# StealthWatch optimise les solutions de défense grâce à une visibilité et à une protection intégrales

**BÉNÉFICES**

- Profitez d'une visibilité sur l'ensemble des conversations du 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 afin de réduire les risques pour votre entreprise
- Procédez à des enquêtes techniques approfondies via des antécédents de vérification de l'activité du réseau
- Simplifiez la gestion de la conformité, la segmentation du réseau, le contrôle des performances et la planification de la capacité en ayant une visibilité sur l'ensemble du réseau

Si vous souhaitez bénéficier d'une visibilité complète sur vos réseaux internes et distribués, nous avons la solution qu'il vous faut. Grâce à une analyse avancée des comportements sur le réseau, le système StealthWatch transforme les données collectées en informations exploitables. Vous renforcez ainsi votre sécurité et pouvez traiter les incidents plus rapidement.

Les réseaux d'entreprise n'ont jamais été aussi complexes et distribués qu'aujourd'hui, et de nouveaux malwares apparaissent chaque semaine. Le développement des malwares, mais aussi le cloud computing et l'Internet des objets, viennent fragiliser une situation déjà préoccupante. Malheureusement, avec la multiplication des utilisateurs et des terminaux, il devient de plus en plus difficile de savoir ce qu'il se passe sur le réseau. Et vous ne pouvez pas protéger ce que vous ne voyez pas.

Avec StealthWatch, ce problème n'en est plus un. En collectant et en analysant de très grandes quantités de données, ce système offre une protection avancée et une visibilité complète sur tous les réseaux, même les plus étendus et les plus dynamiques. Les équipes en charge de la sécurité bénéficient ainsi d'une visibilité en temps réel sur les utilisateurs, les terminaux et le trafic du réseau qui leur permet de réagir efficacement et rapidement en cas d'attaque.

Grâce à une surveillance continue et aux données collectées par le système StealthWatch, vous pouvez détecter un large éventail d'attaques. Vous pouvez repousser les attaques de type « zero-day », les attaques internes, les attaques persistantes avancées, les attaques par déni de service distribué (DDoS) et d'autres types d'attaques avant qu'elles n'endommagent votre réseau. Contrairement aux autres solutions de surveillance, StealthWatch surveille non seulement le trafic entrant et sortant du réseau, mais également le trafic interne latéral (est-ouest) afin d'identifier tout comportement anormal ou toute menace interne au réseau.

## Plus d'attaques, moins de visibilité

Les secteurs publics et privés font aujourd'hui face à une multiplication des cyberattaques. Les solutions de sécurité classiques, telles que les pare-feu, les antivirus et les systèmes de prévention des intrusions (IPS) ne parviennent plus à protéger les informations confidentielles contre les cybercriminels. Peu importe le nombre de technologies déployées à la périphérie du réseau, les hackers trouveront toujours un moyen d'y accéder. Ils utilisent notamment des attaques de type « zero-day », des identifiants d'accès volés, des terminaux mobiles infectés ou une vulnérabilité chez un partenaire commercial.

Le piratage en tant que tel est d'ailleurs de moins en moins répandu. Les hackers se contentent de trouver des identifiants pour se connecter. Il leur suffit d'exploiter la crédulité d'un employé pour accéder au réseau comme un utilisateur interne. Avec la montée du piratage psychologique, de plus en plus de collaborateurs peuvent représenter un risque interne, souvent à leur insu. Les entreprises, trop occupées à sécuriser le périmètre du réseau, ne parviennent pas à détecter assez rapidement un hacker déjà infiltré sur le réseau.

Pour gagner cette cyberguerre, vous devez savoir ce qu'il se passe à l'extérieur mais aussi à l'intérieur de votre réseau. Ce constat est aujourd'hui plus vrai que jamais. Plus de 80 % du trafic réseau circule d'est en ouest au sein du data center et ne sort jamais du périmètre. Malheureusement, les technologies de sécurité classiques telles que les solutions de gestion des informations et des événements de sécurité (SIEM) et la capture intégrale des paquets offrent peu de visibilité sur le réseau interne. De plus, ces approches ne sont souvent pas adaptées à des déploiements de grande envergure.

