Offer Description: AMP, Threat Grid, and Cisco Security Connector for iOS

This Offer Description (the "Offer Description") describes Cisco Advanced Malware Protection ("AMP"), Cisco Threat Grid ("Threat Grid") and Cisco Security Connector for iOS (the "Cloud Service(s)"). Your subscription is governed by this Offer Description and the Cisco Universal Cloud Agreement located at www.cisco.com/go/uca (or similar terms existing between you and Cisco) (the "Agreement"). Capitalized terms used in this Offer Description and/or the Order not otherwise defined herein have the meaning given to them in the Agreement.

Table of Contents

1. Offer Description

1.1. AMP

AMP 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 transmitted to a Cisco-managed cloud server where File reputation analysis is performed, 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 have the option (depending on the license(s) purchased) to submit the File to Threat Grid (described below) for further sandboxing analysis up to Your licensed daily submission limit. After the File analysis is completed, AMP will act on the disposition (e.g. by deleting the File and putting it into quarantine if it is determined to be malicious). AMP is available in various forms including AMP for Endpoints Essentials, AMP for Endpoints Advantage, AMP for Email, AMP for Web, AMP Private Cloud, AMP on NGIPS (AMP for Networks), AMP on NGFW, and AMP for Meraki MX.

1.2. Threat Grid

Threat Grid is a cloud-based malware analysis and threat intelligence sandbox solution to which You can submit malware samples for additional analysis. Threat Grid analyzes each File in order to record its behavior and determine whether it is malicious. Threat Grid will search and correlate data elements of a

single malware sample against millions of samples collected and sourced from around the world to give You a global view of malware attacks and its association.

1.3. Cisco Security Connector for iOS

Cisco Security Connector 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 AMP connector details. Using Your correlated data, Cisco Security Connector for iOS and the AMP for Endpoints 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.

1.4. Cisco Threat Response

Your AMP and Threat Grid subscriptions include access to Cisco Threat Response. Cisco Threat Response is a cloud-based aggregator of threat intelligence collected or generated by Cisco security products as well as other third-party security products. Cisco Threat Response allows You to pull together critical threat intelligence and add context from Your organization, so You know which systems and devices are infected.

1.5. Cognitive Intelligence

Your AMP and Threat Grid subscriptions also include access to Cognitive Intelligence. Cognitive Intelligence is a cloud-based threat detection and analytics feature that leverages (1) web proxy logs from a Cisco web gateway solution such as Cisco Web Security Appliance ("WSA") or Cloud Web Security ("CWS") or third party web proxies and (2) netflow from Cisco Stealthwatch Enterprise (which may include enhanced netflow if Customer enables Cisco Encrypted Traffic Analytics ("ETA")). The web proxy logs and/or netflow help identify malware present within a customer's environment, and allow a customer to research related active malicious behaviors. Cognitive Intelligence's implementation of machine-learning based Static File Analysis capability is also available to Cisco AMP customers via an integration with Cisco Threat Grid. Cognitive Intelligence is available through Your subscription or license to (a) AMP for Endpoints, (b) AMP on WSA, and (c) Stealthwatch Enterprise.

1.6. Cisco Orbital Advanced Search

Your AMP for Endpoints Advantage subscription includes access to Cisco Orbital Advanced Search ("Orbital"). Orbital is a new advanced search capability in Cisco AMP for Endpoints Advantage that is designed to make security investigation and threat hunting simple by providing over a hundred pre-canned and customizable queries, allowing You to quickly run complex queries on any or all endpoints. Orbital enables You to gain deeper visibility on any endpoint at any given time by taking a snapshot of its current state.

2. Supplemental Terms and Conditions

2.1. AMP Private Cloud

AMP 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 AMP 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.

2.2. Cognitive Intelligence - Proxy Log and NetFlow Submissions

To use the Cognitive Intelligence feature, You are required to submit web proxy logs from a supported platform and/or netflow from Cisco Stealthwatch (if you are licensed to use Stealthwatch Enterprise). Such logs may contain identifiable data such as user name, machine name, IP address, and browsing information. 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 Cognitive Intelligence.

