# VMware VeloCloud SASE
# SaaS Listing

This SaaS Listing provides delivery standards, features and Service Level Agreement that apply to the VMware VeloCloud SASE (“Broadcom SaaS Offering”) provided to the Customer and defines the parameters for the Broadcom SaaS Offering, in addition to any terms and conditions referenced on the Broadcom quote, order form, statement of work, or other mutually agreed ordering document (each a “Transaction Document”) under the applicable end user agreement or governing contract (collectively, the “Agreement”) entered into by Customer and the Broadcom entity (“Broadcom”) through which Customer obtained a right to use this Broadcom SaaS Offering. These terms shall be effective from the effective date of such Transaction Document. Capitalized terms have the meanings ascribed to them herein, or, otherwise, in the Agreement.

## 1. Technical/Business Functionality and Capabilities

### Service Overview

VMware VeloCloud SASE™ is a cloud-native secure access service edge platform that combines VMware VeloCloud SD-WAN™, VMware VeloCloud SD-Access™, VMware Cloud Web Security™, and VMware Edge Intelligence™ into one holistic solution. The platform’s points of presence (PoPs) are distributed around the world and serve as an on-ramp to SaaS and other cloud services. Details on each of the services is as follows.

VMware VeloCloud SD-WAN - VMware VeloCloud SD-WAN™ is a cloud-delivered software-defined wide area network (SD-WAN) service that provides networking services to enterprise branch locations, and to customers’ remote location workers through the “work from home” offer described below.

VMware VeloCloud SD-Access - VMware VeloCloud SD-Access™ is a cloud-delivered secure remote access solution for remote and hybrid users, devices, and applications. It provides connectivity with end-to-end encryption across peer-to-peer, users-to-applications, and devices-to-applications communications. VMware VeloCloud SD-Access is available as an add-on to VMware VeloCloud SD-WAN, or as a standalone offering, and is included in the VMware VeloCloud SD-WAN Work from Home solution.

VMware Cloud Web Security - VMware Cloud Web Security™ is available as a standalone Per Use Per Year (PUPY) service or as an add-on to VMware SD-WAN. Customer must have an active subscription to the VMware SD-WAN service to purchase an entitlement to VMware Cloud Web Security. The Service helps to protect web traffic, users and devices via cloud-delivered security service.

VMware Edge Intelligence - VMware Edge Intelligence™ is a cloud-delivered AIOps solution that employs machine learning algorithms and big data analytics to process high volumes of data to provide intelligence to help end users and IoT devices get the performance they need.

## 2. Customer Responsibilities

The following outlines Broadcom’s general roles and responsibilities in providing this Broadcom SaaS Offering. While specific roles and responsibilities have been identified as being owned by Customer, any roles or responsibilities not contained in this Service Listing are either not the duty of Broadcom or are assumed to be Customer’s responsibility.

**Service Provisioning**

Broadcom will provide the following provisioning services. Specific Broadcom SaaS Offerings may have different provisioning requirements or capabilities, as set forth in the applicable Service Listing for that Broadcom SaaS Offering.

- Broadcom will create an instance of the Broadcom SaaS Offering for Customer.
- Broadcom will create a corresponding service account and send an email or other notification to the contact that Customer identified in the Transaction Document inviting that contact to the newly created instance. A URL to access the Broadcom SaaS Offering will be provided within that notification.
- Broadcom will ensure that the identified contact can create additional user accounts for other users, as needed.
- Customer’s responsibilities include:
    - Deploying and configuring data agents and the proxy to collect and route data into the Broadcom SaaS Offering as needed.
    - Configuring the Broadcom SaaS Offering to gather metrics from cloud-based services (for example, Amazon Web Services) as needed.

**Incident and Problem Management**

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

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

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

- Customer's account settings in the Broadcom SaaS Offering administrative management console.
- User-deployed and user-configured assets such as proxy agents.
- Anything else not under Broadcom's direct control and administration.

