS or OpenShift cluster

Deployment methods				
	EKS	AKS	OpenShift	Linux
Single Node (Non-production)	✗	✗	✗	✓ *
Multi Node (HA)	✓	✓	✓	✓ **
Online	✓	✓	✓	✓
Offline	✓	✓	✓	✓
Disaster Recovery	✓	✗	✓	✓

*Requires additional HAA license.

**Multi-Node Lite is also supported.

For AKS -> Disaster Recovery: Multi-zone architecture for UiPath® services without zone affinity. Insights not supported.

For Linux -> Disaster Recovery: Active/Passive and Active/Active deployments

For EKS and OpenShift-> Disaster Recovery: Active/Passive deployment

The Automation Suite is designed to harness the intersection of technologies and allow customers to become fully automated enterprises, providing a robust set of capabilities to discover automations, automate processes, and operate automations across the organization.

More details on the Automation Suite Architecture for each supported deployment type are described in the links below:

- Automation Suite on Linux Servers
<https://docs.uipath.com/automation-suite/automation-suite/2024.10/installation-guide/deployment-architecture>
- Automation Suite on AKS/EKS Stack
<https://docs.uipath.com/automation-suite/automation-suite/2024.10/installation-guide-eks-aks/automation-suite-stack>

Cross-deployment Model Capability Comparison

Capability	Automation Suite on EKS	Automation Suite on AKS	Automation Suite on OpenShift	Automation Suite on Linux
Orchestrator	Yes	Yes	Yes	Yes
AI Center	Yes	Yes	Yes	Yes
AI Center with external orchestrator (standalone)	No	No	No	Yes
Apps	Yes	Yes	Yes	Yes
Action Center	Yes	Yes	Yes	Yes
Automation Hub	Yes	Yes	Yes	Yes
Automation Ops	Yes	Yes	Yes	Yes
Data Service	Yes	Yes	Yes	Yes
Document Understanding	Yes	Yes	Yes	Yes
Insights	Yes	Yes	Yes	Yes
Integration Service	Yes	Yes	No	No
Automation Suite Robots	Yes	Yes	Yes	Yes
Process Mining	Yes	Yes	Yes	Yes
Task Mining	Yes	Yes	No	Yes
Test Manager	Yes	Yes	Yes	Yes
Communications Mining	No	No	No	No
Studio Web	Yes	Yes	No	No

Cloud models

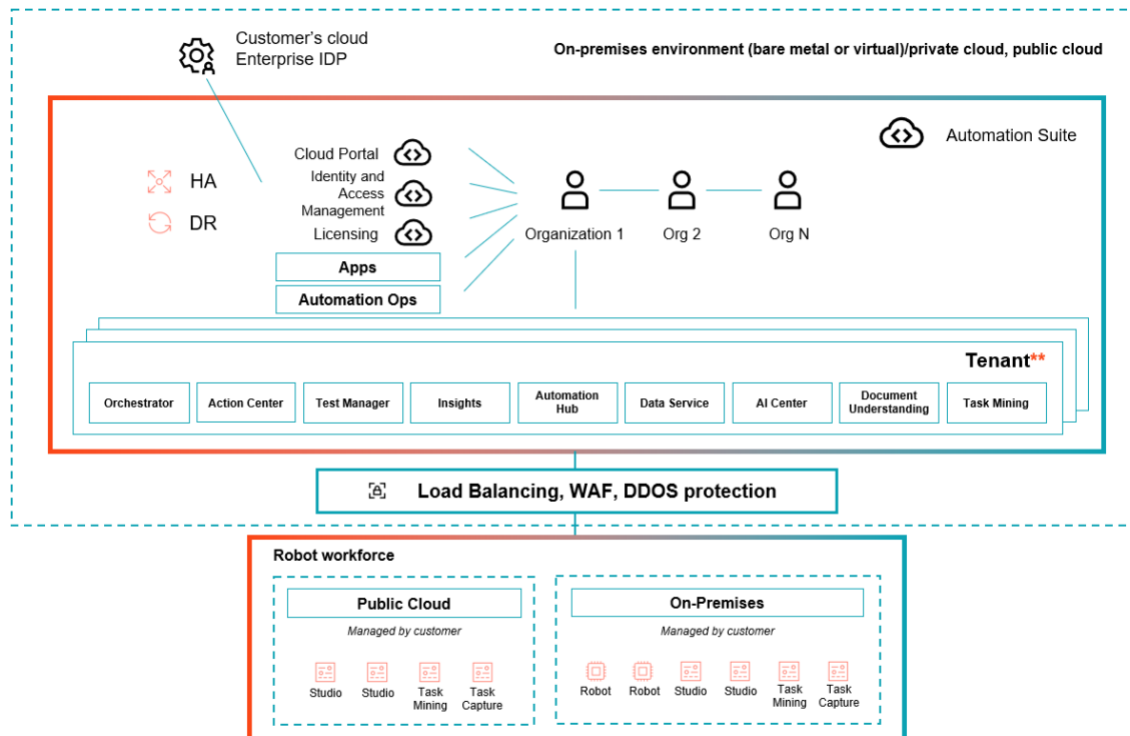
UiPath Automation Cloud™, our SaaS solution, minimizes your burden of infrastructure management and continuous updating. With UiPath handling these, you can focus solely on your automation journey. In terms of service-design principles, UiPath Automation Cloud uses core Azure services, including the compute, storage, networking, SQL database, app configuration, secret storage in Key Vault, and identity and access management. This allows UiPath to focus on the unique aspects of running and improving services while taking advantage of Azure's capabilities with regards to security, privacy, and compliance. The SaaS deployment options **come in three flavors: Automation Cloud, Automation Cloud Dedicated and Automation Cloud Public Sector.**

- **Automation Cloud™** is a multi-tenant SaaS solution recommended for most customers. It eradicates the necessity for infrastructure maintenance and significantly trims down operation costs.
- **Automation Cloud Dedicated** is a dedicated deployment within Automation Cloud, delivering UiPath capabilities with data and computing isolation. It offers a single-tenant SaaS environment with isolated compute and data resources, flexible upgrade controls (including 30-day delay and blackout windows), customizable domain endpoints, and advanced connectivity options for secure, private network integration.
- **Automation Cloud™ Public Sector** is designed for US public sector entities. It ensures meeting the necessary regulatory requirements and compliances of the public sector.

High-level Architecture: UiPath Automation Cloud

UiPath Automation Cloud is delivered via a Software-as-a-Service (SaaS) model that's built and hosted in Microsoft Azure (for the core deployment), leveraging core Azure services including compute, storage, networking, SQL database, app configuration, secret storage in Key Vault, and identity and access management. UiPath Automation Cloud is composed of multiple independent services such as Cloud Portal, Tenant Management Service, Licensing Service, and Orchestrator, among others. These services interact with each other to provide a seamless experience.

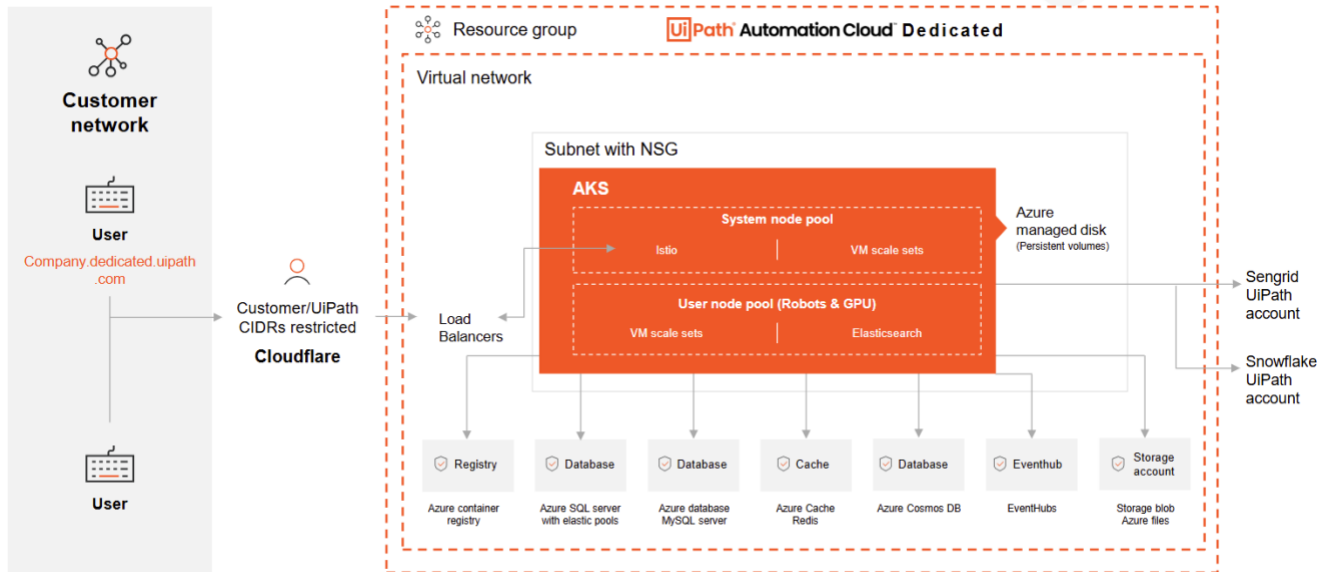
The Cloud Portal serves as the first entry point for customers when they create an account for their organization. It allows customers to invite or remove users, manage user roles and permissions, request licenses for robots, and set up Orchestrator instances for development, testing, and production needs. Orchestrator, the server-side component of the UiPath core platform, allows customers to manage their entire automation infrastructure from one central control plane.



** Not all available services are shown – services here are representative.

High-Level Architecture: UiPath Automation Cloud Dedicated

Automation Cloud Dedicated provides a *single-tenant SaaS deployment* as opposed to the standard multi-tenant Automation Cloud. It's designed for customers with higher data and compute isolation requirements. UiPath Automation Cloud dedicated is built on Microsoft Azure cloud infrastructure with multi-region deployment. At its core, it uses Azure services including AKS, Azure SQL Server, Azure Cosmos DB, and Azure Storage and employs Cloudflare for DNS and CDN services



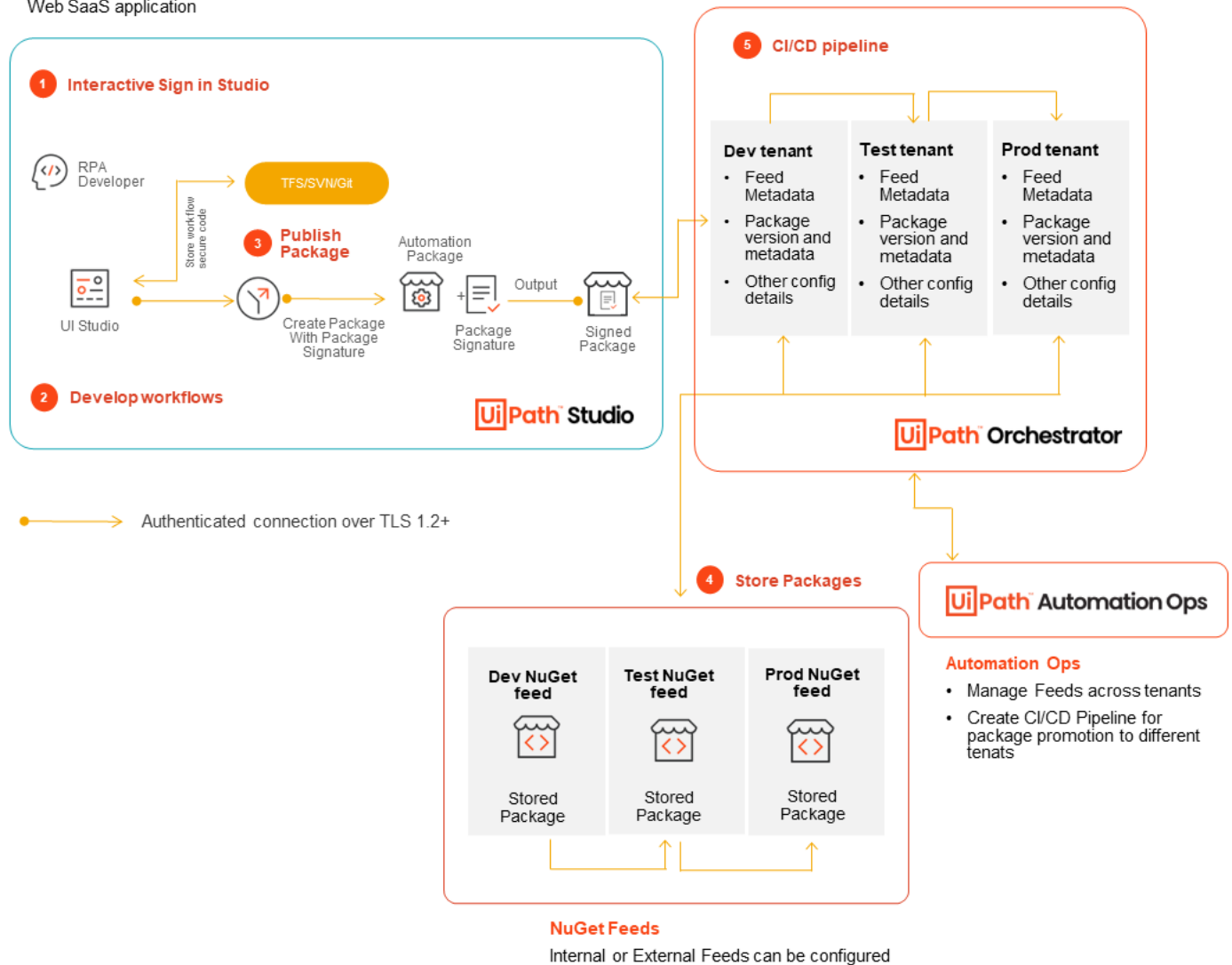
Data Flows

Automation Workflow Development and CI/CD

Studio: Development Environment Studio or StudioX
Installed on-Premise on developer workstations or Studio Web SaaS application

Orchestrator web application installed on premise or leveraged through Automation Cloud SaaS.

- Logically Separated Tenants For Dev, Test & Prod
- Configure Feed Settings at each tenant level

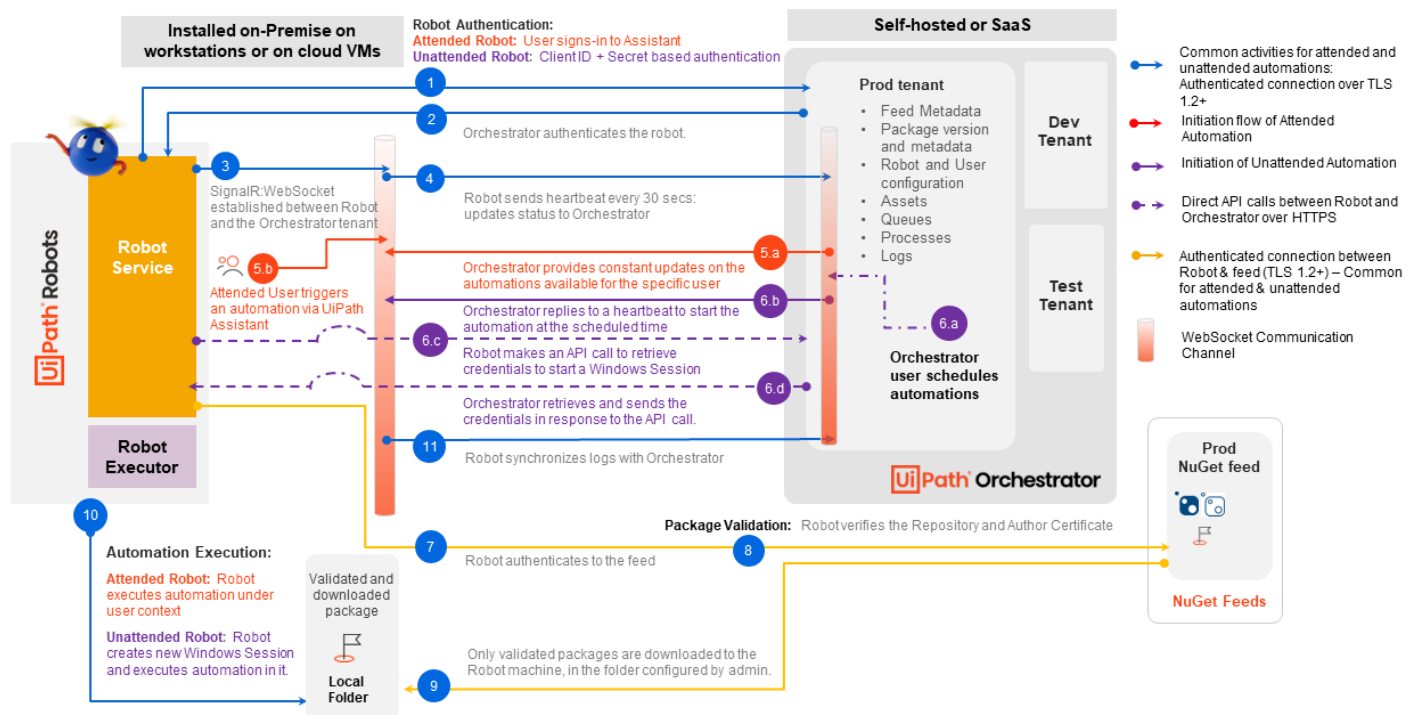


1. Developer Signs into Studio - Connects Studio to the Orchestrator Dev tenant. Logically segregated tenants can be created for Development, Test, and Production purposes.
2. The developer builds the workflow in Studio and can connect Studio to Source control tools for source code management.
3. Developer publishes the workflow. Studio (with the help of the underlying Robot Service) builds the code into an automation package. If package signing is enforced in Studio, then the package is signed using a certificate.

