Cisco Security Agent

Cisco Security Agent 버전 5.2

제품 개요

Cisco® Security Agent 보안 소프트웨어는 서버, 데스크탑 및 POS(Point-of-Service) 컴퓨팅 시스템에 대한 위협을 방지합니다. Cisco Security Agent는 기존의 엔드포인트 보안 솔루션의 기능을 넘어서 타겟팅된 공격, 스파이웨어, 루트키트 및 데이제로 공격에 대해 업계 최고의 방어 기능을 제공합니다. 이전에 볼 수 없었던 알려지지 않은 위협과 새로운 브랜드 공격, 그리고 최근에 발표된 취약점을 악용하기 위해 만들어진 변형에 대해 능동적인 보호를 제공합니다. Cisco Security Agent는 서비스를 실행시켜 운영체제 또는 애플리케이션 특정 취약점 패치를 적용할 수 없는 중요한 서버에 대해 "제로 업데이트" 시스템 무결성 보호를 제공합니다. 이것은 취약점 공지에 응답하는 시스템 긴급 패치를 줄일 수 있도록 도와 패치 관련 다운타임과 IT Man-Hour 지출을 최소화합니다. 조직은 이제 위기 모드가 아닌 그들의 일정에 맞게 패치 작업을 수행할 수 있습니다.

강력한 정책 준수 제어 기능은 중요한 데이터 파일과 핵심 서버에 대한 보호를 제공합니다. 키 파일, 애플리케이션 및 서버에 대한 액세스를 모니터하거나 고의적이고 악의적인 데이터 손실을 중지할 수 있도록 강제로 제어할 수 있습니다. 착탈식 미디어 사용 제어를 통해 위험을 줄이고 작업장의 준수사항을 확실히 준수할 수 있습니다. 필요에 따라 세분화된 제어를 통해 사용자, 애플리케이션, 시스템, 위치 및 네트워크 주소에 대한 정책 준수를 관리할 수 있습니다.

Cisco Security Agent는 독립형 엔드포인트 보안 솔루션보다 더 많은 기능을 제공합니다. 네트워크 보안 장치와 공동 작업을 통해 전체 네트워크 배치 효율성을 높일 수 있습니다. Cisco VPN 장치는 Cisco Security Agent의 개인 방화벽과 호스트 침입 방지(HIPS) 기능을 통해 IP Security(IPSec) 및 SSL VPN 원격 액세스 사용자에 대해 강력한 엔드포인트 보안을 제공합니다. Cisco Security Agent에 의해 수집되는 호스트 정보는 Cisco 네트워크 IPS 장치와 공유되어 네트워크에서 발생하는 IPS 작업의 종합적인 인지 기능과 관련성을 향상시킵니다. Cisco Security Agent에 의해 Cisco ASA 및 Cisco PIX® 보안 어플라이언스의 방화벽과 애플리케이션 검사 기능을 향상시킬 수 있습니다. 즉, Cisco Security Agent 트래픽 마킹에 기반하여 특정 애플리케이션을 검사할 수 있습니다.

네트워크 통합 기능 표

표 1은 Cisco Security Agent의 네트워크 통합 기능을 나타냅니다.