**Change Management**

Broadcom will provide the following change management elements:

- Processes and procedures to release new code versions and bug fixes.
- Customer is responsible for:
  - Management of changes to Customer's tagging process, alert settings, dashboards, and other content.
  - Administration of self-service features provided through the Broadcom SaaS Offering's system console and user portal, up to the highest permission levels granted to Customer.
  - Changes in the data collection agents used.
  - Cooperating with Broadcom when planned or emergency maintenance is required.

**Security**

Responsibility for the end-to-end security of the Broadcom SaaS Offering is shared between Broadcom and Customer. The primary areas of responsibility between Broadcom and Customer are outlined below. Broadcom will use commercially reasonable efforts to implement reasonable and appropriate measures designed to help Customer secure Customer Content against accidental or unlawful loss, access, or disclosure, including the following:

- Information Security: Broadcom will protect the information systems used to deliver the Broadcom SaaS Offering over which Broadcom (as between Broadcom and Customer) has sole administrative level control.
- Security Monitoring: Broadcom will monitor for security events involving the underlying infrastructure servers, storage, networks, and information systems used in the delivery of the Broadcom SaaS Offering over which Broadcom (as between Broadcom and Customer) has sole administrative level control. This responsibility stops at any point where Customer has some control, permission, or access to modify an aspect of the Broadcom SaaS Offering.
- Patching and Vulnerability Management: Broadcom will maintain the systems Broadcom uses to deliver the Broadcom SaaS Offering, including the application of patches Broadcom deems critical for the target systems. Broadcom will perform routine vulnerability scans to surface critical risk areas for the systems Broadcom uses to deliver the Broadcom SaaS Offering. Critical vulnerabilities will be addressed in a timely manner.

Customer is responsible for addressing the following:

- Information Security: Customer is responsible for ensuring adequate protection of the content that Customer deploys and/or accesses with the Broadcom SaaS Offering. This includes, but is not limited to, any level of virtual machine patching, security fixes, data encryption, access controls, roles and permissions granted to Customer's internal, external, or third-party users, etc.
- Network Security: Customer is responsible for the security of the networks over which Customer has administrative level control. This includes, but is not limited to, maintaining effective firewall rules in all software-defined data centers ("**SDDCs**") that Customer deploys in a Broadcom SaaS Offering.
- Security Monitoring: Customer is responsible for the detection, classification, and remediation of all security events that are isolated with Customer's deployed SDDCs, associated with virtual machines, operating systems, applications, data, or content surfaced through vulnerability scanning tools, or required for a compliance or certification program in which Customer is required to participate, and which are not serviced under another Broadcom security program.

## 3. Entitlement and Subscription Information

The Broadcom SaaS Offering is available subject to the Authorized Use Limitation or Meter specified in the applicable Transaction

Document.

## 4. Technical Support

If Broadcom is providing SaaS Support to Customer, SaaS Support for the Broadcom SaaS Offering will be performed in accordance with the applicable support policies published at: https://support.broadcom.com/. If SaaS Support is being provided by a reseller, this section does not apply.

## 5. Additional Terms

In connection with Customer's order for any of the SASE offerings, Customer will need to provide information such as, but not limited to, site count, site location(s), feature(s), throughput(s), and Customer's network administrator's email. The information Customer provides is required to provision this Broadcom SaaS Offering. Notwithstanding anything to the contrary in the Agreement, the Subscription Term will begin on the date Customer's instance of the service has been provisioned. If Customer does not provide the needed information, Broadcom cannot provision this Broadcom SaaS Offering.

For SD-WAN subscription purchases including Equipment, the Subscription Term may begin prior to installation of the Equipment in Customer's location. VMware may permit Customer to continue to use the Broadcom SaaS Offering for an additional period, not to exceed thirty (30) days, after expiration of the committed Subscription Term, at no additional cost, if the 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.

