데이터 시트

CS-MARS GC (글로벌 컨트롤러)

네트워크 및 보안 정보 과부하를 중앙에서 관리합니다.
정교한 위협 및 Zero Day 공격에 대처합니다.
보안 사고 대응 및 운영 비용을 능률화합니다.
감사 및 규정 준수 작업을 자동화합니다.

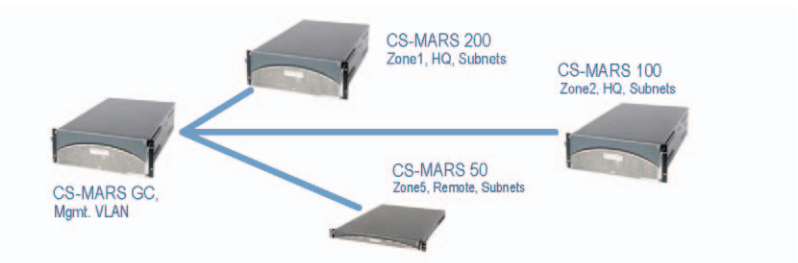
시스코 CS-MARS는 네트워크 및 보안의 원시 데이터를 실제적인 정보로 변환하여 확실한 보안 사고를 차단하고 규정을 준수하도록 합니다. 설치와 사용이 쉬운 이 위협 차단 어플라이언스 제품군은 운영자가 기존의 네트워크 및 보안 인프라를 활용하여 우선 순위가 높은 위협에 집중하고 이를 탐지, 차단 및 보고할 수 있도록 도와줍니다.

CS-MARS GC는 시스코의 전체 CS-MARS 제품군과 함께 사용되어 대규모의 원격 분산 조직 내에서 보안 관리를 단순화하고 자동화합니다. 이 선택적인 어플라이언스는 계층적 관리와 여러 어플라이언스를 확장하는 프로세스를 제공하여 지역별, 보안 팀간에 중앙화된 관리, 기업 전체의 위협 시각화, 고급 분석 및 보안 대응 협업을 가능케 합니다.

애플리케이션

수천 대의 네트워크 장비, 보안 대응책 및 애플리케이션 플랫폼으로 구성된 대규모 인프라에서는 수 백만 개의 이벤트가 발생할 수 있으며 단일 CS-MARS가 제공하는 것 이상의 처리 및 온라인 스토리지 용량이 필요할 수 있습니다. 부서별 조직과 지리적으로 분산된 환경에서는 위치, 시간대, 직원, 애플리케이션 및 보안 정책이 다른 경우가 흔하며 보다 독립된 보안 제어가 필요할 수 있습니다.

또한 서비스 제공업체는 고객 중심의 확장형 보안 관리 및 사고 대응 성능을 자체 운영 센터에서 제공하면서도 고객의 액세스, 무결성 및 프라이버시 문제를 완화할 수 있는 방법을 찾고 있습니다. 여러 개의 CS-MARS 위협 차단 어플라이언스를 로컬로 구현하여 IT 직원이 CS-MARS GC 대시보드를 통해 로컬 어플라이언스의 유지 관리, 전체 기업 보안 상태 파악, 분산된 보안 사고 대응, 광범위한 감사 수행, 규정 준수 리포트 생성 등을 수행할 수 있습니다.



중앙 집중식 관리

GC 어플라이언스는 중앙 위치에 설치가 가능하며 여러 CS-MARS 어플라이언스를 커뮤니케이션하고 관리하기 위한 편리한 구성을 제공합니다. 사용자가 해당 인프라에 가장 경제적인 CS-MARS 어플라이언스를 로컬로 구현할 수 있습니다. 각 CS-MARS 어플라이언스가 독자적으로 작동하여 구역(Zone)이라고 불리는 로컬 인프라 내에서 원시 이벤트 집계, 보안 사고의 상호연관성 분석, 불확실한 정보 감소, 검사 능률화, 인프라를 활용한 완화 기능 등을 제공합니다. CS-MARS GC가 구성되면 모든 구역의 보안 사고를 결합하고, 유지 관리 및 질의 프로세스를 촉진시킵니다. CS-MARS GC를 활용하여 여러 어플라이언스를 하나의 어플라이언스로 효율적이고 효과적으로 관리할 수 있습니다.

