cisco SECURE

Offer Description: Cisco Security Management Platform PaaS Service

This Offer Description (the "**Offer Description**") describes the Cisco Security Management Platform PaaS Service (the "**Cloud Service**"). Your subscription to the Cloud Service is governed by this Offer Description and the Cisco End User License Agreement located at www.cisco.com/go/eula (or similar terms existing between You and Cisco) (the "**Agreement**"). Capitalized terms used in this Offer Description and not otherwise defined herein have the meaning given to them in theAgreement.

Note: Cisco security products are being renamed under our Cisco Secure brand. Cisco Security Management Platform will be renamed Cisco Secure Management for Service Providers. New product names will be updated in phases. You can find a map of our current and new names, and additional information regarding the Cisco Secure naming updates at https://www.cisco.com/c/en/us/products/security/index.html.

1. Description

The SMP PaaS Service is an optional add-on Cloud Service to a Cisco Security Management Platform ("SMP") on-premise software subscription. SMP is a virtualized management and orchestration platform intended for use with various Integrated Products (defined in the Supplemental End User License Agreement for SMP). Cloud Service includes: (i) hosting of SMP and software included with the applicable Integrated Products, (ii) 24X7 monitoring of the hosted environment, and (iii) provisioning of the applicable software releases. Cloud Service is intended as an interim solution to allow customers to accelerate deployment prior to their on-premise installation and deployment of SMP.

2. Supplemental Terms and Conditions

Disclaimers

CISCO DOES NOT REPRESENT OR WARRANT THAT THE CLOUD SERVICE 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 SERVICE OR THE SOFTWARE AND/OR CLOUD SERVICES IT INTEGRATES WITH 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. Service Level Objective

Cisco shall use commercially reasonable efforts to maintain availability of 99.95% of each calendar month for Cloud Service. Availability will be calculated by dividing the total number of minutes of Uptime (defined below) during the applicable calendar month by the total number of minutes in such month, minus minutes of Outages (defined below) occurring due to scheduled maintenance and attributable to Third Party Actions (defined below), and multiplying that amount by 100. The formula for this calculation is as follows:

Availability = (X ☐Y) x 100

X= Total # of minutes of Uptime during calendar month

Y= (Total # of minutes in such calendar month) - (Total # of minutes of Outages from scheduled maintenance and Third-Party Actions)

For the purposes of this calculation, (i) An "Outage" means that SMP is unreachable, or that SMP is not processing or delivering any e-mails, when Your Internet connection is working correctly, (ii) "Uptime" means the number of minutes where there were no Outages, excluding Outages for scheduled maintenance and Third Party Actions, and (iii) "Third Party Action" means any action beyond Cisco's reasonable control including, without limitation, the performance of Internet networks controlled by other companies or traffic exchange points that are controlled by other companies, labor strikes or shortages, riots, insurrection, fires, flood, storm, explosions, acts of God, war, terrorism, governmental action, labor conditions, earthquakes and material shortages. If a dispute arises about whether or not an Outage occurred, Cisco shall make a determination in good faith based on its system logs, monitoring reports and configuration records, and as between customer records and Cisco records, Cisco records shall control. Cisco shall not be responsible for any Outages arising out

of Third-Party Actions or for interruptions or shut down of Cloud Service due to circumstances reasonably believed by Cisco to be a significant threat to the normal operation of the PaaS Service, a Cisco facility, or access to or integrity of data (e.g. hacker or virus attack). In the event of such interruption or shutdown, Cisco will return Cloud Service to normal operation as soon as reasonably possible.

4. Data Protection

The Cisco Security Management Platform with Email Security Privacy Data Sheet (available here) describes the Personal Data that Cisco collects and processes as part of the delivery of the Cloud Services. For further details on how Cisco processes, uses and protects all categories of data, please visit Cisco's Security and Trust Center.

5. Support and Maintenance

The Cloud Service includes 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 for submitted cases based on case severity. Cisco may adjust assigned case severity to align with the Severity definitions herein.

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 Phone Support	24x7 via Phone & Web	Response within 1 hour	Response within next Business Day

The following definitions apply to this Section 4:

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

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

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

Severity 3 means the Cloud Service or Software is impaired, although most business operations remain functional. You 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 or Software. There is little or no impact to Your business operation. You 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 support 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 other locations.

Standard Business Hours means 8am to 5pm Local Time (relative to the location of the Cisco TAC) on Business Days.