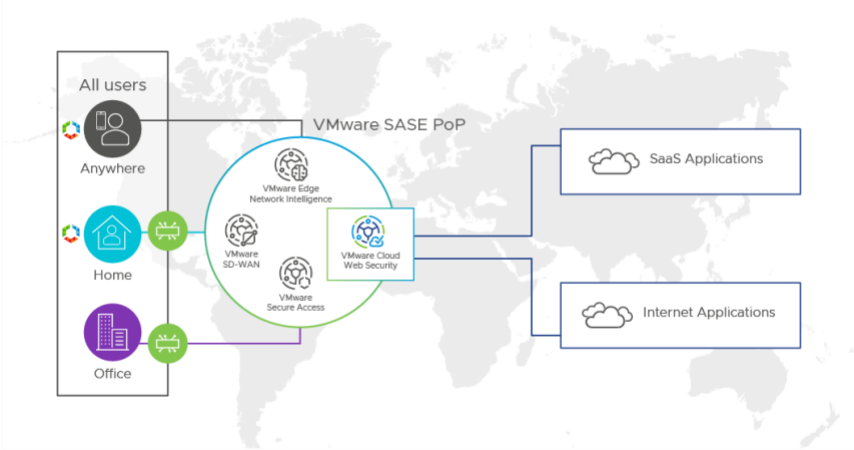
VMware Cloud Web Security – Privacy Datasheet

How VMware Cloud Web Security brings value to you

VMware Cloud Web Security is a Secure Web Gateway service available to users of VMware SD-WAN or VMware Secure Access. Administrators may subject workloads to a variety of security checks at the time the workloads pass through VMware Points of Presence (PoPs) that contain the VMware SD-WAN gateways. The security checks include URL Filtering, Anti-Virus/Anti-Malware (including file hash and full file inspection), and Sandbox. Administrators may define which workloads pass through which security checks based on criteria including network-based filters such as subnet and IP address, and non-network-based filters such as users, context, file type, application, and domain.



For more information, see the *VMware SD-WAN 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 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 Cloud Web Security Service Offering.

ABOUT VMWARE CWS

VMware Cloud Web Security, delivered from the VMware secure access service edge (SASE) platform, is a cloud-hosted service that better protects 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.*

Types of Personal Data Processed by VMware Cloud Web Security

VMware processes the following categories and attributes of personal data in connection with the provision of the Service Offering to the customer. In subsequent sections, we separately address personal data we process as a controller and personal data we process as a processor, including the respective terms that govern our treatment of that personal data.

Personal Data Category	Personal Data Attributes	Purpose of Processing
Contact Information	Administrators' Name Administrators' Email address	Access and authentication. Service functionality such as role-based access controls, alerting, user identification and auditing.
Online Identifiers	Administrators' IP address	Access and authentication. Service functionality such as role-based access controls, alerting and user identification.
	User and device activity/security posture data including username, user ID, user group, email address, device ID, source IP, Browser type and version. Security analytics data including web traffic URL, Web category, User Agent	Security analysis such as Anti-virus, Anti-malware and Sandboxing. Captured in the logs generated by the Service Offering.
Various	Any personal data within Your Content (content that you choose to submit to CWS for security analysis), *such as* • File/document contents (for file types selected by the customer)	Security analysis such as Anti-virus, Anti-malware and Sandboxing.

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

As part of customers' choices in defining which workloads pass through which VMware Cloud Web Security assessments, customers may select file type(s) from among the following file types.

File Category	File Types
Archives and Packages	GZIP, TAR, ZIP, 7ZIP, LZH, ARJ, BZIP, RAR, CAB
Calendar	ICS
Engineering Applications	Visio, AutoCAD
Multimedia	Audio Files, Video Files
Presentation Tools	PowerPoint, OpenOffice Presentation
Productivity	MS Project, MS One Note
Scripts and Executables	Windows Executable, Linux Executable, Mac Executable, Text Based script files, JAR, Android Executable
Spreadsheets	OpenOffice Spreadsheet, Excel, CSV
Word Processors	Ichitaro, Word, PDF, Hangul, XPS, OpenOffice Text, Word Perfect

Data Processed by VMware 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 processes the categories of data shown in the below table. To the extent such data is personal data, VMware is acting as a "controller" and determines the purposes of the processing.

Data Category	Purposes for which it is used
Relationship Data • Customer account information (including contact information)	Information used in connection with the provision the Service Offering, such as managing the account and maintaining the relationship with the customer.
Service Operations Data • Configuration, usage and performance data • Authentication Data • Service logs, security logs, and diagnostic data • Survey and feedback data	Information used to facilitate the delivery of the Service Offering, including maintaining, managing, monitoring and securing the infrastructure.
Service Usage Data • Configuration, usage and performance data including limited flow statistics (Edge ID, throughput, application) and limited link statistics (ISP name, bandwidth, speed)	Information used by VMware for analytics and product improvement purposes. See *VMware Trust & Assurance Center* for additional details regarding VMware's customer experience improvement programs.

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.

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*.

Data Processed by VMware as a Service Provider (as a Processor)

In connection with the provisioning of the Service Offering, VMware will process 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 Cloud Web Security, including the VMware Terms of Service, the VMware SD-WAN Service Description, and other relevant legal document can be found *here*.

Data Storage and Cross-Border Data Transfers

Other than the Sandbox feature, VMware Cloud Web Security currently processes Your Content in the same PoP through which the workload is processed. The Sandbox feature is performed in regional data centers in the United States, Germany, United Kingdom and Japan (the Sandbox detonation will occur in the data center closest to the PoP through which is the workload is passing). The logs generated by the Service Offering are stored centrally in the United States. Processing location options may be added so please visit the *Sub-Processors list* for up-to-date primary and disaster recovery 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*.

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 sub-processors for VMware SD-WAN and VMware Cloud Web Security is available *here*.

Additional sub-processors providing supporting 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 the Service Offering for as long as it is needed to fulfill the obligations of the VMware Terms of Service.

The *VMware Data Processing Addendum*, the *Terms of Service,* and the relevant Service Description set forth how personal data contained in Your Content is deleted after contract expiration or termination.

During the subscription term, Your Content transmitted to VMware Cloud Web Security by you is processed in memory in the PoP (other than the Sandbox feature which is performed in a separate datacenter) and is not retained after processing, other than data retained in logs. Logs are deleted from the Service Offering within approximately 30 days of creation, or from support systems within approximately 30 days of ticket closure, as applicable.

If a file is deemed malicious during the Sandbox inspection, a copy of the file hash will be retained for threat intelligence purposes. If there is a malicious code embedded within a file (for example, a malicious code is embedded into PDF or Word file type), only the hash of the malicious code will be retained for threat intelligence purposes and not the PDF or Word file itself. The customer may elect to receive screenshots of the files being executed via the Sandboxing feature. Such screenshots will be sent to the customer via email and are not retained by VMware.

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