직관적인 글로벌 관리 콘솔을 통해 GC 관리자가 해당 구역(Zone)과 지역에서 발생하는 보안 사고 및 네트워크 이상을 기업 전체의 토폴로지 뷰로 신속하게 볼 수 있습니다. 고급 웹 GUI는 신속한 공격 확인, 경로 분석, 검사 및 대응 성능을 제공함으로써 MAC 주소, Windows 워크스테이션 이름, VPN 사용자 이름, 최초 홉 스위치 포트, 시간대 및 위치를 식별할 수 있도록 합니다.

로컬 CS-MARS 어플라이언스가 보안 사고를 식별하고 질의를 실행하는 동안, CS-MARS GC에서의 신속한 중앙 집중식 분석 및 보고를 위해 결과가 효율적이고 안전하게 구축되어 통합됩니다. 이 때 네트워크와 WAN 연결에는 영향을 미치지 않습니다.

CS-MARS GC 어플라이언스가 액세스 권한, 구성, 업데이트, 커스터마이즈된 규칙 및 리포트 템플릿을 배포할 수 있으며 효율적인 관리를 위해 복잡한 검사를 통합할 수 있습니다.

사양

관리

- 안전한 웹 인터페이스(HTTPS), 역할 기반 관리, 전체 사용자 감사 추적
- 여러 CS-MARS 어플라이언스에 대한 계층적 관리
- 액세스 권한, 구성, 업데이트 등을 중앙 집중식으로 관리
- 규칙, 질의 및 리포트 템플릿을 중앙에서 만들고 배포
- 비즈니스/관리 컨텍스트에 따라 장비 자산 그룹화(예: 재무용 서버)
- 연속 압축된 보안 사고를 오프라인 NFS 스토리지에 보관

보안 사고 분석 및 대응

- 여러 구역에 걸쳐있는 보안 사고를 보여주는 기업 전체의 토폴로지 뷰
- 상호연관성을 분석하여 보안 사고 압축 및 구축(로컬 CS-MARS와 CS-MARS GC로 구축)
- 공격 핫스팟, 벡터, 규칙 컨텍스트 및 세부 정보를 나타내는 고급 웹 기반 GUI
- 사후 분석을 위해 공격을 그래픽으로 재현하고 저장된 이벤트 데이터를 검색
- 최적의 보안시행 장비 식별(라우터, 스위치, 방화벽)
- 자동화된 차단 시행 장비 명령어 생성
- 보안 사고 확대 보고, 워크플로우 및 알림: 전자메일, 페이지, Syslog, SNMP
- 이벤트 지식 데이터베이스: CVE 참조, 영향을 받은 시스템, 권장 대응 및 패치

