Description du produit pour Cisco Multicloud Defense

Cette Description du produit s'applique à Cisco Multicloud Defense (le « Produit »), qui est soumis au Contrat de licence de l'utilisateur final (CLUF) de Cisco, disponible à l'adresse www.cisco.com/go/eula. Les termes commençant par une majuscule, sauf s'ils sont définis dans le présent document, ont la signification qui leur est donnée dans le CLUF ou les Conditions générales (le « Contrat »). Par souci de clarté, les Descriptions de produits comme celle-ci ont toujours été appelées Descriptions de l'offre ou Contrats de licence de l'utilisateur final supplémentaires. Les références à ces documents dans ce Contrat doivent être interprétées comme une référence à la présente Description de produit.

1. Résumé

Cisco Multicloud Defense est une plateforme de sécurité réseau multinuage fournie en tant que service. Elle dissocie le contrôle et le plan de données, ce qui donne deux composants : le contrôleur Cisco Multicloud Defense et la passerelle Cisco Multicloud Defense. Le contrôleur Cisco Multicloud Defense fournit le plan de gestion et de contrôle. Elle déploie également la passerelle Cisco Multicloud Defense, une plateforme proposée comme un service (PaaS) utilisée dans les comptes de nuage public du client pour fournir des protections de sécurité avancées en ligne pour se défendre contre les attaques externes, empêcher l'exfiltration de données de sortie et empêcher le mouvement latéral des attaques. Le seul point d'entrée du Produit est Cisco Defense Orchestrator. Vous pouvez trouver la Description du produit pour Cisco Defense Orchestrator ici : https://www.cisco.com/c/dam/en_us/about/doing_business/legal/OfferDescriptions/cisco-defense-orchestrator.pdf

Le Produit est disponible en trois niveaux, et chaque niveau comprend les droits et est soumis aux limitations décrites dans les Tarification par niveau et droits disponibles ici : cisco.com/go/multicloud-defense.

2. Services

Le Produit dispose de deux niveaux d'assistance : l'assistance intégrée, qui est incluse dans le produit, et l'assistance aux solutions, qui peut être achetée séparément. Cisco Vous fournira une assistance en fonction du niveau d'assistance indiqué dans la commande.

- L'assistance intégrée est décrite ici : *https://www.cisco.com/c/dam/en_us/about/doing_business/docs/cisco-software-support-service.pdf*.
- L'assistance aux solutions est décrite ici : https://www.cisco.com/c/dam/en_us/about/doing_business/legal/service_descriptions/docs/solution-support-smart-total-care.pdf.
- Les Directives en matière de gravité et de signalisation progressive de Cisco, sont décrites ici : https://www.cisco.com/c/dam/en_us/about/doing_business/legal/service_descriptions/docs/cisco- severity-and-escalation-guidelines.pdf

3. Normes de performance

Cisco déploiera des efforts commercialement raisonnables pour fournir le contrôleur de Cisco Multicloud Defense du Produit de manière à atteindre ou à dépasser le Niveau de service dans cet Objectif de niveau de service (« SLO »). Cet Objectif de niveau de service (SLO) (1) est destiné à aider les parties à superviser la disponibilité du contrôleur Multicloud Defense et (2) ne Vous donne pas droit au paiement de crédits de service ou de remboursements. Le SLO décrit dans la Description de l'offre de Cisco Defense Orchestrator, telle que modifiée ci-dessous, s'applique au Produit :

