UiPath Shared Responsibility Customer Guide

Table of Content

Notices

This document (referred herein as, the "**Guide**") is addressed to companies that have a valid agreement in place with UiPath for the licensing of UiPath products (referred herein as, "**products**"), or companies that have expressed an interest in licensing UiPath products and are in the process of processing the underlying contractual documentation (referred herein as, "**customers**"). The customer is responsible for making their own independent assessment of the information in this Guide. This Guide: (a) is for informational purposes only, (b) represents current UiPath product offerings and practices, which are subject to change without notice, and (c) does not create any commitments or assurances from UiPath. UiPath products or services are provided "as is" without warranties, representations, or conditions of any kind, whether express or implied. The responsibilities and liabilities of UiPath to its customers are controlled by UiPath agreements, and this document is not part of, nor does it modify, any agreement between UiPath and its customers.

Introduction

As customers consider and evaluate different UiPath products, it is essential to explore the different deployment models that changes based on time, cost, ease of use, regulatory factors, etc. It is also equally important that customers understand how privacy and security are managed in these deployment models that helps them to evaluate their own risk appetite based on their own environment, their expectations and the industry to which they belong.

Many organizations that consider cloud products mistakenly assume that after moving to the cloud their role in securing their data shifts entirely to the cloud providers. UiPath may provide security for certain elements as well as support in the protection of data, but customers must be aware of their own responsibility in protecting the security and privacy of their data. It is ultimately the customer's responsibility to determine the level of security that is appropriate for its requirements.

For customers in regulated industries, such as healthcare, where laws regulate protected health information (PHI), the need to understand how different deployment models that affects their privacy, security, and regulatory compliance posture is paramount. Fundamentally, HIPAA compliance boils down to controlling access to ePHI, but the line demarcating responsibility for ePHI between organizations and cloud providers is unclear. This issue becomes more significant when we start considering state and international privacy laws such as GDPR, CCPA, etc.

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.

Shared Responsibility Model

Legend	
Customer (C)	
UiPath (U)	
Azure (A)	

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						

The above diagram clearly articulates the different ownership responsibilities for both the customer, as well as UiPath depending on which deployment model the customer is building their environment with.

Data and End Point Protection

For both on-premises and cloud products, the customer is ultimately accountable and responsible for all aspects of security and operations of the customer data and its end point protections. The customer decides who can access their data and for how long. This is also required by some of the industry regulations such as HIPAA where the customers take the role of a covered entity or with GDPR where the customer takes the role of a controller. UiPath plays an important role in supporting the customer to maintain the security of data to the best of its ability by signing contractual agreements and providing various security measures which are in built in both on--premise and cloud products.

Identity & Access Management, Applications

This is where the ownership model starts changing to include more shared responsibilities between UiPath and the customer. For on-premises products, the customer is still accountable and responsible for all aspects of security and operations when it comes to identity and access management, but when it comes to cloud products their

responsibility is limited to their own UiPath cloud tenancy. For cloud products, UiPath undertakes major responsibility in identity and access management to and within the cloud.

For both deployment models, the customer is completely responsible for the design, development, testing, deployment, maintenance and behavior of any automation that the customer chooses to create using the products either on-premises or in the cloud. The customer is also responsible for determining whether its use and the behavior of any such automations are compliant with relevant in-scope regulations. The Customer is also responsible for managing their organization's instance(s) of the platform, installed applications (as applicable), as well as establishing any customized security solutions or automated processes through the use of setup features, application development tools, and API integration tools.

UiPath's responsibility is to make sure that the product release itself follows a secure development lifecycle based on industry standards and security by design principles that have been ingrained in personnel actually developing the products.

Network Controls

For on-premises products, the customer is accountable and responsible for all aspects of security and operations of network controls which includes the configuration, management, and securing of network elements such as virtual networking, load balancing, DNS, and gateways. These controls provide a means for services to communicate and interoperate. For cloud products, UiPath is responsible for all aspects of network security to and within the cloud.

Operating System, Physical Hosts & Network, Physical Datacenter

For on-premises products, the customer is accountable and responsible for all aspects of security and operations of all types of hosting infrastructure including the operating system, storage and platform services.

For cloud products, customer completely relies on UiPath to own the controls for all the remaining layers. UiPath shares the responsibility of the operating system with Azure depending on the PaaS and SaaS solutions used to deploy the UiPath platform. UiPath relies completely on Azure to owning the physical and environmental security of the cloud that includes datacenters, servers and network devices.

