Offer Description – Product
Cisco Hypershield

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

Cisco Hypershield (the "**Product**") is a hybrid, AI-native security Subscription Offer that embeds hyper-distributed security across applications, servers, and cloud infrastructures. The Product enables customers to streamline security policy automation and infrastructure updates, by leveraging extended Berkeley Packet Filtering (eBPF) for comprehensive visibility and a dual data plane architecture for more secure updates. The Product allows customers to place security enforcements across their environments with autonomous segmentation and distributed exploit protection to guard against common vulnerabilities and exposures (CVEs).

2. Support and Other Services

2.1 **Prerequisite Product.** The Product requires that You have an existing license for Cisco Defense Orchestrator[1] for its unified cloud management functionality. For more information on Cisco Defense Orchestrator, see the Cisco Defense Orchestrator Offer Description.

2.2 **Support.** Your purchase of the Product includes 24/7 access via online and email technical support as described below. Support requests can be opened (1) online via the Hypershield portal at https://support.hypershield.cloud or (2) via e-mail to hypershieldsupport@external.cisco.com. All support request emails must have an assigned SEV-# included in the subject line (see Table 1 below). If Your support request email does not include a SEV-# in the subject line, Your request will automatically be assigned as SEV-4. Your support request may be re-assigned a SEV-# by the support team. For escalations: email hypershieldsupportescalation@cisco.com.

Table 1. Cisco Hypershield Severity Levels

SEV-#	Description of Severity Levels	Response Times
SEV-1	Critical impact on business operations. Product is down.	Response within 1 hour
SEV-2	Substantial impact on business operations. Product is degraded.	
SEV-3	Minimal impact on business operations. Product is partially degraded.	Response within Next Business Day

---

[1] Effective November 11, 2024, Cisco Defense Orchestrator will be rebranded as Cisco Security Cloud Control ("SCC"). Some materials may refer to CDO or SCC interchangeably.

SEV-4	No impact on the business operations. Support requests are about information about features, implementation, or configuration for Product.	

3. Performance Standards

Service Level Objective. The Product is managed by customers through Cisco Defense Orchestrator which is subject to the availability Service Level Objective ("**SLO**") available in the Cisco Defense Orchestrator Offer Description.

4. Data Protection

Privacy Data Sheets. The Cisco Hypershield Privacy Data Sheet and the Cisco Defense Orchestrator Privacy Data Sheet describe the Personal Data that Cisco collects and processes as part of delivering the Product.

5. Special Terms

5.1 **Meter and Usage.** The Product subscription price is based on the quantity of Protection Units purchased (the purchased quantity is referred to as the "subscription entitlement"). A minimum of 100 Protection Units is required for an active subscription. You can reassign Your Protection Unit subscription entitlements to the various Product deployment options at any time (e.g., from Linux workload VM to VM Appliance, etc.) and purchase additional Protection Units during Your active subscription term. During Your active subscription, Cisco may periodically review Your usage of Protection Units against Your subscription entitlement and reserves the right to require You to prospectively purchase additional Protection Units if Your usage exceeds such subscription entitlement. Usage is measured based on the average number of deployed Protection Units on a rolling 30 calendar day basis during Your Use Term.

5.2 **Deployment Models and Scale**

Enforcer Type	Deployment	Protection Unit Cost	Specification	Tier
Tesseract Security Agent (end-system enforcer)	Linux workload VM	12 Protection Units per deployment	An agent deployed at the Linux workload VM	Essentials
	Kubernetes node (each 16 vCPU, 64GB RAM)	36 Protection Units per deployment	An agent deployed at Kubernetes node	Essentials
Network-based enforcer	VM Appliance	36 Protection Units per deployment	A virtual image of a network enforcement point	Essentials

5.3 **Limitations.** In addition to any restrictions described in the Agreement or Documentation, You will not use Software or technology to circumvent, manipulate, or disguise Your usage of Protection Units.

5.4 **Competitive Testing.** You will not publish or disclose to any third party any Product performance information or analysis (e.g., the result of benchmark or competitive testing) except with Cisco's advance written permission.

5.5 **Software Updates.** Cisco reserves the right to automatically update the Product to the most recent version of the Software; however, You will have the option to schedule or defer Your automatic updates. You may delay updates provided that Your current Software version is still supported by Cisco. You understand and agree that delaying updates to the latest Software release may introduce

security risks to Your environment and Cisco is not responsible for any security-related incidents that result from that delay.

5.6 **Disclaimer. While Cisco uses commercially reasonable efforts to create effective security technologies, Cisco does not represent or warrant that the Product 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.**

6. Definitions

Term	Meaning
Protection Unit	The billing meter used to describe the subscription unit allocable to Your enforcement point.
VM	VM means virtual machine.