## L'architecture StealthWatch et ses composants

L'architecture StealthWatch à deux niveaux du système se compose d'appliances collecteur de flux StealthWatch et console de gestion StealthWatch. Ces composants sont déployés sous la forme d'appliances physiques ou virtuelles avec des licences de collecte de flux.

Le capteur de flux StealthWatch fournit une visibilité complète sur le réseau, ainsi que des indicateurs de performances des serveurs via une inspection approfondie des paquets. Si le réseau de l'entreprise ne prend pas en charge la solution NetFlow, le capteur FlowSensor est déployé en tant qu'appliance pour générer des données de télémétrie. Ces données sont transmises à un collecteur de flux (FlowCollector) qui procède à une analyse des comportements. Celui-ci peut ainsi identifier les applications et les protocoles utilisés afin d'optimiser la sécurité, les opérations du réseau et les performances applicatives.

Grâce aux collecteurs de flux, le système StealthWatch peut stocker et analyser plus de 4 000 sources de données télémétriques avec un débit de 240 000 flux par seconde. Jusqu'à 25 collecteurs de flux peuvent être déployés sur un même réseau pour prendre en charge jusqu'à six millions de flux par seconde.

> « Avec la solution StealthWatch, quelques secondes suffisent pour résoudre un problème, alors que plusieurs jours étaient nécessaires auparavant. Elle nous permet d'anticiper les risques potentiels et les attaques. »
> **— Edge Web Hosting**

## Les principales fonctionnalités

StealthWatch s'appuie sur votre infrastructure pour fournir une visibilité et des informations de veille complètes sur tout votre réseau.

### Une surveillance continue du réseau

En sachant exactement ce qu'il se passe sur leur réseau, les entreprises de tout type et de toute taille peuvent avoir une vision précise des comportements normaux au sein de leur environnement, ce qui les aide à déceler plus facilement les comportements suspects. Elles peuvent également identifier et segmenter au mieux les ressources réseau stratégiques afin de renforcer le contrôle d'accès et les systèmes de protection.

### Une détection précoce des attaques

Le système StealthWatch prend en compte les données contextuelles pour détecter automatiquement les comportements anormaux. Il est capable d'identifier un large éventail d'attaques, notamment les programmes malveillants, les attaques de type « zero-day », les attaques par déni de service distribué, les attaques persistantes avancées et les menaces internes. Contrairement aux autres solutions de surveillance, StealthWatch surveille non seulement le trafic entrant et sortant du réseau, mais également le trafic latéral (est-ouest). Il peut ainsi détecter toute utilisation frauduleuse du réseau ainsi que les hackers qui y opèrent.

### Des investigations après l'incident

StealthWatch propose bien plus qu'une détection avancée et en temps réel des malwares. Il réduit de façon significative les délais de réponse en cas d'incident, limitant le dépannage à quelques minutes, contre quelques jours ou quelques mois avec d'autres solutions de sécurité. Les données du réseau qui peuvent être stockées pendant des mois, voire des années, représentent une piste d'audit inestimable qui garantit une très grande précision des analyses techniques après incident menées par StealthWatch.

Si StealthWatch offre une visibilité complète sur le trafic du réseau, il propose également plusieurs niveaux de données contextuelles : l'identification des utilisateurs et des terminaux, la visibilité sur le cloud, la reconnaissance des applications et des flux de données sur les malwares.

### StealthWatch et les autres technologies de sécurité

StealthWatch collecte et analyse les données de télémétrie réseau comme les flux (NetFlow, sFlow, JFlow, etc.) provenant de vos routeurs, commutateurs et pare-feu afin de surveiller le comportement du réseau et des utilisateurs. Le système applique des méthodes propriétaires sophistiquées pour analyser les données du réseau et détecter automatiquement les comportements anormaux pouvant correspondre à une attaque.