2.3. Disclaimers

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. CISCO DOES NOT MAKE ANY REPRESENTATIONS OR WARRANTIES REGARDING ANY THIRD PARTY SYSTEM OR SERVICE TO WHICH A CLOUD SERVICE INTEGRATES OR TO ANY ONGOING INTEGRATION SUPPORT. INTEGRATIONS MADE ACCESSIBLE TO YOU THAT ARE NOT A GENERALLY AVAILABLE PRODUCT INCLUDED ON YOUR ORDER ARE PROVIDED ON AN "AS IS" BASIS.

3. Data Protection

Cisco's data protection obligations are set forth in the Agreement. Additionally, the AMP, Threat Grid Cisco Threat Response, Cognitive Intelligence and Orbital Advanced Search Privacy Data Sheet(s) (available here) supplement the Cisco Privacy Statement and describe the Personal Data that Cisco collects and processes as part of the delivery of the Cloud Services.

4. Support & Maintenance

The Cloud Services include online support and phone support. Cisco will respond as set forth in the table below and may require information from you to resolve service issues. You agree to provide the information requested and understand that a delay in providing the information to Cisco may delay resolution and response time.

Online Support allows access for support and troubleshooting via online tools, email and web case submission only. No telephone access is provided. Case severity or escalation guidelines are not applicable. Cisco will respond to a submitted case no later than the next business day during standard business hours.

Phone Support provides Cisco Technical Assistance Center (TAC) access 24 hours per day, 7 days per week to assist by telephone, or web case submission and online tools with use and troubleshooting issues. Cisco will respond within one (1) hour for Severity 1 and 2 calls received. For Severity 3 and 4 calls, Cisco will respond no later than the next business day.

You will also have access to Cisco.com, which provides helpful technical and general information about Cisco products, as well as access to Cisco's on-line knowledge base and forums. Please note that access restrictions identified by Cisco from time to time may apply.

The below table outlines Cisco's response objectives based on case severity. Cisco may adjust assigned case severity to align with the Severity definitions below.

Software Support Service	Technical Support Coverage	Response Time Objective for Case Severity 1 or 2	Response Time Objective for Case Severity 3 or 4
Basic with Phone Support	24x7 via Phone & Web	Response within 1 hour	Response within next Business Day

Basic with Online Support	Web	Response to all cases within next Business Day during Standard Business Hours

The following definitions apply to this Section.

Response time means the time between case submission in the case management system to support engineer contact.

Severity 1 means the Cloud Service is unavailable or down or there is a critical impact to a significant impact to Case Submitter's business operation. Case Submitter and Cisco both will commit full-time resources to resolve the situation.

Severity 2 means the Cloud Service is degraded or significant aspects of Case Submitter's business operation are negatively impacted by unacceptable software performance. Case Submitter and Cisco both will commit full-time resources during Standard Business Hours to resolve the situation.

Severity 3 means the Cloud Service is impaired, although most business operations remain functional. Case Submitter and Cisco both are willing to commit resources during Standard Business Hours to resolve the situation.

Severity 4 means minor intermittent functionality or performance issue, or information is required on the Cloud Service. There is little or no impact to Case Submitter's business operation. Case Submitter and Cisco both are willing to provide resources during Standard Business Hours to provide assistance or information as requested.

Business Day means the generally accepted days of operation per week within the relevant region where the Cloud Services will be performed, excluding local holidays as observed by Cisco.

Local Time means Central European Time for support provided in Europe, Middle East and Africa, Australia's Eastern Standard Time for support provided in Australia, Japan's Standard Time for support provided in Japan and Pacific Standard Time for support provided in all otherlocations.

Standard Business Hours means 8am to 5pm Local Time at the location of the respective Cisco TAC, on Business Days, for the handling of TAC calls.

Definition

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 computerworkstations.

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 file (.ZIP).

Non-Confidential File(s) mean a File submitted to Threat Grid that You do not elect to maintain as "private" and thus can be viewed by other users of Threat Grid.

Private File(s) mean a File submitted to Threat Grid that You elect to maintain as "private" so that it can't be viewed by other users of Threat Grid.