Carbon Black Cloud

SaaS Listing

The definitions set out in the Agreement will apply to this SaaS Listing document.

The Broadcom software program(s) ("Broadcom Software") listed below is provided under the following terms and conditions in addition to any terms and conditions referenced on the Broadcom quote or other transaction document entered into by you and the Broadcom entity ("Broadcom") through which you obtained a license for the Broadcom Software (hereinafter referred to as the "Agreement"). These terms shall be effective from the effective date of such ordering document.

This SaaS Listing describes Carbon Black Cloud ("Service"). All capitalized terms in this SaaS Listing have the meaning ascribed to them in the Agreement (including the Broadcom Glossary) or in the Definitions section.

Table of Contents

Carbon Black Cloud

SaaS Listing

1: Technical/Business Functionality and Capabilities

Service Overview

Carbon Black Cloud is a cloud-native endpoint and workload protection platform that enables customers to protect, prevent, detect, and respond to cybersecurity attacks on their endpoints and server workloads.

Service Features

- **Service Provisioning**. Broadcom will create an instance of the Service 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 Service will be provided within that notification. Broadcom will ensure that the identified contact can create additional user accounts for other users, 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 Service.

2: Customer Responsibilities

CA can only perform the Service if Customer provides required information or performs required actions, otherwise CA's performance of the Service may be delayed, impaired or prevented, and Customer may lose eligibility for any Service Level Agreement.

- Customer is responsible for deploying and configuring data agents and the proxy to collect and route data into the Service as needed.
- Customer is responsible for configuring the Service to gather metrics from cloud-based services (for example, Amazon Web Services) as needed.
- 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 Service administrative management console. User-deployed and user-configured assets such as proxy agents. Anything else not under Broadcom's direct control and administration.
- 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 Service'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.
- Information Security: Customer is responsible for ensuring adequate protection of the content that Customer deploys and/or accesses with the Service. 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 Service.
- 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

Charge Metrics

The Service is available under the following License Metric as specified in the Transaction Document:

- "Sensor Software" means software agents installed on a customer's Endpoints or workloads.

Carbon Black Cloud

SaaS Listing

4: Customer Assistance and Technical Support

Customer Assistance

CA will provide the following assistance as part of the Service, during regional business hours:

- Receive and process orders for implementation of the Service
- Receive and process requests for permitted modifications to Service features; and
- Respond to billing and invoicing questions

Technical Support

If CA is providing Technical Support to Customer, Technical Support is included as part of the Service as specified below. If Technical Support is being provided by a reseller, this section does not apply.

- Support for Services will be performed in accordance with the published terms and conditions and technical support policies published in the "Broadcom Software Maintenance Policy Handbook" at: https://support.broadcom.com/external/content/release-announcements/CA-Support-Policies/6933.

Maintenance to the Service and/or supporting Service Infrastructure

CA must perform maintenance from time to time. For information on Service status, planned maintenance and known issues, visit https://status.broadcom.com/. The following applies to such maintenance:

- **Planned Maintenance:** Planned Maintenance means scheduled maintenance periods during which Service may be disrupted or prevented due to non-availability of the Service Infrastructure. During Planned Maintenance, Service may be diverted to sections of the Infrastructure not undergoing maintenance which may result in no disruption of the Service. For Planned Maintenance, CA will provide seven (7) calendar days' notification.
- **Unplanned Maintenance**: Unplanned Maintenance means scheduled maintenance periods that do not allow for seven (7) days notification and during which Service may be disrupted or prevented due to non-availability of the Service Infrastructure. CA will provide a minimum of one (1) calendar day notification. During Unplanned Maintenance, Service may be diverted to sections of the Infrastructure not undergoing maintenance which may result in no disruption of the Service. At times CA will perform Emergency Maintenance. Emergency Maintenance is defined as maintenance that must be implemented as quickly as possible to resolve or prevent a major incident. Notification of Emergency Maintenance will be provided as soon as practicable.
- **Note:** For Management Console Maintenance, CA will provide fourteen (14) calendar days' notification. CA may perform minor updates or routine maintenance to the Management Console with no prior notification as these activities do not result in Service disruption.

5: Additional Terms

CA may modify the Service 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 Service during the Term.

