Cisco Stealthwatch Enterprise

Pour le matériel UCS

Stealthwatch™ Enterprise est la solution leader en matière de visibilité et d'analyses de sécurité. Elle exploite les données de télémétrie de l'entreprise à partir de l'infrastructure réseau. Elle offre une détection avancée des malwares, elle accélère la réponse aux menaces et simplifie la segmentation du réseau à l'aide de l'apprentissage automatique multicouche et de la modélisation comportementale avancée, sur l'ensemble du réseau.

Avec Stealthwatch Enterprise, vous bénéficiez d'une visibilité en temps réel et ainsi d'informations précieuses sur les activités de votre réseau. Cette visibilité peut être étendue au cloud, à l'ensemble du réseau, aux sites distants, au data center et jusqu'aux terminaux.

Stealthwatch Enterprise intègre la licence Flow Rate, le collecteur de flux, la console de gestion et le capteur de flux. Pour bénéficier de fonctionnalités supplémentaires, consultez les fiches techniques suivantes :

- Licence Cisco Stealthwatch Endpoint : une licence complémentaire qui étend la visibilité aux périphériques des utilisateurs.
- Cisco Stealthwatch Cloud : une offre de produits permettant d'améliorer la visibilité et de détecter les menaces au sein d'infrastructures de cloud public telles qu'Amazon Web Services (AWS), Microsoft Azure et la plate-forme cloud Google.
- **Licence Threat Intelligence** : un flux d'informations à l'échelle mondiale collectées par Cisco Talos, l'équipe de Threat Intelligence leader du secteur, fournissant une couche supplémentaire de protection contre les botnets et autres attaques sophistiquées. Les activités suspectes de l'environnement réseau local sont mises en corrélation avec les données de milliers de campagnes et de serveurs contrôle-commande connus, pour assurer une détection ultraprécise et répondre plus vite aux menaces. Cisco Talos analyse 1,5 million d'échantillons de malwares uniques et bloque 20 milliards de menaces par jour.

Les bénéfices du système

Grâce à une vision et à une analyse uniques du trafic réseau, Stealthwatch Enterprise offre des améliorations significatives dans plusieurs domaines :

- Détection des menaces en temps réel
- Investigation et gestion des incidents
- Segmentation du réseau
- Performances du réseau et planification de la capacité
- Conformité aux exigences réglementaires

Les composants obligatoires du système

La licence Flow Rate

La licence Flow rate est requise pour la collecte, la gestion et l'analyse des données télémétriques et agrège les flux de données au niveau de la console de gestion. La licence Flow Rate définit également le volume des flux pouvant être collectés. Elle est octroyée sur la base du nombre de flux par seconde (FPS). Les licences peuvent être combinées de différentes manières pour prendre en charge le volume de flux requis.

Le collecteur de flux

Le collecteur de flux tire parti des données télémétriques de l'entreprise comme NetFlow, IPFIX et d'autres types de données comme celles des routeurs, des commutateurs, des pare-feu, des terminaux et d'autres périphériques de l'infrastructure réseau. Le collecteur de flux peut également recevoir et collecter des données télémétriques à partir des sources de données proxy, qui sont analysées par Global Threat Analytics (anciennement Cognitive Threat Analytics), un moteur d'apprentissage automatique multicouche, pour une visibilité approfondie sur le web et le trafic réseau. En outre, avec Encrypted Traffic Analytics, Stealthwatch Enterprise utilise l'analytique pour détecter les signes d'activité malveillante dans le trafic chiffré afin d'identifier les menaces et d'accélérer la riposte. Même si cette fonctionnalité est intégrée au système sans frais supplémentaires, vous devez l'activer lors du déploiement.

Les données télémétriques sont analysées afin d'offrir une visibilité complète sur l'activité du réseau. Vous pouvez stocker des mois, voire des années de données en créant une piste d'audit pour faciliter les recherches et les projets de conformité. Le volume de données télémétriques collectées à partir du réseau est déterminé par la capacité des collecteurs de flux déployés. Plusieurs collecteurs de flux peuvent être installés. Ils sont fournis sous la forme d'appliances matérielles ou de machines virtuelles. Le Tableau 1 présente les bénéfices du collecteur de flux.