표 1. 네트워크 통합 기능

주요 특징	설명
무선 정책 제어	Cisco Security Agent 는 무선 정책 제어를 통해 종합적인 보안을

	향상시키고 무선 배치의 대역폭을 최적화합니다. 정책을 통해 사무실 외부에 있는 사용자가 무선 트래픽에 대한 VPN 연결을 요구하는 상황처럼 특정 매개변수에 대한 무선 연결을 제한할 수 있습니다. 중요한 애플리케이션에 대해 우선순위를 지정하여 무선 LAN 인프라에 대한 지연을 최소화할 수 있습니다. 사용자가 사무실 외부에 있을 경우 Cisco Security Agent 의 위치 기반 정책 제어를 통해 추가 보호 레이어를 제공합니다.
트래픽 마킹	Cisco Security Agent 는 유무선 네트워크에서 per-application 기반 하에 트래픽을 분류하여 Oracle financials 또는 음성/비디오 등의 중요 애플리케이션에 대해 서비스 품질을 제공할 수 있습니다. 웹 브라우징이나 이메일과 같이 덜 중요한 애플리케이션은 낮은 우선순위로 분류하여 가용 네트워크 대역폭을 최적화할 수 있습니다. 또한 Cisco Security Agent 트래픽 마킹은 특정 애플리케이션 검사 정책을 적용할 수 있도록 Cisco ASA 5500 시리즈와 Cisco PIX 보안 어플라이언스의 방화벽 검사 기능을 개선하는 데 사용될 수 있습니다.
IPS 통합	Cisco Security Agent 는 Cisco 네트워크 IPS 장치와 통합되어 네트워크 내 식별 가능한 공격에 대한 효과를 늘릴 수 있습니다. Cisco Security Agent 는 중요한 엔드포인트 보안 정보를 Cisco ASA 5500 시리즈 및 Cisco Catalyst® 6500/7600 시리즈용 Cisco IPS 4200 시리즈 어플라이언스와 IPS 모듈에 제공함으로써 완벽한 엔드 투 엔드 보안 솔루션을 제공합니다.
NAC(Network Admission Control) 통합	Cisco NAC 어플라이언스 또는 NAC 프레임워크 배치 내에서 전체 네트워크 액세스 권한을 가질 수 있도록 Cisco Security Agent 가 실행되고 있는 호스트를 식별하여 트러스트할 수 있습니다. 비준수 호스트는 치료가 수행되어 규정을 준수할 수 있을 때까지 검역소에 격리시킬 수 있습니다. Cisco Security Agent 는 엔드포인트에서 NAC 에이전트의 무결성을 보호함으로써 원하지 않는 수정(modification)을 방지합니다. 이 기능은 DoS(denial of service) 및 악성 프로그램의 공격을 완화시켜 엔터프라이즈 네트워크의 자가 방어 기능을 강화시킵니다.
Cisco Security MARS 이벤트 통합	Cisco Security Agent 는 중요한 엔드포인트 정보를 보안 모니터링, 분석 및 응답 시스템인 Cisco MARS(Security Monitoring, Analysis, and Response System)로 제공합니다. 이러한 정보는 네트워크에서 위협을 식별하고 조사하는 Cisco Security MARS 기능을 강화시킵니다.

주요 기능 및 이점

Cisco Security Agent는 다음을 포함하여 이 외에도 수 많은 이점을 제공합니다.

- 규제 정책 준수 시행
- 타겟팅된 공격에 대해 방어적인 보호 제공
- 루트키트에 대한 식별 및 격리 기능
- 업계 최고의 호스트 침입 방지 기능, 개인 방화벽 및 데이제로 공격 보호 기능 제공
- Wi-Fi 대역폭 최적화
- 중요한 클라이언트 서버 애플리케이션 및 트랜잭션 가용성 확보
- 서버 및 데스크탑뿐만 아니라 소매점 POS(point of service) 터미널 보호

제품 아키텍처

Cisco Security Agent 솔루션

Cisco Security Agent는 호스트 기반 에이전트들로 구성되며, Cisco Security Agent를 위한 Cisco Management Center로 보고되는 중요한 업무 데스크탑과 서버에 배치됩니다. Management Center는 Cisco Security Agent 배치의 구성을 수행하는 독립형 애플리케이션으로 실행됩니다. 이 에이전트들은 관리 인터페이스와, 에이전트 및 Management Center 간 커뮤니케이션에 대해 HTTP 및 128비트 SSL을 사용합니다. Cisco Security MARS를 사용하는 Cisco의 다른 보안 제품으로부터의 경고를 같이 통합시킬 수 있습니다.