When a package is signed, the certificate used for signing is embedded within the package itself. This allows anyone who receives the package to verify the signature and ensure that the package has not been tampered with since it was signed.

4. Studio publishes the package to the tenant it is connected to. Developers can also select the folder to which the package is published.
 - Orchestrator allows tenant-level settings for the feed. You can configure to use an internal feed (Orchestrator tenant's feed), or provide an external feed path for storing the packages and libraries. You can also manage authentication information to the feeds. Internal Feeds support Secure Deployment and API authentication, whereas External Feeds supports basic authentication and API authentication.
5. Admin users can configure CI/CD pipelines for package promotion to different tenants via Automation Ops. They can use native Automation Ops - Pipelines feature -or- integrate with another third-party system such as Azure DevOps or Jenkins. In a CI/CD pipeline, the automation project is tested and republished in the higher environment (e.g., from Dev to Test or Test to Prod). When you publish a package, the CI/CD pipeline uses the storage feed to store packages and will then pull from it to make additional updates.

Automation Execution - Runtime



The robot is installed on-premises, either on workstations or in cloud VMs. It has two components: Robot Service, which is responsible for enabling connection with Orchestrator and Robot Executor, which executes the automation. The Orchestrator can either be self-hosted or used as a service via UiPath Automation Cloud. It is important to note that **communication always initiates from the Robot Service to Orchestrator**.

1. Robot Authentication:

- ▶ **Attended Robots** are typically installed in user mode. The Robot Service leverages a Windows process started under the user's context to connect with Orchestrator. Authentication with Orchestrator is OAuth-based, by having the user sign in.
 - ▶ **Unattended Robots** are typically installed in service mode, which allows them to perform tasks without a user being logged in. This is essential for automations that need to be run at any time, regardless of user presence. Authentication with Orchestrator is OAuth-based, using a client ID and secret for Unattended Robots.
2. Orchestrator authenticates the robot based on the Robot details available in the Orchestrator and provides an access token.
 3. The Robot service uses this access token to establish and maintain a secure WebSocket connection for real-time communication with Orchestrator. The Robot Service creates a WebSocket channel through which it subscribes to the Orchestrator's SignalR communication.
 4. The Robot service performs a poll (or heartbeat) every 30 seconds to signal its availability (available, busy, unresponsive, or disconnected) and to retrieve configuration and other information required from the Orchestrator. The communication is over HTTPS using TLS 1.2+.

5. Attended Automation Initiation/ Triggering:

5.a Attended automation cannot be scheduled, and therefore attended users can use UiPath Assistant to trigger automation on-demand. Assistant is where individuals (attended users) can easily view and run automations with just a couple of clicks. Orchestrator ensures that Assistant is provided with information on automations that are available for the user. The list of these automations is accessible to the user via Assistant.

5.b User can start the automation from the Assistant.

6. Unattended Automation Initiation/ Triggering:

6.a An Orchestrator user with an appropriate role can create a job based on the published automation package. The job can be scheduled for execution of specific robots in unattended mode.

6.b Orchestrator responds to heartbeat to start an automation (i.e., an automation is scheduled to run).

6.c When the Robot Service receives a response to start an automation, it will first send an API request to the Orchestrator service to retrieve a set of credentials (for the Windows session) stored in Orchestrator storage (SQL Server) or a [third party credential store](#) based on the configuration.

6.d The Orchestrator retrieves the credentials either from the SQL Server or from the Credential Store and sends the credentials back to the Robot Service via HTTPS response. Please note that credentials or other sensitive information is never sent via SignalR.

7. The Orchestrator provides the robot with the location of the NuGet feed and facilitates the authentication process for the robot to access the feed.
8. The Robot Service validates the package signature before downloading it for execution. At the time of publishing an automation, you can enforce Package Signature to ensure robots only execute signed packages. A package can have both a repository and author certificate, but only the repository certificate is mandatory.

The Robot Service checks the repository certificate and, if required, also verifies the author signature before installing the package.

9. If the package signature is not trusted, either because the repository or author certificate is not recognized, the package will not be installed on the machine. Since the packages are signed, users cannot tamper with the automation code. Modifying the package contents would break the signature validation, preventing the package from being installed and executed.
10. **Automation Execution:** The Robot Executor executes the downloaded automation.
 - ▶ **Attended Automation:** Automations are executed under the context of the user signed in via UiPath Assistant.
 - ▶ **Unattended Automation:** Robot Service uses the credentials to the Windows Session provided by Orchestrator to create a user session. The Robot Executor leverages this user session to run the automation process.

During the automation, based on the folder-level permissions of the Robots, the Robot Executor can use APIs to access Queues (a collection of work items to be processed by robots) and Assets (e.g., sign in credentials required for target applications such as SAP that are being automated) while executing the automation.

11. Upon completion of the job, the Attended Robot (Robot Service) waits for the user to trigger the next automation. When an Unattended Robot completes an automation, it signs out of its user session in Windows and waits for the next job trigger. Also, Robots continuously synchronize the execution logs with the Orchestrator, and these are visible in the Orchestrator

Physical Security

UiPath facilities are governed by the Physical Protection Policy that is reviewed at least once annually. Physical security measures are designed to prevent unauthorized physical access or damage caused by physical and environmental threats to UiPath employees, premises, system and network devices and information, or interruptions to the organization's activities. However, note that UiPath does not own a data center or host customer data.

For the SaaS deployment options, UiPath Automation Cloud and Automation Cloud Dedicated, UiPath leverages Azure data centers for hosting the solution. Automation Cloud (multi-tenant SaaS) additionally has supporting deployments in GCP and AWS depending on the service availed. Physical security measures are provided by the cloud provider who have industry-certified physical security and compliance capabilities.

For the self-hosted options, both UiPath Automation Suite as well as the standalone products, it is deployed in the customer environment, and the implemented solution is bound by the physical security features and procedures set up in the customer environment.

It's important to note that UiPath Automation Cloud is a great deployment option for customers who want to start delivering automation quickly then scale up over time, with enterprise-scale manageability and optimization from day one.

Network Security

With the SaaS deployment options, UiPath manages the underlying cloud environments and network security by way of being the SaaS provider. UiPath leverages Cloudflare to front the cloud platform, providing both DDOS and WAF protection. Cloudflare ensures the performance of the platform by distributing user entity traffic, making web page load times faster by

serving content from locations closer to the user entity. It also provides DNS and web application firewall (WAF) services that protect the service from malicious traffic and distributed denial of service (DDoS) events. Additionally, UiPath uses Azure's DDoS defense system to help prevent attacks against the service. This system uses standard detection and mitigation techniques such as SYN cookies, rate limiting, and connection limits. UiPath has Site Reliability Engineering teams who monitor the services 24x7 using tools such as Azure Sentinel and MS Azure Security Center.

From an automation perspective, Robots connect to the Orchestrator service using an encrypted HTTPS channel. There are only ever outgoing connections from Robot to Orchestrator. Customer needs to enable outbound HTTPS from their network to the cloud Orchestrator. Inbound connections are not required by default.

If your company restricts access to only allowed websites, you must allow access to the necessary domains based on the UiPath products you use and the scenarios per product.

Please refer to links below for firewall configuration:

- UiPath Automation Cloud (SaaS): <https://docs.uipath.com/automation-cloud/automation-cloud/latest/admin-guide/configuring-firewall>
- Automation Cloud Orchestrator Outbound IP Address (*if you choose to use secrets servers, SMTP servers, AWS S3, and Azure Key Vault, from your own on-premises or cloud networks*): <https://docs.uipath.com/orchestrator/automation-cloud/latest/user-guide/orchestrator-outbound-ip-addresses>
- Automation Cloud Dedicated: <https://docs.uipath.com/automation-cloud-dedicated/automation-cloud-dedicated/latest/admin-guide/configuring-firewall>
- UiPath Automation Suite (Linux): <https://docs.uipath.com/automation-suite/automation-suite/2024.10/installation-guide/network-requirements>
- Standalone Orchestrator: <https://docs.uipath.com/orchestrator/standalone/2024.10/installation-guide/configuring-the-firewall>
- Robots: <https://docs.uipath.com/robot/standalone/latest/admin-guide/services-the-robot-connects-to>
- Studio: <https://docs.uipath.com/studio/standalone/latest/user-guide/services-studio-connects-to>

6. Operational Security

Release Cycle and Security Updates

UiPath has adopted a release strategy that emphasizes both innovation and stability. Starting with 2024, UiPath simplified its release approach for self-hosted products by moving to a single Long-Term Support (LTS) release every year, typically in October. This change aims to enhance the value brought with each update and streamline the upgrade process for users.

Cumulative updates (CUs) - In addition to the LTS release, we provide Cumulative Updates (CUs) throughout the year. These updates include security patches, accessibility improvements, and other important fixes. In 2025, we simplified our release cadence by delivering cumulative updates every three months.

Hotfixes - When necessary, we release hotfixes outside the regular CU cycle to address critical issues or vulnerabilities that require immediate attention.

Interim desktop releases - There may be interim releases for desktop (client-side) products to take full advantage of new capabilities that would otherwise be available only in Automation Cloud™.

These regular updates and on-demand hotfixes ensure customers stay secure, stable, and up to date throughout the year without waiting for the next LTS release.

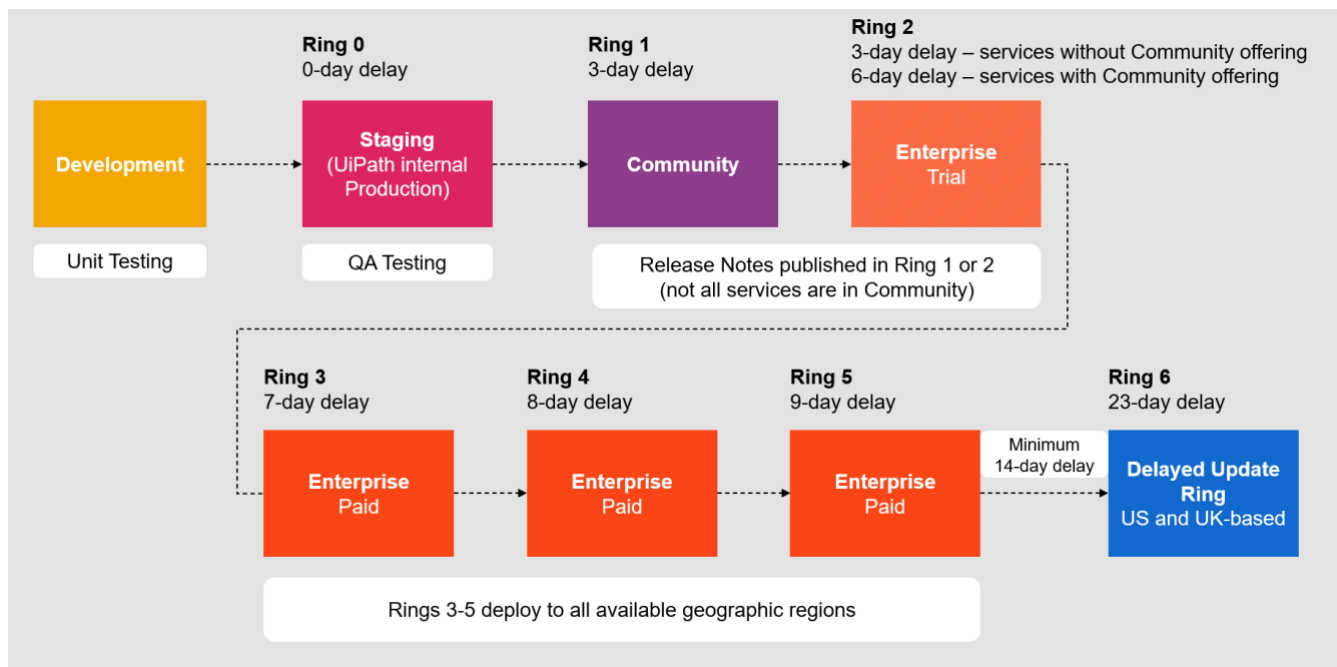
Customers are responsible for managing the installation and upgrades in case of the self-hosted deployment options.

UiPath Automation Cloud™, being a SaaS offering hosted by UiPath, is continuously evolving. It benefits from a more dynamic release cycle with updates approximately every two weeks. This allows for rapid deployment of new features and security updates, ensuring that users have access to the latest advancements in automation technology.

This approach to release cycles and security updates reflects our commitment to delivering high-quality, secure software that meets the needs of its customers while also fostering an environment of continuous improvement and innovation.

Ring-Based Deployment for Seamless and Disruption-Free Upgrades: UiPath Automation Cloud

UiPath Automation Cloud uses a ring-based deployment model for upgrades. This process begins with updates being applied to internal staging sites first. After confirming the stability of the updates, they are then rolled out to the hosting community and beta versions. The updates are then applied to sites with fewer customers, gradually moving to sites hosting larger groups of customers. At every stage, UiPath performs rigorous testing and continuous monitoring to ensure stability of the upgrades. This approach ensures that any instability or error due to the update is identified and addressed before it reaches a larger enterprise customer base.



Risk Mitigation through Canary Tenants and Delayed Update regions: UiPath Automation Cloud

Customers can add a *canary tenant* to their organization to view and test upcoming changes before they reach their other tenants. The canary tenant serves as an isolated medium that uses the current customer tenant setup where they can check on the impact that upcoming changes have within the context of the current organization. The canary tenant receives updates to enterprise functionality for all of the supported services (currently Orchestrator) as soon as they are announced in the release notes, while other tenants receive them *at least 3 days later*.

Delayed Update Region: UiPath Automation Cloud

Customers in the Life Sciences industry (e.g. pharmaceuticals) are subject to very strict regulations for their production environments referred to as GxP. It is important to note that it is UiPath customers who are regulated under GxP, not UiPath directly – but in order to enable them to comply, they must have sufficient time after UiPath pushes changes to:

- Test their regulated production processes with any pending changes to ensure that the results are consistent.
- Make sure that their internal documentation of how a user interacts with the system is completely consistent with the product as it appears. For example, even changing the name of a tab or button in the UI requires them to update their internal documentation.

To enable this, UiPath offers the Delayed update regions in Automation Cloud (multi-tenant). Delayed Update is an additional, paid service (available as paid add-on option in the Unified Pricing model and for customers with an **Advanced Tier** license in Flex Pricing model) that covers all Automation Cloud features and offers a longer (and guaranteed) pre-release validation period than the free canary tenant update. Originally designed to support “good practice” (GxP) compliance scenarios in life sciences, it's now available to any enterprise customers who need this capability and have production tenants in the United States and the European Union.

Enterprise organizations (UiPath Automation Cloud customers in regular regions) can expect to see the updates 3 days after they are first announced in the release notes, or later. The exact number of days it takes for the changes to become available to customers in their chosen hosting region varies depending on when we finish deploying the changes to all the regions. With a Delayed Update Organization, customers will receive updates for Automation Cloud and its services

at least 2 weeks after they are pushed into the Enterprise Production Organization. The Enterprise Production Organization can be used as a pre-production environment and the Delayed Update Organization as the production environment. Depending on whether US or UK-based delayed update region is opted for, some services may be not available for delayed update. Please refer to the documentation for [data residency](#).

Delayed Updates: Automation Cloud Dedicated

One of the main advantages of Automation Cloud Dedicated is the ability to control upgrades. We provide two types of controls:

1. Delayed release: This allows you to postpone updates for up to 30 days.
2. Blackout window: We ensure no updates take place for a specific period with a blackout window of up to 30 days.

To ensure Automation Cloud Dedicated organizations stay updated, we have placed the following restrictions:

- Blackout windows can only last for a continuous period of 30 days. This is to accommodate a 30-day freeze period for your end of the year needs.
- Each blackout window must be followed by a break of at least 10 days, which ensures that UiPath has ample time to roll out updates after a prolonged blackout window.
- Any modifications to the blackout window must be submitted via a ticket 5 business days ahead of the intended change.
- You are not allowed to implement any changes that would result in time being blocked within the next 48 hours, which was previously unblocked.

