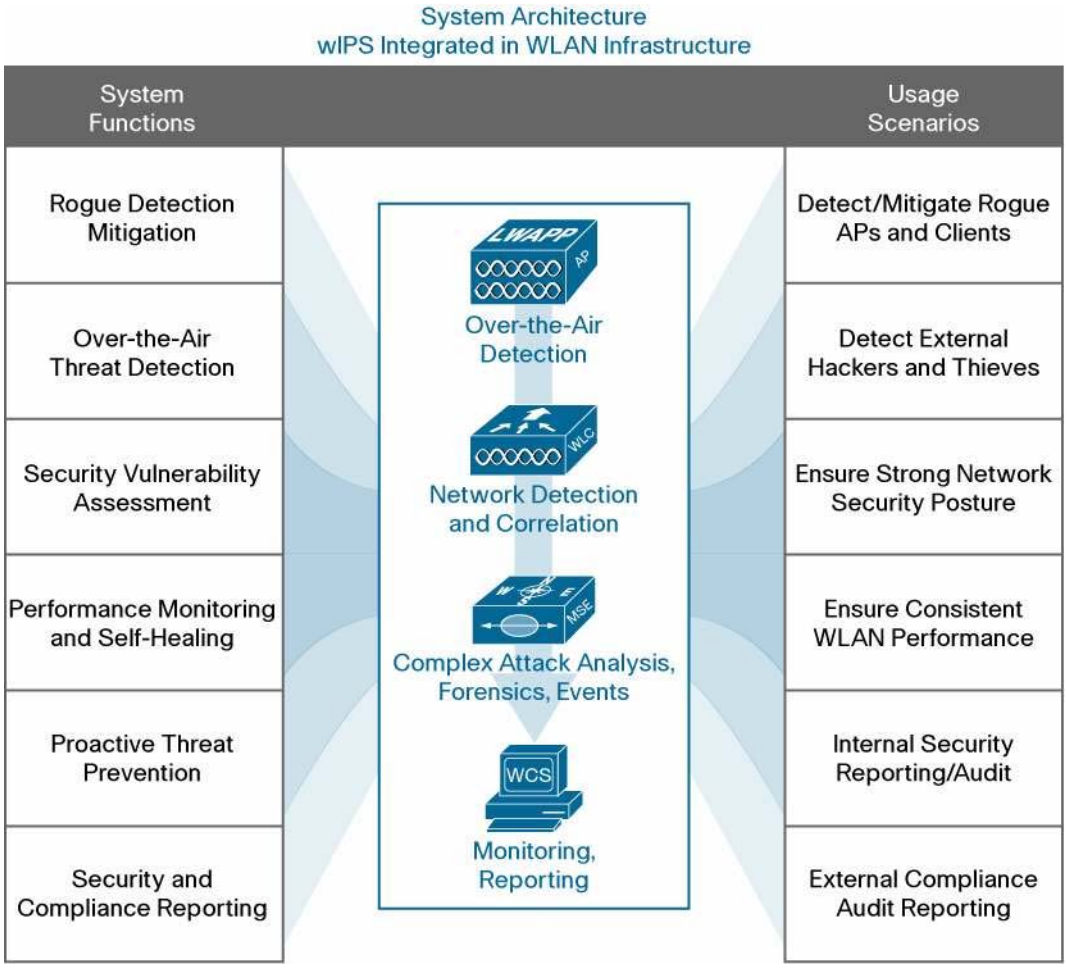
시스코 적응형 무선 침입 방지 시스템

제품 개요

무선 스펙트럼은 많은 IT 조직에게 새로운 개척 분야라고 할 수 있습니다. 다른 네트워크 미디어처럼, 무선 스펙트럼에 대한 보안이 제대로 이루어져야 하며 이는 무선 네트워크가 사이트에 구축되지 않은 경우에도 마찬가지입니다.

