데이터 시트

Cisco Security Agent Version 4.5

Cisco Security Agent 엔드포인트 보안 소프트웨어를 통해 시스코는 대규모 기업 네트워크를 보호하기 위한 가장 광범위한 네트워크 보안 위협 차단 포트폴리오를 고객에게 제공합니다.

차세대 Cisco Security Agent 네트워크 보안 소프트웨어는 "엔드포인트"라고도 불리는 서버와 데스크톱 컴퓨팅 시스템에 위협 차단 기능을 제공합니다. Cisco Security Agent는 악의적 동작이 발생하기 전에 식별하고 차단하며 기업 네트워크와 비즈니스에 위협이 될 수 있는 알려지거나 알려지지 않은 보안 위협을 제거할 수 있기 때문에 기존의 엔드포인트 보안 솔루션보다 한 단계 더 발전한 솔루션입니다. Cisco Security Agent는 패턴 매칭을 사용하는 것이 아니라, 애플리케이션 동작을 분석하기 때문에 저렴한 운영 비용으로 강력한 보안을 제공할 수 있습니다.

주요 이점

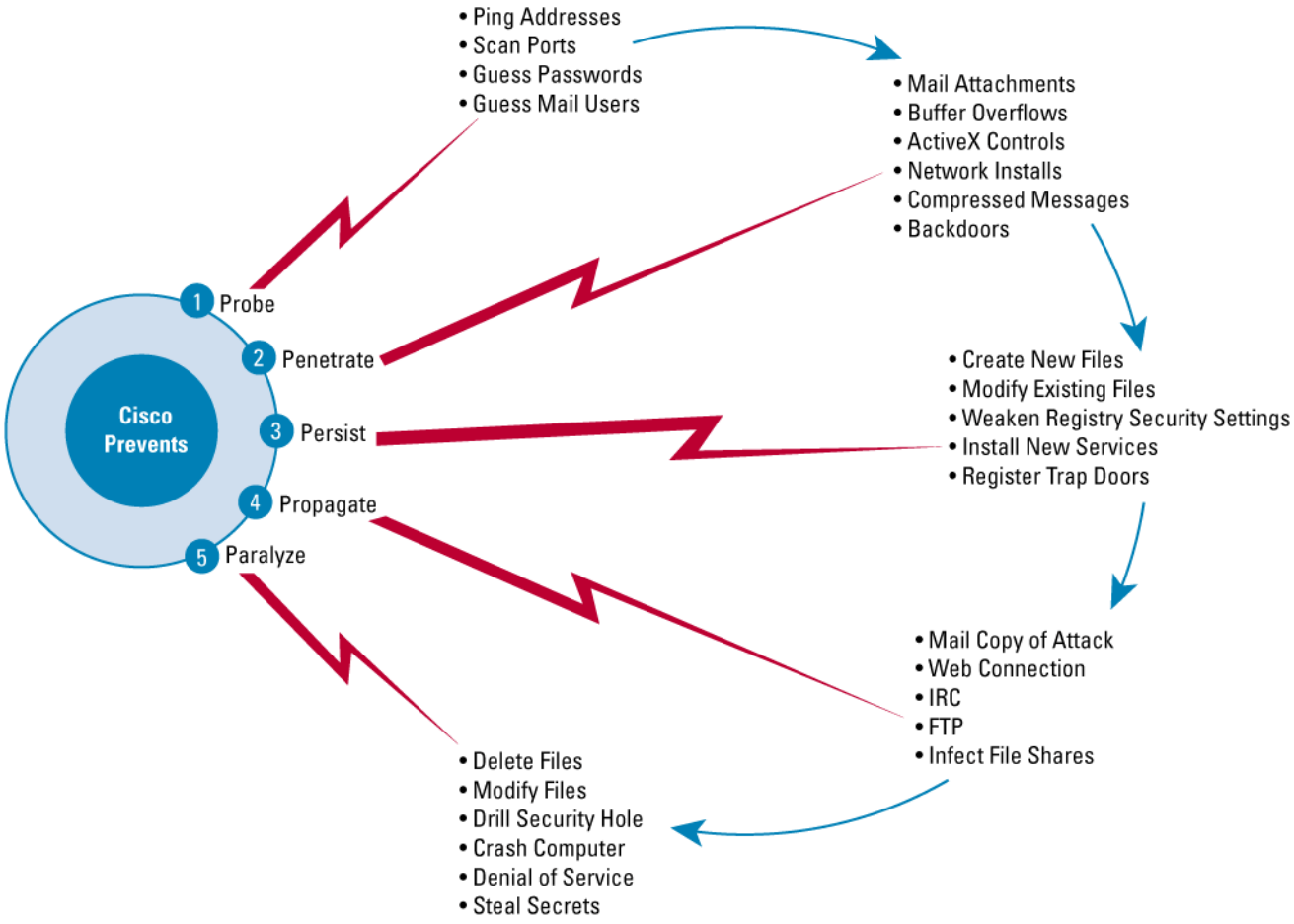
- 호스트 침입 차단, 분산 방화벽, 악의적 모바일 코드 차단, 운영체제 무결성 보호 및 감사 로그 통합 기능을 모두 단일 에이전트 내에서 제공하여 여러 엔드포인트 보안 기능을 통합하고 확장합니다.
- 포트 스캔, 버퍼 오버플로우, 트로이 목마, 잘못 구성된 패킷 및 전자메일 웜과 같은 모든 종류의 공격을 미리 차단할 수 있습니다.
- 알려지거나 알려지지 않은 공격에 대해 "제로 업데이트(업데이트가 필요 없는)" 차단을 제공합니다.
- 고객이 자체 일정에 따라 시스템에 패치를 적용할 수 있도록 Unix 및 Windows용 서버와 Windows 데스크톱을 위한 업계 최고 수준의 보호를 제공합니다.
- 확장이 가능한 개방형 아키텍처에서 회사 정책에 따라 보안을 정의하고 시행합니다.
- 하나의 관리 서버당 수천 대의 에이전트로 확장하여 대기업 적용을 지원합니다.

