

Plateforme Cisco Secure Workload

Août 2023

Table des matières

Présentation du produit	3
Scénarios de protection de la charge de travail	3
Fonctionnalités et avantages	4
Sauvegarde et récupération des données	6
Modèles de déploiement et échelle	7
Licences logicielles	10
Conditions de licence	11
Prise en charge et compatibilité	11
Renseignements sur la commande	11
Profitez de l'expertise de Cisco pour accélérer l'adoption	13
Durabilité de l'environnement Cisco	13
Cisco Capital	14
Pour en savoir plus	14
Historique du document	15

Cisco Secure Workload (anciennement Tetration) offre une microsegmentation Zero Trust fluide pour toutes les charges de travail, tous les environnements ou emplacements à partir d'une console unique. Grâce à une visibilité complète sur chaque interaction avec la charge de travail et à sa puissante automatisation basée sur l'intelligence artificielle et l'apprentissage automatique, Cisco Secure Workload réduit la surface d'attaque en empêchant le déplacement latéral, identifie les anomalies de comportement de la charge de travail, aide à corriger rapidement les menaces et supervise en permanence la conformité.

Présentation du produit

Traditionnellement, dans le secteur informatique, notre vision était centrée sur l'infrastructure. Nos données les plus précieuses se trouvaient dans le centre de données, et notre tâche consistait donc à laisser entrer le bon trafic et à empêcher les intrusions d'acteurs malveillants. Et notre outil de prédilection était le pare-feu.

Dans les entreprises d'aujourd'hui, le centre de gravité a résolument changé en faveur des applications. Les applications sont essentielles à la façon dont vous communiquez avec vos clients, gérez vos opérations et êtes payés. Mais la prolifération constante et la nature dynamique de ces applications ont créé un défi de sécurité sans précédent pour les professionnels de l'informatique.

Les applications sont distribuées. Elles sont déployées à la fois sur site et dans le nuage, ou sur plusieurs nuages, et les charges de travail critiques ne sont plus conservées dans le centre de données où elles peuvent être protégées par un pare-feu de périmètre. D'une certaine manière, on pourrait même considérer que le périmètre n'existe plus. Pour prospérer dans ce monde centré sur les applications, vous avez besoin d'une solution de sécurité capable de rapprocher la sécurité des applications à l'aide d'un « nouveau pare-feu ou micropérimètre » qui entoure chaque charge de travail, vous permettant de protéger ce qui compte le plus pour vous : vos applications et vos données.

Avec Cisco Secure Workload, vous pouvez sécuriser vos applications en créant des micropérimètres au niveau de la charge de travail pour l'ensemble de votre infrastructure de manière cohérente, qu'elles soient déployées sur des serveurs sans système d'exploitation, des machines virtuelles ou des conteneurs.

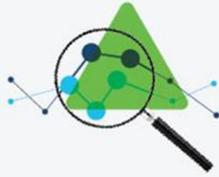
Scénarios de protection de la charge de travail

Cisco Secure Workload offre une microsegmentation Zero Trust pour protéger les applications, réduire les risques et maintenir la conformité grâce à :

- des politiques de microsegmentation générées automatiquement au moyen d'une analyse complète des schémas et des dépendances de communication des applications,
- la définition dynamique de politiques en fonction d'attributs avec un modèle de politique hiérarchique pour fournir des contrôles complets dans plusieurs groupes d'utilisateurs avec des contrôles d'accès basés sur le rôle,
- la mise en œuvre cohérente de politiques à grande échelle grâce au contrôle distribué des pare-feu et de l'infrastructure de l'hôte natif, y compris des contrôleurs de distribution d'applications (Application Delivery Controllers ou ADC) et des pare-feu,
- la supervision en temps quasi réel de la conformité de toutes les communications afin d'identifier une infraction à la politique ou une compromission potentielle, et d'émettre des alertes,
- la définition d'un ensemble de règles comportementales sur la charge de travail et la détection proactive des anomalies,
- la détection des vulnérabilités courantes grâce à l'atténuation dynamique et à la quarantaine basée sur les menaces.



Multidimensional Workload Protection Approach Using Cisco Secure Workload



Proactively identify threats with behavior analysis



Reduce attack surface with vulnerability detection



Contain lateral movement using microsegmentation

Figure 1.

Approche multidimensionnelle de protection de la charge de travail à l'aide de Cisco Secure Workload

Par cette approche multidimensionnelle de protection de la charge de travail (Figure 1), Cisco Secure Workload diminue considérablement la surface d'attaque, réduit le déplacement latéral en cas d'incidents de sécurité, et décèle plus rapidement les comportements anormaux dans le centre de données.