Vulnerability Management and Penetration Testing

Our Security program performs vulnerability assessments as a continuous exercise. UiPath will address vulnerabilities based on the provided SLAs. UiPath leverages a number of tools to find vulnerabilities in our code and products. All UiPath developers are trained in OWASP security guidelines and UiPath's information security management system has been certified for conformity with ISO/IEC 27001 since 2020. All source code is entered into an open-source software management system, which keeps track of any vulnerabilities that may arise in 3rd-party libraries that are leveraged in our products. Additionally, all releases are handed over to our internal pen test team to perform manual and automated testing prior to GA release. We also have a [bounty program with HackerOne](#).

UiPath Security performs automated static and dynamic (SAST/DAST) as part of our CI/CD pipeline. Advanced Security is run both for Code Pull Requests and as part of the pipeline. Security then runs third-party dependency check and container scan from the pipeline (SAST and CVE detection.) UiPath security also leverages tools for DAST. Security also utilizes a secret scanner, malware scanning and other tools. In addition, UiPath Security has an in-house pen test team that examines every pull request and then leverages a variety of tools and code tests to then attack any weaknesses they find in the code. By doing this, UiPath security has true grey hat pen testing for every product release (which also includes API testing).

CVE Risk Management

The evaluation framework for new CVEs (Common Vulnerabilities and Exposures) involves a comprehensive process where the UiPath Security team adjusts the CVSS (Common Vulnerability Scoring System) score based on internal assessments and temporal factors. This framework ensures a more accurate representation of the risk posed by each CVE within our specific environment. These evaluations are also consistent with the CVSS-BTE scoring which incorporates

Base, Threat, and Environmental metrics rather than relying solely on the base metrics typically provided by a vulnerability scanner.

Process Breakdown:

1. Technical Analysis:

- Conduct an in-depth technical analysis of the vulnerable function, including how it is used in the code.
- Assess exploitability based on the context within our environment.

2. Remote vs. Local Execution:

- Determine if the exploit requires remote execution or local access.
- Review access controls on inter-pod communication and external interfaces to understand the access level required for exploitation.

3. Special Configuration Requirements:

- Analyze any special configurations needed to run the exploit.
- Review container context and other environmental configurations that might affect exploitability.

4. Function Usage Monitoring:

- Use tools such as *ldd* or *lsof* to check if the vulnerable library and function are called in our systems.
- Employ eBPF function tracing to monitor file access within our development clusters for better accuracy.

5. User Role Analysis:

- Determine the user role needed for the execution of the exploit.
- Consider mitigation factors, especially since most of our pods operate in a non-privileged context.

6. Mitigating Controls:

- Identify existing mitigating controls in the product deployment that could reduce the impact or likelihood of exploitation.

7. Contextualize Attack Paths:

- Use detailed data on possible attack paths within our applications and services to understand the full scope of potential exploits.

8. Exploit Prediction Scoring System (EPSS):

- Incorporate EPSS, which estimates the likelihood that a software vulnerability will be exploited, into the assessment process.

9. CISA Known Exploited Vulnerabilities (KEV):

- Reference the CISA KEV database to identify if the vulnerability has been actively leveraged by attackers.
How the Evaluation Framework Affects CVSS Scores: Environmental and Supplemental Metrics
The CVSS (Common Vulnerability Scoring System) score is influenced by environmental and supplemental metrics, and the evaluation framework detailed in the provided document feeds into these metrics as follows:

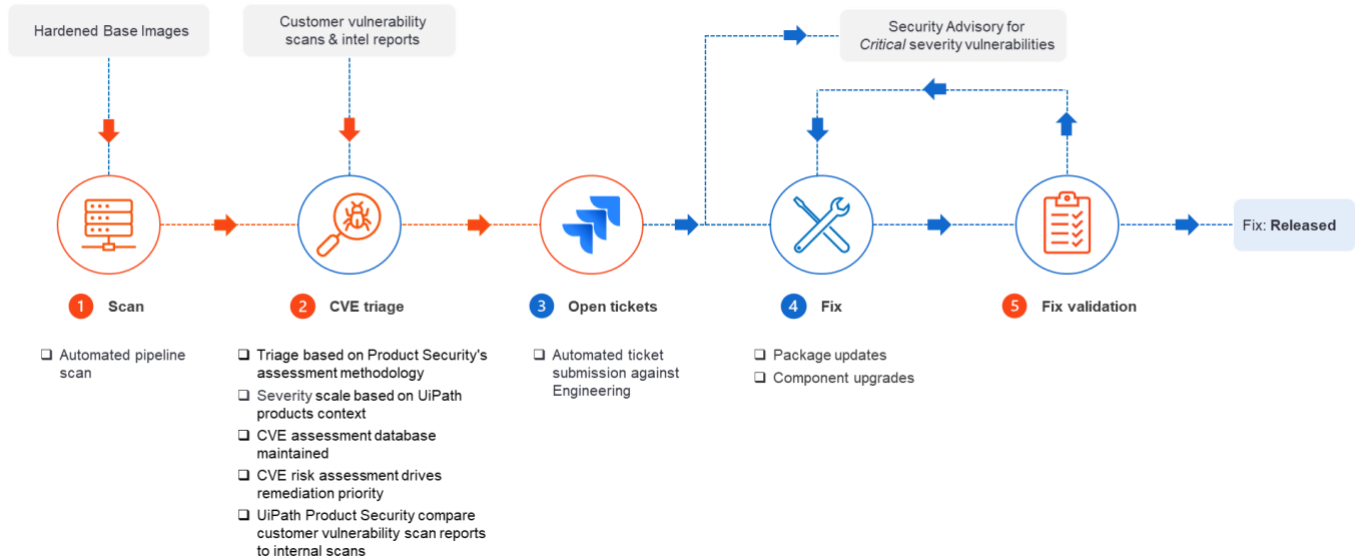
10. Environmental Metrics:

- Confidentiality, Integrity, Availability Requirements (CR, IR, AR): Analysis of the context and criticality of the vulnerable functions and data affected helps in determining these requirements.
- Modified Base Metrics (MAV, MAC, MAT, MPR, MUI, MVC, MVI, MVA, MSC, MSI, MSA): Evaluations of remote/local execution, user roles needed, special configurations, and mitigating controls inform the modified metrics.
- Exploit Prediction Scoring System (EPSS): Used to adjust the likelihood of exploitation, which affects MAV, MAC, MAT, etc.

11. Supplemental Metrics:

- Safety (S): Determined by assessing the potential impact on user safety from exploitation.
- Automatable (AU): Evaluated by understanding if the exploit can be automated, affecting the ease of exploitation.
- Recovery (R): Assessed by determining the effort needed to recover from an exploit.
- Value Density (V): Based on the criticality of the affected data/function.
- Vulnerability Response Effort (RE): Assessed by evaluating the effort needed to mitigate the vulnerability.
- Provider Urgency (U): Determined by the urgency from advisories and known exploits, such as CISA KEV.

CVE Risk Management Workflow



Common Vulnerability Mitigations in Automation Suite

Automation Suite is a collection of multiple server products made available as a collection of more than 100 containers. The deployment offering is intended to provide a similar experience as the UiPath Automation Cloud environment, but deployable in a customer managed environment. Customers can choose whether to leverage an existing Kubernetes stack in the form of Azure AKS, AWS EKS, OpenShift, or leverage the full Automation Suite package which includes Rancher and several additional components to assist in managing a container deployment. Each container is built as multiple image layers. These often contain a base image layer that provides the Operating System such as Red Hat or Debian, one or more infrastructure layers to provide software frameworks or web servers, and at least one application layer installed on top. Each layer will require dependencies just as Linux itself requires certain software to be installed.

A common challenge in scanning Automation Suite and containers in general is that vulnerability scanners often lack context. Typically a vulnerability scanner including CSPMs like Wiz or Prisma will match the name of a piece of software and its version against a list of known vulnerabilities or CVEs. The list of CVEs typically comes from a mixture of the NIST National Vulnerability Database and the vendors own research. Vendor specific vulnerabilities typically start with the vendor name such as AQUA-<Year>-<number> or PRISMA-<Year>-<number> instead of starting with CVE. In almost all cases, these scans leverage the CVSS-B scoring which includes only the base scoring metrics of a vulnerability intended to be representative of the worst possible risk that a vulnerability can present.

As described in the CVE Risk Management section, UiPath will evaluate risk based on the CVSS-BTE scoring that includes Base, Threat, and Environmental metrics rather than relying solely on the base metrics. UiPath can provide this level of analysis while still maintaining principles of zero trust, because the evaluation only includes components of Automation Suite or the container itself and does not take into consideration customer managed infrastructure or other environmental controls.

Common Mitigations in Automation Suite:

1. Privileged Access Required for Containers:

- Automation Suite containers require privileged access for users to run any commands at the CLI. This blocks normal users or attackers from being able to exploit vulnerabilities located in system libraries or dependencies that do not accept or handle requests coming in from outside of the container.
- Reverse Proxy:**
 - Automation Suite leverages a reverse proxy to front communications from outside the environment. This serves to mitigate or block vulnerabilities where a web server or library incorrectly handles network requests such as malformed HTTP calls.
 - OPA Policy Enforcement**
 - Automation Suite leverages Gatekeeper policies in addition to secure defaults to ensure various secure configurations are set and enforced across containers
 - Root Accounts are disabled and escalation to root is disabled everywhere possible.

Production Environment Access Controls

SaaS Services (Automation Cloud and Automation Cloud Dedicated): UiPath maintains strict control over who has access to the production environment and customer data. UiPath uses Azure Privileged Identity Management (Azure or MS Entra PIM) to manage, control, and monitor access to important resources within UiPath. By using PIM, UiPath minimizes the number of personnel who have standing access to secure information or resources, thereby reducing the risk of access abuse or accidental impact on sensitive resources or data. Users who need to perform privileged functions must use PIM to temporarily elevate their access level and provide a justification for the access. These requests are approved by management or authorized reviewers, and all activities conducted under PIM are logged and recorded; at the end of the session, privileges are revoked.

Additionally, UiPath has established controls to ensure that access to confidential data is restricted to those who require it to perform their business functions. A formal process is in place for managing user accounts and controlling access within the production environment, with role changes or terminations initiated by the People Operations team in Workday, triggering the appropriate changes in Active Directory. UiPath employees or UiPath third party services do not have any default access to customer data in the cloud.

This approach to privileged access management aligns with best practices for security and compliance, ensuring that only authorized personnel have access to sensitive information and resources when necessary, and that such access is monitored and auditable.

Note that Customer is responsible for managing logical access to their tenant in the Automation Cloud service and the Automation Cloud Dedicated service.

Self-hosted Deployment Models (UiPath Automation Suite and Standalone Product deployment): Only the customer's authorized users have access to the platform, the underlying data, and the underlying infrastructure. UiPath does not store, process, or transmit any data by way of the self-hosted products.

Availability and Disaster Recovery

SaaS Services (Automation Cloud and Automation Cloud Dedicated): With respect to the Automation Cloud SaaS services, it is of utmost importance to us to ensure that the services are available for users to access their organization's assets. That is why we employ backup mechanisms from the CSPs and also employ other fail-safes to help ensure availability. The CSP provides regular updates for known security vulnerabilities. The company also performs regular updates for systems, with security updates performed out of band of any product updates.

UiPath's security program performs vulnerability assessments as a continuous exercise, addressing vulnerabilities based on provided SLAs. The company leverages tools to find vulnerabilities in code and products, and all releases are given to an internal pen test team to perform manual and automated testing prior to GA release. UiPath Automation Cloud and Automation Cloud Dedicated are cloud-based Enterprise SaaS solutions that have a documented Business Continuity

Plan (BCP) and Disaster Recovery (DR) policy that is reviewed and tested annually. The services leverage Azure's native resilience for all components, triggering appropriate fail-safe measures in the event of any component failure. In case of a security event, UiPath has security response plans in place to minimize data leakage, loss, or corruption. The service is designed to withstand attacks from both outside and within Azure, including distributed denial-of-service (DDoS) attacks. For UiPath Automation Cloud, UiPath provides a target uptime of 99.9%. UiPath provides transparency to the availability and uptime of the services via the status portal (<https://status.uipath.com/>). Customers can sign up for notifications and alerts via their preferred communication method: email, text, ATOM, or RSS feed.

Self-hosted Deployment Models (UiPath Automation Suite and Standalone Product deployment): For on-premises or customer cloud deployments, UiPath provides customers with different deployment options that support configuring the platform to support their availability and disaster recovery requirements.

UiPath Automation Suite (Linux) supports Active/Active and Active/Passive configuration. The deployment can withstand the complete failure of nodes, entire data centers, or even regions. The following scenarios are supported:

- Same-site deployment: Two Automation Suite clusters deployed in the same site or data center.
- Cross-site deployment: Two Automation Suite clusters deployed in different data centers.
- Same-region deployment: Two Automation Suite clusters deployed in the same region, either in the same data center or in different data centers in the same area.
- Cross-region deployment: Two Automation Suite clusters deployed in different regions.

UiPath Automation Suite on EKS and OpenShift support multi-site deployments in Active/Passive mode support the following scenarios:

- **Same-region deployment** – Two Automation Suite clusters deployed in the same region;
- **Cross-region deployment** – Two Automation Suite clusters deployed in different regions.

Only specific services are currently supported in the DR mode with Active/Passive. You can install products that are not supported in Disaster Recovery with Active/Passive. However, you cannot use these products when the primary cluster is down.

UiPath Automation Suite on OpenShift, AKS and EKS provides intra-region resilience and fault tolerance capabilities by distributing resources across multiple zones and automating the recovery process in case of zone-level failures. It supports multi-zone architecture without zone affinity. The worker nodes are distributed across multiple zones to provide resilience to zone failure and scale when required. The platform has no affinity rules to ensure that worker pods are distributed equally across the zone. If there is any zone-level failure, there may be a momentary degradation of the service, which would be resolved when that service is automatically moved to a new zone by the AKS/EKS control plane.

In the case of **standalone deployment** of products, UiPath Orchestrator supports both Active-Passive and Active-Active deployment models. The Active/Passive model: extends the High-Availability configuration in the Primary Datacenter with a Disaster Recovery option in a secondary datacenter. The Active-Active deployment model can be implemented to ensure both High Availability and Disaster Recovery. Here, both Orchestrator nodes are active, and the Load Balancer directs traffic to them using a specific algorithm, such as Round Robin or one of its variants.

For more details on the Disaster Recovery models, please refer to the below links:

- Automation Suite (Linux): <https://docs.uipath.com/automation-suite/automation-suite/2024.10/installation-guide/disaster-recovery>
- Automation Suite (EKS): <https://docs.uipath.com/automation-suite/automation-suite/2024.10/installation-guide-eks-aks/disaster-recovery>

- Automation Suite (OpenShift): <https://docs.uipath.com/automation-suite/automation-suite/2024.10/installation-guide-openshift/disaster-recovery>
- Automation Suite (AKS/EKS) multizone architecture: <https://docs.uipath.com/automation-suite/automation-suite/2024.10/installation-guide-eks-aks/deployment-scenarios>
- Standalone Orchestrator: <https://docs.uipath.com/orchestrator/standalone/2024.10/installation-guide/about-deployment>

Backup and Restoration

SaaS Services (Automation Cloud and Automation Cloud Dedicated): UiPath Automation Cloud employs High Availability Services and Disaster Recovery Services as part of its security controls. This service utilizes Azure's native resilience for all its components. To meet availability requirements, data processing environments are designed with redundancy and systems are equipped with failovers within availability zones. Regular backups are conducted in line with our documented backup and restoration policies. In case of any component failure, appropriate fail-safe measures are activated, and logs are recorded accordingly. The frequency of backups is determined based on UiPath policies.

Self-hosted Deployment Models (UiPath Automation Suite and Standalone Product deployment): For the self-hosted deployment options, UiPath provides the Customer with a complete set of capabilities that enable defining its preferred data retention policy and to meet all regulatory requirements. It is important to keep your database free from clutter.

UiPath Automation Suite supports backup and restore functionality across all deployment types to prevent data loss in various scenarios. You can configure a backup at any time after installation, and although optional, enabling it is strongly recommended to ensure recovery to a consistent state in case of a disaster. Velero, an open-source tool, is used to perform snapshot backups and restores for Linux (Embedded) and EKS/AKS deployments. For EKS/AKS, restoration is currently supported only to the same cluster, and if you choose not to install Velero, you should perform backups according to your Disaster Recovery policy. For OpenShift, customers must use their own backup and restore solution, following UiPath's documentation on best practices and maintenance mode.

