The UiPath Automation Cloud: Security, Privacy, and Compliance

Revised January 2021

Executive summary

The **UiPath Automation Cloud** is a great option for customers who want to start delivering Robotic Process Automation (RPA) quickly then scale up over time, with enterprise-scale manageability and optimization from day one.

The security of any and all data associated with your RPA projects is of the upmost importance to UiPath, no matter whether you choose Automation Cloud or alternative options such as on-premises installation or deployment to a 3rd party cloud.

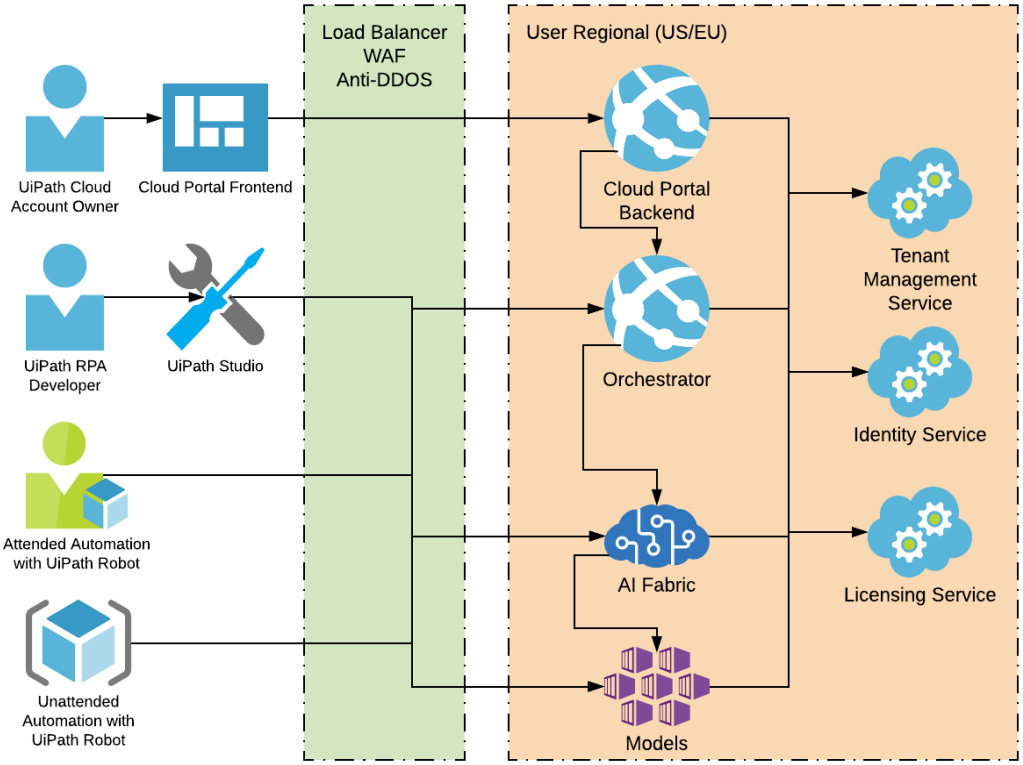
In this whitepaper, we focus specifically on the Automation Cloud service design principles and practices related to security, privacy and compliance.

Our commitment

UiPath goes to great lengths to ensure that data related to your RPA projects remains safe and secure.

When using the UiPath Automation Cloud, your data will benefit from multiple layers of security and governance technologies, operational practices, and compliance policies enforced by UiPath.

UiPath Automation Cloud: design



Data Encryption	Identity and Access	Data Isolation
Package Identity	Privacy	Data Sovereignty
System Hardening	Secure Development	Service & Data Availability
Live Site Testing	Security Incident Response	Production Acecss Control
Secrets Management	Network Isolation	

The UiPath Automation Cloud is composed of multiple independent services, such as Cloud Portal, Tenant Management Service, Licensing Service, and Orchestrator, among others.

To provide a seamless experience, we work hard to abstract these details from the end user. We offer these services through a common front-end called the UiPath Cloud Portal.

Before delving into the details surrounding UiPath's approach to security, privacy, and compliance, we first need to provide some background about the key services in the Automation Cloud.

.

Cloud Portal

Cloud Portal serves as the first entry point for our customers to create an account for their organization. Customers can also:

- Invite additional users and manage their roles and permissions
- Request licenses for robots
- Set up orchestrator service instance(s) for their development, testing, and production needs

Orchestrator

The UiPath core platform's server-side component is known as Orchestrator. It allows customers to manage their entire RPA infrastructure from one central control plane. If you are a current on-premises or 3rd party cloud customer, you are familiar with the functionality and interface.

We now provide a seamless experience for existing and new customers by integrating UiPath Orchestrator into the heart of our cloud offering.