Pour en savoir plus sur les fonctionnalités de protection de la charge de travail et les scénarios d'utilisation, consultez la fiche technique de Cisco Secure Workload pour la protection de la charge de travail :

<https://www.cisco.com/c/en/us/products/collateral/data-center-analytics/tetration-analytics/datasheet-c78-740328.html>.

Fonctionnalités et avantages

Le tableau 1 énumère les principaux avantages et fonctionnalités de Cisco Secure Workload.

Tableau 1. Principaux avantages et fonctionnalités de Cisco Secure Workload

Fonctionnalité	Avantage
Concrétisation du niveau Zero Trust grâce à la microsegmentation	<ul style="list-style-type: none">• Concrétisez la mise en œuvre de la microsegmentation dans votre environnement.• L'approche automatisée de Cisco Secure Workload contribue à accélérer le déploiement de la microsegmentation.• Sécurisez les charges de travail multinuages hybrides et limitez le mouvement latéral grâce à la microsegmentation.
Élargissement des définitions de politiques en fonction du contexte supplémentaire	<ul style="list-style-type: none">• Éliminez les opérations fastidieuses de création manuelle de listes de ressources pour segmenter les applications.• Définissez des politiques par défaut et absolues de microsegmentation à l'aide d'étiquettes de ressources.• Élaborez rapidement des politiques cohérentes pour les applications à l'aide d'un étiquetage des ressources en temps réel :<ul style="list-style-type: none">◦ Associez le contexte opérationnel riche aux serveurs.• Définissez des politiques basées sur les utilisateurs et les groupes d'utilisateurs qui ont besoin d'un accès.

Fonctionnalité	Avantage
Mise en œuvre des politiques en un seul clic dans un centre de données multinuage	<ul style="list-style-type: none"> • Appliquez le cadre de sécurité en utilisant la segmentation des applications et réduisez la surface vulnérable aux attaques. • Appliquez des politiques en un seul clic. Utilisez les mécanismes des environnements Linux et Microsoft Windows pour appliquer la politique de sécurité. • Standardisez la politique pour chaque serveur, éliminant le besoin d'une intervention manuelle pour identifier la politique de chacun des serveurs.
Détection des événements de non-conformité des politiques	<ul style="list-style-type: none"> • Suivez la conformité des politiques des applications en temps réel. • Activez des alertes pour les événements de conformité qui peuvent ensuite être intégrées aux systèmes SIEM à des fins d'enquête et de correction.
Identification des écarts de comportement en matière de charge de travail	<ul style="list-style-type: none"> • Définissez une référence pour le comportement ou les charges de travail en fonction des activités et processus de communication sur les charges de travail. • Détectez de manière proactive les comportements anormaux et identifiez les indicateurs de compromission. • Activez des alertes pour ces événements afin de les intégrer à vos systèmes SIEM pour une gestion supplémentaire des incidents de sécurité.
Détection des vulnérabilités logicielles	<ul style="list-style-type: none"> • Obtenez un inventaire des logiciels de référence et les renseignements sur la version installée sur les serveurs. • Déterminez rapidement si l'une des versions du progiciel comporte des vulnérabilités ou des expositions connues, ainsi que la gravité. • Obtenez un inventaire précis de tous les serveurs sur lesquels le progiciel est vulnérable. • Associez ces renseignements à une politique qui désigne une action spécifique, telle que la mise en quarantaine d'un serveur spécifique.
Options flexibles de collecte des données télémétriques	<p>Agents logiciels :</p> <ul style="list-style-type: none"> • Capturez les activités de communication et de processus ainsi que les renseignements sur le progiciel pour identifier le comportement de référence de la charge de travail. • Conçus pour fonctionner dans le cadre d'ententes de niveau de service (Service Level Agreements ou SLA) pour le traitement des données définies par l'administrateur. • Se trouvent à l'extérieur du chemin des données et n'ont pas d'incidence sur les performances applicatives. • Prennent en charge les serveurs sans système d'exploitation, les machines virtuelles et les conteneurs. <p>Autres options :</p> <ul style="list-style-type: none"> • Capteurs ERSPAN. • Capteurs ADC - F5, Citrix NetScaler. • Capteurs NetFlow. • Journaux de flux du nuage privé virtuel AWS • Journaux de flux du nuage privé virtuel Azure • Journaux de flux du nuage privé virtuel Google
Terminal et contexte utilisateur	<ul style="list-style-type: none"> • Collectez les données télémétriques à partir d'un module Cisco AnyConnect® Network Visibility Module (NVM) s'exécutant sur des terminaux comme des ordinateurs portables, des postes de travail ou encore des téléphones intelligents, ou collectez des renseignements sur les terminaux à partir d'un environnement Cisco Identity Services Engine (ISE) ou VDI à l'aide d'agents logiciels Cisco Secure Workload. • Corréliez les données d'utilisateur avec le groupe d'utilisateurs au sein d'une entreprise. • Définissez des politiques propres à la segmentation, à l'aide des renseignements sur les utilisateurs et les groupes d'utilisateurs, qui peuvent être appliquées aux charges de travail.
Prise en charge de l'évolutivité du centre de données	<ul style="list-style-type: none"> • Recueillez des données télémétriques sur des dizaines de milliers de charges de travail dans un centre de données multinuage. • Offrez des fonctionnalités de microsegmentation et de protection de la charge de travail pour toutes les charges de travail. • Options de déploiement flexibles et évolutives conçues pour prendre en charge les centres de données de grande et de très grande taille.

