UiPath The Foundation of Innovation™

UiPath Automation Suite

Security, Privacy, and Compliance

White Paper

Revised April 2023

Contents

Introduction

UiPath offers multiple delivery options to meet a wide variety of needs, including policy and security requirements. In additional to standalone product installations, we offer two full platform options: Automation Cloud, delivered as SaaS, and Automation Suite, designed for self-hosting in the cloud or on-premises.

Both options are built from the ground up with security, privacy, and compliance in mind. A complete comparison of the two is beyond the scope of this paper – but a key consideration is the control/cost profile that best suits your business, policy, and security needs.

UiPath Automation Cloud, being SaaS, is instantly available and always kept up to date with no infrastructure management costs for you. However, it does not allow any customer management or control of the underlying infrastructure, and it requires Internet connectivity.

UiPath Automation Suite offers a similar user experience to Automation Cloud, but is self-hosted, offering complete control down to the virtual or physical hardware. It can also be installed and run without Internet connectivity, if desired – but it does require IT resources to install and maintain the environment.

The security of any and all data associated with your RPA projects is of the utmost importance to UiPath, no matter whether you choose to deploy Automation Suite within your physical or virtual infrastructure, or you choose to leverage UiPath Automation Cloud.

In this whitepaper, we focus specifically on Automation Suite service design principles and practices related to security, privacy, and compliance. If you are considering whether Automation Suite or Automation Cloud better suits your needs, you may also wish to review the companion paper for Automation Cloud.

Our commitment

UiPath goes to great lengths to ensure that data related to your RPA projects remains safe and secure. When using UiPath Automation Suite, your data will benefit from multiple layers of security and governance technologies, operational practices, and compliance policies enforced by UiPath.

UiPath Automation Suite – Deployment Overview

UiPath Automation Suite is a great option if you want to fully manage the environment, start delivering Robotic Process Automation (RPA) on-premises and then scale up over time, with enterprise-scale manageability and optimization from day one.

Deployment architecture

The UiPath Automation Suite is comprised of server, agent, and specialized agent nodes, as seen in the diagram below.

Server nodes host cluster management services (control plane) that perform important cluster operations such as workload orchestration, cluster state management, load balance incoming requests, etc. Kubernetes may also run a few of the UiPath products and shared components based on underlying resource availability.

Agent nodes are responsible for running UiPath products and shared components only.

Specialized agent nodes run special workloads such as Task Mining analysis and Document Understanding pipelines that require GPU capability. However, the core Task Mining and Document Understanding services still run on the server or agent nodes. Specialized agent nodes do not host any of the UiPath product or shared components.

Automation Suite cannot guarantee which UiPath product runs on each node. This is solely managed by Kubernetes.

Terminology

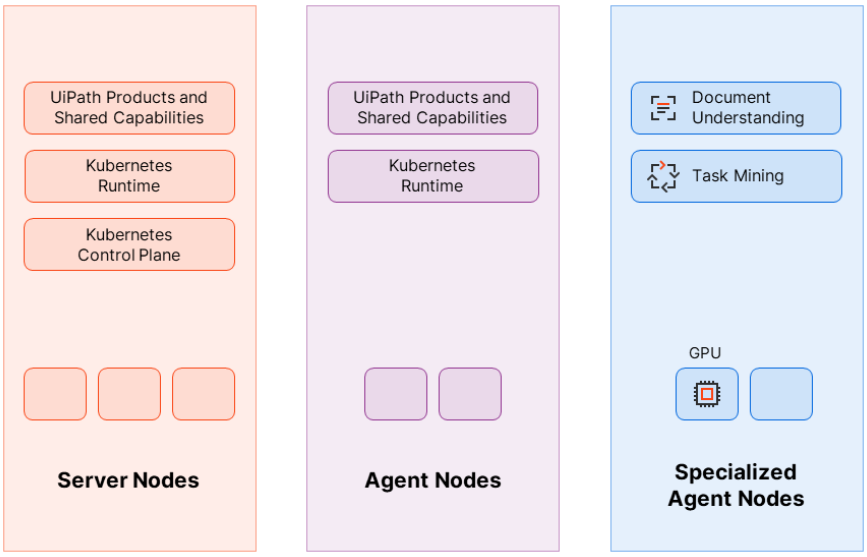
Node – any machine (bare metal, virtual etc.)

