데이터 시트

CS-MARS

CS-MARS 엔터프라이즈 위협 차단(Enterprise Threat Mitigation) 어플라이언스

조직에서 보안 위협을 식별, 관리 및 대응하고 규정 준수를 유지할 수 있도록 도와줍니다.

문제점

지나치게 많은 보안 및 네트워크 정보
공격 및 장애에 대한 잘못된 식별, 우선 순위 부여 및 대응
공격의 정교성, 속도 및 복구 비용 증가
규정 및 감사 요구사항 준수
충분하지 않은 보안 직원 및 예산

솔루션

네트워크 인텔리전스를 통합하여 네트워크 이상 및 보안 이벤트의 상호연관성을 분석하고 최신화합니다.
확실한 보안 사고를 시각화하고 검사를 자동화합니다.
네트워크 및 보안 인프라를 최대한 활용하여 공격을 차단합니다.

시스템, 네트워크 및 보안 운영을 모니터링하여 규정을 준수하도록 지원합니다.

최소한의 총소유 비용(TCO)으로 쉽게 설치, 사용 및 유지보수가 가능한 확장형 위협 차단 어플라이언스를 제공합니다.

CS-MARS(Mitigation and Response System)는 네트워크 및 보안의 원시 데이터를 실제적인 정보로 변환하여 확실한 보안 사고를 차단하고 규정 준수를 유지하도록 합니다. 설치와 사용이 쉬운 이 위협 차단 어플라이언스 제품군은 운영자가 인프라에 이미 설치된 네트워크 및 보안 장비를 활용하여 우선 순위가 높은 위협에 집중하고 이를 탐지, 차단 및 보고할 수 있도록 도와줍니다.

심층 방어의 딜레마

정보 보안 방식은 인터넷, 경계 보호에서 심층 방어 모델로 발전해 왔습니다. 이 심층 방어 모델에서는 인프라 전체에 여러 대응책을 계층화하여 취약성과 공격에 대처합니다. 공격 빈도가 늘어나고 정교해져 그 전파 속도가 더욱 빠르고, 네트워크와 주변 장비의 경계가 모두 모호하므로 이 방어 모델이 필수적입니다.

취약성을 악용하려는 시도로 인해 네트워크 액세스 포인트와 시스템이 매일 수천 회씩 탐색을 당합니다. 최근의 혼합/하이브리드 공격의 경우 여러 공격 방법을 동시에 사용하여 시스템에 불법 액세스하고 조직 내/외부에서 제어를 수행합니다. 웜, Zero Day 공격, 바이러스, 트로이 목마, 스파이웨어 및 공격 툴이 확산됨에 따라 가장 강력한 인프라조차도 공격을 받게 됩니다. 이 결과, 공격 대응 시간이 늦어지고 가동 중단 시간이 길어지며 복구 비용이 증가하게 됩니다.

단순히 서버 및 네트워크 장비의 수와는 상관없이 각 보안 구성요소는 이상 현상(anomaly) 탐지, 위협 대응 및 분석을 위해 이벤트에 대한 로그 및 경보 기능을 별개로 제공합니다. 불행히도 이로 인해 엄청난 양의 노이즈, 경보, 로그 파일 및 확실하지 않은 정보가 발생하며, 이러한 정보를 적절하게 분석할 수 있는 시간과 리소스가 충분하다고 가정하더라도, 운영자가 이러한 정보를 식별하고 효과적으로 활용하는 것이 어렵습니다. 또한 규정 준수 관련 법률에서는 엄격한 데이터 기밀성, 운영상의 보안 개선 및 감사 프로세스의 유지 관리를 요구합니다.

고급 보안 위협 차단

보안 정보/이벤트 관리(SIM) 제품이 이러한 문제를 완화해줄 수도 있습니다. 하지만 측정이 불가능한 것을 관리할 수는 없는 법입니다. SIM을 사용하여 운영자가 보안 이벤트 및 로그를 중앙에서 집계하고 제한적인 상호연관성 분석 및 질의 기술을 통해 이 데이터를 분석한 후 별개의 이벤트들에 대해서 경보와 리포트를 생성할 수 있습니다.