Sauvegarde et récupération des données

Le scénario d'utilisation principal de la fonctionnalité de sauvegarde et de récupération des données consiste à restaurer, pendant une panne, une grappe vers une autre grappe sur le même site ou sur un autre site.

Tableau 2. Comparaison du mode de sauvegarde et de récupération des données et du mode Lean

Caractéristiques de la plateforme	Mode de sauvegarde complète	Mode Lean
Plateformes prises en charge	<ul style="list-style-type: none"> Option de plateforme Cisco Secure Workload (grand format). Cisco Secure Workload-M (petit format). 	Identique au mode de sauvegarde complète.
Type de stockage pris en charge	<ul style="list-style-type: none"> La sauvegarde et la restauration sont prises en charge à partir d'un entrepôt d'objets géré par le client avec une interface S3 compatible avec l'API S3V4, car la majeure partie des données copiées sont immuables, non évolutives et particulièrement adaptées aux entrepôts d'objets. La fonctionnalité de sauvegarde et de récupération des données peut fonctionner avec un entrepôt de données physique installé juste à côté de la grappe, avec un stockage dans le nuage comme AWS S3 dans le nuage ou avec tout emplacement accessible via une adresse IP. 	Identique au mode de sauvegarde complète.
Données sauvegardées	Toutes les sauvegardes seront synchrones et ponctuelles dans tous les entrepôts de données. Les données suivantes sont groupées en tant qu'objets et sauvegardées : une sauvegarde complète copie chaque objet d'un point de contrôle, même s'il est déjà copié et si l'objet n'a pas été modifié.	<p>Le mode de données Lean peut être activé pour exclure de la sauvegarde les données non liées à la configuration.</p> <p>Toutes les données, à l'exception des suivantes, sont sauvegardées :</p> <ul style="list-style-type: none"> Base de données des flux. Données obligatoires pour la découverte automatique des politiques. Politiques de mise en œuvre. Données pour faciliter l'investigation, comme les condensés de fichiers et les modèles de fuites de données. Données relatives à l'analyse de la surface d'attaque. Bases de données CVE.
Limites de stockage	Un stockage de 200 To est conseillé.	1 To est suffisant, car cela ne sauvegarde pas les flux.

Exigences de licence

Afin d'activer la fonctionnalité de sauvegarde et de récupération des données, un droit de licence sous la forme d'une clé d'activation est obligatoire pour l'objet principal (grappe active). La clé d'activation peut être obtenue en envoyant un courriel à ciscosecureworkload-licensing-support@cisco.com avec les renseignements d'identification de la grappe.

Modèles de déploiement et échelle

Cisco Secure Workload offre à la fois des logiciels-services (Software-as-a-Service ou SaaS) et des options sur site permettant aux clients de choisir le modèle qui répond à leurs besoins opérationnels.

Pour les déploiements sur site, les clients peuvent choisir un modèle d'appliance basé sur le matériel (petit ou grand format). Le choix de la plateforme dépendra de considérations relatives à l'évolutivité, y compris le nombre de charges de travail dans l'environnement et le niveau de fidélité souhaité de la télémétrie de flux.

Lorsqu'elle est configurée pour la seule télémétrie de flux de conversation sur toutes les charges de travail, chaque plateforme peut évoluer verticalement jusqu'à deux fois son échelle par défaut avec la télémétrie de flux détaillée activée. De plus, Cisco Secure Workload peut évoluer horizontalement pour répondre aux exigences des très grands environnements d'entreprises géographiquement dispersées grâce à la capacité de fédération.

