AppNeta

Specific Program Documentation ("SPD") and SaaS Listing

The Broadcom software and services ("Broadcom Offering") listed below is provided under the following terms and conditions 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 license for the Broadcom Offering. These terms shall be effective from the effective date of such Transaction Document. Capitalized terms in this document have the meaning ascribed to them herein or, otherwise, in the Agreement.

Broadcom Offering Name: *AppNeta*

1. DEFINITIONS.

- "Monitored Application" is an application or network path monitored by the Broadcom Offering.
- "Monitoring Point" is a data generating and collecting component of the Broadcom Offering for monitoring a Monitored Application. A Monitoring Point may be a native application, container-based, Broadcom-hosted, or embodied as a physical or virtual appliance.
- "Monitoring Point Type" is a classification of available Monitoring Points based on bandwidth, form factor, functionality, and corresponding Monitored Application entitlements. Monitoring Point Types include Type 1 for monitoring workstations, Type 2 for monitoring a standard office (up to 999 employees), Type 3 for monitoring a large office (1000 or more employees), and Type 4 for monitoring a data center (speeds greater than 10 Gbps).
- "AppNeta On-Prem" is an instance of the Broadcom Offering management component hosted in Customer's environment.
- "AppNeta SaaS" is a Software as a Service ("SaaS") management component of the Broadcom Offering.
- "Subscription Term" is the time period for which the Broadcom Offering is agreed as specified in the applicable Transaction Document.
- "Universal License" is a licensable consumption unit valid toward operation of an applicable Monitoring Point Type and Monitored Application allocation. The number of Universal Licenses for a given Customer is set forth in the applicable Transaction Document.
- "Universal License Requirement" is a minimum number of Universal Licenses required to use the Broadcom Offering for an applicable Monitoring Point Entitlement and Monitored Application Entitlement.

2. USE RIGHTS AND LIMITATIONS.

- The **Broadcom Offering** is licensed by the number of **Universal Licenses** set forth in the Transaction Document. Customer receives entitlements to use a specific number and type of

Monitoring Points, and a specific number of Monitored Applications according to the following table:

Universal License Requirement	Monitoring Point Entitlement	Monitored Application Entitlement
1	50 count Monitoring Point Type 1	250 (5 per Monitoring Point)
1	1 count Monitoring Point Type 2	15
6	1 count Monitoring Point Type 3	90
12	1 count Monitoring Point Type 4	180

- Hardware for physical appliance Monitoring Points must be purchased separately by Customer.
- Customer may acquire additional Monitored Applications for 1 Universal License per 15 additional Monitored Applications.
- Customer may be entitled to either the AppNeta SaaS or the AppNeta On-Prem as set forth on the Transaction Document.

3. APPNETA SAAS ADDITIONAL TERMS AND INFORMATION

The Broadcom Offering may include the AppNeta SaaS as indicated within the Transaction Document with the following additional terms and information:

a. AppNeta SaaS has the following built-in data retention capabilities during the Subscription Term:

   i. Delivery data from continuous monitoring, diagnostics, voice and video tests are kept for 365 days.

   ii. Path route history is retained for 90 days.

   iii. Experience milestone details are kept for 45 days. Older tests will contain transaction performance and details only.

   iv. Usage data is kept for 90 days with no limit on data size.

   v. Usage packet captures are kept for 365 days (subject to size limits).

b. Encryption

   i. All communications of any kind from a Monitoring Point up to the AppNeta SaaS are encrypted by default. This includes data for the Broadcom Offering user interface and application programming interface (“API”).

c. Packet Captures

   i. Packet captures are uploaded to a capture server via a Secure Sockets Layer (“SSL”) link, where they remain in encrypted form (e.g, AES-256). The symmetric key used for encryption is based on a per-Monitoring Point, user-defined passphrase, which a Customer sets on the Monitoring Point, and is never shared with, or is otherwise discoverable, by Broadcom. The passphrase is stored on the Monitoring Point in a hashed form (e.g., SHA-1).

ii. For download, packet captures must be decrypted using the symmetric key created from the passphrase. A user is prompted for a passphrase once per Monitoring Point per login session; the passphrase is cached only for the duration of the login session. The actual download is via SSL.

iii. As part of Monitoring Point decommissioning, a user may clears the passphrase and packet captures that have not yet been uploaded. If the Monitoring Point is no longer being used for packet captures, but is not being decommissioned it, a separate “clear passphrase” function is available.

d. Measurement Modes

i. AppNeta SaaS’s measures application performance via multiple instrumentation modes. One mode, delivery network instrumentation, is an active network performance measurement method, which operates by sending and receiving internally generated measurement traffic. No Customer device or application data is used in this method of network performance monitoring.

ii. AppNeta SaaS’s monitoring functionality uses a web synthetics technique, where web transactions are executed by purpose-built Monitoring Points. Customers have full control over all actions taken in the synthetic scripts, and no pages or data outside of those explicitly defined in the script will be accessed. When monitoring Monitored Applications transmitting Personal Data, Customer shall use sample or test records for measurement instead of real user account data.

