# Description du Service pour Cisco Secure Endpoint Professional (Pro)

Le présent document (cette « **Description du service** ») décrit les fonctionnalités, les composants et les conditions du service Cisco Secure Endpoint Pro que Cisco fournira au Client (les « **Services** ») répertorié dans la commande **(**« **Client** »). La quantité et le type précis des Services achetés par le Client (directement ou par l'intermédiaire d'un Revendeur autorisé) seront consignés dans une commande de service, un devis ou une commande Web signée ou acceptée, ou dans tout autre moyen de consentement conforme (par exemple, l'émission d'un achat commande) (« **Commande** ») entre les parties. Cette Description du service doit être lue conjointement avec Prestation de services par Cisco, situé à : Prestation de services par Cisco. L'annexe A de cette Description du service comporte les conditions supplémentaires régissant les Services.

## 1. Description de l'offre

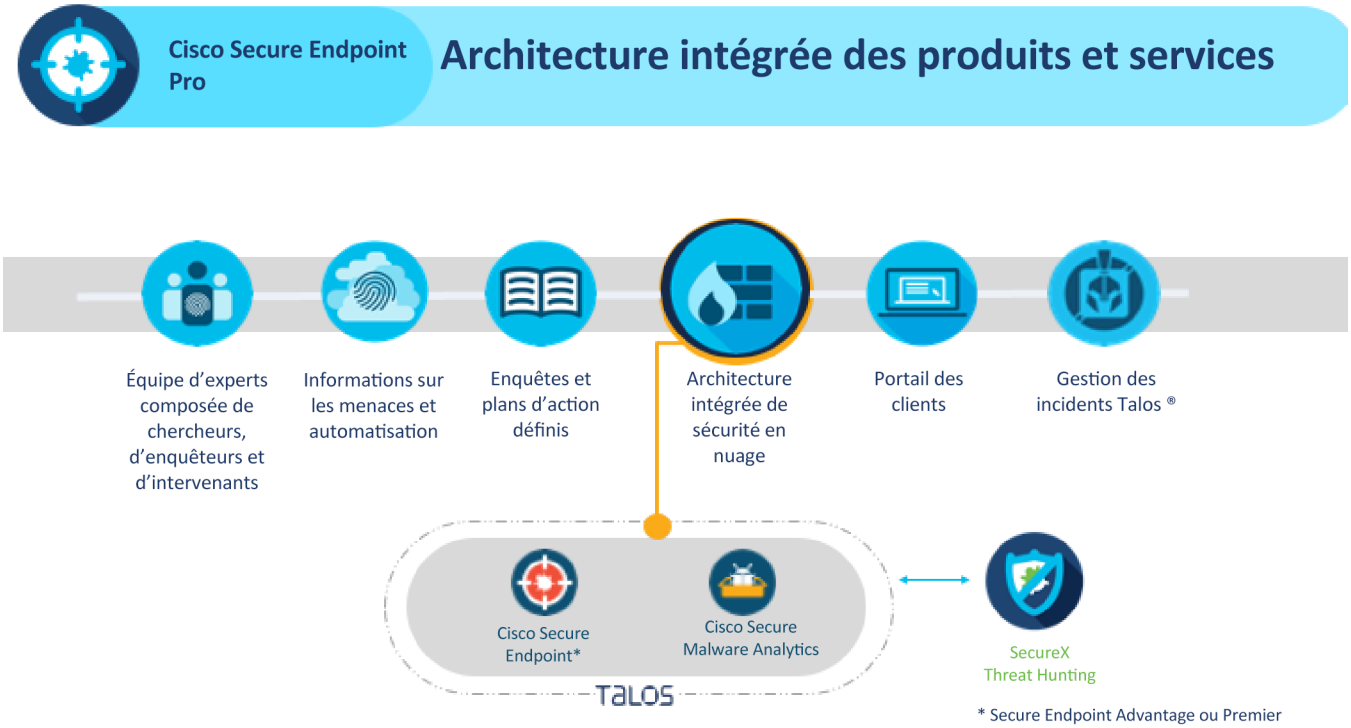
### 1.1 Aperçu de l'offre

Les Services fournissent une solution de sécurité Cisco intégrée en combinant les capacités de Cisco Secure Endpoint avec :

a) la capacité de surveiller des indicateurs supplémentaires de compromission ou d'alerte,

b) un centre des opérations de sécurité (« SOC ») qui surveille les indicateurs de compromission 24 heures sur 24 et 7 jours sur 7, et

c) une équipe de chercheurs, d'enquêteurs et d'intervenants de Cisco qui ont des informations sur les menaces et qui ont défini des guides d'enquête et d'intervention soutenus par la recherche sur les menaces Talos. Les interventions de l'équipe peuvent comprendre des informations, des recommandations ou des modifications en fonction du type de menace ou d'indication de compromission. Les Services sont basés sur les technologies Cisco suivantes :