새로 출현한 알려지지 않은 공격 차단

Code Red 및 SQL Slammer 웜과 같은 공격이 나타나면서 기존의 기술로는 새로이 출현하는 공격의 영향을 차단하는 데 한계가 있습니다. 고객은 모든 단계의 공격을 차단하고 새로이 출현하는 알려지지 않은 위협을 차단하는 호스트 보안을 필요로 합니다. 네트워크 시스템에 대한 공격은 일반적으로 일련의 단계를 거칩니다.

시스코는 네트워크 경계나 서버 수준 또는 파일 수준 등 어느 단계에서나 발생할 수 있는 보안 위협을 차단하기 위해서는 계층화된 방어가 효과적임을 알아냈습니다. Cisco Security Agent는 모든 단계의 공격으로 인한 호스트의 피해를 막아주는 반면 다른 기술의 경우는 시그니처(패턴 파일)가 알려진 경우에만 초기 단계의 보호를 제공합니다. Cisco Security Agent(그림 1)는 알려진 시그니처가 없는 새로운 공격을 차단하도록 특별히 설계되었습니다.

그림 1. Cisco Security Agent



Cisco Security Agent 솔루션

Cisco Security Agent는 Microsoft Windows 2000 서버상의 관리 콘솔과 중요한 데스크톱 및 서버에 배치되는 호스트 기반 에이전트로 구성됩니다. 에이전트는 관리 인터페이스, 에이전트와 관리 콘솔 간의 커뮤니케이션을 위해 HTTP 및 SSL(Secure Sockets Layer) 프로토콜(128비트 SSL)을 사용합니다.

에이전트 아키텍처

Cisco Security Agent는 애플리케이션과 커널 사이에 상주하므로, 기본 운영체제의 안정성과 성능에 최소한의 영향을 미치면서 최대의 애플리케이션 가시성을 제공합니다. 에이전트의 고유 아키텍처는 파일, 네트워크 및 레지스트리 소스에 대한 모든 시스템 호출을 가로챌 뿐만 아니라 메모리 페이지, 공유 라이브러리 모듈 및 COM(Component Object Model) 객체와 같은 동적인 런타임 리소스에 대한 호출도 가로챕니다. 에이전트는 특정 애플리케이션에 적합하거나 적절한 동작을 정의하는 규칙을 기반으로 이러한 시스템 호출 동작의 상호연관성을 지능적으로 분석합니다. 이렇게 애플리케이션의 동작의 상호연관성을 분석하여 이해함으로써 소프트웨어가 보안 직원의 지시대로 새로운 공격을 차단할 수 있습니다.

