DLP Cloud (CloudSOC CASB, CDS)

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 DLP Cloud, CloudSOC CASB Audit, CloudSOC CASB for IaaS, CloudSOC CASB for SaaS, CloudSOC CASB Gateway, CloudSOC CASB Advanced Threat Protection (ATP), Data Loss Prevention Cloud Detection Service for CASB, Data Loss Prevention Cloud Detection Service for API Detection, Data Loss Prevention Cloud Detection Service for Cloud SWG, Data Loss Prevention Cloud Prevent for Microsoft Office 365 Exchange, and Data Loss Prevention Cloud Detection Service for Office 365 Email and Gmail Standalone services (each, a "Service"). All capitalized terms in this Listing have the meaning ascribed to them in the Agreement or in the Definitions section.

Table of Contents

DLP Cloud (CloudSOC CASB, CDS)

Saas Listing

1: Technical/Business Functionality and Capabilities

Service Overview

"DLP Cloud" platform provides multiple services as follows. The Service will be provided in accordance with the terms of the Agreement and the documentation available at the Portal.

- **"CloudSOC CASB Audit"** is a cloud-based service that provides visibility into usage of cloud applications, and the security risk of the applications based on a business reading rating (BRR) model.
- "**CloudSOC CASB Securlet for IaaS**" is a cloud-based service that provides visibility and control over activities of Users in cloud applications, as well as monitoring and protection of data that is transferred, stored, and/or shared. CASB Securlet for IaaS is also used to configure security assessment policies for validating Cloud Security Posture Management (CSPM). Available IaaS applications - a complete list of cloud applications supported by the CloudSOC CASB offerings can be found in the CloudSOC Portal, and includes, but is not limited to Amazon Web Service (AWS) and Microsoft Azure.
- "**CloudSOC CASB Securlet for SaaS**" is a cloud-based service that provides visibility and control over activities of Users in cloud applications, as well as monitoring and protection of data that is transferred, stored, and/or shared. CASB Securlet for SaaS is also used to configure security assessment policies for validating SaaS Security Posture Management (SSPM). Available SaaS applications - a complete list of cloud applications supported by the CloudSOC CASB offerings can be found in the CloudSOC Portal - includes, but is not limited to Microsoft Office 365, G Suite, Box and Slack.
- **"CloudSOC CASB Gateway"** is a cloud-based transparent gateway service that provides visibility and control of user activities through inline inspection of traffic.
- **"CloudSOC CASB Advanced Threat Protection"** detects advanced threats using the Symantec Cynic™ sandbox, and malicious URLs in content. (Service Add-On)
- **"Data Loss Prevention Cloud Detection Service for CASB"** is a cloud-based service and can be used in conjunction with the Symantec CloudSOC CASB service to add Symantec DLP detection to cloud application data monitored by the CASB service.
- **"Data Loss Prevention Cloud Detection Service for API Detection"** is a cloud-based service and can be used with a Custom Integration (defined below). Customers may license a REST API of the DLP Cloud Detection Service from Broadcom for purposes of adding DLP functionality to Customer's internally used application or service ("Custom Integration"), which DLP functionality can be invoked from such internally used application or service to perform DLP detection on data sent to the Service.
- **"Data Loss Prevention Cloud Detection Service for Cloud SWG"** is a cloud-based service and is used in conjunction with the Symantec Cloud Secure Web Gateway (Cloud SWG) to add Symantec DLP detection to outbound web traffic monitoring by the cloud-proxy. (Note: A separate subscription to Cloud SWG is required.)
- **"Data Loss Prevention Cloud Prevent for Microsoft Office 365 Exchange"** is a cloud-based service that provides Symantec DLP detection to email traffic of Microsoft Office 365 Exchange Online.
- **"Data Loss Prevention Cloud Detection Service for Office 365 Email and Gmail Standalone"** is a cloud-based service that provides Symantec DLP detection to outbound email traffic by any of the following supported third-party enterprise email service providers: Microsoft Office 365 Exchange Online, Microsoft Exchange Server, or Google G Suite Gmail.

