Offer Description – Product

Cisco Secure Breach 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 Breach Protection Suite (the "**Product**") includes Cloud Services and Software that together empower security teams to simplify operations and accelerate incident response across the most prominent attack vectors including email, endpoints, network, and cloud environments. It provides unified protection that combines multiple security technologies and leverages AI for enhanced threat detection, streamlined security operations, and improved efficiency.

Your subscription entitles You to access and use (a) the Cloud Services and Software included in the applicable Suite tier listed in the table below, and (b) Security Cloud Control and Security Cloud Sign-On. Security Cloud Control provides You a unified experience in deploying and managing Your Cloud Service, and Security Cloud Sign-on is used as 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 and Software Included in Suite Tier*
Breach Protection Suite Advantage	Secure Endpoint Premier – Includes Talos Threat Hunting (Includes file inspection for 200 files; 1 SMA cloud portal user if <250 Covered Users; 3 SMA cloud portal users if ≥ 250 Covered Users)
	XDR Advantage
	Email Threat Defense (Includes file inspection for unlimited files; no SMA cloud portal users)
	Secure Network Analytics (virtual)
	Cisco Telemetry Broker (virtual)
Breach Protection Suite Essentials	Secure Endpoint Advantage (Includes file inspection for 200 files; 1 SMA cloud portal user if <250 Covered Users; 3 SMA cloud portal users if ≥ 250 Covered Users)
	XDR Essentials
	Email Threat Defense (Includes file inspection for unlimited files; no SMA cloud portal users)

*The Breach Protection Suite also includes file inspection through Secure Malware Analytics ("**SMA**") and SMA cloud portal usage at the quantities listed above.

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 this Product are subject to any Service Level Objective ("**SLO**") or Service Level Agreement ("**SLA**") described in the individual Offer Descriptions. 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 Email Threat Defense, Cisco Secure Endpoint, Cisco Secure Malware Analytics, Cisco Secure Network Analytics, Cisco Security Cloud Control and Cisco Security Cloud Sign-On, Cisco Telemetry Broker, and Cisco XDR Privacy Data Sheets. When You purchase Secure Endpoint through the Breach Protection Suite, Your Secure Endpoint data center region is North America.

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): Secure Endpoint, XDR, Email Threat Defense, Secure Malware Analytics, and Cisco Secure Network Analytics. This Offer Description takes precedence over the individual Offer Descriptions in the event of any conflict.

5.2 **Billing Meter – Covered Users**. Cisco licenses Product subscriptions based on the number of Covered Users – individual Cloud Service billing meters do not apply. In addition, when You purchase the Product, You must purchase a subscription for each Covered User even if that Covered User is not protected by all of the individual Cloud Services included in the Product.

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 (a) set up your subscription in Security Cloud Control, and (b) 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 **Secure Endpoint Usage**. Suite packaging assumes that You have, on average, two (2) endpoints per Covered User for purposes of Cisco Secure Endpoint. If Your average endpoint to Covered User ratio is significantly higher than two to one (2:1) on a recurring basis, Cisco will work with You to assess utilization/consumption and may require You to purchase additional Covered User licenses.

5.6 **Cisco Secure Network Analytics Usage**. Suite packaging assumes that You have, on average, five (5) Flows per Covered User for purposes of Cisco Secure Network Analytics. If Your average Flow to Covered User ratio is significantly higher than five to one (5:1) on a recurring basis, Cisco will work with to assess utilization/consumption and may require You to purchase additional Covered User licenses.

5.7 **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 and software) will guarantee absolute security or that it will protect all your files, network, or endpoints from all malware, viruses, or third-party malicious attacks.

5.8 **Definitions**

"**Covered User**" means an Internet-connected employee, subcontractor, and any other authorized individual covered (i.e., protected) by Your deployment of any of the included Cloud Services or Software.

"**Flow**" means the number of flow records received and processed per second.