cisco SECURE

Description de l'offre : Cisco Umbrella

La présente description de l'offre (**« Description de l'offre »**) décrit Cisco Umbrella (les « Services en nuage »). Votre abonnement est régi par la présente Description de l'offre et par le Contrat de licence d'utilisateur final de Cisco, accessible au www.cisco.com/go/eula (ou toute autre condition similaire existant entre Vous et Cisco) (le **« Contrat »**). Les termes commençant par une majuscule utilisés dans cette Description de l'offre qui ne sont pas autrement définis aux présentes ont le sens qui leur est donné dans le Contrat.

Table of Contents

1. Description

Cisco Umbrella est une plateforme de sécurité infonuagique qui unifie plusieurs services de sécurité en une seule plateforme fournie en nuage pour sécuriser l'accès Internet et contrôler l'utilisation des applications en nuage sur votre réseau, dans vos succursales et par vos utilisateurs itinérants. Selon le forfait et le déploiement, Cisco Umbrella intègre une passerelle Web sécurisée, un pare-feu fourni par le nuage (« CDFW », pour « cloud-delivered firewall ») la sécurité de la couche DNS, la protection contre les logiciels malveillants dans le nuage, la prévention des pertes de données en ligne et d'autres fonctionnalités de contrôle d'accès de sécurité infonuagique (CASB), et une isolation du navigateur à distance pour une protection efficace partout où se rendent les utilisateurs. Avant que les utilisateurs ne se connectent à n'importe quelle destination en ligne, Cisco Umbrella agit comme une bretelle d'accès sécurisé à Internet et offre une inspection et un contrôle approfondis pour assurer la conformité et bloquer les menaces. La plateforme Cisco Umbrella est soutenue par l'une des plus grandes équipes d'informations sur les menaces au monde, Cisco Talos, et offre un accès interactif aux informations sur les menaces grâce à Cisco Umbrella Investigate pour faciliter l'intervention en cas d'incident et la recherche de vulnérabilités.

Cisco Umbrella Investigate permet d'accéder à certaines informations sur les menaces de Cisco indiquant les domaines, les adresses IP, les réseaux et les algorithmes de hachage de fichiers malveillants. En se servant d'un ensemble varié de données tirées de milliards de demandes DNS quotidiennes et de vues en direct des connexions entre différents réseaux sur Internet, Cisco applique des modèles statistiques et des renseignements recueillis par des spécialistes pour repérer les infrastructures des attaquants. Les données générées par Cisco Umbrella Investigate peuvent être consultées à partir d'une console Web ou d'une API. Consultez la documentation de Cisco Umbrella pour en savoir plus sur ses caractéristiques techniques, ses exigences en matière de configuration, ses fonctionnalités et autres caractéristiques; ainsi que la comparaison des offres pour obtenir des renseignements à propos des différentes offres groupées de Cisco Umbrella.

Votre abonnement à Cisco Umbrella inclut également l'accès à Cisco SecureX, la plateforme de sécurité intégrée de Cisco qui regroupe des renseignements sur les menaces, unifie la visibilité sur les divers produits de sécurité de Cisco et de tiers, permet des flux de travail automatisés, et plus encore. Pour en savoir plus sur SecureX, consultez la Description de l'offre de SecureX à l'adresse https://www.cisco.com/c/fr_ca/about/legal/cloud-and-software/cloud-terms.html.

2. Conditions générales supplémentaires

2.1. Restrictions

Si Vous êtes un fournisseur de services Cisco agréé dont le contrat avec Cisco Vous autorise à utiliser les Services en nuage de Cisco pour le compte de clients finaux, Vous pouvez utiliser les Services en nuage uniquement pour ces clients finaux.

