Fiche Technique

Cisco Security Agent

Avec le logiciel de sécurité de point d'extrémité Cisco Security Agent (CSA), Cisco offre à ses clients la gamme de solutions de protection la plus complète qui soit pour sécuriser les vastes réseaux d'entreprise.

La nouvelle génération de logiciels de sécurité de réseau Cisco® Security Agent (CSA) protège contre les menaces 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. CSA procède par analyse de comportement plutôt que par correspondance de signature, garantissant ainsi une protection robuste et des coûts d'exploitation réduits.

Avantages

- Intégration et extension de plusieurs fonctions de sécurité de point d'extrémité – CSA combine dans un agent unique un mécanisme de prévention des intrusions, un pare-feu distribué, une protection contre les codes mobiles malveillants, une garantie d'intégrité du système d'exploitation et le regroupement des historiques d'audit
- Protection contre des classes d'attaque complètes : analyses des ports, débordements de tampons, chevaux de Troie, malformation de paquets, requêtes HTML malveillantes et vers propagés par courrier électronique
- Prévention de type «Aucune mise à jour» (zero update) contre les attaques connues et inconnues
- Meilleure protection du marché pour les serveurs et les stations de travail ainsi que pour Unix et Windows
- Protection spécifique à l'application pour les serveurs Web et les bases de données
- Une architecture ouverte et extensible permet de définir et d'appliquer la sécurité conformément à la politique d'entreprise
- Architecture évolutive dans l'entreprise ; Cisco Security Agent peut atteindre des milliers d'agents par console d'administration
- Gestion intégrée avec les périphériques de sécurité Cisco PIX®, Cisco Secure IDS et Cisco VPN
- Intégration avec Cisco VPN assurée par la fonction AYT («Are You There»)

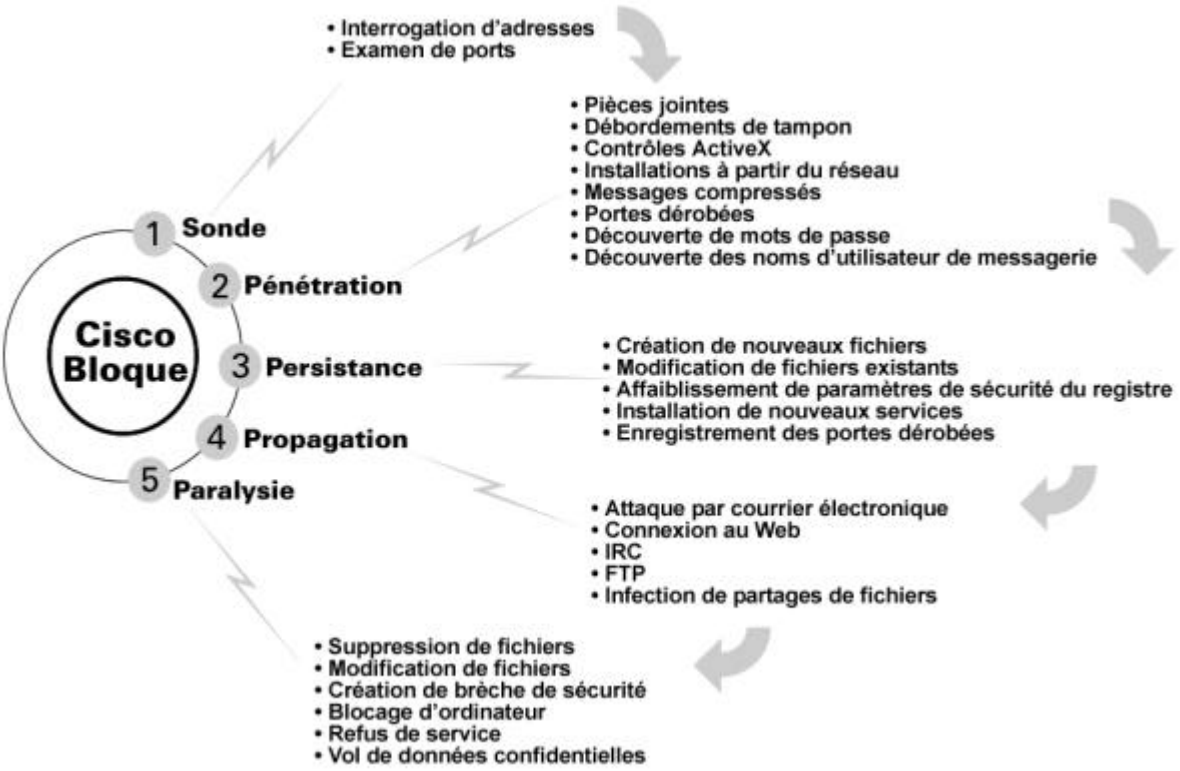
Lutte contre les attaques nouvelles et inconnues

