Offer Description – Product
Cisco Secure Access

This Offer Description is part of the General Terms or similar terms existing between You and Cisco (e.g., the End User License Agreement) (the "**Agreement**"). Capitalized terms, unless defined in this document, have the meaning in the Agreement. Any references to the Supplemental End User License Agreement or SEULA mean Offer Description.

1. Summary

Cisco Secure Access (the "**Product**") is a cloud security service edge solution designed to allow users to securely connect to the Internet and private applications from any device located anywhere. The Product includes, depending upon package purchased, zero trust network access ("**ZTNA**"), VPN-as-a-Service, Secure Web Gateway ("**SWG**"), Cloud Access Security Broker ("**CASB**"), Firewall-as-a-Service, Data Loss Prevention ("**DLP**"), DNS security, remote browser isolation ("**RBI"**), Secure Malware Analytics (sandbox) on suspicious files, and Talos threat intelligence. The Product is designed with common administrative controls, data structures, and policy management designed to ease interoperability with other synergistic components such as SD-WAN.

Cisco Secure Access Essentials includes file inspection through Cisco Secure Malware Analytics for up to 500 files. **Cisco Secure Access Advantage** includes file inspection through Cisco Secure Malware Analytics for unlimited files and three (3) Secure Malware Analytics cloud portal user licenses. A Cisco Secure Access subscription also includes the right to access and use the ThousandEyes Web Platform and embedded Endpoint Agent for digital experience monitoring ("**ThousandEyes Users Embedded**").

In addition, a Cisco Secure Access subscription includes the right to access and use Security Cloud Control and Security Cloud Sign-On Control. Security Cloud Control provides You a unified experience in deploying and managing Your subscription. Security Cloud Sign-on is used as a single sign-on (SSO) across products and operates as the native Identity Provider (IdP) or delegated IdP across selected Cisco products.

For more information on Cisco Secure Access, see the Secure Access Site and the Secure Access Datasheet.

2. Support and Other Services

Support. You will be required to select Enhanced or Premium Support when You purchase the Product. Support for the Product does not include an initial meeting to understand Customer's desired outcomes to define an IT and Infosec adoption plan.

3. Performance Standards

Cisco will use commercially reasonable efforts to deliver the Core Services to meet or exceed 99.999% Availability in accordance with the Secure Access Service Level Agreement ("**SLA**") available from Your Cisco account representative or Cisco authorized partner. Capitalized terms in this section will have the meaning in the SLA.

4. Data Protection

Privacy Data Sheets. The Cisco Secure Access, Cisco Secure Malware Analytics, Cisco ThousandEyes, Cisco Security Cloud Control, and Cisco Security Cloud Sign-On Privacy Data Sheets describe the personal data that Cisco collects and processes as part of the delivery of the Product.

5. Special Terms

5.1 **Covered Users**. You must purchase one Covered User license for each individual protected by the applicable Cisco Secure Access package purchased by You. The quantity of Covered Users You purchase for a Secure Internet Access ("**SIA**") package may be a different quantity than the quantity You purchase for a Secure Private Access ("**SPA**") package.

5.2 **Subscription Start Date; Claim Code**. When Your order for Cisco Secure Access is received and accepted by Cisco, You will receive a subscription claim code via email. The claim code enables You to (i) set up your subscription in Security Cloud Control, and (ii) commencing on the requested start date ("**RSD"**) in the order, provision and access the Product. Your subscription will commence on the RSD whether You elect to provision the Product on the RSD or delay provisioning of the Product.

5.3 **Usage and Range Limits**.

(A) Cisco Secure Access subscriptions are subject to a total aggregate data transfer limit per month across all packages purchased for such Product equal to the quantity of purchased Covered Users multiplied by 20 GB. The data transfer limit applies to the amount of data going through the Product (inbound and outbound) whether resulting from Covered Users and/or non-user devices protected by the Product. If You purchase an SIA and an SPA package with different quantities, the Covered User quantity used to calculate the total data transfer limit is the higher of the two Covered User quantities purchased.

For example:

- If You purchase an SIA subscription for 1000 Covered Users and do not purchase an SPA package, Your subscription is subject to a monthly data transfer limit of 20,000 GB.
- If You purchase SIA for 5000 Covered Users and SPA for 3000 Covered Users, Your monthly data transfer limit across SPA and SIA is 5000 x 20GB = 100,000 GB.

Cisco will work with You in good faith to try and resolve any excess usage. If You cannot sufficiently reduce Your excess usage, You may be required to purchase additional Covered Users to obtain the additional required data transfer capacity.

