VMware SD-WAN™
VMware Secure Access™
VMware Cloud Web Security™

Service Description

Last Updated: 12 October 2021
1. Introduction

1.1 Overview

VMware SD-WAN™ ("VMware SD-WAN" or the "Service Offering") is a SaaS-based software-defined wide area network (SD-WAN) platform that provides networking services to enterprise branch locations, and to customers’ remote location workers through the “work from home” offer described in Section 4, below. The Service Offering’s speed, scale, reliability, and flexibility help enterprise network administrators to rapidly deploy new enterprise branch locations and allow for simultaneous use of all connected transport links. The Service Offering also provides instant visibility into the performance and reliability of the customer’s WAN, connecting the global enterprise locations, and its impact on application performance. Applications can be deployed as part of a distributed services on public, private, and hybrid cloud infrastructures as well as in existing enterprise data centers.

VMware also offers VMware Secure Access™, a zero trust access service, described in Section 5, below, that leverages both VMware SD-WAN and VMware Workspace ONE® functionality, and VMware Cloud Web Security™, a secure web gateway service, described in Section 6, below.

The Service Offering includes access to the following components:

- VMware SD-WAN edge software (the “Software”) which is installed on customer-premise equipment (the “Equipment”) at the customer location (that is, in the customer’s own on-premises environment). The Equipment can be supplied by VMware, or by the customer (provided that the equipment supplied by the customer is x86 compatible). The Software and the Equipment are referred to as the VMware SD-WAN Edge. This functionality performs deep application recognition, application and sub-second steering, performance metrics, and maintains end-to-end quality of service in addition to hosting virtual network function (VNF) services.

- Access to the VMware SD-WAN orchestrator, a solution that provides centralized enterprise-wide installation, configuration and real-time monitoring in addition to orchestrating the data flow through the cloud network. The orchestrator enables one-click provisioning of virtual services in the customer’s location, in the public cloud, or in the customer’s enterprise data center. This centralized management portal provides insight into global network operation, as well as serving as a central policy engine that supplies the VMware SD-WAN Edge with both network intelligence as well as administrative policies on how applications behave in the enterprise SD-WAN network. The VMware SD-WAN orchestrator is hosted and managed by VMware.

- Access to a global, distributed set of VMware SD-WAN gateways. These gateways serve as a distributed forwarding plane, and are responsible for delivering network traffic to its final destination. In the process of transport, reliability and performance enhancements are applied to the carried traffic that improve the end-user application experience at the enterprise locations. The VMware SD-WAN gateways are hosted and managed by VMware.

Existing customers can now purchase additional subscriptions to VMware SD-WAN to provide networking services to the customer’s employees working from home. The Service Offering’s speed, scale, reliability, and flexibility help enterprise network administrators support employees working from home and improves the application experience across one or more WAN links.

v. 12 October 2021
VMware SD-WAN also provides instant visibility into the performance and reliability of the WAN link(s) to the employee’s home, connecting the employee with the customer’s enterprise locations. The applications that the employee working from home is accessing can be deployed as part of a distributed services environment on public, private, and hybrid cloud infrastructures as well as in existing enterprise data centers. See Section 4, below, for details of this offer.

1.2 Technical Documentation and Training

Documentation outlining key concepts and instructions on the configuration of the various features is embedded in the VMware SD-WAN orchestrator. The URL for the VMware SD-WAN orchestrator instance will be provided as part of the service provisioning.

1.3 Legal Terms

Your use of the Service Offering is subject to the Terms of Service found through the links at https://www.vmware.com/download/eula.html. Use of the Equipment is subject to the Equipment Terms found through a link at https://www.vmware.com/download/eula.html.

2. Service Operations

The following outlines VMware’s roles and responsibilities in providing the Service Offering. While specific roles and responsibilities have also been identified as being owned by you, any roles or responsibilities not contained in this Service Description are either not the duty of VMware or are assumed to be your responsibility.