에이전트 아키텍처

Cisco Security Agent는 애플리케이션과 커널 사이에 상주하며, 기본 운영체제의 안전성과 성능에 미치는 영향은 최소화하면서 애플리케이션 가시성은 최대화합니다. 소프트웨어의 고유한 아키텍처가 메모리 페이지, 공유 라이브러리 모듈 및 COM 개체와 같은 동적 런타임 리소스뿐만 아니라 파일, 네트워크 및 레지스트리 소스에 대해서도 모든 운영체제 호출을 인터셉트합니다. 에이전트는 고유한 인텔리전스를 적용하여 특정 애플리케이션 또는 모든 애플리케이션에 대해 부적합하거나 허용할 수 없는 동작을 정의한 규칙에 기반하여 이러한 시스템 호출 동작에 대한 상관관계를 분석합니다. 애플리케이션 동작에 대한 이러한 상관관계와 결과에 대한 이해는 새로운 침입을 방지하기 위해 보안 담당자가 지시하는 대로 해당 소프트웨어를 허용하는 것입니다.

애플리케이션에서 작업을 시도할 경우 Cisco Security Agent는 해당 작업에 대해 실시간 허용 또는 거부 결정을 내리고, 요청이 적합하다고 로깅할지 여부를 결정하기 위해 애플리케이션의 보안 정책을 검사합니다. 보안 정책은 IT 및 보안 관리자가, 보호되는 서버 및 데스크탑에 개별적으로 할당하거나 엔터프라이즈 전체에 할당하는 규칙 컬렉션입니다. 이러한 규칙은 필요한 리소스에 대해 안전한 애플리케이션 액세스를 제공합니다. Cisco Security Agent는 배포된 방화벽, 운영체제 잠금 및 무결성 보장, 모바일 악성 코드 방지, 감사 이벤트 컬렉션 기능 등을 구현하는 보안 정책을 서버 및 데스트탑에 대한 기본 정책과 결합하여 노

출된 기업 시스템에 대해 높은 수준의 방어 및 보호를 제공합니다.
보호는 악의적인 활동을 차단하는 데 기반하므로 기본 정책은 알려졌거나 알려지지 않은 공격 모두를 업데이트 요구 없이 중지합니다. 에이전트와 Management Center 콘솔 모두에 대해 상관관계 분석이 수행됩니다. 에이전트 기반 상관관계 분석 결과 실제 공격, 또는 정상적인 활동을 방해하지 않는 오사용을 정확하게 식별하여 정확성이 대폭 개선되었습니다. Management Center에 대한 상관관계는 네트워크 웜 또는 배포된 스캔과 같은 글로벌 공격을 식별합니다.

중앙 집중화된 관리

Cisco Security Agent의 Management Center는 모든 에이전트에 대해 중앙 집중화된 방식으로 모든 관리 기능을 제공합니다. 역할 기반 웹 브라우저 액세스는 관리자의 에이전트 소프트웨어 배포 패키지 만들기, 보안 정책 만들기/수정, 경고 모니터링 또는 보고서 생성 작업을 수월하게 합니다. Management Center는 관리자가 수 천명의 에이전트를 엔터프라이즈 전체에 쉽게 배치할 수 있도록 완벽하게 구성된 기본 정책을 20개 이상 제공합니다. 그리고 Management Center에서는 활동이 경고를 받아도 차단되지 않는 "IDS 모드"로 고객이 에이전트를 배치할 수 있습니다.
Management Center는 관리자가 기본 정책을 그들의 환경에 맞게 신속하게 사용자 정의할 수 있도록 간단하지만 강력한 사용자 정의 기능을 제공합니다. 관리자는 조직의 요구와 요구사항에 맞게 간단하게 규칙을 수정하거나 완전히 새로운 규칙을 만들 수 있습니다. 또한 관리자는 감사 준수 요구사항을 지원하기 위한 Explain Rules 기능을 통해 특정 규칙 또는 정책에 대한 작업자의 기능 설명을 인쇄할 수 있습니다.
에이전트는 Management Center에서 서버 및 데스크탑으로 바로 배치되고 이러한 방식으로 제어 및 업데이트됩니다. 각 에이전트는 자동으로 작동됩니다. 관리자와의 커뮤니케이션이 가능하지 않은 경우(예를 들어, 원격 랩탑 사용자가 아직 VPN을 통해 연결되지 않은 경우)에는 에이전트가 계속 보안 정책을 시행합니다. 모든 보안 경고는 에이전트에 의해 캐시에 저장되어 커뮤니케이션이 복원되면 관리자에게 업로드됩니다.
또한 Cisco는 Management Center의 분석 보고 툴 제품군을 제공합니다. 배치 분석(Deployment Analysis) 기능은 이러한 애플리케이션의 사용 정보뿐만 아니라 모든 에이전트에 설치되는 애플리케이션에 대한 세부정보를 제공합니다. 동작 분석(Behavior Analysis) 기능은 사용자 지정 또는 알려지지 않은 애플리케이션 및 환경에 대한 포괄적인 데이터 분석 툴입니다. 여기에는 개별 고객의 환경에 맞게 매우 복잡하게 사용자 정의된 애플리케이션뿐만 아니라 모든 애플리케이션에 대해 고객들이 이해할 수 있도록 애플리케이션 동작에 대한 상세한 보고서가 제공됩니다.