There are two variations of the Automation Cloud. Customers who choose the free **UiPath Automation Cloud for community** receive a unique tenant on an instance of Orchestrator shared with other customers. Customers who choose the more feature-rich **UiPath Automation Cloud for enterprise** can have multiple tenants within their single enterprise cloud instance, enabling them to manage multiple RPA environments from within their cloud. Although this instance is also shared with other paying customers, strict virtual separation ensures that no customer ever has access to any other customer's data or configuration.

If you would like to see this experience for yourself, we invite you to try this out at any time with the trials at UiPath.com.

Additional documentation on Orchestrator can be found on our website.

AI Center

UiPath's cognitive services platform is called AI Center. AI Center allows Automation Cloud users to deploy and manage machine learning models within the Automation Cloud. RPA developers can easily integrate their RPA automations with the models to extend a robot's ability to perform complex tasks.

Additional documentation on AI Center can be found on our website.

Tenant Management Service

Each customer is represented as a tenant in the UiPath Automation Cloud. Each tenant can map their organization's internal structure and corresponding users using the tenant

management capabilities. This offers customers the flexibility needed for governance of RPA projects.

Tenant Management Service is decoupled from our portal and offers isolation in the backend while delivering a seamless user experience to the customer.

Licensing Service

The underlying mechanism that keeps track of licenses issued, activation status for robots, and run-time checks on usage is packaged as an independent service that interfaces with Cloud Portal, Orchestrator and the other services.

Identity Service

User identity is managed by a central service in the UiPath Automation Cloud. Users log into the system using either an external identity provider or through a UiPath Automation Cloud account. The UiPath identity service then combines the externally managed user identity with UiPath user and tenant information. This internal identity is used to identify users when they enter the UiPath Automation Cloud and to identify users between the components.

Service-design principles

All of the above services are packaged together as UiPath Automation Cloud and delivered via a Software-as-a-Service (SaaS) model that's built and hosted in Microsoft Azure. They all use core Azure services, including compute, storage, networking, SQL database, app configuration, secret storage in Key Vault, and identity and access management.

This allows us to focus on the unique aspects of running UiPath's services while taking advantage of, and building upon, Azure's state-of-the-art capabilities in security, privacy, and compliance. We also utilize the industry certifications available through Azure.

At UiPath, we share the responsibility of protecting your data with Azure, and strictly adhere to the guidance they publish.

Data encryption

We encrypt all customer data at rest in any data store that is part of our service. For example, we use transparent data encryption in SQL databases.

All data is transmitted over protected channels, whether it travels over the Internet or within our internal service components.

Identity and access management

We support account creation in the Automation Cloud using a variety of identity service providers, such as Google, Microsoft, and LinkedIn, as well as through native accounts. Post account creation, our services manage a given user's access rights using application-managed, role-based access control checks.

Our on-premises customers have long used Orchestrator's roles-based account control (RBAC). With the introduction of tenant management to the Automation Cloud, we now have similar RBAC controls there to provide a seamless experience for our customers.

Tenant data isolation

Data from each tenant is logically separated from others in our service so that we can enforce access and authorization controls for all tenants as they access data inside our service.

Package integrity

Starting with the 2019 fast-track release of our core platform, we added the ability to sign packages and workflows that are uploaded into Orchestrator. As an aside, Automation Cloud customers automatically receive the latest updates approximately every 2 weeks, meaning our Automation Cloud customers also get this new, additional protection. Customers can publish packages to the UiPath-managed Orchestrator service in the Automation Cloud with confidence and not worry about package integrity and corresponding business impact should a server-side compromise occur.

Privacy

UiPath collects two categories of data from users to operate and improve UiPath Automation Cloud Services:

1. **Customer data**: Includes user-identifiable transactional and interactional data that we need to operate the service and to manage your contract with UiPath
2. **System-generated logs**: Includes service-usage data that may be aggregated and contain pieces of customer data

From a GDPR standpoint, UiPath is considered a data processor. As such, we honor all obligations of a data processor by providing customers with full control over their data, in accordance with the product architecture and implementation.

We have ensured that we can export all your data for you, upon request. Should you close your account with the UiPath Automation Cloud, or otherwise request data deletion, we delete that data from our systems after the requisite 30 day soft-delete period.

We recommend our customers assess if their use of our Automation Cloud is in line with their privacy obligations. For more information about UiPath's privacy statement, how UiPath processes your data when using online services, and GDPR commitments, please visit our privacy policy.

Data residency and sovereignty

We know our customers care deeply about data location. As of January 2021, we now support five separate server regions, US, EU, Canada, Australia, and Japan.

Robot and business data associated with the UiPath Automation Cloud for *community* (the free service) is stored in EU.