- For Carbon Black® Managed Detection and Response ("MDR"), any warranties in the General Terms and the Cloud Exhibit are expressly excluded. The sole and exclusive warranty for Carbon Black Managed Detection and MDR, express or implied, is as follows: Carbon Black warrants that Broadcom Carbon Black Managed Detection and MDR will be performed in a professional and workmanlike manner consistent with industry standards for similar types of services.
- Threat Intelligence Data Collection. Certain Carbon Black services may collect data relating to malicious or potentially malicious code, binaries, attacks, activities, and vulnerabilities on a customer's Endpoints or workloads ("Threat Intelligence Data"). Threat Intelligence Data is collected by Broadcom for analysis and possible inclusion in a threat intelligence feed utilized by certain Broadcom Carbon Black services. Prior to inclusion in any threat intelligence feed, Threat Intelligence Data will be: (i) reduced to a unique file hash or to queries or general behavioral descriptions that can be used to identify the same or similar malicious or potentially malicious code in the customer's systems and other customers' systems and/or (ii) be anonymized and made un-attributable to any particular customer or individual (collectively "Un-attributable Threat Intelligence Data"). Broadcom may distribute Un-attributable Threat Intelligence Data to

its customers at its discretion as part of its threat intelligence data feed or in published reports or research. By using a Broadcom Carbon Black Service, Customer is deemed to have agreed that Un-attributable Threat Intelligence Data is not Customer Content, and Broadcom may retain, use, copy, and modify the Threat Intelligence Data for its internal business purposes, and additionally distribute and display the Un-attributable Threat Intelligence Data, for its business purposes, including without limitation for developing, enhancing, and supporting products and services, and for use in its threat intelligence feed or in published reports and research. The information provided via any threat intelligence feed is provided on an "AS IS" and "AS AVAILABLE" basis only.

- Updates and Upgrades to Sensor Software. Broadcom may release patches, bug fixes, updates, upgrades, maintenance and/or service packs ("Updates") for the Sensor Software from time to time, which may be necessary to ensure the proper function and security of the Broadcom Carbon Black Services. Broadcom is not responsible for performance, security, warranty breaches, support or issues encountered in connection with the Broadcom Carbon Black Services that result from Customer's failure to accept and apply Updates within a reasonable time frame.
- Usage Data. Customer agrees to provide the information in this Services Guide, including this Section 2.5, regarding the collection and use of usage data, including any available controls in relation to the cookies or tracking technology, including those provided by third parties, to all users of the Broadcom Carbon Black services.
- **Data Retention and Deletion**: During the subscription Term, data will be retained and deleted as set forth below.

  Carbon Black Endpoint™ Foundations:

  - Short term events are retained and available to Customer for a minimum of thirty (30) days and a maximum of thirty-two (32) days for search and investigation.
  - Alerts and their associated event data ("long term events") are retained for a minimum of one hundred eighty (180) days and a maximum of two hundred ten (210) days.

  Carbon Black Enterprise EDR™:

  - Endpoint data is stored for thirty (30) days in the following two formats: (1) proprietary format for endpoint data optimized for fast retrieval, and (2) Solr indices.
  - Raw protobufs (for troubleshooting purposes) are stored for seven (7) days.

  Carbon Black Live Query:

  - The past query list is retained for thirty (30) days.
  - The results of a query are retained for thirty (30) days (Broadcom stores up to seven thousand five hundred (7,500) results per Endpoint per day). A User can choose to export the results on the User's own device.

  Live Response Feature

  - Using the Live Response feature, the administrator may remote into a device to take an action. If the action involves getting a copy of a file, the file is temporarily captured in the session cache for the duration of the Live Response session and in any event is automatically deleted after fifteen (15) minutes of inactivity. This time frame is configurable.

  Log Data

  - During the subscription Term, diagnostic logs are purged after seven (7) days and audit logs are removed every twelve (12) months. If Customer wishes to extract Customer Content from the Carbon Black ServiceCloud service (to the extent Customer has not already done so prior to termination of the Subscription Term), Customer must notify Broadcom within five (5) days after the effective termination date, and Broadcom will assist Customer in extracting Customer Content from the Carbon Black ServiceCloud service. Customer is responsible for all fees associated with content extraction. If Customer does not notify Broadcom within that five (5)-day period, Customer Content will be permanently deleted and may not be recoverable.

6: Definitions

"**Administrator**" means Customer's designated personnel to manage the Service on behalf of Customer.

"**Service Credit**" means the number of days that are added to Customer's current Term.

"**Service Infrastructure**" means any CA or licensor technology and intellectual property used to provide the Services.

Carbon Black Cloud

SaaS Listing

Exhibit-A

Service Level Agreement(s)

1.0 GENERAL

These Service Level Agreements ("SLA(s)") apply to the Online Service that is the subject matter of this SaaS Listing only. If CA does not achieve these SLA(s), then Customer may be eligible to receive a Service Credit. Service Credits are Customer's sole and exclusive remedy and are CA's sole and exclusive liability for breach of the SLA.