Shared Responsibility Model & CCF Framework

Responsibility Layers	Common Control Families
Data	Backup Management, Data Management
End Point Protection	Asset Management, Mobile Device Management, Logging & Monitoring
Identity & Access Management	Identity & Access Management
Applications	Change Management, Logging & Monitoring, Service Lifecycle, Vulnerability Management
Network Controls	Configuration Management, Network Operations, Logging & Monitoring, Vulnerability Management
Operating System	Configuration Management, Logging & Monitoring
Physical Hosts & Network	Site Operations, Logging & Monitoring, Vulnerability Management
Physical Datacenter	Asset Management, Site Operations
Organizational wide responsibilities	Business Continuity, Entity Management, Incident Response, Risk Management, Human Resources, Security Governance, System Design Documentation, Supplier Management, Training & Awareness

We also mapped the Shared Responsibility Model to UiPath's Common Control Framework (CCF). This helps to explain each layer called out in the Shared Responsibility Model and provide a more in-depth information of the shared responsibility between the customers and UiPath as per the product deployment model (on-premises and cloud). You will also observe that a particular Common Control can be tied to multiple shared responsibility layers (e.g. Logging and Monitoring). This is because each associated layer has some form of responsibility on both customers and UiPath when it comes to the produced application, network and infrastructure.

Organizational wide responsibilities are entity level controls that govern all layers of the shared responsibility model and hence all the entity level Common Control families that are consistent organization wide and are typically maintained centrally are mapped to the final layer.

This matrix also introduces the next section where we look at shared responsibility between customers and UiPath for both cloud and on-premises products as per the established UiPath Common Control families. This drives our contractual agreements, compliance reports and overall risk portfolio .

Customer Shared Responsibility Matrix

This section provides more granular information on the shared responsibility model based on UiPath defined control families. This helps to clearly articulate roles and responsibilities for customers and UiPath per each control domain for both on-premises and cloud products.

Control Family	Control Sub-Family	On-premises Customer Responsibility Matrix		Cloud Customer Responsibility Matrix	
		Customer	UiPath	Customer	UiPath
Asset Management	Device and Media Inventory	The customer is responsible for the IT and production assets they own and operate in their own environment (servers, computers, network equipment, mobile devices, peripherals, etc.).	UiPath is responsible for maintaining inventory of the corporate assets used by the support and professional services functions.	The customer is responsible for the corporate and production assets they use to access and maintain their own UiPath cloud tenancy.	UiPath is responsible for both corporate and production assets that are used to design, develop, operate and maintain the products and the platform used by the customers.
Business Continuity	Business Continuity Planning	The customer is responsible for developing a Business Continuity plan, a Disaster Recovery Plan as well as performing a Business Impact Analysis for their own environment that supports their on-premises deployment.	UiPath is responsible for developing a Business Continuity plan as well as performing a Business Impact Analysis for its support and professional services function.	The customer is responsible for developing a Business Continuity plan, a Disaster Recovery Plan as well as performing a Business Impact Analysis for its own personnel and environment that support their UiPath cloud tenancy.	UiPath is responsible for developing a Business Continuity plan as well as performing a Business Impact Analysis for its own personnel and environment that support the cloud products.
Business Continuity	Capacity Management	The customer is responsible for planning, budgeting and monitoring their own capacity requirements.	Not Applicable	Not Applicable	UiPath is responsible for planning, budgeting and monitoring their own capacity requirements.
Backup Management	Backup	The customer is responsible for their primary and secondary backups, replication functions, if applicable, as well as restoration and failover exercises to meet their specific data retention requirements.	Not Applicable	The customer is responsible for exporting data backups from its UiPath cloud tenancy according to its internally defined policies. customer is responsible for exporting data backups from its UiPath cloud tenancy according to its internally defined policies.	UiPath is responsible to perform regular backups of customer data at geographically separated locations, replication functions as well as restoration and failover exercises per the agreed data retention requirements.
Configuration Management	Baseline Configurations	The customer is responsible to develop and deploy hardened security configuration baseline for its own environment based on industry standards.	Not Applicable	The customer is responsible to develop and deploy hardened security configuration baseline for the environment that supports its UiPath cloud tenancy.	UiPath is responsible to develop and deploy hardened security configuration baseline for its own environment based on industry standards.

