Description de l'offre – Produit
Cisco Secure Email

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

La présente Description de l'offre décrit Cisco Secure Email Cloud Gateway (anciennement Cloud Email Security ou « CES »), Cisco Secure Email Encryption Service (anciennement Cisco Registered Envelope Service ou « CRES »), Cisco Secure Email Domain Protection (anciennement Cisco Domain Protection ou « DMP »), Cisco Secure Email Phishing Defense (anciennement Cisco Advanced Phishing Protection ou « APP ») et Cisco Secure Email Threat Defense (anciennement Cisco Cloud Mailbox Defense ou « CMD ») (collectivement, le « **Produit** »).

1.1 **Cisco Secure Email Cloud Gateway et Cisco Secure Email Encryption.** Cisco Secure Email Cloud est un service de sécurité pour la messagerie en nuage qui bloque les pourriels et les menaces à la sécurité provenant d'Internet. Ce Produit comprend l'option de licence pour Cisco Secure Email Encryption Service, qui aide les entreprises à sécuriser leurs communications par courriel en leur permettant d'envoyer des messages chiffrés par l'intermédiaire d'enveloppes enregistrées.

1.2 **Cisco Secure Email Domain Protection.** Cisco Secure Email Domain Protection permet d'empêcher les courriels d'hameçonnage d'être envoyés à l'aide d'un domaine du client. Ce produit automatise le processus de mise en œuvre de la norme d'authentification des courriels Domain Message Authentication Reporting and Conformance (« **DMARC** ») pour mieux protéger Vos employés, clients et fournisseurs contre les attaques par hameçonnage à l'aide d'un de Vos domaines. Cela protège l'identité de Votre marque et augmente l'efficacité du marketing par courriel en réduisant le nombre de messages d'hameçonnage qui atteignent les boîtes de réception.

1.3 **Cisco Secure Email Phishing Defense.** Cisco Secure Email Phishing Defense bloque les attaques basées sur la tromperie d'identité, telles que l'ingénierie sociale, les imposteurs et la compromission de courriels professionnels. Ce produit fournit aussi des outils locaux d'informations sur les courriels et des techniques avancées d'apprentissage automatique afin de créer des modèles de confiance pour le courriel sur Internet, au sein des entreprises et entre les utilisateurs. La protection de ce produit intègre des techniques d'apprentissage automatique pour faciliter la mise à jour quotidienne des modèles, maintenant une compréhension en temps réel du comportement des messages afin de contrer la tromperie d'identité. Cisco Secure Email Threat Defense.

1.4 **Cisco Secure Email Threat Defense.** Cisco Secure Email Threat Defense est un service de sécurité pour la messagerie en nuage qui bloque les pourriels et les menaces provenant d'Internet. Ses fonctionnalités comprennent un antipourriel, un antipourriel intelligent à analyse multiple, un antivirus, une détection antihameçonnage et une protection avancée contre les logiciels malveillants.

2. Services d'assistance et autres services

Assistance. Votre achat du Produit inclut Cisco Software Support Service.

3. Normes de performance

Contrat de niveau de service. Le Contrat de niveau de service pour Cisco Secure Email s'applique au Produit.

4. Protection des données

Fiche technique sur la confidentialité. Les fiches techniques sur confidentialité de Cisco Secure Email Gateway, Cisco Secure Email Cloud Gateway, Cisco Secure Email Threat Defense, Cisco Secure Email Domain Protection, Cisco Secure Email Encryption Service et Cisco Secure Email Phishing Defense (disponibles sur le portail Cisco Trust) décrivent les données personnelles que Cisco recueille et traite dans le cadre de la fourniture du Produit.

De plus, à Votre discrétion, Cisco Secure Cloud Gateway ou Cisco Secure Email Threat Defense peut envoyer les condensés de fichiers ou les fichiers envoyés à Cisco Secure Malware Analytics pour l'analyse des programmes malveillants et la recherche d'informations sur les menaces. Cela se produit uniquement si Vous choisissez d'activer l'intégration de Cisco Secure Malware Analytics dans Votre compte Cisco Secure Email Cloud Gateway ou Cisco Secure Email Threat Defense.

5. Conditions particulières

5.1 **Reconnaissance d'utilisation des données de Cisco Secure Email Domain Protection.** Cisco et ses sous-traitants peuvent utiliser ces données client relatives aux courriels dont l'authentification a échoué dans Cisco Secure Email Domain Protection (« **Données d'échec d'authentification** ») afin de fournir le Produit conformément aux modalités en vigueur dans le Contrat et la présente Description de l'offre. Sans limiter les droits stipulés dans le Contrat et dans la présente Description de l'offre, Cisco et ses sous-traitants peuvent compiler, agréger, publier, utiliser et partager des résumés anonymisés de ces Données d'échec d'authentification pendant et après la durée de l'abonnement afin de déterminer et de signaler les modèles d'utilisation du Produit, pour analyser et signaler les problèmes et les tendances liés à la sécurité, et pour améliorer et créer de nouveaux produits et des offres de service. Vous reconnaissez également que Cisco et ses sous-traitants qui participent à la prestation du Produit peuvent fournir une licence et fournir de telles données récapitulatives compilées et anonymisées (à l'exclusion de Vos renseignements confidentiels et des renseignements personnels permettant d'identifier une personne, le cas échéant) à Cisco, aux sous-traitants concernés ou à leur détenteur de licence ou à des fins d'utilisation interne pour effectuer la même opération, pendant et après la durée d'utilisation. Dans la mesure où Vous pourriez posséder des droits sur les Données d'échec d'authentification, vous devez fournir à Cisco (et aux sous-traitants qui participent à la prestation du Produit) une licence perpétuelle, gratuite et transférable permettant d'effectuer tout ce qui précède. Le présent paragraphe restera en vigueur en cas d'expiration ou de résiliation du contrat.

5.2 **Limite de licence et d'utilisation**

(A) La licence pour le Produit décrit dans la présente Description d'offre dépend de la quantité d'Utilisateurs couverts. Le terme « **Utilisateurs couverts** » signifie le nombre total de Vos employés, de Vos sous-traitants et d'autres individus autorisés qui sont connectés à Internet et couverts par Votre déploiement du Service infonuagique applicable.

(B) Si nous déterminons en toute bonne foi que Vous utilisez Cisco Secure Email Cloud Gateway ou Cisco Secure Email Threat Defense dans le cadre d'un service d'envoi de courriels en masse, Cisco peut Vous demander d'acheter des services supplémentaires ou de réorganiser Votre flux de messagerie afin d'exclure un des produits ou les deux du flux d'envoi de courriels en masse.

5.3 **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 déclaration et n'émet aucune garantie voulant que les produits protègent tous vos fichiers, vos réseaux et vos points terminaux contre tous les programmes malveillants, les virus et les attaques malveillantes de tiers. Les intégrations mises à votre disposition ne sont pas généralement des produits mis en marché inclus dans votre commande et sont fournies « tels quels ».**