Le système StealthWatch est parfois comparé à d'autres solutions de surveillance comme les solutions de gestion des informations et des événements de sécurité (SIEM) et la capture intégrale des paquets. La technologie SIEM analyse le journal système des ressources du réseau et envoie des alertes et des alarmes à partir d'outils basés sur les signatures. Malheureusement, le journal système provenant de machines infectées n'est pas fiable et les outils de surveillance basés sur les signatures, qui ne peuvent pas détecter les éléments auxquels ils n'ont pas accès, peinent à identifier les changements de comportement.

Quant à la capture intégrale des paquets, elle peut être déployée uniquement dans certaines zones du réseau en raison de sa complexité et de son coût extrêmement élevé. Il est donc primordial de compléter ces sources d'informations avec une surveillance totale des comportements afin de remédier aux vulnérabilités du réseau.

Hautement évolutif, le système StealthWatch offre des fonctionnalités bien plus performantes que celles des technologies de sécurité concurrentes (y compris les autres solutions de surveillance basées sur les flux). En dédupliquant et en faisant converger les enregistrements de flux unidirectionnels, le système est capable de surveiller et de stocker à moindre coût les flux de tous les réseaux d'entreprise, y compris les plus étendus et les plus complexes.

> « Grâce à la solution de Lancope, nous bénéficions d'une meilleure visibilité sur l'activité de notre réseau mondial. Les rapports de données fournis quasiment en temps réel et les fonctionnalités d'alerte nous permettent de détecter et de contrer rapidement les incidents menaçant le réseau. »
> **— Jeff DeLong, architecte en sécurité des informations, Westinghouse Electric Company, LLC**

## Les composants StealthWatch

Le système StealthWatch est personnalisable. Cependant, il intègre deux composants de base que sont les collecteurs de flux (FlowCollectors) et la console de gestion. Comme indiqué précédemment, ces composants sont fournis sous la forme d'appliances physiques ou virtuelles. Voici comment les composants interagissent :

- Les collecteurs de flux recueillent des données NetFlow, IPFIX, et d'autres types de données télémétriques à partir de votre infrastructure pour permettre une visibilité totale et à moindre coût sur tout votre réseau.
- La console de gestion prend en charge, coordonne et configure tous les produits StealthWatch afin de mettre en corrélation les données de sécurité récoltées en temps réel et les informations de veille du réseau à l'échelle de l'entreprise.
- Le capteur FlowSensor associe une inspection approfondie des paquets à une analyse des comportements pour identifier les applications et les protocoles utilisés sur le réseau.
- UDP Director est une appliance hautement performante et à haut débit qui recueille des informations stratégiques sur la sécurité et le réseau à plusieurs endroits. Elle transmet ensuite ces informations vers une ou plusieurs destinations telles que le collecteur de flux, sous la forme d'un flux de données unique.
- Le flux de données sur les menaces du centre de veille des tests StealthWatch (SLIC) utilise des informations collectées à l'échelle mondiale. Il génère des alertes et un indice de dangerosité des événements pour repérer et analyser rapidement les communications suspectes.
- Le composant ProxyWatch collecte des enregistrements de proxy qu'il associe aux enregistrements de flux. Il identifie l'utilisateur d'origine, les applications et les URL associés à chaque flux afin que vous puissiez surveiller les conversations réseau transitant par un proxy web.