### 1.2 Résumé des caractéristiques des Services

| Élément du Service | Description | Type d'abonnement Cisco Secure Endpoint | |
|---|---|---|---|
| | | Advantage | Premier |
| Politique de point d'accès sécurisé validée | La configuration Cisco Secure Endpoint/AMP dans l'environnement du Client est validée et harmonisée à la configuration recommandée par Cisco pendant la phase d'Activation du Client. | ✓ | ✓ |
| Surveillance des Incidents de sécurité et des alertes en tout temps | Corrélation, analyse des menaces, enquête et intervention par une équipe expérimentée de chercheurs, d'analystes, d'intervenants-enquêteurs et de soutien à la clientèle, avec des spécialistes de divers secteurs et régions géographiques du secteur | ✓ | ✓ |
| Automatisation et guides d'enquête et d'intervention orchestrés | Recommandation de détection des problèmes, d'enquête et d'intervention basée sur le guide de gestion géré par les analystes des menaces | ✓ | ✓ |
| Information sur les menaces intégrée (TALOS et tiers) | Détectez, analysez, étudiez et corrélez vos recherches en matière d'informations sur les menaces en tirant parti de TALOS, ce qui permet de réagir plus rapidement aux menaces avant qu'elles ne progressent. | ✓ | ✓ |
| Interventions guidées pour contenir, atténuer, corriger ou éradiquer une menace | Créez un dossier d'Incident de sécurité, notifiez et mettez à jour le Client de l'état de l'Incident de sécurité, recommandez des interventions pour aider à contenir, atténuer, corriger ou éradiquer la menace. | ✓ | ✓ |
| Automatisation et intervention active (atténuation proactive des menaces détectées) | Atténuez, arrêtez ou prévenez les menaces détectées de manière proactive en fonction des informations et des avis, selon la menace et l'environnement du Client. | ✓ | ✓ |
| Séance d'information trimestrielle sur les menaces | Le service de gestion des Incidents Cisco Talos organisera une réunion d'examen des services à distance tous les trimestres qui sera ouverte à tous les Clients (non privés). Cette séance d'information trimestrielle fournira des mises à jour sur les modèles actuels de menaces, les volumes de détection et les tendances en matière d'événements. | ✓ | ✓ |
| Intervention automatisée contre les alertes de la recherche de menaces | Atténuez, arrêtez ou prévenez de manière proactive les menaces générées par les alertes de la recherche de menaces en fonction des informations et des avis de sécurité, selon l'environnement du Client. | | ✓ |

| | | | |
|---|---|---|---|
| Service de gestion des incidents Cisco Talos intégré facultatif* | Les Services de gestion des incidents Cisco Talos fournissent une assistance d'urgence et des services proactifs pour évaluer, renforcer et faire évoluer le programme de préparation aux incidents du Client. Vous trouverez une description de ces Services ici : https://www.cisco.com/c/dam/en_us/about/doing_business/legal/service_descriptions/docs/cisco-talos-incident-response-retainer-service.pdf | ✓ | ✓ |

* Service facultatif – sous réserve de conditions et de frais supplémentaires

1.3 **Cisco Secure Endpoint (anciennement Cisco Advanced Malware Protection [AMP]).** Cisco Secure Endpoint est une solution infonuagique d'analyse et de protection avancées contre les programmes malveillants qui permet au Client de mener des analyses des métadonnées de Fichier dans le but de détecter les programmes malveillants et les menaces informatiques. Des hachages cryptographiques de fichiers sont collectés et transmis à un serveur infonuagique géré par Cisco où des analyses de réputation de fichiers sont exécutées et où un classement est effectué pour déterminer si les fichiers en question sont inoffensifs, malveillants ou inconnus. Si un classement ne peut être effectué après l'analyse de hachage d'un fichier, le Client a l'option (selon les licences que vous possédez) de soumettre le fichier à Cisco Secure Malware Analytics (comme cela est décrit dans l'article 1.4 ci-dessous) pour une analyse en bac à sable plus poussée, jusqu'à la limite quotidienne autorisée de demandes du Client. Après l'analyse du fichier, AMP interviendra en fonction du classement (p. ex., en supprimant le Fichier et en le mettant en quarantaine, s'il est jugé être malveillant). Les Services sont offerts avec Cisco Secure Endpoint Advantage et Premier.