With the standalone deployment of Orchestrator, UiPath provides optional backup and restore functionality using SQL Server Maintenance Solution

Refer here for information on backup and restoration procedures:

- UiPath Automation Suite (Linux): <https://docs.uipath.com/automation-suite/automation-suite/2024.10/installation-guide/backing-up-and-restoring-the-cluster>
- UiPath Automation Suite (AKS/EKS): <https://docs.uipath.com/automation-suite/automation-suite/2024.10/installation-guide-eks-aks/backing-up-and-restoring-the-cluster>
- UiPath Automation Suite (OpenShift): <https://docs.uipath.com/automation-suite/automation-suite/2024.10/installation-guide-openshift/database-maintenance>
- UiPath Orchestrator Standalone deployment: <https://docs.uipath.com/orchestrator/standalone/2024.10/installation-guide/maintenance-considerations>

Operational Monitoring

SaaS Services (Automation Cloud and Automation Cloud Dedicated): For the cloud operations and underlying cloud infrastructure, UiPath enables operational and security logs of activity in cloud environment. Operational logs are used for

monitoring uptime and availability of infrastructure and cloud software. Security logs are used for identifying security incidents, policy violations, fraudulent activity, auditing, and forensic analysis, supporting investigations, establishing baselines, and identifying trends and potential long-term problems. These logs are not exposed to customers but are used internally by UiPath to monitor cloud services. UiPath has Site Reliability Engineering (SRE) teams who monitor the services 24x7 using internal dashboards. A set of alerts are built on top of the security monitoring tools that collect logs from different components of the cloud environment. These alerts are configured to trigger appropriate incident management triggers. Incidents are managed according to the Incident management programs and teams analyze the incidents to perform RCA. Real-time details on uptime and incidents are available on the status portal for UiPath cloud services, ensuring transparency.

Self-hosted Deployment Models (UiPath Automation Suite and Standalone Product deployment): In the case of on-premises/ self-hosted solution, customer is responsible for monitoring the infrastructure and operational level logs. The monitoring stack for Automation Suite on EKS, AKS, and Linux includes Prometheus, Grafana, and Alert manager, which are automatically installed, unless customer chooses to bring your own monitoring stack in case of the AKS/EKS version. Additionally, Thanos is provided by default for Automation Suite on Linux to push the Prometheus matrix to an objectstore for persistence. Automation Suite on OpenShift does not include a monitoring stack; customers must use their own monitoring solution. For all Automation Suite deployment models, to effectively monitor the health of the services, customers can use the health endpoints provided in the documentation.

Details can be found in the documentation links below:

- Status portal for UiPath Automation Cloud: <https://status.uipath.com/>
- Trust Center Updates: <https://trust.uipath.com/>
- UiPath Automation Suite (AKS/EKS) Monitoring: <https://docs.uipath.com/automation-suite/automation-suite/2024.10/installation-guide-eks-aks/using-the-monitoring-stack>
- UiPath Automation Suite (Linux) Monitoring: <https://docs.uipath.com/automation-suite/automation-suite/2024.10/installation-guide/monitoring-automation-suite>
- UiPath Automation Suite (OpenShift): <https://docs.uipath.com/automation-suite/automation-suite/2024.10/installation-guide-openshift/health-endpoints>
- Standalone Orchestrator Logs: <https://docs.uipath.com/orchestrator/standalone/2023.10/user-guide/about-logs>

Incident Management

UiPath has an Incident Management Program that defines how incidents are documented, categorized, resolved, and reported. The Incident Response process addresses incidents related to security, availability, confidentiality, and other product issues. The program is approved by the management and communicated to all stakeholders. The program is reviewed at least once annually. For hosted (SaaS) services, in the event of a breach, we use security response plans to minimize data leakage, loss, or corruption. We provide transparency to our customers throughout the incident. Our 24x7 SRE and Security team is always on hand to rapidly identify the issue and engage the necessary development team resources to contain the impact of the incident.

Communications regarding maintenance and outage incidents in the Automation Cloud platform are posted here: <https://status.uipath.com>. Customers can sign up for notifications and alerts via their preferred communication method: email, text, ATOM, or RSS feed.

For a confirmed data security breach, UiPath will ensure notification to impacted customers without undue delay, and notification terms are governed by specific contracts with each customer.

With respect to the self-hosted deployment of the platform, the customer is responsible for implementing an incident handling capability for security incidents that include preparation, detection and analysis, containment, eradication, and recovery in accordance with their incident response policy

In both SaaS and self-hosted models, Product support is provided based on the support model offered. UiPath has 3 support models –Bronze, Gold, and Platinum support. For details on the support terms and support packages, refer to:

- <https://www.uipath.com/assets/downloads/support-terms>
- <https://www.uipath.com/support/packages-options>

Application Security Features

7. Application Security

User Authentication

User authentication for end-users in the platform is supported in multiple ways that are convenient for customers to configure and manage.

SaaS Services (Automation Cloud and Automation Cloud Dedicated): UiPath Automation Cloud supports local accounts (user's account and are internal to the UiPath Platform), invitation-based SSO (local account) model with Microsoft, Google, or personal emails, federated authentication with Microsoft EntraID (formerly Azure AD) and SAML 2.0 integration with other ID providers that support the same. The SSO integration options and federated sign-in options allow customers to enforce their corporate authentication rules, including MFA and password complexity. With federated sign-in models using Microsoft EntraID and SAML, passwords are not stored by UiPath. With the SSO models using Microsoft or Google accounts as well passwords are not stored in UiPath cloud but managed via the secure Auth0 services. Auth0 is responsible for the authentication process to the UiPath Automation Cloud and the management, and protection of authentication credentials user entities use. If a customer chooses to use local accounts (basic authentication via email and password), the password is hashed and salted by Auth0 using the bcrypt algorithm.

With UiPath Automation Cloud, customers can secure access to their organization and only allow users that are within their corporate network to access it by specifying the IP addresses that must be allowed and the service blocks all other traffic. Organization administrators can configure an organization access control policy to either allow access to all users in a directory or to restrict access to a specified list of allowed members.

Self-hosted Deployment Models (UiPath Automation Suite and Standalone Product deployment): UiPath Automation Suite and standalone Orchestrator support SSO with Microsoft EntraID, SAML model with ID providers that support the protocol, and basic authentication (which represent a local account). The SSO integration options and federated sign-in options allow customers to enforce their corporate authentication rules, including MFA and password complexity. For basic authentication, admin users can enforce their password complexity via the security settings in the solution.

With Automation Suite, customers can secure access to their organization and only allow users that are within their corporate network to access it by specifying the IP addresses that must be allowed and the service blocks all other traffic. Additionally, Organization administrators can configure an organization access control policy to either allow access to all users in a directory or to restrict access to a specified list of allowed members.

For more details, refer to below links:

- UiPath Automation Cloud authentication options: <https://docs.uipath.com/automation-cloud/automation-cloud/latest/admin-guide/authentication-settings#model-comparison>
- UiPath Automation Cloud – IP address restriction: <https://docs.uipath.com/automation-cloud/automation-cloud/latest/admin-guide/restricting-access-by-ip>
- UiPath Automation Cloud – access control policy: <https://docs.uipath.com/automation-suite/automation-suite/2024.10/admin-guide/restricting-organization-access-to-a-set-of-users>
- UiPath Automation Suite authentication options: <https://docs.uipath.com/automation-cloud/automation-cloud/latest/admin-guide/restricting-organization-access-to-a-set-of-users>
- UiPath Automation Suite – IP address restriction: <https://docs.uipath.com/automation-suite/automation-suite/2024.10/admin-guide/restricting-access-by-ip>
- UiPath Automation Suite – access control policy: <https://docs.uipath.com/automation-suite/automation-suite/2024.10/admin-guide/restricting-organization-access-to-a-set-of-users>

- Standalone Orchestrator Authentication options:
<https://docs.uipath.com/orchestrator/standalone/2024.10/user-guide/configuring-authentication-and-security>

Login Consent Configuration

Administrators can configure consent prompts or acknowledgement messages for users logging into the UiPath tenant. These prompts ensure that each user is informed about internal policies, such as the use of AI features, handling of specific data types as part of automation, or organizational compliance requirements, that they must consent to before accessing Automation Cloud. Up to 10 messages can be configured. Each prompt has a priority level, which determines the order in which prompts are shown to users during sign-in. Users must accept all active prompts to access the portal. If a user accepts some prompts but declines one, they are denied access. Users who choose to decline are prevented from logging in, but have the option to accept the consent if they reconsider. For record-keeping, admins have access to detailed logs for each consent interaction. These logs capture the identity of the logged-in user, the login date, whether they accepted or rejected the prompt, and the expiry date of an accepted consent.

Please see: <https://docs.uipath.com/automation-cloud/automation-cloud/latest/admin-guide/configuring-system-prompts>

Authorization and Centralized Access Management

With **both the self-hosted and the SaaS deployment options**, the roles and accounts are managed in a similar way and the customer is responsible for provisioning and managing the user accounts and roles in the platform.

UiPath Platform offers Role-Based Access Control capabilities empowering the Customer to use Unique Accounts, Roles and Permissions in order to create an Advanced Role Based Access Control Matrix. Roles in the platform use an access-control mechanism based on roles and permissions.

Roles are a collection of permissions and represent a more granular layer for managing user access, following the broader option of maintaining access through groups. Predefined groups and roles exist for easy setup, but customer administrators can also create custom ones if you want to apply a layered and flexible access scheme. Administrators can use existing role-based control and permissions or create new custom roles to an extremely granular level in order to manage user and robot access. The Administrator user can add roles to either a group so that all member accounts inherit them, or to individual accounts. A user gets the permissions required to perform particular operations through one or multiple roles. In Automation Cloud and in Automation Suite, roles can include several permissions at either the organization level, or at the service level, so there are:

- **organization-level roles:** these roles control the permissions that accounts have on organization-wide options; they are available in the Automation Cloud portal by default.
- **service-level roles:** these roles control the access rights and actions that accounts can perform in each UiPath service you own; they are managed from within each service and can include default roles which cannot be changed, as well as custom roles that can be created and managed in the service.

Accounts and groups typically have an organization-level role and one or more service-level roles. Admins can define new roles using a combination of permissions from one or multiple services within a tenant, ensuring tailored access control for their specific role needs.

Role management in the Orchestrator facilitates easy delimitation with permissions that apply on the tenant level and permissions that apply on the folder level.

There are three types of roles:

- **Tenant roles** include only tenant-level permissions, which grant rights in relation to the tenant resources.

- **Folder roles** include only folder permissions for working within a folder in Orchestrator.

Additional Access Management Capabilities in SaaS deployment models (Automation Cloud and Automation Cloud Dedicated):

Centralized access management provides customers with streamlined access management processes and enhanced customization capabilities.

- **Check access:** This feature provides enhanced visibility and control over roles and permissions at both service and tenant levels, as well as roles associated with folders. It offers a complete and accurate representation of access permissions for users across various areas of the platform. Moreover, it is also possible to export all the details on roles and permissions to a CSV file. This feature provides streamlined auditing of roles and permissions and boosts overall administrative efficiency
- **Export role assignments via API, or the UI:** Admin users can export roles and role assignments for all products and services across the platform via API, or via the user interface (UI). This feature simplifies audits, compliance, and reporting by providing a centralized view of role assignments across your environment.

For additional information regarding roles, please see:

- UiPath Automation Cloud – Managing Access: <https://docs.uipath.com/automation-cloud/automation-cloud/latest/admin-guide/managing-access>
- UiPath Automation Suite – Managing Access: <https://docs.uipath.com/automation-suite/automation-suite/2023.4/admin-guide/managing-access#assigning-roles-to-an-account>
- Standalone Orchestrator: <https://docs.uipath.com/orchestrator/standalone/2023.10/user-guide/accounts-and-groups#about-roles>

Credential Stores

For storing and managing Robot credentials and credentials to target applications (Assets) Orchestrator supports the use of multiple credential stores at tenant level. The Credential Stores can be used together with the native Orchestrator database, giving you control over how and where you store all credentials and assets in your Orchestrator instance. Beyond the secure stores with built-in support in Orchestrator (e.g. CyberArk, Key Vault, etc.), Orchestrator architecture supports the functionality of loading third party or developing custom plugins, enabling you to use any desired credential store. **SaaS and self-hosted options support this feature.** Additionally, with the SaaS services, for customers that do not allow direct connection from the cloud to credential stores or only want the credentials inside their trusted network, UiPath offers a credential proxy.

For more information, refer:

UiPath Automation Cloud: <https://docs.uipath.com/orchestrator/automation-cloud/latest/user-guide/about-credential-stores>

UiPath Automation Suite: <https://docs.uipath.com/orchestrator/automation-suite/2023.10/user-guide/about-credential-stores>

Orchestrator Credential Proxy: <https://docs.uipath.com/orchestrator/automation-cloud/latest/user-guide/orchestrator-credentials-proxy-installation>

Logs

For the platform, in case of **both self-hosted and SaaS services**, logging and monitoring capabilities are built into the software, which the customer can enable to capture informational events, error, and warning messages relevant to the application as well as audit trails for actions performed. The UiPath Platform provides strong logging capabilities. Logs keep track of all the important pieces of information like execution, error, warning, etc. that can help customers understand what's happening with their Robots, automations, and other services. The platform stores:

- **Robot Logs** that are generated by Robots during the execution of automation. For customized dashboard and reporting, user-defined workflows can be added in the workflows. To protect sensitive information that is logged during the execution of your automation at the Verbose level, you can choose not to log variable and argument values in both Orchestrator and Studio by using the secure flag in automation activities. UiPath currently maintains logs in accordance with GDPR best practice. Customer-accessible logs can be downloaded programmatically if longer storage is required.
- **Audit logs** generated by user actions in the platform for monitoring compliance and security. **Audit 2.0** is the unified and standardized audit platform for UiPath Automation Cloud. It provides a centralized, secure, and scalable way to track critical activities across all services—helping organizations stay compliant, detect security risks, and support investigations with ease. The data in the Audit page can be filtered by date and time, User, Category, Source, Action, Status (failure/success), IP address of the actor. Admins can view and manage audit logs at organization level and at tenant level.

Both the audit logs and the robot logs can be downloaded in a .csv format from the UI, in case of both the self-hosted and the cloud software. The platform also includes API for programmatic access to audit logs including the ability to query, retrieve and download audit events as a CSV file.

Capabilities specific to SaaS deployment options: Robot Logs within the Orchestrator tenant in Automation Cloud services can be exported to an Azure, AWS S3, or Google Cloud Storage account of the customer. In Automation Cloud Dedicated (SaaS), logs can also be exported to an Azure Storage Account managed within the dedicated environment. Customers can then direct the logs to a SIEM or data visualization tool of choice for deeper analysis capabilities.

Capabilities specific to on-premises deployment options: From robot logs perspective, with on-premises software, you can directly integrate logs to be ported to Elasticsearch and then to visualization tools such as Kibana, PowerBI, or Tableau or to other SIEM applications such as Splunk that support NLog format.

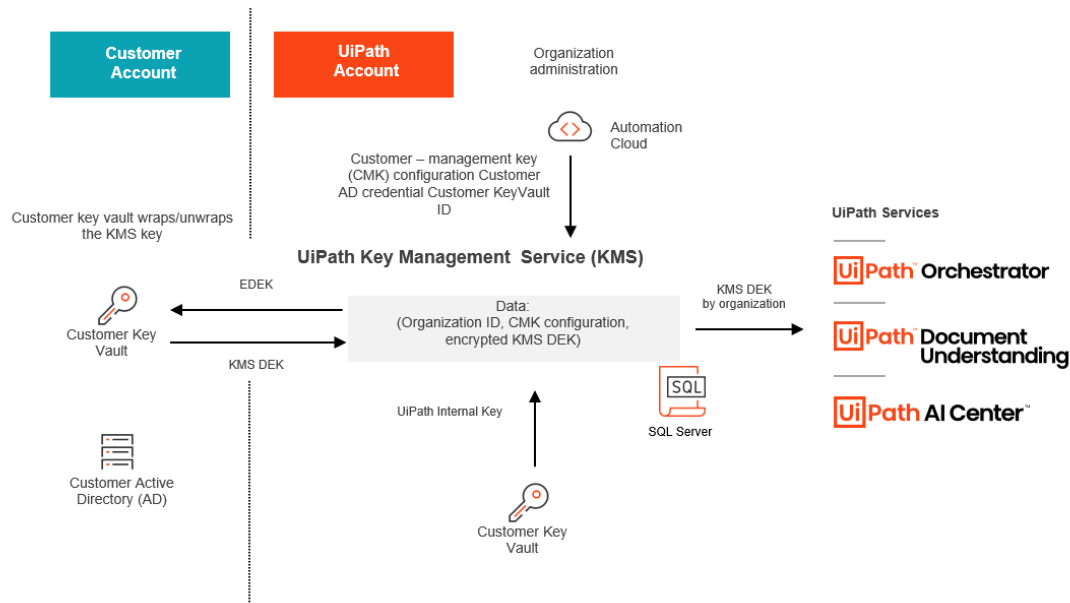
For more information on application-level logs, please refer to the links below:

- Robot Logs: <https://docs.uipath.com/robot/standalone/2024.10/user-guide/robot-logs>
- API for Log extraction: <https://docs.uipath.com/automation-cloud/automation-cloud/latest/api-guide/audit-logs>
- UiPath Automation Cloud Audit logs: <https://docs.uipath.com/automation-cloud/docs/about-logs>
- UiPath Automation Suite Audit Logs: [Automation Suite - Audit logs](#)
- UiPath Orchestrator Audit logs (standalone deployment): <https://docs.uipath.com/orchestrator/standalone/2023.10/user-guide/about-logs>
- Real time logs export: <https://docs.uipath.com/insights/automation-cloud/latest/user-guide/configure-real-time-data-export>

Encryption

UiPath Automation Cloud (SaaS): With UiPath Automation Cloud, UiPath enforces encryption in transit and at rest. All data at rest is encrypted using Transparent Data Encryption (TDE) which leverages AES 256-bit encryption. Beyond TDE, we also employ Application Layer Encryption (ALE) for most services. For services with ALE, either implicit or opted in for, customers have the ability to choose who handles the encryption key. It could be managed by either UiPath or the

customer. With UiPath managed keys, UiPath has internal procedures for key lifecycle management and monitoring. With Automation Cloud, data at rest is encrypted using AES_256 with TDE enabled. UiPath uses Azure Key vault, Cloudflare, and Azure App Certificate Service to manage the encryption keys. All keys are stored in a key vault dedicated to the customer. In case a customer chooses to use a customer-managed key, then the responsibility for managing the Key Encryption Key (KEK) is with the customer, supporting Azure Key Vault for the same. You can apply an extra layer of security to your customer-managed key by enabling a firewall in the Azure Key Vault, and only allowing UiPath services to access the CMK. Additionally, UiPath also support manual and automation key rotation. Manual key rotation involves changing the entire CMK configuration itself. While you could change the whole configuration, it is recommended to change only the key identifier, or key version, to minimize breaking changes. Automatic key rotation enables Automation Cloud to use the latest version of your key automatically, based on the rotation policy defined in Azure Key Vault.



