Offer Description: Cisco Secure Cloud Insights

This Offer Description (the “Offer Description”) describes Cisco Secure Cloud Insights (the “Cloud Service(s)). Your subscription 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/or the order and not otherwise defined herein have the meaning given to them in the Agreement.

1. Description

1.1. Cisco Secure Cloud Insights

Cisco Secure Cloud Insights is a cloud-native platform brought to market in collaboration with JupiterOne® which provides deep insights into an enterprise’s universe of ephemeral and evolving cyber assets. Cisco Secure Cloud Insights monitors multi-cloud deployments, both public and private cloud, as well as hybrid environments with a mix of on-premises infrastructure. Cisco Secure Cloud Insights is API-driven and relies on agentless integrations to ingest data needed to map configuration and interactions between entities in an organization’s digital environment. This rich and connected dataset can be investigated using 550 odd pre-built queries and can be presented in an easy-to-consume visual graph. Users can also easily create their own queries in J1QL, JupiterOne’s proprietary query language. These queries can then be turned into security alerts, augment existing compliance benchmarks such as SOC 2, or be grouped to author custom standards.

Cisco Secure Cloud Insights capabilities address Your organization’s Cloud Security Posture Management (CSPM) needs. With Secure Cloud Insights, organizations can limit exposure resulting from an ever-increasing attack landscape by identifying security and compliance gaps, automating workflows, and maintaining continuous monitoring of Your organization’s security posture. Knowledge of relationships and interactions also fast-tracks investigations and aids threat containment and response. Finally, outbound integrations allow alerts to be routed to ticketing systems, email aliases, and messaging applications or publication/queuing services. Alerts can also be shared with other services via custom APIs, including other Cisco offers such as Secure Cloud Analytics and SecureX. Secure Clouds Insights is a CSPM tool and much more.

1.2. Cisco SecureX

Your Secure Cloud Insights subscription includes access to Cisco SecureX, Cisco’s integrated security platform that aggregates threat intelligence (through SecureX incident manager response or Cisco Threat Response), unifies visibility across various Cisco and third-party security products, enables automated workflows, and more. For more information on SecureX, please see the SecureX Offer Description.

2. Supplemental Terms and Conditions

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.

Data Protection
The Cisco Cisco Secure Cloud Insights and Cisco SecureX Privacy Data Sheets (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**

The Cloud Services include online 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.

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.

If you have access to Software with the Cloud Services, Cisco will provide (i) work-around solutions or patches to reported problems and (ii) major, minor and maintenance releases of the licensed Software version, which can be accessed on Cisco Software Central. You may be required to update to the latest Software release to correct a reported Software problem.

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.

<table>
<thead>
<tr>
<th>Software Support Service</th>
<th>Technical Support Coverage</th>
<th>Response Time Objective for Case Severity 1 or 2</th>
<th>Response Time Objective for Case Severity 3 or 4</th>
</tr>
</thead>
<tbody>
<tr>
<td>Basic with Phone Support</td>
<td>24x7 via Phone &amp; Web</td>
<td>Response within 1 hour</td>
<td>Response within next Business Day</td>
</tr>
<tr>
<td>Basic with Online Support</td>
<td>Web</td>
<td>Response to all cases within next Business Day during Standard Business Hours</td>
<td></td>
</tr>
</tbody>
</table>

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 other locations.

**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.

Your access to and use of the Cloud Services may be suspended for the duration of unanticipated or unscheduled downtime, including as a result of catastrophic events, external denial of service or other security breach, or operational incidents.