불행히도 상당수의 1세대 및 2세대 SIM은 상호연관성을 분석한 이벤트를 좀더 정확하게 식별 하여, 공격 경로를 정확하게 탐지, 위협을 차단하고 많은 이벤트 부하를 유지하기 위해 필요한 충분한 네트워크 인텔리전스와 성능 특성을 가지고 있지 못합니다.

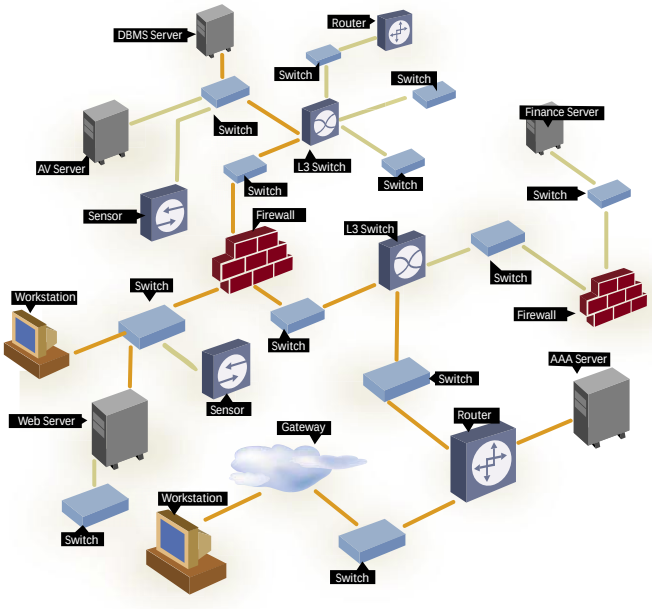
이러한 보안 문제와 관리 결함을 해결하기 위해 시스코는 확장 가능한 보안 위협 차단(STM: Security Threat Mitigation) 어플라이언스 제품군을 사용합니다.

CS-MARS는 네트워크와 보안 인프라 투자를 보완하기 위해 설치와 사용이 쉽고 경제적인 보안 명령 및 제어 솔루션을 제공합니다.

인프라를 활용하여 보안 및 네트워크 운영 강화

CS-MARS는 네트워크 및 보안의 원시 데이터를 실제적인 정보로 변환하여 확실한 보안 사고를 차단하고 규정을 준수할 수 있습니다.

시스코 CS-MARS™는 네트워크 인텔리전스, ContextCorrelation™, SureVector™ 분석 및 AutoMitigate™ 성능을 결합하여 네트워크 장비 및 보안 대응책을 강화해주는 고성능 확장형 위협 차단 어플라이언스입니다. 이를 통해 회사가 네트워크 공격을 신속하게 식별, 관리 및 제거하고 규정을 준수하도록 할 수 있습니다.



뛰어난 성능으로 네트워크 인텔리전트 이벤트 집계

CS-MARS는 라우터, 스위치, 취약성 분석(VA) 툴의 토폴로지 및 장비 구성을 이해하고 네트워크 트래픽을 분류함으로써 네트워크 인텔리전스를 확보합니다. 시스템의 통합 네트워크 검색 기능은 장비 구성 및 현재의 보안 정책이 포함되어 있는 토폴로지 맵을 작성합니다. 이 맵을 통해 CS-MARS가 네트워크 전체의 패킷 플로우를 모델링할 수 있습니다. 이 어플라이언스는 인라인 방식으로 작동하지 않으며 기존 소프트웨어 에이전트를 최소한으로 사용하기 때문에 네트워크 또는 시스템 성능에 영향을 미치지 않습니다.

어플라이언스가 다양한 종류의 네트워크 장비(예: 라우터 및 스위치), 보안 장비 및 애플리케이션(예: 방화벽, 침입 탐지, 취약성 스캐너 및 안티바이러스), 호스트(예: Windows, Solaris 및 Linux 로그), 애플리케이션(예: 데이터베이스, 웹 서버 및 인증 서버) 및 네트워크 트래픽(예: 시스코 Netflow)으로부터 이벤트 및 로그를 중앙에서 집계합니다.