VMware VeloCloud SD-WAN edge software ("**Software**") is installed on customer-premises equipment ("**Devices**") at the Customer location (that is, in Customer's own on-premises environment). The Devices can be supplied by Broadcom, or by Customer (provided that the equipment supplied by the customer is x86 compatible). Use of Devices purchased or rented from Broadcom is subject to the Hardware Terms for Devices set forth in the Agreement.  Customer may provision as many devices as it has licenses for edge software.

The Software and the Devices are referred to collectively as the VMware VeloCloud SD-WAN Edge (the "**Edge**"). The VMware VeloCloud SD-WAN Orchestrator ("**Orchestrator**") is 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 remote provisioning of virtual services in Customer's location, in the public cloud, or in 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 Edge with both network intelligence as well as administrative policies on how applications behave in the enterprise SD-WAN network. The Orchestrator is hosted and managed by VMware. The service also provides access to a global, distributed set of VMware VeloCloud SD-WAN Gateways ("**Gateway(s)**"), that 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. Gateways are hosted and managed by VMware.

**VMware VeloCloud SD-Access**:

Enterprise customers that have employees working remote or on the go can purchase SD-Access subscriptions to support their remote workforce. For the purpose of this SaaS listing, "user" means an individual who is the customer's designated User  (e.g., an employee of Customer, an independent contractor performing services for Customer, or a person who is otherwise one of Customer's designated Users).  An "Appliance" is considered a non-person entity or any type of machine that requires headless login services using a security token. Examples: ATM Machines, Robots, IOT Devices, and other servers.

**Cloud Web Security**

VMware Cloud Web Security™ is available as a standalone Per Use Per Year (PUPY) service or as an add-on to VMware SD-WAN. Customer must have an active subscription to the VMware SD-WAN service to purchase an entitlement to VMware Cloud Web Security. For the purpose of this SaaS listing, "**User**" means an individual person (i) authorized to use the Service, (ii) benefitting from use of the Service, (iii) on behalf of whom Customer derives benefit from the use of the Service, or (iv) that actually uses any portion of the Service. Cloud Web Security may count any and all of the following as a "User": (a) every employee of the Customer, (b) any agent, partner/contractor resource, or other non-employee (i.e., each individual person) authorized by Customer to use and/or benefit from the use of the Service, and (c) any consumption of 8 Gigabytes (and every multiple of 8 Gigabytes thereafter) of Service activity/traffic. A User may have up to four (4) devices.  Cloud Web Security will not count as a "User" the first 8 Gigabytes consumed by any person already counted as a "User" under subsections (a) and (b). **"Bandwidth"** means Megabits/second usage of processed data or traffic. Each customer that has a SD-WAN Edge in a branch location will purchase an associated "Bandwidth" that the SD-WAN Edge can process. Cloud Web Security "Bandwidth" add-on would be an equivalent amount of bandwidth subscribed to enable the customer to protect web traffic, users and devices via cloud-delivered security service.

**Edge Intelligence**

If Customer purchased a license to VMware Edge Intelligence, Customer may use the Edge Intelligence service to monitor up to the number of Nodes for which Customer has paid the applicable license fees.  Customer may use the Edge Intelligence service solely during the Subscription Term. Upon expiration or termination of Customer's licenses to the Subscription Software, Customer must promptly cease use of the service.

Customer’s Subscription Term will begin on the later of the date that is communicated to Customer by VMware order management and the date that VMware accepts Customer’s Order. The Subscription Term may begin prior to installation of the Devices in Customer’s location. VMware may permit Customer to continue to use the Edge Intelligence service for an additional period, not to exceed 30 days, after expiration of Customer’s committed Subscription Term, at no additional cost, if Customer’s Subscription Term began prior to installation of the Devices. All terms, other than payment of fees, will continue to apply during any extended use term.

Broadcom may modify the Broadcom SaaS Offering and/or the corresponding SaaS Listings at any time: (a) due to changes in applicable laws or industry standards; and (b) for any other reason, if the modification does not materially reduce the level of performance, functionality, security or availability of the Broadcom SaaS Offering during the Term.