애플리케이션이 특정 작업을 시도하면 에이전트가 애플리케이션의 보안 정책에 대해 이 작업을 검사합니다. 그런 다음 작업의 계속 여부를 실시간으로 허용하거나 거부하고 요청 로깅의 적절성 여부를 결정합니다. 보안 정책은 IT 및 보안 관리자가 보호된 서버와 데스크톱에 할당하는 일련의 규칙입니다. 이 규칙은 기업 전체에 할당되거나 개별적으로 할당됩니다. 이 규칙은 필요한 리소스에 안전한 애플리케이션 액세스를 제공합니다.

Cisco Security Agent는 분산 방화벽, 운영체제 잠금, 무결성 보호, 악성 모바일 코드 차단 및 감사 이벤트 수집 기능을 서버 및 데스크톱용 기본 정책에 구현하는 보안 정책을 수립함으로써 위험에 노출된 회사 시스템을 보호합니다.

이러한 보호는 악성 동작을 차단하기 때문에 업데이트 없이 기본 정책만으로도 알려진 공격과 알려지지 않은 공격을 차단할 수 있습니다. 상호연관성 분석은 에이전트와 매니저에 대해 수행됩니다. 에이전트 기반 상호연관성 분석은 합법적인 행위는 차단하지 않으면서 실제적인 공격이나 악용을 식별하며, 매니저에 대해 상호연관성 분석을 수행하여 네트워크 웜 또는 분산 스캔과 같은 광범위한 공격을 식별합니다.

중앙 집중식 관리

Cisco Security Agent Manager는 중앙에서 모든 에이전트에 대해 모든 관리 기능을 제공합니다. "어디에서나 관리가 가능한" 역할 기반의 웹 브라우저 액세스를 통해 관리자가 쉽게 에이전트 소프트웨어 분산 패키지 생성, 보안 정책 수정 및 생성, 경보 모니터, 리포트를 작성할 수 있습니다. Cisco Security Agent Manager에는 20개 이상의 완벽하게 구성된 기본 정책이 제공되므로 관리자가 수 천 개의 에이전트를 기업에 쉽게 배치할 수 있습니다. 또한 이 매니저를 통해 고객이 "IDS 모드"로 에이전트를 배치할 수 있습니다. 이 모드에서는 활동에 대해 경보만 발생하고 차단하지는 않습니다.

매니저는 조정 마법사와 같은 단순하지만 강력한 커스터마이즈 성능을 제공하므로, 관리자가 기본 정책을 자신의 환경에 신속하게 맞출 수 있습니다. 관리자가 새로운 규칙을 쉽게 만들거나 수정하여 자신의 필요에 맞는 수요와 요구사항을 충족시킬 수 있습니다. 감사 규정 준수 요구사항을 지원하기 위한 "규칙 설명(Explain Rules)" 기능은 어떤 지정된 규칙이나 정책이 어떤 동작을 수행하는지를 인간의 언어로 설명합니다.

에이전트는 Cisco Security Agent Manager로부터 서버와 데스크톱에 직접 배치되며 이 매니저로부터 제어되고 업데이트됩니다. 각 에이전트는 독자적으로 작동합니다. 매니저와의 커뮤니케이션이 불가능한 경우(예: 원격 랩탑 사용자가 VPN을 통해 아직 연결되지 않은 경우) 에이전트가 보안 정책을 계속해서 시행합니다. 커뮤니케이션이 복원되면 모든 보안 경보가 에이전트를 통해 저장되어 매니저에 업로드됩니다.

