VMware Edge Intelligence
SaaS Listing

This SaaS Listing provides delivery standards, features and Service Level Agreement that apply to the VMware Edge Intelligence ("Broadcom SaaS Offering") provided to the Customer and defines the parameters for the 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 Edge Intelligence™ is a SaaS-based Artificial Intelligence for IT Operations (AIOps) solution that provides intelligence to enable end-users and IoT devices at the edge of distributed and secure enterprise networks to get the performance and analytics they need from WLAN, LAN, WAN, and SASE network services and applications to which they connect. VMware Edge Intelligence employs machine learning algorithms (ML) and big data analytics to process high volumes of data from a wide range of networks, devices, and applications. In doing so, the service auto-discovers end-user and IoT devices, automatically establishes baselines, understands client interactions, and monitors for deviations to provide actionable insights that operations teams can proactively remediate.

- VMware Edge Intelligence Crawler software ("**Software**") is installed on edge devices provided by Broadcom (each, a "**Device**") or on other equipment ("**Equipment**") at Customer's location as a virtual appliance. As used in this SaaS Listing, any Device or Equipment with the Software installed is a "**Crawler**".

- The Software collects performance metrics from across the network stack and examines network traffic by performing deep packet inspection. The extracted performance metrics are sent to the service platform for analysis.

- VMware Edge Network Intelligence is included as an entitlement in the VMware VeloCloud SD-WAN product, but it is also available as a standalone cloud service offering. On-premise installations of the Broadcom SaaS Offering are out of scope for this document.

Service Software Components

- The SaaS Offering includes the following software components: VMware Edge Intelligence Crawler

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 SaaS 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 SaaS Listing for that Broadcom SaaS Offering.

- Broadcom will create an account within the Broadcom SaaS Offering for Customer, as needed.
- 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:
    - Activate the Crawler by either

    - Enabling the function in an SD-WAN Edge
    - Deploying and activating a standalone crawler on customer owned and managed hardware
  - 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:

- Account Security: Customer is responsible for securing passwords are ensuring they are sufficiently complex.
- 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

Notwithstanding the provisions in the General Terms, the Cloud Exhibit, and Customer's Order, the Subscription Term will begin on the first to occur of (i) the date Customer's instance of the VMware Edge Intelligence service has been provisioned or (ii) the end of Customer's deployment window if a deployment window was quoted and ordered. The Subscription Term may begin prior to installation of the Edge in Customer's designated location. Broadcom may permit Customer to continue to use the VMware Edge Intelligence service 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 Edge. All terms, other than payment of fees, will continue to apply during any extended use term.

Data Retention and Deletion: During the Subscription Term, Customer Content transmitted to VMware Edge Intelligence will be retained and available for querying and alerts for approximately two weeks from the date and time the data point was originally ingested into the service, after which time it is deleted. During the Subscription Term, any log files containing Customer Content will be deleted approximately thirty (30) days after their creation.

Termination of the Subscription Term will result in deletion of all Crawler configuration and data. Customer Content will be deleted within approximately fourteen (14) days after the termination date. Any log files containing Customer Content will be deleted approximately thirty (30) days after the termination date. During this fourteen (14)-day period, data will not be generally accessible. Any deleted data is non-recoverable.

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.

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

3. Unavailability and SLA Events for VMware Edge Network 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 SaaS Offering's UI.

4. 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