1.4 **Cisco Secure Malware Analytics (anciennement Threat Grid).** Threat Grid est une solution infonuagique d'analyse en bac à sable des menaces et des programmes malveillants qui permet à votre Client de soumettre des échantillons de programmes malveillants pour une analyse plus poussée. Threat Grid analyse chaque Fichier pour enregistrer son comportement et déterminer s'il est malveillant. Threat Grid recherchera et mettra en corrélation des éléments de données d'un échantillon de programme malveillant avec des millions d'échantillons collectés et provenant de partout dans le monde pour aider votre Client à obtenir un aperçu global des attaques de programmes malveillants et de son association.

1.5 **SecureX Threat Hunting.** SecureX Threat Hunting est une approche proactive centrée sur l'analyste pour détecter les menaces avancées cachées. Elle est utilisée dans le cadre des interventions automatisées lors d'alertes provenant de la recherche de menaces du Service et est offerte exclusivement dans le cadre du nouveau niveau de licence Premier pour Secure Endpoint. Il aide à donner aux intervenants un récit de la façon dont une attaque a été repérée ou comment elle a évolué et propose une marche à suivre en matière d'intervention. L'objectif est de détecter et de contrer les attaques avant qu'elles ne causent des dommages. SecureX Threat Hunting met à profit l'expertise de Talos et de l'équipe de recherche et d'efficacité de Cisco pour vous aider à déterminer les menaces présentes dans l'environnement du Client. Cisco offre des recherches menées par un humain hautement automatisées, basées sur des guides qui produisent des alertes à fidélité élevée. Le processus combine de manière unique la technologie de recherche avancée Orbital avec l'expertise des chercheurs de menaces d'élite ayant une vaste expérience du secteur, pour trouver des menaces plus sophistiquées de manière proactive. (Remarque : la licence Secure Endpoint Premier est offerte dans le monde entier et dans toutes les régions. Cependant, l'infrastructure SecureX Threat Hunting qui traite la télémétrie du Client et exécute les recherches est actuellement disponible uniquement en Amérique du Nord.)

1.6 **Points d'accès couverts.** Les Services dépendent du fait que le Client dispose de services infonuagiques et de logiciels de point d'accès précis, et que la configuration de ces éléments soit effectuée comme défini dans la documentation fournie par Cisco (« **Points d'accès couverts** »). Le Client doit également obtenir et maintenir tous les contrats d'assistance et de maintenance Cisco applicables ainsi que toute infrastructure requise (c.-à-d. les types d'appareils compatibles) pour répondre aux besoins typiques du Client. Les frais et les Services ne comprennent pas les Points d'accès couverts, leur soutien, leur entretien, leur mise en œuvre ou leur configuration, et ceux-ci doivent être achetés séparément.

## 2 Activation du service.

Cisco définira les exigences pour activer les Services. Ces exigences comprennent la modification des configurations des Points d'accès couverts, la programmation d'API, l'ouverture de connexions réseau pour permettre à Cisco de recevoir des données de télémétrie aux SOC de Cisco et des tests pour confirmer que les Services sont activés. Enfin, Cisco recommandera une politique de configuration initiale pour les Points d'accès couverts

**Responsabilités de Cisco**

- Fournir une documentation au Client pour l'aider à définir les étapes nécessaires à la configuration des Points d'accès couverts, y compris les exigences d'interface API nécessaires pour connecter les Points d'accès couverts au SOC et aux autres systèmes nécessaires pour fournir les Services;
- Mettre en œuvre sa Plateforme de services gérés Cisco (CMSP) et effectuer des tests pour confirmer que les Services sont actifs; et
- Recommander les politiques de configuration initiale pour les Points d'accès couverts.

**Responsabilités du Client**

- Programmer/configurer les API pour créer et maintenir la connectivité des Points d'accès couverts au SOC de Cisco;
- Aider Cisco à établir et à valider la connectivité entre les Points d'accès couverts et la Plateforme de poins d'accès sécurisés gérés; et
- Effectuer les modifications de configuration nécessaires aux Points d'accès couverts pour activer les Services et (le cas échéant) mettre en œuvre les politiques recommandées pour les Points d'accès couverts.

## 3 Procédure des Services

Cisco utilise la procédure suivante pour fournir les Services (lorsque combinés aux Points d'accès couverts) et aider à prévenir et à atténuer les menaces :

**3.1 Surveillance et détection**. Cisco surveillera les alertes de sécurité des Points d'accès couverts pour détecter d'éventuels Incidents de sécurité. Cisco mettra en corrélation les alertes avec les menaces courantes, les informations sur les menaces Talos et certaines informations sur les menaces de tiers en utilisant des systèmes d'analyse, d'orchestration de la sécurité et d'automatisation pour déterminer si les événements observés sont un Incident de sécurité ou un Incident de sécurité probable.

