Cisco Stealthwatch

Améliorer la visibilité dans toute votre entreprise

Connaître tous les hôtes

Enregistrer chaque conversation

Comprendre les activités normales

Être alerté des changements

Réagir rapidement aux menaces

La protection des entreprises numériques exige une visibilité accrue

Aujourd'hui, le réseau d'entreprise se développe rapidement. Il connecte différentes succursales, les utilisateurs mobiles, le cloud et les data centers. Les entreprises se détournent des infrastructures IT classiques, leur préférant une infrastructure réseau prête pour le numérique. Beaucoup d'entreprises tirent profit de la numérisation, de la rationalisation des opérations à la gestion des stocks, en passant par l'offre de services à valeur ajoutée.

Toutefois, plus elles se transforment en entreprises numériques et adoptent de nouvelles pratiques et technologies, plus elles doivent optimiser la visibilité pour protéger leurs activités.

76 % des professionnels de l'informatique déclarent que la visibilité est leur principal défi.
Source : Ponemon Institute

Bénéfices

- **Profitez d'une visibilité** sur l'ensemble du trafic réseau, y compris sur les trafics est-ouest et nord-sud, afin de détecter les attaques internes et externes
- **Exécutez des analyses de sécurité avancées** et collectez des informations contextuelles étendues pour détecter un large éventail de comportements anormaux pouvant correspondre à une attaque
- **Accélérez et optimisez la détection des attaques,** la gestion des incidents et l'analyse sur tout le réseau, y compris le trafic chiffré
- **Procédez à des enquêtes techniques approfondies** via des antécédents de vérification de l'activité réseau
- **Simplifiez** la segmentation du réseau, la surveillance des performances et la planification de la capacité
- **Garantissez la conformité de l'entreprise** en identifiant l'étendue et la qualité du chiffrement sur le réseau
- **Optimisez la visibilité et la détection des anomalies** avec la corrélation du trafic mondial et local
- **Identifiez les menaces internes** en obtenant des informations contextuelles à partir des services cloud

Cisco Stealthwatch

Surveiller · Détecter · Analyser · Agir

Réseau étendu

Data center

Site distant

Cloud

Cisco Stealthwatch fournit une surveillance continue en temps réel et une visibilité complète du trafic réseau. Cette solution améliore considérablement la visibilité sur le réseau étendu et accélère les délais de réponse en cas d'incidents suspects. Elle crée un point de comparaison pour évaluer la normalité des activités web et réseau par rapport à l'hôte réseau de référence et recourt à l'analyse contextuelle pour détecter automatiquement les comportements anormaux. StealthWatch identifie de très nombreuses formes d'attaques, y compris les malwares, les attaques de type « zero-day », les attaques par déni de service distribué, les attaques persistantes avancées et les menaces internes.

Maintenant, avec Cognitive Analytics, une fonctionnalité d'analyse et de détection des menaces basée dans le cloud, Cisco Stealthwatch obtient des informations contextuelles supplémentaires pour identifier et hiérarchiser toutes les menaces, nouvelles et émergentes, sur l'ensemble du réseau. Stealthwatch avec Cognitive Analytics permet d'avoir plus de visibilité et d'informations contextuelles sur le trafic mondial et local et utilise l'apprentissage automatique pour analyser et détecter en continu le trafic de type commande-contrôle. Il est maintenant possible de détecter les menaces ayant échappé aux contrôles de sécurité et d'identifier l'exfiltration des données vers des services cloud légitimes.

L'analyse du trafic chiffré pour améliorer la sécurité

En matière de sécurité, le chiffrement est important. Mais bien que vous puissiez utiliser le chiffrement pour protéger les données et la confidentialité, les hackers s'en servent pour masquer les malwares et échapper à la détection. Cisco Stealthwatch et ses fonctionnalités d'analyse améliorées vous permettent de comprendre si le trafic chiffré sur le réseau est malveillant. Stealthwatch applique l'apprentissage automatique et la modélisation statistique pour les métadonnées intraflux ou utilise Encrypted Traffic Analytics pour améliorer l'analyse NetFlow. Cognitive Analytics apprend à partir de ce qu'il voit et s'adapte aux changements de comportement du réseau sur le long cours.

Stealthwatch avec Cognitive Analytics améliore la visibilité sur les flux de trafic en centralisant la gestion du réseau et le trafic web dans la Console de gestion. Plutôt que de déchiffrer le trafic, Stealthwatch avec Cognitive Analytics détecte les schémas malveillants dans le trafic chiffré afin d'identifier les menaces et d'accélérer la riposte.

À l'aide de la solution Encrypted Traffic Analytics, Stealthwatch assure la conformité avec les protocoles cryptographiques et fournit une visibilité accrue sur les éléments chiffrés et non chiffrés de votre réseau.

La visibilité étendue au cloud

Les workloads sont de plus en plus pris en charge dans des clouds. Si les bénéfices sont réels en termes de souplesse pour l'entreprise, il est également plus difficile de surveiller les flux de trafic dans ces instances virtuelles. Heureusement, StealthWatch permet d'étendre la visibilité et les fonctionnalités de détection des menaces et d'analyse aux environnements de cloud public, privé et hybride. Vous bénéficiez d'une visibilité en temps réel et d'une sécurité renforcée sur l'ensemble de votre infrastructure.