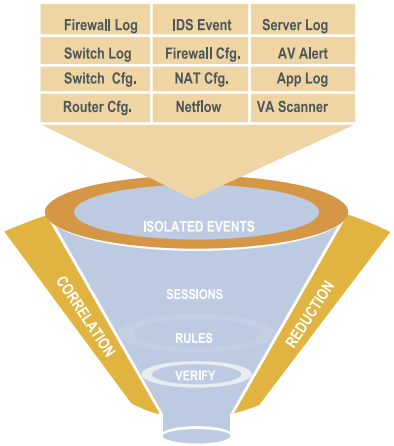
ContextCorrelation™ 은 네트워크 수준의 정보를 사용하여 NAT(Network Address Translation) 영역도 포함하여 여러 보안 이벤트와 네트워크 행위를 세션으로 그룹화하고, 시스템 및 사용자 정의 상호연관성 분석 규칙을 여러 세션에 적용하여 확실한 보안 사고를 식별합니다. 시스템에는 미리 정의된 규칙이 제공됩니다. 이 규칙은 시스코를 통해 자주 업데이트되며 주요 공격 시나리오, Zero Day 공격 및 웜을 식별합니다. 그래픽으로 표시되는 규칙 정의 구조를 사용하여 모든 애플리케이션에 대해 사용자 정의 커스터마이즈 규칙을 쉽게 만들 수 있습니다. ContextCorrelation은 원시 이벤트 데이터를 상당히 줄여주고, 대응 우선 순위를 쉽게 부여하고, 구현된 대응책의 효과를 극대화합니다.

신속한 집계 및 통합 CS-MARS 솔루션은 수천 개의 원시 이벤트를 캡처하고, 뛰어난 데이터 축소정리를 통해 보안 사고를 효율적으로 분류하고, 이 정보를 압축하여 보관합니다. 많은 양의 보안 이벤트를 관리하기 위해서는 안전하고 안정적인 중앙 로깅 플랫폼이 필요합니다. 특별한 용도의 CS-MARS 어플라이언스는 보안이 강화되었으며, 초 당 10,000개 이상의 이벤트와 초 당 300,000개 이상의 Netflow 플로우가 있는 엄청난 양의 이벤트 트래픽을 처리하는 데 최적입니다.

이것이 가능한 이유는 특허 대기 중인 시스코 파이프라인 인메모리(in-memory) 이벤트 처리 아키텍처와 내장된 Oracle®을 최적으로 사용하기 때문입니다. 모든 데이터베이스 기능과 조정은 사용자에게 투명하게 실행됩니다. 온보드 스토리지와 연속 압축, NFS 예비 대용량 스토리지에 기록 데이터를 보관하는 CS-MARS는 전체 보안 로그 주기를 유지 관리하기에 적절한 보안 로그/이벤트 어그리게이션 제품입니다.

질문: Day Zero 공격 및 심각한 비즈니스 문제를 비롯한 수십 여 개의 보안 사고를 식별하기 위해 어떻게 수 백만 개에 달하는 보안 및 네트워크 이벤트를 정렬합니까?

대답: 상세한 최신 네트워크 맵을 확보하십시오. 방화벽 구성을 분석하여 NAT 영역까지 포함하여 별개의 모든 이벤트를 정규화하고 연관시킵니다. 이벤트 상세 정보를 평가하여 잘못된 경보와 해결된 문제를 제거합니다. 대응 계획을 통합하고 결과를 보고합니다. 위 과정을 계속 반복하든지 CS-MARS를 설치하도록 합니다.



