NOVEMBER 2021

Horizon Service Cloud Security Overview

vmware®

Table of contents

vmware®

vmware®

Document Scope

This document provides an overview of the security controls implemented in the cloud connected components of Horizon Service. Within this document, VMware Horizon® Service ("Horizon Service" or the "Service Offering") includes the following individual services: VMware Horizon® 8 subscription and VMware Horizon® Cloud Service on Microsoft Azure.

The Service Offering provides access to the Horizon Cloud Control Plane that is hosted in VMware-managed Microsoft Azure instances located in the US, Ireland, Germany, Australia, Japan and the UK. The Horizon Cloud control plane provides access to the VMware Horizon Cloud Manager console to orchestrate and manage the customer's Horizon Service workloads. This document also provides details for components leveraged by the solution such as the Universal Broker, and Cloud Monitoring Service.

Horizon Services have achieved PCI-DSS compliance; customers can review the PCI Attestation of Compliance (PCI AOC) for component scoping and compliance details with the PCI-DSS standard. *The PCI AOC* is available to download directly from the *VMware Cloud Trust Center*.

This document's intent is to provide readers with an understanding of how Horizon Service approaches cloud security, the key mechanisms and processes that VMware uses to manage information security as well as describing shared responsibilities for providing security in a modern cloud computing environment.

This document assumes at least intermediate knowledge of Horizon Service and focuses on the policies, processes, and controls supporting the cloud delivered service. Federal Risk and Authorization Management Program (FedRAMP) is not in scope for this document.

Shared Responsibilities

The end-to-end security of the Horizon Service is shared between VMware and our customers. Responsibilities change by the underlying Horizon Service workload.

VMware provides security for the aspects of the Horizon Service offering over which we have sole physical, logical, and administrative level control. Customers are responsible for the aspects of the service offering over which they have administrative level access or control.

VMware leverages IaaS providers globally to support the Horizon Service offering. These providers maintain physical and environmental security controls for the cloud-delivered service. Specific details regarding these providers can be found in the *Horizon Service Sub-Processors Addendum*

Compliance Reports

Horizon Cloud control plane and Horizon Cloud Service on Microsoft Azure are PCI-DSS certified and have achieved Service Organization Control (SOC) 2 Type 2 and SOC 3 audits.

VMware can provide copies of audit reports under an NDA; please contact your VMware account representative to request this report. Refer to the *VMware Cloud Trust Center* for the latest list of industry certifications by service.

VMware Information Security Program

Core Principles

Maintaining the service and stored customer data confidentiality, integrity, and availability requires a wide array of tools and processes that must all be expertly designed to consider customer satisfaction, business needs, product efficiency, product deadlines, revenue, shareholder expectations, regulations and laws. VMware helps balance these needs with a set of controls and management processes designed to both mitigate risk and enhance our product offerings. VMware created controls and processes using a set of driving principles to provide the underlying general rules and guidelines for security within our cloud delivered services. Overarching principles include:

- Risk – Managing risk by understanding the threat landscape, building a solid platform, and leveraging all decision makers when calculating risk.
- Controls – Establishing a balance of effectiveness and efficiency by implementing the appropriate controls for the associated risk.
- Security – Providing preventative and protective capabilities to better ensure a secure service.

The VMware Information Security Program leverages guidance from industry best practices and regulatory standards, including NIST SP 800-53 and ISO 27001. We maintain a written Information Security Program and Policies to protect customer data hosted in our systems, and we perform annual reviews and audits of our program to ensure the integrity of our hosted offerings.

VMware has an Information Security Governance Committee (ISGC) that is chaired by members of senior management and representatives from our Information Security, IT Operations, HR, Marketing, Facilities and Legal teams. Our CSO is ultimately responsible for our Information Security program.

Figure 1: Security Framework

VMware's Information Security Management System

VMware has implemented various information security policies and procedures that are in line with its overall corporate objectives, which demonstrate a commitment to the management of a formal Information security Management System (ISMS) that fulfils VMware's obligations to its customers regarding information confidentiality, integrity, and availability. Our ISMS reflects the following considerations and objectives:

- The threats, vulnerabilities, and likelihood of occurrence identified by assessment of risks relative to the overall business strategy and objectives.
- The legal, statutory, regulatory, and contractual requirements that VMware and relevant and applicable partners, contractors, and service providers must comply with.
- The principles, objectives, and business requirements for information handling, processing, storing, communicating, and archiving developed by VMware to support its business operations.

VMware personnel are obligated to comply with VMware ISMS data protection requirements in their respective roles, process, projects, and programs. Failure to adhere to these policies and procedures may result in disciplinary action, including possible termination, and civil and/or criminal liability.

Asset Management

VMware maintains an asset management program as part of our ISMS to categorize both physical and logical assets. The Asset Management program is reviewed at least annually, and all changes are approved by our Information Security Governance Committee.

Data Center Operations teams maintain an inventory of all production assets including, but not limited to, software license information, software version numbers, component owners, machine names, and network addresses. Inventory specifications may include device type, model, serial number, and physical location (where applicable).

Data Classification and Handling

VMware has a comprehensive Data Classification Policy and handling and protection standards for all electronic and paper media. Data classification is one of the foundational elements of the VMware ISMS. Controls and protections for information are dependent upon identifying proper data classifications. VMware's Confidential Data Classification Program provides a matrix of controls arranged by the data lifecycle, from creation of the data to its destruction, and covers all forms of media while in use, in transit or archived, and the program is audited annually by independent third-party auditors. The policy focuses on data classification sources, status, risks, and categories associated with the normal data lifecycle. Assets are classified in terms of their value, legal requirements, sensitivity, and criticality to VMware and our customers. Customer-owned information is classified as "Restricted" which is the most stringent data classification at VMware.

Physical Security

VMware physical security policy governs security for our offices, data centers, support centers, and other global business locations to safeguard information systems and staff.

Key elements of this policy include controls around: physical security perimeters, physical entry controls, physical access, securing offices, rooms and facilities, visitors to facilities, records, preventing the misuse of facilities, protecting against external and environmental threats, working in secure areas, access to restricted areas, delivery and loading areas, equipment siting and protection, supporting utilities, equipment maintenance, removal of assets, security of equipment and assets off-premises, secure disposal or reuse of equipment, unattended user equipment and clear desk and clear screen.

Horizon Cloud Service components are hosted in various third-party data center locations globally. These data center partners maintain physical and environmental security controls for the cloud delivered service.

Data Center Security

VMware partners with *third-party IaaS providers* to host applicable components of Horizon Cloud Service (Horizon Cloud control plane, Horizon Cloud on Microsoft Azure, etc.). The IaaS providers have undergone SOC2 Type 2 audits and have achieved at least ISO 27001 certification. Physical addresses for Horizon Cloud Service hosting locations are confidential and on-site visits are forbidden.

Our data center providers are required to follow the same minimum requirements for redundancy and physical access control, including:

- Ingress and egress points are secured with devices that require individuals to provide multi-factor authentication before granting entry or exit through a minimum combination of badge access, biometrics and mantraps.
- Physical access is controlled at building ingress points by 24x7 on-site professional security staff utilizing surveillance, detection systems, and other electronic means.
- Door alarming devices are configured to detect instances where an individual exits or enters a data layer without providing multi-factor authentication.
- Physical access points to data centers are recorded by Closed Circuit Television Camera (CCTV). Recordings are retained according to legal and compliance requirements.
- Environmental control systems are equipped minimally with N+1 power, cooling and fire suppression measures to ensure continuous operations.
- Data center partners are required to maintain certifications that are minimally in alignment with ISO 27001 standards.