Good to know:

This feature is only available if you are on the Enterprise licensing plan and requires the Advanced tier.

When choosing to manage your own keys, we recommend that you follow the [best practices](#) documented in UiPath Documentation portal.

For data in transit, communication between external systems and UiPath Automation Cloud is encrypted with ECDSA_P256 encryption with a SHA256ECDSA signature, a 6-month rotation, and accepting TLS 1.2 and TLS 1.3. Communications between services in the cloud platform are RSA 2048 encryption with a SHA256RSA signature, a 90-day rotation, and accepting only TLS 1.2+.

UiPath Automation Cloud Dedicated (SaaS): UiPath enforces encryption in transit and at rest. All communications inbound to the UiPath Platform services and products require at least TLS 1.2. Additionally, all data at rest is encrypted using Transparent Data Encryption (TDE), which leverages AES 256-bit encryption. In Automation Cloud Dedicated, encryption at rest is enabled by default for data stores such as SQL and Azure storage (Blob, disks, and files). Currently, UiPath manages the TDE protector as the default setting. UiPath creates, stores, and protects the keys used for encrypting your data. This is the default option, and it is automatically enabled. By default, key auto-rotation is enabled and occurs every 18 months. This operation only decrypts and re-encrypts the database encryption key. The system auto-updates the TDE protector with the latest key version found in Azure's key vault within 24 hours. The auto-updating

feature, combined with the regular, automatic protector rotation, provides an end-to-end zero-touch rotation system for the TDE protector. Customer-managed key is currently not available.

Self-hosted Deployment Models (UiPath Automation Suite and Standalone Product deployment): With the self-hosted delivery options (UiPath Automation Suite and standalone Orchestrator), the SQL Server is used by the Orchestrator to store configuration data for robots, users, roles, processes, and all other information managed through the Orchestrator, including data related to Queues and transactions. SQL Server is also used to store the Audit Logs and can be optionally used to store the Robot logs. All sensitive data that the Orchestrator stores in the SQL Server, such as Robot Credentials or Credentials stored as Assets, are encrypted at-rest using the AES_CBC_256 algorithm. Customers can choose to implement an additional layer of security to the data at rest in the SQL server using Transparent Data Encryption (TDE). Customers can also set up an encryption key per tenant. With Automation Suite, you can enable FIPS 140-2 enforcement on the machines on which you install Automation Suite

All the web services are TLS Enabled (supporting TLS 1.2+). The communication can be over HTTP or HTTPS with any of the Web Services and with the Web Application. The encryption type is AES_CBC_256. The customer should provide the SSL certificate. The certificate can either be a Domain certificate (generated by IIS for that specific domain, and that can be used only in that domain) or can be a web security certificate generated by a Certification Authority (like VeriSign).

For more information, refer to:

- Automation Cloud encryption: <https://docs.uipath.com/automation-cloud/automation-cloud/latest/admin-guide/encryption>
- Automation Cloud Dedicated: <https://docs.uipath.com/automation-cloud-dedicated/automation-cloud-dedicated/latest/admin-guide/encryption>
- UiPath Automation Suite - Encryption Key per Tenant: <https://docs.uipath.com/automation-suite/automation-suite/2024.10/admin-guide/setting-up-encryption-key-per-tenant>
- UiPath Automation Suite (Linux) Certificate Requirements: <https://docs.uipath.com/automation-suite/automation-suite/2024.10/installation-guide/certificates-overview>
- UiPath Automation Suite (AKS/EKS): <https://docs.uipath.com/automation-suite/automation-suite/2024.10/installation-guide-eks-aks/certificate-requirements>
- Standalone Orchestrator – encrypting SQL Server: <https://docs.uipath.com/orchestrator/standalone/2024.10/installation-guide/encrypting-the-sql-server>
- Standalone Orchestrator Certificate Requirements- <https://docs.uipath.com/orchestrator/standalone/2024.10/installation-guide/certificate-considerations>

API Security

UiPath API implementation is based on the OData protocol. OData (Open Data Protocol) is an ISO/IEC approved, OASIS standard that defines a set of best practices for building and consuming RESTful APIs. The Open Data Protocol (OData) enables the creation of REST-based data services, which allow resources, identified using URLs and defined in a data model, to be published and edited by Web clients using simple HTTP messages. This specification defines the core semantics and the behavioral aspects of the protocol. All API requests and responses to and within the services are encrypted using TLS 1.2+.

Authentication is supported via multiple ways; each tailored to different scenarios and use cases:

- **Personal Access Tokens: (Applicable only for UiPath Automation Cloud)** Personal Access Tokens are a convenient way for individual users to access our platform programmatically. These tokens act as a secure bridge between your applications and our API. Users can generate and manage their tokens through their user

preferences, allowing fine-grained control over the data they can access. Personal Access Tokens are ideal for scripts, automated tasks, or small-scale integrations.

- ▶ **OAuth 2.0 for External Apps (Applicable to SaaS and on-prem versions of UiPath platform):** OAuth 2.0 is designed for third-party applications seeking access to our platform on behalf of users. It facilitates secure authorization without exposing user credentials. External apps can register with us, obtaining client credentials that identify them. This method is recommended for larger integrations and applications accessing multiple users' data. With Automation Cloud, External Client APIs can be used to automate client secret rotation for external applications. This helps meet security requirements by reducing the risks associated with secrets used on a long term, or with manually rotated secrets. The APIs allow to list and manage OAuth external client applications, create, update, and delete secrets for OAuth external applications, and generate secrets using fine-grained scopes.

For more details, please refer to links below:

- UiPath Automation Cloud API Guide: <https://docs.uipath.com/orchestrator/automation-cloud/latest/api-guide/consuming-cloud-api>
- UiPath Automation Cloud – External Client APIs: <https://docs.uipath.com/automation-cloud/automation-cloud/latest/api-guide/external-client>
- UiPath Automation Suite API Guide: <https://docs.uipath.com/orchestrator/automation-suite/2024.10/api-Guide/about-odata-and-references>
- Standalone Orchestrator API Guide: <https://docs.uipath.com/orchestrator/standalone/2024.10/api-Guide/authentication-methods>

8. AI Features and Integrations in UiPath

UiPath provides automation solutions empowered by cognitive and artificial intelligence (AI). UiPath builds, partners, and integrates AI functionality into our product.

Specialized AI is AI that is trained and suited for a specific purpose. These models excel at performing predefined tasks within their specialized area, such as data extraction. They are tailored and optimized for efficiency and accuracy within their narrow scope. It doesn't carry the broad cognitive abilities of humans and can't easily adapt to tasks outside its training without further adjustments.

Generative AI is a type of artificial intelligence that can understand content and create new content, such as text, images, or music, by learning patterns from existing data. **Large language models (LLMs)** are a type of generative AI that are trained on huge amounts of text, like books, articles, and websites in order to understand and generate human-like text. LLMs can help with tasks like answering questions, writing essays, translating languages, and chats. A popular example of LLM is ChatGPT.

UiPath offers both specialized and generative AI capabilities in the following ways:

1. **Specialized AI models in UiPath:** UiPath offers proprietary, specialized AI models for enterprise automation, enhancing the automation of documents, screens, tasks, and processes. Examples are UiPath Document Understanding data extraction models for specific document types and Communications Mining models for emails and tickets. Products that have specialized AI/ML capabilities are:
 - i. **AI Computer Vision:** specialized AI for UI element detection on screens
 - ii. **UiPath IXP-Document Understanding:** Pretrained ML models for extracting data from 35+ different document types, such as invoice, passports etc., and for classifying documents for their types. Please note that Document Understanding also comes with generative AI capabilities described later.
 - iii. **UiPath IXP-Communications Mining:** Various unsupervised and supervised models including large transformer-based model responsible for generating embeddings used by other models, Unsupervised multi-membership clustering models to identify commonly occurring intents and requests, Supervised models responsible for intent and entity recognition. Please note that Communications Mining also comes with generative AI capabilities described later.
 - iv. **Task Mining:** Specialized model designed around clustering screenshots of desktop activities and used to auto-merge traces. Task Mining will analyze the steps and actions and define what to merge and where to add decision points. You can edit the merged results if you need to align them with your expectations.
 - v. **AI Center:** Infrastructure and application for deploying and retraining specialized ML models in UiPath. AI also has various out-of-the-box specialized ML models such as for language translation, object detection, etc. Please note that as UiPath continues to enhance its AI capabilities through alternative and more advanced approaches, the platform is undergoing [phased deprecation of AI Center models](#).

Key aspects of these models are:

- Specialized AI models available in UiPath are trained with data/documents that are very specific to the task that they are intended to perform. For example, a Document Understanding model for extracting data from invoices is trained on multiple invoice documents, enabling the AI model to identify and extract key fields from the document.
- These models do not generate any content of their own.
- The out of the box, pretrained specialized ML models are proprietary to UiPath and are built and maintained by UiPath
- In most cases, customers can retrain the out-of-the-box models using their own dataset to deploy custom models specific to their use.

2. **Generative AI powered capabilities in UiPath Products:** UiPath provides GenAI enhanced product capabilities that improve developer productivity as well as augment existing product capabilities. Products that support GenAI capabilities are:
 - i. **UiPath IXP-Document Understanding:** Generative Extraction, classification, validation, and annotation.
 - ii. **UiPath IXP-Communications Mining:** Generative Annotation, Extraction, Zero-shot discovery, and Conversational Filters (Autopilot).
 - iii. **UiPath IXP-Generative Extraction for Unstructured & Complex Documents:** **generative AI experience for extracting data from complex unstructured documents such as contracts and lease agreements.**
 - iv. **Autopilot for Developers** enhances productivity for developers of all kinds. 'Text to workflow' transforms descriptions easily into automated workflows, reducing complexity, particularly for non-technical users. 'Text to expressions' generates expressions using natural language descriptions, allowing developers to focus on the problem at hand rather than syntax.
 - v. **Autopilot for Testers** accelerates every phase of the testing lifecycle. Generate tests from requirements, generate automation test code and surface actionable insights from execution results.
 - vi. **Autopilot for Apps** allows developers to quickly build Low-Code Apps with natural language, screenshots of legacy applications, or PDF forms.
 - vii. **Autopilot for Everyone** is an AI companion that helps you tackle your daily task list. It is an AI assistant for work that knows you and your context. It can complete tasks, run automations in context, process documents, run and even help build your own automation.
 - viii. **GenAI Activities:** GenAI Activities in Integration Services allow customers to use pre-built Generative-AI based activities for Context Generation, Summarization of text, PII filtering, Language Detection, Rewriting, Generation of email, and translation.
 - ix. **Agents:** They are software workers that can plan, act, learn, and adapt - making them ideal for processes that require judgment, flexibility, and contextual awareness. They are powered by LLMs and are designed to operate in dynamic, non-deterministic environments. They use natural language instructions (prompts), along with context grounding and tools to accomplish the goal defined by the user.
 - x. **Healing Agent:** Healing Agent is an AI-powered capability designed for intelligent self-healing of UI-based automations. It works across UiPath Robots, Orchestrator, and Studio to reduce automation downtime and enhance efficiency.
 - xi. **Task Mining:** Audio capture allows you to conveniently provide additional context around each step via voice input. This helps the Business Analyst when reviewing the task graph and the collected data.

Key aspects of these GenAI capabilities in UiPath products are:

- ▶ GenAI powered capabilities in UiPath products leverage **UiPath managed 3rd party LLMs** via the AI Trust Layer and UiPath in-house LLMs in certain features of UiPath Document Understanding and UiPath Communications Mining.
- ▶ GenAI capabilities leveraging UiPath managed third-party LLMs are currently not retrainable. Data will be sent through UiPath LLM Gateway to the third party LLM model. UiPath is making sure that the data sent to the LLM model is never stored by the third-party model. UiPath agreements with third-party LLMs prevent UiPath customer data retention. Data is sent securely via transit to the third-party model provider, but data may not be used for training, logging, or monitoring.
- ▶ **UiPath LLMs (in-house):** UiPath DocPath and CommPath are the underlying LLMs used to power certain GenAI features in Communications Mining and Document Understanding, respectively. DocPath LLM and CommPath LLM do not go through the AI Trust Layer, and all security-related aspects pertaining to the GenAI features powered by these LLMs are managed directly within the services themselves (i.e. - within Communications Mining and Document understanding, respectively)
- ▶ Using custom LLMs with Agents: With LLM Configurations in AI Trust Layer, customers can 1) Bring their own Subscription or 2) Bring their own LLM.
- ▶ **Autopilot** leverages some additional specialized ML models specific to it, as well as Document Understanding and Computer Vision. For generative AI capabilities, Autopilot leverages the UiPath AI Trust Layer similar to all other

UiPath products leveraging generative AI. This means that while Autopilot uses a variety of AI/ML services on the backend, they have the same level of security control as our other products

3. **Integration with Generative AI services:** UiPath facilitates direct API-based integration with third-party LLMs via UiPath Integrations Service. This is supported in two ways:
 - ▶ **Using Custom LLMs for Agents:** Customers can use the LLM Configurations capability in AI Trust Layer to bring their own models for use in Agents instead of using the UiPath-managed LLMs. This is supported through the following approaches:
 - a) Bring your own LLM subscription: Customers can replace UiPath-managed AI subscriptions with their own, provided the model matches the supported family and version. This option gives the customer complete control over AI usage and costs—while still benefiting from the scalability, security, and integration of the UiPath Platform.
 - b) Bring your own LLM: Customers can use any LLM that meets UiPath compatibility standards. With the OpenAI V1 Compliant LLM connector, they can easily integrate models from any inference provider following the OpenAI API format. A simple probe call ensures the model is ready to power AI agents within the UiPath Platform.
 - ▶ **Using Connectors Within Automation Processes:** Customer can use **Integration Service connectors** to connect to *customer-managed third-party LLMs*, in which case the integration is direct with the third party LLM through APIs, not managed via AI Trust Layer. Prebuilt Connectors are available to third party GenAI technologies such as Open AI, Google PaLM2, Azure OpenAI, Amazon Sage Maker, and more, using UiPath Integration Service. Customers also can build connectors for others that customers may prefer.

Securing AI Integrations in UiPath

UiPath does extensive security testing on all services provided, including the AI capabilities. Specialized ML models such as Document Understanding ML models and Computer Vision are not prone to the same issues as LLMs or generative AI models such as Bias or Information Disclosure. They are designed to solve a specific problem rather than being predictive and generative in answering a scope of problems. As such, the development of these specialized AI models is governed by UiPath's security and privacy teams along with the various compliance and governance standards enforced by UiPath as a whole. From a product perspective, UiPath offers various security capabilities in its products to support security and privacy when using specialized AI features. These include logical segregation of data between customers, RBAC (Role-Based Access Control), encryption keys per tenant, and logs. The customer has complete control over the data sent for retraining the model (if retraining is supported), data sent at runtime for processing, and how the data output from the AI is used in the automation workflow.

Generative AI is a powerful technology; however, it requires guardrails to get the most value out of it. This is why UiPath has invested in a robust AI security framework through the AI Trust Layer. UiPath has a Responsible AI Committee that includes members from Security, Privacy, Legal, and Product teams to govern the company's implementation of generative AI tools.