Kubernetes cluster – a set of nodes that run containerized applications

Server node – a machine (bare-metal or virtual) running the cluster management server.

Agent node – a machine running the worker pods (the functional services). A machine can be designated to be used as both server and agent. Having separate server and agent nodes in a deployment is a topology design decision.

Offline (air-gapped) environment – a setup where the machines do not have access to the Internet.



Deployment options

Automation Suite supports the following two deployment modes:

Deployment mode	Description
Single-node Evaluation	Supported for evaluation and demo scenarios.
Multi-node Production, HA-enabled	Supported for production use. You can perform additional configuration post-deployment to have full HA capabilities.

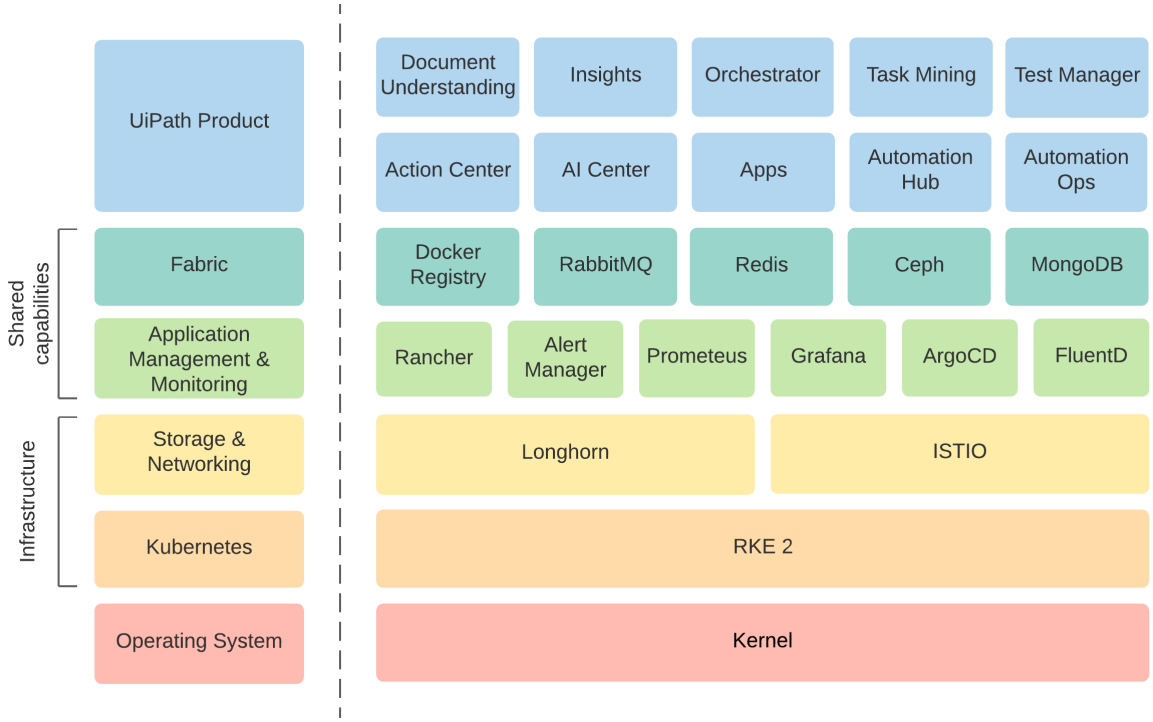
Automation Suite can be deployed to an environment connected to the Internet (online deployment) or to an environment with restricted Internet access (offline or air-gapped).

An **online deployment** means Automation Suite requires access to the Internet during both installation and runtime. All UiPath products and supporting libraries are hosted either in a UiPath registry or UiPath-trusted third party store.