Cisco Secure Workload offre également une capacité de reprise sur sinistre, grâce à des fonctionnalités de sauvegarde et de restauration en continu qui permettent aux clients de restaurer les données et les opérations sur une grappe de secours en cas de défaillance majeure ou de sinistre.

Option Cisco Secure Workload SaaS

Grâce à l'option Cisco Secure Workload SaaS, les clients peuvent bénéficier des fonctionnalités de protection de la charge de travail sans avoir à déployer ni à entretenir la plateforme sur site. Avec cette option, le logiciel Cisco Secure Workload s'exécute dans le nuage. Il est cependant géré et exploité par Cisco. Le client est responsable d'acheter les licences par abonnement nécessaires et de déployer les agents logiciels sur les charges de travail.

Cette option de déploiement est bien adaptée aux clients qui utilisent uniquement le logiciel-service ou qui lui donnent la priorité, car elle permet d'évoluer de manière flexible. Vous pouvez commencer petit et grandir à mesure que votre demande augmente. Autres avantages de l'option SaaS :

- Réduction importante du coût total d'acquisition (TCO).
- Rentabilisation plus rapide.

Le tableau 3 présente l'évolutivité vérifiée et prise en charge de l'option SaaS.

Tableau 3. Évolutivité de Cisco Secure Workload SaaS.

Caractéristiques de la plateforme	Fiche technique
Nombre maximal d'adresses IP pouvant être étiquetées par détenteur (CMDB uniquement)	6 000/100 licences (SaaS uniquement)
Nombre maximal de sous-réseaux pouvant être étiquetés par détenteur (CMDB uniquement)	120/100 licences (SaaS uniquement)
Nombre d'événements de flux pouvant être traités par seconde	5 000 flux par seconde/100 licences

Option Cisco Secure Workload-M (petit format)

Le tableau 4 présente les caractéristiques vérifiées et prises en charge. Le tableau 5 présente les exigences d'alimentation et de refroidissement pour la plateforme Cisco Secure Workload-M.

Tableau 4. Évolutivité de la plateforme Cisco Secure Workload-M.

Caractéristiques de la plateforme	Fiche technique
Nombre de charges de travail simultanées (machine virtuelle, sans système d'exploitation ou hôte de conteneur) à partir duquel les données de télémétrie peuvent être analysées	Jusqu'à 10 000 charges de travail en mode détaillé. Jusqu'à 20 000 charges de travail en mode conversation.
Nombre d'événements de flux pouvant être traités par seconde	Jusqu'à 500 000 flux par seconde
Nombre de détenteurs	7
Nombre de portées enfants par détenteur	1 000
Nombre total de portées enfants pour tous les détenteurs	7000
Nombre d'espaces de travail par détenteur	1 000
Nombre total d'espaces de travail pour tous les détenteurs	5 000
Nombre de filtres d'inventaire par détenteur	1 000
Nombre total de filtres d'inventaire pour tous les détenteurs	7000
Nombre de rôles par portée enfant	6
Nombre maximal d'adresses IP pouvant être étiquetées pour toutes les portées racines	500 000
Nombre maximal de sous-réseaux pouvant être étiquetés pour toutes les portées racines	50 000

Tableau 5. Caractéristiques d'alimentation et de refroidissement pour Cisco Secure Workload-M

Exigences de la plateforme	Appliance Cisco Secure Workload M5	Appliance Cisco Secure Workload M6
Puissance maximale	5,5 kW	6 kW
Exigence maximale de refroidissement	13 500 BTU par heure	14 171 BTU par heure
Caractéristiques du bâti	https://www.cisco.com/c/en/us/products/collateral/servers-unified-computing/r-series-racks/datasheet-c78-738217.html?cachemode=refresh .	

Option de plateforme Cisco Secure Workload (grand format)

Le tableau 6 présente les caractéristiques vérifiées et prises en charge. Le tableau 7 présente les exigences d'alimentation et de refroidissement pour la plateforme Cisco Secure Workload.

Tableau 6. Évolutivité de la plateforme Cisco Secure Workload grand format.