VMware Offices

All VMware offices deploy physical and environment security measures to safeguard VMware facilities, staff, and assets. VMware uses a combination of building design, environmental controls, security systems, and designated security personnel, in conjunction with corresponding procedures, physical and environmental controls, to restrict access to information services and information assets. Controls include, but are not limited to:

- Implementing entry controls to secure VMware facilities.
- Maintaining and monitoring an audit trail of all access to the site through badge and visitor logs.
- Requiring visitor sign in with date and time of entry and departure, and supervising visitation.
- Performing regular access right reviews to secure areas and updating or revoking these rights as necessary.
- Revoking all access rights to VMware facilities and restricted areas immediately and deactivating access codes known by the staff upon staff termination.

Human Resources and Personnel Security

Human Resource considerations include processes for background screening, employment agreements, training, and employee termination.

Employee Background Screening

Pursuant to local laws, regulations, ethics, and contractual constraints, all employment candidates, contractors, and involved third parties are subject to background verification. VMware conducts criminal background checks, commensurate with the employee position and level of access to the service.

Confidentiality Agreements

VMware personnel and alternative workforce (AWF) are required to sign confidentiality agreements. Additionally, upon hire, personnel are required to read and accept the Acceptable Use Policy and the VMware Business Conduct Guidelines. Employees who violate VMware standards or protocols are subject to appropriate disciplinary action.

Employee Training

In alignment with the ISO 27001 standard, all VMware personnel and AWF are required to complete annual business conduct and security awareness training. Personnel with access to cloud production environments receive additional training as they assume job roles and responsibilities. VMware periodically validates that employees understand and follow the established policies through compliance audits.

VMware uses an enterprise Learning Management System (LMS) to deliver required onboarding and annual security awareness training. The LMS records successful completion and reports are reviewed during ISMS review meetings. This training must be completed before authorizing access to production systems.

Awareness training topics include, but are not limited to:

- Secure system configuration
- User account management policies
- Environmental control implementation and operation
- Incident Response plans and procedures
- Disaster Recovery plans and procedures
- Physical Security controls

Employee Termination

VMware terminates access privileges to systems when an employee leaves the company. An employee who changes roles within the organization will have access privileges modified according to their new position. Terminated employees are required to return assets.

Business Continuity

This program implements appropriate security controls to protect its employees and assets against natural or man-made disasters. As a part of the program, a runbook system automates policy review, and policy updates are made available to appropriate individuals. Additionally, these policies and procedures include defined roles and responsibilities supported by regular workforce training. VMware determines the impact of any disruption to the organization through identifying dependencies, critical products, and services.

Our business continuity plan identifies what preparations must be made in advance of a disruption and the procedures for if an event actually occurs. The plan is reviewed annually to determine which business processes are most critical and what resources – people, equipment, records, computer systems, and office facilities – are required for operation. All documented plans follow an annual standard maintenance, assessment, and testing schedule.

Risk Management

In alignment with the ISO 27001 standard, VMware maintains a Risk Management program to mitigate and manage risk companywide. We perform risk assessments at least annually to ensure appropriate controls implementation to reduce the risk related to the confidentiality, integrity, and availability of sensitive information.

VMware cloud management has a strategic business plan to mitigate and manage risks which requires management to identify risks within its areas of responsibility and to implement appropriate measures designed to address those risks. VMware cloud management re-evaluates the strategic business plan at least bi-annually.

VMware's Risk Management Program includes:

- Identifying and characterizing threats.
- Assessing the vulnerability of critical assets to specific threats.
- Determining the risk (i.e., the expected likelihood and consequences of specific types of attacks on specific assets).
- Identifying ways to reduce those risks.
- Prioritizing risk reduction measures based on a strategy.

Vendor Risk Management

VMware has a comprehensive vendor procurement and risk management program to choose providers that meet identified security baseline requirements. Supplier agreements require that providers comply with applicable laws, security and privacy obligations.

VMware has a formal process to document and to track non-conformance as a part of our ISMS. To assure reasonable information security across our information supply chain, VMware also conducts risk assessments for service sub-processors at least annually to ensure appropriate controls are in place to reduce risks to the confidentiality, integrity, and availability of sensitive information."

Sub-processors

VMware leverages sub-processors to provide certain services on our behalf. Refer to the *Horizon Services Sub-Processors Addendum* for a list of sub-processors used globally. VMware is responsible for any acts, errors, or omissions of our sub-processors that cause us to breach any of our obligations. VMware enters into an agreement with each sub-processor that obligates the sub-processor to process the Personal Data in a manner substantially similar to the standards set forth in the *VMware Terms of Service*, and at a minimum, at the level of data protection required by applicable Data Protection Laws. Please refer to the *VMware Data Processing Addendum* for additional information.

Customers can sign up to receive updates to service sub-processors, please go to the *Cloud Services Preference Center* and enable notifications for updates to this sub-processor list.

Change Management

VMware maintains a detailed Change Management policy that defines controlled changes to production environments. Changes are processed through a formal program that includes approval, testing, and implementation.

Third-party and internal audits of these processes are performed at least annually under the VMware ISMS program and are essential to the VMware continuous improvement programs.

Configuration Management

VMware maintains a detailed Configuration Management policy based on industry best practices to harden the cloud environment; revisions and exceptions to the Configuration Management policy are processed through the Change Management policy to help ensure the confidentiality, integrity, and availability of our hosted offering.

VMware-managed components for Horizon Cloud Services are configured to meet PCI-DSS requirements, such as:

- Disabling unnecessary ports, services, and protocols.
- Inbound and outbound network controls.
- Reviewing server builds for gaps prior to image configuration.
- Hardening server configurations using GPO policies (i.e., account policies, user rights, security options, event log settings, app restrictions).

Vulnerability and Patch Management

VMware employs a rigorous Vulnerability Management program as part of the VMware ISMS. Risk analysis and acceptance activities are performed on vulnerabilities to confirm the vulnerability and to determine the appropriate means of addressing the vulnerability. VMware-managed Horizon Cloud Service components are patched according to PCI-DSS requirements: VMware applies CVSS scores from vendor and industry-specific bulletins to rank risks (ex., high, medium, low) and remediates risks accordingly. Critical vendor-supplied security patches are applied within one month of release.

System Monitoring

VMware Cloud Operations is staffed 7x24x365 and the team deploys several commercial and custom purpose-built tools to monitor the performance and availability of all hosted solution components. Components include the VMware-managed Horizon Cloud Service underlying infrastructure servers, storage, networks, portals, services, and information systems.

Vulnerability Scanning

Vulnerability scans are performed at least monthly on internal and external systems. System and application owners are required to address critical and high vulnerabilities with a plan of corrective action after vulnerability discovery. Other vulnerabilities are addressed with a plan of corrective action within a reasonable period.

VMware Security Response Center (VSRC)

The VMware Security Response Center (VSRC) leads the analysis and remediation of software security issues in VMware products. VSRC works with customers and the security research community to achieve our goals of addressing these issues and providing customers with actionable security information in a timely manner.

VSRC receives reports directly, and proactively monitors the security landscape and receives direct reports concerning security issues in VMware products. After validating a report, VSRC works with VMware Research and Development to develop a solution and schedule releases that address the issue. Meanwhile, VSRC keeps the reporter informed on progress. Upon remediating the issue, VSRC releases a VMware Security Advisory.