An **offline deployment** (air-gapped) is a completely isolated setup without access to the internet. This kind of setup requires the installation of an additional registry to store all the UiPath products' container images and binaries, which are shipped in the form of tar ball.

UiPath Automation Suite – Architecture Overview

The Automation Suite installer bundles both required and optional components. The full package looks like the diagram below:



The following table lists out these components:

Component	Required / Optional	Description
RKE2	Required	Rancher-provided Kubernetes distribution. It is the container orchestration platform that runs all the architectural components and services.
Rancher Server	Required	Rancher's Kubernetes management tool.
Longhorn	Required	Rancher-provided distributed block storage for Kubernetes. It helps expose external storages inside Kubernetes clusters for workloads to claim and use like mounted persistent storage.
CEPH Object Store	Required	Open-source storage provider that exposes Amazon S3-compliant object/blob storage on top of persistent volumes created by Longhorn. It enables services to use blob storage like functionality for their operations.
Argo CD	Required	Open-source declarative CD tool for Kubernetes. It follows the GitOps pattern of using Git repositories as the source of truth for defining the desired application state. It provides application lifecycle management (ALM) capabilities for Automation Suite components and UiPath services that run in a Kubernetes cluster.
Docker registry	Required	Open-source docker registry used for pushing and pulling install time and runtime container images in your premises.
Istio	Required	Open-source service mesh that provides functionality such as ingress, request routing, traffic monitoring etc., for the microservices running inside the Kubernetes cluster.
Prometheus	Required	Open-source system monitoring toolkit for Kubernetes. It can scrape or accept metrics from Kubernetes components as well as workloads running in the clusters and store those in time series database.
Grafana	Required	Open-source visualization tool used for querying and visualizing data stored in Prometheus. You can create and ship a variety of dashboards for cluster and service monitoring.
Alertmanager	Required	Open-source tool that helps handling alerts sent by client applications such as the Prometheus server. It is responsible for deduplicating, grouping, and routing them to the correct receiver integrations, such as email, PagerDuty, or OpsGenie.
Redis	Required	Redis Enterprise non-HA (single shard) used by some UiPath services to get centralized cache functionality.
RabbitMQ	Required	Open-source reliable message broker used by some UiPath services to implement asynchronous execution patterns.
MongoDB	Optional	MongoDB is a source-available cross-platform document-oriented database program. Classified as a NoSQL database program, MongoDB uses JSON-like documents with optional schemas. MongoDB is deployed only when **UiPath Apps** is enabled.
FluentD and Fluentbit	Required	Open-source reliable log scraping solution. The logging operator deploys and configures a background process on every node to collect container and application logs from the node file system.
Gatekeeper	Required	Open-source tool that allows a Kubernetes administrator to implement policies for ensuring compliance and best practices in their cluster.

A few external components may also be required such as external load balancers, an SQL server, blob/file storage, key vaults, log sinks, and notification tools. Note that the suite provides some extension points.

UiPath The Foundation of Innovation™

Automation Suite Portal

The Automation Suite Portal serves as the first entry point for our customers to create an account for their organization. As a customer, you can also:

- Invite or remove users
- Manage user roles and permissions
- Set up SSO
- Request licenses for robots
- Set up Orchestrator instance(s) for development, testing, and production needs

Orchestrator

The UiPath core platform's server-side component is called Orchestrator. It allows you as a customer to manage your entire RPA infrastructure from one central control plane. If you are a current Orchestrator customer, you are probably already familiar with the functionality and interface. We provide a seamless experience for existing and new customers by integrating UiPath Orchestrator into the heart of our Automation Suite offering.

Additional documentation on Orchestrator can be found here.

AI Center

UiPath's cognitive services platform is called AI Center. AI Center allows Automation Suite users to deploy and manage machine learning models within the Automation Cloud. RPA developers can easily integrate RPA automations with AI/ML models to extend a robot's ability to perform complex tasks. AI solutions templates provide building blocks for enhancing automations with AI, pre-built ML models, sample datasets, or analytics. You can quickly address use cases that benefit from AI models, such as document understanding, language analysis and comprehension, image analysis, or tabular data processing.

