VMware vSphere+

Privacy Datasheet

SECURITY, CERTIFICATIONS AND THIRD-PARTY ATTESTATIONS

All compliance certifications are available in the VMware Trust Center's Compliance Page.

ABOUT VSPHERE+

VMware vSphere+ is a multi-cloud workload platform that brings the benefits of VMware Cloud Services to your on-premises

workloads. vSphere+ combines the industry-leading virtualization technology, an enterprise-ready Kubernetes environment, and high-value cloud services to transform your existing on-premises deployments into a SaaS-enabled infrastructure. Find more details at *https://www.vmware.com/products/vsphere/vsphere-plus.html*

ABOUT VMWARE'S PRIVACY PROGRAM

- Trust Center – At VMware, we want to bring transparency that underlies trust. *The VMware Trust Center* is the primary vehicle to bring you that information.
- Data Privacy Officer - Please contact the VMware Privacy Team via the *Privacy Contact Form* or by mail at Office of the General Counsel of VMware, Inc., 3401 Hillview Ave, Palo Alto, California, 94304, USA.

How vSphere+ brings value to you!

VMware vSphere+™ ("Service Offering") is a multi-cloud workload platform that brings the benefit of VMware Cloud Services to your on-premises workloads by providing access to a wide selection of cloud services and centralizes management through the VMware Cloud Console. Workloads remain on-premises, running on ESXi hosts orchestrated by vCenter instances, just like traditional vSphere today. But now vCenter can connect to the Cloud Console through a VMware cloud gateway, allowing metadata to be collected and used to centrally manage the entire distributed vSphere+ estate. Admin services can then be used to simplify global operations, developer services can be used to manage the Kubernetes environment, and optional add-on hybrid cloud services can be purchased to extend the capabilities of vSphere+ even further.

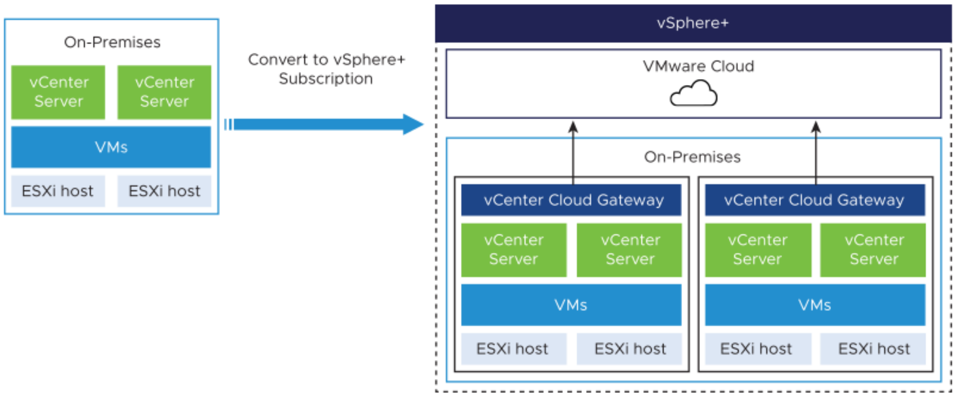


FIGURE 1: vSphere+ Architecture and Ecosystem

For more information, see the description of vSphere+ in the Cloud Services Guide available here.

VMware and Privacy

In a complex world of data and the digital era our goal is simple: At VMware, you, our customers, and your data are our primary concern. VMware takes privacy and data protection very seriously and is committed to providing clear information about how we collect, use, and process your personal data. We have established policies and practices designed to protect the personal data we process on behalf of our customers (as a processor), and as a controller. We are also committed to privacy-by-design when developing products and services. The VMware Privacy Team actively works with the development teams to identify and embed privacy controls for customers.

DATA PRIVACY REQUESTS

If you wish to exercise any of your rights under applicable data privacy laws for personal data processed by your organization while using the Cloud Service, please contact your organization. See the *VMware Privacy Notice* for information about how to exercise your rights where VMware is processing personal data in connection with its business operations.

FOR MORE INFORMATION OR TO PURCHASE VMWARE PRODUCTS

Contact your VMware account representative or call 877-4-VMWARE (outside North America, +1-650-427-5000), visit *vmware.com/products*, or search online for an authorized reseller.

UPDATES

Reading from a PDF? Don't be outdated, be informed! Find the latest information in the current version of this document from the *VMware Trust Center Privacy Page*.

The personal data collected and processed by VMware are largely dependent on the type of offering you purchase. This Privacy Datasheet provides you with information about how VMware processes and protects your personal data in connection with vSphere+.

Types of Data Collected by vSphere+

VMware only collects and further processes the following categories and types of personal data in connection with the provision of the Service Offering to the Customer

VMware Data Classification	Description and Purpose of processing	Categories of Personal Data
Identity Details	First Name, Last Name, and Email address of customer's IT administrator(s)	Service functionality such as role-based access controls, alerting and user identification.
Online Identifiers	IP addresses of customer's IT administrator(s)	Service functionality such as role-based access controls, alerting and user identification.