Comme l'ont montré les récentes attaques hautement visibles telles que Code Red ou le ver SQL Slammer, les technologies classiques n'offrent qu'une capacité limitée de lutte contre les répercussions des types d'intrusion nouveaux et mutants. Les clients ont besoin d'une sécurité hôte qui protège leurs systèmes dans toutes les phases d'une attaque et assurent en outre une protection efficace contre les menaces nouvelles et inconnues.

Les intrusions sur les systèmes de réseau se déroulent généralement par étapes. Cisco a compris que seule une approche en couches s'avère efficace contre les brèches de sécurité qui peuvent se produire à n'importe quel stade, à l'extérieur du périmètre, sur le serveur ou au niveau des fichiers. Cisco Security Agent offre une défense proactive de l'hôte contre les dégradations, à chaque étape d'une intrusion, contrairement à d'autres technologies qui n'assurent qu'une protection anticipée (et ce, uniquement lorsque la signature est connue). Cisco Security Agent est spécialement conçu pour protéger les systèmes contre les nouvelles attaques dont la signature n'est pas encore connue (figure 1).

Figure 1

Cycle de vie d'une attaque



Solution Cisco Security Agent

La solution Cisco Security Agent se compose d'agents basés sur l'hôte et déployés sur des stations de travail et serveurs stratégiques qui transmettent des rapports à la console Management Center installée sur CiscoWorks VPN/Security Management Solution (VMS). Les agents utilisent les protocoles HTTP et SSL (Secure Sockets Layer) (SSL 128 bits) pour l'interface d'administration et les communications entre les agents et le centre d'administration. Toutes les configurations reposent sur CiscoWorks VMS et les alertes sont intégrées à celles d'autres produits de sécurité Cisco par l'intermédiaire de CiscoWorks Security Monitor (SecMon).

Architecture de l'agent

Cisco Security Agent s'installe entre les applications et le noyau pour une visibilité d'application maximale et des répercussions minimales sur la stabilité et les performances du système d'exploitation sous-jacent. L'architecture unique de l'agent intercepte tous les appels du système d'exploitation aux ressources du système de fichiers, du réseau et de la base de registre, ainsi qu'aux ressources d'exécution dynamique telles que les pages mémoire, les modules de bibliothèque partagés et les objets COM. Grâce à son modèle d'intelligence unique, l'agent met en corrélation les comportements de ces appels système en se fondant sur les règles qui définissent les comportements inappropriés ou inacceptables d'une application spécifique ou de toutes les applications. Cette corrélation et l'interprétation du comportement d'application qui en résulte permettent au logiciel, piloté par le personnel chargé de la sécurité, d'empêcher de nouvelles intrusions.

Lorsqu'une application tente d'exécuter une opération, l'agent recherche l'opération dans la politique de sécurité de l'application, décide en temps réel d'accepter ou de refuser sa poursuite et détermine s'il est nécessaire d'enregistrer la demande dans le journal. Les politiques de sécurité consistent en un ensemble de règles que les administrateurs informatiques et/ou de sécurité affectent aux serveurs et aux stations de travail protégés, de manière individuelle ou globale (dans toute l'entreprise). Ces règles garantissent la sécurité de l'accès des applications aux ressources demandées. En combinant des politiques de sécurité mettant en œuvre un pare-feu distribué, le verrouillage du système d'exploitation, une garantie d'intégrité, la protection contre les codes mobiles malveillants et la collecte d'événements d'audit dans des politiques standard pour serveurs et stations de travail, Cisco Security Agent assure une protection efficace des systèmes d'entreprise exposés.

Du fait que cette protection repose sur le blocage des comportements malveillants, les politiques par défaut arrêtent les attaques connues et inconnues sans nécessiter de mise à jour. La corrélation s'effectue sur l'agent et sur la console Management Center. La corrélation sur l'agent améliore considérablement la précision en identifiant les attaques ou abus réels sans bloquer l'activité légitime. La corrélation sur la console Management Center identifie les attaques globales telles que les vers de réseau ou les examens distribués.