Control Family	Control Sub-Family	On-premises Customer Responsibility Matrix		Cloud Customer Responsibility Matrix	
		Customer	UiPath	Customer	UiPath
Change Management	Change Management	The customer is responsible to enforce all infrastructure and application changes to be reviewed, tested and approved by authorized personnel before being implemented as per a documented change management policy.	UiPath is responsible to enforce all application changes to be reviewed, tested and approved by authorized personnel before being released as per a documented change management policy.	The customer is responsible to enforce all application customizations to be reviewed, tested and approved by authorized personnel before being implemented as per a documented change management policy.	UiPath is responsible to enforce all infrastructure and application changes to be reviewed, tested and approved by authorized personnel before being implemented as per a documented change management policy.
Data Management	Data Classification	The customer is responsible to classify their own data in risk tiers and maintain security measures based on their risk management process.	Not Applicable	The customer is responsible to classify their own data in risk tiers and maintain security measures based on their risk management process.	UiPath is responsible to classify customer data as the top risk tier and maintain security measures per its risk management process.
Data Management	Data Encryption	The customer is responsible to encrypt all customer data at rest, in transit to, from, and within its own environment, per a documented encryption policy.	Not Applicable	The customer is responsible to configure provided encryption standards by UiPath for customer data at rest, in transit to, from, and within its own UiPath cloud tenancy.	UiPath is responsible to encrypt all customer data at rest, in transit to, from, and within the cloud, per a documented encryption policy.
Data Management	Data Removal	The customer is responsible to design, develop, operate and maintain all data deletion processes to meet their data retention requirements.	Not Applicable	Customer is responsible to request data deletion for its UiPath cloud tenancy to meet its data retention requirements.	UiPath is responsible to schedule deletion of customers data upon request within an agreed upon timeline as per contractual agreements.
Identity and Access Management	Logical Access Account Lifecycle	The customer is responsible for designing, developing and maintaining an identity and access management program within and outside their environment as well to meet any applicable regulatory requirements.	Not Applicable	The customer is responsible for designing, developing and maintaining an identity and access management program for their own UiPath cloud tenancy to meet any applicable regulatory requirements.	UiPath is responsible for designing, developing and maintaining an identity and access management program in the cloud to meet any applicable regulatory requirements.
Identity and Access Management	Authentication	The customer is responsible for designing, developing and maintaining an authentication program which includes unique ids, multi factor authentication, account lockouts etc. within their environment	Not Applicable	The customer is responsible for designing, developing and maintaining an authentication program which includes unique ids, multi factor authentication, account lockouts etc. within their own UiPath	UiPath is responsible for designing, developing and maintaining an authentication program which includes unique ids, multi factor authentication, account lockouts etc. within the cloud to meet any applicable regulatory requirements.

Control Family	Control Sub-Family	On-premises Customer Responsibility Matrix		Cloud Customer Responsibility Matrix	
		Customer	UiPath	Customer	UiPath
		to meet any applicable regulatory requirements.		cloud tenancy to meet any applicable regulatory requirements.	
Identity and Access Management	Role-Based Logical Access	The customer is responsible for granting and removing access for UiPath personnel and defining an appropriate expiration date when granting the access.	Not Applicable	The customer is responsible for granting and removing access for UiPath personnel within their own UiPath cloud tenancy and defining an appropriate expiration date when granting the access.	UiPath is responsible for granting and removing access for UiPath personnel within the cloud.
Identity and Access Management	Key Management	The customer is responsible for designing, developing and maintaining a key management program for their own environment	Not Applicable	Not Applicable	UiPath is responsible for designing, developing and maintaining a key management program within the cloud
Incident Response	Incident Response	The customer is responsible for implementing an incident handling capability for security incidents that includes preparation, detection and analysis, containment, eradication, and recovery in accordance with their incident response policy.	UiPath is responsible to support any customer incident management processes that the customer needs assistance on limited to contractual agreements.	The customer is responsible for implementing an incident handling capability for security incidents that includes preparation, detection and analysis, containment, eradication, and recovery in accordance with their incident response policy within their UiPath cloud tenancy	UiPath is responsible for implementing an incident handling capability for security incidents that includes preparation, detection and analysis, containment, eradication, and recovery in accordance with their incident response policy within the cloud.
Incident Response	Incident Communication	The customer is responsible for communicating relevant security, availability and confidentiality problems or incidents impacting its UiPath tenancy to UiPath or, as necessary, to external regulatory bodies.	Not Applicable	The customer is responsible for communicating relevant security, availability and confidentiality problems or incidents impacting its UiPath tenancy to UiPath or, as necessary, to external regulatory bodies.	UiPath is responsible for communicating relevant security, availability and confidentiality incidents in cloud to customers or, as necessary, to external regulatory bodies.
Mobile Device Management	Mobile Device Security	The customer is responsible for designing, developing and maintaining a mobile device management program for portable assets that support their environment including usb, thumb drives mobile devices, etc.	Not Applicable	The customer is responsible for designing, developing and maintaining a mobile device management program for portable assets that support their UiPath cloud tenancy including usb, thumb drives mobile devices, etc.	UiPath is responsible for designing, developing and maintaining a mobile device management program for portable assets that support the cloud environment including usb, thumb drives mobile devices, etc.

