Description de l'offre – Produit
Secure Endpoint

La présente Description de l'offre fait partie des Conditions générales ou de toute autre condition similaire existant entre Vous et Cisco (p. ex., Contrat de licence d'utilisateur final) (le « **Contrat** »). Les termes commençant par une majuscule, sauf s'ils sont définis dans le présent document, ont la signification qui leur est donnée dans le Contrat. Les références au Contrat de licence de l'utilisateur final supplémentaire ou au CLUFS font référence à la Description de l'offre.

1. Résumé

Secure Endpoint. Cisco Secure Endpoint (le « **Produit** ») est une solution infonuagique avancée d'analyse des programmes malveillants et de protection contre ces programmes qui Vous permet d'effectuer des analyses des métadonnées de Fichiers dans le but de détecter les programmes malveillants et les cybermenaces. Des hachages cryptographiques des fichiers sont collectés et envoyés aux fins d'analyse de réputation de fichier, et un classement est effectué pour déterminer si le fichier est inoffensif, malveillant ou inconnu. Si un classement ne peut être effectué après l'analyse de hachage d'un fichier, Vous pouvez avoir l'option (selon les licences que vous possédez) de soumettre le fichier à Cisco Secure Malware Analytics pour une analyse en bac à sable plus poussée, jusqu'à votre limite quotidienne autorisée de soumissions. Le Produit est offert sous les formes Secure Endpoint Essentials, Advantage ou Premier.

1.1 **Secure Endpoint pour iOS**. Cisco Secure Endpoint pour iOS est une solution de sécurité infonuagique qui fournit visibilité et protection contre les menaces avancées sur les appareils iOS. Les renseignements relatifs aux applications et au réseau (c'est-à-dire les domaines, les adresses IP, les ports et les URL) provenant de Vos appareils iOS sont cernés et transmis à un serveur infonuagique géré par Cisco, où ils sont corrélés à d'autres renseignements pertinents sur les connecteurs de Cisco Secure Endpoint. L'utilisation de vos données corrélées, de Cisco Secure Endpoint pour iOS et de la console Cisco Secure Endpoint (la « **Console** ») vous permet de bénéficier d'une visibilité accrue sur les comportements inhabituels afin de mettre en évidence les appareils iOS susceptibles d'être visés par des activités suspectes. Les fonctionnalités de la Console et de la création de rapports peuvent être utilisées pour rechercher des activités suspectes sur Vos Terminaux.

1.2 **Nuage privé virtuel Cisco Secure Endpoint**. Le nuage privé virtuel Cisco Secure Endpoint offre une instance de nuage privé qui reste sur Votre site (le « **Nuage privé** ») et qui peut être configurée pour extraire des mises à jour du serveur infonuagique public géré par Cisco (le « **Nuage public** »). Vous pouvez choisir d'exécuter le nuage privé en mode « mandataire » ou en mode « isolement physique ». Si Vous choisissez le mode « mandataire », Vos hachages cryptographiques de Fichiers seront transmis de votre Nuage privé vers le Nuage public afin d'effectuer une analyse de la réputation des Fichiers. Si vous choisissez le mode « isolement physique », aucune donnée ne sera transmise au Nuage public; vos données resteront dans le Nuage privé.

1.3 **Orbital**. Cisco Secure Endpoint Advantage et Premier comprennent l'accès à Cisco Orbital, une fonctionnalité de recherche avancée qui fournit plus de cent requêtes prédéfinies et personnalisables. Vous pourrez ainsi exécuter rapidement des requêtes complexes sur n'importe quel terminal.

2. Services d'assistance et autres services

Assistance. Votre achat du Produit inclut le niveau Basic (de base) pour Cisco Software Support Services.

3. Protection des données

La Fiche technique sur la confidentialité de Cisco Secure Endpoint décrit les Renseignements personnels que Cisco recueille et traite dans le cadre de la livraison du Produit.

4. Conditions particulières

4.1 **Licence et restrictions des droits d'utilisation.** Cisco établit le nombre de licences du Produit en fonction du nombre de terminaux.

4.2 **Avis de non-responsabilité. Cisco ne fait aucune représentation et n'émet aucune garantie voulant que le produit procure une sécurité absolue, car les technologies utilisées pour effectuer des attaques et des intrusions malveillantes envers les fichiers, les réseaux et les points terminaux évoluent continuellement. Cisco ne fait aucune représentation et n'émet aucune garantie voulant que les produits protègent tous vos fichiers, vos réseaux et vos points d'extrémité contre tous les programmes malveillants, les virus et les attaques malveillantes de tiers.**

4.3 **Définitions**

« **Terminal** » : tout appareil capable de traiter des données qui peut accéder à un réseau, y compris des ordinateurs personnels, des appareils mobiles, des appareils iOS et des postes de travail de réseau.

« **Fichiers** » : les types de fichiers définis dans la documentation pertinente, tels qu'un fichier d'exécution, un fichier PDF, des documents Office de Microsoft (Word, Excel, PowerPoint) et les fichiers contenus dans une archive compressée (.ZIP).