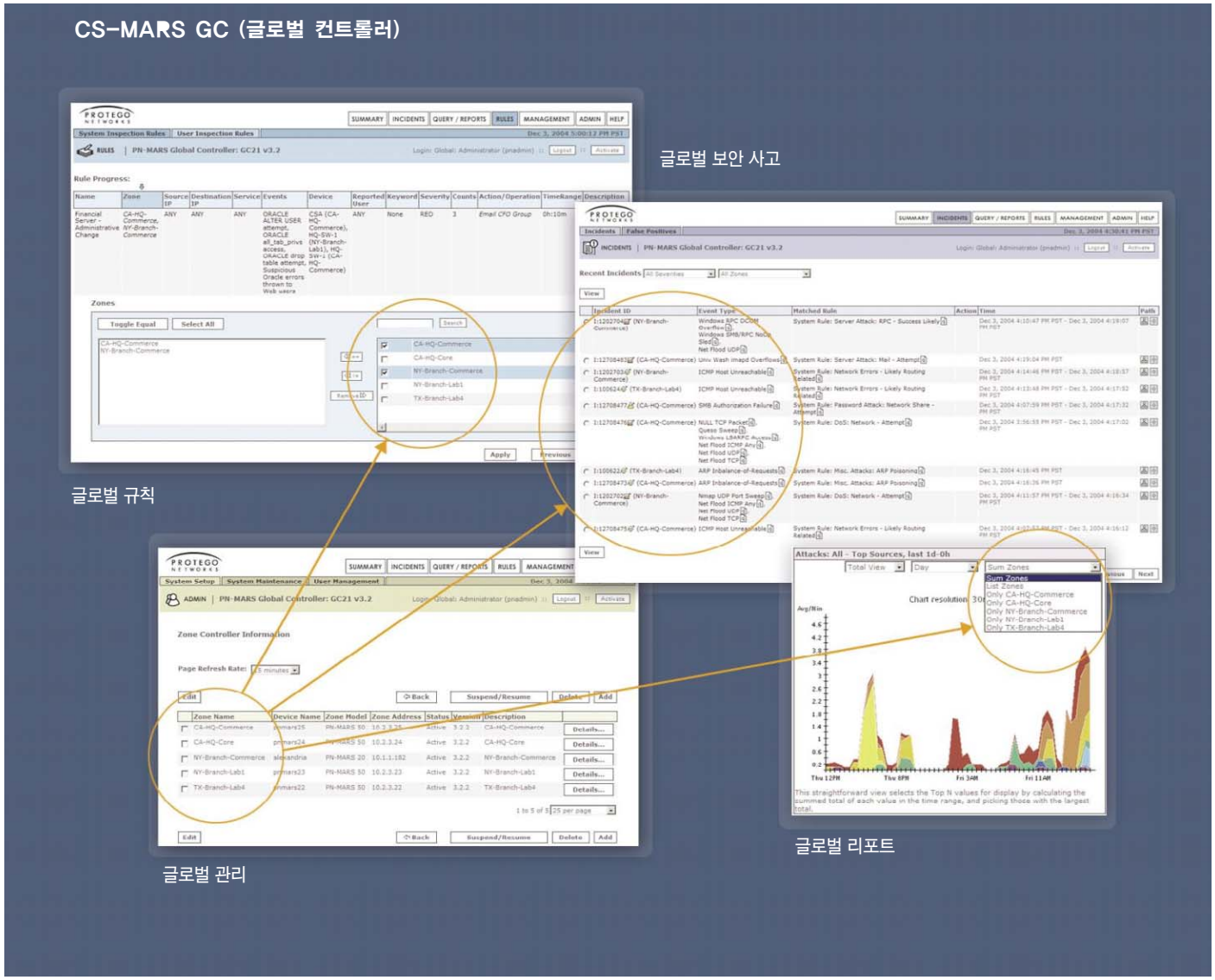
글로벌 규칙, 질의, 리포트

- GC에서 실행된 규칙, 질의 및 리포트는 설치된 CS-MARS 어플라이언스들에 효율적으로 처리됩니다.
- 규칙, 질의 및 리포트 생성을 능률화하는 직관적인 분석 구조
- 여러 구역(Zone) 및 자산 그룹상에서 전체 규칙 커스터마이즈 및 애플리케이션
- 키워드 검색 지원을 비롯하여 보다 정밀한 보안 사고 식별 이벤트 질의
- 범용 장비 로그 지원 기능으로 모든 애플리케이션 로그를 분석/상호연관성을 분석 가능
- 완벽한 커스터마이즈 기능이 있는 리포트

- 운영, 부서별, 보안 사고 및 네트워크 활동 및 감사 리포트
- Sarbox, GLBA, HIPAA, FISMA, Basel II 규정 준수 요구사항을 지원하는 리포팅 기능
- 데이터, 동향 및 차트 형식을 지원하는 일괄 및 실시간 리포트

하드웨어 사양

- 특별한 용도의 19인치 4RU 랙 장착 가능 어플라이언스: UL, FCC, CE, VCCI 승인
- 보안이 강화된 OS, 서비스가 줄어든 방화벽
- 2개의 10/100/1000 이더넷 인터페이스, 복구 미디어가 있는 DVD-ROM
- 스토리지: 1TB, RAID 10 핫스왑 가능
- 전원: 리던던시형 로드 공유 500W 전원, 120/240 V 자동 전환



요약

시스코의 솔루션은 네트워크 및 보안 정보 과부하를 효율적으로 관리하고, 정교한 공격과 Zero Day 위협에 대응하며, 보안 사고 대응 통합 및 보안 운영 비용을 능률화하고, 회사가 감사 및 규정 준수 요구사항을 충족시킬 수 있도록 합니다. CS-MARS GC는 한 단계 더 높은 중앙 집중식 관리, 인텔리전트 처리 및 스토리지를 제공하여 대규모의 원격 분산 조직에서 요구되는 엔터프라이즈 위협 차단을 제공합니다.

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		