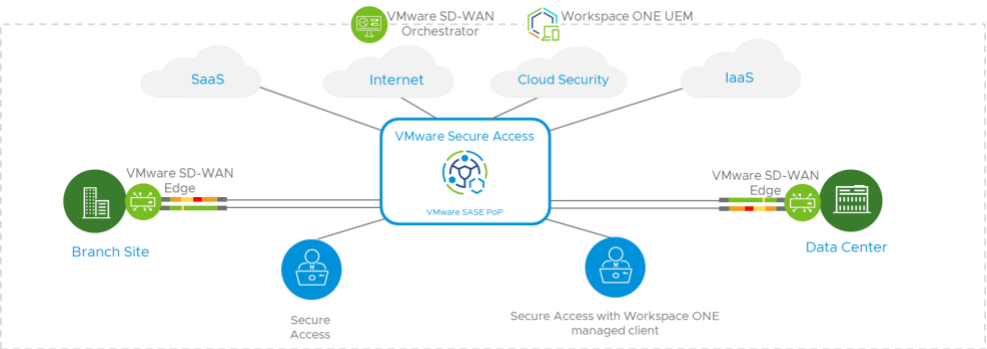
VMware Secure Access Privacy Datasheet

How VMware Secure Access brings value to you

VMware Secure Access is a hosted offering that helps provide remote and mobile users consistent, optimal, and secure cloud application access through a worldwide network of managed service nodes. VMware Secure Access is based on the Zero Trust Network Access (ZTNA) architecture. VMware Secure Access grants application access based on the user identity and end-device posture. VMware Secure Access consists of three main components:

- The Workspace ONE UEM Console, offered as a hosted service, manages enrollment of devices and ZTNA policies.
- The VMware Cloud Orchestrator is used for configuring the networking settings on VMware Secure Access.
- VMware Workspace ONE® Tunnel™ client and VMware Workspace ONE® Intelligent Hub are the client applications installed on the end user devices. Workspace ONE Tunnel client builds secure tunnels from the end device to the nearest VMware point of presence ("PoP"). Workspace ONE Intelligent Hub manages user onboarding and policy enforcement on the end device.



For more information, see the *Service Description*.

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

ABOUT VMWARE SECURE ACCESS

VMware Secure Access, delivered from the VMware secure access service edge (SASE) platform, is a cloud-hosted service that helps customers better protect users and infrastructure accessing SaaS and Internet applications.

Learn more at: *sase.vmware.com*

ABOUT VMWARE'S PRIVACY PROGRAM

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

SECURITY, CERTIFICATIONS AND THIRD-PARTY ATTESTATIONS

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

privacy-by-design when designing our products and services and VMware's Privacy Team works with the development teams to identify and embed privacy controls for customers.

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 your personal data in connection with the VMware Secure Access Service Offering.

Types of Data Processed by VMware Secure Access

VMware Secure Access helps enterprise customers to protect the confidentiality, security and integrity of their information and systems accessed and made available to its end-users through corporate owned or personal devices by providing the customer a platform to deliver and manage such apps and devices. Details regarding the types of data collected in connection with the customer's and its end-users use of VMware Secure Access's Workspace ONE UEM console and mobile applications can be found in the *Workspace ONE Privacy Disclosure*. The *Workspace ONE Privacy Disclosure* is intended to assist our customers in better understanding the types of data that may be processed in connection with their use of VMware offerings that leverage Workspace ONE components, and to assist the customer in complying with their own notice obligations to end-users, if any. Within the end-user app for Workspace ONE UEM, VMware provides the end user with a privacy dashboard so they can understand the types of data processed by their organization.

In addition to the data processing associated with the Workspace ONE UEM console and mobile applications referenced above, VMware also processes the following categories of data in connection with the provision of the VMware Secure Access Service Offering:

VMware Data Classification	Description and Purpose of processing	Categories of Personal Data
Customer Content	Content submitted by customer to the Service Offering for processing, storage, or hosting (described as "Your Content" in *VMware's Terms of Service*). To the extent the Service Offering processes Customer Content, VMware processes such Content to provide the Service.	Customer controls and needs to determine which type of personal data it submits to Service Offerings. The specific personal information collected and processed will depend on the customer's specific configurations and deployment. Typically, Customer Content processed by VMware Secure Access is limited to - IP addresses of end users - Destination IP addresses - Destination URL

Support Request Content	Data provided by customer to VMware to address a technical support issue.	Any personal data customer shares with VMware in connection with a support request (as controlled and determined by Customer).
Account Data	Data collected and used by VMware to manage the customer account and maintain the relationship with customer, such as to bill the customer or deliver notifications and alerts.	Contact Information, such as customer name, email address, address and phone number. Online Identifiers such as customer's IP address or login credentials.
Service Operations Data	Data used by VMware to facilitate the delivery of the Service. This may include (i) tracking entitlements, (ii) providing support, (iii) monitoring the performance, integrity, and stability of the Service's infrastructure, and (iv) preventing or addressing Service or technical issues. For example: • Configuration, usage and performance data • Authentication Data • Service logs, security logs, and diagnostic data Survey and feedback data	Contact Information, such as administrators' email address. Online Identifiers such as administrators' and developers' IP address, login credentials or login time stamps.
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).	Contact Information, such as administrators' email address (e.g. to provide proactive support). Online Identifiers such as administrators' IP address.

* Content submitted by Customer to the Service Offering (described as "Your Content" in *VMware's Terms of Service*). Customer is responsible for determining which types of personal data (if any) it includes in data submitted to the Service Offering.

How We Process and Protect Data as a Controller

To the extent VMware acts as the Controller, the following privacy notices explain how VMware collects, uses and protects any personal data included in the above categories of data:
VMware Privacy Notice: This notice addresses the personal information we collect when you purchase VMware products and services and provide account-related personal information.

VMware Products and Services Privacy Notice: This notice applies only to the limited personal information 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 Process and Protect Data as a Processor

In connection with the provisioning of the Service Offering, VMware will process any personal data contained in Your Content (as such term is used in the *VMware Terms of Service*) on behalf of the customer. With respect to personal data included in Your Content, 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 Your Content in accordance with the applicable agreement and the DPA. The applicable agreements for VMware Secure Access, including the VMware Terms of Service, the Service Description, and other relevant legal document can be found *here*.

Data Storage and Cross-Border Data Transfers

VMware Secure Access enables customers to choose five primary PoP locations that align to their needs. Disaster recovery locations are contingent on the primary PoP locations. Please visit the *VMware SD-WAN/Secure Access/Cloud Web Security Sub-processors list* for PoP location details and the *Workspace ONE UEM Sub-processors list* for UEM Console location details.

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 Cloud Trust Center*.

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 Service Offering, please contact your organization. See *VMware's 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 Cloud Trust Center's Privacy Page*.

Sharing with Sub-Processors

For our Service Offerings, VMware may utilize 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. Lists of sub-processors are available *here*.

Additional sub-processors providing support services functionality for the Service Offering is 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

VMware retains personal data that we may collect in connection with the customer's use of a Service Offering for as long as it is needed to fulfill the obligations of the VMware Terms of Service.

Details regarding deletion of Customer Content processed by the Workspace ONE UEM console can be found in the *Workspace ONE Privacy Disclosure*. Other Customer Content is processed in real time upon establishment of the user session and is not retained after session termination.

Last Updated: March 2022

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