2.2. Avis de non-responsabilité

CISCO NE FAIT AUCUNE REPRÉSENTATION ET N'ÉMET AUCUNE GARANTIE VOULANT QUE LES SERVICES EN NUAGE GARANTISSENT LA SÉCURITÉ ABSOLUE EN RAISON DU DÉVELOPPEMENT CONTINUEL DE NOUVELLES TECHNIQUES POUR S'INTRODUIRE DANS LES FICHIERS, LES RÉSEAUX ET LES POINTS TERMINAUX. CISCO NE FAIT AUCUNE REPRÉSENTATION ET N'ÉMET AUCUNE GARANTIE VOULANT QUE LES SERVICES EN NUAGE PROTÈGENT TOUS VOS FICHIERS, VOS RÉSEAUX ET VOS POINTS D'EXTRÉMITÉ CONTRE TOUS LES PROGRAMMES MALVEILLANTS, LES VIRUS ET LES ATTAQUES MALVEILLANTES DE TIERS. CISCO NE FAIT AUCUNE REPRÉSENTATION ET N'ÉMET AUCUNE GARANTIE RELATIVE AUX SYSTÈMES ET AUX SERVICES DE FOURNISSEURS TIERS AUXQUELS S'INTÈGRE UN SERVICE EN NUAGE OU CONCERNANT UNE ASSISTANCE PERMANENTE POUR L'INTÉGRATION. LES INTÉGRATIONS MISES À VOTRE DISPOSITION NE SONT PAS GÉNÉRALEMENT DES PRODUITS MIS EN MARCHÉ INCLUS DANS VOTRE COMMANDE SONT FOURNIS « TELS QUELS ».

2.3. Utilisateurs couverts

Pour les offres groupées avec tarification basée sur l'utilisateur, Vous devez acheter une licence d'utilisateur pour chaque Utilisateur couvert, sauf si une fiche technique publiée de Cisco Umbrella indique le contraire. Par « Utilisateur couvert », on entend chaque employé, sous-traitant et autre personne autorisée qui sont connectés à Internet et couverts (c.-à-d., protégés) par le déploiement de Cisco Umbrella. Des licences d'utilisateur supplémentaires peuvent être nécessaires, comme décrit dans les sections 2.4 et 2.6 ci-dessous.

2.4. Cisco Umbrella SIG – Bande passante moyenne

Cisco Umbrella Security Internet Gateway (« SIG ») Essentials, Cisco Umbrella SIG Advantage et Cisco Umbrella SIG pour l'éducation (collectivement, « Umbrella SIG ») sont soumis à une bande passante moyenne allant jusqu'à 50 kilobits par seconde (« kbit/s ») par utilisateur, sur la base d'un calcul au 95^{e} percentile. Cela signifie que 95 % du temps, l'utilisation sera égale ou inférieure à cette vitesse. L'utilisation d'un modèle au 95^{e} percentile permet des pics d'utilisation qui dépassent la limite pendant de brèves périodes. Le calcul est effectué comme décrit ci-dessous.

Cisco mesurera continuellement Votre utilisation de Cisco Umbrella SIG pendant une période de 30 jours consécutifs pour déterminer Votre Bande passante moyenne par utilisateur. Si Cisco détermine à tout moment que Votre Bande passante moyenne par utilisateur a dépassé 50 kbit/s, Cisco se réserve le droit de Vous demander d'acheter des licences supplémentaires si nécessaire afin de réduire Votre Bande passante moyenne à 50 kbit/s. La formule permettant de calculer la Bande passante moyenne est la suivante :

Bande passante moyenne = Bande passante au 95^{e} percentile/nombre d'Utilisateurs couverts

Le 95^{e} percentile de la bande passante est calculé comme suit :

- observation de Vos échantillons de trafic pendant 30 jours dans chaque centre de données Cisco Umbrella auquel votre trafic est envoyé,
- élimination des 5 % des échantillons de trafic les plus élevés dans chacun de ces centres de données pour prendre la valeur d'échantillon de trafic suivante la plus élevée (cette valeur d'échantillon de trafic la plus élevée suivante est appelée « Valeur de pointe »), et
- addition de la Valeur de pointe pour chaque centre de données.

Les échantillons de trafic aux fins de ce calcul comprennent le trafic DNS de Cisco Umbrella, la passerelle Web sécurisée (proxy) et le pare-feu fourni dans le nuage (« CDFW », pour « cloud-delivered firewall ») pour les offres groupées applicables.