확실한 보안 사고

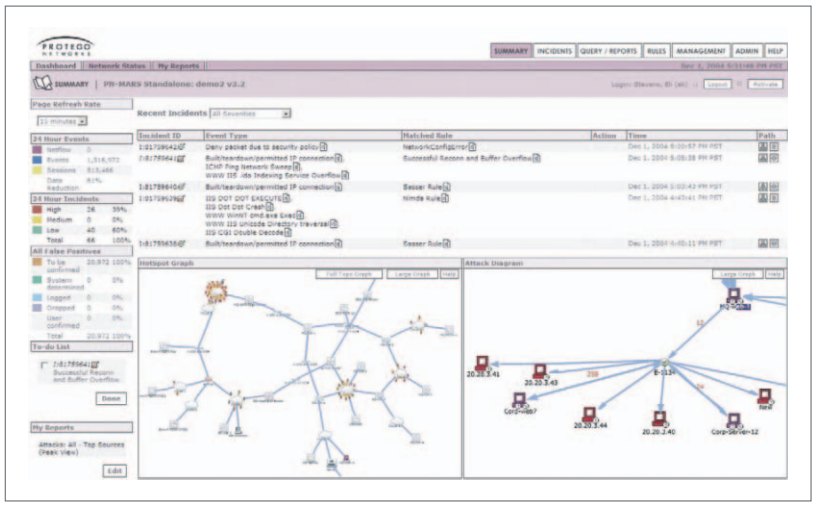
격리된 이벤트를 기록하는 이유. 보안 사고 대응 조정 및 자동화.

해결 및 복구를 위해 상당한 시간이 소모되는 분석 과정이 필요한 이벤트가 종종 발생합니다.

위협을 식별, 검사, 확인 및 차단하는 프로세스를 버튼 하나만 눌러서 신속하게 수행합니다.

보안 사고 시각화 및 인프라를 활용한 차단

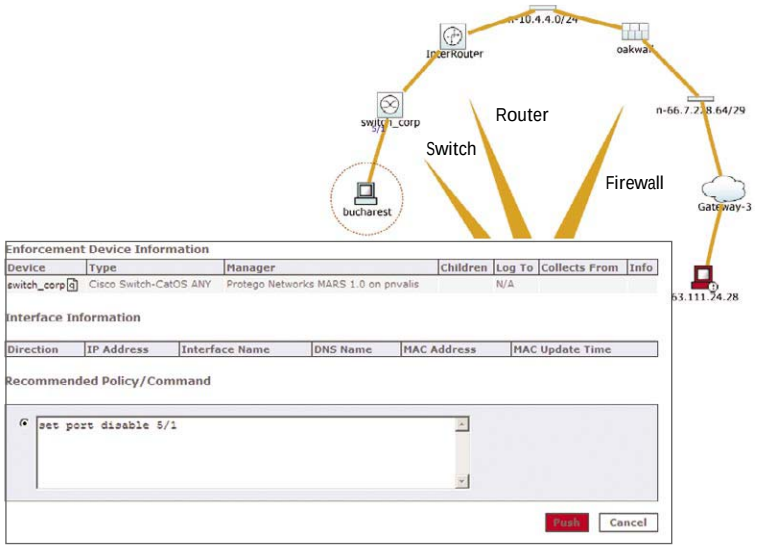
CS-MARS의 성능을 알 수 있는 가장 좋은 곳은 대화식 보안 관리 대시보드(dashboard)입니다. 운영자 GUI는 실시간 핫스팟, 보안 사고, 공격 경로 및 정밀 검사로 구성된 토폴로지 맵을 제공하므로 확실한 위협을 신속하게 확인할 수 있습니다.



SureVector™ 분석에서는 시스코 규칙 상호연관성 분석을 통해 생성된 보안 사고를 처리하며 공격지점에서 목적지까지 전체 공격 경로의 장비들에 대한 토폴로지를 분석하여 위협이 확실한지 아니면 이미 처리되었는지 결정합니다. 이러한 자동화된 프로세스를 수행하기 위해 방화벽 및 침임 탐지 애플리케이션, 타사의 취약성 평가 데이터로부터 로그를 분석하고, CS-MARS 취약성 탐색을 통해 오탐 정보를 제거합니다. 사용자가 시스템을 미세 조정하여 신속하게 오탐 정보를 추가로 줄일 수 있습니다.