OEM 기간 중 시스코는 판촉으로서 Cisco Security Agent Manager에 Okena StormFront 애플리케이션을 함께 제공하고 있습니다. StormFront는 Cisco Security Agent Manager용 애플리케이션이며 커스터마이즈 애플리케이션 및 환경에 대해 광범위한 애플리케이션 분석 및 정책 작성 툴을 제공합니다. StormFront는 실제적인 애플리케이션 동작을 분석하여 커스터마이즈 정책을 수립하므로, 개별 고객의 특정 환경에 맞게 커스터마이즈된 매우 복잡한 애플리케이션을 비롯한 모든 애플리케이션을 보호할 수 있습니다.

기술 사양

Server Agent 지원:
- Windows 2000 Server 및 Advanced Server
- Windows NT v4.0 Server 및 Enterprise Server(서비스 팩 5 이상)
- Solaris 8 SPARC 아키텍처(64비트 커널)

Desktop Agent 지원:
- Windows NT 4 Workstation(서비스 팩 5)
- Windows 2000 Professional
- Windows XP Professional

사용 가능한 매니저:
- Windows 2000 Server 및 Advanced Server(서비스 팩 3)

사용 가능한 기본 보안 정책(필요한 경우 조합할 수 있음):
- 일반적인 서버
- 일반적인 데스크톱

- Microsoft IIS v4.0 및 v5.0
- Apache v1.3
- Microsoft SQL Server
- Microsoft Exchange
- Sendmail
- DNS(Domain Name Server) 서버
- DHCP(Dynamic Host Control Protocol) 서버
- NTP(Network Time Protocol) 서버
- 도메인 컨트롤러
- 분산 방화벽
- 브라우저 보호
- 인스턴트 메신저 제어
- Microsoft Office 보호
- 데이터 도난 방지
- Cisco Security Agent Manager 보호

사용 가능 언어:
- 지원되는 모든 운영체제에 대해 영어(미국)만 지원

설치 요구사항

참고로 영어(미국) 버전의 운영체제만 지원됩니다.

서버 에이전트-Windows
- Windows NT v4.0 Server(서비스 팩 5 이상)
- Windows NT v4.0 Enterprise Server(서비스 팩 5 이상)
- Windows 2000 Server(최대 서비스 팩 3)
- Windows 2000 Advanced Server(최대 서비스 팩 3)
- 단일 또는 여러 개의 Pentium 프로세서, 200 MHz 이상
- 128 MB RAM(최소)

서버 에이전트-Solaris
- Solaris 8 SPARC 아키텍처(64비트 커널)
- Ultra SPARC 프로세서 500 MHz 이상
- 256 MB RAM(최소)

데스크톱 에이전트
- Windows NT v4.0 Workstation(서비스 팩 5 이상)
- Windows 2000 Professional(최대 서비스 팩 3)
- Windows XP Professional(최대 서비스 팩 1)
- 단일 또는 여러 개의 Pentium 프로세서, 200 MHz 이상
- 128 MB RAM(최소)

매니저(필수)
- Windows 2000 Server 또는 Advanced Server(서비스 팩 1 또는 서비스 팩 2)

- Pentium 500 MHz 프로세서 이상
- 384 MB RAM(최소)
- 2 GB 디스크

주문 정보

Cisco Security Agent는 에이전트와 매니저의 두 기본 구성 요소로 구성됩니다. 에이전트를 실행하기 위해서는 매니저가 필요하며 사용 허가되지 않은 매니저에 대해서는 에이전트를 사용 허가할 수 없습니다.

표 1. Cisco Security Agent 부품 번호

부품 번호	제품 설명
CSA-MANAGER-K9	Cisco Security Agent Manager(CD 키트)
CSA-SRVR-K9=	Cisco Security Server Agent(Win & Sol), 1개 에이전트
CSA-B10-SRVR-K9	Cisco Security Server Agent(Win & Sol), 10개 에이전트 번들
CSA-B25-SRVR-K9	Cisco Security Server Agent(Win & Sol), 25개 에이전트 번들
CSA-B50-SRVR-K9	Cisco Security Server Agent(Win & Sol), 50개 에이전트 번들
CSA-B100-SRVR-K9	Cisco Security Server Agent(Win & Sol), 100개 에이전트 번들
CSA-B25-DTOP-K9	Cisco Security Desktop Agent, 25개 에이전트 번들
CSA-B100-DTOP-K9	Cisco Security Desktop Agent, 100개 에이전트 번들
CSA-B250-DTOP-K9	Cisco Security Desktop Agent, 250개 에이전트 번들
CSA-B500-DTOP-K9	Cisco Security Desktop Agent, 500개 에이전트 번들
CSA-B1000-DTOP-K9	Cisco Security Desktop Agent, 1000개 에이전트 번들