DLP Cloud (CloudSOC CASB, CDS)

Saas Listing

Features by Service Option

	Audit	SaaS Securelet	IaaS Securlet	Posture Management	Gateway	DLP CASB	DLP Web	DLP Email	ATP	DLP API
DLP Cloud	✓	✓	✓	✓	✓	✓	✓	✓		
CloudSOC CASB Audit	✓									
CloudSOC CASB for IaaS	✓		✓	✓						
CloudSOC CASB for SaaS	✓	✓		✓						
CloudSOC CASB Gateway	✓				✓					
Data Loss Prevention Cloud Detection Service for CASB						✓				
Data Loss Prevention Cloud Detection Service for Cloud SWG							✓			
Data Loss Prevention Cloud Prevent for Microsoft Office 365 Exchange								✓		
Data Loss Prevention Cloud Detection Service for Office 365 Email and Gmail Standalone								✓		
Data Loss Prevention Cloud Detection Service for API Detection										✓
CloudSOC CASB Advanced Threat Protection									✓	

Service Features

- Customer can access the Service through a self-service online portal ("Portal", "CloudSOC"). Customer may configure and manage the Service, access reports, and view data and statistics, through the Portal, as well as manage DLP policies, remediating incidents, when available as part of the Service.
- "**Enforce Server**" is an administration console that is a centralized, web-based interface for the Data Loss Prevention Cloud Detection and Cloud DLP services for authoring policies, remediating incidents, and managing the system. Customer can configure and manage the Service, access reports, and view data and statistics, through the Enforce Server administration console.
- The Service is managed on a twenty-four (24) hours/day by seven (7) days/week basis and is monitored for hardware availability, service capacity and network resource utilization. The Service is regularly monitored for service level compliance and adjustments are made as needed.
- The Service is intended to enable Customer to implement a valid and enforceable computer use policy, or its equivalent.

Service Software Components

- The Service includes software components dependent on the licensed service component:
    - Symantec DLP Enforce Server - This software is required for DLP policy administration and incident management if a customer wants to manage DLP from on-premises
    - Synchronization virtual appliance - This software is required to import users, groups information and/or collect, compress and/or tokenize proxy or firewall logs before transferring to CloudSOC Audit for processing

DLP Cloud (CloudSOC CASB, CDS)

Saas Listing

- Traffic Steering Agent - This software can be deployed on endpoints to connect to the Service
- Software that can be used to create file outputs required for DLP Indexes (i.e. EDM, IDM)
- Images (i.e. docker) and/or scripts (i.e. shell, terraform) that can be used for respective service components to configure the integration

2: Customer Responsibilities

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

- Setup Enablement: Customer must provide information required for Broadcom to begin providing the Service.
- Adequate Customer Personnel: Customer must provide adequate personnel to assist Broadcom in delivery of the Service.
- Renewal Credentials: If applicable, Customer must apply renewal credential(s) provided in the applicable Transaction Document within its account administration, to continue to receive the Service, or to maintain account information and Customer data which is available during the subscription Term.
- Customer Configurations vs. Default Settings: Customer must configure the features of the Service through the Portal, if applicable, or default settings will apply. In some cases, default settings do not exist and no Service will be provided until Customer chooses a setting. Configuration and use of the Service(s) are entirely in Customer's control, therefore, Broadcom is not liable for Customer's use of the Service, nor liable for any civil or criminal liability that may be incurred by Customer as a result of the operation of the Service.
- For Cloud DLP and Data Loss Prevention Cloud services:
  - On-premise installation and use of administration console: Customer can install and use an on-premise version of the Enforce Server administration console if not using the cloud based management console.
  - Customer Configurations: Customer must configure features of the Service through the Enforce Server administration console or the cloud-based management console.
- Connecting Applications: If the service is used by Customer with their Integrating Service, the Integrating Service must comply with the API specification for the REST API when calling the Service.
- Customer developing Custom Integrations must specify the name of the internally used application or service to be integrated with the Service using a Custom Integration request form provided by Broadcom. Broadcom reserves the right in its sole discretion to decline any proposed Custom Integration with the Service, and shall notify Customer promptly upon such determination.