2.1 Service Provisioning

VMware will provide the following provisioning services:

- VMware will create a service account and send an email or other notification to the contact that you identified in your Order inviting that contact to the newly created enterprise account. A URL to access the Service Offering will be provided within this notification.
- VMware will ensure that the identified contact can create additional user accounts for other users, as needed.
- VMware will provide access to the VMware SD-WAN orchestrator
- VMware will ensure that distributed VMware SD-WAN gateways are made available for use.
- VMware will provide SD-WAN software and/or hardware in accordance with the order

Your responsibilities include:

- Ordering last mile transport links and connecting these to the VMware SD-WAN Edges.
- Provisioning and deploying the VMware SD-WAN Edges in accordance with the ordered quantities.
- Configuring the Service Offering with business appropriate policies that control how the associated traffic behaves in the enterprise SD-WAN.
- Maintaining the security posture through configurable firewall rules on the VMware SD-WAN orchestrator or via a third-party security solution.
• Monitoring your usage and traffic patterns to ensure these are in line with the network capacity connected to the VMware SD-WAN Edges. VMware does not guarantee performance characteristics of the solution as this is conditional on the available bandwidth and quality of the bandwidth.
• Procuring and installing appropriate Equipment to run the Software if you do not obtain the Equipment from VMware.

2.2 Support
We will provide support for problems that you report to assist with adoption of and related to the Service Offering. Support may be provided in any country in which we or our agents maintain facilities.

Support may include updates to the Service Offering that address security fixes, critical patches, general maintenance functionality, and documentation. VMware is under no obligation to develop any future functionality or enhancements, but VMware may update the Service Offering as provided in the Terms of Service. Where practical, VMware will schedule Service Offering updates during non-business hours and will provide you with advance notice. Updates addressing critical and high security vulnerabilities may be implemented with no advance notice.

For additional information, see the knowledge base article at: https://kb.vmware.com/s/article/53907

2.3 Monitoring
VMware will provide the following services with respect to monitoring:

• VMware SD-WAN will provide you with the ability, through the Service Offering, to view and monitor the link quality metrics such as bandwidth, packet loss, latency and jitter as well as link and application utilization statistics at which you are transmitting data from each of the enterprise branch locations to the destination of the traffic.
• We will provide you with detailed event logs, recording events in relation to changes in link and IPsec tunnel state.
• We will provide you with a global overview of the status of each of the enterprise branch locations and their attached links.

You are responsible for the following services with respect to monitoring:

• You are responsible for monitoring the availability of the transport links attached to the VMware SD-WAN Edges (e.g., broadband internet service), which are not supplied by VMware.
• You are responsible for monitoring overage use of connected wireless broadband links as well as other links that may be charged on a volume basis. You are responsible for analyzing firewall logs that the Service Offering may collect and taking appropriate action if a security incident is detected.
### 2.4 Incident and Problem Management

VMware will provide incident and problem management services (e.g., detection, severity classification, recording, escalation, and return to service) pertaining to:

- Infrastructure over which VMware has direct, administrative access and control, including servers and services used to provide the Service Offering.

You are responsible for incident and problem management (e.g., detection, severity classification, recording, escalation, and return to service) pertaining to:

- Your account settings in the Service Offering’s orchestrator console.
- User-deployed and user-configured assets such as laptops, servers, etc.
- Anything else not under VMware’s direct control and administration.
- Availability of connected WAN links to the VMware SD-WAN Edges.

### 2.5 Change Management

VMware will provide the following change management elements:

- Processes and procedures to release new code versions, bug fixes related to the Service Offering.

You are responsible for:

- Management of changes to your alert notifications and other content.
- Administration of self-service features provided through the Service Offering’s orchestrator portal, up to the highest permission levels granted to you.
- Cooperating with VMware when planned or emergency maintenance is required.

### 2.6 Service Operations Data

In connection with providing the Service Offering, VMware collects and processes information from VMware’s software or the systems hosting the Service Offering, and from your systems, applications and devices that are used to access and use the Service Offering. That information is processed to facilitate delivery of the Service Offering, including but not limited to (i) tracking entitlements, (ii) providing support, (iii) monitoring and ensuring the performance, integrity, and stability of the Service Offering’s infrastructure, and (iv) preventing or addressing service or technical issues. To the extent that any of this data is considered personal data under applicable data protection laws, the data will be treated in accordance with VMware’s Privacy Notice, including the VMware Products and Services Notice, available at: [https://www.vmware.com/help/privacy.html](https://www.vmware.com/help/privacy.html)

### 2.7 Usage Data

The Service Offering collects data (such as configuration, performance, and usage data, including limited flow statistics [Edge ID, throughput, application], and limited link statistics [ISP name, bandwidth, speed]) directly from the machines and/or devices involved in the use of the Service Offering, to improve VMware products and services, and your and your users’ experiences, as more specifically described in VMware’s Trust & Assurance Center at [https://www.vmware.com/solutions/trustvmware/usage-data-programs.html](https://www.vmware.com/solutions/trustvmware/usage-data-programs.html). To the extent that any of this data is considered personal data under applicable data protection laws, the data will be treated in accordance with VMware’s Privacy Notice, including the VMware Products and...
In connection with the collection of usage data, VMware and its service providers may use cookies. Detailed descriptions of the types of cookies we use can be found in VMware Privacy Notices available at https://www.vmware.com/help/privacy.html. More information on how to choose whether to accept certain cookies used by VMware websites and solutions can also be found from that link.