요약 및 결론

Cisco Security Agent는 Cisco Self-Defending Network 솔루션의 핵심 구성요소입니다. 서로 결합되는 엔드포인트 및 네트워크 구성요소에서 검사를 수행하여 이종 시스템에서 가능하지 않았던 새로운 주요 보안 서비스를 이제 사용할 수 있습니다.

제품 사양

표 2는 Cisco Security Agent 버전 5.2의 제품 사양을 나타냅니다.

표 2. 제품 사양

설명	사양
Cisco Security Server 에이전트의 소프트웨어 호환성	• Windows Embedded for Point of Service(WEPOS) • Windows 2003(Standard, Enterprise, Web 또는 Small Business Editions) • Windows 2000 Server 및 Advanced Server • Windows NT 4.0 Server 및 Enterprise Server(SP 6a) • Solaris 8 SPARC 아키텍처(64비트 커널) • Solaris 9 SPARC 아키텍처(64비트 커널) • Red Hat Enterprise Linux WS Version 3.0 • Red Hat Enterprise Linux 4.0 ES 및 AS
Cisco Security Desktop 에이전트의 소프트웨어 호환성	• Windows XP Professional • Windows XP Tablet Edition • Windows 2000 Professional • Windows NT 4.0 Workstation(SP 6a) • Red Hat Enterprise Linux 3.0 WS • Red Hat Enterprise Linux 4.0 WS
Cisco Security Agent 의 하드웨어 호환성(Windows OS 최소 요구사항)	• 200MHz x86 프로세서 • 25MB 하드 디스크 공간 • 128MB RAM • 이더넷 또는 전화접속 네트워크 연결
Cisco Security Agent 의 하드웨어 호환성(Solaris OS 최소 요구사항)	• UltraSPARC 400MHz 프로세서 • 25MB 하드 디스크 공간 • 256MB RAM • 이더넷 네트워크 연결
Cisco Security Agent 의 하드웨어 호환성(Linux OS 최소 요구사항)	• 500MHz x86 프로세서 • 25MB 하드 디스크 공간 • 256MB RAM • 이더넷 네트워크 연결
Cisco Security Agent 의 Management Center 에 대한 소프트웨어 호환성	• Windows 2003 R2 Server
Cisco Security Agent 의	• 1GHz x86 프로세서

Management Center 에 대한 하드웨어 호환성	• 1GB RAM • 2GB 가상 메모리
국제화	• 영어(미국) 및 인터내셔널용(아프리카 및 히브리어 제외) Windows 운영체제 지원 • Windows 운영체제의 사용자 인터페이스 현지화: 영어(미국), 중국어(간체), 프랑스어, 독일어, 이탈리아어, 일본어, 한국어, 폴란드어, 포르투갈어 및 스페인어

주문 정보

Cisco Security Agent 솔루션은 두 구성요소 Cisco Security Agent(데스크탑 및 서버 에이전트) 및 Management Center로 구성됩니다. Management center는 에이전트를 실행하는 데 필요하며, 라이센스가 없는 콘솔로 에이전트의 라이센스를 부과할 수 없습니다. Cisco Security Agent를 위한 Management Center는 Cisco Security Agent 스타터 번들과 함께 제공됩니다.
표 3과 4는 각각 Cisco Security Agent 제품과 유지보수 부품 번호를 나타냅니다. 주문을 하려면 시스코 주문 홈 페이지를 방문해주십시오.