**Data Retention and Deletion:**

**VMware VeloCloud SD-WAN**: As VMware VeloCloud SD-WAN is used, the 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 VMware VeloCloud SD-WAN will be retained in the Orchestrator and available for querying and alerts for at least two (2) weeks (by default) from the date and time the data was originally ingested into VMware VeloCloud SD-WAN. The amount of data stored depends on the storage space available on the Orchestrator and the amount of data generated by each site’s Edge.

**VMware VeloCloud SD-Access:** VMware VeloCloud SD-Access processes identity and authentication information, communications metadata (which device talked to which device, amount of data transferred, performance), geo-location data (based on IP geo-location). Data is retained for one (1) year after ingestion.

**VMware Cloud Web Security:** Depending on Customer’s configuration of VMware Cloud Web Security, workload data selected by Customer is sent to VMware Cloud Web Security for security checks as designated by Customer. Customer 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, groups, file type, application, and domain.

Additional terms and conditions that may apply to the SaaS Offering are available at:

## 6. THIRD PARTY INFORMATION AND TERMS

Any required third-party software license terms are incorporated by this reference and are set forth in online documentation at https://techdocs.broadcom.com/ or http://legaldocs.broadcom.com/.

# Exhibit A

# Service Level Agreement

## 1. GENERAL

This Service Level Agreement ("SLA") is subject to the Agreement. Capitalized terms not defined in this SLA will have the meanings specified in the Agreement. We reserve the right to change the terms of this SLA in accordance with the Agreement.

## 2. Availability

Broadcom will use commercially reasonable efforts to ensure that the SaaS Offering is available during a given month equal to the "Availability Commitment" specified in the table below.

| SaaS Offering | Availability Commitment |
|---|---|
| VMware VeloCloud SD-WAN | 99.99% |
| VMware VeloCloud SD-Access | 99.99% |
| VMware Cloud Web Security | Inline Service Availability 99.999%<br>Non-inline Service Availability 99.5% |
| VMware Edge Intelligence | 99.90% |

Availability in a given billing month is calculated according to the following formula:

"Availability" = ([total minutes in a billing month – total minutes Unavailable] / total minutes in a billing month) x 100

**Inline (Data Plane) Service Availability** means access to the core features of the Service that impact the data in transit to and from Customer to the Internet. Cloud Web Security is an Inline Service that includes Content-Filtering and Anti-Malware scanning

**Non-inline (Control Plane) Service Availability** is access to the controls that govern the features of Cloud Web Security that do not impact data in transit to and from the end-user to the Internet (e.g., reporting tools used by the administrator. Examples of Non-Inline Service for Cloud Web Security include: Reporting and Advanced Malware sandboxing.

## 3. Unavailability and SLA Events for VMware VeloCloud SD-WAN

**VMware VeloCloud SD-WAN** will be considered "Unavailable", subject to the Service Level Agreement Limitations set forth below, if Broadcom's monitoring tools determine one of the following events (each, an "SLA Event") has occurred.

The following will be considered an SLA Event for VMware VeloCloud SD-WAN:

- "**Data Plane ("DP") Event**" is the period of time (at least one minute) that the VMware VeloCloud SD-WAN gateway and/or controller functionality is unable to transmit or receive packets. During a Data Plane Event, a VMware VeloCloud SD-WAN Edge is unable to receive or transmit IP packets as measured by the applicable Broadcom trouble ticket or Broadcom log files.

- "**Control and Management Plane ("CMP") Event**" is the period of time (at least 30 seconds) that the VMware VeloCloud SD-WAN orchestrator is unavailable to monitor and configure the Edges.