(B) RBI is subject to a total aggregate data transfer limit per Covered User per day of 2 GB. If a Covered User exceeds this limit, RBI may bypass the domain having the highest data transfer impact, typically a streaming site such as YouTube, Netflix, TikTok and other video streaming services. If a domain is bypassed, it means that the user's access to the domain is not blocked but that domain will not pass through the RBI service. RBI is also subject to a limit of 25 active concurrent sessions. If a user tries to open a 26th session, the user will receive a message indicating that they will need to close an existing session in order to start a new session.

(C) The Product is subject to other technical usage and range limitations as set forth in the Cisco Secure Access Documentation.

5.4 **Remote Browser Isolation.** RBI is included only with an SIA subscription; it is not included with an SPA subscription. You are authorized to use RBI only for the Covered Users under the SIA subscription.

5.5 **Acceptable Use.** You will not (and will not allow any third party to): (i) establish regular and frequent automated queries to an external site, such as port scanning of a third-party entity not in Your control, or use offensive security technologies against a third party through the use of the Product (because these actions could reasonably be viewed by the external site as a denial of service attack or a violation of the third party's terms and could lead to Cisco being blacklisted); (ii) use the Product to access websites or blocked services in violation of applicable law and/or regulation; or (iii) use the Product for the purpose of intentionally masking Your identity in connection with the commission of unlawful activities or to otherwise avoid legal process. If Cisco receives a third-party request for information, demand letter, or other similar inquiry in connection with Your use of the Product relating to alleged unlawful activity on Your network, Cisco may disclose Your name to such third party as necessary to comply with legal process or meet national security requirements; protect the rights, property, or safety of Cisco, its business partners, You, or others; or as otherwise required by applicable law.

5.6 **Unlicensed Feature Usage.** You may have access to certain features that are not included in the Cisco Secure Access subscription package You purchase. If You utilize features not covered by Your subscription, You are required to upgrade Your subscription prospectively at the next anniversary date of the subscription. Prior to the upgrade, You may use such unlicensed features for evaluation purposes for up to 100 Covered Users. Cisco's support and Service Level Agreement obligations do not apply to unlicensed features. Cisco reserves the right to terminate access and/or usage rights to unlicensed features at any time with or without notice. Unlicensed feature usage does not apply to ThousandEyes Users Embedded.

5.7 **Feature Previews**. Cisco may offer You the ability to participate in a preview of new Cisco Secure Access features before they are generally available ("Preview"). Your usage of such features during a Preview is subject to the terms in the Agreement specifically related to beta and evaluation software use, except as follows: (a) You may use Cisco Secure Access features in production during a Preview; and (b) participation in a Preview does not alter Your obligation to pay any fees owed to Your Approved Source during the Use Term.

5.8 **Data Centers**. Data center(s) located in mainland China, when and if available, require a separate subscription purchased directly through the applicable service operator in China.

5.9 **Cisco Secure Client.** Your subscription to Cisco Secure Access includes the right to use Cisco Secure Client. If you wish to use Cisco Secure Client with other products, You must purchase a separate Cisco Secure Client license.

5.10 **ThousandEyes.** Your subscription to Cisco Secure Access includes the ThousandEyes Embedded Endpoint Agent license. See Section 5.1 of the ThousandEyes Offer Description for information regarding features and restrictions associated with the Embedded Endpoint Agent license. If You deploy ThousandEyes Users Embedded, Your ThousandEyes account will be provisioned by default to ThousandEyes' datacenter in the United States. You may contact support@thousandeyes.com to make a request to change your data center location to ThousandEyes' EU data center. Additional information about ThousandEyes' use, storage, and processing of Your data is available in the ThousandEyes Privacy Data Sheet.

5.11 **Competitive Testing**. You will not publish or disclose to any third party any Product performance information or analysis (including without limitation the results of benchmark or competitive testing) except with Cisco's prior written consent.

5.12 **Cisco Secure Access Reserved IP.** If You are entitled in writing to a Cisco Secure Access Reserved IP subscription, please see the Reserved IP Supplemental Terms for additional terms and conditions applicable to Your subscription. Your Approved Source reserves the right to charge a fee, and You agree to pay, for Your Cisco Secure Access Reserved IP subscription.

5.13 **Disclaimers. While Cisco has used commercially reasonable efforts to create effective security technologies, due to the continual development of new techniques for intruding upon and attacking files,**

networks, and endpoints, Cisco does not represent or warrant that the product will guarantee absolute security or that it will protect all your files, network, or endpoints from all malware, viruses, or third-party malicious attacks.

5.14 **Definitions**

"**Covered User**" means each Internet-connected employee, subcontractor, and other authorized individual covered (i.e., protected) by Your deployment of the Product.