**Responsabilités de Cisco**

- Surveiller les Points d'accès couverts et fournir des systèmes d'alerte d'Incident de sécurité renforcés pour les attaques connues et émergentes en mettant l'accent sur l'utilisation de la détection précoce pour prendre en charge l'accélération des opérations de sécurité pour aider à arrêter, prévenir ou contenir la menace ou l'attaque :
    - déployer des défenses adaptatives pour aider à détecter les attaques hors normes;
    - détecter les activités suspectes et anormales à l'aide d'analyses de sécurité en nuage natif;

- utiliser Cisco Talos pour identifier les menaces, les indicateurs d'attaques ou de compromission et d'atténuation;
- utiliser la recherche et les outils de recherche de menaces pour recueillir des données sur les nouvelles tactiques, techniques et procédures d'attaque (TTP) pour vous aider à identifier les Incidents de sécurité.

**Responsabilités du Client**

- Aviser Cisco des activités ou des pannes prévues (p. ex. des mises à jour logicielles) ou s'il détecte un possible Incident de sécurité.

**3.2 Analyse.** Cisco analysera les événements anormaux et le trafic afin d'identifier les menaces.

**Responsabilités de Cisco**

- Effectuer le suivi et l'analyse des fichiers étiquetés comme suspects sur les Points d'accès couverts, lorsqu'ils traversent le réseau, ainsi qu'aux courriels et au contenu Web; et
- Étudier certaines catégories d'événements et de trafic anormaux où il n'y a aucune cause connue, où ces événements ou ce trafic peuvent constituer une menace importante.

**Responsabilités du Client**

- Sur demande, fournir les données contextuelles demandées (p. ex., les systèmes en cours d'exécution, les activités de maintenance, etc.)

**3.3 Enquête.** Cisco étudiera les menaces sur les Points d'accès couverts, les comportements des utilisateurs, les applications et les éléments de réseau protégés par les Points d'accès couverts.

**Responsabilités de Cisco**

- Utiliser les informations sur les menaces pour rechercher des indicateurs de compromission (IOC) et d'attaque (IOA) pour confirmer les menaces, les attaques, les compromissions ou l'exploitation;
- Créer un dossier d'Incident et aviser le Client si un Incident de sécurité est identifié par Cisco ou signalé par le Client et vérifié par Cisco;
- Utiliser la méthodologie d'enquête établie pour ajouter du contexte aux produits de sécurité intégrés de Cisco et aider à identifier l'incidence, la gravité et la portée de l'Incident de sécurité sur le point d'accès; et
- Étudier l'Incident de sécurité pour déterminer l'incidence, le niveau de réussite de l'attaquant et ses tactiques, techniques et procédures.

**3.4 Intervention.** Cisco informera et mettra à jour le Client de l'état de l'Incident de sécurité et, en fonction de la nature de l'Incident de sécurité : effectuera les modifications approuvées aux Points d'accès couverts, fournira des recommandations guidées ou fournira des recommandations générales en matière d'interventions pour aider à contenir, à atténuer, à corriger, ou éradiquer l'Incident de sécurité.

### Responsabilités de Cisco

- Fournir des conseils (voir les sous-puces ci-dessous pour plus de détails) sur la façon d'atténuer, d'arrêter ou de prévenir un Incident de sécurité en fonction des renseignements et des conseils fournis, selon l'environnement du Client. La réponse recommandée par Cisco à l'Incident peut être une ou plusieurs des solutions suivantes :
  - avec la permission du Client, apporter des Modifications aux Points d'accès couverts pour aider à atténuer ou à arrêter l'Incident de sécurité (Remarque : les réponses automatisées sont limitées à celles du Guide d'intervention);
  - lorsque l'Incident est une attaque connue, recommander des mesures pour atténuer ou arrêter l'attaque et fournir des conseils sur la façon de mettre en œuvre les mesures d'atténuation sur les Points d'accès couverts;
  - lorsque la menace n'est pas complètement découverte ou comprise, recommander au Client d'effectuer une analyse plus approfondie en mettant l'accent sur les zones clés;
  - lorsque la menace ou l'attaque se produit en dehors de la couverture des Points d'accès couverts, faire des recommandations générales au Client pour étudier ou résoudre l'Incident.
- Créer et modifier les guides de détection et d'intervention d'en fonction des nouvelles informations et des menaces issues des événements de sécurité détectés à partir des Points d'accès couverts et des processus décrits ci-dessus.
- Cisco publiera des avis au fur et à mesure que de nouvelles informations sont obtenues sur des menaces nouvelles ou différentes (ces avis ne sont pas spécifiques au Client).
- Si le Client a acheté le service facultatif de gestion des incidents Cisco Talos (CTIR), Cisco en informera l'équipe CTIR et leur dirigera le Client.