Security Advisories

VMware Security Advisories document remediation for security vulnerabilities that are reported in VMware products. Optionally, sign up to receive new and updated advisories via e-mail.

Customer Security Contact

VMware encourages users who become aware of a security vulnerability in our products or services to contact VMware with details of the vulnerability.

Please partner with your Technical Account Manager, Professional Services or Sales representative to open a support request on *VMware Customer Connect*, or you may file a support request directly to notify the appropriate support channels.

When raising a support request, please provide as much detail as possible, including CVE identifiers, VMware product version and build number, and any details regarding which vulnerability scanner was used, etc. as applicable.

Note: VMware does not permit direct vulnerability scans of VMware-hosted production environments.

- We encourage use of encrypted email. Our public PGP key is found at kb.vmware.com/kb/1055.

Incident Management & Response

The VMware Incident Response program plans, and procedures have been developed in alignment with the ISO 27001 standard. VMware maintains contacts with industry bodies, risk and compliance organizations, local authorities and regulatory bodies. Points of contact are regularly updated to ensure direct compliance liaisons have been established and prepared for a forensic investigation requiring rapid engagement with law enforcement. Under the VMware ISMS program, the incident response plan is tested at least once annually, whether or not a security incident has occurred.

Figure 2: Incident Response Lifecycle

VMware Security Operations Center (SOC)

The VMware SOC is staffed and monitors alerts on security anomalies 7x24x365. The SOC leverages multiple log capture, security monitoring technologies and intrusion detection tools to look for unauthorized access attempts, monitor for incoming threats, and detect activity from malicious insiders.

Incident Reporting

All staff are responsible for reporting information security events as quickly as possible. At a minimum, these situations include:

- Ineffective security controls or access violations.
- Breach of information integrity, confidentiality or availability expectations.
- Human errors.
- Non-compliances with policies or guidelines.
- Breach of physical security arrangements.
- Uncontrolled system changes.
- Malfunction of software or hardware

Breach Notification

In the case of a confirmed data breach of a VMware-managed service component, VMware shall without undue delay notify affected customers of the breach in accordance with applicable laws, regulations, or governmental requests.

Software Development Lifecycle

Code Security Development Lifecycle Principles

VMware's Security Development Lifecycle (SDL) program is designed to identify and mitigate security risk during the development phase of VMware software products. The development of VMware's SDL has been heavily influenced by industry best practices and organizations such as SAFECode (the Software Assurance Forum for Excellence in Code) and BSIMM (Building Security in Maturity Model).

VMware Security Evangelism team works to actively cultivate relationships in the security community. VMware has been an active participant in the broader software industry security community and became an early BSIMM member in 2009: We have completed several reviews by BSIMM of our SDL. Findings are incorporated into our SDL to drive continuous improvements. VMware is a member of SAFECode, an organization driving security and integrity in software products and solutions. VMware also works closely with Industry Organizations, Security Analysts and Researchers, etc. to stay current on the Industry threat landscape and security best practices. VMware Product Security VMware SDL is continuously assessed for its effectiveness at identifying risk and new techniques are added to SDL activities as they are developed and mature.

VMware encourages continuous employee training through programs which subsidize certification attempts (i.e., CISSP, CCSP), relevant conference passes, training classes, and subscriptions to leading online training platforms for enhancing technical and business acumen. Additionally, employees can use job rotation programs designed to reignite and broaden employee work experience. Please refer to the *VMware Product Security Whitepaper* for additional information.

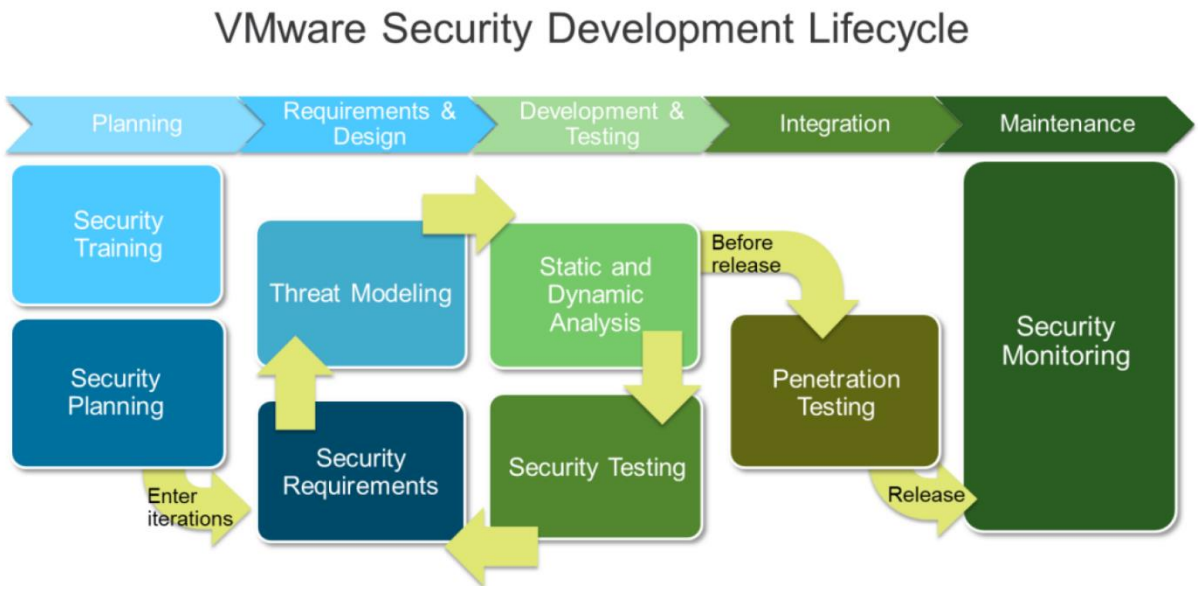

Figure 3: VMware Security Development Lifecycle

Security Engineering Processes

The VMware Security Engineering, Communications & Response (vSECR) team develops Product Security Requirements (PSR) to establish a security baseline for our products. These requirements are intended to guide teams through all stages of the SDL, from product inception through development and product testing to release. It also serves as a tool for senior management to benchmark product security against market expectations. VMware SDL activities include:

- Security Training – vSECR works with R&D Education to create and maintain training programs about product security. Managers, developers, and quality engineers can avail of these courses early in the lifecycle of their product.
- Security Planning – Good security starts with early planning, at the genesis of the SDL process. The SDL planning template forms the basis of the Security Review activity. VMware builds milestones and security reviews for the product so that security is continuously evaluated.
- Serviceability and Response Planning – vSECR works with product teams to help build security into their products' servicing model, which includes planning for:
    - Secure patching.
    - Open-source and third-party software licensing.
    - End of life support.
    - Security and management contacts for security response.
- Product Security Requirements Assessment – This activity examines how a product adheres to VMware PSR, which includes standards for:
    - Authentication
    - Authorization
    - Encryption
    - Certificates
    - Network security
    - Virtualization
    - Accountability
    - Software packaging and delivery
- Threat Modeling – This activity identifies security flaws and incorrect design assumptions present in the VMware Product Security architecture of a product.
- Open-Source and Third-Party Software Validation (OSS/TP) – This activity validates that OSS/TP software with known vulnerabilities are fixed before being included in a product release.
- Static Code Analysis – This activity uses automated tools to detect defects and security flaws in code.

- **Vulnerability Scanning** – This activity uses automated tools to detect security vulnerabilities in running systems.
- **Penetration Testing** – This activity uses internal and external security teams to try to break systems in isolated environments.
- **Security Review** – This activity examines the output and completion of all the other activities.

