

## Cisco **Security** Agent Profiler

La nouvelle génération de logiciels de sécurité de réseau Cisco® Security Agent (CSA) protège contre les menaces de sécurité les systèmes serveur et station de travail, également nommés « points d'extrémité ». CSA va plus loin que les solutions de sécurité de point d'extrémité classiques, car il identifie et empêche les comportements malveillants avant qu'ils ne se produisent, éliminant ainsi des risques de sécurité connus et inconnus qui pèsent sur les réseaux et les applications d'entreprise. Le CSA procédant par analyse de comportement plutôt que par correspondance de signature, la solution garantit une protection robuste et des coûts d'exploitation réduits.

Le module Cisco Security Agent Profiler élargit ces fonctionnalités de sécurité en automatisant l'analyse des activités d'applications spécifiques et en élaborant des politiques de protection personnalisées pour ces applications.

### Avantages

- Simplification de l'analyse réglementaire des applications inconnues par observation automatique de toutes les demandes d'accès à des fichiers, au réseau, au registre et à des objets COM émises par ces applications
- Élaboration de politiques de protection fondées sur l'observation du comportement des applications
- Protection de toutes les applications, nouvelles et existantes, de l'entreprise
- Intégration à la console Management Center pour Cisco Security Agents ; lien hypertexte direct permettant, à partir des alertes, de lancer la surveillance des applications sur n'importe quel système protégé par un CSA
- Réduction du coût de l'administration de la sécurité grâce à l'analyse automatique centralisée de l'activité liée à la sécurité
- Architecture évolutive dans l'entreprise pouvant atteindre plusieurs milliers d'agents par profiler

### Automatisation des investigations de sécurité

L'un des aspects les plus complexes de la gestion de la sécurité réside dans le choix de l'action à mettre en place à la réception d'une alerte. Les alertes contiennent seulement une partie des informations dont l'opérateur chargé de la sécurité a besoin pour prendre une décision pertinente concernant l'action à entreprendre. La politique de sécurité en cours doit-elle être modifiée ? L'incident doit-il être renvoyé vers les administrateurs du système ? Une politique a-t-elle été enfreinte ou cet événement est-il normal et prévu ? Les informations parfois incomplètes fournies par les alertes rendent cette décision difficile, voire impossible à prendre.

Le module Cisco Security Agent Profiler offre une méthode centralisée d'analyse des alertes reçues de n'importe quel CSA. Il peut configurer un agent à partir d'un point central pour surveiller une application spécifique en observant toutes les demandes comportementales qu'elle émet. Chaque demande d'accès au système de fichiers, au réseau, au registre ou à un objet COM est enregistrée dans un journal et téléchargée de l'agent vers la console Management Center, où le profiler analyse les données et transmet une série de rapports à l'opérateur.

Cette surveillance centralisée silencieuse du comportement des applications génère une grande richesse d'informations concernant toutes les activités d'une application et non uniquement les comportements contrevenant à la politique de sécurité. Cet ensemble d'informations permet de détecter plus facilement une activité malveillante et facilite l'identification d'activités bénignes qui peuvent avoir été classées comme suspectes. Le module Cisco Security Agent Profiler transporte l'opérateur d'un milieu où la prise de décisions s'appuie sur des données anecdotiques vers un environnement où les décisions sont prises à partir d'une vue exhaustive de l'application considérée.



Facteurs entrant dans la prise de décision :

- Quelles sont toutes les connexions réseau issues de cette application ? Quels sont les systèmes distants qui communiquent avec cette application ? L'application a-t-elle un rôle de client réseau ? De serveur ? Les deux ? Un nombre croissant d'applications utilisent des connexions cryptées par SSL (Secure Sockets Layer) pour masquer leurs actions. Le module Cisco Security Agent Profiler vous permet de voir ces applications.
- Quels sont tous les fichiers auxquels cette application accède ? Certains d'entre eux sont-ils des fichiers de données sensibles ou des fichiers interdits (par exemple, cas d'une application de réseau distribuant des fichiers MP3 à des systèmes distants) ? Les fichiers sont-ils lus ou écrits ?
- Quelles sont les clés de registre lues ou écrites ? Dans la plupart des cas, la réponse à cette question permet d'identifier nommément l'application et le fournisseur.
- Des objets COM sont-ils chargés ? De nombreuses applications mettent leurs fonctions à disposition sous forme d'objets téléchargeables (par exemple Microsoft Office ou des programmes de courrier électronique). L'utilisation de ces objets peut faciliter la détection des tentatives d'action d'une application inconnue.

L'observation de cette activité et la présentation d'une vue centralisée et unifiée à l'opérateur de sécurité permet de prendre des décisions de sécurité plus rapidement et avec un degré de confiance supérieur.

### **Intégration à la console Management Center pour Cisco Security Agents**

Le module Cisco Security Agent Profiler s'installe sur la console Management Center pour Cisco Security Agents et peut être utilisé pour surveiller le comportement de n'importe quelle application d'un système quelconque doté d'un CSA. La console Management Center fournit un lien hypertexte direct à partir des alertes affichées dans le journal des événements, ce qui permet au profiler d'analyser l'application spécifique sur l'agent qui a généré l'alerte. Une tâche d'analyse peut également être créée pour une application qui n'a provoqué aucune alerte. Par exemple, si une alerte est enregistrée par un capteur Cisco Secure IDS, une tâche de détermination de profil peut faciliter son analyse.

