



## Offer Description

# Secure Email

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 Secure Email Gateway (Software) and the following Cloud Services: Cisco Secure Email Cloud Gateway (formerly Cloud Email Security or “CES”), Cisco Secure Email Encryption Service (formerly Cisco Registered Envelope Service or “CRES”), Cisco Secure Email Domain Protection (formerly Cisco Domain Protection or “DMP”), Cisco Secure Email Phishing Defense (formerly Cisco Advanced Phishing Protection or “APP”), Cisco Secure Email Threat Defense (formerly Cisco Cloud Mailbox Defense or “CMD”); and any Cisco Offer that references this Offer Description (collectively, the “**Cisco Offer**”).

### 2. Support and Other Services

**Support.** Your purchase of the Cisco Offer includes [Cisco Software Support Services](#).

### 3. Performance Standards

**Service Level Agreement.** The [Secure Email Service Level Agreement](#) applies to the Secure Email Cloud Gateway, Secure Email Encryption Service, Secure Email Domain Protection and Secure Email Phishing services. The [Secure Email Threat Defense Service Level Objective](#) applies to the Email Threat Defense service.

### 4. Data Handling

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

### 5. Special Terms

**5.1 Cisco Secure Email Domain Protection Data Usage Acknowledgement.** Cisco and its applicable subcontractor(s) may use Customer Data relating to emails that fail authentication through Cisco Secure Email Domain Protection (“**Authentication Failure Data**”) to provide the Cisco Offer and as authorized under the Agreement and this Offer Description. Without limiting rights otherwise set forth in the Agreement and this Offer Description, Cisco and its applicable subcontractor(s) may compile, aggregate, publish, use, and share anonymized summaries of such Authentication Failure Data both during and after the Use Term to determine and report Cisco Offer usage patterns, analyze and report security related issues and trends, and improve upon and create new products and service offerings. You further acknowledge that Cisco and its applicable subcontractor(s) involved in the delivery of the Cisco Offer may license and provide such aggregated and anonymized summary data (excluding Your Confidential Information and any personally identifiable information (if any is actually received)) to Cisco, applicable subcontractors, or their applicable licensees, for internal use in doing the same, both during and after the Use Term. To the extent You may have any rights in or to any Authentication Failure Data, You hereby grant Cisco (and our applicable subcontractor(s) involved in the delivery of the Cisco Offer) a perpetual, royalty-free, transferable license to do all the foregoing. This paragraph will survive the expiration or termination of the Agreement.

#### 5.2 Licensing and Use Limitation

- (A) The Cisco Offer described in this Offer Description are licensed based on the quantity of Covered Users. The term “**Covered Users**” means the total number of your internet-connected employees, subcontractors and other authorized individuals covered by your deployment of the applicable Cloud Service.
- (B) If we determine in good faith that You are using Cisco Secure Email Cloud Gateway or Cisco Secure Email Threat Defense as part of an outbound bulk email delivery service, Cisco may require You to purchase additional services

or require You to re-architect the email flow to exclude one or both of those products from Your outbound bulk email flow.

- 5.3 **Disclaimers.** Cisco does not represent or warrant that the Cisco Offer will guarantee absolute security 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 protect all your files, network, or endpoints from all malware, viruses or third-party malicious attacks. Integrations made accessible to you that are not a generally available Cisco Offer included on your order are provided on an “AS-IS” basis.