Open-Source Software

VMware uses some third-party and/or open-source code in our solution offerings, and we perform open-source and third-party (OSS/TP) software validation to safeguard against known vulnerabilities prior to being included in a VMware product release. Please refer to the publicly available *Open Source Disclosure page* for additional information on OSS/TP components.

Penetration Testing

VMware Testing

VMware performs extensive internal and external penetration tests at least annually. The penetration tests focus on identifying high impact vulnerabilities that could lead to exploitation, theft of data, and/or overall privilege escalation. The tests follow a method intended to simulate real-word attack scenarios and threats that could critically impact the data privacy, integrity, and overall business reputation.

Customer Penetration Testing

Customer-initiated penetration testing against the production environment is explicitly forbidden in the *Terms of Service.*

Horizon Service Cloud Security Overview

Horizon Service delivers virtual desktops and applications across multiple deployment options, including public cloud infrastructure in Microsoft Azure and/or on-premises deployments of Horizon. VMware-managed Horizon Cloud control plane and Horizon Cloud Service on Microsoft Azure environments are certified against PCI-DSS requirements. *The PCI AOC* is available to download directly from the *VMware Cloud Trust Center*

VMware and our customers share roles and responsibilities managing the security of Horizon Services. Applicable detail can be found in the applicable *Service Description*. Controls in the proceeding sections apply to VMware-managed components of the Horizon Cloud Service unless otherwise specified.

Key components of the Horizon Cloud Service and their functionality are as follows:

Horizon Cloud Service Component	Functionality	Hosting Management
Horizon Control Plane Management Services	Horizon Control Plane Services include the Horizon Cloud Administrator Console and additional optional features, such as *Universal Brokering*.	Shared Responsibility[1]
Horizon Cloud Pods on Microsoft Azure	Logical construct that defines a Horizon Cloud Service resource in customers' Microsoft Azure cloud capacity.	Shared Responsibility[2]
Horizon Pods	Horizon Pod deployments on VMC on AWS or on-premises.	Customer Managed
Horizon Cloud Monitoring Service	The Cloud Monitoring Service (CMS) gives you the ability to monitor capacity, usage, and health within and across your fleet of cloud-connected Pods, regardless of the deployment environments in which those individual Pods reside.	VMware Managed
Horizon Cloud Service on Microsoft Azure Component		
SmartNode	Manages all infrastructure resources such as creating resources on Microsoft Azure infrastructure and makes it available to users.	VMware Managed
Unified Access Gateway (UAG)	Provide secure Internet access to RD Session Hosted desktops and applications. Each deployment contains two Unified Access Gateways.	VMware Managed
Horizon Cloud Service on Microsoft Azure capacity	Sizing your Microsoft Azure infrastructure capacity and Horizon Cloud Service on Microsoft Azure capacity according to the number of users and workloads expected and maintaining the required Microsoft Azure infrastructure limits. Your Microsoft Azure capacity must also include room for the necessary Horizon Cloud components.	Customer Managed

Data Center Locations

Data center locations depend on the customer's use of Horizon Service. Specific details regarding sub-processors such as Data Center Partners and relevant Horizon Control Plane Management Services details can be found by visiting the *Horizon Service Sub-processors Addendum*

VMware-managed Horizon Cloud Service components are available in the US, Ireland, Germany, Australia, Japan and the UK in Microsoft Azure data centers. Data center physical addresses are confidential and on-site visits are forbidden.

[1] Please Note – This component is a shared responsibility which is detailed in the *Horizon Service Description*
[2] Please Note – This component is a shared responsibility which is detailed in the *Horizon Service Description*

Please see the *Horizon Service Sub-processors Addendum* for a full listing of Horizon Cloud Service components, such as Horizon Cloud Monitoring Service and Universal Broker.

Security Operations Controls

VMware Access to VMware Managed Production Environments

Access privileges to VMware-managed Horizon Cloud Service components are enforced using role-based access control, separation of duties, and the principle of least privileges. Production environment access is secured through an allowlist of source address and multi-factor authentication; and access is restricted to authorized members of applicable teams. Network Access Control Lists and NAT policies forward authorized inbound traffic. Logs are in place to review support staff access to all systems and environments per PCI-DSS requirements.

Configuration Hardening

VMware disables unnecessary ports, protocols, and services as part of baseline hardening standards to protect customer data according to stringent requirements laid out by PCI-DSS. Quarterly ASV scans are run and remediated according to the requirements determined by PCI-DSS.

Key Management

Policies and procedures for key management for Horizon Cloud Service are in place to guide personnel on proper encryption key management in alignment with PCI-DSS requirements. Access to cryptographic keys is restricted to named personnel and all access is logged and monitored.

Time Synchronization

Time synchronization is in place to ensure system times are accurate per PCI-DSS requirements.

Cloud Environment Monitoring

VMware Cloud Operations is staffed 7x24x365 and deploys several commercial and custom purpose-built tools to monitor the performance and availability of all hosted solution components. Components include the underlying infrastructure servers, storage, networks, portals, services, and information systems used in the delivery of VMware-managed service components.

Intrusion Detection & Prevention

VMware deploys several mechanisms to detect intrusions. These range from real-time IDS/IPS technologies, internal logs and tools to external intelligence (OSINT) data sources. VMware monitors for security events involving the underlying infrastructure servers, storage, networks, and information systems, used in service delivery.

Malware Controls

Per PCI-DSS requirements, regularly updated anti-virus software protects all VMware-managed Horizon Cloud Service systems susceptible to malware, such as Windows machines. Antivirus software is also installed on all employee workstations and configured to scan for updates to antivirus definitions and update registered clients routinely and users cannot disable the software.

Log Management

VMware-managed Horizon Cloud Services leverage a robust, centralized SIEM infrastructure per PCI-DSS requirements. All critical systems and privileged access, firewall and IDS logs are logged and monitored. VMware System Security logs and events are centrally aggregated and monitored in real-time 7x24x365 by the VMware Security Operations Center (SOC). Logs forwarded to the VMware SOC are retained for 1 year and up to 5 years in archive.

Disaster Recovery

Horizon Cloud Services are supported by defined enterprise resiliency programs which include business continuity and disaster recovery mechanisms for VMware-managed components per PCI-DSS requirements. VMware publishes a shared responsibility model for disaster recovery in the *Horizon Service Description*.

Recovery Time Objectives (RTO) and Recovery Point Objectives (RPO)

All VMware-managed Horizon Cloud Service components are covered by disaster recovery and business continuity processes; we have defined applicable RTO and RPOs in the table below. VMware does not provide disaster recovery and backup processes for customer-hosted infrastructure and customer-managed data.

Horizon Cloud Service	RTO	RPO
Horizon Cloud control plane	4 hours	4 hours
Horizon Cloud Service on Microsoft Azure – VMs and images	Data is customer managed	Data is customer managed
Horizon Subscription – VMs and images	Data is customer managed	Data is customer managed

Horizon Cloud Control Plane

Horizon Cloud control plane is a multi-tenant cloud service that has been built with security in mind and is PCI-DSS certified. A customer is paired with only one Horizon Cloud control plane instance at any time.

The Horizon Cloud Control Plane is used for both Horizon Cloud Service on Microsoft Azure and Horizon Subscription components.

Customer Access to their Production Environment and Data

Customers manage applicable access to the Horizon Cloud application administrative interfaces, such as the Horizon Administrative Portal and Horizon Cloud Control Plane orchestration services. Identity is tied to customers' Active Directory.