3: Entitlement and Subscription Information

Charge Metrics

The Service is available under one of the following Meters as specified in the Transaction Document:

- "**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.
- **"Usage"** means GB/day usage for processed data for IaaS applications as set forth in the description for CloudSOC CASB for IaaS and GB overall processed data for DLP API as set forth in the description for DLP Cloud Detection Service for API Detection in the SaaS Listing
- Each subscription purchased for **"DLP Cloud"**
  - May only be used by a single User in conjunction with any Cloud Applications available for SaaS Securlet and Gatelet.
  - The monthly upper limit for SaaS, IaaS Securlet, and DLP API across the entire organization is 1GB per licensed "**DLP Cloud"** User. For every additional increment of 1GB scanned per month, the Customer will incur an additional licensed User charge. The initial onboard SaaS and IaaS scan is not factored into the 1GB per user limit.
- Each subscription purchased for **"CloudSOC CASB Securlet for SaaS"** may only be used by a single User in conjunction with a single Cloud Application. As used herein and for purposes of determining the applicable User count for the Service, "Cloud Application" means the target application or hosted service scanned by an Integrating Service. Where Symantec CloudSOC CASB service is the Integrating Service,

Saas Listing

each Securlet for a target application constitutes one Cloud Application and all Gatelets taken together constitute one Cloud Application.

- In the case of AWS S3 as the Integrating Service, AWS S3 constitutes one Cloud Application whereby Customer must purchase a maximum User count of "**CloudSOC CASB Securlet for IaaS**" Service subscriptions (i.e., a Service subscription for each individual person within Customer's organization) for such Cloud Application.
- Each subscription purchased for "**CloudSOC CASB Gateway**" a "User" may be calculated by Broadcom at its sole discretion through counting the number of devices or measuring equivalent activity/expected data consumption (8 Gigabytes per month) for an individual person across features where usage by individuals cannot be determined.
- In case **"CloudSOC CASB Audit"** is unable to uniquely identify a user in the proxy or firewall logs, client IP addresses are used for user identification.
- Where Symantec Cloud Secure Web Gateway (Cloud SWG) is the Integrating Service, Cloud SWG constitutes one Cloud Application that requires a **Data Loss Prevention Detection Service For Cloud SWG** subscription for each User licensed to Cloud SWG otherwise as a stand-alone service.

4: Customer Assistance and Support

Customer Assistance

Broadcom 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 Broadcom is providing Support to Customer, Support is included as part of the Service as specified below. If 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 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

Broadcom 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, Broadcom 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. Broadcom 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 Broadcom 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, Broadcom will provide fourteen (14) calendar days' notification. Broadcom may perform minor updates or routine maintenance to the Management Console with no prior notification as these activities do not result in Service disruption.

DLP Cloud (CloudSOC CASB, CDS)