Objectif de niveau de service	Pendant chaque Période de mesure, la Disponibilité ciblée sera de : Cisco Defense Orchestrator (à l'exclusion de cdFMC) : 99,99 % cdFMC : 99,99 % Cisco Multicloud Defense : 99,99 %
« Période de mesure »	Un mois civil
Calcul et définitions connexes	La « **Disponibilité** » est calculée comme suit, convertie en pourcentage : $\frac{\text{Durée totale du service – Durée totale des pannes}}{\text{Durée totale du service}}$ La « **Durée totale du service** » correspond au nombre total de minutes d'une Période de mesure calculé en multipliant 60 (minutes) par 24 (heures) par le nombre de jours civils compris dans la Période de mesure. La « **Durée totale des pannes** » est la durée totale agrégée de toutes les Pannes admissibles au cours d'un mois civil (arrondi à la minute supérieure). Pour calculer la Durée totale d'une panne admissible, chaque Panne admissible : i. Commence lorsque Cisco enregistre un billet d'incident sur la base de l'identification par Cisco d'une panne ou lors de la confirmation d'une panne que Vous signalez à Cisco ii. Se termine lorsque Cisco Defense Orchestrator ou cdFMC, selon le cas, est restauré « **Panne admissible** » signifie : i. Pour Cisco Defense Orchestrator, le nuage régional applicable (c.-à-d. Defenseorchestrator.com, Defenseorchestrator.eu ou apj.cdo.cisco) est totalement inaccessible, sauf si une telle panne est une Panne justifiée. La Disponibilité est calculée uniquement en fonction du nuage régional applicable. ii. Pour cdFMC, Vous êtes totalement incapable d'accéder à cdFMC lorsque le nuage régional Cisco Defense Orchestrator applicable est disponible, sauf si une telle panne est une Panne justifiée. iii. Pour Cisco Multicloud Defense, Vous êtes totalement incapable d'accéder à cdFMC lorsque le nuage régional Cisco Defense Orchestrator applicable est disponible, sauf si une telle panne est une Panne justifiée. **« Panne justifiée »** désigne toute panne causée par **:** i. une maintenance planifiée; ii. une maintenance d'urgence où Cisco doit effectuer des travaux pour prévenir ou atténuer une panne ou une dégradation de la technologie Cisco applicable afin d'éviter ou d'atténuer un incident de sécurité. Cisco fournira autant de préavis que possible avant d'entreprendre une maintenance d'urgence; iii. Vos intégrations ou tout logiciel, matériel ou service tiers applicable non fourni par Cisco; iv. les versions bêta, d'évaluation ou d'essai des Services en nuage; v. Votre incapacité à : (i) respecter les configurations, les mises à jour ou les mises à niveau requises, (ii) suivre les politiques d'utilisation acceptables ou (iii) utiliser les Technologies Cisco applicables conformément à la Documentation ou à d'autres directives publiées; vi. les problèmes causés par Votre violation du contrat ou par Votre manquement à Vos responsabilités; vii. des facteurs échappant au contrôle raisonnable de Cisco, tels que : les performances des réseaux Internet contrôlés par d'autres sociétés (p. ex., les FAI), les pannes d'AWS, d'Okta ou d'autres pannes de l'authentification unique, et les événements de force majeure (p. ex., les grèves ou les pénuries de main-d'œuvre, les émeutes, les insurrections, les incendies, les inondations, les tempêtes, les explosions, les guerres, le terrorisme, les pandémies, les lois gouvernementales, y compris, sans s'y limiter, les réglementations locales, les pénuries de matériel, les défaillances ou les retards des transporteurs publics, etc.).

4. Protection des données

Les fiches techniques sur la confidentialité de Cisco Multicloud Defense et de Cisco Defense Orchestrator décrivent les renseignements personnels que Cisco recueille et traite dans le cadre de la prestation de Cisco Multicloud Defense. Vous pouvez y accéder en effectuant une recherche ici : https://trustportal.cisco.com/c/r /ctp/trust-portal.html?doctype=Privacy%20Data%20Sheet|Privacy%20Data%20Map. Pour en savoir plus sur la manière dont Cisco traite, utilise et protège toutes les catégories de données, consultez le Centre de sécurité et de confiance de Cisco : https://www.cisco.com/c/en/us/about/trust-center/data-management.html.

5. Conditions particulières

Avis de non-responsabilité :

BIEN QUE CISCO AIT DÉPLOYÉ DES EFFORTS COMMERCIALEMENT RAISONNABLES POUR CRÉER DES TECHNOLOGIES DE SÉCURITÉ EFFICACES, EN RAISON DU DÉVELOPPEMENT CONTINUEL DE NOUVELLES TECHNIQUES D'INTRUSION ET D'ATTAQUE DES FICHIERS, DES RÉSEAUX ET DES TERMINAUX, CISCO NE REPRÉSENTE PAS ET N'ÉMET PAS DE GARANTIE QUI VEUT QUE LE PRODUIT CISCO GARANTISSE UNE SÉCURITÉ ABSOLUE OU PROTÈGE TOUS VOS FICHIERS, VOTRE RÉSEAU OU VOS TERMINAUX CONTRE L'ENSEMBLE DES PROGRAMMES MALVEILLANTS, VIRUS OU ATTAQUES MALVEILLANTES DE TIERS.