Customer administrators can configure role-based access controls (RBAC) to restrict the depth of access and user management information and features available to each Horizon Administrative Portal user. Horizon Cloud application administrator changes are retained for review within the console event log. Please refer to *VMware Docs* for additional information.

Service Resiliency

Horizon Cloud Control Plane uses multiple Availability Zones in available regions. The Horizon Cloud Control Plane stores data in a fully replicated cluster across multiple fault domains within the service's region. Furthermore, explicit offline backups of the data are taken and stored in region for disaster recovery and high availability.

Disaster recovery plans are documented, reviewed annually, and tested against various disaster scenarios. The infrastructure is designed to ensure that customers will typically not notice a disruption during a component or system failure. Service resiliency strategies include, but are not limited to:

- The use of multiple Availability Zones.
- Daily point-in-time backups are stored for 30 days and support staff review backup processes to ensure data integrity. System audit log data is retained for 90 days.
- Backups are encrypted in transit (TLS 1.2) and at rest (AES 256).

Recovery Time Objectives (RTO) and Recovery Point Objectives (RPO)

RTO and RPO for the Horizon Cloud Control Plane is 4 hours.

Data Collection

Data collected and stored by the Horizon Cloud Control Plane differs depending on customers' use of Horizon Cloud Service on Microsoft Azure and/or Horizon 8 Subscription. Please see the corresponding sections for details.

Horizon Cloud Service on Microsoft Azure

Horizon Cloud Service on Microsoft Azure is certified against PCI-DSS. Importantly, VMware and customers share ownership of and responsibility for various aspects of the service which are outlined in the *Horizon Service Description*.

Horizon Cloud Pods on Microsoft Azure use three networks to connect components:

- DMZ – Enables inbound traffic from the Internet to the external Unified Access Gateways. Network Security Groups (NSG) that are a feature of Microsoft Azure are used to inbound control access and allow only the required ports and protocols to the external Unified Access Gateways.
- Management – An internal management network, allowing the Pod Managers to control the Unified Access Gateways and providing an outbound Internet channel for connection to the Control Plane and the Azure API. There is no inbound networking connectivity to this network.
- Desktop – Customer-controlled network for the VDI desktops and RDSH Farms (supporting both multi-session desktops and applications), internal Unified Access Gateways, and Pod Managers (user-facing interface).

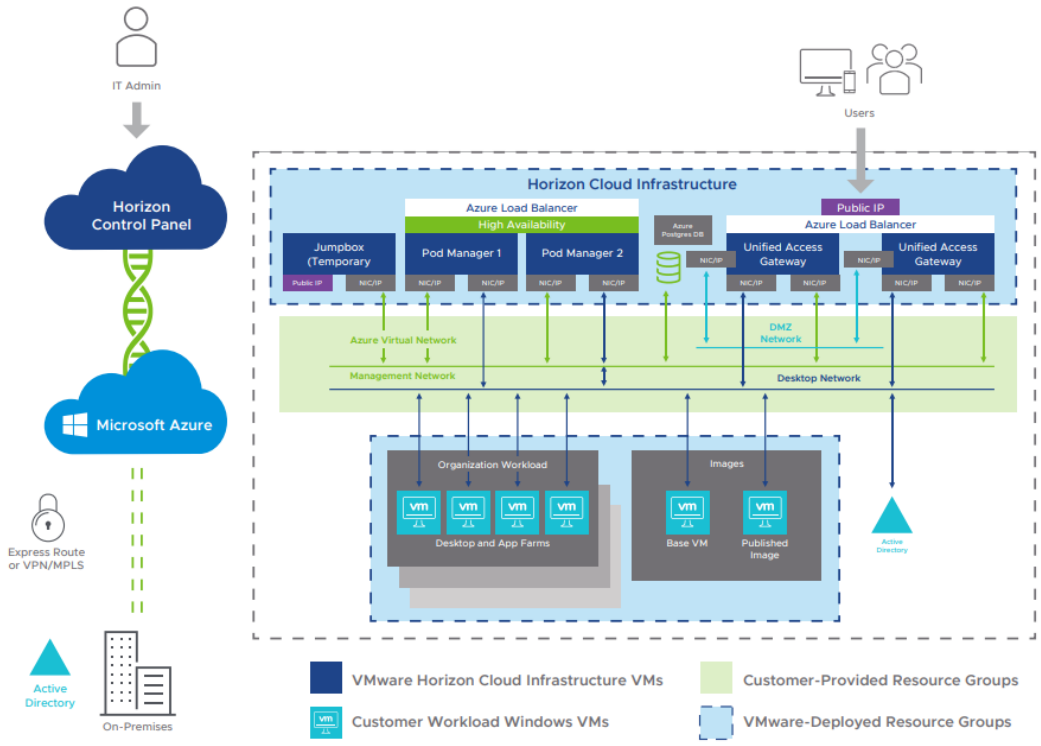

Figure 4: Horizon Cloud on Microsoft Azure Architecture Diagram

Horizon Cloud Service can optionally communicate with on-premises, corporate network resources via VPN or ExpressRoute connection. This connection may be required if the Active Directory or user data and applications are located on premises. Typically, internal end users connect to the Pod over this connection. To help ensure data is secure, the Horizon Cloud Control Plane uses strong in transit encryption over the public internet as prescribed by PCI-DSS Standard.

For detailed, up-to-date information about the protocols and ports for the service, please review the product documentation and detailed diagrams are available in a TechZone article entitled *VMware Horizon Cloud Service on Microsoft Azure Network Ports Diagrams*.

Active Directory

The Horizon Cloud Service uses customer Active Directory for user management and entitlements. There are two types of Active Directory accounts required by the service:

AD Account	Permission Requirements	Bind Type
Domain bind and domain bind aux account	Active Directory domain bind and domain aux account (a standard user with read access) that has permission to read objects in AD	GSSAPI and NTLMSSP binds are used for these accounts Optionally toggle Microsoft GPO of "Require Signing"
Domain join and domain join aux account	Active Directory domain join and domain join aux account that has additional permissions to perform Sysprep operations and join computers to the domain, create new accounts, and more	Only GSSAPI binds are used for these accounts.

Horizon Cloud on Microsoft Azure uses an industry-standard approach / design to securely communicate with Microsoft Active Directory using SASL-GSSAPI. All communication with Active Directory is encrypted using Kerberos (SASL-GSSAPI); this is referred to as "signed and sealed" connection. With SASL-GSSAPI, you can help ensure that you continue to follow Microsoft best practices to reject unsigned/unencrypted LDAP Requests, by having the LDAP "Require Secure Signing Policy" enabled on your Active Directory Servers with Horizon Cloud on Microsoft Azure.

Connectivity to the Horizon Cloud Control Plane

The Microsoft Azure Pod makes outbound calls to the Horizon Cloud Control Plane over the Internet via the Pod Managers. There is no inbound management connectivity from the Microsoft Azure Pods. Data is transmitted between the Horizon Cloud Control Plane and Microsoft Azure Pods, over the public internet, via TLS 1.2 and authenticated with strong, periodically rotated keys and authentication tokens. The connection to the Horizon Cloud Control Plane allows access to the Horizon Pods on Microsoft Azure to enable:

- Configuration changes.
- Live state queries.
- Supportability requests, including interactive support, log fetching, and component health queries.

