



Offer Description – Product

Cisco Secure Cloud Protection Suite

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

The Cisco Secure Cloud Protection Suite (the “**Product**”) includes Cloud Services that provides consolidated management of security policies, centralized controls, asset discovery, attack path management, and risk-based vulnerability management across data centers and clouds. This Product provides visibility for hybrid and multi-cloud environments and enables teams to simplify operations and to protect and manage complex environments with confidence and ease.

Your subscription entitles You to access and use (a) the Cloud Services included in the applicable tier in the table below and (b) Security Cloud Control and Security Cloud Sign-On. Security Cloud Control unifies the experience of deploying and managing Your Cloud Service. Security Cloud Sign-on is a single sign-on (SSO) across products, operating as the native Identity Provider (IdP) or delegated IdP across selected Cisco products.

Suite Tier	Cloud Services Included in Suite Tier
Cloud Protection Suite Advanced	Multicloud Defense Premier*
	Attack Surface Management
	Panoptica
Cloud Protection Suite Essentials	Multicloud Defense Advanced*
	Vulnerability Management Premier
	Secure Workload as a Service

*Access to Cisco Multicloud Defense is delivered through Cisco Defense Orchestrator

2. Support

You will be required to select [Enhanced or Premium Support](#) when You purchase the Product.

3. Performance Standards

The Cloud Services included in the Product are subject to any Service Level Objective (“**SLO**”) or Service Level Agreement (“**SLA**”) described in the individual Offer Description. If a Cloud Service SLA or SLO includes a termination right, that termination right is not applicable to the Product subscription.

4. Data Protection

The Cisco Privacy Data Sheets for the following Cloud Services (available at [Cisco's Trust Portal](#)) describe the personal data that Cisco collects and processes as part of the delivery of the Product: Cisco Attack Surface Management (formerly, Secure Cloud Insights), Cisco Multicloud Defense, Panoptica, Cisco Secure Workload as a Service, Cisco Vulnerability Management, and Cisco Security Cloud Control and Cisco Security Cloud Sign-On.

5. Special Terms

- 5.1 **Additional Offer Terms.** Each Cloud Service included in the Product is subject to its individual Offer Description. The following Offer Descriptions apply (depending on Suite Tier): [Attack Surface Management \(formerly, Secure Cloud Insights\)](#), [Multicloud Defense](#), [Panoptica](#), [Secure Workload as a Service](#), and [Vulnerability Management](#). This Offer Description takes precedence over the individual Offer Descriptions in the event of any conflict.
- 5.2 **Billing Meter – Workload.** Cisco licenses the Product based on the number of workloads – individual Cloud Service billing meters do not apply. In addition, when You purchase the Product, You must purchase a minimum of twenty-five (25) workloads.
- 5.3 **Subscription Start Date; Claim Code.** When Cisco receives and accepts Your order, You will receive a claim code via email. The claim code enables You to (i) set up your subscription in Security Cloud Control, and (ii) commencing on the requested start date (RSD) in the order, provision and access the Cloud Services included in the purchased tier. Your subscription will commence on the RSD whether You elect to provision Cloud Service(s) on the RSD or delay provisioning of one or more of the Cloud Services.
- 5.4 **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.
- 5.5 **Attack Surface Management Usage.** Suite packaging assumes that for your usage of Attack Surface Management, You have, on average, no more than twenty-five (25) billable entities per workload. You understand that if Your average billable entity to workload ratio is significantly higher than twenty-five to one (25:1) on a recurring basis, Cisco will work with You to assess utilization/consumption and may require You to purchase additional workload licenses.
- 5.6 **Multicloud Defense Usage.** Suite packaging assumes that for your usage of Multicloud Defense Advanced or Premier tiers, You have fourteen (14) gateway hours per workload per month. You understand that if Your gateway hours per workload per month exceeds fourteen (14) hours per month, Cisco will work with You to assess utilization/consumption and may require You to purchase additional workload licenses.
- 5.7 **Vulnerability Management Usage.** Suite packaging assumes that for your usage of Vulnerability Management Premier tier, You have, on average, no more than 20 assets per workload. You understand that if Your average asset to workload ratio is significantly higher than 20:1 on a recurring basis, Cisco will work with You to assess utilization/consumption and may require You to purchase additional workload licenses.
- 5.8 **Disclaimers.** While Cisco has used commercially reasonable efforts to create effective security technologies, 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 product (and included cloud services) will guarantee absolute security or that it will protect all your files, network, or endpoints from all malware, viruses, or third-party malicious attacks.