iii. AppNeta SaaS’s usage analysis allows the Customer to perform deep packet inspection on network traffic to identify the applications in use on the network. This includes the capability for the Customer to perform packet capture. All packet captures are encrypted in memory on the Monitoring Point with a FIPS 140-2 and PCI-DSS compliant encryption algorithm (e.g., AES-256) to ensure data encryption in transit and at rest. As mentioned above, the passphrase for this encryption is set by the Customer on the Monitoring Point, and is never shared with Broadcom.

e. Personal Data Terms

i. When monitoring Monitored Applications, with the AppNeta SaaS that may transmit synthetic Personal Data, Customer agrees to use fictional records for measurement that do not include actual Personal Data. Broadcom shall accept no responsibility or liability for data processing that occurs as a result of Customer’s non-compliance with this section

4. APPNETA ON-PREM ADDITIONAL TERMS AND INFORMATION

a. Access to AppNeta On-Prem Software

- Customer shall grant Broadcom or a Broadcom designated partner access to its AppNeta On-Prem software at least annually for license utilization, maintenance and upgrades or for emergency maintenance at a time mutually agreed by Customer and Broadcom.

5. APPNETA SAAS--SAAS LISTING

The following SaaS Listing terms shall apply to AppNeta SaaS (the “Service”):

a. Service Description

AppNeta SaaS is the component of the Broadcom Offering that monitors the end user experience of applications and networks through a combination of active and passive testing to ensure applications are reachable and performant for users. Broadcom will collect, modify and analyze metadata and/or operations data which does not contain any data entered into the Service by Customer, such as system log files and transaction counts which related to system utilization and performance statistics, all as deemed necessary by Broadcom.

b. Data Location

All client data, including backups, will physically reside and be processed within the following countries:

United States

Broadcom reserves the right to change the location of the data within these stated countries and will notify customers of any such changes.

c. Security and Audit Requirements

The following audits will be performed at the frequency defined below for the Service:

Type of Audit	Frequency
System and Organization Controls (SOC) 2 Type II	Annual
3rd Party Penetration Testing	Semiannual

d. Service Level Availability (SLA)

Broadcom will use commercially reasonable efforts to provide 99% Service Availability ("Uptime Target"). Any failure of Broadcom to achieve the Uptime Target does not constitute a breach of contract nor will any money damages or other remedies be available at law or equity.

e. Method of Measuring SLA

Service Availability will be calculated on a monthly basis using the following formula: Actual Availability divided by Expected Availability (expressed as a percentage).

Definitions. The following definitions will apply with respect to the calculation of Service Availability:

"Actual Availability" means (in minutes) Expected Availability minus Unpermitted Downtime. **"Expected Availability"** means (in minutes) seven (7) days per week, twenty-four (24) hours per day.

"Downtime" means the time (in minutes) that users of the Service are not able to access the Service due to failure, malfunction or delay.

"Permitted Downtime" includes Downtime relating to (i) Maintenance, (ii) the facilities, infrastructure, network, products or services of Customer (or any supplier, agent or representative of Customer), (iii) the acts, omissions,

products or services of a third party, (iv) the negligence, willful misconduct or breach of this Agreement by Customer, or (v) any other cause not within Broadcom's reasonable control.

"Unpermitted Downtime" means Downtime minus Permitted Downtime.

"Maintenance" means time (in minutes) that the Service is not accessible to Customer due to maintenance of the Service, including maintenance and upgrading of the software and hardware used by Broadcom to provide the Service. Maintenance includes scheduled maintenance and unscheduled or emergency maintenance. Broadcom will use commercially reasonable efforts to provide Customer with at least two business days' prior written notice of any scheduled maintenance or sixty minutes' advance written notice for unscheduled, emergency maintenance. Broadcom will provide such notice to Customer by email to an address provided by Customer. Maintenance in any given month will not exceed eight (8) hours per month. Any time during which the Service is unavailable to Customer due to maintenance or other activity by Broadcom for which Broadcom fails to give notice, which exceeds the permitted time allotment, or which occurs outside of the foregoing permitted hours will be included in the calculation of Downtime. Broadcom will use commercially reasonable efforts to schedule all scheduled maintenance windows beginning at 8:00 p.m. Eastern Time.

f. Data Backup

Broadcom commits to the following data backup and replication during the Subscription Term:

Data Backup: All Customers of the Service shall have their data backed up on a daily basis by Broadcom. Backups are securely replicated to an alternate location (within the same geographic location) limiting data loss to no more than 24 hours in the event of a primary data location disaster.

- Daily backups are retained for a minimum of 30 days
- Removable media are not used for data or backup storage

g. Disaster Recovery

The Service maintains a DR plan in the event the primary site is rendered inoperable. The following are the key measures of the DR plan:

Recovery Time Objective (RTO):
48 hours

Recovery Point Objective (RPO):
Maximum data loss: 24 hours

Data that is uploaded, but not backed up within the 24 hours will be lost.

Recovery Time Objective or RTO is defined as the duration of time within which the Service will be restored after a major interruption or incident.

Recovery Point Objective or RPO is defined as the maximum period in which data might be lost from the Service due to a major interruption or incident.

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 techdocs.broadcom.com or legaldocs.broadcom.com.