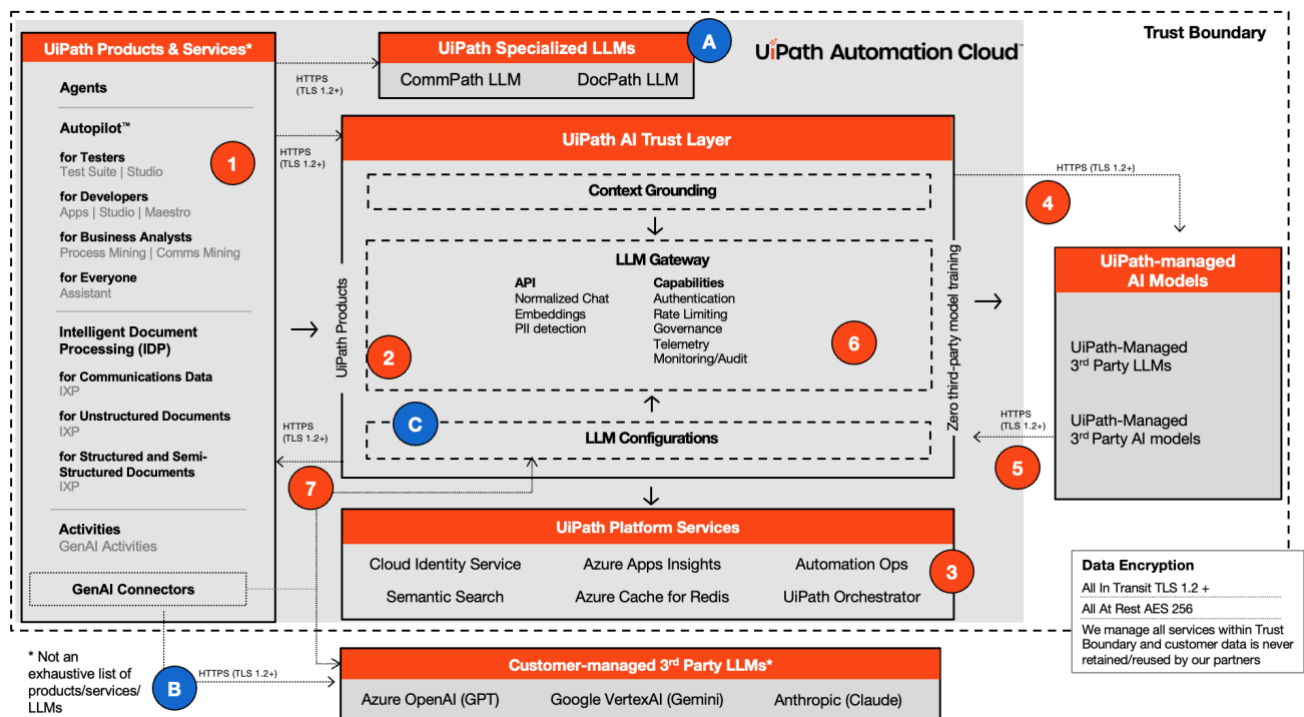
UiPath allows for: the use of UiPath-managed third-party LLMs -or- the use of customer-managed 3rd party LLMs.

- UiPath managed 3rd party LLMs are leveraged via the UiPath AI Trust Layer, which provides a governance and security control point.
- Customer Managed 3rd party LLMs are leveraged via integration activities where UiPath is only providing the means to easily connect to a customer-implemented LLM. The connectors/ activities do not use the AI Trust Layer but execute requests directly to their respective cloud services. Consequently, the security of data processed within these LLMs is solely the responsibility of the customer.

The UiPath AI Trust Layer allows contextualized customer data, and customer interactions with UiPath products, to securely flow to trusted, UiPath-managed third-party large language models (LLMs), i.e. UiPath private subscriptions to the models or services. It enables transparency, trust, and control over the interactions between GenAI, your organizational data, and third-party LLMs.

Data flow

The diagram on the next page details the AI Trust Layer architecture and how the data flows through:



The UiPath AI Trust Layer includes capabilities such as (but not limited to):

- **Usage auditing:** Visibility into GenAI feature usage distribution through UiPath managed GenAI models as well as your connected models. Inputs and outputs available may vary by product.
- **GenAI feature governance:** Administrative controls (i.e.- being able to disable specific GenAI features and LLMs) and usage at a tenant, group, and user level.
- **A set of filters ensuring proper use of the LLMs (e.g., harmful content filtering):** This is automatically built into, and enabled on, all third-party models. Please see the ‘Harmful Content Filtering’ section of this handbook for more details.
- **LLM gateway:** A centralized and secure proxy service in which all customer data sent to LLMs is confidential, load-balanced, and adheres to defined data governance policies. As part of the UiPath Trust Boundary, UiPath

has taken measures to ensure customer privacy by disabling logging of customer data or adhering to features that prevent storing such data.

UiPath has released a new, growing set of GenAI functionality into its platform designed to help developers be more productive, and companies see more value faster from their automations.

UiPath upholds the highest standards of data privacy, customer experience, and automation performance. UiPath LLM Gateway is a backend secure proxy server designed to maintain data privacy and compliance while load balancing and routing LLM requests from these GenAI features to a variety of UiPath-managed LLMs.

In-platform AI controls

Policies in UiPath Automation Ops can be used to centrally manage all third-party AI features used across UiPath products. These policies allow you to specify exactly which products can access third-party AI models and deploy them to the appropriate audience with granularity at the tenant, group, or user level. This ensures you maintain full control over feature usage while minimizing potential exposure.

Policies can be managed at multiple levels:

- A. Product level:** You can disable/enable calls to 3rd party LLMs, or disable/enable it only for specific products;
- B. Feature level:**
 - a. Inputs/outputs for audit purposes: You can specify if you would like to save inputs/outputs for audit purposes. Once this feature is disabled, the inputs/outputs will no longer be stored and will not appear in the audit log, and cannot be recovered later by UiPath;
 - b. PII In-Flight Masking (enabled on a product level): PII In-Flight Masking allows for the pseudonymization of PII before the input is sent to LLMs when using UiPath's Generative AI features. This masking occurs before the data reaches the LLM, ensuring that no raw PII is processed. Once the response is received from the LLM, rehydration takes place—replacing pseudonymized tokens with the original PII entities. You can also specify which PII entities to detect and filter, and configure confidence thresholds for each entity type to control detection sensitivity.

Please note: No data is logged by UiPath or the model provider in the PII masking process. This is currently available for the following products, with additional products being onboarded over time.

 - Agents
 - GenAI Activities

Please note: Similar to the PII masking GenAI activity, the PII in-flight filtering is only applied to text-based inputs (i.e.- this will not cover documents, images, etc.) in the products listed above.
- C. Model level:** You can specify what models are allowed to be used in your organization. When models are enabled, you are accepting their terms of use. A priority can be set on each policy to decide what policy should be applied if a user is set to receive multiple policies.

All of these policies can be deployed at a **tenant** level, a **group** level, or an **individual user** level.

Agentic Security

Agentic automation applies AI agents' autonomous decision-making capabilities to business process automation. Unlike traditional automation that follows predefined rules, agentic systems understand context and objectives, allowing them to adaptively handle complex workflows while making informed choices about process execution.

Agents & Agent Builder

Agent Builder experience in Studio Web provides a guided experience for automation developers and business users to build, evaluate, and publish agents, and is the foundation for agentic automation. While agents can operate autonomously to perform their tasks, they remain constrained by the parameters defined for them within Agent Builder.

For the latest information around UiPath Agents and Agent Builder, please consult the **UiPath AI Trust Layer (AITL), GenAI, and Agentic Security Handbook**, available upon request.

Context Grounding

Context Grounding allows you to bring in your data to generate more accurate, reliable GenAI predictions, and is designed to make your business data LLM-ready without the need for any additional subscription to embedding models, vector databases, or large language models (LLMs). You can create representative indexes and embeddings of business data that UiPath GenAI features can reference for contextual evidence at runtime.

Context Grounding is a tenant-scoped platform service designed to support UiPath GenAI experiences (such as GenAI Activities and Autopilot for everyone) by grounding your prompts with relevant information before they are executed by the LLM via retrieval augmented generation (RAG).

For more details around how Context Grounding works, please refer to the official documentation [here](#).

Maestro (Agentic Orchestration)

In the context of maintaining controlled agency, agentic orchestration is crucial for governance because it ensures AI-driven processes operate within defined rules, compliance requirements, and organizational oversight.

By orchestrating different agents, the system ensures that each component—whether AI-driven, rule-based, or human—performs tasks at the right time, in the right sequence, with proper oversight. This prevents duplication, enforces governance policies, and enables smooth transitions between automated and human-led tasks.

From a governance perspective, Agentic Orchestration ensures clear accountability, auditability, and policy compliance across AI-driven processes.

Autopilot

Autopilot is a set of AI-powered experiences designed to automate and streamline various day-to-day tasks. Its diverse functionalities handle both general productivity and department-specific tasks across an array of business areas.

Autopilot understands the context of various elements like documents, screens, communications, and processes, and performs actions accordingly.

Autopilot provides different experiences, tailored to the specific needs and requirements of different user personas. For more information regarding capabilities and functionality for each Autopilot available, please refer to the following links:

- Autopilot for Developers - [Documentation](#)
- Autopilot for Testers - [Documentation](#)
- Autopilot for Everyone - [Documentation](#)

Continuous monitoring of AI models

Regular security and risk checks are performed for all AI models used as part of the provided services.

The performance and maintenance of the UiPath LLMs are regularly monitored by the UiPath team (to prevent bias and model drift).

Although the performance of the third-party LLMs are managed and maintained directly by the LLM providers themselves, the performance of the LLMs are still monitored by the UiPath team.

In both cases, it is the customer's responsibility to ensure that the performance of the model(s) used are suitable for their use case on an ongoing basis.

Ethics & responsible AI

Harmful content filtering is automatically applied on all AI models going through the AI Trust Layer, to ensure end-users are not exposed to potentially harmful AI-generated content.

All models used are stateless, so any previously processed data is not accessible. This helps to ensure that all users interacting with the AI model do not gain access to unauthorized information by querying the model.

All employees and contractors of UiPath regularly receive mandatory compliance training on the use and development of Generative AI.

Additionally, UiPath takes a cautious approach to ensure security and governance to AI Systems and relies on the responsible AI development principles. When integrating third-party AI components, UiPath performs due diligence to assess the third-party technology's security posture, secure development practice, ethical practices, data handling procedures, and commitment to avoiding bias and discrimination.

More details on UiPath's responsible AI principles can be found [here](#).

Responsible AI Principles

UiPath takes a cautious approach to ensure security and governance of AI systems and relies on responsible AI development principles. UiPath is committed to meeting the needs of customers and has the following guiding principles and approach to building AI solutions tailored for the enterprise environment: open, flexible, and responsible. These principles are developed and maintained by a Responsible AI Committee that includes representation from throughout UiPath to ensure that they are applied appropriately to AI technologies deployed by UiPath as well as those developed by UiPath directly.

We believe in the power of responsible AI, and are guided by the following principles:

- (i) **Safeguards for data protection.** AI systems should be designed, developed, implemented, and used with a strong focus on protecting personal data, to foster trust and demonstrate commitment to respecting privacy rights.
- (ii) **Human -centricity and transparency.** AI systems should employ guardrails and tests that can account for uncertainties in AI models, flagging issues, and requesting human review when necessary.
- (iii) **Technical and security robustness.** Security should be at the core of any AI system implementation, to ensure the reliability, stability, and protection of AI systems against technical failures, vulnerabilities, and malicious activities.
- (iv) **Empowering digital education and upskilling.** AI systems should be leveraged to enhance the effectiveness of upskilling initiatives while equipping individuals with capabilities to navigate through AI technologies with dedicated training initiatives. It is our view that AI systems need to be assessed in view of sound and reasonable principles, and we consider it our duty to further promote these to our partners and customers.

Please refer here: <https://www.uipath.com/assets/downloads/responsible-ai-principles>

For more information regarding AI usage in UiPath products, refer to the below links:

- **Specialized Document Understanding Models:** <https://docs.uipath.com/document-understanding/automation-cloud/latest/user-guide/out-of-the-box-pre-trained-ml-packages>
- **Specialized Communications Mining Models Explained:** <https://docs.uipath.com/communications-mining/automation-cloud/latest/developer-guide/how-machines-learn-to-understand-words-a-guide-to-embeddings-in-nlp>
- **DocPath:** <https://www.uipath.com/blog/ai/generative-ai-trained-for-document-processing>
- **CommPath:** <https://docs.uipath.com/communications-mining/automation-cloud/latest/user-guide/overview>
- **Gen AI Activities:** <https://docs.uipath.com/activities/other/latest/integration-service/uipath-uipath-airdk-about>
- **UiPath Integration Service:** <https://docs.uipath.com/integration-service/automation-cloud/latest/user-guide/introduction>
- **AI Trust Layer Governance Policies:** <https://docs.uipath.com/automation-ops/automation-cloud/latest/user-guide/settings-for-ai-trust-layer-policies>
- **UiPath Generative AI Security Handbook:** Detailed architecture of the AI Trust Layer and a deep dive into specific dataflows for products using Generative AI capabilities are available in a dedicated security handbook.

9. Data Governance and Privacy

Data Residency

UiPath customers have the flexibility to choose where their data is stored.

Self-hosted Deployment Models (UiPath Automation Suite and Standalone Product deployment): In the case of the self-hosted options, the customer chooses to host the software and its associated data within their own infrastructure. Therefore, the customer can decide where the data center hosting the solution will be physically located.

UiPath Automation Cloud (SaaS): In the case of UiPath Automation Cloud (multi-tenant SaaS), customers can choose a region for their tenant from UiPath supported regions based on their requirements. Based on the licensing plan opted, Customers have complete control over establishing their tenancy in the UiPath cloud within the jurisdiction that best aligns with their business needs. Data and services are hosted in regions **(not specific countries)**. A region can span multiple data centers and physical locations.

Please note that upgrading your license plans may have an impact on the regions based on your upgrade path. Therefore, consider the following with respect to the regions supported and used under different licensing plans.

Data Residency for Unified Pricing and Licensing

Data residency for Automation Cloud organization and tenants	Community	Free	Basic Trial	Basic	Standard Trial	Standard	Enterprise
Cloud organization regions	European Union only	European Union only	European Union only	European Union only	Inherited	Inherited	Inherited (can be changed)
Tenant regions	European Union only	European Union only	European Union only	European Union only	One region inherited from the organization	One region inherited from the organization	Inherited for Default Tenant (can be changed)
							<div> <i>NOTE:</i> Multiple regions are available for new tenants. </div>
Max. number of tenants	1	1	1	1	Unlimited	Unlimited	Unlimited

Available regions for services: UiPath provisions and processes cloud data in the region where each service is hosted. Available Regions for Tenant-level Services are Australia, Canada, European Union, India, Japan, Singapore, Switzerland, United Arab Emirates, and United Kingdom. Not all services are available in all regions. You can create multiple tenants in different regions under the same organization to access services that are not available in your primary region.

Before you check the data residency of each service, keep the following in mind:

- Products are provisioned either at the tenant level or the organizational level.
- When a product is available in a region, UiPath stores and processes data mainly in that region. Note: Some services might process data beyond their designated storage region. However, no data is stored outside the services' respective region.
- If a product uses AI-powered features, data may be temporarily routed to a nearby region where a specific model is available. UiPath does not store data in the routed region.

UiPath also supports delayed update regions, currently supporting United States and European Union. Delayed Update Organizations receive updates at least 14 days after they are deployed to standard Enterprise environments.

Also important to note is that **UiPath Automation Cloud™ Public Sector** is hosted in U.S. government cloud and has received the authorized status in FedRAMP. UiPath Automation Cloud™ Public Sector will bring more value to federal agencies who want the ease and flexibility of a secure and compliant cloud-based platform.

Refer here for more information on regions available in UiPath Automation Cloud:

Data Residency in UiPath Automation Cloud: <https://docs.uipath.com/automation-cloud/automation-cloud/latest/admin-guide/data-residency-cloud>

UiPath Automation Cloud Dedicated (SaaS): Automation Cloud Dedicated allows you to select the Azure cloud region where your data is stored. When onboarding, choose the cloud region where you want to deploy your Automation Cloud Dedicated instance. Some Azure regions may have limited features or hardware availability, such as GPU, and as a result, we may not be able to deploy Automation Cloud Dedicated instances to those regions. For more information on Azure regions availability, contact your UiPath account team.

Data Isolation

Self-hosted Deployment Models (UiPath Automation Suite and Standalone Product deployment): In case of the self-hosted options, the entire infrastructure is managed by the customer and dedicated to the specific customer. If a customer chooses to model the solution to accommodate their organizational structure (e.g., multiple business units, different departments etc.), then the platform also supports multi-tenancy which provides logical segregation of data within the platform.

