Offer Description: Crosswork Cloud

This Offer Description (the “Offer Description”) describes Cisco Crosswork Cloud (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 not otherwise defined herein have the meaning given to them in the Agreement.

1. Description
   The Cloud Service may contain one or more of the following cloud services depending on the license You have purchased:

   • Crosswork Trust Insights
   • Crosswork Network Insights – External Route Analysis
   • Crosswork Network Insights – Traffic Analysis

1.1. Crosswork Trust Insights
   Cisco Crosswork Trust Insights (“Trust Insights”) is a hosted application service that reports on integrity of enrolled network devices and provides forensics for assured inventory. It empowers network and security operations with visibility to track trust posture and changes in hardware and software of the device. It helps maintain authoritative proof and evidence to reinforce system integrity for audits and compliance. In addition, it simplifies forensic analysis with extensive and verifiable history of inventory changes.

   Trust Insights utilizes Cisco Crosswork Data Gateway as a proxy deployed in your network to collect data from enrolled network devices using a cryptographically secured channel.

   Trust Insights is offered in two tiers:
   • Essentials: Supports visualization and reporting of trust and inventory data along with visibility into hardware and software changes needed for audit and compliance; and/or
   • Advanced Function Packs: Extends Essentials enhanced trust analysis, change notifications, collaboration integration and longer data retention for forensic analysis.

1.2. Crosswork Network Insights – External Route Analysis
   Cisco Crosswork Network Insights – External Route Analysis (“External Route Analysis”) is a hosted application service that provides network routing analysis, visualization, and alerting on actionable network events. External Route Analysis collects near real-time routing information from active peering routers and maintains their Border Gateway Protocol (BGP) event history, aggregates Network Routing Data and Public Data Sources (defined below), and identifies the source of anomalies based on a consensus of the routing databases.

1.3. Crosswork Network Insights – Traffic Analysis
   Cisco Crosswork Network Insights – Traffic Analysis (“Traffic Analysis”) is a hosted application service that provides network traffic analysis, visualization, and alerting on actionable network events. Traffic Analysis collects near real-time traffic information from active routers and maintains their IP route prefix traffic history, aggregates Autonomous System Number (ASN), Device and Interface Traffic Data and identifies optimization opportunities.
2. Supplemental Terms and Conditions

External Route Analysis does not provide raw, unprocessed Network Routing Data to You. Cisco makes no warranty as to the accuracy, completeness, or the availability of the Network Routing Data obtained from the Public Data Sources or Your peering routers. If You reduce the number of Your peering routers, the quality analytics of Crosswork Network Insights and richness of Network Routing Data will be similarly reduced, and Cisco is not liable for such reduction.

Traffic Analysis does not store raw, unprocessed Network Traffic Flow Data from Your routers. Cisco aggregates Network Traffic Flow Data based on Network Routing Data obtained from Your Routers. Cisco makes no warranty as to the accuracy, completeness, or the availability of the Network Traffic Flow Data obtained from the Your network routers. If You reduce or stop the amount of Traffic Flow Data from Your routers, the quality analytics of Crosswork Network Insights and richness of Network Traffic Flow Data will be similarly reduced, and Cisco is not liable for such reduction.

Cisco does not resell, repackage, distribute, publish, or otherwise make publicly available Network Traffic Flow Data from Your routers to any other party.

Event Notification as part of both External Route Analysis and Traffic Analysis provides You network event notifications and alarms via the software dashboard, SMS, and email. However, Cisco cannot guarantee that each instance of an alarm or event notification will be delivered to You via SMS or email because Cisco does not control third party systems, equipment, or connectivity services.

2.4. Crosswork Network Insights External Route Analysis: Internet Number Resources; Crosswork Network Insights Traffic Analysis: Internet Number Resources
Internet Number Resources as part of both External Route Analysis and Traffic Route Analysis gives You access to the contact information of internet number registrants. You may only use such contact information (a) to ensure the uniqueness of internet number resource usage; or (b) in Your normal course of business in providing network and internet services. If You wish to use such contact information for other purposes, You must obtain permission from the applicable Regional Internet Registry entity.

You will not resell, repackage, distribute, publish, or otherwise make publicly available such contact information. Additionally, You may not use such contact information in any manner that (a) violates or infringes the rights of others, including privacy rights; or (b) is unlawful, threatening, abusive, defamatory, obscene, or otherwise objectionable.

2.5. Data Storage
As a default, the Cloud Services leverage AWS Americas data centers. If You wish to use AWS data centers located elsewhere, You will need to pay an additional fee.

2.6. Additional Features
The Cloud Services may contain additional programs, features and functionality outside the scope of Your Entitlement. If you wish to use out of scope items, You will need to purchase separate licenses.

3. Data Protection
The Cisco Crosswork Cloud 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.

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.

For Software, 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 Service 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.

Definitions

“Device” means, as applicable, a single, physical or virtual router, switch, or network function in Your network.

“Interface Traffic Data” means Simple Network Management Protocol (SNMP) measurements of interface utilization from a Device.

“Network Routing Data” means a collection of one or more IP address blocks that provide availability and path information.

“Network Traffic Flow Data” means a collection of aggregated traffic sum measurements of one or more IP address blocks that provide the usage and path information about the IP Address Block.

“Public Data Sources” means the data made publicly available on the websites hosted by Reseaux IP Europeans Network Coordination Center, the University of Oregon, any successor website to one or both of these websites, and any additional public website that hosts data substantially similar to these websites.