Personal data other than those listed above may also be included in any content that the customer submits to the Service Offering (i.e., "Customer Content"). VMware may not know what types of personal data are submitted to the Service Offering by the customer and the customer is responsible for understanding the types of personal data processed in connection with the customer's use of the Service Offering.

Service Usage Data	Information used by VMware for analytics, product improvement purposes, and proactive support. See *VMware Trust & Assurance Center* for additional details regarding VMware's Service Usage Data Program (SUDP). For example: • Configuration, usage, and performance data • Survey and feedback data	Contact Information, such as administrators' email address (e.g., to provide proactive support). Online Identifiers such as administrators' or users' IP address.

How We Protect Data Processed in Connection with the Operation of Our Business (as a Controller)

In connection with VMware's provision of the Service Offering to the Customer, VMware collects and further processes the types of data shown in the table below, which may include personal data. In this instance, VMware is acting as a "controller" in relation to such personal data and determines the purposes of the processing.

Data Category	Purposes for which it is used
Relationship Data – Authentication and customer account data	Used to provision the Service Offering, such as managing the account and maintaining relationship data.
Service Operations Data – Configuration Data, Feature Usage Data, Authentication Data, Performance Data, Service Logs, Memory Dumps, Security Logs, Diagnostic Data, Support and Survey Data.	Information used to facilitate the delivery of the Service Offering, including managing, and monitoring the infrastructure, and providing support. See VMware Products and Services Privacy Notice for details.
Service Usage Data – Configuration Data, Feature Usage Data, Performance Data.	Information used for VMware's own analytics and product improvement purposes See VMware Service Usage Data Program disclosure for details.

The following privacy notices explain the different ways in which VMware collects, uses, and protects any personal data included in the above categories of data:

VMware Privacy Notice: This notice addresses the personal data we collect when you purchase VMware products and services and provide account-related personal data.

VMware Products and Services Privacy Notice: This notice applies only to the limited personal data we collect and use for our own purposes in connection with our provision of VMware products and services, including (i) any cookies and similar tracking technologies we may use when providing the products or services; (ii) any information we use to facilitate the delivery of VMware services; and (iii) any data we collect to improve our products and services and our customer's experience.

How We Protect Data as a Service Provider (Processor)

In connection with the provisioning of the Service Offering, VMware will process personal data contained in Customer Content (as such term is defined in the relevant VMware agreement, e.g. VMware Terms of Service) on behalf of the Customer. In this instance, VMware is acting as a "processor" (acts on the instruction of the controller), while the Customer has the role of the "controller" (determines the purposes of the processing).

Data Protection Addendum

VMware's obligations and commitments as a data processor are set forth in VMware's Data Processing Addendum ("DPA"). VMware will process personal data contained within Customer Content in accordance with the applicable agreement and the DPA. The applicable agreements for each product and service, including the VMware Terms of Service, the Service Descriptions for each specific service, and other relevant legal documents can be found here.

Data Storage and Cross-Border Data Transfers

VMware vSphere+ stores Customer Content in certain Amazon Web Services, Inc. (AWS) availability regions depending on their geolocation and current vSphere+ service coverage. Customer Content will not be relocated, replicated, archived, or copied outside of the country of the AWS availability region selected by Customer without the explicit request or actions of Customer.

For cross-border personal data transfers, VMware has achieved Binding Corporate Rules ("BCR") as a processor, thus acknowledging we have met the standards of the EU General Data Protection Regulation for international transfers of personal data it processes on behalf of our customers. View the VMware BCR or the EU Commission BCR Listing in the VMware Trust Center

Sharing with Sub-Processors

For the Service Offering, VMware utilizes third-party companies to provide certain services on its behalf. As set forth in the Data Processing Addendum, VMware has agreements and data transfer mechanisms in place with each sub-processor. A list of these sub-processors is available at the VMware End User Terms and Conditions *One Contract Center* page.

Additional sub-processors providing supporting functionality for the Service Offering are available in the Support Services Sub-Processer List.

VMware also provides customers with an easy mechanism to monitor changes to our list of sub-processors. If you would like to receive notifications, please visit this page here.

Data Retention and Deletion Practices

Retention and storage policies associated with Customer Content (including any personal data stored within Customer Content) are solely managed by the Customer. VMware does not back up Customer Content and therefore will not be able to recover any Customer Content (including personal data therein) in any unforeseen event or following termination or expiration of the Service Offering instance. The VMware Data Processing Addendum, the General Terms, and the relevant Cloud Service Guide set forth how personal data contained in Customer Content is deleted after expiration or termination.

VMware retains personal data that we may collect in connection with the Customer's use of the Service Offering (which does not include Customer Content not personal data contained in Customer Content) for as long as it is needed to fulfill the obligations of the VMware General Terms. The personal data collected as part of system audit logs, also referred to as Software-Defined Data Center (SDDC) audit logs, are retained for three (3) years and log events that exceed the three (3) year life cycle are automatically purged.