Saas Listing

5: Additional Terms

- Broadcom may modify the Online Services 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 Online Services during the subscription Term.
- Excessive Consumption. If Broadcom determines that Customer's aggregate activity on the Service imposes an unreasonable load *(Customer's average per User usage is greater than the average per User usage generated by 95% of inline Users of the Service on a monthly basis)* on bandwidth, infrastructure, or otherwise, Broadcom may impose controls to keep the usage below excessive levels. Upon receiving notification (e.g., email) of excessive (vs. expected) usage, Customer agrees to remediate their usage within ten (10) days, or to work with its reseller to enter into a separate fee agreement for the remainder of the subscription Term. If the parties are not able to establish a resolution within ten (10) days after the initial notification, then Broadcom may institute controls on the Service or terminate the Service and this Agreement, without liability. In addition, if Broadcom determines that the excessive usage may present a risk to the Service, Broadcom may implement technical and business measures to bring usage into compliance.
- User/Usage Count. In the event that Customer exceeds its licensed Users or Usage amount (as measured in Broadcom's reporting system or as otherwise calculated by Broadcom), Customer agrees to promptly pay the amounts invoiced for the excess usage and/or submit a new order for the excess use. In addition, the parties agree to meet in good faith to determine the number of new User/Usage amount subscriptions required by Customer for the remainder of the subscription Term.
- Retention of data in the Portal is limited to a maximum of three (3) full calendar months for use with the Service. During the first week of each calendar month, one (1) calendar month of older data will be summarized for Audit and archived for other services and made available for download for one (1) calendar year after the date that the data was archived or to the date of the service expiration, whichever comes first.
- Customer User in CSPM can assess up to five hundred (500) Resources during the subscription period, each additional five hundred (500) Resources or fraction thereof assessed will be counted as an additional User for subscription purposes. For example, if a User assesses seven hundred fifty (750) Resources during the month, the count for that User will be two (2).
- Customer can create up to twenty (20) unique log data sources from CloudSOC Audit app.
- A CloudSOC CASB Audit entitlement provides access to CloudSOC CASB Audit AppFeed that allows cloud application discovery and controls from EdgeSWG or Cloud SWG.
- Any templates supplied by Broadcom are for use solely as a guide to enable Customer to create its own customized policies and other templates.
- If supported, API (as part of Cloud DLP or the standalone CloudSOC CASB for IaaS and CloudSOC CASB for SaaS) connectivity and scanning content within cloud applications is limited to all documents and last thirty (30) days of messages, posts, emails and attachments.
- Default content object size of maximum thirty megabytes (30MB) compressed and uncompressed can be ingested for scanning.
- The following conditions apply to Data Loss Prevention Cloud Detection Service for Office 365 Email and Gmail Standalone:
    - The Service is only available to a Customer who has its own email domain name and has the ability to configure the DNS for that domain name.
    - Customer may choose to route emails scanned by the Service to Symantec Email Security.cloud, Microsoft Office 365 Exchange Online, or Google Workspace (Gmail) for delivery to recipients. Customer that chooses to route emails scanned by the Service to Symantec Email Security.cloud must have a concurrent subscription to the Symantec Email Security.cloud Safeguard service in order for CA to deliver the Service. Customer that chooses to route emails scanned by the Service to Microsoft Office 365 Exchange Online or Google Workspace (Gmail) for delivery to recipients must have a concurrent subscription to the Microsoft Office 365 Exchange Online or Google Workspace (Gmail), maintain a valid certificate provided by Broadcom for the Service, and designate the Broadcom-provided certificate as trusted by Customer's Microsoft Office 365 Exchange Online service or Google Workspace (Gmail). Customer, and not Broadcom, is solely responsible for any failure of the Service to function due to lack of valid certificate unless Broadcom fails to provide such certificate.
    - Emails, per User per calendar month = ten thousand (10,000)
    - Default maximum email size = thirty megabytes (30MB). Customer can request any maximum email size up to fifty megabytes (50MB). Any emails that are received by the Service that exceed the specified limit will be scanned for the first fifty megabytes (50MB) of a received email against detection policy configured by Customer. If the first fifty megabytes (50MB) of a received

email violates the policy, automated remediation actions will be applied to the entire email (including portions of the email beyond the 50MB threshold). Otherwise, if the first 50MB of a received email does not violate any policy, such email will be passed along to either Symantec Email Security.cloud, Microsoft O365 Exchange Online, or Google Workspace (Gmail) without application of any automated remediation action based on routing configurations chosen by Customer.

- Customer must route their outbound email through the Service using the routing information provided by Broadcom.
- Customer must ensure that all domains (including sub-domains) requiring the Service are provisioned. Customer accepts that Service features may not function correctly, and email delivery may be unavailable for domains that are not provisioned.
- In the event that continued provision of the Service to Customer would compromise the security of the Service, including, but not limited to, hacking attempts, denial of Service attacks, mail bombs or other malicious activities either directed at or originating from Customer's domains, Customer agrees that Broadcom may temporarily suspend Service to Customer. In such an event, Broadcom will promptly inform Customer and will work with Customer to resolve such issues. Broadcom will reinstate the Service upon removal of the security threat.
- Should the Service be suspended for any reason whatsoever, the Service will not be applied to Customer's emails, and emails will not be routed through Broadcom's Infrastructure. Customer is responsible for redirecting their email during suspension and confirming that all configurations are accurate if the Service is reinstated.
- Should a Service be terminated for any reason whatsoever, Customer's account will be deleted, and Customer will not have access to the Service.
- Customer will not allow its systems to: (i) act as an Open Relay or Open Proxy or (ii) send Spam. Broadcom reserves the right at any time to review Customer's compliance with this restriction. For the avoidance of doubt, any breach of this restriction will constitute a material breach of the Agreement and Broadcom reserves the right to suspend all or part of the Service immediately and until the breach is remedied or terminate the Agreement with respect to the affected Service.
- If at any time (i) Customer's email systems are blacklisted, or (ii) Customer causes the Broadcom systems to become blacklisted due to the sending of Spam, or (iii) Customer fails to meet any of the obligations set out in this SaaS Listing, Broadcom shall inform Customer and reserves the right at its sole discretion to immediately withhold provision of, suspend or terminate all or part of the Service.