### Responsabilités du Client

- Participer aux tests de diagnostic afin d'aider à identifier la source de l'Incident.
- Effectuer les modifications recommandées par Cisco aux Points d'accès couverts et être responsable de donner suite aux recommandations de Cisco, y compris la détermination des dépendances résultant des mesures recommandées.

## Annexe A : Conditions

### 1. Conditions reliées aux Services

**1.1 Portée des Services et exclusions.** À moins que les Services ne soient expressément mentionnés, tous les autres services Cisco sont exclus de cette Description de service. Pour plus de clarté, les éléments suivants sont exclus :

a) la gestion des modifications ou mise en œuvre de modifications non répertoriées dans le catalogue de services;
b) la connectivité, comme (par exemple) un circuit local.

**1.2 Production de rapports.** Cisco fournira, ou mettra à disposition par l'entremise du portail, les rapports énumérés au nombre des documents de rapport pour les services. Cisco se réserve le droit d'ajouter, de modifier ou de supprimer des rapports à sa discrétion.

**1.3 Journalisation.** Les Points d'accès couverts comprennent leurs propres capacités de journalisation. Veuillez consulter la description du produit ou service et les données de journalisation des composants des Points d'accès couverts. Les Services conservent les données des dossiers d'Incident pendant un an, puis celles-ci sont supprimées ou remplacées sur une base continue (les données les plus anciennes en premier).

**1.4 Échange de données.** Sauf dans les cas expressément prévus, les services du centre des opérations de sécurité, de gestion des incidents, etc. ne sont pas inclus dans les Services. Par conséquent, si le Client souhaite qu'un partenaire ou un tiers reçoive des données sur l'Incident (p. ex., des dossiers d'Incident de sécurité) pour fournir des services complémentaires au nom du Client, le Client fournira à Cisco une lettre d'autorisation permettant ce partage de données et la coordination des Services.

**1.5 Capacités de détection et d'intervention.** Bien que Cisco ait mis en œuvre des technologies et des processus commercialement raisonnables dans le cadre du Service, Cisco ne peut pas garantir qu'il préviendra, détectera, arrêtera ou atténuera tous les Incidents de sécurité.

**1.6 Assistance technique pour les Points d'accès couverts.** Les Services ne comprennent pas d'assistance technique pour les Points d'accès couverts. Si le problème du Client nécessite une assistance technique pour les Points d'accès couverts, les Services gérés de Cisco peuvent effectuer un triage initial, puis diriger le Client vers les services d'assistance technique de Cisco ou demander au Client de contacter directement l'assistance technique de Cisco.

### 2. Modalités commerciales

**2.1 Sommaire des prix.** Les Crais comprennent des frais mensuels basés sur le nombre et le type de points d'accès couverts par les Services.

**2.2 Frais.** Les frais pour les Services (les « **Frais** ») et les conditions de paiement seront décrits dans la Commande ou le Contrat applicable. Sauf dans les cas précisés dans la commande ou en cas de manquement grave de Cisco et qui donnent au Client un droit de résiliation, tous les Frais payés ne sont pas remboursables. Les droits de Cisco de percevoir les Frais pour les Services et l'obligation de paiement du Client ne seront pas touchés par i) tout retard causé par un Partenaire ou par le Client (ou toute personne agissant au nom du Client), ii) le manquement ou le retard du Client dans l'exécution de ses obligations en vertu de la présente Description de service ou de tout document complémentaire ou iii) le manquement du Client d'émettre un bon de commande ou les retards ou défauts de paiement du Client envers un revendeur autorisé.

**2.3 Activation du Service.** La Commande contiendra la date d'Activation du Service demandée. Les parties activeront les Services dans les 10 jours ouvrables suivant la date d'Activation du Service demandée, ou les Services seront réputés être activés. Si Cisco est la principale cause du retard dans l'Activation du Service, la date d'Activation du Service sera reportée sur une base journalière.

**2.4 Durée, résiliation et renouvellement**

2.4.1 **Durée.** La durée des Services sera indiquée dans les Commandes. Sauf indication contraire dans les Commandes, la période de la Durée des Services commencera à la Date d'entrée en vigueur de la Commande.

2.4.2 **Résiliation.** Lorsqu'une Commande précise un engagement ou une valeur de contrat minimal, si le Client met fin aux Services pour des questions de commodité, Cisco facturera le reste de la valeur du contrat ou de l'engagement minimal dû en vertu de la Commande. Si la Commande ne précise pas d'engagement minimal, le Client ne peut pas mettre fin aux Services pour plus de commodité, même si le Contrat l'autorise, sauf indication contraire dans la Commande. Les droits de résiliation pour violation de matériel sont indiqués dans le Contrat.