모든 보안 프로그램의 최종 목표는 시스템을 온라인에서 제대로 동작시키는 것입니다. 즉, 보안 노출을 예방하고, 보안 사고를 차단하며, 복구를 촉진하는 것입니다. CS-MARS은 시스템을 침범하여 손상시키는 공격에 연관된 모든 구성 요소를 운영자가 신속하게 파악하도록 도와줍니다.

AutoMitigate™ 성능은 공격 경로상의 관문 장비들을 식별하고 장비에 따른 적절한 명령을 자동생성하여 위협을 차단하도록 도와줍니다. 또한 MAC 주소, Windows 워크스테이션 이름, VPN 사용자 이름 및 최초 홉 스위치 포트와 같은 여러 필수 특성을 자동으로 식별합니다. 이 결과를 사용하여 공격을 신속하고 정확하게 차단하고 인프라를 활용하여 피해를 최소화할 수 있습니다.

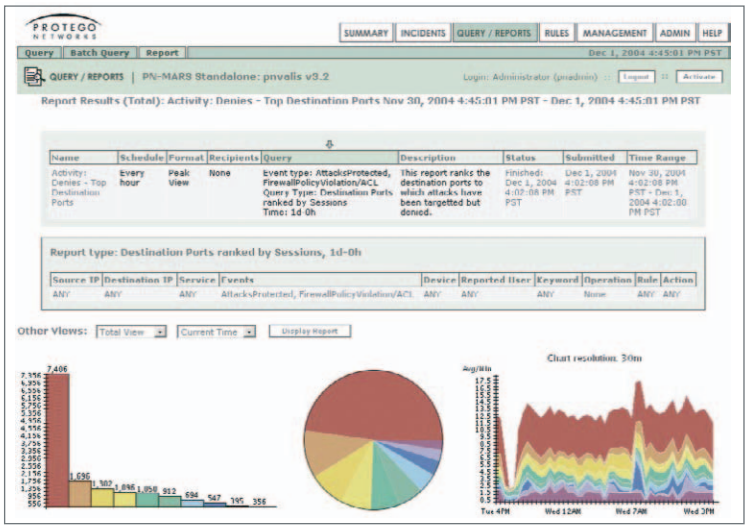


인프라를 활용한 자동화된 차단

실시간 검사 및 규정 준수 리포팅

CS-MARS의 사용이 쉬운 분석 구조는 기존의 보안 작업 플로우를 능률화함으로써 일상적인 운영이나 특별한 감사를 위해 사례 지정, 검사, 에스컬레이션(escalation), 알림 및 주석 기능을 자동화합니다. CS-MARS는 예전의 이벤트를 분석하도록 공격을 그래픽으로 재현하고 저장된 이벤트 데이터를 검색할 수 있습니다. 이 시스템은 실시간 및 연속적인 데이터 마이닝 작업을 위해 임시 질의를 완벽하게 지원합니다.

CS-MARS는 운영 요구사항을 충족시키고 Sarbox, GLBA, HIPAA, FISMA 및 Basel II를 비롯한 규정 준수 작업을 지원하기 위해 수많은 미리 지정된 리포트를 제공합니다. 직관적인 리포트 생성기는 100개 이상의 표준 리포트를 수정할 수 있으며 대응 계획 및 복구 계획, 보안 사고 및 네트워크 행위, 보안 상태 및 감사 그리고 부서별 리포트를 위한 새로운 리포트(데이터, 동향 및 차트 형식)를 만들 수 있습니다. 시스템은 또한 일괄 리포팅 및 전자메일 리포팅을 제공합니다.