### **Élaboration de politiques de protection personnalisées**

Dans la plupart des organisations, des applications personnalisées sont affectées à des fonctions stratégiques. Si les entreprises sont nombreuses à souhaiter bénéficier d'une protection accrue pour ces applications, il n'était jusqu'à présent pas possible de leur donner satisfaction sans modifier le code source des applications. Même s'il avait existé un moyen d'appliquer une sécurité à l'application à partir d'un point externe, il était impossible de savoir si de telles mesures de sécurité ne risquaient pas de bloquer des fonctions requises. Autrement dit, il a toujours existé un risque important pour que les mesures de sécurité elles-mêmes provoquent une panne de l'application.

L'aptitude du module Cisco Security Agent Profiler à surveiller tous les comportements des applications offre un moyen unique d'adapter la sécurité aux besoins de l'application au lieu de limiter son activité pour respecter des critères de sécurité. Le processus employé pour analyser le comportement des applications inconnues peut être appliqué pour surveiller tous les accès aux ressources enregistrés au cours de l'exécution normale d'une application. Ces données sont collectées par l'agent, à la suite de quoi le profiler élabore automatiquement une politique de protection CSA pour cette application. Cette politique reflétant le comportement réel observé de l'application, la protection s'adapte automatiquement aux besoins de cette dernière.

Le module Cisco Security Agent Profiler peut créer une politique de protection pour n'importe quelle application. Il n'est pas nécessaire de connaître le mode de fonctionnement de l'application – ni d'accéder au code source de l'application. Les politiques de protection créées par le profiler peuvent être utilisées sur n'importe quel agent administré à partir de la console Management Center ; elles peuvent également être exportées et utilisées en totalité par un autre Management Center.

### **Caractéristiques techniques**

Langues disponibles : anglais (États-Unis) uniquement pour tous les agents.

### **Spécifications pour l'installation**

Une clé de licence doit être installée sur le Management Center pour permettre au profiler de fonctionner.



### Références pour commande

Le module Cisco Security Agent Profiler est activé par l'installation d'une clé de licence sur une console Management Center pour Cisco Security Agents. Le tableau 1 contient les références du module Cisco Security Agent Profiler.

**Tableau 1** Références pour Cisco Security Agent

<b>Références</b>	<b>Description du produit</b>
<b>CSA-PROFILER-K9</b>	Cisco <b>Security</b> Agent Profiler
<b>Référence de maintenance</b>	<b>Description du produit de maintenance</b>
<b>CON-SAS-CSA-PRO</b>	Services Software Application Support (SAS) pour Cisco Security Agent Profiler



Siège social  
Cisco Systems, Inc.  
170 West Tasman Drive  
San Jose, CA 95134-1706  
États-Unis  
[www.cisco.com](http://www.cisco.com)  
Tél. : 408 526-4000  
800 553-NETS (6387)  
Fax : 408 526-4100

Siège Europe  
Cisco Systems Europe  
11, rue Camille Desmoulins  
92782 Issy-les-Moulineaux  
Cedex 9  
France  
[www.cisco.com](http://www.cisco.com)  
Tél. : 33 1 58 04 60 00  
Fax : 33 1 58 04 61 00

Siège Amérique  
Cisco Systems, Inc.  
170 West Tasman Drive  
San Jose, CA 95134-1706  
États-Unis  
[www.cisco.com](http://www.cisco.com)  
Tél. : 408 526-7660  
Fax : 408 527-883

Siège Asie/Pacifique  
Cisco Systems Australia, Pty., Ltd  
Level 9, 80 Pacific Highway  
P.O. Box 469  
North Sydney  
NSW 2060, Australie  
[www.cisco.com](http://www.cisco.com)  
Tél. : +61 2 8448 7100  
Fax : +61 2 9957 4350

Cisco Systems compte plus de 200 bureaux dans les pays suivants. Les adresses, numéros de téléphone et de fax sont répertoriés sur le site Web [Cisco.com](http://Cisco.com) à l'adresse [www.cisco.com/go/offices](http://www.cisco.com/go/offices).

Argentine • Australie • Autriche • Belgique • Brésil • Bulgarie • Canada • Chili • République populaire de Chine • Colombie • Costa Rica  
Croatie • République tchèque • Danemark • Dubaï • Finlande • France • Allemagne • Grèce • Hong-Kong • Hongrie • Inde • Indonésie  
Irlande • Israël • Italie • Japon • Corée • Luxembourg • Malaisie • Mexique • Pays-Bas • Nouvelle-Zélande • Norvège • Pérou • Philippines  
Pologne • Portugal • Porto Rico • Roumanie • Russie • Arabie saoudite • Écosse • Singapour • Slovaquie • Slovénie • Afrique du Sud  
Espagne • Suède • Suisse • Taiwan • Thaïlande • Turquie • Ukraine • Royaume-Uni • États-Unis • Venezuela • Vietnam • Zimbabwe

Copyright © 2001 Cisco Systems, Inc. Tous droits réservés. Aironet, Catalyst, Cisco, Cisco IOS, Cisco Systems et le logo de Cisco Systems sont des marques déposées de Cisco Systems, Inc. ou de ses filiales aux États-Unis et dans certains autres pays. Tous les autres noms ou marques de fabrique mentionnés dans ce document ou site Web appartiennent à leurs propriétaires respectifs. L'utilisation du mot partenaire n'implique pas nécessairement une relation de partenariat entre Cisco et une autre société (0012R) 12/00 BW6904