Administration centralisée

La console Management Center pour Cisco Security Agents assure toutes les fonctions d'administration requises pour l'ensemble des agents de manière centralisée, à partir de la plate-forme CiscoWorks VMS. Son accès par navigateur Web de type « gestion à partir de n'importe quel site », supportant plusieurs profils d'administration, facilite la création de souches de distribution du logiciel agent, la création ou la modification de politiques de sécurité, la surveillance d'alertes et la génération de rapports. Fournie avec 20 politiques standard entièrement configurées, elle permet aux administrateurs de déployer en toute simplicité des milliers d'agents à tous les niveaux de l'entreprise. La console d'administration aide également les clients à déployer des agents en « mode IDS » ; dans ce cas, l'activité potentiellement malicieuse donne lieu à des alertes mais n'est pas bloquée.

La console Management Center pour Cisco Security Agents offre des options de personnalisation simples mais puissantes, telles qu'un assistant de réglage qui permet aux administrateurs d'adapter rapidement les politiques standard à leur environnement. Les administrateurs peuvent facilement modifier des règles ou en créer de nouvelles pour répondre à des besoins et attentes spécifiques. Pour simplifier l'audit des critères de conformité, une fonctionnalité « description des règles » imprime un descriptif des actions de règles ou de politiques particulières.

Les agents sont déployés sur des serveurs et des stations de travail directement à partir de Management Center pour Cisco Security Agents et contrôlés et mis à jour à partir de cette console d'administration. Chaque agent fonctionne en mode autonome : si la communication avec la console d'administration est impossible (par exemple, si un utilisateur de portable distant n'est pas encore connecté sur le VPN), l'agent applique la politique de sécurité de manière continue. Il met en cache toutes les alertes de sécurité, puis les télécharge vers la console d'administration lors du rétablissement des communications.

Cisco propose également le module Cisco Security Agent Profiler, une application logicielle enfichable destinée à la console Management Center pour Cisco Security Agents qui constitue un outil complet d'analyse de données et de création de politiques pour applications et environnements personnalisés. Le profiler analyse le comportement réel des applications en vue de créer des politiques personnalisées permettant aux clients de protéger tous les types d'application, même les applications extrêmement complexes et hautement spécialisées pour un environnement de client spécifique.

Caractéristiques techniques

Cisco Server Agent supporte :

- Windows 2000 Server et Advanced Server
- Windows NT 4.0 Server et Enterprise Server (Service Pack 5 ou ultérieur)
- Architecture Solaris 8 Service Pack ARC (noyau 64 bits)

Cisco Desktop Agent supporte :

- Windows NT 4 Workstation (Service Pack 5 ou ultérieur)
- Windows 2000 Professionnel
- Windows XP Professionnel

La console Management Center pour Cisco Security Agents sur CiscoWorks est disponible pour :

- Windows 2000 Server et Advanced Server (Service Pack 3)

Les politiques de sécurité standard sont disponibles pour (elles peuvent être combinées au gré de l'utilisateur) :

- Serveur générique
- Station de travail générique
- Microsoft IIS 4.0 et 5.0
- Apache v1.3
- Microsoft SQL Server
- Microsoft Exchange
- Sendmail
- Système DNS (Domain Name System)
- Serveurs DHCP (Dynamic Host Control Protocol)
- Serveurs de temps NTP
- Contrôleurs de domaine
- Pare-feu distribué
- Protection de navigateur
- Contrôle de la messagerie instantanée
- Protection de Microsoft Office
- Prévention du vol de données
- Protection Cisco Security Agent Manager

- CiscoWorks VMS
- Protection Cisco CallManager

Langues disponibles :

- Anglais (États-Unis) uniquement pour tous les systèmes d'exploitation supportés

Spécifications pour l'installation

Remarque : seules les versions anglaises (États-Unis) des systèmes d'exploitation sont supportées.