표 2. Cisco Security Agent 유지보수 부품 번호

유지보수 부품 번호	유지보수 제품 설명
CON-SAS-CSA-MAN	Cisco Security Agent Manager용 SAS SVS(Software Application Support Services)
CON-SAS-CSA-SRVR	Server Agent용 SAS SVS(Win & Sol)
CON-SAS-CSA-B10S	10 Server Agent 번들용 SAS SVS(Win & Sol)
CON-SAS-CSA-B25S	25 Server Agent 번들용 SAS SVS(Win & Sol)
CON-SAS-CSA-B50S	50 Server Agent 번들용 SAS SVS(Win & Sol)
CON-SAS-CSA-B100S	100 Server Agent 번들용 SAS SVS(Win & Sol)
CON-SAS-CSA-B25D	25개 Desktop Agent 번들용 SAS SVS
CON-SAS-CSA-B100D	100개 Desktop Agent 번들용 SAS SVS
CON-SAS-CSA-B250D	250개 Desktop Agent 번들용 SAS SVS
CON-SAS-CSA-B500D	500개 Desktop Agent 번들용 SAS SVS
CON-SAS-CSA-1000D	1000개 Desktop Agent 번들용 SAS SVS

CISCO SYSTEMS

www.cisco.com/kr

2005-07-15

■ Gold 파트너	• ㈜데이타크레프트 코리아	02-6256-7000	• ㈜인네트	02-3451-5300	• ㈜인성정보	02-3400-7000
	• 한국아이비엠㈜	02-3781-7800	• ㈜콤텍 시스템	02-3289-0114	• 쌍용정보통신㈜	02-2262-8114
	• 에스넷시스템㈜	02-3469-2400	• ㈜링네트	02-6675-1216	• 한국후지쯔㈜	02-3787-6000
	• 한국휴렛팩커드㈜	02-2199-0114	• ㈜LG 씨엔에스	02-6363-5000	• SK 씨앤씨㈜	02-2196-7114/8114
■ Silver 파트너	• 포스데이타㈜	031-779-2114				
■ Local 디스트리뷰터	• ㈜소프트뱅크 커머스 코리아	02-2187-0176	• ㈜아이넷뱅크	02-3400-7490	• ㈜SK 네트웍스	02-3788-3673
■ IPT 전문 파트너	• 인네트	02-3451-5300	• ㈜데이타크레프트 코리아	02-6256-7000	• 에스넷시스템㈜	02-3469-2900
	• ㈜인성정보	02-3400-7000	• ㈜크리스넷	1566-3827	• ㈜LG 씨엔에스	02-6363-5000
	• ㈜링네트	02-6675-1216				
■ IPCC 전문 파트너	• 한국아이비엠㈜	02-3781-7114	• 한국휴렛팩커드㈜	02-2199-4272	• GS 네오텍	02-2630-5280
	• ㈜인성정보	02-3400-7000	• 삼성네트웍스㈜	02-3415-6754		
■ WLAN 전문 파트너	• ㈜에어키	02-584-3717	• ㈜해창시스템	031-389-0780		
■ Security 전문 파트너	• 나래시스템	02-2190-5533	• 인포섹㈜	02-2104-5114	• 코코넛	02-6007-0133
	• UNNET Systems	02-565-7034				
■ Optical 전문 파트너	• ㈜LG 씨엔에스	02-6363-5000	• 에스넷시스템㈜	02-3469-2900	• 미리넷㈜	02-2142-2800
■ CN 전문 파트너	• ㈜메버릭시스템	02-845-4280				
■ Storage 전문 파트너	• ㈜패킷시스템즈 코리아	02-558-7170	• 매크로임팩트	02-3446-3508		