MLSA Product Terms
Stealthwatch Cloud

Additional Product Terms

Service Provider's use of the Stealthwatch Cloud Service under the MSLA Program Terms is subject to these Product Terms. In the event of a conflict, the order of precedence will be (a) these Stealthwatch Cloud Product Terms; and (b) the Program Terms. Capitalized terms used but not defined in these Product Terms are defined in the Program Terms or the Master Agreement. Cloud Service is Stealthwatch Cloud for the purposes of these Product Terms.

Cloud Services Description

Stealthwatch Cloud technology provides cloud-based dynamic behavioral modeling of entities on the network; it provides Service Provider with the ability to gain real-time situational awareness of users, IP connected assets and traffic on the network, in the data center or the cloud. Its cloud-native, machine learning techniques help Service Provider to identify insider and external threats through modeling algorithms that detect changes in behavior. Stealthwatch Cloud is available as Private Network Monitoring and Public Cloud Monitoring. Please consult the Stealthwatch Cloud Documentation for further information on its technical specifications, configuration requirements, features and functionalities.

1. Supplemental Terms

1.1. Scheduled Maintenance. In all cases where scheduled maintenance for Stealthwatch Cloud will be performed, Cisco will make reasonable attempts to ensure that scheduled maintenance that affects the availability of Stealthwatch Cloud for more than 30 minutes is performed between 12:00 AM and 5:00 AM Central Time, Monday through Friday (excluding U.S. holidays), or between 12:00 PM and 5:00 AM Central Time on Saturday, Sunday and U.S. holidays, or on Tuesday between 14:00 and 15:00 UTC.

1.2. Cisco Threat Response. Stealthwatch Cloud includes 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 Service Provider to pull together critical threat intelligence and add context from its customers' organizations so Service Provider knows which systems and devices are infected. Please see the Cisco Threat Response Privacy Data Sheet regarding any Personal Data processed by Cisco Threat Response.

1.3. Warranties. In addition to the warranties and disclaimers set forth in the Master Agreement, Cisco warrants that it will provide the Cloud Services in a manner consistent with general industry standards reasonably applicable to the provision thereof. 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 SERVICE PROVIDER FILES, NETWORKS, 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 SERVICE PROVIDER THAT ARE NOT A GENERALLY AVAILABLE PRODUCT INCLUDED ON SERVICE PROVIDER'S ORDER ARE PROVIDED ON AN "AS IS" BASIS.

2. Program Requirements

2.1. Training. Prior to using the MSLA Software to provide the Software Services, any of Service Provider's employees or Authorized Third Parties engaged in providing the Software Services must complete, at Service Provider's cost (as applicable), any and all required Cloud Service training courses required by Cisco. In addition, Service Provider must comply with Section 2.2 of the Program Terms related to its Authorized Third Parties.

2.2. Cisco Support Obligations. Service Provider and its Authorized Third Parties (as applicable) are the sole entities authorized to engage Cisco for support services related to the Software Services. Cisco's support obligations to Service Provider or its Authorized Third Parties are solely set forth in the Program Terms. In no event shall Cisco have any obligation to respond to any support requests initiated by an End User.

2.3. Security. When providing the Software Services, Service Provider and/or its Authorized Users shall implement and maintain appropriate industry standard technical and organizational measures to protect End User data against accidental or unlawful use or destruction, accidental loss, alteration, and unauthorized disclosure of, or access to, any End User data.

2.4. Ordering. Service Provider will follow the ordering process as instructed by Cisco. Cisco may change or update its ordering process at any time, upon prior written notice to Service Provider.

2.5. Reporting. Notwithstanding Section 4.3 of the MSLA, Cisco reserves the right at any time, in its sole discretion and upon at least six months' notice to Service Provider, to migrate Service Provider to a Cisco-billed invoicing model whereby Cisco will collect Service Provider's End User usage data directly from the Stealthwatch Cloud instance(s) and invoice Service Provider based on the data collected. If Service Provider does not agree to the updated invoicing model, then Cisco may terminate these Stealthwatch Cloud Product Terms upon 30 days written notice to Service Provider without any liability to Service Provider.

2.6. Stealthwatch Cloud Premium Program Monthly Minimum Requirements.

2.6.1. The Service Provider will select either the Basic Program or the Premium Program option for the applicable Stealthwatch Cloud Service purchased. Each Premium Program has its own monthly minimum commitment (each a "**Monthly Minimum**") as follows:

Private Network Monitoring ("**PNM**"): 10,000 Endpoints
Public Cloud Monitoring ("**PCM**"): 5,000 Effective Megaflows

If Service Provider selects both the PNM and the PCM Premium Program, then both Monthly Minimums will apply to Service Provider. The Program Effective Date will be the date of last signature on Schedule 1 (License Fee Program Selection). Service Provider may request to upgrade from the Basic Program to the Premium Program at any time during the MSLA by submitting a request to: **ask_mssp_swc@cisco.com**. Cisco will promptly respond to such requests. If Cisco accepts such request, Cisco will provide email approval. The applicable Monthly Minimum(s) will be effective on the date that Cisco emails the approval to Service Provider. In no event shall Service Provider be permitted to downgrade from the Premium Program to the Basic Program**.**

2.6.2. Commencing upon the Program Effective Date, if Service Provider selects one or both Premium Programs, Service Provider shall have a six-month ramp-up period (**"Ramp-Up Period"**) per Premium Program to meet the applicable Monthly Minimum. If Service Provider does not meet the applicable Monthly Minimum by the last day of the Ramp-Up Period, Cisco, in its sole discretion, may:

a. Terminate this Stealthwatch Cloud Product Terms attachment, without liability to Service Provider, upon 30 days written notice to Service Provider, provided however, that Service Provider has an opportunity to cure such failure to meet the applicable Monthly Minimum within 30 days of receipt of such written notice from Cisco; or

b. Invoice Service Provider each month for the remainder of the term for the applicable Monthly Minimum(s) until such time that Service Provider exceeds such applicable Monthly Minimum(s). Upon exceeding the applicable Monthly Minimum(s), Cisco will invoice Service Provider for the License Fees tied to the applicable volume tier met by Service Provider during that month. In no event will Cisco invoice Service Provider for an amount less than the applicable Monthly Minimum(s) set forth in this Section.

2.6.3. Service Provider may terminate its use of Stealthwatch Cloud upon 90 days prior written notice to Cisco.

3. Definitions

"Effective Megaflows" means the lines of flow log data generated by the Stealthwatch Cloud monitored environment and processed by Cisco.

"**Endpoint(s)**" means any device capable of processing data and that can access a network, ***including but not limited to devices in a data center such as servers***, and/or individual devices such as personal computers, mobile devices, iOS devices and network computer workstations.

Schedule 1 – Stealthwatch Cloud License Fee Program Selection

Service Provider hereby selects the following License Fee Program(s):

Stealthwatch Cloud Public Cloud Monitoring:

Basic License Fee Program _____

Premium License Fee Program _____

Stealthwatch Cloud Private Network Monitoring:

Basic License Fee Program _____

Premium License Fee Program _____

Agreed to by:

Cisco	**Service Provider**
Signature:_____	Signature:_____
Name (Printed):_____	Name(Printed): _____
Title: _____	Title:_____
Date:_____	Date:_____