Control Family	Control Sub-Family	On-premises Customer Responsibility Matrix		Cloud Customer Responsibility Matrix	
		Customer	UiPath	Customer	UiPath
Network Security	Perimeter Security	The customer is responsible for designing, developing and maintaining a network security program which includes installing firewalls, network segregation, network monitoring, etc., for its own environment to meet any applicable regulatory requirements.	Not Applicable	The customer is responsible for designing, developing and maintaining a network security program for their own UiPath cloud tenancy to meet any applicable regulatory requirements.	UiPath is responsible for designing, developing and maintaining a network security program for the cloud environment which includes installing firewalls, network segregation, network monitoring, etc., to meet any applicable regulatory requirements and contractual agreements.
Human Resources	On-boarding	The customer is responsible for designing, developing and maintaining an onboarding program which includes background check investigation, acceptable use policy, code of conduct, new hire training, vendor onboarding for all personnel accessing their environment.	UiPath is responsible for designing, developing and maintaining an onboarding program which includes background check investigation, acceptable use policy, code of conduct, new hire training, vendor onboarding for all personnel supporting customers as per the agreed contracts.	The customer is responsible for designing, developing and maintaining an onboarding program which includes background check investigation, acceptable use policy, code of conduct, new hire training, vendor onboarding for all personnel accessing their UiPath cloud tenancy.	UiPath is responsible for designing, developing and maintaining an onboarding program which includes background check investigation, acceptable use policy, code of conduct, new hire training, vendor onboarding for all personnel accessing the cloud environment.
Human Resources	Off-boarding	The customer is responsible for designing, developing and maintaining an offboarding program which includes terminations, job changes, access reviews and vendor offboarding for all personnel accessing their environment.	Not Applicable	The customer is responsible for designing, developing and maintaining an offboarding program which includes terminations, job changes, access reviews and vendor offboarding for all personnel accessing their UiPath cloud tenancy.	UiPath is responsible for designing, developing and maintaining an offboarding program which includes terminations, job changes and access reviews, vendor offboarding for all personnel accessing the cloud environment.
Risk Management	Risk Assessment & Mitigation	The customer is responsible for designing, developing and maintaining a risk assessment and mitigation program for their environment to meet any applicable regulatory requirements. Customers are also responsible to make sure the management is accountable for the associated risks.	UiPath is responsible for designing, developing and maintaining a risk assessment and mitigation program for the secure development lifecycle process as well as personnel supporting the customers to meet any applicable regulatory requirements. UiPath is also responsible to make sure the management is accountable for the associated risks.	The customer is responsible for designing, developing and maintaining a risk assessment and mitigation program for their UiPath cloud tenancy to meet any applicable regulatory requirements. Customers are also responsible to make sure the management is accountable for the associated risks.	UiPath is responsible for designing, developing and maintaining a risk assessment and mitigation program for the cloud environment to meet any applicable regulatory requirements. UiPath is also responsible to make sure the management is accountable for the associated risks.

