Offer Description – Product

Cisco Security Cloud Control

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 the Supplemental End User License Agreement or SEULA mean Offer Description.

1. Summary

Cisco Security Cloud Control, formerly known as Cisco Defense Orchestrator[1], (the "**Product**") is a cloud-based, AI native security policy management Subscription Offer that allows You to manage multiple Cisco security products across multiple Cisco and cloud-native platforms for the following functionalities: policy change management, policy analysis and optimization, policy monitoring and reporting, orchestration of policy changes, log analytics, advanced threat detection, device and element management, and more. The Product also delivers Cisco's cloud-delivered Firewall Management Center ("**cdFMC**"), Cisco's AI Assistant, and AI Ops to streamline policy management, enhance security posture with best practice recommendations, and avoid deployment issues using predictive analysis and guided remediation. If additionally purchased, Your Product subscription can: (1) encompass Cisco Security Analytics and Logging's ("SAL") logging and troubleshooting (LT) capabilities[2]; and/or (2) include access to Cisco Multicloud Defense.

More information on the capabilities and features of the Product can be found in the Product documentation.

2. Support and Other Services

Your purchase of the Product includes Basic Cisco Software Support Services.

3. Performance Standards

Service Level Objective. The Service Level Objective ("**SLO**") attached to this Offer Description applies to the Product.

4. Data Protection

Privacy Data Sheet. The Cisco Security Cloud Control Privacy Data Sheet, and if applicable Cisco Multicloud Defense Privacy Data Sheet (if Cisco Multicloud Defense access purchased) and Cisco Security Analytics and Logging Privacy Data Sheet describes the Personal Data that Cisco collects and processes as part of delivering the Product.

[1] Effective November 11, 2024, Cisco Defense Orchestrator ("CDO") will be rebranded as Cisco Security Cloud Control ("SCC"). Some materials may refer to CDO and SCC interchangeably.

[2] SAL's LT functionality is the "Essentials" version of SAL which provides scalable central logging service with long-term retention options, with drill–down enabled through advanced viewer controls such as search, filer, download, etc. For more information on the SAL capabilities offered under SCC, see Cisco platform integration: Native integration to other key Cisco applications section located on: https://www.cisco.com/c/en/us/products/collateral/security/defense-orchestrator/datasheet-c78-736847.html#CiscoDefenseOrchestratorbenefits.

5. Special Terms

5.1 **Credentials.** You are responsible for all activities related to Your account using Your credentials (e.g., purchases, sharing of data with third parties, etc.) and will protect their confidentiality. You must immediately report any disclosed or stolen credentials to Cisco or Your administrator (as appropriate).

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

5.3 **Disclaimers. While Cisco uses commercially reasonable efforts to create effective security technologies, Cisco does not represent or warrant that the Product will guarantee absolute security or that it will protect all of Your files, systems, network, or endpoints from all malware, malicious attacks or other threats.**

Service Level Objective
Cisco Security Cloud Control

This Service Level Objective ("**SLO**") applies to Security Cloud Control and cdFMC as set out in the applicable Offer Description. If capitalized terms are not defined in this SLO, then they have the same meaning as under the Offer Description.

1. Service Level

Cisco will use commercially reasonable efforts to deliver the Cloud Service so that the Core Services meet or exceed the performance standards described in the table below ("**Service Level**"). For clarity, this SLO is intended only to describe Cisco's target availability of the Core Services and does not constitute a warranty or obligation beyond using commercially reasonable efforts as stated above.

Service Level	During each Measurement Period, the target Availability of the Core Services will be: • Security Cloud Control (excluding cdFMC): 99.99% • cdFMC: 99.99%
Measurement Period	One calendar month

2. Response to missed Service Level

2.1 **Response**. If the Availability of the Core Services falls below the Service Level described in Section 1 for a given Measurement Period, Cisco will:

(A) Conduct an internal technical analysis of why the Service Level was not met; and

(B) When practicable, implement reasonable measures based on the technical analysis to help prevent any recurrence.

2.2 **Exclusions.** The following will not be considered Downtime for the purposes of this SLO:

(A) Scheduled, planned, or emergency maintenance ('emergency maintenance' is unscheduled maintenance where Cisco performs work to prevent or mitigate downtime or degradation of the Cloud Service or to prevent or mitigate a security incident);

(B) Your integrations of any software, hardware, or services not provided by Cisco or other integrations that have not been certified by Cisco;

(C) You are using a beta, evaluation, or trial version of the Product;

(D) Your failure to (1) use the Product or perform responsibilities in accordance with Your applicable agreement (e.g., General Terms or Enterprise Agreement), Offer Description, or the Documentation, or (2) apply updates or upgrades when made available; or

(E) Factors outside of Cisco's reasonable control, such as events described as Force Majeure in Your applicable agreement, Internet outages, pandemics, acts of government, cyber-attacks, industry-wide shortages, failures (including failures involving software, hardware, equipment or technology) for which Cisco is not responsible under Your applicable agreement, or delays of common carriers.

3. Definitions

Term	Meaning
Availability	Calculated as follows and converted into a percentage: $\frac{\text{Total Service Time – Total Downtime}}{\text{Total Service Time}}$
Core Services	Security Cloud Control and cdFMC (as set out in the Offer Description)
Downtime	The period during which: (A) For Cisco Security Cloud Control, the applicable regional cloud (https://us.manage.security.cisco.com,https://eu.manage.security.cisco.com, https://in.manage.security.cisco.com, https://apj.manage.security.cisco.com/, https://aus.manage.security.cisco.com) is completely unreachable (Availability is calculated solely based on the applicable regional cloud); and (B) For cdFMC, You are completely unable to access cdFMC when the applicable Security Cloud Control regional cloud is available; subject to the exclusions stated in Section 2.2 (Exclusions) of this SLO, and which: (1) begins (i) when Cisco logs an incident ticket based on Cisco's identification of Core Services downtime, or (ii) upon Cisco's confirmation of Core Services downtime You report to Cisco; and (2) ends when the Core Services are restored.
Total Downtime	The aggregate total Downtime during a Measurement Period (rounded upward to the nearest minute).
Total Service Time	The total number of minutes in a Measurement Period (calculated by multiplying 60 (minutes) by 24 (hours) by the number of calendar days in the Measurement Period).