Additional documentation on AI Center can be found here.

Document Understanding

UiPath Document Understanding is designed to help you combine different approaches to extracting information from various document types. The aim is to make extracting data as easy as possible: create one single workflow that will extract data from a variety of documents.

Additional documentation on Document Understanding can be found here.

Insights

UiPath Insights is a web application that serves as a platform for data modeling and analytics using a combination of business metrics and operational insights. With pre-loaded dashboard templates, as well as user-defined dashboards to visualize company data across desired metrics, it enables you to discover new analytical insights, track performance indicators, and be alerted of errors.

Additional documentation on Insights can be found here.

Task Mining

UiPath Task Mining is an automation opportunity discovery service. It collects desktop data from enrolled employees, comprising of screenshots and log data upon each user action (i.e. mouse click, keystroke). It then runs a machine learning model to analyze the data and suggest a list of processes with high automation potential.

Additional documentation on Task Mining can be found here.

Test Manager

Part of the overall UiPath Test Suite, Test Manager is a web application that allows you to manage your testing process. The act of testing covers an extensive set of activities, including test case execution, reporting, requirements management, defect management, CI/CD integration, or exploratory testing just to name a few.

Additional documentation on Test Manager can be found here.

Action Center

UiPath Action Center offers a way for business users to handle actionable items and provide business inputs to Robots. It enables support for long-running unattended workflows that require human intervention. As workflow execution is fragmented, it can be suspended and resumed at a later time after human input is provided.

Additional documentation on Action Center can be found here.

Apps

UiPath Apps is a low-code application development platform that enables you to build and share enterprise-grade custom applications that deliver engaging user experiences. Using Apps, you can quickly build custom business applications that connect to data in any underlying cloud or on-premises system using the power of automation.

Additional documentation on UiPath Apps can be found here.

Automation Hub

UiPath Automation Hub is a collaborative process identification, automation pipeline management, and process repository tool. Its goal is to accelerate the adoption of RPA across your organization, by building an RPA Community of Interest.

Additional documentation on Automation Hub can be found here.

Automation Ops

UiPath Automation Ops is a centralized, web-based platform that enables a simple and convenient way to manage and implement governance policies based on user profiles, and to manage the feeds available in the organization.

Additional documentation on Automation Ops can be found here.

Tenant Management Service

Tenants allow you to model your organization structure, separating your business flows and information just like in real-life organizations. They are containers where you can organize your services and manage them for a group of users. For example, you can create a tenant for each of your departments and decide which services you want to enable for each based on their needs. In every tenant you can have one instance of each of the services. The Tenant Management Service is decoupled from our portal and offers isolation in the backend while delivering a seamless user experience.

Identity Service

User identity is managed by a central identity service in UiPath Automation Suite. Users sign into the system using either an external identity provider or through a UiPath Automation Suite account. The UiPath Identity Service combines externally managed user identities with UiPath user and tenant information. The internal identity is used to identify users when they access the UiPath Automation Suite, as well as to establish user identity between various components.

Service-Design Principles

All of the above services are packaged together as **UiPath Automation Suite**.

You can install everything in the package or pick which services you want, and deploy in a private or public cloud, or air-gapped on-premises. All the tools for monitoring, alerting and back-up are in the box, and you can integrate them with external systems thanks to a few service-design principles:

Data encryption

All data is transmitted over protected channels. Installations can be customized to only allow specific versions of SSL/TLS and specific ciphers.

Use of transparent data encryption for SQL server is also supported for data at-rest encryption of application data. Environmental secrets for Kubernetes are encrypted at-rest by default.

Identity and access management

We support account creation in Automation Suite using a variety of identity service providers, such as Active Directory (AD), Azure AD, Google Auth, federation via SAMLv2, as well as through native accounts. After 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). Thanks to tenant management in Automation Suite, you have similar RBAC controls available for a seamless experience when managing user roles and access.