Par exemple, si la Valeur de pic d'un centre de données est de 1 million de kbit/s et que la Valeur de pointe d'un deuxième centre de données est de 10 000 kbit/s, la bande passante au 95e percentile est de 1 000 000 + 10 000 = 1 010 000 kbit/s. La Bande passante moyenne par utilisateur est de 1 010 000 kbit/s, divisés par le nombre d'Utilisateurs couverts selon Votre abonnement. Si Vous avez 25 000 Utilisateurs inclus dans Votre abonnement. Votre Bande passante moyenne par utilisateur pour la période évaluée est 1 010 000 / 25 000 = 40,4 kbit/s.

2.5. Restrictions d'utilisation acceptable pour Cisco Umbrella SIG et Cisco Umbrella CDFW

Dans le cadre de Votre utilisation de Cisco Umbrella SIG et de Cisco Umbrella CDFW, Vous vous abstiendrez (et ne permettrez à aucun tiers) d'effectuer les actions suivantes : (i) établir des requêtes automatisées régulières et fréquentes vers un site externe si ce site externe peut raisonnablement les considérer comme étant une attaque par déni de service ou une violation des conditions de service du tiers, ou de toute autre manière qui pourrait raisonnablement conduire à l'inscription de Cisco sur une liste noire, y compris, à titre d'exemple, l'analyse des ports d'une entité tierce hors de votre contrôle et l'utilisation de technologies de sécurité offensives contre un tiers par l'intermédiaire de Cisco Umbrella; (ii) utiliser le Service en nuage pour accéder à des sites Web ou à des services bloqués en violation de la loi ou de la réglementation en vigueur; ou (iii) utiliser le Service en nuage dans le but de masquer intentionnellement Votre identité dans le cadre d'activités illégales ou pour éviter toute procédure légale. Dans le cas où Cisco reçoit une demande d'informations, une lettre de demande ou toute autre demande similaire en relation avec Votre utilisation de Cisco Umbrella SIG ou de Cisco Umbrella CDFW, et concernant des allégations d'activités illicites sur Votre réseau, Cisco peut divulguer Votre nom à un tiers si cela est nécessaire pour se conformer à un processus juridique ou répondre à des exigences nationales en matière de sécurité; pour protéger les droits, les propriétés ou la sécurité de Cisco, de ses partenaires commerciaux, de Vous ou d'autres personnes; ou pour tout autre motif conformément à la loi en vigueur.

2.6. Cisco Umbrella DNS Security – Moyenne mensuelle des requêtes DNS

Cisco Umbrella DNS Security Essentials et Cisco Umbrella DNS Security Advantage (collectivement, « DNS Security ») ont une limite mensuelle de requêtes DNS (comme défini ci-dessous) de 3 000 requêtes DNS par Utilisateur couvert par jour. Cisco effectue un suivi en continu de votre utilisation de DNS Security sur une base mensuelle pour déterminer Votre Moyenne mensuelle de requêtes DNS. Si, à tout moment, Cisco détermine que Votre moyenne mensuelle de requêtes DNS a dépassé 3 000 requêtes DNS par Utilisateur et par jour, Cisco se réserve le droit de Vous demander d'acheter les licences supplémentaires.

Moyenne mensuelle de requêtes DNS = (nombre de requêtes DNS dans le mois en question/nombre de jours dans le mois en question)/nombre d'Utilisateurs couverts sous licence.

Par exemple, si Vous avez acheté des licences pour mille (1000) Utilisateurs couverts sous licence et qu'ils ont envoyé un total de 3 millions (3 000 000) de requêtes DNS au cours du mois précédent, Votre Moyenne mensuelle de requêtes DNS est la suivante :

(3 000 000 / 30) / 1000 = 100

2.7. Cisco Umbrella Investigate for MSSP

Nonobstant toute disposition contraire dans le Contrat, si Vous avez acheté Cisco Umbrella Investigate for MSSP avec un code UGS portant le numéro de référence UMB-INV-CONSOLE-SP ou UMB-INV-INT-API-SP (collectivement, « Investigate for MSSP »), Vous pouvez utiliser Investigate for MSSP comme outil pour effectuer des recherches et générer des rapports à l'intention de Vos clients tiers uniquement dans le cadre de services de connectivité, de gestion ou d'administration que Vous fournissez à Vos clients tiers.