Cisco® Adaptive Wireless IPS(WIPS)는 Cisco Unified Wireless Network 인프라에 통합되어 무선 네트워크에 대한 특정 위협을 탐지하고, 악성 공격을 제어하며, 보안 취약점 및 성능 저하의 원인에 대한 정보를 제공합니다. Cisco Adaptive WIPS(그림 1)는 무선 위협을 탐지, 분석 및 식별할 수 있는 기능을 제공하고, 보안 및 성능과 관련된 문제를 중앙에서 관리하여 이를 제어 및 해결합니다. 또한, Cisco Adaptive WIPS는 대부분의 무선 공격을 막아내는 견고한 무선 네트워크 코어를 위한 사전 위협 방지 기능을 제공하며, 유/무선 네트워크에 계층화된 위협 방지 수퍼셋을 제공하는 Cisco Self-Defending Network 보안 포트폴리오를 보강할 수 있습니다.

그림 1. Cisco Adaptive Wireless IPS: 시스템 개요



기능 개요

Cisco Adaptive WIPS는 무선 네트워크 인프라에 완벽한 무선 위협 탐지 및 제어 기능을 포함시켜 업계에서 가장 포괄적이면서도 정확하며 운영 비용도 저렴한 무선 보안 솔루션을 제공합니다. Adaptive WIPS의 기능으로는 악성 액세스 포인트 및 클라이언트와 Ad-Hoc 연결 탐지 및 제어, 무선 해킹 및 위협 탐지, 보안 취약점 모니터링, 성능 모니터링 및 자가 옵티마이제이션, 사전 위협 방지를 위한 네트워크 강화, 완벽한 무선 보안 관리 및 보고 등이 있습니다. Cisco Unified Wireless Network를 기반으로 구축되었으며 효율적인 Cisco Motion의 이점을 활용하는 Adaptive WIPS는 보다 간편해진 설치로 언제든지 기업용으로 사용될 수 있는 엔터프라이즈 레디(enterprise ready) 솔루션입니다.

무선 네트워크 인프라의 통합 기능

Cisco Adaptive Wireless IPS는 시스코 무선 LAN 컨트롤러, 시스코 액세스 포인트, Cisco Mobility Services Engine, Cisco Wireless Control System 등을 비롯한 Cisco Unified Wireless Network의 인프라 컴포넌트로 직접 통합됩니다. 이 통합된 무선 위협 탐지 및 방지 기능은 비용을 절감시키고, 운영을 효율화하며, 포괄적인 보호 기능을 제공합니다.

무선 IPS를 무선LAN 인프라에 통합하면 무선 IPS 및 무선LAN 서비스의 단일 인프라를 사용함으로써 얻게 되는 비용 및 운영 효율성 측면의 이점 외에도 더 많은 혜택을 누릴 수 있습니다. 즉, 인프라 통합으로써 단독 오버레이 무선 IPS 시스템으로는 구조상 구현키 힘든 수퍼셋 기능을 구현할 수 있습니다. 네트워크 관리자는 Cisco Adaptive WIPS의 인프라 통합 아키텍처를 통해 제공되는 새로운 기능을 이용해 다음을 할 수 있습니다.

- **전체적인 그림 보기:** 일반적인 WIPS 솔루션은 오로지 RF 에어 모니터링에 의존해 위협을 탐지합니다. Adaptive WIPS는 위협 탐지 및 성능 모니터링을 위한 실시간 장치 인벤토리 분석과 네트워크 구성 분석뿐만 아니라 액세스 포인트와 무선LAN 컨트롤러 내에서 네트워크 트래픽 및 이상 분석을 실시함으로써 RF 에어 모니터링을 보완하고 있습니다. 이러한 접근 방식을 통해 보다 정확하고 철저하게 위협을 탐지할 수 있습니다.
- **올바른 해결 조치 취하기:** Cisco Adaptive WIPS는 위협, 취약점 및 성능 문제를 단순히 탐지하는 데서 끝나지 않고 적절한 해결 조치까지 제시해 줍니다. Adaptive WIPS는 무선 LAN 인프라에 통합되어 수동적인 모니터링에 그치는 것이 아니라 인프라 상에서 보안 위협과 성능 문제를 실시간으로 해결합니다.
- **전체 무선LAN 풋프린트 이용하기:** Adaptive WIPS는 네트워크의 모든 액세스 포인트를 사용하여 악성 장치를 탐색하고 문제를 제어할 수 있습니다. 이 기능은 위치 탐색의 정확도를 높이고 제어 가능한 범위를 확대합니다.
- **유연한 설치 아키텍처 활용하기:** Cisco Adaptive WIPS는 풀타임 에어 모니터링 전용 액세스 포인트 또는 무선LAN 사용자를 지원하는 액세스 포인트를 사용할 수 있습니다. 이와 같은 유연성을 활용하여 특정 사이트에 맞는 적당한 보안 모델을 구현할 수 있습니다.