Tenant & organization data isolation

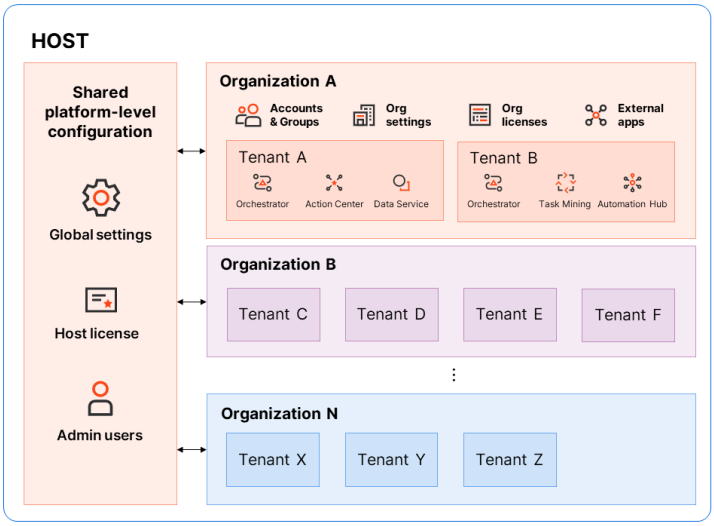
Customers can define separate organizations each with their own administration, data, users, and licenses. From within an organization, they can further define tenants. Data from each tenant is logically separated from others in our service so that we can enforce access and authorization controls for all tenants as they access data inside our service.

Logging

Automation Suite includes several levels of logging that align to the levels of hierarchy available in the product. Audit logs are available at both the **host level** and the individual **organization level**. These audit logs will capture login and administrative events such as changes in licenses, settings, or accounts. Additional logging is available per product within Automation Suite that is best suited for that individual product.

Monitoring

Automation Suite includes a number of tools provided to help monitor the health of the underlying components. These include the ability to create customized alerts and send them to a centralized source. Additional details can be found **here**.



Privacy

UiPath collects two categories of data from users in order to operate and improve Automation Suite:

1. **License data**: includes basic information from the customer to activate licenses – *note that this can be performed fully air-gapped as well*.
2. **Telemetry data**: includes anonymized performance data used by UiPath to enhance our products. Customers can **opt out of collecting telemetry** data.

Service and Data Availability

In addition to offering multi-node deployment options for high availability. Automation Suite can be configured to perform automated backups in addition to any backup functions performed by the database(s) used.

- **High availability** setup requirements can be found **here**.
- **Backup and restore** functionality can be found **here**.

Security & 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:

Secure development life cycle

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

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 UiPath Automation Suite.

UiPath is also committed to addressing all vulnerabilities that may be reported to us – for more information see our latest **Security Advisories**.

Release cadence and patching

UiPath issues two major releases each year, one in the Spring around April and one in the Fall around October. These releases come with new features and functionality. Additionally, patches are released every 2 months for updates and bug fixes. Security fixes are rated by the severity of the vulnerability they are fixing using CVSS. They may be included in a regular patch, or an out-of-band hotfix release if the next patch cycle is too far away.

For more information on our release cadence and patches see our **Product Lifecycle**.

Compliance – Certifications and Attestations

UiPath has obtained the ISO 27001:2013 certification (including alignment with the additional control sets for ISO 27017:2015 and ISO 27018:2019) for our information security management system (ISMS) and the ISO 9001:2015 certification for our quality management system (QMS). You can check our **Trust Portal** for reference. While not specific to this product, UiPath has also obtained a SOC 2® type 2 report that can be shared with customers and prospects under NDA. UiPath will continue to obtain SOC 2® Type 2 reports indefinitely. Additionally, your UiPath representative can assist with any security architecture or capability questions not covered in this whitepaper.

Summary Overview

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 **UiPath Automation Suite**, a solution that is as secure and reliable as it is cost-effective and scalable.

To learn more

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

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 Business Automation 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™.