Toute alliance de marque de Investigate for MSSP réalisée par Vous est soumise aux lignes directrices qui se trouvent ici : https://www.cisco.com/c/dam/en/us/products/collateral/security/umbrella/umbrella-sps-co-branding-guidelines.pdf ainsi qu'aux autres politiques de propriété intellectuelle et de marque de commerce mentionnées dans le Contrat. Par souci de clarté, si Vous fournissez des résultats de recherche, de données ou de résultats provenant de Votre utilisation de Investigate for MSSP auprès de Vos clients tiers, Vous devez à tout moment créditer Cisco comme source de ces informations, en respectant les lignes directrices énoncées ci-dessus.

2.8. Stockage S3 des journaux géré par Cisco

Certaines offres groupées de Cisco Umbrella comprennent la possibilité de sélectionner le stockage S3 géré par Cisco ou le stockage géré par l'Entreprise (c.-à-d., Votre propre stockage) pour le DNS, le proxy et les journaux d'événements. Le stockage S3 des journaux géré par Cisco est offert avec des options de rétention de 7, 14 ou 30 jours. Si Vous avez besoin de plus de 30 jours de rétention, Vous devez sélectionner le stockage géré par l'Entreprise ou exporter les données du stockage géré par Cisco vers le stockage géré par Votre Entreprise avant l'expiration de la période de rétention. Si la journalisation vers un compartiment S3 géré par Cisco est activée, le téléchargement ou la synchronisation des fichiers de ce compartiment doivent être configurés de sorte que chaque fichier journal soit téléchargé une seule fois. Cisco se réserve le droit de suspendre le téléchargement des journaux à partir d'un compartiment S3 (par la rotation des clés ou d'autres méthodes) si les fichiers journaux sont téléchargés plusieurs fois au lieu d'une seule. Veuillez consulter la documentation relative au compartiment S3 géré par Cisco, disponible ici : https://docs.umbrella.com/deployment-umbrella/docs/cisco-managed-s3-bucket

3. Contrats de niveau de service

3.1 Cisco Umbrella DNS Security

Dans le cadre de ce Contrat de niveau de service de Cisco Umbrella DNS Security, le terme « Service » désigne un service DNS récursif de Cisco et ne comprend pas d'interfaces utilisateur Web, de systèmes de configuration ou d'autres méthodes d'accès ou de manipulation de données. Cisco déploiera tous les efforts commercialement raisonnables pour maintenir un Taux de disponibilité de 99,999 % de chaque mois civil pour le Service Cisco Umbrella. Le taux de disponibilité sera calculé en divisant le total des minutes de Temps de disponibilité durant le mois civil en question par le nombre total de minutes de ce même mois, moins les minutes d'Inaccessibilité où le Service Cisco Umbrella est indisponible en raison des périodes de maintenance planifiées et imputables aux Interventions d'un tiers (définies ci-dessous), le tout multiplié par 100. La formule du calcul est comme suit :

Taux de disponibilité = (X ÷ Y) x 100 X = total des minutes de Temps de disponibilité au cours du mois civil

Y = (nombre total de minutes dans ce même mois civil x) - (nombre total de minutes d'Inaccessibilité en raison des périodes de maintenance planifiées et des Interventions de tiers)

Aux fins de ce calcul, (i) « Inaccessibilité » signifie que Cisco Umbrella est totalement inaccessible même si Votre connexion Internet fonctionne correctement, (ii) « Temps de disponibilité » désigne le nombre de minutes où le Service DNS de Cisco Umbrella était accessible, à l'exception des périodes d'Inaccessibilité en raison des opérations de maintenance planifiées et des Interventions d'un tiers, et (iii) « Intervention d'un tiers » désigne toute intervention hors de la volonté de Cisco, y compris, sans s'y limiter, l'efficacité des réseaux Internet ou de carrefours d'échanges de données qui sont gérés par d'autres entreprises, les conflits de travail, les pénuries de main-d'œuvre, les émeutes, les insurrections, les incendies, les inondations, les perturbations météorologiques ou solaires, les explosions, les conflits armés, les actes de terrorisme, les interventions gouvernementales, les conditions de travail, les séismes et les pénuries de matériel. En cas de différend, Cisco rendra sa décision sur l'Inaccessibilité en toute bonne foi sur la base de ses journaux du système, des rapports de surveillance et des registres de configuration et, en ce qui concerne la préséance des documents, ceux de Cisco prévalent sur ceux des clients. Cisco ne peut être tenue responsable d'aucune Inaccessibilité découlant des Interventions d'un tiers.