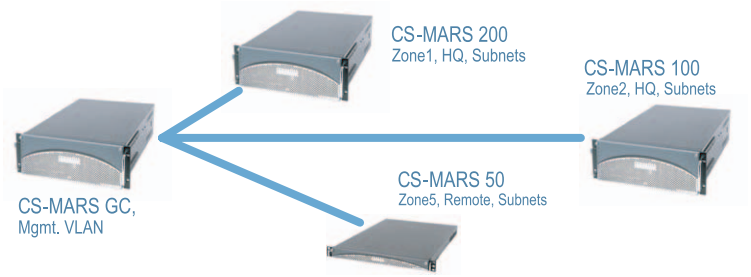
규정 준수 및 운영 관리 리포팅

신속한 설치 및 확장 가능한 관리

CS-MARS가 네트워크에 설치되는 위치는 Syslog, SNMP 트랩을 송수신할 수 있고 표준 프로토콜 또는 공급업체 전용 프로토콜을 통해 네트워크 및 보안 장비와 안전한 세션을 구성할 수 있는 위치입니다. 연결하기만 하면 작동하며 추가적인 하드웨어, 운영 체제 패치, 라이센스 또는 전문가의 관여가 필요 없습니다. CS-MARS 어플라이언스를 가리키도록 로그 소스를 구성하고 토폴로지 검색을 시작하고 웹 GUI를 통해 로그 소스를 정의하기만 하면 됩니다.

어플라이언스는 역할 기반 관리를 지원하는 안전한 웹 기반 인터페이스를 통해 중앙에서 관리됩니다. 옵션으로 선택할 수 있는 CS-MARS GC 어플라이언스는 광범위한 보안 작업을 중앙에서 관리하여 전체 엔터프라이즈를 하나의 뷰로 제공합니다. 시스템이 액세스 권한, 구성, 업데이트, 커스터마이즈된 규칙 및 리포트 템플릿을 배포할 수 있으며 로컬로 처리되는 신속한 질의와 리포팅을 통해 복잡한 검사를 통합할 수 있습니다.

로컬 CS-MARS 어플라이언스가 엔터프라이즈상에서 질의와 규칙을 실행하는 동안, CS-MARS GC(글로벌 컨트롤러) 어플라이언스에서의 신속한 중앙 분석을 위해 결과가 효율적으로 구축되어 통합됩니다. 이 확장형 아키텍처는 분산 처리 및 저장 수준을 한 단계 더 높여줍니다. 이 결과 더 경제적인 배치가 가능하며 관리성이 향상되므로 지리적으로 분산된 대규모 조직의 요구사항을 충족시킵니다.



CS-MARS 사양

세션 기반의 동적 상호연관성 분석

- 자동화된 NAT 정규화를 통한 세션 기반 이벤트 병합
- NetFlow 프로필을 비롯한 이상 현상 탐지
- 동작 기반 및 역할 기반의 이벤트 상호연관성 분석
- 광범위한 기본 제공 규칙 및 사용자 정의 규칙
- 커스터마이즈 규칙 및 키워드 분석을 지원하는 GUI 규칙 정의

토폴로지 검색

- 레이어 3 및 레이어 2; 라우터, 스위치, 방화벽 등
- 네트워크 IDS: 블레이드 및 어플라이언스
- 수동 검색 및 예약 검색
- SSH, SNMP, 텔넷 및 장비 전용 커뮤니케이션

취약성 분석

- 토폴로지에 따른 공격 경로 분석
- 스위치, 라우터, 방화벽 및 NAT 구성 분석
- 취약성 분석(VA: Vulnerability Analysis) 스캐너 데이터 캡처 및 상호연관성 분석
- 네트워크 및 호스트 기반 지문에 의해 트리거되는 보안 사고
- 확실하지 않은 정보에 대한 자동화된 분석과 사용자 조정된 분석

보안 사고 분석 및 대응

- 개별화된 보안 이벤트 관리 대시보드(dashboard)
- 전체 규칙 컨텍스트로 세션 기반 이벤트 표시
- 정밀 검사를 사용하여 그래픽으로 공격 경로 시각화
- 최적의 장애 지점 식별 및 확실하지 않은 정보 평가
- 차단이 적용될 수 있는 장비의 명령어 생성 및 푸시(라우터, 스위치, 방화벽)
- 순차적인 공격 패턴을 그래픽으로 상세하게 표시
- 즉각적인 보안 사고 정보: 규칙, 원시 이벤트, CVE 및 차단
- 공격자 ID: MAC, 워크스테이션 이름, VPN 사용자 이름 등
- 이벤트 지식 데이터베이스: CVE 참조, 영향을 받은 시스템, 권장 대응 및 패치