Caractéristiques de la plateforme	Fiche technique
Nombre de charges de travail simultanées (machine virtuelle, sans système d'exploitation ou hôte de conteneur) à partir duquel les données de télémétrie peuvent être analysées	Jusqu'à 25 000 charges de travail en mode détaillé. Jusqu'à 75 000 charges de travail en mode conversation.
Nombre d'événements de flux pouvant être traités par seconde	Jusqu'à 2 millions de flux par seconde
Nombre de détenteurs	35
Nombre de portées enfants par détenteur	5 000
Nombre total de portées enfants pour tous les détenteurs	35 000
Nombre d'espaces de travail par détenteur	3500
Nombre total d'espaces de travail pour tous les détenteurs	20 000
Nombre de filtres d'inventaire par détenteur	5 000
Nombre total de filtres d'inventaire pour tous les détenteurs	35 000
Nombre de rôles par portée enfant	6
Nombre maximal d'adresses IP pouvant être étiquetées pour toutes les portées racines	1 500 000
Nombre maximal de sous-réseaux pouvant être étiquetés pour toutes les portées racines	200 000

Tableau 7. Caractéristiques d'alimentation et de refroidissement pour la plateforme grand format

Exigences de la plateforme	Appliance Cisco Secure Workload M5	Appliance Cisco Secure Workload M6
Puissance de pointe pour l'option avec bâti unique*	22,5 kW	31,8 kW
Exigences de refroidissement maximales pour l'option avec bâti unique*	50 000 BTU par heure	72 117 BTU par heure
Poids total de l'option avec bâti unique	800 kg (1 800 lb)	800 kg (1 800 lb)
Puissance consommée et alimentation pour l'option avec bâti unique	4 x unités de répartition d'alimentation triphasées (les courants et les tensions nominatifs varient selon la zone géographique)	4 x unités de répartition d'alimentation triphasées (les courants et les tensions nominatifs varient selon la zone géographique)

Exigences de la plateforme	Appliance Cisco Secure Workload M5	Appliance Cisco Secure Workload M6
Puissance de pointe pour l'option avec bâti double	11,25 kW par bâti (22,5 kW au total)	15,9 kW
Exigences de refroidissement maximales pour l'option avec bâti double	25 000 BTU par heure et par bâti	36 059 BTU par heure et par bâti
Poids total de l'option avec bâti double	400 kg par bâti (900 lb par bâti)	400 kg par bâti (900 lb par bâti)
Puissance consommée et alimentation pour l'option avec bâti double	4 x unités de répartition d'alimentation monophasées par bâti (les courants et les tensions nominatifs varient selon la zone géographique)	4 x unités de répartition d'alimentation monophasées par bâti (les courants et les tensions nominatifs varient selon la zone géographique)
Caractéristiques du bâti	https://www.cisco.com/c/en/us/products/collateral/servers-unified-computing/r-series-racks/datasheet-c78-738217.html?cachemode=refresh	

Licences logicielles

La licence du logiciel Cisco Secure Workload est octroyée en fonction du nombre d'équivalents de charges de travail ou d'appareils (terminaux), selon le type d'agent ou de capteur utilisé. Les données de télémétrie peuvent être collectées à l'aide d'agents, soutenus par d'autres capteurs ou collecteurs pris en charge, dans n'importe quelle combinaison. L'application des politiques est permise par des agents avec des capacités de mise en œuvre, la mise en œuvre de l'infrastructure étant assurée par l'intégration de Cisco Secure Firewall, des contrôleurs ADC et des groupes de sécurité dans une infrastructure de nuage public ou orchestrée par la politique Kafka diffusée en flux continu. Une charge de travail est définie comme une machine virtuelle, un serveur sans système d'exploitation ou un hôte de conteneur, et comprend les systèmes d'exploitation de serveur et de poste de travail.

Il existe deux types de licence principaux pour Cisco Secure Workload (y compris les options SaaS et de déploiement sur site) :

- **Licence de protection Cisco Secure Workload** : cette licence fournit des fonctionnalités de protection de la charge de travail, y compris la collecte de données de télémétrie, l'observation des applications, l'investigation, la détection de vulnérabilités logicielles, la recommandation, la simulation et la mise en œuvre de politiques, ainsi que les fonctions de suivi de la conformité.
- **Licence de terminaux Cisco Secure Workload** : cette licence fournit la collecte complète de données de télémétrie à partir d'un client Cisco AnyConnect installé sur les terminaux (ordinateurs portables, postes de travail, téléphones intelligents, etc.) à l'aide d'un module NVM. Cela fournit des observations sur l'utilisateur, l'appareil, le groupe, l'ID de processus, la hiérarchie de processus et le système d'exploitation, ainsi que sur les noms de domaines accessibles à partir du terminal. De plus, cette licence fournit un contexte riche provenant des appareils des utilisateurs pour tout terminal géré par Cisco ISE via l'intégration PxGrid. Les clients doivent acheter la licence de visibilité des terminaux s'ils souhaitent utiliser la capacité de la plateforme à collecter, analyser et définir des politiques et fournir une visibilité sur les activités des terminaux. Cette licence peut être indépendante des licences de protection de la charge de travail. Cela n'inclut pas les autres licences nécessaires pour activer AnyConnect NVM ou Cisco ISE (ces licences doivent être achetées séparément).