2.0 SERVICE LEVEL AGREEMENT(S)

- **Availability** means the amount of time as measured as a percentage per calendar month when the user interface for the Service can be logged into. Availability excludes any period of time that the Service cannot be logged into due to: (i) a failure between the customer's computing environment, computer(s), or system(s) and the Internet; (ii) factors outside of VMware's reasonable control; (iii) any action or inaction of Customer or a Customer user, administrator, or anyone acting on behalf of Customer; or (iv) scheduled maintenance periods and necessary but unscheduled Emergency Maintenance.
- **Availability Target:** Broadcom sets an availability target of 99.9%.

3.0 AVAILABILITY CALCULATION

Availability is calculated as a percentage of 100% total minutes per calendar month as follows:

$$\frac{\text{Total Minutes in Calendar Month} - \text{Excused Outages} - \text{Non-Excused Outages*}}{\text{Total} - \text{Excused Outages}} \times 100 > \text{Availability Target}$$

**Non-Excused Outages = Minutes of Service disruption that are not an Excused Outage*

Note: The availability calculation is based on the entire calendar month regardless of the Service start date.

4.0 SERVICE CREDIT

If a claim is made and validated, a Service Credit will be applied to Customer's account.

CA will provide a Service Credit equal to two (2) days of additional service for each 1 hour or part thereof (aggregated) that the service is not available in a single 24-hour period, subject to a maximum of seven (7) calendar days for all incidents occurring during that 24 hour period. A Customer may only receive up to twenty-eight (28) days maximum, for up to four (4) Service Credits, over twelve (12) months. The maximum is a total for all claims made in that twelve (12) month period.

Service Credits:

- May not be transferred or applied to any other CA Online Service, even if within the same account.
- Are the only remedy available, even if Customer is not renewing for a subsequent term. A Service Credit is added to the end of Customer's current Subscription Term.
- May not be a financial refund or credit of any kind.
- Do not apply to failure of other service level SLAs if such failure relates to non-availability of the Service. In such cases Customer may only submit a claim for the Availability SLA.

5.0 CLAIMS PROCESS

Customer must submit the claim in writing via email to CA Customer Support. Each claim must be submitted within ten (10) days of the end of the calendar month in which the alleged missed SLA occurred for CA to review the claim. Each claim must include the following information:

(i) The words "Service Credit Request" in the subject line.
(ii) The dates and time periods for each instance of claimed outage or other missed SLA, as applicable, during the relevant month.
(iii) An explanation of the claim made under this SaaS Listing, including any relevant calculations.

All claims will be verified against CA's system records. Should any claim be disputed, CA will make a determination in good faith based on its system logs, monitoring reports and configuration records and will provide a record of service availability for the time period in question to Customer.

6.0 EXCUSED OUTAGES AND EXCLUSIONS TO CLAIMS

The following are minutes of downtime that are defined as Excused Outages:

- Planned Maintenance and Unplanned Maintenance as defined in the SaaS Listing.
- Force Majeure as defined in the Agreement.
- Any downtime that results from any of the below listed exclusions to a claim.

If any of the following exclusions apply, a claim will not be accepted:

- Any Service provided on a provisional basis, including but not limited to: trialware, evaluation, Proof of Concept, Not for Resale, pre-release, beta versions.
- Customer has not paid for the Service.
- Third party, non-CA branded products or services resold with the Service.
- Hardware, software or other data center equipment or services not in the control of CA or within the scope of the Service.
- Any item that is not a Service Component that is provided for use with the Service.
- Technical support provided with the service.
- Failure of Customer to correctly configure the Service in accordance with this SaaS Listing.
- Hardware or software configuration changes made by the Customer without the prior written consent of CA.
- Unavailability of a specific web page or a third party's cloud application(s).
- Individual data center outage.
- Unavailability of one or more specific features, functions, or equipment hosting locations within the service, while other key features remain available.
- Unavailability or performance impact caused by acts of government or intermediate carriers
- Failure of Customer's internet access connections.
- Suspension and termination of Customer's right to use the Service.
- Alterations or modifications to the Service, unless altered or modified by CA (or at the direction of or as approved by CA
- Defects in the Service due to abuse or use other than in accordance with CA's published Documentation unless caused by CA or its agents.
- Customer-requested hardware or software upgrades, moves, facility upgrades, etc.

END OF EXHIBIT A