UiPath Automation Cloud (SaaS): With Automation Cloud multi-tenant SaaS deployment, multiple customers share the underlying infrastructure, including the database. Data from each tenant is logically separated from others in our service. Unique key per customer is used for data encryption for services with application-level encryption enabled. Data encryption is enforced at the application level for sensitive information such as passwords, queues, etc. Additionally, all data stored in the database is then encrypted again using transparent data encryption (TDE). Additionally, customer-managed keys are supported for some services allowing customers to manage the key encrypting key for their tenant. We enforce access and authorization control inside our services to data belonging to each tenant. For users to gain access to the cloud account, the Authentication of Automation Cloud is integrated with the ID platform (IDP) enabled via Auth0. Auth0 is a cloud-based authentication service with adherence to best-in-class compliance frameworks. All user accounts and application accounts are tied to a customer identity that serves as a separate domain. All accounts are added or invited by the initial admin account created by the customer. Each Orchestrator Service has its own RBAC and with the tenant management in our Automation Cloud, we map each tenant in Automation Cloud to their unique Orchestrator level tenant (service), giving a seamless experience to our end customers. UiPath support operates on the principle of least privilege and has no access to the environment unless first approved by the customer.

UiPath Automation Cloud Dedicated (SaaS): It is a single tenant SaaS offering with dedicated compute and data resources managed by UiPath same as our Automation Cloud offering. This provides complete data isolation with logically isolated cloud resources provisioned exclusively for the customer's tenant. Isolation is achieved with separate storage, compute, and networking and with strong access controls and dedicated encryption keys per customer.

Data Retention and Destruction

With the Automation Cloud (SaaS) services, UiPath manages the data retention based on predefined retention policies. Customer data entered in the Automation Cloud is maintained for the life of the contract, plus a sufficient period of time (usually at least 30 days, regardless of the amount of data) after termination or expiration thereof to allow for deletion from back-ups and the performance of UiPath's rights under the applicable law.

For some components, such as Queues and Processes in Orchestrator, the data retention policy can be directly configured via the application to either use the default data retention policy configured in the application or use a custom retention period as required. Audit logs are retained for 2 years. Customers may also download logs in csv format for longer storage in their local storage.

Should you close your account with UiPath, or otherwise request data deletion, we delete that data from our systems after the requisite 30-day soft-delete period. During the licensing period and at the end of contract, customers may export data from cloud services using APIs or place a data export request with UiPath support. Robot Logs and Backups are maintained for 30 days.

With the self-hosted deployment options (UiPath Automation Suite and standalone deployment), customers can control and manage the data retention for the entire data stored by the platform. At the database level, managing data retention involves scheduling backup and cleanup activities to remove old data and logs periodically. For some components, such as Queues and Processes in Orchestrator, the data retention policy can be directly configured via the application to either use the default data retention policy configured in the application or use a custom retention period as required.

Recommended best practices for these activities are provided in the online documentation here:

- UiPath Automation Suite (AKS/EKS)
<https://docs.uipath.com/automation-suite/automation-suite/2023.10/installation-guide-eks-aks/database-maintenance>
- UiPath Automation Suite (Linux)
<https://docs.uipath.com/automation-suite/automation-suite/2023.10/installation-guide/database-maintenance>
- UiPath Orchestrator (Standalone deployment)
<https://docs.uipath.com/orchestrator/standalone/2023.10/installation-guide/maintenance-considerations>
- UiPath Orchestrator (UiPath Automation Cloud) – Process Data Retention
<https://docs.uipath.com/orchestrator/automation-cloud/latest/user-guide/process-data-retention-policy>
- UiPath Orchestrator (UiPath Automation Cloud) – Queue Item Retention Policy
<https://docs.uipath.com/orchestrator/automation-cloud/latest/user-guide/queue-item-retention-policy>

Data Classification

With both on-premises and SaaS deployments, the customer is the data controller, which means that the customer is responsible for the types of data that are collected and processed within the UiPath Platform.

In the case of self-hosted deployment options (e.g., UiPath Automation Suite and standalone product deployment), no data is transmitted to, stored, or processed by UiPath. The customer is responsible for classifying its own data in risk tiers and maintaining security measures. UiPath provides necessary security features and capabilities such as encryption, session management, access control management etc., which the customer can use to secure the data at the application level.

In the case of UiPath Automation Cloud (SaaS) services, UiPath has no knowledge of or access to the customer's data. For signing up or creating accounts in Automation Cloud, email address (used as username) and password are required. No other PII/PHI/cardholder data is required by default. The customer is responsible for provisioning and de-provisioning its authorized users of the UiPath cloud. UiPath does not collect, store, process or transmit any other forms of PII data by default. The type of data processed or stored in the service is determined by the customer, and dependent on the customer's automation requirements and how they design and use these automations. From UiPath's perspective, UiPath classifies all customer data stored in cloud as **Confidential** and maintains the highest security measures for data storage, processing, and handling. This commitment extends across various facets, including robust application-level security controls, encryption mechanisms, and adherence to established security and operational standards, as shown in UiPath's SOC 2® and HIPAA reports.

Personal Data: In its capacity as a data controller, the customer is responsible for collecting, handling, maintaining and governing personal information input by the customer when using UiPath cloud products in accordance with GDPR and the customer's own internal policies and procedures. If customers use personal data with UiPath cloud products, they will be processed on the customer's behalf by UiPath adhering to the data processing agreements and GDPR standards.

Health Data: The cloud platform does not require any health data to be stored or processed by default. Where the use of health data is allowed by UiPath in the appropriate legal documentation, the transfer of health data to UiPath can only take place if a Business Associate Agreement has been signed by the Parties.

Cardholder Data: UiPath is not a service provider with respect to the Payment Card Industry Data Security Standard (PCI DSS), and UiPath does not have a PCI DSS Report on Compliance (ROC)/Attestation of Compliance (AOC). UiPath contractually prohibits customers from transmitting, storing, or processing cardholder data (CHD) or sensitive authentication data (SAD) in the UiPath cloud. Also note that the UiPath cloud is not a payment application and is not subject to the Payment Application Data Security Standard (PA-DSS).

Refer here for details:

- Standard Data Processing Agreement (DPA): <https://www.uipath.com/assets/downloads/dpa-cloud>
- Standard Business Associate Agreement (BAA): <https://www.uipath.com/assets/downloads/business-associate-agreement>

Data Collection

When customers use UiPath cloud products, UiPath processes different types of data in order to provide you with the product functionalities, to ensure the reliability of the products you use and to improve them so you get better products and services and more efficient automations.

This means that, depending on the products you use, UiPath will process and sometimes store data that you use to design and run your automations. Please refer to the detailed [documentation here](#) to understand how customer data is used based on the product/ services that you use.

UiPath implements data minimisation, masking wherever possible, and deletes the data at the latest at contract termination. Customer **can opt-out during contracting or by raising a support ticket**.

Please note: Healthcare customers (with a BAA) are excluded from using their data for secondary purposes such as product improvement.

Use by LLM providers: UiPath has established agreements with all managed third-party LLM providers ensuring that no customer data is retained or used for model training.

Refer here for details:

- Standard MSA: <https://www.uipath.com/assets/downloads/mssa>
- Legal Terms: <https://www.uipath.com/legal/trust-and-security/legal-terms>
- Customer data usage with cloud products: <https://docs.uipath.com/overview/other/latest/overview/customer-data-usage-with-cloud-products>

10. Compliance

UiPath has numerous certifications and attestations in place to provide customers with the confidence and support needed in meeting security and compliance standards.

Name of the Certification or Attestation	Details
ISO/IEC 27001, ISO/IEC 27017, ISO/IEC 27018	UiPath maintains an ISO/IEC 27001 certification. UiPath's ISMS has been augmented with additional criteria found in ISO/IEC 27017 and ISO/IEC 27018.
ISO 9001	UiPath's quality management system (QMS) is audited annually for conformity with the ISO 9001 standard.
SOC 1	UiPath has engaged an independent certified public accounting firm to examine controls that may be relevant to a customer's internal control over financial reporting (ICFR) in accordance with American Institute of Certified Public Accountants (AICPA) System and Organizational Control (SOC®) 1 guidance.
SOC 2	UiPath has engaged an independent certified public accounting firm to examine controls relevant to American Institute of Certified Public Accountants (AICPA) Trust Services Criteria for security, availability, and confidentiality relevant to the UiPath cloud offerings and issue SOC 2® reports.
Health Insurance Portability and Accountability Act (HIPAA)	Under HIPAA, UiPath acts as a business associate to covered entities and other business associates. HIPAA attestation provides independent assurance to customers and business partners that UiPath has designed and implemented administrative, physical, and technical safeguards applicable to UiPath's business as a cloud service provider.
HITRUST®	HITRUST CSF® v9.6.2 Risk-based, 2-year (r2) certification status demonstrates that UiPath has met demanding regulatory compliance and industry-defined requirements and is appropriately managing risk. This achievement places UiPath in an exclusive group of organizations worldwide that have earned this certification.
Cyber Essentials Plus	Companies undergoing annual Cyber Essentials Plus audits help reduce the level of cyber security risk in the UK government supply chains. The Cyber Essentials Plus scheme defines a set of controls which, when properly implemented, will provide organizations with basic protection from the most prevalent forms of threat coming from the internet. UiPath has engaged a certification body authorized by IASME to audit UiPath UK Limited annually against UK National Cyber Security Centre (NCSC) technical requirements for IT infrastructure and issue a Cyber Essentials Plus certificate.

NHS Data Security & Protection Toolkit (DSPT) Self-assessment	<p>UiPath UK Limited has submitted its 2023/2024 National Health Service (NHS) Data Security & Protection Toolkit (DSPT) self-assessment and has met the standards. The DSPT allows organizations to measure performance against the UK National Data Guardian's ten data security standards. Annual submission of the DSPT self-assessment provides assurance that UiPath is practicing good data security, and that personal information is handled correctly.</p>
FedRAMP® Authorized Impact Level: Moderate	<p>UiPath Automation Cloud Public Sector has achieved the Authorized status from the Federal Risk and Authorization Management Program (FedRAMP®). Available on the FedRAMP Marketplace, the UiPath Platform can be used to securely and transparently process data, speed operations, and empower government workers. UiPath offers FedRAMP-certified core management, governance, analytics, idea capture and management, and support for self-hosted automations on-premises or in the cloud. UiPath also offers public sector agencies continuous testing capabilities for apps and automations.</p>
ISO/IEC42001	<p>UiPath has officially achieved ISO/IEC 42001 certification the world's first international standard for Artificial Intelligence Management Systems (AIMS). This certification demonstrates our commitment to responsible, ethical, and secure AI practices. ISO 42001 provides a structured framework for managing AI systems throughout their lifecycle covering governance, risk management, transparency, and compliance.</p>
IRAP	<p>UiPath has completed the IRAP (Information Security Registered Assessors Program) assessment. IRAP consists of a set of requirements listed in the Australian Government Information Security Manual (ISM) which is produced by the Australian Cyber Security Centre (ACSC). These requirements are assessed by an independent third party to evaluate our security posture.</p>
C5 (Cloud Computing Compliance Controls Catalogue)	<p>C5 is a government-backed attestation framework, which was introduced in Germany by the Federal Office for Information Security (BSI). C5 helps companies demonstrate operational security against common cyber attacks within the context of the German government's "Security Recommendations for Cloud Providers" guidelines. C5 is a mandated requirement in Germany for those providing cloud services to government agencies, applicable to any service provider inside or outside of Germany. UiPath's C5 Type 2 attestation demonstrates our commitment to providing security assurance and transparency to our German customers.</p>
ENS (Esquema Nacional de Seguridad)	<p>ENS is a set of security controls and standards that are required to be implemented by government agencies, public organizations, and service providers that process data for public services in Spain. Spain's National Security Schema (ENS) establishes a uniform set of requirements, promotes continuous security management, and offers a reference for effective security posture. Under the Spanish Royal Decree 3/2010, ENS is a compulsory requirement for central government customers in Spain. UiPath has undergone an independent ENS audit report of UiPath Automation Cloud services.</p>

UiPath continuously works to improve quality and security standards and design an internal roadmap of assurance and standards relevant to, and adequate for the industry in which UiPath operates.

Please visit the Trust portal to access certifications and attestation reports: <https://trust.uipath.com/>

11. Third Party Security Integrations

UiPath and CrowdStrike have teamed up to make human and robot work more secure than ever. Endpoint protection platforms protect your organization when people put you at risk of a breach. UiPath and CrowdStrike were the first to accept the challenge of delivering EDR for a world where humans and robots work side by side.

With this integration:

- UiPath Robots can now connect seamlessly to the CrowdStrike Falcon agent
- Security teams can monitor robot actions and outcomes in the Falcon dashboard
- Security teams can accurately identify and track source of malicious activity to automation robots in addition to human-initiated activity
- It is possible to quarantine compromised hosts without impacting broader automations or hosts, to ensure business continuity in the event of an incident

Benefits of the integration:

- Extended security posture for your organization
- Business continuity for your robot workforce
- Improved visibility and analysis capability for your security team
- Seamless technical integration included in:
 - ▶ UiPath Robot 2021.10+
 - ▶ Falcon Insight (EDR) 6.33+
 - ▶ Optional: UiPath Orchestrator 2021.10+
- No additional licensing costs for customers of UiPath and CrowdStrike with the above integration

Refer here for more information: <https://docs.uipath.com/robot/standalone/2024.10/user-guide/crowdstrike-integration>

12. Conclusion

UiPath is committed to upholding the highest standards of data security, privacy, and compliance. We live up to this mission through a combination of platform design, service-design principles, and security and compliance best practices. The culmination of these efforts is the UiPath Platform, a solution that is scalable and offers complete flexibility in deployment and security for customers. Customers can adopt built-in platform security features such as customer-managed keys, credential stores, access control, logging, and automation governance controls. UiPath serves its customers by implementing relevant, measurable, and industry-recognized information security and quality assurance frameworks, including ISO/IEC 27001, ISO/IEC 27017, ISO/IEC 27018, ISO 9001, ISO/IEC42001, IRAP and FedRAMP®, as well as independent assurance through SOC 1®, SOC 2® and HIPAA attestations. Transparent disclosure represents an additional layer of assurance accessible to all UiPath customers. This includes the sharing of SOC 2® reports, HIPAA reports, and ISO certificates with customers. For more information, please reach out to your UiPath account team or contact the UiPath team [here](#).

Revision History

Date	Version	Author	Description
September 2024	1	Gayathri Narayanan, Ken Czajkowski, Adrian Petrisoia, Constantin Badea, Lucian Ionescu, Matthew Rodger, Kevin Mooney, Emilian Ionescu	First Version
April 2025	1.1	Sebastian Ungureanu	Added section on Agentic Security
August 2025	1.2	Kevin Mooney	Added MFA Guidance as Appendix

About UiPath

UiPath (NYSE: PATH) is on a mission to uplevel knowledge work so more people can work more creatively, collaboratively, and strategically. The AI-powered UiPath Platform combines the leading robotic process automation (RPA) solution with a full suite of capabilities to understand, automate, and operate end-to-end processes, offering unprecedented time to value. For organizations that need to evolve to survive and thrive through increasingly changing times, UiPath is The Foundation of Innovation™.

© 2005–2025 UiPath. For informational purposes only. All rights reserved.

13. Appendices

Appendix 1: UiPath Robots — Guidance for Handling Multi-Factor Authentication

Multi-Factor Authentication, often referred to as MFA, refers to a security measure put in place that requires more than one type of authentication in order to be authenticated. Most commonly, MFA is broken up into three types: something you know, something you have, and something you are. A security system may require any combination of these authenticators or multiple instances of the same factor. Often referred to as out of band authentications, the more secure implementations of MFA also require that these authentications are performed via different devices or different protocols.

There are many advantages to leveraging multiple factors of authentication. Multiple credentials are much harder to steal, making it much more difficult for an attacker to impersonate a legitimate user. This is especially true of authentications done out of band as it requires an attacker to compromise more than just the user's computer. There is greater assurance that the user authenticating is in fact the user who should have access. Passwords combined with other factors of authentication do not need to be as complex, as long, or changed as frequently to achieve the same level of assurance compared to when they are used by themselves.

Many of these same advantages pose a challenge for Robotic Process Automation (RPA) as MFA is designed in part to prevent an attacker from being able to impersonate a user via code, exactly what RPA tries to emulate. To that end, there are a number of strategies or options that can be leveraged to address MFA when using UiPath robots.