표 3. Cisco Security Agent 의 주문 정보

제품 이름	부품 번호
버전 5.2 를 위한 Cisco Security Agent 스타터 번들(Cisco Security Agent 를 위한 Management Center, 서버 에이전트 1 개, 데스크탑 에이전트 10 개 포함)	CSA-START-5.2-K9
Cisco Security Server Agent(Windows, Linux, 및 Solaris), 에이전트 1 개	CSA-SRVR-K9
Cisco Security Server Agent(Windows, Linux, 및 Solaris), 에이전트 번들(10 개)	CSA-B10-SRVR-K9
Cisco Security Server Agent(Windows, Linux, 및 Solaris), 에이전트 번들(25 개)	CSA-B25-SRVR-K9
Cisco Security Server Agent(Windows, Linux, 및 Solaris), 에이전트 번들(50 개)	CSA-B50-SRVR-K9
Cisco Security Server Agent(Windows, Linux, 및 Solaris), 에이전트 번들(100 개)	CSA-B100-SRVR-K9
Cisco Security Server Agent(Windows, Linux, 및 Solaris), 에이전트 번들(500 개)	CSA-B500-SRVR-K9
Cisco Security Server Agent(Windows, Linux, 및 Solaris), 에이전트	CSA-B1000-

번들(1000 개)	SRVR-K9
Cisco Security Server Agent(Windows, Linux, 및 Solaris), 에이전트 번들(2500 개)	CSA-B2500-SRVR-K9
Cisco Security Server Agent(Windows, Linux, 및 Solaris), 에이전트 번들(5000 개)	CSA-B5000-SRVR-K9
Cisco Security Server Agent(Windows, Linux, 및 Solaris), 에이전트 번들(10,000 개)	CSA-B10000-SRVR-K9
Cisco Security Desktop Agent(Windows 및 Linux), 에이전트 번들(25 개)	CSA-B25-DTOP-K9
Cisco Security Desktop Agent(Windows 및 Linux), 에이전트 번들(100 개)	CSA-B100-DTOP-K9
Cisco Security Desktop Agent(Windows 및 Linux), 에이전트 번들(250 개)	CSA-B250-DTOP-K9
Cisco Security Desktop Agent(Windows 및 Linux), 에이전트 번들(500 개)	CSA-B500-DTOP-K9
Cisco Security Desktop Agent(Windows 및 Linux), 에이전트 번들(1000 개)	CSA-B1000-DTOP-K9
Cisco Security Desktop Agent(Windows 및 Linux), 에이전트 번들(2500 개)	CSA-B2500-DTOP-K9
Cisco Security Desktop Agent(Windows 및 Linux), 에이전트 번들(5000 개)	CSA-B5000-DTOP-K9
Cisco Security Desktop Agent(Windows 및 Linux), 에이전트 번들(10,000 개)	CSA-B10000-DTOP-K9
Cisco Security Desktop Agent(Windows 및 Linux), 에이전트 번들(25,000 개)	CSA-B25000-DTOP-K9
Cisco Security Desktop Agent(Windows 및 Linux), 에이전트 번들(50,000 개)	CSA-B50000-DTOP-K9
Cisco Security Desktop Agent(Windows 및 Linux), 에이전트 번들(75,000 개)	CSA-B75000-DTOP-K9
Cisco Security Desktop Agent(Windows 및 Linux), 에이전트 번들(100,000 개)	CSA-B100000-DTOP-K9

Cisco Security Desktop Agent(Windows 및 Linux), 에이전트 번들(200,000 개)	CSA-B200000-DTOP-K9
Cisco Security Desktop Agent(Windows 및 Linux), 에이전트 번들(300,000 개)	CSA-B300000-DTOP-K9

서비스 및 지원

시스코 시스템즈는 고객의 성공을 촉진하는 수많은 종류의 서비스 프로그램을 제공합니다. 이러한 혁신적인 서비스 프로그램은 수준 높은 인력, 프로세스, 고객지원 툴 및 파트너의 기술력이 어우러진 것으로서 그 결과는 높은 고객 만족도로 나타납니다. 시스코 서비스는 여러분의 네트워크 투자를 보호하고 네트워크 운영을 최적화하며, 새로운 애플리케이션에 대비해 네트워크 인텔리전스와 비즈니스 역량을 높일 수 있도록 도와줍니다. 시스코 서비스에 대한 자세한 내용은 시스코 기술 지원 서비스 또는 시스코 어드밴스드 서비스를 참조하십시오.