3.2 Cisco Umbrella SIG

Aux fins du présent contrat de niveau de service Cisco Umbrella SIG, le terme « Service » désigne les Services en nuage Umbrella Secure Internet Gateway (« SIG ») Essentials, Cisco Umbrella SIG Advantage et Cisco Umbrella SIG pour l'éducation, à l'exclusion des interfaces utilisateur Web, des tableaux de bord, des rapports ou d'autres services à la disposition des administrateurs de Cisco Umbrella du client. Cisco déploiera tous les efforts commercialement raisonnables pour atteindre et maintenir un Taux de disponibilité de 99.99 % de chaque mois civil pour le Service Cisco Umbrella.

Le taux de disponibilité sera calculé en divisant le total des minutes de Temps de disponibilité durant le mois civil en question par le nombre total de minutes de ce même mois, moins les minutes d'Inaccessibilité où le Service Cisco Umbrella est indisponible en raison des périodes de maintenance planifiées et imputables aux Interventions d'un tiers (définies ci-dessous), le tout multiplié par 100. La formule du calcul est la suivante :

Taux de disponibilité = (X ÷ Y) x 100

X = nombre total de minutes de Temps de disponibilité au cours du mois civil

Y = (nombre total de minutes dans ce même mois civil) – (nombre total de minutes d'Inaccessibilité en raison des périodes de maintenance planifiées et des Interventions d'un tiers)

« Temps de disponibilité » signifie que le Service est disponible pour accepter votre trafic Internet d'utilisateur final lorsque le Service est correctement configuré pour Vous permettre de tirer parti de l'infrastructure mondiale redondante de Cisco Umbrella. Pour les clients qui utilisent des tunnels IPSec, « correctement configuré » signifie que le Service est configuré avec un tunnel principal et un tunnel secondaire avec un comportement de basculement.

« Inaccessibilité » signifie que le Service n'est pas disponible pour accepter Votre trafic Internet d'utilisateur final lorsque le Service est correctement configuré comme indiqué ci-dessus, à l'exclusion des périodes d'Inaccessibilité dues à des maintenances planifiées et à des Interventions de tiers.

Par « Intervention d'un tiers », on désigne toute intervention échappant au contrôle raisonnable de Cisco, y compris, sans s'y limiter, l'échec de Votre réseau à transférer le trafic Internet à Cisco, la performance des réseaux Internet contrôlés par d'autres entreprises (p. ex., ISP) ou de points d'échange de trafic qui sont contrôlés par d'autres entreprises, les réglementations ou pratiques locales qui empêchent ou limitent le traitement du trafic Internet par Cisco dans certaines régions, 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, les actes de terrorisme, les interventions gouvernementales, les conditions de travail, les tremblements de terre et les pénuries de matériel), et Votre incapacité à acheter un nombre de licences adéquat pour répondre au volume ou à la capacité d'utilisation du Service, si l'objectif de niveau de service aurait été atteint sans cette incapacité.

En cas de différend, Cisco rendra sa décision sur l'Inaccessibilité en toute bonne foi sur la base de ses journaux du système, des rapports de surveillance et des registres de configuration et, en ce qui concerne la préséance des documents, ceux de Cisco prévalent sur ceux des clients. Cisco ne peut être tenue responsable d'aucune Inaccessibilité découlant des Interventions d'un tiers.