Tableau 1. Principaux bénéfices du collecteur de flux

Bénéfice	Description
Détection des menaces	Regroupe les enregistrements de proxy et les associe aux enregistrements de flux afin d'afficher des informations contextuelles plus précises telles que les applications pour l'utilisateur et les adresses URL associées à chaque flux. Ce processus permet à votre entreprise de détecter les menaces de manière plus précise et plus rapide.
Surveillance des flux de trafic	Surveille simultanément les flux de trafic sur des centaines de segments du réseau pour identifier tout comportement suspect. Cette fonctionnalité est une arme précieuse pour les entreprises.
Plus longue conservation des données	Permet aux entreprises et aux organismes de conserver de grandes quantités de données pendant de longues périodes.
Évolutivité	Convient parfaitement aux environnements à très haut débit et protège chaque zone du réseau accessible par IP, peu importe son étendue.
Déduplication et convergence	Déduplique les données pour que chaque flux ayant transité par plus d'un routeur ne soit comptabilisé qu'une seule fois. Il fait ensuite converger les informations sur les flux pour offrir une visibilité totale sur chaque transaction réseau.
Options de déploiement multiples	La solution est disponible sous la forme d'une appliance matérielle qui s'adapte aux entreprises de toute taille. Vous pouvez également commander l'édition virtuelle, conçue pour offrir les mêmes fonctionnalités que l'édition matérielle, mais dans un environnement VMware. Elle offre une évolutivité dynamique selon les ressources qui lui sont affectées.

* Le nombre maximal de flux par seconde varie en fonction des conditions du réseau.

Les caractéristiques du collecteur de flux

- Collecteur de flux Stealthwatch 4200 – Référence : ST-FC4200-K9
- Collecteur de flux Stealthwatch 5200 – Référence : ST-FC5200-K9
- L'édition virtuelle du capteur de flux Stealthwatch peut être configurée comme FCVE-1000, FCVE-2000 ou FCVE-4000 – Référence : L-ST-FC-VE-K9

Remarque : Ces caractéristiques concernent le système Stealthwatch versions 6.9.1 et ultérieures

La console de gestion

La console de gestion Stealthwatch peut rassembler, organiser et présenter les analyses de 25 collecteurs de flux, de Cisco ISE (Identity Services Engine) et de bien d'autres sources. Elle utilise des représentations graphiques du trafic réseau, des informations sur les identités, des rapports de synthèse personnalisés et des informations intégrées sur la sécurité et le réseau pour un traitement analytique global.

La capacité de la console détermine le volume de données télémétriques pouvant être analysé et présenté, ainsi que le nombre de collecteurs de flux déployés. La console est disponible sous la forme d'une appliance matérielle ou virtuelle. Le Tableau 2 présente les bénéfices des consoles.

Tableau 2. Principaux bénéfices de la console de gestion

Bénéfice	Description
Flux de données en temps réel	Fournit un flux de données permettant la surveillance simultanée du trafic sur des centaines de segments du réseau et l'identification des comportements suspects. Cette fonctionnalité est une arme précieuse pour les entreprises.
Détection et hiérarchisation des menaces	Détecte et classe rapidement les menaces par ordre de priorité, identifie les utilisations frauduleuses du réseau et les performances insuffisantes, et gère le traitement des incidents pour l'ensemble de l'entreprise depuis un centre de contrôle unique.
Gestion des appliances	Configure, coordonne et gère les appliances Cisco Stealthwatch, notamment les collecteurs de flux, les capteurs de flux et UDP Director.
Utilisation de plusieurs types de données sur les flux	Exploite plusieurs types de données sur les flux, notamment les données NetFlow, IPFIX (Internet Protocol Flow Information Export) et sFlow. Résultat : une protection économique du réseau, basée sur les comportements.
Évolutivité	Répond aux exigences de tous les réseaux, quelles que soient leur taille et leur complexité. Convient parfaitement aux environnements à très haut débit et protège chaque zone du réseau accessible par IP, peu importe son étendue.
Pistes d'audit pour les transactions réseau	Fournit une piste d'audit complète de toutes les transactions réseau pour optimiser l'efficacité des enquêtes techniques.
Mappages de flux relationnels personnalisables et en temps réel	Fournit des représentations graphiques de l'état actuel du trafic réseau de l'entreprise. Les administrateurs peuvent facilement procéder au mappage de leur réseau à partir de divers critères comme l'emplacement, la fonction ou l'environnement virtuel. En créant une connexion entre deux groupes d'hôtes, les opérateurs peuvent rapidement analyser le trafic circulant entre ces deux groupes. Ensuite, il leur suffit de sélectionner un point de donnée spécifique pour bénéficier d'une meilleure visibilité sur ce qui se passe à un instant T.
Options de prestation souples	La solution est disponible sous la forme d'une appliance physique qui s'adapte aux entreprises de toute taille. Vous pouvez également commander l'édition virtuelle, conçue pour offrir les mêmes fonctionnalités que l'édition matérielle, mais dans un environnement VMware.