2.4.3 **Renouvellement.** Si le renouvellement automatique des Points d'accès couverts est activé, les Services seront également renouvelés automatiquement sur la même base, sauf si les parties sont avisées qu'elles ne souhaitent pas renouveler les Services comme suit :

**a)** Cisco doit aviser le Client par écrit au moins quatre-vingt-dix (90) jours avant la date de renouvellement du Contrat qu'il ne le renouvellera pas.
**b)** Le Client doit aviser Cisco par écrit au moins trente (30) jours avant la date de renouvellement du Contrat qu'il ne le renouvellera pas.

## 3. Conditions juridiques

**3.1 Licence.** À l'expiration ou à la résiliation des Services, la licence pour l'utilisation du Portail, des Services et de tous les logiciels associés cessera automatiquement d'être en vigueur. Remarque : cette licence est distincte de la licence et des droits associés aux Points d'accès couverts, qui sont couverts par leurs licences applicables.

**3.2 Protection des données.** Les fiches techniques sur la confidentialité de Cisco SecureX (accessibles ici) précisent les Données personnelles que Cisco recueille et traite dans le cadre de la prestation des Services et du traitement des données par les Points d'accès couverts. Les fiches de données sur la confidentialité pour les Points d'accès couverts sont distinctes, mais se trouvent au même endroit.

## Annexe B : Niveaux de priorité

Cette annexe décrit la méthodologie et la terminologie associée utilisées pour définir le niveau de priorité d'un Incident.

### 1. Définition du terme « Priorité »

La Priorité d'un Incident est basée sur l'Incidence et l'Urgence d'un Incident.

| **Incidence :** un Incident de sécurité est classé en fonction de l'étendue de son Incidence sur l'entreprise du Client (à savoir, l'ampleur, la portée et la complexité de l'Incident). | **Urgence :** l'Urgence d'un Incident de sécurité est classée en fonction de son incidence sur les points d'accès surveillés et de son incidence sur les activités du Client. |
|---|---|
| Il existe quatre niveaux d'Incidence :<br>**Généralisée :** l'ensemble du Service est affecté. **Grande envergure :** plusieurs emplacements sont touchés. **Localisée :** un seul emplacement ou un utilisateur individuel à plusieurs emplacements sont touchés.<br>**Individualisée :** un seul utilisateur est touché. | Il existe quatre niveaux d'urgence :<br>**Critique :** incident de sécurité important entraînant l'arrêt de la fonction principale ou une perte importante, une corruption ou un chiffrement non autorisé de données sensibles. Cette situation peut avoir une incidence financière immédiate et importante sur l'entreprise du Client.<br>**Majeure :** la fonction principale est gravement endommagée en raison de la perte de fonctionnalité ou de données, de la corruption ou du chiffrement non autorisé. Il est probable que la situation ait une incidence financière importante sur l'entreprise du Client.<br>**Mineure :** des fonctions non essentielles sont interrompues ou fortement dégradées. Il est possible que la situation ait une incidence financière sur l'entreprise du Client.<br>**Faible/Avertissement :** des fonctions non essentielles sont dégradées. Il n'y a aucune incidence concrète. Le Client considère le problème comme faible. |

### 3.3 Définition du terme « Priorité »

La Priorité définit le niveau d'effort qui sera fourni par Cisco et le Client pour résoudre l'Incident. Le niveau de Priorité est déterminé en se basant sur les définitions des termes « Incidence » et « Urgence » indiquées dans le tableau ci-dessous.

| | | **INCIDENCE** | | | |
|---|---|---|---|---|---|
| **URGENCE** | | Généralisée | De grande envergure | Localisée | Individualisée |
| | Critique | P1 | P1 | P2 | P2 |
| | Majeure | P1 | P2 | P2 | P3 |
| | Mineure | P2 | P3 | P3 | P3 |
| | Faible / Avertissement | P4 | P4 | P4 | P4 |

- P1 : Cisco et le Client engageront toutes les ressources raisonnables, 24 heures sur 24, 7 jours sur 7 pour aider à résoudre l'Incident (comme indiqué ci-dessus).
- P2 à P4 : Cisco et le Client consacreront des ressources raisonnables à temps plein pendant les heures de travail normales pour résoudre l'Incident, fournir l'information ou fournir de l'aide (le cas échéant).

Cisco ajustera le niveau de priorité des dossiers d'incident en fonction de la mise à jour du niveau de priorité de l'incidence ou de la résolution de l'Incident. De plus, le dossier peut rester ouvert après le confinement ou la restauration pendant une période prescrite durant l'évaluation des mesures correctives.