Si un client dispose de plusieurs grappes Cisco Secure Workload, les licences logicielles peuvent être regroupées pour ces grappes.

Si un client dispose de licences Cisco Secure Workload SaaS, celles-ci ne peuvent pas être transférées vers une option de licence sur site, et inversement.

Conditions de licence

Déploiement de Cisco Secure Workload SaaS :

L'abonnement SaaS est régi par la Description de l'offre Cisco Secure Workload SaaS (https://www.cisco.com/c/dam/en_us/about/doing_business/legal/OfferDescriptions/cisco_tetration_saas_offer_description.pdf) et le Contrat Cisco Universal Cloud, accessible à l'adresse www.cisco.com/go/uca (ou des conditions semblables existant entre Cisco et vous) (le « Contrat »), et tout logiciel que vous installez est concédé sous licence en vertu des Conditions générales de Cisco disponibles à l'adresse www.cisco.com/go/eula (les « Conditions générales »).

Option de déploiement sur site :

Les abonnements Cisco Secure Workload sur site sont régis par les Conditions générales de Cisco (voir www.cisco.com/go/eula). En outre, le logiciel Cisco Secure Workload est soumis aux conditions du Contrat de licence utilisateur final supplémentaire de Cisco (CLUFS; voir www.cisco.com/c/dam/en_us/about/doing_business/legal/seula/cisco-secure-workload.pdf).

Prise en charge et compatibilité

Pour obtenir des renseignements détaillés sur la prise en charge et la compatibilité des systèmes d'exploitation pour Cisco Secure Workload, consultez les renseignements de prise en charge des plateformes à l'adresse www.cisco.com/c/en/us/products/security/tetration/platform-info.html.

Renseignements sur la commande

Le tableau 8 fournit les numéros de pièce de l'offre groupée de logiciels par abonnement utilisés pour l'option de déploiement Cisco Secure Workload SaaS.

Tableau 8. Offre groupée de logiciels pour l'option Cisco Secure Workload SaaS.

Numéro de pièce de l'offre groupée	Numéros de pièce inclus dans l'offre groupée	Description
C1-TAAS-SW-K9		Numéro de pièce de l'offre groupée Cisco Secure Workload qui comprend la licence par abonnement au logiciel pour l'option SaaS.
	C1-TAAS-WP-FND-K9	Numéro de pièce de l'offre groupée pour la licence par abonnement à la protection Cisco Secure Workload. La quantité minimale est de 100, et des incréments de 1 s'appliquent par la suite.
	C1-TAAS-ENDPT-K9	Licence par abonnement au logiciel pour la visibilité des terminaux Cisco Secure Workload pour les terminaux. Choisissez une quantité comprise entre 1 000 et 999 999. Par exemple, une quantité de 5 000 indiquera le prix de la licence pour un maximum de 5 000 terminaux suivis via Cisco AnyConnect ou Cisco ISE.

Notez également les renseignements supplémentaires suivants concernant le numéro de pièce de la licence par abonnement au logiciel :

- Vous pouvez sélectionner une durée d'abonnement de 1, 3 ou 5 ans.
- Le prix de l'abonnement comprend l'assistance logicielle.
- Vous pouvez sélectionner l'option de facturation annuelle, mensuelle ou trimestrielle, ou encore payer à l'avance pour toute la durée.
- Vous pouvez ajouter d'autres licences d'instance de charge de travail en modifiant l'abonnement.
- Cette licence par abonnement au logiciel peut être utilisée uniquement avec un déploiement Cisco Secure Workload SaaS.

Le tableau 9 présente les numéros de pièces de l'offre groupée de matériel et de logiciels pour l'option de plateforme Cisco Secure Workload-M.

Tableau 9. Offre groupée de matériel et de logiciels par abonnement pour l'option Cisco Secure Workload-M.

Numéro de pièce de l'offre groupée	Numéros de pièce inclus dans l'offre groupée	Description
C1-TETRATION-M		Numéro de pièce de l'offre groupée Cisco Secure Workload qui comprend la licence par abonnement pour le matériel et les logiciels.
	TA-CL-8U-M5-K9	Grappe 8RU Cisco Secure Workload de 2e génération.
	TA-CL-8U-M6-K9	Grappe 8RU Cisco Secure Workload de 3e génération.
	C1-TA-SW-K9	Numéro de pièce de l'offre groupée pour la licence par abonnement au logiciel Cisco Secure Workload; voir le tableau 9 pour en savoir plus.