Updates and Troubleshooting

As part of initial deployment, VMware deploys a temporary jump box inside customers' Horizon Pod on Microsoft Azure. This transient jump box facilitates the creation of the external Unified Access Gateway (UAG) in a dedicated Azure Virtual Network (VNet) and any subsequent updates to the UAG. The jump box VM is deleted after the UAG deployment process is complete. For subsequent UAG updates or for troubleshooting, the jump box VM is re-recreated and then deleted.

In the event of troubleshooting or diagnosing an issue, VMware can:

- Obtain log files and crash reports from the Horizon Cloud Pod (made available as "Support Bundle"), which will show usernames, times when users have accessed the system, and other environment information, including IP addresses and hostnames.
- Obtain other files, such as configuration files, from the deployed infrastructure VMs within the Horizon Cloud Pod.
- Have real-time access to the current operational health status of the Horizon Cloud Pod.
- Have interactive shell access on the Pod Manager for troubleshooting and support.

Secure Credential Storage

The Horizon Cloud on Microsoft Azure service stores the following credentials for each Horizon Cloud subscription account:

- Active Directory domain bind and domain bind aux username and password.
- Active Directory domain join and domain join aux username and password.
- File share username and password.
- Azure subscription credentials.

These user credentials are protected with AES 256-bit encryption when stored in the cloud. The credentials are accessible by the Horizon Cloud Service when performing operations on behalf of the account or to distribute to components that need access.

On the Horizon Cloud Pods on Microsoft Azure, encryption keys used by the platform are unique per Pod. The credentials are accessible by the Pod service when performing operations on behalf of the organization.

Data Collection

Horizon Cloud Service on Microsoft Azure service stores and handles different categories of data. The table below defines each category, indicating where the data is stored, who has access to it, and privacy notes. Please refer to the Cloud Monitoring Service Section and corresponding table for details regarding what is collected when that service is enabled

WHAT	WHERE	WHO	PRIVACY NOTES
End User Data			
• Data created by end users, for example, files, user settings, and user-installed applications.	• This is stored only in the VDI desktops, RDSH Farms and external services (for example, file servers) which you deploy and configure. VMware has no access to this data.	• End users access this data from within their VDI desktop sessions or RDSH app and desktop sessions. • VMware does not have access, nor does it manage this data • Customers manage access to the VMs or external file services that are under your control.	• Because this data is authored by end users, it may contain personal data. • You have full control of where this data is stored. • The disk images storing this information may be encrypted.
Horizon Cloud Subscription Account Definition			
• Data about the definition of your service, for example, Active Directory configuration. • Pod configuration; desktop assignments, application assignments, farm, and app definitions; entitlements to services; and assignments to services. • This includes storing usernames and credentials for integrated services like Active Directory and Microsoft Azure. • *See Secure Credential Storage* for more information – including details on credential encryption.	• This data is stored in both the Azure Pods and in the Horizon Cloud Control Plane.	• You own this data and manage it through the Administration Console. • VMware can access this data to provide support and understand the service usage. • The service itself can use the supplied credentials to operate. • VMware operations and support staff are not given access to stored credentials.	• The following personal data is stored: ○ User/admin identity: name, username, user IDs (for example, AD SID and GUIDs). • The main use of the personal data is to identify the entitlement of end users to services (VDI desktops, remote applications, AV applications, Workspace ONE UEM policies), and the assignment of end users to resources (for example, linking an end user to a specific VDI desktop VM in a dedicated assignment). • In addition, IT administrators are identified and given rights within the system.

IT Administrator			
• Data about your usage of the system, for example, login times, and audit information tracking changes to service configuration and operations.	• This data is stored in both the Pods and in the control plane.	• You can see audit data. • VMware can access this data to provide support and understand the service usage.	• The following data is stored: o Admin identity: name, username, user IDs (for example, AD SID and GUIDs). • Audit and log data for system changes will identify the IT administrator who caused the change.
Licensing Data			
• Order number, • SID, • SKU, • Quantity of users, • License duration, • Type of license.	• The Data Lives within the Horizon Cloud Control Plane	• You can see this data when you login to the Horizon Cloud Administrative Console • VMware can access this data to provide support and understand service entitlement.	• This data enables customers to compare what they have chosen to how they are using the solution on a day-to-day basis • This data enables VMware to help ensure correct allocation of resources to customer as well as support other license related activity

The Horizon Cloud Service on Microsoft Azure service caches minimal Active Directory group information to entitle desktop and application assignments, URL redirection assignments, and more. When a user logs in, they are authenticated and authorized without using the cache to ensure that only the most recent data is used. Once logged in, entitlement checks are made against the cached data to better ensure high performance.

Horizon Subscription

To access Horizon Cloud Services, customers connect their on-premises and/or VMC on AWS Horizon Pods to the VMware-managed Horizon Cloud Control Plane. As part of the pairing process, the Horizon Cloud Connector virtual appliance connects the Connection Server to the Horizon Cloud to manage the Horizon subscription license and other services. VMware does not have access to customer Horizon Pods. Please see the *Horizon Service Description* for more detail.

Architecture Diagram

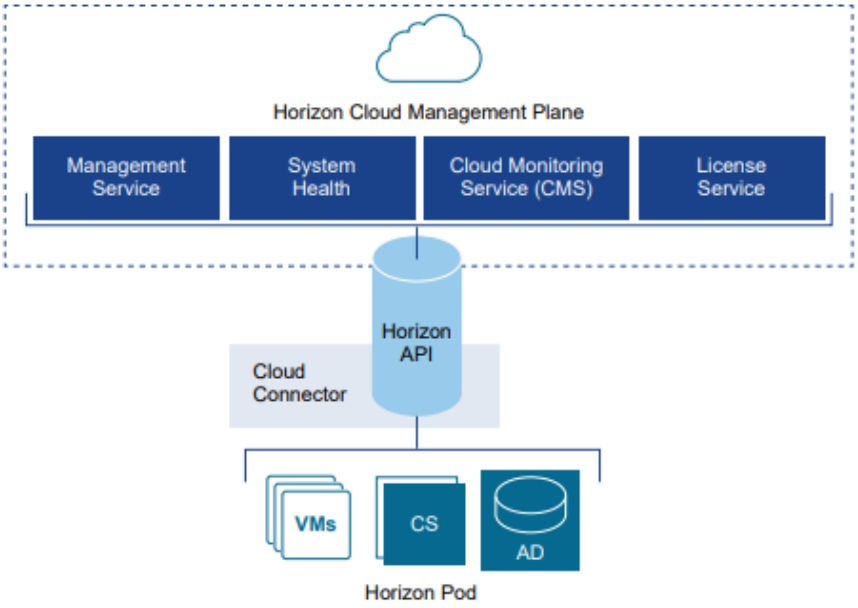

Figure 5: Horizon Subscription Architecture Diagram

Connection to the Horizon Cloud Control Plane

Horizon Cloud Connector

The Horizon Cloud Connector is a virtual appliance that connects a Connection Server in a Pod with the Horizon Cloud Service. The Horizon Cloud Connector is required to use Horizon 8 subscription licenses. To help ensure data is secure, the Horizon Cloud Control Plane uses strong in transit encryption, over the public internet, as prescribed by PCI-DSS Standard.

Universal Broker

The Universal Broker is an optional feature of the Horizon Cloud Control Plane. The Universal Broker client runs within the Horizon Cloud Connector for each of your cloud-connected Horizon Pods. The client is part of the OVA file for Cloud Connector 1.5 or later and is automatically installed when you pair the Cloud Connector with your Pod. In general, a minimal amount of data is stored in the Universal Broker and includes Certificates and User to Homesite Mapping.

Data Collection

Horizon Subscription store and handles different categories of data. The table below defines each category, indicating where the data is stored, who has access to it, and privacy notes.

