Offer Description – Product

AI Defense

This Offer Description is part of the General Terms or similar terms existing between You and Cisco (e.g., the End User License Agreement) (the "**Agreement**"). Capitalized terms, unless defined in this document, have the meaning in the Agreement. Any references to a Supplemental End User License Agreement or SEULA mean Offer Description.

1. Summary

AI Defense (the "**Product**") includes Software and/or Cloud Services to protect Your Artificial Intelligence (AI) Applications.

- AI Runtime helps safeguard production AI applications against adversarial attacks, sensitive data leaks, and harmful responses in real-time.
- AI Validation helps identify security and safety vulnerabilities in AI models so You can understand the risks and protect against them.
- AI Visibility discovers enterprise AI assets running in Your organization's public and virtual cloud environments.
- AI Access finds third-party and shadow AI Applications being used by employees across Your organization and protect against sensitive data loss, threats, and safety risks.

2. Support and Other Services

Your purchase of Cisco AI Defense includes Enhanced Support. Premium Support is an optional add-on. Cisco will provide You with support for the Product as described here.

3. Performance Standards

The AI Defense Service Level Objective ("**SLO**") applies to the Cloud Service version of the Product.

4. Data Protection

The Privacy Data Sheet for AI Defense (available at Cisco's Trust Portal) describes the Personal Data that Cisco collects and processes as part of delivering the Product.

5. Special Terms

5.1 **Meter and Usage**. The Product subscription price is based on the quantity of AI Applications. The Product features You are entitled to use are defined by the AI Defense subscription package purchased (e.g., Advantage, Validation Essentials, or Runtime Essentials) and described in the Documentation.

5.2 **AI Validation**. If You purchase an AI Defense subscription package with AI Validation, the Product uses attack prompts to test Your AI Application. Such attack prompts are considered Cisco Content. You may not use the Product's attack prompts and related reports to develop any products or models that compete with the Product. You may not use the Product's attack prompts to train any AI models.

5.3 **AI Visibility**. If You purchase a Product subscription package with AI Visibility, You will be entitled to use the Cisco Multicloud Defense Controller. For Advantage and Runtime Essential subscription packages, You will be entitled to Cisco Multicloud Defense Premier, specifically 3,504 Gateway Hours per AI Application per year. You understand that if You exceed Your entitled Gateway Hours, Cisco will work with You to assess utilization/consumption and may require You to purchase additional Gateway Hours. Cisco Multicloud Defense is subject to its individual Offer Description located at https://www.cisco.com/c/en/us/about/legal/cloud-and-software/software-terms.html.

5.4 **AI Runtime**. For AI Defense Runtime, the subscription package assumes you will use a total aggregate query limitation of 10 million per AI Application per year. In the event of continuous excessive usage, You and Cisco will work in good faith to try and resolve any excessive usage.

5.5 **AI Access**. AI Access is only available for use with Cisco Secure Access with the Secure Access Advantage Package.

5.6 **Subscription Start Date; Claim Code**. You will receive a subscription claim code via email at the requested start date (RSD). The claim code enables You to (i) set up Your subscription in Security Provisioning and Administration, and (ii) provision and access the Product. Your subscription will commence on the RSD whether You elect to provision the Product on the RSD or delay provisioning of the Product.

5.7 **Mid-Term Changes**. During the Product subscription term, You can upgrade Your subscription to a higher tier by placing an upgrade order through Your Approved Source, but You cannot downgrade Your subscription to a lower tier.

5.8 **Software Updates**. For hybrid deployments, Cisco reserves the right to automatically update the Product to the most recent version of the Software; however, You will have the option to schedule or defer Your automatic updates. You may delay updates provided that Your current Software version is still supported by Cisco. You understand and agree that delaying updates to the latest Software release may introduce security risks to Your environment and Cisco is not responsible for any security-related incidents that result from that delay.

5.9 **Competitive Testing**. You will not publish or disclose to any third party any Product performance information or analysis (e.g., the result of benchmark or competitive testing) except with Cisco's advance written permission.

5.10 **Disclaimer**

(A) While Cisco has used commercially reasonable efforts to create effective security and safety technologies, due to the continual development of new techniques for intruding upon and attacking AI Applications, Cisco does not represent or warrant that the Product will guarantee absolute safety and security or that it will protect Your AI Applications against all security attacks or threats.

(B) You are responsible for (i) configuring the Product (including selecting the desired guardrails) and updates as needed from time to time to align with Your AI governance framework and policies, (ii) determining what actions to take (if any), based on results or recommendations generated by the Product, and (iii) complying with all applicable laws related to Your use and development of AI.

(C) Attack prompts are intended to provide an assessment of vulnerabilities, including but not limited to security and safety, related to the configured guardrails. Depending on the guardrails You configure, attack prompts from AI Validation may include attack prompts that are offensive or not aligned with the views and values of Cisco.

5.11 Definitions

Term	Meaning
AI Application	Software system that utilizes Artificial Intelligence (AI) or machine learning model(s) as a core component in order to automate specific tasks or services.
Gateway Hour	See Cisco Multicloud Defense Offer Description.