Le tableau 10 présente les numéros de pièces de l'offre groupée de matériel et de logiciels pour l'option de plateforme Cisco Secure Workload.

Tableau 10. Offre groupée de matériel et de logiciels par abonnement pour l'option Cisco Secure Workload.

Numéro de pièce de l'offre groupée	Numéros de pièce inclus dans l'offre groupée	Description
C1-TETRATION		Numéro de pièce de l'offre groupée Cisco Secure Workload qui comprend la licence par abonnement pour le matériel et les logiciels.
	TA-CL-39U-M5-K9	Grappe 39RU Cisco Secure Workload de 2e génération.
	TA-CL-39U-M6-K9	Grappe 39RU Cisco Secure Workload de 3e génération.
	C1-TA-SW-K9	Numéro de pièce de l'offre groupée pour la licence par abonnement au logiciel Cisco Secure Workload; voir le tableau 9 pour en savoir plus.

Le tableau 11 présente les numéros de pièce de l'offre groupée de logiciels pour la licence par abonnement au logiciel Cisco Secure Workload.

Tableau 11. Licence par abonnement au logiciel pour les options de déploiement sur site de Cisco Secure Workload.

Numéro de pièce de l'offre groupée	Numéros de pièce inclus dans l'offre groupée	Description
C1-TA-SW-K9		Numéro de pièce de l'offre groupée pour la licence par abonnement au logiciel Cisco Secure Workload
	C1-TA-CWP-K9	Licence par abonnement Cisco Secure Workload sur site pour la protection de la charge de travail. La quantité minimale est de 100, et des incréments de 1 s'appliquent par la suite. Cette licence combine des capacités de base et de mise en œuvre antérieures. Par exemple, une quantité de 500 fournira la licence pour un maximum de 500 charges de travail.
	C1-TA-ENDPT-K9	La licence par abonnement au logiciel pour la visibilité des terminaux Cisco Secure Workload est commandée par incréments de 1 terminal. La quantité minimale obligatoire est de 1 000. Par exemple, une quantité de 1 505 fournira le prix de la licence pour 1 505 terminaux suivis via Cisco AnyConnect ou Cisco ISE.

Notez également les renseignements supplémentaires suivants concernant les numéros de pièce de la licence par abonnement au logiciel :

- Vous pouvez sélectionner une durée d'abonnement de 1, 3 ou 5 ans.
- Le prix de l'abonnement comprend l'assistance logicielle.
- Le niveau d'abonnement est sélectionné automatiquement en fonction de la quantité saisie.
- Vous pouvez sélectionner l'option de facturation annuelle ou payer à l'avance pour toute la durée.
- Vous pouvez ajouter d'autres licences d'instance de charge de travail en modifiant l'abonnement.
- Cette licence par abonnement au logiciel peut être utilisée avec les deux formes de grappes matérielles Cisco Secure Workload.

Votre licence pour le logiciel de terminal Cisco Secure Workload n'inclut pas de licence AnyConnect ou AnyConnect NVM. Vous êtes responsable de l'acquisition de ces licences séparément.

Profitez de l'expertise de Cisco pour accélérer l'adoption

Cisco fournit des services professionnels et de soutien, allant des conseils, de la mise en œuvre et de l'optimisation au soutien continu de solutions, pour aider les entreprises à tirer le meilleur parti de la plateforme Cisco Secure Workload. Les experts des services Cisco vous aident à intégrer la plateforme dans votre environnement de production du centre de données, à définir les cas d'utilisation adaptés à vos objectifs commerciaux, à configurer l'apprentissage automatique et à valider les politiques et la conformité pour améliorer les performances applicatives et les performances de fonctionnement. Le service d'assistance pour la solution Cisco Secure Workload offre une assistance matérielle, logicielle et pour l'ensemble de la solution. Nous proposons une sélection de services personnalisés à prix fixe et à étendue fixe pour Cisco Secure Workload qui vous garantissent une rentabilisation accélérée des investissements, l'adoption exhaustive dans votre environnement, des politiques et des performances applicatives optimisées, ainsi que l'assistance pour l'ensemble de la solution.

Durabilité de l'environnement Cisco

Des renseignements sur les politiques et les initiatives de Cisco en matière de durabilité environnementale pour nos produits, nos solutions, nos activités et nos activités étendues ou notre chaîne d'approvisionnement sont fournis dans la section « Durabilité de l'environnement » du [rapport sur la responsabilité sociale d'entreprise de Cisco](#) (CSR).