Les caractéristiques de la console de gestion

- Console de gestion Stealthwatch 2200 – Référence : ST-SMC2200-K9
- L'édition virtuelle de la console de gestion Stealthwatch peut être configurée comme SMC VE ou SMC VE 2000 – Référence : L-ST-SMC-VE-K9

Remarque : Ces caractéristiques concernent le système Stealthwatch versions 6.9.1 et ultérieures

Les composants facultatifs du système

Le capteur de flux

Le capteur de flux est un composant facultatif de Stealthwatch Enterprise qui génère des données télémétriques pour les segments de l'infrastructure de commutation et de routage qui ne peuvent pas générer de données NetFlow de façon native. Il fournit également une visibilité sur les données de la couche application. En plus de toutes les données télémétriques collectées par Stealthwatch, le capteur de flux fournit un contexte supplémentaire sur la sécurité pour améliorer l'analyse de la sécurité Stealthwatch. La modélisation comportementale avancée et l'apprentissage automatique multicouche dans le cloud sont appliqués à cet ensemble de données pour détecter les menaces avancées et accélérer les recherches.

Le capteur de flux est installé sur un port de mise en miroir ou un système de surveillance du réseau et génère des données télémétriques en fonction du trafic observé. Le volume des données télémétriques générées à partir du réseau est déterminé par la capacité des capteurs de flux déployés. Plusieurs capteurs de flux peuvent être installés. Ils sont fournis sous la forme d'appliances matérielles ou d'appliances virtuelles pour surveiller les environnements de machine virtuelle. Le capteur de flux est également utilisé dans les environnements où le modèle opérationnel de l'équipe IT requiert une solution de surveillance sur plusieurs couches offrant un contexte supplémentaire sur la sécurité.

Le Tableau 3 présente les principaux bénéfices du capteur de flux.

Tableau 3. Principaux bénéfices du capteur de flux

Bénéfice	Description
Visibilité sur les applications de couche 7	Fournit une vraie visibilité sur les applications de couche 7 en collectant à la fois des informations sur les applications et des captures de paquets ponctuelles à la demande (PCAP). Ces informations incluent les caractéristiques des données, telles que la durée de transmission, le temps de réponse du serveur et les retransmissions.
Statistiques de performance et analyse au niveau des paquets	Fournit une vraie visibilité sur les applications de couche 7 en collectant à la fois des informations sur les applications et des captures de paquets ponctuelles à la demande (PCAP). Ces informations incluent les caractéristiques des données, telles que la durée de transmission, le temps de réponse du serveur et les retransmissions.
Alertes en cas de détection d'anomalies sur le réseau	Les autres données télémétriques du capteur de flux, comme les URL de trafic web et les indicateurs TCP, génèrent des alarmes avec des informations contextuelles afin que le personnel de sécurité puisse rapidement prendre des mesures et limiter les dommages.
Réduction des coûts	Améliore l'efficacité opérationnelle et réduit les coûts en identifiant et en isolant en quelques secondes la cause première de l'incident.
Options de déploiement multiples	La solution est disponible sous la forme d'une appliance matérielle qui s'adapte aux entreprises de toute taille. Vous pouvez également commander l'édition virtuelle conçue pour offrir les mêmes fonctionnalités que l'édition matérielle, mais dans un environnement VMware ou d'hyperviseur KVM.

*Ces chiffres sont générés dans nos environnements de test avec les données client moyennes.