WHAT	WHERE	WHO	PRIVACY NOTES
End User Data			
• Data created by end users, for example, files, user settings, and user-installed applications.	• This is stored only in the VDI desktops, RDSH Farms and external services (for example, file servers) which you deploy and configure. VMware has no access to this data.	• End users access this data from within their VDI desktop sessions or RDSH app and desktop sessions. • VMware does not have access, nor does it manage this data • Customers manage access to the VMs or external file services that are under your control.	• Because this data is authored by end users, it may contain personal data. • You have full control of where this data is stored. • The disk images storing this information may be encrypted.
Horizon Cloud Account Data			
• In a "subscription-only" implementation of Horizon, this type of data would entail the following information: o Company Name o Customer VMware customer connect email address o Customer contact info, First Name and Last Name o Pod Name, Pod Version, Pod Health, Pod Location • Cloud Connector Logs	• This data is stored in both the Cloud Connected Pods and in the Horizon Cloud Control Plane.	• You own this data and manage it through the Administration Console. • VMware can access this data to provide support and understand the service usage. • The service itself can use the supplied credentials to operate. • VMware operations and support staff are not given access to stored credentials.	• The following personal data is stored: o User/admin identity: name, username, user IDs (for example, AD SID and GUIDs). • The main use ofthe personal data is to identify the entitlement of end users to services (VDI desktops, remote applications, AV applications, Workspace ONE UEM policies), and the assignment of end users to resources (for example, linking an end user to a specific VDI desktop VM in a dedicated assignment). • In addition, IT administrators are identified and given rights within the system.

IT Administrator			
• Data about your usage of the system, for example, login times, and audit information tracking changes to service configuration and operations.	• This data is stored in both the Pods and in the Horizon Cloud Control Plane.	• You can see audit data. • VMware can access this data to provide support and understand the service usage.	• The following data is stored: ○ Admin identity: name, username, user IDs (for example, AD SID and GUIDs). • Audit and log data for system changes will identify the IT administrator who caused the change.
Licensing Data			
• Order number, • SID, • SKU, • Quantity of users, • License duration, • Type of license.	• The Data Lives within the Horizon Cloud Control Plane	• You can see this data when you login to the Horizon Cloud Administrative Console • VMware can access this data to provide support and understand service entitlement.	• This data enables customers to compare what they have chosen to how they are using the solution on a day-to-day basis • This data enables VMware to help ensure correct allocation of resources to customer as well as support other license related activity

Universal Broker

The Universal Broker is an optional feature of the Horizon Cloud Control Plane. The Universal Broker client runs within the Horizon Cloud Connector for each of your cloud-connected Horizon Pods. The client is part of the OVA file for Cloud Connector 1.5 or later and is automatically installed when you pair the Cloud Connector with your Pod. In general, a minimal amount of data is stored in the Universal Broker and includes Certificates and User to Homesite Mapping.

Horizon Cloud Monitoring Service

Whether a cloud-connected Pod lives on-premises, in VMware Cloud on AWS, or in Microsoft Azure, the Horizon Cloud Monitoring Service obtains capacity-, health-, and usage-related data from the Pod and presents that data to you within the Horizon Cloud Administration Console. That console is your single pane of glass for working with your tenant's fleet of cloud-connected Pods. The Horizon Cloud Monitoring Service is optional and resides outside the Horizon Cloud Control Plane boundary. Due to this design, CMS is not in scope for the PCI certification and corresponding controls.

The Horizon Cloud Monitoring Service enables collection of user session information for service utilization, trending, and historical analysis. The data is used in charts on the Dashboard page and in reports on the Reports page. The data collected is regarding the end users' usage of the system, for example, login times, application and desktop launches, VDI desktop and RDSH performance data, VDI and RDSH server hostnames, client IP address, and username. You can opt out of the monitoring service at any time.

When the monitoring service is enabled, there are two modes of operation:

- User Session Information is collected.
- User Session Information is not collected.

You can use the Enable User Session Information toggle to enable or disable this mode at any time.

When the Enable User Session Information is disabled, the system will collect user session information for a limited period and will no longer store user identities for historical queries. Instead, the data is anonymized using hashing so that certain aggregated queries are still possible to enable real-time administration, but individual users cannot be identified. In addition, the historical and aggregated viewing of that user information will be disabled. Thus, the reports that would display historical and aggregated viewing of monitoring data, such as the Session History report, will not be available.

Note: When Enable User Session Information is disabled, user-identifying data is stored for up to 24 hours to provide real-time support of the service. Customer administrators can disable the Horizon Cloud Monitoring service completely if you do not want any of the monitoring data to be stored in the cloud monitoring service at all.

WHAT	WHERE	WHO	PRIVACY NOTES
Cloud Monitoring Service details: This functionality is optional and can be disabled			

• Data about the end users' usage of the system, for example, login times, application and desktop launches, VDI and RDSH performance data, VDI and RDSH server hostname, and client metrics such as IP Address, version etc.
• This data is not collected if you disable Horizon Cloud Monitoring Service (see Monitoring for more details) .
• The data is normally stored for the life of your Horizon Cloud subscription and provides historical reporting and aggregated viewing of data.
• Once the monitoring service is enabled, you may further opt out of collecting user session information (Enable User Session Information = No) to reduce the long-term storage and anonymize the PII data as stored by the monitoring service .
	• End-user usage data is maintained both in the Horizon Pods and in the Horizon Cloud Control Plane.
	• Data is explicitly stored in the Pod for immediate and historic query.
	• Data is implicitly logged in log files as part of the operation of the system.
	• Data is explicitly stored in the Horizon Cloud Control Plane for immediate and historic query.
	• Data is implicitly stored in the Horizon Cloud Control Plane as part of administrator notifications that may identify end users.
		• This data is used by you to help manage your end user's experience.
		• VMware may use this data to monitor the overall service and provide service support.
			• The following PII data is stored unless the Horizon Cloud monitoring service is disabled.
			  ○ User identity: name, username, user IDs (for example, AD SID)
			  ○ Client IP address
			  ○ Login timestamp
			  ○ VDI and RDSH VM hostname
			  ○ Application launches
			• Both you and VMware can see both Primary and Secondary PII data.
			• Opting in or out of Enable User Session Information determines how long the Primary PII data is stored.
			• When disabled, this data is maintained to provide immediate service and support (for example, who is currently logged in), but this data is not stored historically (for example, who logged in last week).

Release Management and Maintenance

VMware has defined applicable Horizon Service uptime SLAs in the *VMware Horizon Service SLA*., Updates are a shared responsibility between VMware and customers as outlined in the *Horizon Service Description*.

Release Schedules

VMware communicates feature releases and service announcements through *VMware Docs*, *VMware Blogs*, *VMware Customer Connect*, and by email.

Routine Maintenance

Occasionally, it is necessary for VMware to perform maintenance that has the potential to impact the availability of customer environments outside of scheduled maintenance windows, and VMware reserves the right to do so. A minimum of five days' advance notice is given for routine maintenance.

Per the *Horizon Service Description* which governs the service

> *"In the event of issues that require diagnosis and troubleshooting, select personnel from the VMware Horizon Cloud Service operations team will have the ability to remotely log in to the Horizon Pod appliances in your Microsoft Azure infrastructure to review and gather logs or to perform remote emergency remediation."*

Emergency Maintenance

Emergency maintenance is defined as potentially impactful maintenance activity that must be executed quickly due to an immediate, material threat to the security, performance, or availability of the Service Offering. Every attempt will be made to provide as much advance notice as possible, but notice depends on the severity and critical nature of the emergency maintenance.