Les liens de référence vers des renseignements sur les principaux sujets de durabilité environnementale (mentionnés dans la section « Durabilité de l'environnement » du Rapport RSE) sont fournis dans le tableau suivant :

Sujet concernant la durabilité	Numéro de référence
Renseignements sur les lois et règlements sur le contenu des produits	Matériel
Renseignements sur les règlements concernant les déchets électroniques, notamment les produits, les batteries et les emballages	Conformité

Cisco rend les données relatives à l'emballage accessibles à titre informatif seulement. Il se peut qu'ils ne reflètent pas la situation juridique actuelle. Par conséquent, Cisco n'en garantit pas l'exhaustivité, l'exactitude ou la mise à jour. Les informations sont modifiables sans préavis.

Cisco Capital

Des solutions de paiement flexibles pour vous aider à atteindre vos objectifs

Cisco Capital facilite l'obtention des bonnes technologies pour atteindre vos objectifs, favorise la transformation de votre entreprise et vous aide à rester compétitif. Nous pouvons vous aider à réduire le coût total des droits de propriété, à économiser sur le capital et à accélérer la croissance. Dans plus de 100 pays, nos solutions de paiement flexibles peuvent vous aider à acquérir du matériel, des logiciels, des services et des équipements tiers complémentaires au moyen de paiements simples et prévisibles. [Pour en savoir plus.](#)

Pour en savoir plus

Pour plus de renseignements sur la plateforme Cisco Secure Workload, consultez la page <https://www.cisco.com/go/Secureworkload> ou communiquez avec votre représentant de compte Cisco local.

Historique du document

Nouveau sujet ou sujet révisé	Décrite dans	Date
Mise à jour des sections relatives à la présentation du produit, aux fonctionnalités clés, aux avantages et aux renseignements sur la commande pour inclure le contenu actualisé	Présentation du produit , fonctionnalités et avantages principaux , et renseignements sur la commande	30 janvier 2019
Mises à jour des systèmes d'exploitation pris en charge pour la visibilité et la mise en œuvre, et des conditions de licence	Renseignements sur la commande , conditions de licence et systèmes d'exploitation pris en charge	13 mai 2019
Mise à jour du document pour inclure les nouvelles fonctionnalités, les ID d'abonnement actualisés et les systèmes d'exploitation pris en charge	Fonctionnalités et avantages , renseignements sur la commande et systèmes d'exploitation pris en charge	20 juillet 2019
Mise à jour de la matrice de prise en charge des agents, spécifications matérielles de Cisco Secure Workload-V et intégration des caractéristiques de bâti pour les formats 39RU et 8RU	Systèmes d'exploitation pris en charge , option Cisco Secure Workload Virtual, option grand format Cisco Secure Workload et option petit format Cisco Secure Workload	24 février 2020
Document mis à jour pour reformuler les termes et la matrice de prise en charge des agents	Présentation du produit , fonctionnalités et avantages principaux , et systèmes d'exploitation pris en charge	16 juin 2020
Mise à jour de la présentation du produit, des fonctionnalités et avantages principaux, ainsi que de la matrice de prise en charge des agents	Présentation du produit , fonctionnalités et avantages principaux , et systèmes d'exploitation pris en charge	6 octobre 2020
Mise à jour des options de déploiement et de l'évolutivité, de la matrice de prise en charge des agents et des renseignements sur la commande		2 mars 2021



Siège social aux États-Unis
Cisco Systems, Inc.
San Jose, Californie

Siège social d'Asie-Pacifique
Cisco Systems (USA) Pte. Ltd.
Singapour

Siège social en Europe
Cisco Systems International BV Amsterdam,
Pays-Bas

Cisco compte plus de 200 bureaux à l'échelle mondiale. Les adresses, numéros de téléphone et de fax sont indiqués sur le site Web de Cisco à l'adresse suivante : <https://www.cosco.com/go/offices>.

Cisco et le logo Cisco sont des marques de commerce ou des marques de commerce déposées de Cisco ou de ses filiales aux États-Unis et dans d'autres pays. Pour consulter la liste des marques de commerce Cisco, rendez-vous à l'adresse URL suivante : <https://www.cisco.com/go/trademarks>. Les autres marques de commerce mentionnées appartiennent à leurs détenteurs respectifs. L'utilisation du terme « partenaire » ne signifie pas nécessairement qu'il existe un partenariat entre Cisco et une autre entreprise. (1110R)