



## Offer Description

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

### 1. Summary

This Offer Description applies to Cisco Multicloud Defense and any Cisco Offers that reference this Offer Description (collectively, the “**Cisco Offer**”). The Cisco Offer consists of two components – the Cisco Multicloud Defense Controller (the “Controller”), which is managed by Cisco, and the Cisco Multicloud Defense Gateway (the “Gateway”), which is deployed in Your public cloud account(s).

The Multicloud Defense Gateway instance may either be a Multicloud Defense Gateway or a Cisco Secure Firewall Threat Defense Virtual instance (“FTDv”) based on Your specification. For more information on Cisco Multicloud Defense, see can be: [cisco.com/go/multicloud-defense](https://cisco.com/go/multicloud-defense). For more information on Cisco Secure Firewall Threat Defense Virtual, see can be found here: <https://www.cisco.com/c/en/us/products/collateral/security/firepower-ngfw-virtual/threat-defense-virtual-ngfwv-ds.html>.

### 2. Support and Other Services

The Cisco Offer has two levels of support: (1) Embedded Support, which is included with the Cisco Offer, and (2) Solution Support, which is available for purchase. Cisco will provide You with support depending on the support level listed in the order.

- Embedded Support is described here: [Cisco Software Support Services](#).
- Solution Support is described here: [Cisco Solution Support](#).
- Cisco Severity and Escalation Guidelines are described here: [Cisco Severity and Escalation Guidelines](#).

### 3. Performance Standards

**Service Level Agreement.** The [Cisco Multicloud Defense Service Level Agreement](#) applies to the Cisco Offer.

### 4. Data Handling

The [Disclosure Documents](#) for Cisco Multicloud Defense provide information about data handling practices, security controls, and other features specific to this Cisco Offer.

### 5. Special Terms

**5.1 Meter and Gateways.** The Cisco Offer is priced and metered based on the number of Gateway Hours You purchase. Gateway Hours are sold in units of 100. One “Gateway Hour” means one Gateway running for one hour in the calendar month. “Gateway” means either a Multicloud Defense Gateway or an FTDv instance. For the Premier Tier, the Product subscription includes FTDv. Customer can utilize the included FTDv licenses and/or their separately purchased FTDv licenses. Only the FTDv licenses included with the Premier Tier are metered by Gateway Hours. A subscription to Cisco Security Cloud Control – Firewall Management is required to leverage FTDv as a Gateway. During Your active subscription, Cisco may periodically review Your usage of Gateway Hours against Your subscription entitlement and reserves the right to require You to purchase additional Gateway Hours if Your usage exceeds such subscription entitlement.

**5.2 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 Product. Your subscription will commence on the RSD whether You elect to provision the Cisco Offer on the RSD or delay.

**5.3 Unlicensed Feature Usage.** You may have access to certain features that are not included in the Cisco Offer subscription package You purchase. If You utilize features not covered by Your subscription, You are required to upgrade Your subscription prospectively at the next anniversary date of the subscription. Prior to the upgrade, You

may use such unlicensed features for evaluation purposes for up to 100 Gateway Hours. Cisco's support and Service Level Agreement obligations do not apply to unlicensed features. Cisco reserves the right to terminate access and/or usage rights to unlicensed features at any time with or without notice.

- 5.4 **Competitive Testing.** You will not publish or disclose to any third party any Cisco Offer performance information or analysis (including without limitation the results of benchmark, testing for the effectiveness of security protection, or any competitive testing) except with Cisco's prior written consent.
- 5.5 **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 Cisco Offer will guarantee absolute security or that it will protect all your files, network, or endpoints from all malware, viruses, or third-party malicious attacks.