Offer Description: Secure Endpoint

This Offer Description (the **"Offer Description"**) describes Cisco Secure Endpoint (formerly AMP for Endpoints and Clarity) ("**Secure Endpoint"** or, the **"Cloud Service"**). Your subscription is governed by this Offer Description and the Cisco End User License Agreement located at www.cisco.com/go/eula (the "EULA") (or similar terms existing between you and Cisco) (the **"Agreement"**). If capitalized terms are not defined in this Offer Description, then they have the meaning given to them in the Agreement or order(s).

1. Description

1.1. Secure Endpoint

Secure Endpoint is a cloud-based advanced malware analysis and protection solution that allows You to conduct metadata File analysis to detect malware and cyber threats. Cryptographic hashes of Files are collected and submitted for File reputation analysis, and a disposition is made as to whether the File is good, bad or unknown. If a disposition is unable to be made after analysis of the hash of a File, then You may have the option (depending on the license(s) purchased) to submit the File to Cisco Secure Malware Analytics for further sandboxing analysis up to Your licensed daily submission limit. Secure Endpoint is available as Secure Endpoint Essentials, Advantage or Premier.

Secure Endpoint for iOS is a cloud-based security solution that provides visibility and protection against advanced malicious threats on iOS devices. Application and network connectivity details (i.e. domains, IPs, ports, URLs) from Your iOS devices are identified and transmitted to a Cisco-managed cloud server where Your information is correlated against other Secure Endpoint connector details. Using Your correlated data, Secure Endpoint for iOS and the Secure Endpoint Console (the "**Console**") provide You with visibility on non-standard behavior to highlight those iOS devices that may be experiencing suspicious activity. The Console and reporting capabilities can be used to investigate suspicious activity across Your Endpoints.

Secure Endpoint Virtual Private Cloud offers You a private cloud instance that remains on Your premises (the "Private Cloud") and may be configured to pull updates from the Cisco managed public cloud server ("**Public Cloud**"). You can choose to run Secure Endpoint Private Cloud in either "proxy" or "air gap" mode. If You choose "proxy" mode, Your cryptographic hashes of Files will be transmitted from your Private Cloud to the Public Cloud for file reputation analysis. If You choose "air gap" mode, no data is transmitted to the Public Cloud; Your data will remain in the Private Cloud.

1.2. Cognitive Intelligence

Your Secure Endpoint subscription also includes access to Cognitive Intelligence ,a cloud-based threat detection and analytics feature that leverages (i) web proxy logs, (ii) event log data, and (iii) netflow from Secure Network Analytics and/or Secure Cloud Analytics (which may include enhanced netflow if Customer enables Cisco Encrypted Traffic Analytics) Cognitive Intelligence's implementation of machine-learning based Static File Analysis capability is also available to Secure Endpoint customers via an integration with Secure Malware Analytics. Cognitive Intelligence is available through Your subscription or license to (a) Secure Endpoint, (b) Secure Endpoint on Secure Web Appliance, (c) Secure Network Analytics and (d) Secure Cloud Analytics.

1.3. Orbital

Your Secure Endpoint Advantage subscription includes access to Cisco Orbital, an advanced search capability in Secure Endpoint Advantage and Secure Endpoint Premier that provides over a hundred pre-canned and customizable queries, allowing You to quickly run complex queries on any or all Endpoints.

1.4. Cisco SecureX

Your Secure Endpoint subscription includes access to Cisco SecureX, Cisco's integrated security platform that aggregates threat intelligence, unifies visibility across various Cisco and third party security products, enables automated workflows, and more. Cisco SecureX Threat Hunting, available in Secure Endpoint Premier, leverages the expertise of both Talos and the Cisco Research and Efficacy Team to help identify threats found within the customer environment. The terms associated with Your use of SecureX can be found here.

2. Supplemental Terms and Conditions

2.1. License and Usage Rights Restrictions.

a. **Secure Endpoint.** The Cloud Services described in this Offer Description are licensed based on the quantity of Endpoints.

b. **Cognitive Intelligence.** To use the Cognitive Intelligence feature, You are required to submit web proxy logs from a supported platform and/or netflow from Secure Network Analytics or Secure Cloud Analytics (if You are licensed to use Secure Network Analytics and/or Secure Cloud Analytics). Cognitive Intelligence may use this data to perform analysis to identify the presence of malware on Your systems and relate communications to and from such systems affected to and from suspected malicious machines or sites. If You do not want to provide Your web proxy logs and/or netflow and related information to the Cognitive Intelligence cloud to have the ability to analyze for active malware inside Your environment, then You must not enable the Cognitive Intelligence feature.

2.2. Use of Cisco's Cloud Service.

CISCO DOES NOT REPRESENT OR WARRANT THAT THE CLOUD SERVICES WILL GUARANTEE ABSOLUTE SECURITY 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 PROTECT ALL YOUR FILES, NETWORK, OR ENDPOINTS FROM ALL MALWARE, VIRUSES OR THIRD-PARTY MALICIOUS ATTACKS.

3. Data Protection

The Cisco Secure Endpoint, Cognitive Intelligence and SecureX Privacy Data Sheet(s) (available here) describes the Personal Data that Cisco collects and processes as part of the delivery of the Cloud Services. For further information on how Cisco processes, uses and protects all categories of data, please visit Cisco's Security and Trust Center.

4. Support & Maintenance

We will provide You with Support and Maintenance for the Cisco Technology based on the tier of services purchased as follows: https://www.cisco.com/c/dam/en_us/about/doing_business/docs/cisco-software-support-service.pdf.

5. Definitions

"**Endpoint**" means any device capable of processing data and that can access a network, including but not limited to personal computers, mobile devices, iOS devices and network computer workstations.

"**Files**" mean those types of files identified in the applicable Documentation, such as an executable, Portable Document Format (PDF), Microsoft Office Documents (MS Word, MS Excel, MS PowerPoint), and those files in a ZIP (.ZIP) file.