2.8 Content

As the Service Offering is used, the VMware SD-WAN Edges and gateways send data to the orchestrator including flow statistics (Edge ID, hostname, source and destination IP address, source MAC address, throughput, destination domain name, protocol, application and application category) and link statistics (ISP name, Public IP address, bandwidth, speed, latency, packet loss and jitter). During the Subscription Term, data transmitted to the Service Offering will be retained in the orchestrator and available for querying and alerts for at least two weeks (by default) from the date and time the data was originally ingested into the Service Offering. The amount of data stored depends on the storage space available on the VMware SD-WAN orchestrator and the amount of data generated by each site’s VMware SD-WAN Edge.

3. Business Operations

3.1 Ordering

The Service Offering is available from authorized VMware channel partners. The Service Offering can be purchased for committed Subscription Terms of one, three, or five years.

Contact your VMware sales specialist to understand which combination of Service Offering dimensions (bandwidth tiers (Mbps), feature editions, and component bundles) meet your business needs.

In connection with your order for the Service Offering, you will need to provide site count, site location(s), feature(s), throughput(s), and your network administrator’s email. The information you provide is required to configure the VMware SD-WAN orchestrator to provision the Service Offering for you.

Your Subscription Term will begin on the date your instance of the Service Offering has been provisioned. If you do not provide the needed information, VMware cannot provision the Service Offering for you. Your Subscription Term may begin prior to installation of the Equipment in your location. VMware may permit you to continue to use the Service Offering for an additional period, not to exceed 30 days, after expiration of your committed Subscription Term, at no additional cost, if your Subscription Term began prior to installation of the Equipment. All terms, other than payment of fees, will continue to apply during any extended use term.

Additional services/products, or upgrades, may be purchased at the time of your initial Order or through the VMware customer portal at any time during the Subscription Term. Additional terms and fees will apply to such additional services. If services/products are added during the term of an existing contract, the contract termination date for the add-on services/products defaults to the same date as that of the existing contract. For the add-on orders, you may be required to configure the VMware SD-WAN orchestrator to activate the additional services and products.

Service Offering capacity reductions must be coordinated with VMware at the time of subscription renewal, and will require a manual renewal order for the reduced Service Offering capacity.
Orders for reduced capacity must be submitted to VMware at least five (5) calendar days prior to the date of subscription renewal.

3.2 Renewal

VMware reserves the right to not renew an SID at the end of its subscription term. In the event of a non-renewal by VMware, we will notify you 30 days prior to the end of the subscription term.

If you do not renew your subscription at least 30 days prior to the last day of the then-current Subscription Term, then your existing SID may be flagged for termination after your grace period ends.

3.3 Suspension and Re-Enablement

While a SID is suspended by VMware for delinquent payment or any other reason as set forth in the Terms of Service, VMware will disable your VMware SD-WAN orchestrator account. VMware will retain SIDs with configurations and data intact until the issue is resolved or the subscription expires or is terminated.

SID re-enablement will be initiated within three (3) business days upon resolution of the issues that led to suspension; access to the VMware SD-WAN orchestrator will be restored.

Suspension (when access to VMware SD-WAN orchestrator is disabled) does not suspend your financial obligations, nor does it extend the end date of the Subscription Term.

3.4 Termination

Termination of a SID due to termination of the Agreement will result in permanent loss of access to the Service Offering, and a deletion of all Equipment configuration and data. Data from a terminated SID will be deleted within 90 days of the termination date of the SID. Data will continue to survive in backups for up to one year following termination of your account, and will be deleted as part of periodic deletion activities. During this period, data will not be generally accessible, as the data is intended to be used for disaster recovery purposes (if needed). VMware may retain any anonymized or hashed data. The Service Offering is not eligible for early termination. Any deleted data is non-recoverable.