4. Protection des données

Les Fiches techniques sur la confidentialité de Cisco Umbrella et de Cisco SecureX (accessibles ici) précisent les Données personnelles que Cisco recueille et traite dans le cadre de la prestation des Services en nuage. De plus, certaines offres groupées de Cisco Umbrella exploitent les fonctions de réputation des fichiers et d'analyse des fichiers malveillants de Cisco Secure Malware Analytics (anciennement AMP Ecosystem et Threat Grid). Veuillez consulter les Fiches techniques de confidentialité applicables disponibles sur le portail de confiance de Cisco. Pour de plus amples renseignements concernant la façon dont Cisco traite, utilise et protège toutes les catégories de données, consultez le Centre de sécurité et de confiance de Cisco.

5. Assistance et maintenance

5.1. Service d'assistance technique de Cisco Umbrella SIG et DNS Security

Les offres groupées de Cisco Umbrella SIG et DNS Security comprennent une assistance en ligne et une assistance téléphonique. À moins que nous ne receviez de l'assistance directement de Votre Partenaire Cisco, Cisco répondra à Vos demandes comme convenu dans le tableau ci-dessous pour ces offres groupées et peut Vous demander des renseignements supplémentaires pour résoudre les problèmes liés au service. Vous acceptez de fournir les renseignements demandés et comprenez qu'en retardant votre réponse, vous risquez de prolonger le temps nécessaire pour que Cisco règle les problèmes et vous réponde.

L'assistance téléphonique permet un accès 24 h sur 24 et 7 jours sur 7 au Centre d'assistance technique (TAC) de Cisco pour recevoir de l'assistance par téléphone ou l'ouverture de dossier en ligne et l'utilisation d'outils en ligne pour l'assistance relative à l'utilisation ou au dépannage.

Vous aurez également accès au site Cisco.com, qui fournit des informations générales et techniques utiles à propos des produits Cisco, ainsi qu'à la base de connaissances en ligne et aux forums de Cisco. Notez que des restrictions d'accès déterminées par Cisco peuvent s'appliquer occasionnellement.

Le tableau ci-dessous décrit les objectifs de temps de réponse de Cisco en fonction de la gravité des cas. Les clients ont la possibilité de sélectionner l'assistance Améliorée ou Supérieure pour ces offres groupées. Cisco peut ajuster la gravité des cas pour s'aligner avec les définitions de gravité ci-dessous.

Service d'assistance logicielle	Couverture de l'assistance technique	Objectif de temps de réponse aux demandes de Gravité 1 ou 2.	Objectif de temps de réponse aux demandes de Gravité 3 ou 4.
Améliorée	En tout temps par téléphone et par Internet	Réponse en 30 minutes	Réponse en 2 heures
Supérieure	En tout temps par téléphone et par Internet	Réponse en 15 minutes	Réponse en 1 heure

Les définitions suivantes s'appliquent à la présente section :

Temps de réponse : le délai entre le moment où la demande est soumise dans le système de gestion des cas et celui où l'ingénieur en assistance communique avec vous.

Gravité 1 : Cisco Umbrella SIG ou DNS Security, selon le cas, n'est pas disponible ou ne fonctionne plus, ou le problème a une incidence critique ou importante sur les opérations commerciales de la personne ayant soumis la demande. La personne ayant soumis la demande et Cisco mobiliseront des ressources à temps plein pour résoudre la situation.

Gravité 2 : le fonctionnement de Cisco Umbrella SIG ou DNS Security, selon le cas, est défaillant, ou des aspects importants des opérations commerciales de la personne ayant soumis la demande sont touchés par une performance logicielle inacceptable. La personne ayant soumis la demande et Cisco mobiliseront des ressources à plein temps pendant les heures d'ouverture pour résoudre la situation.

Gravité 3 : le fonctionnement de Cisco Umbrella SIG ou DNS Security est altéré, bien que la plupart des tâches opérationnelles restent fonctionnelles. Le client et Cisco sont prêts à mobiliser des ressources pendant les heures d'ouverture pour résoudre la situation.

Gravité 4 : il y a un problème mineur intermittent de fonctionnalité ou de rendement, ou de l'information est requise sur Cisco Umbrella SIG ou DNS Security, selon le cas. Il y a peu ou pas d'incidence sur les opérations commerciales de la personne ayant soumis la demande. La personne ayant soumis la demande et Cisco sont tous deux disposés à mobiliser des ressources pendant les heures d'ouverture afin de fournir de l'information ou de l'assistance, selon les besoins.

