MSLA Product Terms
Cisco XDR

Product Terms

Service Provider's use of Cisco XDR includes these Product Terms, which take precedence over anything in the Program Terms that conflicts. Capitalized terms used but not defined in these Product Terms are defined in the Program Terms. For purposes of this document, "Cloud Service" means Cisco XDR.

Cloud Service Description

Cisco XDR enables teams to detect, prioritize, and respond to advanced threats. It is a cloud-based solution that streamlines security operations by presenting prioritized incidents that are correlated across telemetry ingested from Cisco and multiple 3rd party sources. The process of event correlation involves continuous data analytics across current and historical data. Embedded automation, orchestration, and guided remediation recommendations help mitigate threats, reduce response times, and increase coverage without additional staff. With a data-driven approach, SOC teams can prioritize impactful events and strengthen overall security while enhancing resilience.

1. Supplemental Terms

1.1 **Scope of Use/Limitations.** Service Provider will use the Cloud Service as a Cisco-branded Cloud Service to provide Software Services to End Users and will not alter or modify the Cloud Service except at Cisco's request or with Cisco's authorization. Service Provider will not use a single Cisco XDR tenant for multiple End Users.

XDR Automate enables End Users to program automated workflows. End Users are responsible for ensuring that workflows are programmed in accordance with the Technical Documentation supplied by Cisco. Cisco recommends all workflows be tested in a non-production environment prior to implementation in production.

1.2 **Warranties.** In addition to the warranties and disclaimers set forth in the Program Terms, Cisco warrants that it will provide the Cloud Service in a manner consistent with general industry standards reasonably applicable to the provision thereof. CISCO DOES NOT REPRESENT OR WARRANT THAT THE PRODUCT 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 PRODUCT 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 PRODUCT 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.

1.3 **License Fee Calculation.** Cisco XDR is licensed based on the quantity of Covered Users, with options to increase data ingestion limits and/or data retention period.

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 **Security.** When providing the Software Services to End Users, Service Provider and/or its Authorized Third Parties will 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 or access.

2.3 **Data Protection.** The Cisco XDR Privacy Data Sheet (available at https://trustportal.cisco.com/c/r/ctp/trust-portal.html?doctype=Privacy%20Data%20Sheet) describes the Personal Data that Cisco collects and processes as part of delivering the Cloud Service.

3. Support

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 Solution Support document located at https://www.cisco.com/c/dam/en_us/about/doing_business/legal/service_descriptions/docs/solution-support-smart-total-care.pdf. In no event shall Cisco have any obligation to respond to any support requests initiated by an End User.

4. Definitions

"**Covered Use**r" means the employees, contractors and other individuals who have online and/or cloud activity (e.g. internet, email, use of cloud applications) protected through use of this Cloud Service.