Server Agent pour Windows

- Windows NT 4.0 Server (Service Pack 5 ou ultérieur)
- Windows NT 4.0 Enterprise Server (Service Pack 5 ou ultérieur)
- Windows 2000 Server (jusqu'au Service Pack 3)
- Windows 2000 Advanced Server (jusqu'au Service Pack 3)
- Processeurs Pentium simples ou multiples, 200 MHz ou plus rapides
- RAM minimum : 128 Mo

Server Agent pour Solaris

- Architecture Solaris 8 SPARC (noyau 64 bits)
- Processeur Ultra SPARC, 500 MHz ou plus rapide
- RAM minimum : 256 Mo

Desktop Agent

- Windows NT 4.0 Workstation (Service Pack 5 ou ultérieur)
- Windows 2000 Professionnel (jusqu'au Service Pack 3)
- Windows XP Professionnel (jusqu'au Service Pack 0 ou 1)
- Processeurs Pentium simples ou multiples, 200 MHz ou plus rapides
- RAM minimum : 128 Mo

CiscoWorks VMS avec Management Center pour Cisco Security Agents

- Windows 2000 Server ou Advanced Server (Service Pack 1 ou 2)
- Processeur Pentium, 500 MHz ou plus rapide
- RAM minimum : 384 Mo
- Disque dur : 2 Go

Références pour commande

Cisco Security Agent comporte deux éléments principaux : les agents et la console Management Center pour Cisco Security Agents. Une console Management Center pour Cisco Security Agents est requise pour exécuter les agents ; ces derniers ne peuvent pas être licenciés sur une console non licenciée. La console Management Center pour Cisco Security Agents est fournie sans frais supplémentaire avec le produit

CiscoWorks, licencié séparément (licence limitée ou non). Les tableaux 1 et 2 contiennent les références pour Cisco Security Agent.

Tableau 1 Références pour Cisco Security Agent

Références	Description du produit
CSA-SRVR-K9	Cisco Security Server Agent (Windows et Solaris), 1 agent
CSA-B10-SRVR-K9	Cisco Security Server Agent (Windows et Solaris), pack de 10 agents
CSA-B25-SRVR-K9	Cisco Security Server Agent (Windows et Solaris), pack de 25 agents
CSA-B50-SRVR-K9	Cisco Security Server Agent (Windows et Solaris), pack de 50 agents
CSA-B100-SRVR-K9	Cisco Security Server Agent (Windows et Solaris), pack de 100 agents
CSA-B500-SRVR-K9	Cisco Security Server Agent (Windows et Solaris), pack de 500 agents
CSA-B25-DTOP-K9	Cisco Security Desktop Agent, pack de 25 agents
CSA-B100-DTOP-K9	Cisco Security Desktop Agent, pack de 100 agents
CSA-B250-DTOP-K9	Cisco Security Desktop Agent, pack de 250 agents
CSA-B500-DTOP-K9	Cisco Security Desktop Agent, pack de 500 agents
CSA-B1000-DTOP-K9	Cisco Security Desktop Agent, pack de 1000 agents
CSA-B5000-DTOP-K9	Cisco Security Desktop Agent, pack de 5000 agents

Tableau 2 Références de maintenance pour Cisco Security Agent

Référence de maintenance	Description du produit de maintenance
CON-SAS-CSA-SRVR	SAS (Software Application Support Services) SVS pour Server Agent (Windows et Solaris)
CON-SAS-CSA-B10S	SAS SVS pour pack de 10 Server Agents (Windows et Solaris)
CON-SAS-CSA-B25S	SAS SVS pour pack de 25 Server Agents (Windows et Solaris)
CON-SAS-CSA-B50S	SAS SVS pour pack de 50 Server Agents (Windows et Solaris)
CON-SAS-CSA-B100S	SAS SVS pour pack de 100 Server Agents (Windows et Solaris)
CON-SAS-CSA-B500S	SAS SVS pour pack de 500 Server Agents (Windows et Solaris)
CON-SAS-CSA-B25D	SAS SVS pour pack de 25 Desktop Agents
CON-SAS-CSA-B100D	SAS SVS pour pack de 100 Desktop Agents
CON-SAS-CSA-B250D	SAS SVS pour pack de 250 Desktop Agents
CON-SAS-CSA-B500D	SAS SVS pour pack de 500 Desktop Agents
CON-SAS-CSA-B1000D	SAS SVS pour pack de 1000 Desktop Agents
CON-SAS-CSA-B5000D	SAS SVS pour pack de 5000 Desktop Agents

Siège social
Cisco Systems, Inc.
170 West Tasman Drive
San Jose, CA 95134-1706
Etats-Unis
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
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
Etats-Unis
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
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 à l'adresse 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

12/00 BW6904