La visibilité étendue aux terminaux

Dans notre monde connecté, la mobilité est la clé. Les utilisateurs sont de plus en plus nombreux à se connecter aux réseaux d'entreprise avec un nombre croissant de terminaux, depuis des endroits toujours plus variés. Mais pour véritablement surveiller toutes les activités réseau, les professionnels de la sécurité doivent observer les applications et les processus en périphérie du réseau, jusqu'aux périphériques à distance. Avec la licence Cisco Stealthwatch Endpoint, les professionnels de la sécurité exécutent des analyses contextuelles plus performantes sur les ordinateurs des utilisateurs

« À chacune de mes missions, quand je dois savoir ce qui s'est passé ou ce qui se passe sur un réseau spécifique, Stealthwatch est d'une aide précieuse. ... Pour mon équipe, la plus grande qualité de Stealthwatch, c'est qu'il surveille le réseau en permanence, même lorsque nous ne nous en occupons pas. »

Phil Agcaoili.
RSSI, Elavon. En savoir plus

ayant un comportement suspect, accélèrent la gestion des incidents et éliminent rapidement les infractions à la politique.

Visibilité étendue aux succursales

Il peut être complexe et coûteux de surveiller le réseau de vos succursales, notamment lorsqu'elles occupent plusieurs sites. La licence Cisco Stealthwatch Learning Network est une solution économique d'extension de la sécurité du réseau aux succursales et aux réseaux distants. Tirez parti de vos investissements dans les technologies réseau Cisco en utilisant les données NetFlow générées par les équipements Cisco pour améliorer la visibilité et la sécurité de votre réseau. Il intègre la détection des anomalies de sécurité dans les éléments du réseau eux-mêmes, à l'aide de la capture de paquets et de détecteurs intelligents, afin d'identifier, de contrôler et d'éliminer les menaces. Cette solution accroît la visibilité sans affecter la bande passante et limite les interactions et les mouvements de données aux situations où une intervention est requise.

Une sécurité conçue pour la collaboration

Cisco Stealthwatch améliore la visibilité sur l'ensemble de l'entreprise en tirant parti de votre infrastructure réseau. Cette solution convertit les données NetFlow en informations exploitables et transforme votre réseau en capteur. Le gain de visibilité ainsi obtenu sur l'ensemble du trafic réseau vous permet d'identifier les menaces potentielles.

En intégrant Stealthwatch à d'autres solutions de sécurité Cisco, vous améliorez la segmentation, la détection des menaces et les fonctionnalités d'analyse sur vos réseaux WAN, vos succursales, vos data centers et le cloud.

L'intégration de Cisco Stealthwatch avec Cisco ISE (Identity Services Engine) permet aux entreprises d'obtenir une vue à 360° de leur réseau étendu. Vous bénéficiez ainsi d'une visibilité unique sur l'intégralité de votre entreprise en utilisant votre réseau comme capteur, vous simplifiez la segmentation sur l'ensemble de vos réseaux avec le contrôle centralisé et la mise en application de la politique et vous ripostez aux attaques plus rapidement, de façon proactive avec la détection des menaces et rétroactive avec l'analyse avancée.

Cisco a combiné les fonctionnalités d'analyse NetFlow et d'analyse de paquets. Nous avons intégré Cisco Stealthwatch et Cisco Security Packet Analyzer, l'analyseur de paquets de sécurité Cisco. Ces deux technologies facilitent la résolution des problèmes liés à la sécurité et la gestion des incidents réseau, mais l'une est souvent sacrifiée au bénéfice de l'autre, généralement pour des questions de budget ou de manque de ressources. Notre approche ciblée vous permet de stocker uniquement les paquets d'intérêt, réduisant les coûts de stockage tout en fournissant un enregistrement contextuel plus détaillé des événements survenus sur le réseau. La visibilité accrue et le contexte supplémentaire fournis par NetFlow se combinent avec une solution plus économique et plus précise d'obtention des données au niveau des paquets pour vous permettre d'approfondir l'analyse d'un problème spécifique si besoin.

Étapes suivantes

Pour en savoir plus, consultez le site http://www.cisco.com/go/stealthwatch ou contactez votre conseiller Cisco local.

Cisco Stealthwatch

- Une visibilité étendue sur le périmètre du réseau, le réseau interne, le data center et les clouds publics et privés, jusqu'aux terminaux
- Une meilleure compréhension de ce qui constitue un comportement normal sur le réseau, avec NetFlow qui établit un point de comparaison afin d'identifier facilement les comportements anormaux
- Un contrôle continu des terminaux, des applications et des utilisateurs sur les réseaux distribués
- Des analyses de sécurité avancées et des informations exploitables pour détecter un large éventail de comportements pouvant correspondre à une attaque
- Un traitement accéléré des incidents grâce à une détection des attaques en temps réel
- Des investigations plus approfondies basées sur des pistes d'audit complètes
- Des fonctionnalités simplifiées pour la segmentation du réseau, la validation de la conformité, la résolution des problèmes et les diagnostics