Jours ouvrables : jours de travail généralement acceptés pour le travail hebdomadaire au sein de la région concernée, durant lesquels les Services en nuage sont offerts, hormis les jours fériés observés par Cisco.

L'Heure locale correspond à l'heure de l'Europe centrale pour l'assistance offerte en Europe, au Moyen-Orient et en Afrique; à l'heure normale de l'Est australienne pour l'assistance offerte en Australie; à l'heure normale du Japon pour l'assistance offerte au Japon; et à l'heure normale du Pacifique pour l'assistance offerte dans tous les autres pays.

5.2. Assistance technique de Cisco Umbrella pour les offres groupées autres que Cisco Umbrella SIG et DNS Security

À l'exception des offres groupées de Cisco Umbrella SIG et DNS Security, et à moins que Vous ne receviez un service d'assistance technique directement de votre Partenaire Cisco, Cisco fournira le service d'assistance conformément au Niveau de service d'assistance technique applicable et aux Cibles de priorité/réponse définies ci-dessous. Pour les offres groupées de Cisco Umbrella autres que Cisco Umbrella SIG et DNS Security, l'option de prise en charge intégrée de Cisco Umbrella correspond au Niveau de base décrit ci-dessous.

Cisco peut modifier la gravité ou la priorité des demandes afin de s'harmoniser avec les définitions énoncées dans le document ci-dessous.

Niveau de l'assistance technique	Description
Niveau de base	Accès seulement par courriel Accès aux outils en ligne (p. ex., les bases de connaissances, les forums, la Documentation, les portails de demandes et les notifications)
Or	Accès par courriel Accès aux outils en ligne (p. ex., les bases de connaissances, les forums, la Documentation, les portails de demandes et les notifications) Assistance téléphonique 24 h sur 24, 7 jours sur 7 pour les demandes de niveau prioritaire P1 Assistance téléphonique 24 h pour les demandes de niveaux prioritaires P2 et P3 (dimanche à 16 h HNP au vendredi 17 h HNP).
Platine	Gestionnaire de compte technique (TAM) dédié Accès par courriel Accès aux outils en ligne (p. ex., les bases de connaissances, les forums, la Documentation, les portails de demandes et les notifications) Assistance téléphonique 24 h sur 24, 7 jours sur 7 pour les demandes de niveau prioritaire P1 Assistance téléphonique 24 h pour les demandes de niveaux prioritaires P2 et P3 (dimanche à 16 h HNP au vendredi 17 h HNP).

Priorité d'assistance	Délai de traitement cible	Description
P1 Inaccessibilité (comme définie dans le Contrat de niveau de service relatif à la disponibilité)	30 minutes pour les demandes par téléphone 2 heures pour les demandes par courriel	Cisco travaillera pour la résolution concernant une base 24 h sur 24 et 7 jours sur 7 ou pour résoudre le problème, ou développer un contournement raisonnable.
P2 : Problème technique	1 jour ouvrable	Un problème survient lorsque les Services en nuage sont accessibles, mais les délais de traitement sont lents alors que Votre connexion Internet fonctionne correctement. Les problèmes peuvent être des questions techniques ou des problèmes de configuration relatifs à Votre compte qui a des effets modérés sur Votre capacité à utiliser les Services en nuage. Cisco travaillera en permanence sur la résolution du problème pendant les heures d'ouverture jusqu'à ce que le problème ait été résolu, ou qu'un plan ait été élaboré et convenu entre Vous et Cisco.
P3 : Demande de renseignements	2 jours ouvrables	Les demandes de renseignements comprennent des questions portant sur le compte, les réinitialisations de mot de passe et les questions de fonctionnalité. Du personnel de Cisco sera mis à contribution pour travailler sur la résolution au moment de la réponse ou dès que possible.

Vous aurez également accès au site Cisco.com, qui fournit des informations générales et techniques utiles à propos des produits Cisco, ainsi qu'à la base de connaissances en ligne et aux forums de Cisco. Notez que des restrictions d'accès déterminées par Cisco peuvent s'appliquer occasionnellement.