## Les utilisations

| | |
|---|---|
| **Tout secteur d'activité** | • Surveiller le réseau en permanence<br>• Détecter les attaques en temps réel<br>• Réduire les délais d'investigation et de gestion des incidents<br>• Simplifier la segmentation du réseau<br>• Répondre aux exigences réglementaires<br>• Améliorer les performances du réseau et la planification de la capacité |
| **Commerce/Distribution** | • Surveiller des centaines de systèmes distants afin d'identifier les problèmes de sécurité et de performance<br>• Protéger les terminaux aux points de vente<br>• Rester conforme aux normes PCI |

| | |
|---|---|
| **Santé** | • Garantir la confidentialité des dossiers des patients<br>• Contrer les cyberattaques visant les équipements médicaux d'importance vitale pour les patients<br>• Rester conforme aux normes HIPAA<br>• Protéger la propriété intellectuelle<br>• Maintenir un niveau élevé de performances<br>• Détecter et protéger rapidement les nouveaux appareils sur le réseau |
| **Services financiers** | • Détecter à la fois les risques externes et internes<br>• Protéger les données des clients<br>• Se conformer à des exigences réglementaires strictes<br>• Garantir un accès 24 h/24 aux informations financières stratégiques<br>• Identifier et traiter les attaques et les problèmes de performance avant qu'ils ne causent trop de dégâts |
| **Secteur public** | • Protéger les réseaux contre les attaques avancées grâce à une surveillance permanente<br>• Protéger les informations confidentielles<br>• Rester conforme aux réglementations strictes en matière de sécurité<br>• Détecter les risques internes |
| **Enseignement supérieur** | • Protéger les terminaux mobiles<br>• Détecter le partage de fichiers en P2P<br>• Protéger les informations sensibles<br>• Protéger le réseau des comportements inappropriés et malveillants<br>• Maintenir un niveau élevé de performances et de disponibilité<br>• Rationaliser les workflows de sécurité<br>• Se conformer aux exigences réglementaires |

## Pourquoi choisir Cisco ?

En tant que créateur de la solution NetFlow, Cisco est idéalement positionné pour proposer une solution de sécurité qui fournit une visibilité sur le réseau basée sur les données de flux. En 2000, le groupe Lancope a été le premier à utiliser les données télémétriques pour renforcer la visibilité sur les réseaux et leur sécurité via StealthWatch. En collectant et en analysant les données NetFlow, IPFIX et d'autres types de données de télémétrie, StealthWatch transforme le réseau en un détecteur virtuel toujours actif et procède à des analyses avancées des comportements pour détecter rapidement de nombreux types d'attaques et renforcer la sécurité de centaines d'entreprises à travers le monde. Désormais membre de la famille des solutions Cisco, StealthWatch vous offre le meilleur de ces deux technologies.

## La garantie d'un déploiement simple et de qualité

Nos équipes en charge des services professionnels et nos partenaires agréés conçoivent, déploient et gèrent les produits StealthWatch depuis de nombreuses années. Grâce à une excellente connaissance des clients et du marché, une équipe en charge des services externes aide les entreprises à optimiser leur déploiement StealthWatch afin de répondre à leurs besoins, d'optimiser leur productivité et de réduire les risques. Grâce à une combinaison unique de compétences en matière de réseau et de sécurité, l'équipe met rapidement et efficacement en œuvre le système StealthWatch pour protéger les entreprises des attaques avancées.

Les services professionnels de Cisco comprennent l'installation initiale, une évaluation de l'intégrité de l'infrastructure, l'ajustement de la solution, l'automatisation des groupes d'hôtes, l'intégration de proxy, des supports de formation, ainsi que des services d'intégration et des conseils personnalisés.

> « [StealthWatch] nous permet de mieux suivre ce qui se passe sur notre réseau interne… et de contrôler facilement nos zones sécurisées afin d'éviter que certains types de trafic n'en sortent pas. »
> **— Ryan Laus, administrateur réseau, Central Michigan University**

## Cisco Capital

**Un financement pour vous aider à atteindre vos objectifs**

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, accélérer votre croissance, 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. Vous n'avez qu'une échéance mensuelle à honorer. L'offre de financement Cisco Capital est disponible dans plus de 100 pays. En savoir plus.

## Étapes suivantes

Pour en savoir plus sur StealthWatch, visitez http://www.cisco.com/go/stealthwatch ou contactez votre conseiller Cisco.


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 C22-736505-00 03/16