- "**DLP Innovation Labs**" is an early access/beta feature available to customers who are using "**DLP Cloud**" (in particular SaaS Securlet with DLP for CASB features). Customer's enablement of DLP Innovation Labs allows Customer access to certain prototype features. Prototype features may contain bugs, errors and/or other issues. These prototypes are provided "AS IS, WITH NO WARRANTIES." Broadcom does not guarantee the availability of these prototypes, and any outages or downtime of the prototypes will not count towards service credits pursuant to the Service Level Agreement in Exhibit A. There is no guarantee, representation, or obligation that the prototypes will ever be made generally available, and the prototypes may be added to or deprecated from DLP Innovation Labs at Broadcom's discretion, notwithstanding any established Broadcom deprecation strategy. Technical Support is not provided as part of Data Loss Prevention Innovation Labs or in connection with its prototypes.
- You may not publish the results of any benchmark tests run on the Software without Symantec's prior written permission.
- Customer setup that is unused (in example but not limited to, not being connected to a management, not configured or used) for more than 90 days will be subject to reset so that the entitlements can be redeployed by the customer.
- Customer setup that is insufficient or produces a risk to the SaaS platform, Broadcom will take commercially reasonable efforts to get in contact with Customer, but reserves the right to deactivate service components that produces a risk to the SaaS platform.
- The Service incorporates generative artificial intelligence (AI) technology to implement certain features. Features that use AI are typically identified in the Service interface. AI-generated output may contain errors and generate unexpected results. Customer should carefully review output before use. Customer should not use the AI technology in this Service to generate content that is illegal, harmful, misleading, or that violates third-party rights or privacy. Broadcom makes no representations and provides no warranties about the completeness, reliability, or accuracy of AI-generated output. For more information on Broadcom's use of AI, Customer may contact Technical Support.

6: Definitions

"**Administrator**" means Customer's designated personnel to manage the Service on behalf of Customer. Administrators may have the ability to manage all or part of a Service as designated by Customer.

DLP Cloud (CloudSOC CASB, CDS)

Saas Listing

For the purposes of this Service, the definition of **"Network Data"** includes Cloud Application Data.

"Cloud Application Data" means cloud application data that Broadcom may receive, store, and/or process to configure and provide the Service, and/or to provide any included support for the Service, including but not limited to time of transaction, User IP address, username, URL, URL category, status (success or error), file type, filter result (allowed or denied), virus ID, files, records, Customer selected account names and activity types, and other metadata (e.g. browser software used), and any other network traffic (and data related thereto) sent to or received from Customer through use of the Service, in detail and/or in an aggregated form.

"Email" means any inbound or outbound SMTP message passing through the Service.

"IaaS" means Infrastructure-as-a-Service, a third party service component that Customer uses independently and wants to apply some of the named Services of this document to.

"Open Proxy" means a proxy server configured to allow unknown or unauthorized third parties to access, store, or forward DNS, web pages or other data for the Service.

"Posture Management" means the process of monitoring for security risks in the *configuration* of your SaaS and IaaS applications and environments, ensuring that they adhere to industry benchmarks and best-practices.

"SaaS" means Software-as-a-Service, a third party service component that Customer uses independently and wants to apply some of the named Services of this document to.

"Open Relay" means an Email server configured to receive Email from an unknown or unauthorized third party and forward the Email to one or more recipients that are not users of the Email system to which that Email server is connected. Open Relay may also be referred to as "Spam relay" or "public relay."

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

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

DLP Cloud (CloudSOC CASB, CDS)

Saas Listing

Exhibit-A

Service Level Agreement(s)

1.0 GENERAL

These Service Level Agreements ("SLA(s)") apply to the Service that is the subject matter of this SaaS Listing only. If Broadcom 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 Broadcom's sole and exclusive liability for breach of the SLA.