Control Family	Control Sub-Family	On-premises Customer Responsibility Matrix		Cloud Customer Responsibility Matrix	
		Customer	UiPath	Customer	UiPath
Security Governance	Policy Governance	The customer is responsible for designing, developing, documenting and maintaining a policies governance framework. All policies have a designated owner and are reviewed, approved and communicated to workforce members at least annually.	UiPath is responsible for designing, developing, documenting and maintaining a policies governance framework. All policies have a designated owner and are reviewed, approved and communicated to workforce members at least annually.	The customer is responsible for designing, developing, documenting and maintaining a policies governance framework. All policies should have a designated owner and are reviewed, approved and communicated to workforce members at least annually.	UiPath responsible for designing, developing, documenting and maintaining a policies governance framework. All policies have a designated owner and are reviewed, approved and communicated to workforce members at least annually.
Security Governance	Information Security Management System	The customer is responsible to define its scope, roles and responsibilities and key stakeholders for their own environment supporting the UiPath product deployment as per the applicable regulatory requirements.	UiPath is responsible to define its scope and roles and responsibilities as per contractual agreements for developing and supporting on premise products.	The customer is responsible to define its scope, roles and responsibilities and key stakeholders for their own UiPath cloud tenancy as per the applicable regulatory requirements.	UiPath is responsible to define its scope, roles and responsibilities and key stakeholders for their cloud environment as per the applicable regulatory requirements.
Service Lifecycle	SDLC	The customer is responsible for designing, developing, documenting and maintaining a secure development program as per industry standards for all UiPath product customizations in its own environment.	UiPath is responsible for designing, developing, documenting and maintaining a secure development program as per industry standards to ship secure on-premises products.	The customer is responsible for designing, developing, documenting and maintaining a secure development program as per industry standards for all UiPath product customizations in its own application instance.	UiPath is responsible for designing, developing, documenting and maintaining a secure development program for the cloud products as per industry standards.
Systems Monitoring	Logging	The customer is responsible for designing, developing, documenting and maintaining a logging process for their own environment.	Not Applicable	The customer is responsible for exporting and archiving audit logs from its UiPath cloud tenancy according to its internally defined policies.	UiPath is responsible for designing, developing, documenting and maintaining a logging process for the cloud environment. UiPath is also responsible for making relevant application logs available for customers as per contractual agreements.
Systems Monitoring	Security Monitoring	The customer is responsible for reviewing and analyzing all audit records in their own environment as well as activity logs of actions performed by the customer support	Not Applicable	The customer is responsible for reviewing application logs for their instance as well as activity logs of actions performed by the customer support personnel at an	UiPath is responsible for reviewing and analyzing all audit records in the cloud environment at an organization-defined frequency for

Control Family	Control Sub-Family	On-premises Customer Responsibility Matrix		Cloud Customer Responsibility Matrix	
		Customer	UiPath	Customer	UiPath
		personnel at an organization-defined frequency for indications of unusual activity and remediating issues as necessary.		organization-defined frequency for indications of unusual activity and remediating issues as necessary.	indications of unusual activity and remediating issues as necessary.
Systems Monitoring	Availability Monitoring	The customer is responsible to set up monitoring tools to track and notify on the availability of their internal systems and services.	Not Applicable	Not Applicable	UiPath is responsible to set up monitoring tools to track and notify on the availability of UiPath internal systems and services.
Site Operations	Physical Access Account Lifecycle	The customer is responsible for designing, developing, documenting and maintaining a physical access control system for corporate offices as well as their production environment (e.g., data centers, private cloud etc.)	UiPath is responsible for designing, developing, documenting and maintaining a physical access control system for corporate offices that host support and professional services functions.	The customer is responsible for designing, developing, documenting and maintaining physical access control processes for its corporate offices and other operating environments that access its UiPath cloud tenancy.	UiPath is responsible for designing, developing, documenting and maintaining a physical access control system for corporate offices that host personnel that support professional services, cloud and support operations. UiPath relies on Azure for their physical access controls for the data centers that host UiPath customers' data.
Site Operations	Environmental Controls	The customer is responsible for designing, developing, documenting and maintaining an environmental control program for corporate offices as well as their production environment (e.g., data centers, private cloud etc.).	UiPath is responsible for designing, developing, documenting and maintaining an environmental protection program for corporate offices that host support and professional services functions.	The customer is responsible for designing, developing, documenting and maintaining an environmental protection program for its corporate offices and other operating environments that access its UiPath cloud tenancy.	UiPath is responsible for designing, developing, documenting and maintaining an environmental protection program for corporate offices that host personnel that support professional services, cloud and support operations. UiPath relies on Azure for their environmental controls for the data centers that host UiPath customers' data.
Training and Awareness	General Awareness Training	The customer is responsible for designing, developing, documenting and maintaining a security awareness training program, which includes updates about relevant	UiPath is responsible for designing, developing, documenting and maintaining a security awareness training program, which includes updates about relevant policies and	The customer is responsible for designing, developing, documenting and maintaining a security awareness training program, which includes updates about relevant	UiPath is responsible for designing, developing, documenting and maintaining a security awareness training program, which includes updates about relevant policies and

