Offer Description

Cisco Tetration Software-as-a-Service (Tetration SaaS)

IMPORTANT: READ CAREFULLY

1. OVERVIEW

This Offer Description describes supplemental terms and conditions that will govern Your use of the Cisco Tetration SaaS and related Software and services, as indicated in the Order(s) for internal business purposes only.

The Cisco Universal Cloud Agreement ("Agreement") and the terms referenced herein govern Your use of Tetration SaaS and the Software provided for use with Tetration SaaS. A current copy of the Agreement is located at: https://www.cisco.com/c/en/us/products/universal-cloud-agreement.html. For more information regarding Cisco software terms see: http://www.cisco.com/c/en/us/about/legal/cloud-and-software.html.

If Tetration SaaS and Software provided for use with Tetration SaaS is compatible for use with other Cisco products or service offerings not referenced herein, such other products and/or offerings may have additional license terms that apply to Your use of such products and offerings. You are also responsible for complying with the terms for such other Cisco products and offerings, as applicable. The terms set forth herein apply to Tetration SaaS whether purchased for use on a standalone basis, or purchased for use with such other Cisco products or offerings.

Cisco reserves the right to change this Service Description at any time.

2. Description and Definitions

With Cisco Tetration SaaS, IT organizations can realize consistent workload protection by enabling whitelist-based segmentation, behavior baselining and analysis, and detecting common vulnerabilities allowing users to proactively quarantine affected servers. Through an open policy model, workloads are secured consistently across bare metal, virtual and containerized workloads on-premises and in the public cloud through a single pane of glass. With this holistic approach, Tetration significantly reduces the attack surface, minimizes lateral movement in case of security incidents, and more quickly identifies anomalies and suspicious behavior. The open policy can also be enforced across any vendor's infrastructure. Tetration SaaS is a Cloud service, fully managed and operated by Cisco. Tetration SaaS offer allows customers to take advantages of all the features supported by deploying a software sensor on workloads on-premises, private and public clouds; without having to procure any hardware on-premises or virtual instances in public clouds. With Tetration SaaS, customers can get flow telemetry data retention in accordance with the Tetration SaaS data sheet. Please consult Cisco Tetration Documentation for further information on its technical specifications, configuration requirements, features and functionalities. Capitalized terms not otherwise defined herein shall have the meanings defined in the Agreement.

Definitions:

- "Cisco Content" means any Cisco-provided content or data including, but not limited to, geographic and domain information, rules, signatures, threat intelligence or other threat data feeds, suspicious URLs and IP address data feeds.
- "Endpoint" means a computer, smartphone or other mobile device running Cisco AnyConnect Secure Mobility Client 4.x (or above) Software *and* the Cisco AnyConnect Network Visibility Module.
- "Telemetry Data" means information generated by instrumentation and system logs created through the use and operation of the Software.
- A "Workload" means a Server, Virtual Machine (or "VM") or other server equivalent.

A. Use Limitations: You may not deploy or use Tetration SaaS in a manner that (i) extends beyond the duration of the applicable subscription term, or (ii) without remittance of additional payments, or (iii) exceeds any use limitations or other metrics related to Your license (e.g. Workloads licensed) as set forth in this Offer Description, an Order, SKU or product identifier (PID), or Documentation for the Service. If Your use of Tetration SaaS requires or permits You to use any Cisco Content, then You (and Your agents acting on your behalf) may only use such Cisco Content for use with Tetration SaaS and with those third-party products or services offerings that Cisco has identified as being compatible. You agree not to extract Cisco Content from or use any Cisco Content separate from Tetration SaaS, or provide Cisco Content to a third party.

B. Data Security: Cisco will maintain administrative, physical and technical safeguards consistent with industry standards and the Documentation, which are designed to provide security, confidentiality and integrity of the Data used by Cisco.

C. APIs. Tetration APIs and Tetration Apps provide additional functionality that are subject to these additional terms, which you agree to if you make use of the Tetration APIs or Tetration Apps. Cisco hereby grants to you a worldwide, non-exclusive, non-transferable, non-sublicensable license to use and make calls to the Tetration APIs and Tetration Apps for the sole purpose of developing and implementing software applications that work, communicate, or interact with Your licensed Tetration products. You agree not to assert any of your intellectual property developed with use of and/or used with the Tetration APIs or Tetration Apps against Cisco or any of its affiliates, customers, resellers, distributors, or other licensees of the Tetration APIs and Tetration Apps for making, having made, using, selling, offering for sale, or importing: (i) any products or services implementing, interfacing with or operating in combination with the Tetration APIs or Tetration Apps; or (ii) any applications developed using the Tetration APIs or Tetration Apps. If You do not agree with the foregoing terms for Tetration APIs and Tetration Apps, do not make use of such functionality as you are not licensed to use the Tetration APIs or Tetration Apps.