Customer Support Services

VMware's Global Customer Support Services teams are strategically *placed around the world* operating in a follow-the-sun model from locations in the US, Costa Rica, Ireland and the UK, India, China, Japan, Australia, and Singapore. Each center is staffed with engineers that provide industry-leading expertise in mobility and have experience supporting real-world mobile environments. Support is available in seventeen languages. Support may be provided from other offices as support team continues to expand to meet customer requirements.

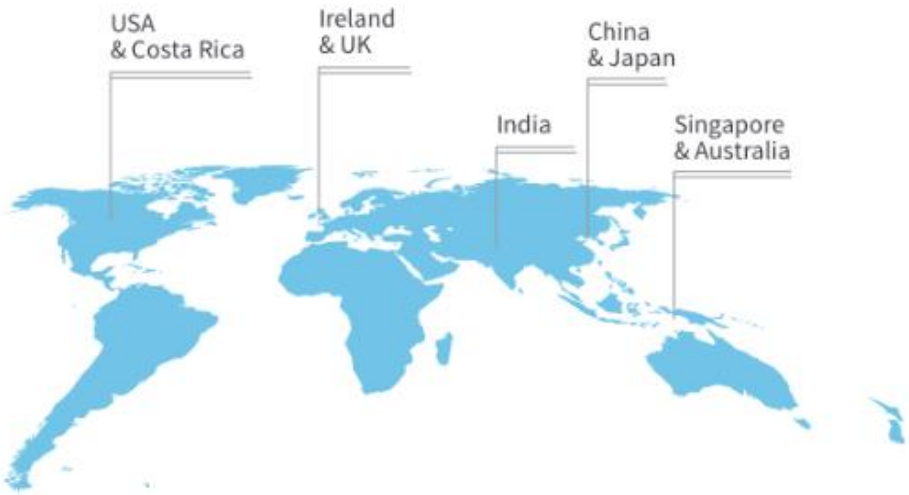

Figure 6: Global Support Locations

Support Packages

VMware provides multiple support options designed to fit specific customer requirements. The following support packages are available for Horizon Cloud Service:

- *SaaS Basic Support* – Weekday global support for SaaS products, 12x5 (SaaS Severity 1 issues 24x7)
- *SaaS Production Support* – Focused, 24-hour support for SaaS products, (SaaS Severity 1 issues 24x7)
- *VMware Success 360* – Priority access to Senior Engineers, Account Management, and advanced Skyline features, 24x7

For the most up-to-date support offerings, please refer to the *VMware Customer Support Offerings* page. Existing support customers can leverage the *VMware Customer Connect*. Please visit the *Cloud Service Support Policies page* for additional information.

Privacy and Compliance

Data Sovereignty and Service Sub-Processors

For data processing locations please refer to the *Horizon Service Sub-processors Addendum*. VMware affiliates may also process Content. As set forth in the VMware Data Processing Addendum, VMware has adequate data transfer mechanisms in place with each sub-processor. Please refer to the VMware Data Processing Addendum and service Sub-processors Addendum for additional information.

Privacy and the EU General Data Protection Regulation (GDPR)

Horizon Cloud Service customers are responsible for using and configuring the service in a manner which enables the customer to comply with applicable Data Protection Laws, including the GDPR, as a data controller or as a data processor with respect to Personal Data. VMware complies with applicable data processor obligations.

End users can also contact privacy@vmware.com if they wish to exercise data subject rights (outlined in the VMware Privacy Notice), so that VMware may consider the request under applicable law. To protect privacy and security, VMware may take steps to verify requestor identity before complying with the request.

For additional information regarding customer and VMware responsibilities please refer to *VMware Privacy Policy* and *VMware Data Processing Addendum*.

Binding Corporate Rules

Whenever VMware, acting as a processor, shares personal information originating in the European Economic Area ("**EEA**"), it will do so on the basis of its Irish Data Protection Commissioner and peer approved binding corporate rules known as the VMware Binding Corporate Rules ("**VMware's BCRs**") which establish adequate protection of such personal information and are legally binding on the VMware Group.

VMware's BCRs were approved by the European Data Protection Authorities on May 23, 2018. You can review confirmation that this review has now been completed here. To access VMware's BCRs, please see VMware's Processor Binding Corporate Rules, which apply when VMware processes personal data on behalf of its customers. To see a listing of the VMware affiliates that have signed an Intra-Group Agreement for VMware's BCRs, click here. For further information, click here.

Data Protection Requests

If VMware receives any requests from individuals or applicable data protection authorities relating to the processing of Personal Data within Horizon Cloud Service, including requests from individuals seeking to exercise their rights under Data Protection Law, VMware will promptly redirect the request to the customer. VMware will not respond to such communication directly without the customer's prior authorization, unless legally compelled to do so. If VMware is required to respond to such a request, VMware will promptly notify the customer and provide a copy of the request, unless legally prohibited from doing so.

VMware will reasonably cooperate with customers to respond to any requests from individuals or applicable data protection authorities relating to the processing of personal data to the extent that customer is unable to access the relevant personal data in their use of the service. Please refer to the *VMware Data Processing Addendum* for definitions and standard hosting terms.

Audit Reports and Trust Assurance

SOC 2 Type 2 Audit Reports

Horizon Cloud Services cloud-delivered environments have undergone SOC 2 Type 2 and SOC 3 audits; SOC 2 reports are available under an NDA with VMware.

Cloud Security Alliance (CSA) Cloud Alliance Initiative Questionnaire (CAIQ)

VMware has completed and published a response to the CAIQ to provide transparency into technologies and processes that vendors implement to manage risks for cloud-delivered environments.

Standard Hosting Agreements and Service Resources

Service Description

Please refer to the *Horizon Service Description* for an overview of the hosted service, including roles and responsibilities shared between VMware and the customer.

Service Level Agreement

Horizon Cloud Service will maintain a monthly availability measurement of 99.9% as defined in the *Horizon Service SLA*.

Terms of Service

VMware Cloud Terms of Service governs VMware cloud delivered services together with the *VMware Data Processing Addendum*

VMware U.S. Export/Re-Export Laws and Regulations

VMware, Inc. is committed to complying with all applicable U.S. export/re-export laws and regulations. We observe applicable restrictions on the export and re-export of our products, services, or technical data.

If you are exporting or re-exporting VMware products, services, or technical data, U.S. export control applies to you, and you are required to ascertain your compliance obligations. Please contact the VMware Trade Compliance Legal Team with any questions regarding export compliance for our products, services, or technical data at *export@vmware.com*.

Additional information on VMware's Export Control Policies can be found on vmware.com:

- *VMware Product Export Control Classification List*
- *VMware Bundle Product Export Control Classification List*

Export Restrictions

The U.S. Department of Commerce and the U.S. Department of Treasury administer and maintain exclusion lists. VMware does not ship products to any entity or individual, whether in the U.S. or abroad, specified on these lists.

- *U.S. Department of Commerce Denied Persons List*
- *U.S. Department of Commerce Denied Entity List*
- *U.S. Department of Commerce Unverified List*
- *U.S. Department of Treasury Specially Designated Nationals List*
- *U.S. Department of State Debarred List*
- *U.S. Department of State Nonproliferation Sanctions*

VMware, Inc. 3401 Hillview Avenue Palo Alto CA 94304 USA Tel 877-486-9273 Fax 650-427-5001 www.vmware.com.