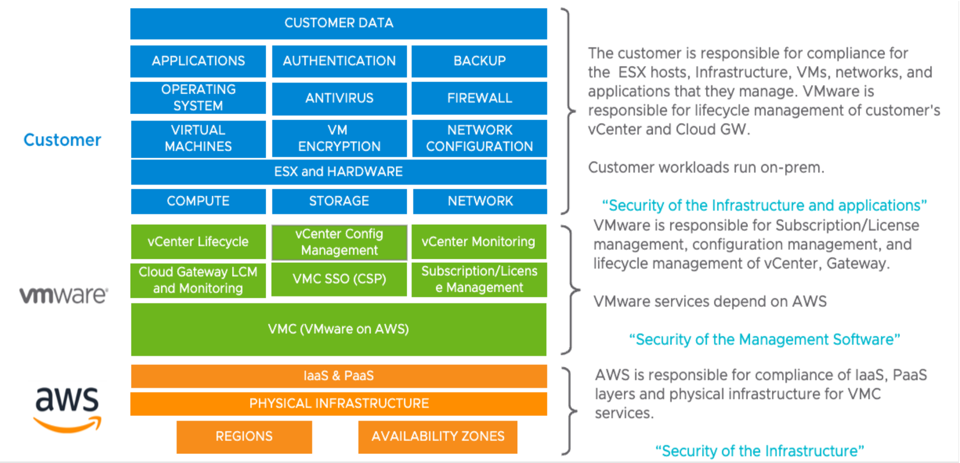
Security

VMware maintains technical and organizational measures to protect against data breaches and to preserve the security and confidentiality of data processed by VMware on behalf of the Customer in the provision of the Service Offering. Controls are provided to enable the customer to configure the service in a manner compliant with its own security policies and practices.

vSphere+ undergoes independent third-party audits on a regular basis to provide assurance to our Customers that VMware has implemented industry leading practices and controls. vSphere+ has been audited for key industry certifications including ISO 27001, ISO 27017, ISO 27018 and SOC2. You can view existing compliance and certifications for vSphere+ at https://www.vmware.com/products/trust-center.html#compliance.

Shared Responsibility Model

VMware vSphere+ provides a shared accountability model where security and compliance responsibilities are shared between VMware, the Customer and Amazon Web Services (AWS).



The customer is responsible for compliance for the ESX hosts, Infrastructure, VMs, networks, and applications that they manage. VMware is responsible for lifecycle management of customer's vCenter and Cloud GW.

Customer workloads run on-prem.

"Security of the Infrastructure and applications"

VMware is responsible for Subscription/License management, configuration management, and lifecycle management of vCenter, Gateway.

VMware services depend on AWS

"Security of the Management Software"

AWS is responsible for compliance for IaaS, PaaS layers and physical infrastructure for VMC services.

"Security of the Infrastructure"

FIGURE 2: Shared Responsibility Model

Access Control

Access to Customer Content is governed by Customer's use of authentication and authorization mechanisms to Virtual Machines (VMs) and filesystems that hold the VMs' data. Neither VMware nor Amazon Web Services (AWS) require any user accounts that would provide access to any Customer Content. The separation of Customer Content from VMC Operations is shown below:

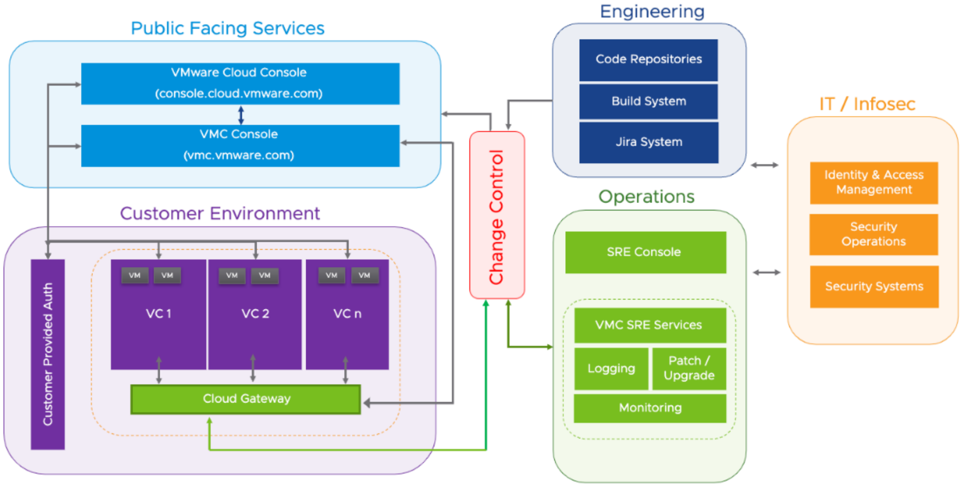


FIGURE 3: Separation of Customer Content

VMware will not access or use Customer Content except as necessary to maintain or provide support for the Service Offerings as provided in the Agreement.