종합적인 보안 및 정확한 탐지

에어 모니터링, 네트워크 트래픽/이상 분석, 네트워크 장치 및 토폴로지에 대한 실시간 정보, 네트워크 구성 분석을 모두 결합한 시스코의 위협 탐지에 대한 고급 접근 방식은 Cisco Adaptive WIPS 분석 엔진의 종합적인 이벤트 보기를 통해 나타납니다. Adaptive WIPS는 다양한 정보를 이용하여 OTA(Over the Air) 서명만으로는 추적할 수 없었던 이벤트를 탐지하고, 참/거짓에 대한 결정의 정확도를 높여 오탐지율은 줄이면서 동시에 효율성은 높여 줍니다.

코어 탐지 기능을 바탕으로 설계된 Cisco Adaptive WIPS는 보안 이벤트를 자동으로 분류 및 제어할 수 있는 유연한 규칙을 사용자에게 제공함으로써 공격을 다양하게 분류하고 있습니다. 시스템 자체의 정확도가 뛰어나기 때문에 이 자동 분류 기능을 이용하면 시스템에 의해 탐지된 잠재적 위협에 대한 수동 조사와 관련된 운영비를 크게 줄일 수 있습니다.

시스코는 이러한 고급 탐지 및 분류 기술을 광범위한 공격, 취약점 및 성능 탐지 라이브러리에 결합합니다. 탐지된 이벤트 클래스의 예로는 악성 액세스 포인트/클라이언트, Ad-Hoc 연결, 해커 액세스 포인트(예: 허니팟 및 이블 트윈스), 네트워크 정찰, 인증 및 암호화 확인, 메시지 가로채기(man-in-the-middle) 공격(예: 스푸핑 확인/식별), 재전송 공격, 프로토콜 공격, DoS 공격, OTA 및 네트워크 보안 취약점, 성능 문제(채널 간섭, 커버리지 홀 등) 등이 있습니다.

사전 위협 방지 기능으로 보완된 Adaptive WIPS

네트워크를 보호하는 가장 좋은 방법은 피해를 입기 전에 공격을 예방할 수 있는 시스템을 설계하는 것입니다. Cisco Unified Wireless Network에 내장된 네트워크 보안 강화 기능은 Adaptive WIPS 솔루션을 보완하여 다음과 같은 사전 위협 방지 기능을 제공합니다.

- **네트워크에서 보안 공격자 제거:** 클라이언트 제외 정책(Client Exclusion Policy)은 가장 높은 수준의 사용자 인증 실패 및 IP 주소 스푸핑에 자동으로 대응할 수 있습니다.
- **네트워크 정찰, 스푸핑 및 메시지 가로채기(man-in-the-middle) 공격 약화:** IEEE 802.11w 기반인Cisco Management Frame Protection은 무선LAN 관리 프레임을 암호화하고 인증하여 많은 일반적인 OTA(Over the Air) 공격을 방어합니다.
- **데이터 도난 방지:** 강력한 사용자 인증, WPA2(Wi-Fi Protected Access 2) 및 802.11i 암호화 표준을 통해 무선LAN을 경유하는 네트워크와 데이터에 대한 액세스를 보호합니다.
- **악성 액세스 포인트 잠금:** 시스코 액세스 포인트에서 802.1X 유선 포트 인증을 사용하면 악성 액세스 포인트가 유선 네트워크에 침범할 가능성이 사실상 사라집니다.

기능 및 이점: 기술 개요

다음 섹션에서는 Cisco Adaptive Wireless IPS 솔루션의 각 기능 영역 및 관련 이점에 대해 개략적으로 설명합니다.

악성 탐지, 분류 및 제어

Cisco Adaptive Wireless IPS 기능은 표 1과 같이 악성 탐지 및 제어 기능을 제공합니다. 악성 액세스 포인트 및 클라이언트는 네트워크에 대한 백도어 액세스를 가능케 하여 무선 클라이언트들이 데이터를 훔치는 데 이용될 수 있습니다. Adaptive WIPS는 악성 액세스 포인트, 악성 클라이언트, 스푸핑된 클라이언트 및 클라이언트 Ad-Hoc 연결을 탐지하고, 사용자가 지정한 규칙에 기반하여 자동 분류하며, 제어합니다.