D. Cisco Tetration Add-on Features. The Tetration Policy Enforcement feature is included and licensed (on a per Workload basis) with Tetration SaaS. Customers of Tetration SaaS may optionally license the Tetration Endpoint Visibility add-on feature for use with Tetration SaaS.

The Tetration Endpoint Visibility feature is an add-on capability that is licensed (on a per Endpoint basis) separately from, and in addition to, the Tetration base license. Your license to the Tetration Endpoint Visibility feature provides an integration of telemetry from Endpoints running the Cisco AnyConnect Network Visibility Module. Tetration Endpoint Visibility feature requires that you separately subscribe for the Cisco AnyConnect Network Visibility Module for each Endpoint providing telemetry to Tetration. Note, if no Endpoint quantity is specified for Tetration Endpoint Visibility in your order, Your license does not extend to Tetration Endpoint Visibility. Cisco AnyConnect Secure Mobility Client Apex License and the Cisco AnyConnect Network Visibility module must also be purchased in sufficient quantities to meet your needs. The Cisco AnyConnect Network Visibility Module is subject to separate terms and conditions, located here: https://www.cisco.com/c/en/us/about/legal/cloud-and-software/software-terms.html.

Cisco may offer additional add-on features in the future, which may be licensed separately from the current Tetration SaaS offering for an additional fee.

E. Smart Licensing. Cisco Smart Licensing will become mandatory for Use of Cisco Tetration in a future release. Once enabled, each license to Tetration will be subject to and conditioned upon You enabling and maintaining Smart Licensing for Tetration. Cisco Smart Licensing is described in the Smart Licensing terms available at: http://www.cisco.com/c/dam/en/us/products/collateral/smart-licensing-agreement.pdf.

F. Cisco Content. If Your use of Tetration requires or permits You to use any Cisco Content, then You (and Your agents acting on your behalf) may only use such Cisco Content for use with Tetration and with those third-party products

or services offerings that Cisco has identified as being compatible. You agree not to extract Cisco Content from or use any Cisco Content separate from Tetration, or provide Cisco Content to a third party.

G. Technical Support. The Tetration SaaS subscription service includes a basic level of support services. As part of that basic support, You have access to the Cisco TAC, as set forth below, to assist you by phone, email, or via the Web with your use, configuration, and troubleshooting of the Tetration SaaS service.

Cisco TAC: 800-553-2447.

https://www.cisco.com/c/en/us/support/web/tsd-cisco-worldwide-contacts.html

You will also have access to Cisco.com, which provides Customer with helpful technical and general information, 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 online tool is the tool located at: https://www.cisco.com/c/en/us/support/index.html

Tetration SaaS Support	
Severity and Response Time	**Hours of Operation**
Severity 1 (Urgent)	**1 Hour Response / 24x7 phone support**
Severity 2 (High)	**4 Hour Response / 24x5 phone support** (between Monday 9am – Friday 5pm PST)
Severity 3 (Normal)	**8 Business Hour Response / 8x5 phone support** (between Monday 9am – Friday 5pm PST)
Severity 4 (Low)	**12 Business Hour Response / 8x5 email & web support** (between Monday 9am – Friday 5pm PST)
Online Resources	**Included**
Documentation	Yes
FAQ	Yes
Support Portal	
Ticket Management (open & update support cases)	Yes
Forums	Yes
Knowledge Base (Searchable)	Yes
Notifications	Yes
Managing Third Party Solutions	No

Cisco Severity and Escalation Guidelines:

https://www.cisco.com/c/dam/en_us/about/doing_business/legal/service_descriptions/docs/Cisco_Severity_and_E

scalation_Guidelines.pdf

H. Scheduled Maintenance, Modifications and Unscheduled Downtime.

1. From time to time, Cisco performs scheduled maintenance to update the servers and software that are used to provide the Cisco Tetration Cloud Service. Cisco agrees to use reasonable efforts to provide You with prior notice of any scheduled maintenance in advance of any planned downtimes that would impact Your use of the Cloud Service. Notwithstanding the foregoing, You acknowledge that Cisco may, in certain situations, need to perform emergency maintenance of the Cloud Service without providing advance notice.
2. Cisco reserves the right to modify and update the features and functionality of the Cloud Services. Cisco will make good faith efforts to provide notice of any material modification or updates to the Cloud Services and will use commercially reasonable efforts to implement modifications or updates in a manner that minimizes the impact on your use of and the performance of the Cloud Services. Service will be impacted during upgrades and any planned or unplanned maintenance.
3. 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, or other operational incidents.