## 4. Unavailability and SLA Events for VMware VeloCloud SD-Access

**VMware VeloCloud SD-Access** will be considered "Unavailable", subject to the Service Level Agreement Limitations set forth below, if Broadcom's monitoring tools determine one of the following events (each, an "SLA Event") has occurred:

- "**Data Plane ("DP") Event**" is the period of time (at least one minute) that the VMware VeloCloud SD-Access tunnel functionality is unable to transmit or receive packets. During a Data Plane Event, a VMware VeloCloud SD-Access or Client connector is unable to receive or transmit IP packets as measured by the applicable Broadcom trouble ticket or Broadcom log files.
- "**Control Plane ("CP") Event**" is the period of time (at least 30 seconds) that the VMware VeloCloud SD-Access orchestrator is unavailable to respond to SD-WAN Clients
- "**Management Plane ("MP") Event**" is the period of time (at least 30 seconds) that the VMware VeloCloud SD-Access orchestrator is unavailable for Administrators to login with their correct credentials.

## 5. Unavailability and SLA Events for VMware Cloud Web Security

VMware Cloud Web Security will be considered “Unavailable”, subject to the Service Level Agreement Limitations set forth below, if Broadcom’s monitoring tools determine one of the following events (each, an “SLA Event”) has occurred:

- **“Data Plane (“DP”) Event**” is the period of time (at least one minute) that the Cloud Web Security dataplane is unable to transmit or receive packets. During a Data Plane Event, Cloud Web Security is unable to receive or transmit IP packets as measured by the applicable Broadcom trouble ticket or Broadcom log files.
- **“Control and Management Plane (“CMP”) Event**” is the period of time (at least 30 seconds) that the Cloud Web Security portal is unavailable to monitor and configure the security policy or rules.

## 6. Unavailability and SLA Events for VMware Edge Intelligence

**VMware Edge Intelligence** will be considered “Unavailable”, subject to the SLA Limitations set forth below, if Broadcom’s monitoring tools determine one of the following events (each, an “SLA Event”) has occurred:

- any period of time (at least one minute) during which users are not able to access the service’s UI.

## 7. Service Level Agreement Limitations

The total minutes that a SaaS Offering is Unavailable for a particular SLA Event is measured from the time that Broadcom validates the SLA Event has occurred, until the time that Broadcom resolves the SLA Event such that the SaaS Offering is not unavailable to the Customer.

All SLA Event measurements will be rounded up or down to the nearest one-minute increment, with increments equal to or greater than 30 seconds being rounded up to the next minute. Final determinations of the length of the cumulative periods of SLA Events over a calendar month shall be based on Broadcom’s monitoring. Broadcom’s monitoring tools, data, and records will be the sole source of information used to track and validate Unavailability.

The following will be excluded from any time-based calculations related to the SaaS Offering being Unavailable:

(i) scheduled maintenance where Customer has been notified at least 24 hours in advance,

(ii) recurring or zero-impact maintenance that is generally applicable to all customers,

(iii) Customer’s misuse of any of the SaaS Offerings,

(iv) improper configuration of any of the SaaS Offering’s redundancy by Customer,

(v) force majeure events, denial of service attacks, viruses, or hacking attacks for which there is no commercially reasonable known solution, or any other events that are not within Broadcom’s control or that could not have been avoided with commercially reasonable care,

(vi) acts or orders of government,

(vii) any failure or malfunction of equipment, applications or systems not owned or controlled by Broadcom or under its direction or control,

(viii) unavailability of any Customer personnel required to restore the SaaS Offering, including as a result of Customer’s failure to provide Broadcom with accurate, current contact information, and/or

(ix) emergency maintenance where, in Broadcom’s reasonable judgment, such maintenance cannot be performed during a scheduled maintenance window due to the urgent nature of the threat or potentially negative impact of failure to perform the maintenance.

Changing the geographic location of Customer’s associated account may need re-acquisition of services or the SaaS Offering that were available to Customer in the previous region. Any downtime caused by this will be excluded from time-based calculations related to Unavailability.

END OF EXHIBIT A