Model	CS-MARS 20	CS-MARS 50	CS-MARS 100e	CS-MARS 100	CS-MARS 200	CS-MARS GC
EPS*	500	1,000	3,000	5,000	10,000	n/a
NetFlow flows per sec	15,000	25,000	75,000	150,000	300,000	n/a
Storage**	120GB	120GB	750GB	750GB	1TB	1TB
Rack Size	1RU	1RU	3RU	3RU	4RU	4RU

*EPS: 동적 상호연관성 분석 및 모든 기능이 활성화되어 있는 경우 초 당 최대 이벤트.

질의 및 리포팅

- 수많은 기본 질의와 커스터마이즈 질의를 지원하는 GUI
- 100개 이상의 리포트: 관리, 운영 및 규제
- 무제한적인 커스터마이즈 리포트를 위한 직관적인 리포트 생성
- HTML 및 CSV 내보내기를 지원하는 데이터, 차트 및 동향 형식
- 리포트 시스템: 임시, 일괄, 템플릿 및 전자메일 전송

관리

- 안전한 웹 인터페이스(HTTPS); 역할 기반 관리, 전체 사용자 감사 추적
- 보안 사고 에스컬레이션, 작업 플로우 및 알림: 전자메일, 페이지, Syslog, SNMP
- 여러 CS-MARS에 대한 CS-MARS GC(글로벌 컨트롤러) 계층적 관리
- 입증되고 자동화된 업데이트: 장비 지원, 새로운 규칙 및 기능
- 연속 압축된 원시 데이터와 보안 사고를 오프라인 NFS 스토리지에 보관

장비 지원(최신 목록은 웹 사이트에 있음)

- **네트워크:** Cisco IOS 11.x, 12.x, Catalyst OS 6.x, NetFlow v5/ v7, IDS/IPS, NAC ACS 3.x, Extreme Extremeware 6.x
- **방화벽/VPN:** Cisco PIX Firewall 6.x, IOS Firewall, FWSM 1.x, 2.2, VPN Concentrator 4.0, Checkpoint Firewall-1 NG FPx, VPN-1, NetScreen Firewall 4.x, 5.x, Nokia Firewall 등
- **IDS:** Cisco NIDS 3.x, 4.x, Cisco NIDS 모듈 3.x, 4.x, Enterasys Dragon NIDS 6.x, ISS RealSecure Network Sensor 6.5, 7.0, Snort NIDS 2.x, McAfee Intrushield NIDS 1.x, NetScreen IDP 2.x, Symantec ManHunt 3.x 등
- **VA:** eEye REM 1.x, FoundStone FoundScan 3.x 등

- **호스트 보안:** CSA(Cisco Security Agent) 4.x, McAfee Entercept 2.5, 4.x, ISS RealSecure Host Sensor 6.5, 7.0, Symantec AntiVirus 9.x 등
- **호스트 로그:** Windows NT, 2000, 2003(에이전트 및 에이전트 없음), Solaris, Linux
- **애플리케이션:** 웹 서버(IIS, iPlanet, Apache), Oracle 9i, 10i Database Audit Logs, Network Appliance NetCache
- 모든 애플리케이션 Syslog를 집계하고 모니터링하는 범용 장비 지원

하드웨어

- 특별한 용도의 19인치 랙 장착 가능 어플라이언스; UL, FCC, CE 및 VCCI 승인
- 보안이 강화된 OS, 서비스가 줄어든 방화벽
- 2개의 10/100/1000 이더넷 인터페이스, 복구 미디어가 있는 DVD-ROM
- 스토리지**: CS-MARS 50 RAID 0 / CS-MARS 100, 200, GC RAID 10 핫스왑 가능
- 전원: 300W 전원 CS-MARS 20, 50 / 리던던시형 로드 공유 500W 전원
  CS-MARS 100, 200, GC
  모든 모델은 120/240 V 자동 전환입니다.

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		