## Annexe C : Contrat de niveau de service (« CNS ») pour Cisco Managed Secure Endpoint

### 1. Aperçu

Le présent CNS décrit les responsabilités des parties et établit les objectifs de rendement de Cisco pour les Services (« Niveaux de service ») et le montant que Cisco accordera au Client en tant que crédit dans le cas où Cisco n'arriverait pas à atteindre les objectifs de rendement des Niveaux de service stipulés dans ce CNS (« Crédits de service »). Ce SLA s'applique uniquement aux Services.

### 2. Niveaux de priorité des Incidents

Cisco classera et traitera les Incidents en fonction de la méthodologie de Niveau de priorité décrite dans l'annexe B de la description des Services.

### 3. Niveaux de service, crédits de service, objectifs de niveau de service, indicateurs de rendement clés.

Sous réserve des conditions du présent CNS, Cisco fournira les Services de sorte qu'ils atteignent ou dépassent les objectifs de rendement des Niveaux de service et que le Client aura le droit de demander des Crédits de service pour l'échec non justifié de Cisco à atteindre les Niveaux de service.

### 4. Mesures du rendement

a) Cisco utilisera ses processus et outils standards pour mesurer son rendement et déterminer si les Niveaux de service ont été atteints.

b) La période pour mesurer le rendement par rapport aux Niveaux de service se nomme la Période de mesure. La première Période de mesure commence 60 jours après l'Activation du service.

c) Dans les trente (30) jours suivant la fin de chaque Période de mesure, Cisco vous rendra les données de Rendement de niveau de service accessibles pour le Client pour la Période de mesure en question (« Rapport sur le rendement »).

d) Si le Client conteste le Rapport sur le rendement, les parties examineront la question, y compris en fournissant des informations sous-jacentes pour appuyer ou contester le contenu du Rapport sur le rendement.

### 5. Renseignements confidentiels

Les Rapports sur le rendement et toutes les données sous-jacentes fournies au Client pour appuyer le Rapport sur le rendement sont des Renseignements confidentiels et ne peuvent être publiés.

### 6. Admissibilité et paiement des Crédits de service

Le Client doit envoyer une demande écrite à Cisco pour recevoir des Crédits de service dans les soixante (60) jours suivant la réception du Rapport sur le rendement, sinon le droit de les recevoir sera supprimé. Les Crédits de service seront fournis sous la forme d'une Lettre de crédit, qui doit être utilisée pendant la durée des Services.

### 7. Restrictions

a) Le Client ne peut pas réclamer plusieurs violations de Niveau de service (et les crédits associés) si un seul Incident a empêché Cisco d'atteindre plusieurs Niveaux de service. Si cela se produit, le Client aura le droit de demander (1) le Crédit de service de son choix.

b) Le Client ne peut appliquer un Crédit de service à moins que le Client ait d'abord payé le reste des Frais (c.-à-d., les Frais moins le montant du Crédit de service).

c) Le Client ne peut vendre, transférer ou céder des Crédits de service ou convertir le Crédit de service en argent.

d) Les Crédits de service maximum et agrégés seront de (5 %) des frais récurrents payés par le Client pour le Service pour la Période de mesure en question.

## 8. Unique recours

L'émission de Crédits de service par Cisco représente la seule responsabilité de Cisco envers le Client et le seul recours exclusif du Client contre Cisco en cas de non-respect des Niveaux de service par Cisco. Tous les Crédits de service payés par Cisco en vertu du présent CNS seront pris en compte dans la limitation de la responsabilité de Cisco en vertu du Contrat.

## 9. Responsabilités du Client

Le Client fournira à Cisco une personne-ressource pour coopérer avec Cisco et fournira les informations raisonnablement demandées pour aider à vérifier le Rendement du niveau de service

## 10. Exceptions

Tout manquement de Cisco à atteindre les Niveaux de service sera excusé s'il est causé par :

a) une action ou une omission grave par le Client qui constitue une violation des conditions générales du Contrat, de la Description du service ou de la Commande;

b) le Client ne respecte pas ses responsabilités en vertu de la Description de service ou du présent CNS ou ne met pas en œuvre les recommandations raisonnables de Cisco qui pourraient empêcher le non-respect du CNS;

c) tout retard ou toute défaillance entraînés par le Client, un équipement, un logiciel, des services, une assistance ou des fournisseurs tiers hors du contrôle de Cisco (p. ex., durée du cycle de transport);

d) périodes de maintenance où des mises à jour, des correctifs, etc. sont installés et configurés (c.-à-d. fenêtres de maintenance);

e) un événement de force majeure;

f) les Points d'accès couverts sont postérieurs à la date de fin de la période d'assistance (EOS) ou ne sont pas couverts par l'assistance et la maintenance;