Customers on the UiPath Automation Cloud for *enterprise* may choose the location of their tenants, and robot and business data is then stored in each tenant's region. By default, the location of services for enterprise cloud users is based on the location of the account: Japan for Japanese customers, Canada for Canadian customers, Australia for Australian and New Zealand customers, US for North American (excluding Canada) customers, and the EU for the rest of the world. Customers can also request at any time that one of more of their tenants be moved to a different region. We will serve all content, and store all robot and business data, from the region each tenant is hosted in. We may continue to add additional regions as options for enterprise cloud customers as we see demand grow.

Please note also that although data from robots and business data is kept, encrypted, within the tenant region, some account-related data such as account name, user lists, and license information may be replicated outside the region as part of normal operations.

Security and compliance practices

UiPath addresses the following aspects of security and compliance in order to help prevent breaches and uphold the highest standards for data security, privacy, and availability:

Systems hardening

UiPath Cloud Services use Azure's Platform-as-a-Service (PaaS) offering for much of its infrastructure. PaaS automatically provides regular updates for known security vulnerabilities.

Secure development life cycle

UiPath security and development teams work hand in hand to address security threats throughout the development process of UiPath Automation Cloud.

Teams perform threat modeling during service design. They adhere to design and code best practices and verify security in the final product using a multi-pronged approach that leverages internally built tools, commercial static and dynamic analysis tools, internal penetration testing, and external bug bounty programs.

We also monitor vulnerabilities introduced in our code base through third-party libraries and minimize our dependency on these libraries and corresponding exposure. Because the security landscape is continually changing, our teams stay current with the latest in best practices. We also enforce annual training requirements for all engineers and operations personnel working on the UiPath Automation Cloud.

Service and data availability

Ensuring that the Automation Cloud services are available so you can access your organization's assets is of the utmost importance to us. That is why we rely on Azure's backup mechanism and practice data recovery.

We employ other fail-safes to help ensure availability. A malicious distributed denial-of-service (DDoS) attack, for example, could affect UiPath Automation Cloud service availability. Azure has a DDoS defense system that helps prevent attacks against our service. It uses standard detection and mitigation techniques such as SYN cookies, rate limiting, and connection limits.

The system is designed not only to withstand attacks from the outside, but also from within Azure.

Live site testing

We emulate adversarial tactics on our services and underlying infrastructure using internal red teams.

The goal is to identify real-world vulnerabilities, configuration errors, and other security gaps in a controlled manner so that we can test the effectiveness of our prevention, detection, and response capabilities.

Security incident response

We strive to minimize the attack surface of our services and go to great lengths to reduce the probability of a data breach ever occurring. Nevertheless, security incidents can still happen.

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.

Once the team has contained an issue, our security incident management process continues as we identify the root cause and track the necessary changes to ensure we prevent similar issues in the future.

Production access control

We maintain strict control over who has access to our production environment and customer data.

Access is only granted at the level of least privilege required and only after proper justifications are provided and verified. If a team member needs access to resolve an urgent

issue or deploy a configuration change, they must apply for "just in time" access to the production service.

Access is revoked as soon as the situation is resolved. Access requests and approvals are tracked. If the username and password for one of our developers or operation staff were ever stolen, data is still protected because we use two-factor authentication for all production system access.

Secrets Management

Secrets that we use to manage and maintain the service, such as encryption keys, are managed, stored, and transmitted securely through the Azure Management Portal.

All secrets are rotated on a regular cadence and can be rotated on-demand if there is a security event.

Security and Compliance Certifications

UiPath has obtained the ISO 27001:2013 and Veracode continuous certifications that specifically include and name the Automation Cloud (under its former name, the “UiPath Cloud Platform”) as well as other UiPath products. They can be seen on this page for reference. UiPath has also obtained a SOC 2 type 1 report that can be shared with customers and prospects under NDA. We are working towards completing the SOC 2 type 2 certification next in early 2021, with additional certifications to follow. Additionally, your UiPath team can assist with any security architecture or capability questions not covered in this whitepaper.

Summary overview

The UiPath Automation Cloud 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 an automation cloud that is as secure and reliable as it is cost-effective and scalable.

If you have questions or concerns about our Automation Cloud security, privacy or compliance approach, your UiPath representative can assist in getting you any further information you may need from our team.

Thank you for considering UiPath and the UiPath Automation Cloud!

and machine learning. Led by a commitment to bring digital era skills to more than a million people, the company's enterprise Robotic Process Automation (RPA) platform has already automated millions of repetitive, mind-numbing tasks for business and government organizations all over the world, improving productivity, customer experience and employee job satisfaction.

Recently named by Comparably as the 6th happiest place to work and recognized for having the 11th best company culture among large businesses, UiPath is one of the fastest growing and highest-valued AI enterprise software companies worldwide.