Offer Description – Product

Cisco Secure User Protection Suite

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

The Cisco User Protection Suite (the "**Product**") includes Cloud Services that protect against attack vectors that target users while they are connected to the resources they need, anytime and anywhere. This provides users with safe access to websites, software-as-a-service (SaaS) applications, and private applications.

Your subscription entitles You to access and use (a) the Cloud Services included in the applicable tier in the table below and (b) Security Cloud Control and Security Cloud Sign-On. Security Cloud Control unifies the experience of deploying and managing Your Cloud Service. Security Cloud Sign-on is a single sign-on (SSO) across products, operating as the native Identity Provider (IdP) or delegated IdP across selected Cisco products.

Suite Tier	Cloud Services Included in Suite Tier*
User Protection Suite Advanced	**Secure Endpoint Advantage** *(Includes file inspection for 200 files; 1 SMA cloud portal user if <250 Covered Users; 3 SMA cloud portal users if ≥ 250 Covered Users)*
	Cisco Secure Access Advantage *(Includes file inspection for unlimited files; 3 SMA cloud portal users)*
	Duo Premier
	Email Threat Defense *(Includes file inspection for unlimited files; no SMA cloud portal users)*
User Protection Suite Essentials	**Cisco Secure Access Essentials** *(Includes file inspection for 500 files; no SMA cloud portal users)*
	Duo Premier
	Email Threat Defense *(Includes file inspection for unlimited files; no SMA cloud portal users)*

*The User Protection Suite also includes file inspection through Secure Malware Analytics ("**SMA**") and use of the SMA cloud portal at the quantities listed in the table above.

2. Support

You will be required to select Enhanced or Premium Support when You purchase the Product.

3. Performance Standards

The Cloud Services included in this Product are subject to any Service Level Objective ("**SLO**") or Service Level Agreement ("**SLA**") described in the individual Offer Descriptions. If a Cloud Service SLA or SLO includes a termination right, that termination right is not applicable to the Product subscription.

4. Data Protection

The Cisco Privacy Data Sheets for the following Cloud Services (available at Cisco's Trust Portal) describe the personal data that Cisco collects and processes as part of the delivery of the Product: Cisco Secure Access, Cisco Secure Malware Analytics, Duo, Cisco Email Threat Defense, Cisco Secure Endpoint, and Cisco Security Cloud Control and Cisco Security Cloud Sign-On. When You purchase Secure Endpoint through the User Protection Suite, Your Secure Endpoint data center region is North America.

5. Special Terms

5.1 **Additional Offer Terms.** Each Cloud Service included in the Product is subject to its individual Offer Description. The following Offer Descriptions apply (depending on Suite Tier): Cisco Secure Access, Secure Endpoint, Duo, Email Threat Defense, and Secure Malware Analytics. This Offer Description takes precedence over the individual Offer Descriptions in the event of any conflict.

5.2 **Billing Meter – Covered Users**. Cisco licenses Product subscriptions based on the number of Covered Users – individual Cloud Service billing meters do not apply. In addition, when You purchase the Product, You must purchase a subscription for each Covered User even if that Covered User is not protected by all the individual Cloud Services included in the Product.

5.3 **Subscription Start Date; Claim Code**. When Cisco receives and accepts Your order, You will receive a 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 Cloud Services included in the purchased tier. Your subscription will commence on the RSD whether You elect to provision Cloud Service(s) on the RSD or delay provisioning of one or more of the Cloud Services.

5.4 **Mid-Term Changes**. During the Product subscription term, You can upgrade Your subscription to a higher tier by placing an upgrade order through Your Approved Source, but You cannot downgrade Your subscription to a lower tier.

5.5 **Secure Endpoint Usage**. Suite packaging assumes that You have, on average, two (2) endpoints per Covered User for purposes of Cisco Secure Endpoint. You understand that if Your average endpoint to Covered User ratio is significantly higher than two to one (2:1) on a recurring basis, Cisco will work with You to assess utilization/consumption and may require You to purchase additional Covered User licenses.

5.6 **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 Umbrella (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 a Cloud Service to access websites or blocked services in violation of applicable law and/or regulation; or (iii) use a Cloud Service 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 a Cloud Service 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.

5.7 **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 cloud services will guarantee absolute security or that it will protect all your files, network, or endpoints from all malware, viruses, or third-party malicious attacks.**

5.8 **Definitions**

"**Covered User**" means an Internet-connected employee, subcontractor, and any other authorized individual covered (i.e., protected) by Your deployment of any of the included Cloud Services.