g) des erreurs logicielles nécessitant l'installation de mises à jour logicielles majeures ou la réinstallation du logiciel sur l'équipement Cisco;

h) les Modifications dans les Points d'accès couverts ou le réseau qui n'ont pas été validées ou approuvées par Cisco ou des retards du Client dans la mise en œuvre des Modifications demandées par Cisco ou autrement acceptées par le Client et Cisco;

i) le non-respect du Client à fournir la réponse exigée et nécessaire à Cisco pour respecter les Niveaux de service (Remarque : les dossiers d'Incident seront en « attente » lorsque Cisco ne reçoit pas les informations requises du Client, de l'Utilisateur final ou des fournisseurs de services tiers concernés dans les délais fixés);

j) les Modifications apportées aux Points d'accès couverts qui n'ont pas été approuvées par Cisco.

## 11. Audit de sécurité

En cas d'Incidents de sécurité répétés qui, selon Cisco, peuvent être évités grâce à une utilisation appropriée des Services et des Points d'accès couverts, Cisco peut procéder, à ses frais et à sa discrétion, à un examen de l'environnement de sécurité du Client. Le Client collaborera raisonnablement avec cet examen. Après un tel examen, le Client fera des efforts commercialement raisonnables pour mettre en œuvre toute recommandation raisonnable de Cisco. Si le Client ne le fait pas, ce SLA ne s'appliquera pas.

## 12. Gouvernance et procédure d'escalade

Cisco et le Client se réuniront régulièrement pour examiner et évaluer le Rendement du niveau de service, répondre aux préoccupations du Client et travailler de bonne foi pour résoudre tout différend entre les Parties concernant le Rendement du niveau de service.

## Annexe D : Niveaux de service, objectifs de niveau de service et indicateurs de rendement clés

**Disponibilité du portail**

**Définitions**

« **Disponibilité** » désigne ce qui suit, converti en pourcentage :

**Calcul** : (Nombre de minutes dans le mois - Temps d'interruption)/Nombre de minutes dans le mois.

**Disponibilité du portail** : il s'agit de la disponibilité du portail accessible sur le Web mis à la disposition du Client pour afficher les rapports et soumettre les dossiers.

La Période de panne commencera, selon la première de ces éventualités, à : 1) la détection de la panne par Cisco et l'enregistrement d'un dossier d'Incident ou 2) l'enregistrement par Cisco d'un dossier d'Incident à la réception d'une notification du Client concernant une panne et renfermant suffisamment d'information pour permettre à Cisco de confirmer que la panne se produit dans le système. La Période de panne prend fin lorsque le système est revenu à un Niveau de service utilisable. La durée de la Période de panne devra être arrondie à la minute près. Cisco enregistrera un dossier d'Incident rapidement après réception de la notification du Client ou de sa propre détection d'une panne.

**Niveau de service**

**Disponibilité de la plateforme** : 100 %

**Disponibilité du portail** : 99 %

**Crédit de service**

| Disponibilité de la plateforme | Crédit de service (% des frais de service mensuels fixes pour la Période de mesure) | Disponibilité du portail | Crédit de service (% des frais de service mensuels fixes pour la Période de mesure) |
|---|---|---|---|
| > 100 % et < 99,9 % | 1 % | < 99 % et > 98,5 % | 1 % |
| > 99,99 % et ≥ 99,9 % | 2 % | < 98,5 % et > 98 % | 2 % |
| > 99 % et < 98,5 % | 3 % | < 98 % et > 97,5 % | 3 % |
| > 98,5 % | 5 % | < 97,5 % | 5 % |

**Période de mesure :** Mensuellement (un mois civil)

**Temps d'engagement**

**Définition**

Cisco communiquera avec la personne-ressource désignée par le Client par téléphone ou par clavardage MSS dans les 30 minutes suivant la priorité d'un Incident de sécurité P1 (45 minutes pour un P2) si aucune recommandation d'atténuation, d'arrêt, de recherche, etc. n'a déjà été fournie.

**Calcul** : Cisco communique avec le Client dans les délais ci-dessus pour les Incidents P1 et P2 non résolus/Nombre total d'Incidents de sécurité P1 et P2 dans le mois qui nécessitent un engagement après la hiérarchisation (c.-à-d., aucune recommandation automatique fournie).

**Niveau de service** : engagement à temps 95 %

**Crédit de service**

| Disponibilité de la plateforme | Crédit de service (% des frais de service mensuels fixes pour la Période de mesure) |
|---|---|
| < 95 % et > 90 % | 1 % |
| < 90 % et > 80 % | 2 % |
| < 80 % et ³ 75 % | 3 % |
| < 75 % | 5 % |

**Période de mesure :** Mensuellement (un mois civil)