OPTIONS FOR ALL MFA Types

- **Option 1 (most preferred by customers), complex single-factor authentication with frequent rotation:** In certain cases, the option to reduce the requirement for authentication to only be a single-factor is an option. The downside being that a less secure entry point is created. To compensate for this added risk, often mitigating factors can be added such as IP-filters, extremely long passwords, or even building regular password changes into the automation workflow. While a human may have difficulty remembering a 100 character long password that changes every minute, a robot does not. Starting in 2019.10, UiPath offers a pluggable credential vault system for credentials stored in Orchestrator. This allows customers to use a wide variety of privileged access managers to automate password rotation and governance. By implementing long, complex, and frequently changing passwords, customers can effectively create a random generated token similar to that of a Yubikay or Oauth token as a compensating control.
- **Option 2, attended robots:** One option for all RPA implementations is to use attended robots for automations. The robot pauses its work when authentication must be performed, allowing the user to perform that function, and continue the process later. The downside of this is that the attended robots are inherently less efficient than unattended robots as they can only be executed when the user triggers them. This also means that the robot requires human supervision and is unable to run behind a locked screen.
- **Option 3, bypass via API call or admin access:** Most MFA systems offer a way to issue a token that can be used in place of the actual authentication mechanism. Vendors frequently refer to this as a bypass token or a static token. Normally this mechanism is used by an administrator to allow users who have lost their physical device for receiving a MFA code to login temporarily. Robots can leverage the same mechanism to create a just-in-time (JIT) authentication scheme where a robot creates a code and then the same robot or a separate robot leverages the code to login. Ideally, this can be implemented out of band of the actual robot performing the login to maintain separation of powers.

Knowledge Based Security Questions are predefined questions and answer sets that can be asked in addition to username and password. They can be predefined questions such as “What is your mother’s maiden name?” or “What was the make and model of your first car?”. They can also come as free-form questions that the user enters.

- **Option:** The easiest way to handle these type of questions is to treat them the same as username and password credentials where the username is the question and the password is the answer.

SMS-Based Authentication is where a security system sends a random code, often numeric, to a cellular phone where the code must be retrieved and entered by a user.

- **Option:** There are a wide number of VOIP systems that can be accessed via a browser or installed application. This allows the robot to obtain the code via a get text activity and enter it in order to complete the authentication. The speed of delivery can sometimes be an issue with this scenario as SMS delivery, especially to VOIP can be variable. To avoid re-use or phishing, these tokens expire after a certain period, so if the robot cannot retrieve the token and enter it in time, the authentication has to be restarted.

Interactive Voice Recording (IVR) Authentication is where an automated recording calls a user and speaks a random code to them that must then be entered to authenticate.

- **Option:** Similar to handling SMS-based authentication, there are a wide number of VOIP systems that can be accessed via a browser or installed application. Many of these include a visual voicemail feature, enabling the code to be retrieved and entered. Accuracy of Visual VoiceMail can sometimes be an issue for this option, causing the bot to enter the wrong code.

Physical Random-Number Token Authentication comes in a wide variety of options. They are generally small devices that have a calculator type screen that can fit on a keychain. The most common of which are RSA SecurId or Oauth based tokens that have a number, usually 6 digits, that changes on a regular schedule, usually 1 minute or less. Users are asked to enter the number or code displayed. Sometimes a Personal Identification Number or PIN is required in addition to that code such as with RSA.

- **Option 1 (Partial/Full Solution):** Leverage a virtual token, sometimes referred to as a soft token, rather than a physical one. Almost every vendor that sells a physical token also sells a virtual version that can be installed as an application on a computer. The Virtual token will display the code after entering some form of authentication, generally a PIN. A Robot can use a *get text activity* to copy the code as it would do for any other application. Not every company has both physical and virtual offerings. As well, many of these vendors require separate licenses for the two different options. Specifically for Okta, Microsoft, and Google tokens, UiPath offers activities to allow robots to leverage these software tokens. See <https://marketplace.uipath.com/listings/two-steps-authentication-component?searchId=561ebe7f-0ef5-4596-ab7b-a1c3074cca54>
- **Option 2 (Partial Solution):** Generate a list of one time use or time-sensitive codes out of band of the authentication. Most token vendors provide a mechanism to allow administrators to provide static codes to users in lieu of them using the code provided by the physical token. This is to allow a user a way to login in case they lost their token and are unable to get a new one right away. Often times, a list of codes can be generated for use as each code can only be used once. In this scenario an administrator or a separate robotic process generates a list of codes and enters them as a queue in orchestrator for the robot logging in to leverage. This could all be done by a single process, but it is generally preferred from a strictly security perspective to have a separation of powers between processes. Employing this option requires that there is access to the system issuing the codes which is often a problem if the customer is working with a third party application. Additionally, codes must be replenished at the same rate in which they are used.

Smart Card Authentication is a way to issue users a certificate and keypair securely so that they can perform authentication via Public Key Infrastructure (PKI). Smart Cards can be physical cards that have a chip that is read by a computer. They can also be virtual where the information is installed as part of an application or in a protected chip such

as a Trusted Platform Module (TPM) or a Hardware Security Module (HSM). Whether virtual or physical, the authentication process is essentially the same. The user enters a Personal Identification Number (PIN) that provides access to the private key portion of the certificate / key-pair. The certificate is then presented as part of a mutual-TLS authentication. Organizations that typically issue only physical Smart Cards, likely have a virtual offering for devices such as Smart Phones or Tablets where physical cards are not feasible, but heavy involvement with the security team will be required to leverage these as they are not standard.

- **Option 1:** ***This option requires a virtual smart card installed on the machine or a physical smart card issued to the robot where the robot is installed on a machine with a smart card reader. Additionally, both robot and orchestrator must be version 2018.4 or later***. Orchestrator web.config is configured to allow smart card authentication. When the robot is created or configured in Orchestrator, check the box for Smart Card Pin and store the PIN there rather than entering the username and password. The robot can leverage this PIN for initial login as it would username and password. The robot can also use the get credential activity if the PIN is needed for additional logins.
- **Option 2 (Partial or Full Solution Depending on Vendor):** If the robots are required to be installed on virtual machines and the smart card private key must still be installed on a hardware chip, not software, then a Hardware Security Module or HSM can be deployed as a solution. Currently, only the ThalesTCT Luna Credential System and nShield HSMs support end to end login for robots. Other HSM solutions can be leveraged for logging into applications or websites, but cannot be used today to have the robot perform the remote console or remote desktop login. In this solution, the private key is stored in an HSM and the robot leverages the key by supplying a PIN to access it. The connection to the HSM is typically done by vendor specific middleware and leverages a type of API call referred to as a PKCS#11 connection. Secrets such as the PIN can be stored as a credential or credential asset in Orchestrator depending on exact configuration.

*Note neither Option 1 or Option 2 are currently supported for High Density (HD) Robots for Windows Login. This is due to the Robot RDP library not supporting smart card login.

Recommendations and Factors to Consider

As mentioned in the introduction, MFA is designed in part to prevent login without the presence of a human. Customers looking to leverage unattended robots should consider what the login requirements are. This whitepaper lays out several potential solutions for various types of MFA, but does not look into the legal or ethical considerations. Customers must look closely at the terms of use and other legal contracts in place for using applications they may want to automate. If an application is third party to the customer and requires MFA, automating or bypassing MFA may violate an existing agreement.

Identity and access management implementation is an area of IT that often varies wildly from one implementation to the next. Like much of security, it is constantly evolving to mitigate an ever growing threat landscape and meet the needs of IT. No one solution will work for every company, but the usage of a privileged access manager to provide governance and rotation of credentials has proven to be the best option so far. While imitating MFA for the purpose of a robot logging in may be necessary to perform some automations due to solution limitations, it defeats the core principles behind having MFA in the first place and reduces security overall. The industry is moving towards just in time access as the leading mechanism to secure logins. A robot having a credential that changes at the speed of a robot matches that paradigm and therefore is recommended.

Appendix 2: UiPath Automation Cloud — Security Configuration Guide

1. Functional Security

These are built-in capabilities of Automation Cloud that enforce security in how users interact with the system.

- Audit Logging: Enable and review regularly: [Automation Cloud - About logs](#)
- Authentication Models: Choose local accounts, directory accounts, or hybrid; enforce MFA: [Automation Cloud - Understanding authentication models](#)
- Access Control Features: [Automation Cloud - Restricting access by IP](#), enforce [Automation Cloud - Session policy](#), least privilege [Automation Cloud - Roles](#)
- Data Encryption: UiPath-managed keys or customer-managed keys, TLS/HTTPS, review settings: [Automation Cloud - Encryption](#) and [Automation Cloud - ALE with customer-managed keys](#)
- Let's Encrypt Certificate Authority (CA): [Automation Cloud - Certificates](#)

2. Authentication & Identity Management

These settings determine how users prove who they are and how directory/user identities are handled: [Automation Cloud - Understanding authentication models](#)

- Use Directory accounts via a trusted IdP when possible.
- Enable Multi-Factor Authentication (MFA) where supported.
- Review inactive accounts regularly.
- Manage user/group provisioning to reduce mistakes.

3. Access Control & Authorization

Ensuring users have the right permissions: [Automation Cloud - Roles](#)

- Roles & Role Assignments: Use built-in roles; create custom roles only when necessary.
- Manage Accounts & Groups: Keep membership up to date; remove unused accounts.
- Least Privilege Principle: Assign only required permissions.

4. Firewall & Network Domain Whitelisting

For strict network rules or proxies, allow certain domains for Automation Cloud:

- Whitelist required domains for services [Automation Cloud - Configuring the firewall](#), and [Studio - Services Studio Connects To](#) and [Robot - Configuring networking settings](#).
- Handle region-specific domain for customer-managed key [Automation Cloud - Configuring the firewall](#).

- Monitor changes to domain/IP lists from UiPath [Orchestrator - Orchestrator Outbound IP Addresses](#).

5. SAML / Single Sign-On (SSO) Configuration

For organizations on the Enterprise plan, SAML SSO offers centralized identity control.

Prerequisites: [Automation Cloud - Configuring the SAML integration](#)

- Enterprise license
- Admin permissions in both Automation Cloud and the IdP
- Compatible versions of UiPath Studio/Assistant

Limitations & Risks:

- Encrypted SAML assertions may not be supported.
- Some functionality (API access, searching directory users) may be limited.
- Update signing certificate in case of rotation.

6. Credential Store Integration

For organizations that wish to utilize their existing Credential Store instead of UiPath

Prerequisites: [Orchestrator - Integrating credential stores](#)

UiPath comes with built-in support for several major secure stores:

- CyberArk CCP (Central Credential Provider)
- CyberArk Conjur Cloud (read-only)
- Azure Key Vault (read/write and read-only modes)
- HashiCorp Vault (with multiple authentication methods, read/write & read-only)
- BeyondTrust Password Safe (Managed Accounts; Team Passwords)
- Thycotic Secret Server
- AWS Secrets Manager
- Google Secret Manager

Additionally, Orchestrator supports **third-party or custom plugins** so you can add your own vault/secure store by implementing a plugin.

7. Data Encryption & Audit Logging

Protect data at rest, in transit, and ensure traceability of actions

- All external communication use TLS 1.2+ by default and by design.
- Use UiPath-managed or, for more control, customer-managed keys: [Automation Cloud - Encryption](#) and [Automation Cloud - ALE with customer-managed keys](#)

- Enable audit logging, capture critical actions: [Automation Cloud - About logs](#)
- Automatically export logs and define retention policies and secure logs with SIEM to prevent alteration: [Automation Cloud - Exporting logs](#)

8. Data Residency, HA/DR strategy, Compliance & Governance

Understand where your data lives and what regulations apply:

- UiPath Automation Cloud has various security attestations and certificates. All UiPath security documents can be downloaded at [UiPath Trust Center | Powered by SafeBase](#).
- Know your tenant's region and data storage location: [Automation Cloud - Data residency](#)
Under NDA, UiPath can provide more detailed operational security info through your account manager.
- High availability and disaster recovery strategy including recovery time objective (RTO) and recovery point objective (RPO): [Automation Cloud - High availability and disaster recovery strategy](#)
- **RTO:** Less than or equal to four hours.
- **RPO:** Less than or equal to 15 minutes.

9. Best Practices Checklist

- Review and disable/remove all inactive user accounts.
- Define and enforce least privilege via roles/groups.
- Choose UiPath managed keys or customer-managed keys.
- Set up Single Sign-On / SAML where possible.
- Enable Multi-Factor Authentication (MFA) for all users.
- Restrict access by IP and/or set up session policies.
- Whitelist required domains and outgoing connections.
- Ensure all communication is encrypted (TLS) and data at rest is encrypted.
- Enable audit logging, define retention policies, and regularly review logs.
- Understand your data residency and compliance obligations.
- Monitor UiPath's updates to required domains/IPs/certificates.
- Document your security policies accordingly.
- Obtain all security documents from UiPath [Trust Center](#) and subscribe to updates.

Appendix 3: UiPath Automation Suite — Security Configuration Guide

1. Security and Compliance Principles

- All data transmitted between components is protected (TLS/SSL).
- Installations may be online or offline / air gapped. In air-gapped setups, you must host container images and binaries locally.
- Use least privilege for network access, containers, namespaces, etc. [Automation Suite - Security and compliance](#)
- Strong identity and access management: external identity providers, directory integration, role-based access, SSO. [Automation Suite - Understanding authentication models](#)

2. Deployment & Infrastructure Security

- **Network Policies and Kubernetes Security**
 - Use Kubernetes Network Policies (or equivalent, e.g., with your CNI) to enforce least-privilege network access between namespaces and services.
 - Gatekeeper and OPA policies are preconfigured in some deployment profiles; if you bring your own, ensure you align with UiPath's hardened policies.
- **FIPS 140-2 Compliance (when needed)**
 - If you require FIPS compliance (Federal or high-security environments), enable FIPS 140-2 on the host nodes *before* installation (or follow steps if enabling afterwards) for Automation Suite 2023.4+.
 - Ensure certificates used are FIPS-compatible; replace self-signed ones if needed.

3. Identity, Access, and Authentication

- **Authentication Models**
 - *Local accounts model*: Users are managed within Automation Suite.
 - *Directory accounts model*: Integration with external identity providers (Active Directory, SAML 2.0, Microsoft Entra ID, etc.), which supports SSO, directory search, and possibly automatic provisioning.
- **Host-level vs. Organization-level Settings**
 - Many authentication/security settings are inherited from the *host* level but can be overridden per organization.
- **Basic Authentication vs. Directory/SSO**
 - You can allow or restrict basic (username/password) authentication. Best practice is to rely on directory/SSO when possible.
 - Even when basic auth is disabled, you may allow system administrators to have basic access as a fallback or emergency.
- **Password and Account Policies**

- Enforce password complexity: include digits, lowercase, uppercase, special characters as your security policy demands.
- Minimum length, expiration, and prevention of reuse.
- Account lockout policies: configure number of failed login attempts, lockout duration.

4. Application / Component Security and Process Apps

- **Process App Security for Process Mining**
 - Use `app_security_mode` setting in `input.json`: options include `system_managed` (default — better for least privilege), `single_account`. [UiPath Documentation](#)
 - `system_managed` ensures each process app has its own SQL user; passwords are rotated per use. Requires SQL Authentication. [Automation Suite - Configuring process app security](#)
- **Blobs, Pre-signed URLs, Storage**
 - Disable use of pre-signed URLs for S3 if not needed. Rotate storage credentials.
- **Kerberos / SQL Authentication**
 - If using Process Mining with SQL Server, ensure proper roles are assigned (server roles like `securityadmin` or equivalent, database roles such as `db_owner`, `db_securityadmin`, `db_accessadmin`) for the provisioning user.

5. Host / Org Administration

- **Configuring Organization Security Settings**
 - Admins can customize security settings from the UI under *Admin* → *Security Settings*. These include email settings, audit logging, password policies, etc.
- **Audit Logs / Logging**
 - Enable audit logs for critical actions (user / group changes, security settings changes, login attempts, API usage). [Automation Suite - Logs](#)
- **Basic Authentication Controls**
 - As above, manage basic authentication settings at host, organization, or account level. Ensuring least access and fallback options. [Automation Suite - Allowing or restricting basic authentication](#)

6. Certificates, Encryption & Transport Security

- Use TLS for all component communications. Enforce minimum TLS version, strong cipher suites.
- Replace self-signed certificates with CA issued certificates. This is especially important for production, and particularly when using FIPS modes. [Automation Suite - How to address weak ciphers in TLS 1.2](#)

7. Operational Security & Lifecycle

- **Secure Development and Patch Management**
 - Keep the platform updated, with security patches applied for both OS, Kubernetes stack, and UiPath components.

- **Monitoring & Alerts**
 - Use built-in tools or integrate with your external monitoring/alerting systems for detecting anomalous behavior, node/pod failures, certificate expiry, etc. [Automation Suite - Monitoring Automation Suite](#)
- **Backups / Disaster Recovery**
 - Use regular backups and test restores. For high-availability deployment, design accordingly (multi-node, redundant components). [Automation Suite - Configuring the backup store](#)

8. Additional Guidelines / Best Practices

- ✓ Principle of least privilege everywhere: services, network, identity.
- ✓ Minimize the attack surface: disable or don't install unused components.
- ✓ Use dedicated namespaces in Kubernetes. Use proper segregation.
- ✓ Document security policies and ensure they are enforced by configuration, not manually.
- ✓ Regularly audit your security settings and user accounts.
- ✓ Obtain all security documents from UiPath [Trust Center](#) and subscribe to updates.