



## Offer Description

# Cisco Secure Firewall Portfolio

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

This Offer Description applies to the Cisco Secure Firewall Portfolio, which includes both on-premises Software and Cloud Services, and any Cisco Offers that reference this Offer Description (collectively, the “**Cisco Offer**”). On-premises Software solutions include: The Cisco Firepower 1000s, 1200s, 3100s, 4100s, 4200s, 9300s Series Appliances and Cisco Secure Firewall ISA3000 (collectively the “Next-Generation Firewalls”), Cisco Secure Firewall Management Center (“FMC”), Cisco Secure Firewall Threat Defense (“FTD”), Cisco Adaptive Security Appliance (“ASA”), the Firewall Device Manager (“FDM”), Secure Web Application Firewall (“WAF”), and Cisco Secure DDoS Protection. Cloud Services solutions include: Cisco Secure Firewall Threat Defense Virtual for public cloud and for private cloud (“FTDv”), Cisco Adaptive Security Appliance Virtual (“ASAv”), Secure Cloud Web Application Firewall (“CWAf”), and Cisco Secure Cloud DDoS Protection.

### 2. Support and Other Services

- 2.1 **Support sold separately.** Your purchase of the Cisco Offer does not include support, but You can purchase support separately.
- 2.2 **Integrations.** Additional products, services, and integrations that may be available for Your use with the Cisco Offer but are not considered part of the Cisco Offer include, but are not limited to: Cisco Security Cloud Control (formerly Cisco Defense Orchestrator), including the cloud-delivered Firewall Management Center (cdFMC), Cisco Multicloud Defense (MCD), Cisco Secure Workload, Cisco Security Analytics and Logging, Cisco XDR, Cisco Identity Services Engine, and other third-party solutions.

### 3. Data Handling

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

### 4. Special Terms

- 4.1 **Competitive Testing.** You will not publish or disclose to any third party any Cisco Offer performance information or analysis (e.g., the result of benchmark or competitive testing) except with Cisco’s advance written permission.
- 4.2 **Additional Terms for Secure Web Application Firewall.** If You purchase Secure Web Cloud Application Firewall (WAF) and/or Cisco Secure Cloud DDoS Protection, You are also subject to the Master Cloud Services Agreement located at: <https://www.radware.com/WorkArea/DownloadAsset.aspx?ID=f78d23de-791f-435e-8d02-a564992231d8>
- 4.3 **Disclaimer.** While Cisco uses commercially reasonable efforts to create effective security technologies, Cisco does not represent or warrant that the Cisco Offer 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.