표 1. 주요 기능 및 이점: 악성 탐지, 분류 및 제어

주요 기능	이점
탐지	
채널 검사 설정/해제	802.11 관련 스펙트럼에서 모든 채널의 악성 액세스 포인트, 악성 클라이언트, 스푸핑된 클라이언트 및 클라이언트 Ad-Hoc 연결을 탐지합니다.
서명 기반/네트워크 분석 기반 탐지	악성/Ad-Hoc/스푸핑 탐지의 범위와 정확성이 늘어나고, 직원의 수동 위협 조사가 감소됩니다.

주요 기능	이점
스펙트럼 인텔리전스	블루투스, 레이더 및 마이크로파와 같은 비802.11 주파수 대의 악성 장치와 DoS를 탐지합니다.
이벤트 분류	
사용자 지정이 가능한 악성 이벤트 자동 분류	사용자 지정 분류 규칙에 기반하여 악성 이벤트의 위협 수준을 자동으로 분류함으로써 직원의 개입이 감소됩니다.
악성 스위치 포트 추적	탐지된 악성 액세스 포인트가 고객 네트워크에 있는지를 확인하여 직원이 위협을 평가하기 위해 직접 조사하는 일이 줄어듭니다.
악성 액세스 포인트의 실제 위치 탐색	플로어 맵에 악성 액세스 포인트 및 클라이언트의 위치를 표시하여 악성 위협을 평가하고 제거하는 작업을 용이하게 합니다.
제어	
악성 스위치 포트 비활성	악성 액세스 포인트가 연결된 이더넷 포트를 원격으로 비활성시켜 제어 속도가 빨라집니다.
OTA(Over the Air) 제어	설치된 시스코 액세스 포인트를 사용하여 악성 액세스 포인트, 클라이언트 및 Ad-Hoc OTA(Over the Air) 연결을 제어합니다. 그 결과 제어 속도가 빨라지고 제어 규모가 확장됩니다.
자동/수동 제어	고객 리스크 환경 및 운영 모델에 맞는 유연한 제어가 가능합니다.

OTA(Over the Air) 공격 탐지

Cisco Adaptive WIPS는 표 2와 같이 OTA(Over the Air) 공격 탐지 기능을 제공합니다. OTA 공격은 고객의 RF 환경 가까운 곳에 있는 해커에 의해 발생합니다. RF 신호는 벽을 침투할 수 있기 때문에 사무실 앞 주차장에 앉아 있는 누군가가 공격자일 수도 있습니다. 공격 유형에는 크랙, DoS(서비스 거부), 메시지 가로채기 공격(man-in-the-middle), 위장 공격(impersonation attack) 및 새로운 알 수 없는 공격 등이 있습니다.