표 4. Cisco Security Agent 유지보수 주문 정보

제품 이름	부품 번호
Cisco Security Agent 스타터 번들용 소프트웨어 애플리케이션 지원+업그레이드(SASU)	CON-SAU-CONSAS5K
1 개의 서버 에이전트용 SASU(Windows, Linux 및 Solaris)	CON-SAU-CSA-SRVR
10 개의 서버 에이전트용 SASU(Windows, Linux 및 Solaris)	CON-SAU-CSA-B10S
25 개의 서버 에이전트용 SASU(Windows, Linux 및 Solaris)	CON-SAU-CSA-B25S
50 개의 서버 에이전트용 SASU(Windows, Linux 및 Solaris)	CON-SAU-CSA-B50S
100 개의 서버 에이전트용 SASU(Windows, Linux 및 Solaris)	CON-SAU-CSA-B100S
250 개의 서버 에이전트용 SASU(Windows, Linux 및 Solaris)	CON-SAU-CSA-B250S
500 개의 서버 에이전트용 SASU(Windows, Linux 및 Solaris)	CON-SAU-CSA-B500S
1000 개의 서버 에이전트용 SASU(Windows, Linux 및 Solaris)	CON-SAU-CSA-

	B1000S
2500 개의 서버 에이전트용 SASU(Windows, Linux 및 Solaris)	CON-SAU-CSA-B2500S
5000 개의 서버 에이전트용 SASU(Windows, Linux 및 Solaris)	CON-SAU-CSA-B5000S
10,000 개의 서버 에이전트용 SASU(Windows, Linux 및 Solaris)	CON-SAU-CSA-B10000S
Desktop Agent 에이전트 번들(25 개)용 SASU(Windows 및 Linux)	CON-SAU-CSA-B25D
Desktop Agent 에이전트 번들(100 개)용 SASU(Windows 및 Linux)	CON-SAU-CSA-B100D
Desktop Agent 에이전트 번들(250 개)용 SASU(Windows 및 Linux)	CON-SAU-CSA-B250D
Desktop Agent 에이전트 번들(500 개)용 SASU(Windows 및 Linux)	CON-SAU-CSA-B500D
Desktop Agent 에이전트 번들(1000 개)용 SASU(Windows 및 Linux)	CON-SAU-CSA-B1000D
Desktop Agent 에이전트 번들(2500 개)용 SASU(Windows 및 Linux)	CON-SAU-CSA-B2500D
Desktop Agent 에이전트 번들(5000 개)용 SASU(Windows 및 Linux)	CON-SAU-CSA-B5000D
Desktop Agent 에이전트 번들(10,000 개)용 SASU(Windows 및 Linux)	CON-SAU-CSA-B10KD
Desktop Agent 에이전트 번들(25,000 개)용 SASU(Windows 및 Linux)	CON-SAU-CSA-B25KD
Desktop Agent 에이전트 번들(50,000 개)용 SASU(Windows 및 Linux)	CON-SAU-CSA-B50KD
Desktop Agent 에이전트 번들(75,000 개)용 SASU(Windows 및 Linux)	CON-SAU-CSA-B75KD
Desktop Agent 에이전트 번들(100,000 개)용 SASU(Windows 및 Linux)	CON-SAU-CSA-B100KD

Desktop Agent 에이전트 번들(200,000 개)용 SASU(Windows 및 Linux)	CON-SAU-CSA-B200KD
Desktop Agent 에이전트 번들(300,000 개)용 SASU(Windows 및 Linux)	CON-SAU-CSA-B300KD

<업데이트: 2008년10월15일>