2.0 SERVICE LEVEL AGREEMENT(S)

a. **Availability.** Availability is the amount of time that the Service is operational in minutes, expressed as a percentage per calendar month, excluding Excused Outages. Availability SLAs may exist for i) Inline (Data Plane) Service, and ii) Non-Inline (Control Plane) Service, separately:

- **Inline Service Availability** means access to the core features of the Service that impact the data in transit to and from Customer to the Internet. CASB Gateway, DLP Cloud Detection Service with CloudSOC (CASB) (if using Gatelet), DLP Cloud Detection Service with Cloud SWG, DLP Cloud Service for Email, and DLP Cloud Detection Service for API Detection that includes content inspection and enforcement of policies (i.e. blocking or modifications) are Inline Services that are the subject of the Inline SLA

Inline Service Availability	**≥99.9%**

- **Non-inline Service Availability** is access to the controls that govern the features of the Service 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 this Service include: Reporting, CASB Audit, Posture Management, Setting policies, Incident remediation, Advanced Threat Protection and DLP Cloud Detection Service and DLP Cloud Detection Service with CloudSOC (CASB) (if using Securlet).

Non-Inline Service Availability	**≥99.5%**

b. Other service levels:

- **CloudSOC CASB Gateway**: Average latency for transactions passing through the CloudSOC CASB Gateway service is based on end-user performance and will not exceed one (1) second or twice the Direct Response Time (as defined below). The CloudSOC CASB Gateway average latency is assessed on the difference between: (a) The completion time for a cloud application transaction when its traffic is sent to a cloud service via an CloudSOC CASB Gateway; and (b) the completion time for an identical cloud application transaction from the same end-point device and location when its traffic is sent directly to the cloud service, without using an CloudSOC CASB Gateway ("Direct Response Time"). Average latency is determined by the monthly average among samples taken by Broadcom in a given month. Average Latency excludes file transfer activities requiring content inspection and/or encryption.

Latency SLA for Gateway	**1 second or twice the Direct Response Time**

- **CloudSOC Audit**: The average latency for processed data to be available in CloudSOC Audit will be no later than six (6) hours after periodic uncorrupted data batch in formats supported by Broadcom is completely streamed/uploaded by the end device. Average latency is determined by the monthly average among samples taken by Broadcom in a given month. Maximum daily streaming exceeding one day's worth of logs and re-/processing of data post Service reactivation will be excluded from average latency calculations.

Latency SLA for Audit	**≤6 hours**

- **CloudSOC CASB Securlet for SaaS and IaaS.** The average latency to process an event and associated data within the CloudSOC CASB monitored SaaS or IaaS application will take no more than six (6) hours after the occurrence of that event. Average latency is determined by the monthly average among samples taken by Broadcom in a given month. Initial processing of events and associated data triggered by the activation or re-activation of a Securlet, rescanning and addition or migration of new users and their data to the application, is excluded from average latency calculations. Latency introduced by (i) the SaaS or IaaS application, either due to delayed availability of events and associated data from their API or due to throttling of API calls made by CloudSOC , or (ii) in any way attributable to third party SaaS or IaaS providers, is excluded from average latency calculations.

Latency SLA for Securlet	**≤6 hours**

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.

Broadcom 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 Broadcom Service, even if within the same account.
- Are the only remedy available, even if Customer is not renewing for a subsequent Tterm. 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 Broadcom 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 Broadcom 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 Broadcom's system records. Should any claim be disputed, Broadcom 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

DLP Cloud (CloudSOC CASB, CDS)

Saas Listing

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 or Customer's late payment post service suspension results in backlog processing.
- Third party, non-Broadcom branded products or services resold with the Service.
- Hardware, software or other data center equipment or services not in the control of Broadcom 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 Broadcom.
- 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.
- 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 Broadcom (or at the direction of or as approved by Broadcom
- Defects in the Service due to abuse or use other than in accordance with Broadcom's published Documentation unless caused by Broadcom or its agents.
- Customer-requested hardware or software upgrades, moves, facility upgrades, etc.

END OF EXHIBIT A