표 2. 주요 기능 및 이점: OTA(Over the Air) 공격 탐지

특징	이점
다양한 탐지 범위	
네트워크 정찰 및 프로파일링 탐지	트래픽 동작을 분석하고 패턴 매칭을 통해 Netstumbler, Wellenreiter, Kismet, 허니팟 액세스 포인트 등과 같은 툴 및 기술을 탐지하며 해커가 공격 방법을 찾고 있다는 조기 경보를 발행합니다.
인증 및 암호화 크래킹 탐지	트래픽 동작을 분석하고 패턴 매칭을 통해 AirSnarf, AirCrack, ASLEAP, Chop-Chop 등과 같은 툴 및 기술을 탐지하며 잠재적인 데이터 도난 또는 시도된 데이터 도난에 대한 경보를 발행합니다.
악의적인 DoS 또는 부주의에 의한 DoS 탐지	트래픽 동작을 분석하고 패턴 매칭을 통해 802.11 프로토콜 남용, AirJack, RF 방해 전파, 자원 고갈 공격 등과 같은 툴 및 기술을 탐지하며 잠재적인 네트워크 서비스 손상 또는 시도된 네트워크 서비스 손상에 대한 경보를 발행합니다.
메시지 가로채기(Man-in-the-Middle) 공격 탐지	트래픽 동작을 분석하고 패턴 매칭 및 인증 방식을 통해 재전송 공격(Replay attacks), 위장 액세스 포인트, 802.11 프로토콜 조작 등과 같은 툴 및 기술을 탐지하며 잠재적인 데이터 도난 또는 허가 받지 않은 네트워크 액세스에 대한 경보를 발행합니다.
위장(impersonation) 및 스푸핑 탐지	트래픽 동작을 분석하고 패턴 매칭 및 인증 방식을 통해 MAC/IP 스푸핑, 위장 액세스 포인트, Evil Twin(불법 복제 AP) 액세스 포인트, DHCP(동적 호스트 구성 프로토콜) 스포일링 등과 같은 툴 및 기술을 탐지하며 잠재적인 데이터 도난 또는 허가 받지 않은 네트워크 액세스에 대한 경보를 발행합니다.
제로데이 공격 탐지	트래픽 동작을 분석하여 새로 유입되었거나 이전에는 분류되지 않았던 공격 방식을 탐지하며 잠재적인 위협에 대해 경보를 발행합니다.
지속적인 위협 및 취약점 연구/탐지 기술 개발	시스코는 새로운 공격 기법을 발견하고, 악용될 소지가 있는 취약점을 발견하기 위해 네트워크를 사전에 분석하는 작업을 전담하는 '무선 위협 및 취약점 연구팀'을 운영하여 Cisco Adaptive WIPS 탐지 기술이 최신 공격을 앞서 나갈 수 있도록 하고 있습니다.
이벤트 분류 및 튜닝	
기본 탐지 프로파일	고객 유형에 따라 사용자 정의된 기본 탐지 튜닝 및 프로파일링을 통해 시스템을 시작하자마자 효율적으로 운영할 수 있으며 시스템을 튜닝하는 데 있어 유용합니다.
지식 기반 튜닝	탐지 튜닝은 WCS의 위협 지식 기반에 연결되어 있어 운영자에게 튜닝 지침뿐만 아니라 공격 유형, 탐지 방법을 쉽게 설명하여 제공하기 때문에 초보 보안 운영자들도 쉽게 튜닝할 수 있습니다.

보안 취약점 모니터링

Cisco Adaptive WIPS는 표 3과 같이 보안 취약점 모니터링 기능을 제공합니다. 무선 네트워크의 보안 상태(security posture)를 실시간으로 파악하는 것은 공격을 예방하는 데 있어 가장 중요합니다. Cisco WCS 관리 시스템은 보안이 약한 네트워크 또는 정책에 어긋나는 구성을 사전에 끊임없이 조사함으로써 365일 24시간 무선 취약점 자동 모니터링 및 평가를 자동으로 수행합니다.

표 3. 주요 기능 및 이점: 보안 취약점 모니터링

특징	이점
자동화된 365일 24시간 구성 분석	모든 무선 컨트롤러, 액세스 포인트 및 관리 인터페이스 보안 구성을 분석합니다. WCS는 OTA(Over the Air) 취약점 스니핑(sniffing)에만 의존하기보다는 실제 구성을 분석하는 방식을 통해 관리 프로토콜 보안 분석 및 네트워크 상의 보안 서비스 운영 분석 등과 같은 보다 정확하고 깊이 있는 분석을 제공합니다.
산업 모범사례 또는 특정 고객의 보안 정책 분석	WCS에는 무선 보안 취약점 평가와 관련된 업계 최고의 경험과 사례들이 반영되어 있습니다. 또한, WCS Config Audit 기능을 사용하면 고객의 자체적인 특정 보안 정책에 어긋나는 구성을 분석할 수 있습니다. 이러한 이중적 접근 방식은 뛰어난 유연성을 제공하며 취약점 분석의 범위를 확장시켜 줍니다.
광범위한 취약점 식별	허가 받지 않은 관리 및 네트워크 액세스, 데이터 도난, 메시지 가로채기(man-in-the-middle) 공격, DoS 공격, 프로토콜 공격 등을 야기할 수 있는 취약점을 식별하고, 무선 네트워크에서 실행할 보안 서비스에 대한 조언을 제공합니다.