4. VMware SD-WAN Work from Home Offer

Enterprise customers that have employees working from home can purchase Service Offering subscriptions to support their remote workforce, through the VMware SD-WAN™ WFH Subscription (“WFH Subscription”) and the VMware SD-WAN™ WFH Pro Subscription (“WFH Pro Subscription”) offer.

Subscriptions purchased through this offer can only be used at employees’ home locations. For the WFH Subscription there is a limit of one business user with two concurrent devices and up to 350 Mbps or the max throughput of the Edge (whichever is lower). For the WFH Pro Subscription there is a limit of one business user with three concurrent devices and up to 1 Gbps or the max throughput of the Edge (whichever is lower). Both the WFH Subscription and the WFH Pro Subscription offers allow for an unlimited number of home users and devices. The key difference between a business user and home user is that the business user can send traffic to the gateways, to other SD-WAN Edges, or directly to the Internet, but the home user can only send traffic directly to the Internet. Business users and home users must use separate network segments. Both WFH
Subscription and WFH Pro Subscription subscriptions will provide access to the same feature set as VMware SD-WAN.

For purposes of this Service Description and this work from home offer, a “business user” means an individual who is the customer’s designated User, as defined in the Terms of Service, (e.g., an employee of the customer, an independent contractor performing services for the customer, or a person who is otherwise one of the customer’s designated Users). A “home user” means an individual who is not a “business user” or who is not acting as a “business user” but is connected to the VMware Edge in the business user’s home, by WiFi or physical port. A “home user” may also be a “business user” of the customer (i.e., a “business user” acts as a “home user” when (s)he is using a personal device (e.g., personal laptop, personal mobile device, gaming system, smart TV, etc.).

VMware reserves the right to audit customers by checking the Edge logs to verify adherence to the requirements of this work from home offer.

VMware reserves the right to terminate this work from home offer at any time. However, termination of the offer will not operate to terminate SD-WAN WFH Subscriptions or WFH Pro Subscriptions purchased pursuant to the offer; those subscriptions will expire according to their terms, but cannot be renewed.

5. **VMware Secure Access™**

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 SD-WAN 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.

Subscriptions to VMware Secure Access are sold on a per-Named User basis (entitling you to manage up to five Devices for each Named User), where “Named User” means your employee, contractor or Third-Party Agent who has been identified and authorized by you to use the Service Offering in accordance with the Agreement, and “Device” means any client hardware that enables installing and running of the Service Offering client applications on that client hardware. You must purchase a committed term subscription of one, three, or five years. Fees for the committed term may be paid in full at the time of purchase or may be paid annually or monthly. Additionally, VMware Secure Access is also available as an add-on to VMware Workspace ONE® Enterprise Edition and VMware Workspace ONE® Advanced Edition.
6. **VMware Cloud Web Security™**

VMware Cloud Web Security is available as an add-on to VMware Secure Access or to VMware SD-WAN services. That is, you must have an active subscription to the VMware SD-WAN service or to VMware Secure Access to purchase an entitlement to VMware Cloud Web Security.

VMware Cloud Web Security is a Secure Web Gateway service. Administrators may subject workloads to a variety of security checks at the time the workloads pass through VMware PoPs that contain the VMware SD-WAN gateways. The security checks include URL filtering, anti-virus/anti-malware, cloud sandbox, and data loss prevention. Administrators may define which workloads pass through which filters 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.

Subscriptions to VMware Cloud Web Security are sold on a per-Named User basis or on a bandwidth basis. For these purposes, “Named User” means your employee, contractor, or Third-Party Agent who has been identified and authorized by you to use the offering. “Bandwidth” refers to the bandwidth tier associated with your VMware SD-WAN services purchase.

Subscriptions are offered for committed terms of one, three, or five years. You may pay subscription fees in full upfront, annually, or on a monthly basis.

In accordance with settings selected by your IT administrator, select workload data is processed by VMware Cloud Web Security on the applicable PoP, other than the workload data processed for cloud sandbox which is performed by VMware’s sub-processors. Other than to the extent snippets of that workload data are retained in logs, screenshots, or copies of confirmed malicious files or URLs, the workload data will not be retained by VMware Cloud Web Security after it is processed through the designated security checks. Logs may contain information including URL destination, IP address, and the user’s User ID, Username, name, email address. Logs and screenshots are deleted from the Service Offering within approximately 30 days of creation. Copies of confirmed malicious files and URLs may be retained and used by VMware and its service providers for threat intelligence purposes.