Les caractéristiques du capteur de flux

- Capteur de flux Stealthwatch 1200 – Référence : ST-FS1200-K9
- Capteur de flux Stealthwatch 2200 – Référence : ST-FS2200-K9
- Capteur de flux Stealthwatch 3200 – Référence : ST-FS3200-K9
- Capteur de flux Stealthwatch 4200 – Référence : ST-FS4200-K9
- Édition virtuelle du capteur de flux Stealthwatch – Référence : L-ST-FS-VE-K9

Remarque : Ces caractéristiques concernent Cisco Stealthwatch versions 6.9.1 et ultérieures

UDP Director

L'appliance UDP Director simplifie la collecte et la distribution des données de réseau et de sécurité à l'échelle de l'entreprise. Elle réduit la puissance de traitement au niveau des routeurs et des commutateurs du réseau en recueillant les informations de sécurité et de réseau stratégiques provenant de diverses sources et en les transmettant vers une ou plusieurs destinations sous la forme d'un flux de données unique. Le Tableau 4 présente les principaux bénéfices d'UDP Director.

Tableau 4. Principaux bénéfices d'UDP Director

Bénéfice	Description
Moins d'interruptions non prévues et d'interruptions de service	La haute disponibilité est prise en charge sur l'appliance UDP Director 2200.
Simplifie les opérations de surveillance et de protection du réseau.	UDP Director est le point de collecte centralisé des données NetFlow, sFlow, SNMP et du journal système. Les appliances UDP Director peuvent recevoir des données de toutes les applications UDP hors connexion, puis les retransmettre à plusieurs destinataires en dupliquant les données le cas échéant.
Acheminement des données UDP de tout type de source vers tout type de destination	Reçoit les données des applications UDP hors connexion, puis les retransmet à plusieurs destinataires en dupliquant les données le cas échéant.
Aucune reconfiguration de l'infrastructure	Achemine les données de journal (NetFlow, sFlow, journal système, SNMP) vers une destination unique sans que l'infrastructure ait besoin d'être reconfigurée lorsque de nouveaux outils sont ajoutés ou supprimés.

Les caractéristiques d'UDP Director

- Stealthwatch UDP Director 2200 – Référence : ST-UDP2200-K9
- Édition virtuelle de Cisco Stealthwatch UDP Director – Référence : L-ST-UDP-VE-K9

Pour commander

Le guide de commande du système Cisco Stealthwatch comprend toutes les informations relatives aux modèles, aux composants et aux types de licences disponibles. Pour passer commande, contactez votre conseiller.

Service et assistance

Un certain nombre de programmes sont proposés pour l'assistance technique du système Cisco Stealthwatch. Ils vous permettent de protéger vos investissements en matière de réseau, d'optimiser le fonctionnement du réseau et de le préparer à accueillir de nouvelles applications pour le rendre plus intelligent et favoriser le succès de votre entreprise. Pour plus d'informations sur les services aux entreprises, rendez-vous sur la page Assistance technique.

Cisco Capital

L'offre de financement Cisco Capital® peut vous aider à acquérir la technologie dont vous avez besoin pour atteindre vos objectifs et rester compétitif. Nous pouvons vous aider à réduire vos CapEx, à accélérer votre croissance, et à optimiser vos investissements et votre ROI. L'offre de financement Cisco Capital permet une certaine flexibilité pour l'achat de matériel, de logiciels, de services et d'équipements tiers complémentaires. Le montant du paiement est connu à l'avance. L'offre de financement Cisco Capital est disponible dans plus de 100 pays. En savoir plus.

Informations complémentaires

Pour en savoir plus sur Cisco Stealthwatch, rendez-vous sur https://www.cisco.com/go/stealthwatch ou contactez votre conseiller Cisco pour découvrir comment votre entreprise peut gagner en visibilité sur l'ensemble de son réseau en participant à une évaluation gratuite de la visibilité Stealthwatch.

Siège social aux États-Unis
Cisco Systems. Inc.
San José. CA

Siège social en Asie-Pacifique
Cisco Systems (États-Unis) Pte. Ltd.
Singapour

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

Cisco compte plus de 200 agences à travers le monde. Les adresses, numéros de téléphone et de fax sont répertoriés sur le site web de Cisco, à l'adresse : **www.cisco.com/go/offices**.

Imprimé aux États-Unis C78-739398-03 04/18