성능 모니터링 및 자동 옵티마이제이션

Cisco Adaptive WIPS는 표 4와 같이 성능 모니터링 기능을 제공합니다. 네트워크의 성능이 저하되면 네트워크 및 애플리케이션 가용성에 영향을 미치고, 악의적이거나 의도하지 않은 공격을 야기할 수도 있습니다. 본 시스템은 RRM(무선 자원 관리)을 통해 우수한 성능과 네트워크 자가 치료 기능을 제공합니다. 노이즈 및 간섭 정보와 클라이언트의 신호 세기 및 기타 데이터 등을 이용하여 사용채널을 동적으로 지정하고 액세스 포인트 전송 전력을 실시간으로 조정합니다. 이를 통해, 동일 채널 간섭을 피하며, 실패한 장치를 피해 루트를 지정하고, 커버리지 홀을 최소화할 수 있습니다.

표 4. Features and Benefits: Performance Monitoring and Auto-Optimization

주요 기능	이점
네트워크의 상태 및 성능에 대한 지속적인 실시간 모니터링	OTA(Over the Air) 간섭, 악의적이거나 의도하지 않은 공격을 방어합니다.
RF 도메인 내의 문제를 자동으로 수정	관리자가 개입할 필요 없이 RF 기반 DoS 등과 같은 문제를 해결하기 때문에 최소한의 운영 인력으로 네트워크 가동 시간을 최대화할 수 있습니다.
전문가 수준의 스킬이 필요 없는 완벽한 RF 관리	본 시스템에는 RF 관리 전문 기술이 탑재되어 네트워크 운영 직원의 부담을 덜어 줍니다.

관리, 모니터링 및 보고

Cisco Adaptive WIPS는 표 5와 같이 완벽한 보안 관리, 모니터링 및 보고 기능을 제공합니다. WIPS 관리는 Cisco WCS와 완벽하게 통합되어, 무선 네트워크 및, 무선 보안 운영을 위한 통합 도구를 제공합니다. 무선 네트워크 및 무선 보안 관리의 통일을 통해 액세스 포인트 및 클라이언트 장치 인벤토리와 보안 정책을 일치시키고 이벤트 관리 및 리포트를 단순화함으로써 관련 문제를 최소화합니다.

표 5. 주요 기능 및 이점: 관리, 모니터링 및 보고

주요 기능	이점
무선 네트워크 및 보안을 위한 단일 관리 플랫폼	
실시간 장치 인벤토리	액세스 포인트 및 클라이언트 장치 인벤토리는 이중 입력 또는 상호 공급업체 관리 통합 문제 없이도 항상 최신 상태를 유지하기 때문에 관리 오버헤드를 최소화하는 동시에 악성공격을 아주 정확하게 탐지할 수 있습니다.
가상 관리 도메인	WIPS는 다른 무선 관리 역할 또는 지역으로부터 무선 보안 관리 및 모니터링을 분리할 수 있도록 합니다.
단일 관리 플랫폼	모든 WIPS 및 일반 무선 관리는 WCS에서 수행되기 때문에 서로 다른 플랫폼에 대한 직원 교육 및 지원의 필요성이 최소화됩니다.
Cisco Unified Wireless Network 기능과 통합	WIPS는 일반 무선 네트워크 구성, 무선 보안 정책 정의 및 위치 서비스 운영을 통합한 단일 워크플로우를 제공합니다.
명령 허가 및 감사 추적	AAA(인증, 권한 부여 및 계정 관리)를 통해 모든 관리 명령에 대해 권한을 지정하고 기록된 구성, 조사 및 제어 작업은 나중에 관리자가 추적할 수 있기 때문에 신뢰성이 강화됩니다.
엔터프라이즈 급 규모를 위한 설계	WCS는 규모가 가장 큰 환경을 위해 설계되었습니다. WCS 인스턴스 하나에 최대 3000명/개의 사용자 또는 WIPS 액세스 포인트를 지원합니다.
WCS 보안 대시보드	
단일 개요 뷰	모든 보안 이벤트 및 취약점에 대한 단일 스크린 요약 창이 간결하고 한눈에 보기 쉬운 형식으로 제공됩니다. 이벤트 종류와 개별 이벤트를 마우스로 클릭하면 상세보기가 가능하며 이로써 매일 모니터링하는 작업이 용이해 집니다.
유선 보안 통합	WCS 보안 대시보드를 통해 무선 사용자와 관련된 악성 이벤트 및 해킹 이벤트를 모니터링하여 무선 사용자의 활동을 전체 네트워크 차원에서 볼 수 있도록 해줍니다.
WCS 성능(RRM) 대시보드	
단일 개요 뷰	모든 성능 관련 이벤트에 대한 단일 스크린 요약 창이 간결하고 한눈에 보기 쉬운 형식으로 제공됩니다. 이벤트 종류와 개별 이벤트를 마우스를 클릭하면 상세보기가 가능하며 이로써 매일 모니터링하는 작업이 용이해 집니다.
WCS 이벤트 관리 및 보고	
완벽한 이벤트 포렌식	하나의 공격과 연관된 모든 트래픽을 수집하기 때문에 공격에 대한 조사 작업이 용이해 집니다.
직원에게 이벤트 경보 발행	직원에게 중요 이벤트에 대한 경보를 자동으로 발행함으로써 대응 시간을 단축할 수 있습니다. 이벤트 유형별로 완벽하게 사용자 지정이 가능합니다.
개별 관리자 보고서	개별 관리자는 각자의 성향과 책임 영역에 따라 내역 보고서를 사용자 지정할 수 있어 이벤트 분석이 보다 간결해 집니다.
보고 자동 예약	특정 시간에 자동으로 실행되도록 내역 보고서를 예약할 수 있어 워크플로우가 간결해집니다.
PCI(Payment Card Industry) 보고	PCI(Payment Card Industry) 컴플라이언스에 적합한 이벤트를 사용자 지정할 수 있으므로 감사 관련 작업이 간결해집니다.
이벤트 저장 및 보관	Cisco Mobility Services Engine에 보안 공격 이벤트가 저장되어 장기간 보관되기 때문에 내역 분석 작업이 간결해집니다.

