UIPATH CLOUD PLATFORM SECURITY PRACTICES

Commitment	UiPath is committed to ensuring that data related to your RPA projects remain safe and secure, without exception. When using UiPath Cloud Platform, your data will benefit from multiple layers of security and governance technologies, operational practices, and compliance policies that UiPath enforces. This information notice provides users of UiPath Cloud Platform, a view into UiPath's service design principles, practices and roadmap from a security, privacy and compliance perspective.
What is included in the UiPath Cloud Platform	UiPath's cloud platform is composed of multiple independent services, such as orchestrator, tenant management, licensing service, and others. To provide a seamless experience, we work hard to abstract these details from the end user and offer these services through a common front-end called UiPath Cloud Portal.
Data encryption	We encrypt all customer data in each data store that makes up our service stack. All data is transmitted over protected channels, regardless of it being over the internet or within our internal service components.
Data residency	We know our customers care deeply about data location. UiPath Cloud Platform has chosen a safe location for storing your data. Therefore, the servers are located in Ireland.
Infrastructure and code security	**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 cloud platform. Teams perform threat modeling during service design, following design and code best practices and verifying security in the final product using a multi-pronged approach that includes the use of 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 keep current with the latest in best practices. We have annual training requirements for all engineers and operations personnel working on UiPath Cloud Platform.

Service Availability	**Denial of Service**: A malicious distributed denial-of-service (DDoS) attack can affect UiPath Cloud Platform 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. For UiPath application-specific attacks that can penetrate the Azure defense systems, UiPath establishes application and organization level quotas and throttling to prevent any overuse of key service resources during an attack or accidental misuse of resources.
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, configurations errors or other security gaps in a controlled manner such that we can test the effectiveness of our prevention, detection and response capabilities.
Access controls	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.
Control Plane secret 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 in the case of a security event.