Control Family	Control Sub-Family	On-premises Customer Responsibility Matrix		Cloud Customer Responsibility Matrix	
		Customer	UiPath	Customer	UiPath
		policies and how to report security events to the authorized response team.	how to report security events to the authorized response team.	policies and how to report security events to the authorized response team.	how to report security events to the authorized response team.
Training and Awareness	Role-Based Training	The customer is responsible for designing, developing, documenting and maintaining a role-based training program, based on their applicable regulatory requirements.	UiPath is responsible for designing, developing, documenting and maintaining a role-based training program for UiPath personnel from the application development, support and professional services function.	The customer is responsible for designing, developing, documenting and maintaining a robust role-based training program, based on their applicable regulatory requirements.	UiPath is responsible for designing, developing, documenting and maintaining a role-based training program, based on applicable regulatory requirements.
Supplier Management	Vendor Assessments	The customer is responsible for designing, developing, documenting and maintaining a vendor management program for all new and existing suppliers based on self-defined risk tiers and applicable regulatory requirements.	Not Applicable	The customer is responsible for designing, developing, documenting and maintaining a vendor management program for new and existing supplier that support their UiPath cloud tenancy.	UiPath is responsible for designing, developing, documenting and maintaining a vendor management program for all new and existing suppliers based on their defined risk tiers that support cloud products.
Supplier Management	Vendor Agreements	The customer is responsible for creating, documenting and maintaining all vendor agreements for the vendors who support their infrastructure based on their applicable regulatory requirements and risk management process. Customers are also responsible to make updates to the agreement whenever necessary.	UiPath is responsible for creating, documenting and maintaining vendor agreements for those who support application development and release. UiPath is also responsible to make updates to the agreements whenever necessary.	The customer is responsible for creating, documenting and maintaining vendor agreements for those who support their own UiPath cloud tenancy customization. Customers are also responsible to make updates to the agreements whenever necessary.	UiPath is responsible for creating, documenting and maintaining all vendor agreements for the vendors who support their cloud infrastructure based on the applicable regulatory requirements and risk management process. UiPath is also responsible to make updates to the agreements whenever necessary.
Vulnerability Management	Production Scanning & Remediation	The customer is responsible for designing, developing, documenting and maintaining a vulnerability management program for their own infrastructure which includes monitoring its environment for technical vulnerabilities using security scanning tools and assigning a risk rating to identified vulnerabilities and prioritizing	Not Applicable	The customer is responsible for designing, developing, documenting and maintaining a vulnerability management program for their own UiPath cloud tenancy.	UiPath is responsible for designing, developing, documenting and maintaining a vulnerability management program for the cloud infrastructure which includes monitoring its environment for technical vulnerabilities using security scanning tools and assigning a risk rating to identified vulnerabilities and prioritizing

Control Family	Control Sub-Family	On-premises Customer Responsibility Matrix		Cloud Customer Responsibility Matrix	
		Customer	UiPath	Customer	UiPath
		remediation of legitimate vulnerabilities according to the assigned risk.			remediation of legitimate vulnerabilities according to the assigned risk.
Vulnerability Management	Penetration Testing	The customer is responsible for performing periodic internal and external penetration tests for their own infrastructure, identify gaps and create remediation timelines to remediate them.	Not Applicable	The customer is responsible for performing periodic internal and external penetration tests for their own applications and the applications they create, identify gaps and set remediation timelines to remediate them.	UiPath is responsible for performing periodic internal and external penetration tests for their own infrastructure, identify gaps and create remediation timelines to remediate them.
Vulnerability Management	Malware Protection	The customer is responsible for designing, developing, documenting and maintaining a malware protection program for their own infrastructure.	Not Applicable	Not Applicable	UiPath is responsible for designing, developing, documenting and maintaining a malware protection program for the cloud infrastructure.
Vulnerability Management	Code Security	The customer is responsible for source code checks for all application customizations for vulnerabilities before releases.	UiPath is responsible to conduct source code checks for vulnerabilities before releases.	The customer is responsible for source code checks for all application customizations for vulnerabilities before releases.	UiPath is responsible to conduct source code checks for vulnerabilities before releases.

Change History

Version	Date Published	List of Changes
V1.0	6/30/2021	