개발 구성요소, 확장성 및 플랫폼 지원

Cisco Adaptive WIPS의 표준 구성요소는 다음과 같습니다.

- WIPS 모니터링을 위한 Cisco LWAPP 엑세스 포인트
  - Cisco Aironet® 1130 AG, 1140, 1240 AG 및 1250 시리즈 액세스 포인트는 Cisco Unified Wireless Network Version 5.2 이상과 Adaptive WIPS 기능 세트를 지원합니다.
- WIPS 모니터링 액세스 포인트를 지원하는 시스코 무선 LAN 컨트롤러
  - Cisco 2100 시리즈 무선 LAN 컨트롤러, Cisco 4400 시리즈 무선 LAN 컨트롤러, Cisco 5500 시리즈 무선 LAN 컨트롤러, Catalyst® 6500 시리즈를 위한 시스코 무선 서비스 모듈, Catalyst 3750G 통합 무선LAN 컨트롤러, Cisco 2800 및 3800 시리즈 라우터를 위한 무선LAN 컨트롤러 네트워크 모듈
  - Cisco Unified Wireless Network Version 5.2 이상부터 Adaptive WIPS 기능 세트를 지원합니다.

- Cisco Mobility Services Engine 3310 Series 및 Cisco Adaptive WIPS 소프트웨어 라이센스는 Cisco Unified Wireless Network Version 5.2 이상을 사용하여 Adaptive WIPS 기능 세트를 지원할 수 있습니다. Cisco Unified Wireless Network Version 6.0 이상을 사용할 때, 동일한 MSE 3310에서 Cisco Adaptive WIPS와 함께 여러 무선 네트워크 서비스가 존재할 수 있습니다.
  - 단일 Mobility Services Engine은 최대 2000개의 WIPS 액세스 포인트를 지원할 수 있습니다.
- Cisco Mobility Services Engine 3350 Series 및 Cisco Adaptive WIPS 소프트웨어 라이센스는 Cisco Unified Wireless Network Version 6.0 이상을 사용하여 Adaptive WIPS 기능 집합을 지원합니다. 동일한 MSE 3350에서 Cisco Adaptive WIPS와 여러 무선 네트워크 서비스가 함께 존재할 수 있습니다.
  - 단일 Mobility Services Engine은 최대 3000개의 WIPS 액세스 포인트를 지원할 수 있습니다.
- 관리, 구성 및 보고를 위해 Cisco WCS Version 5.2 이상이 요구됩니다.
  - 단일 WCS는 최대 3000개/명의 WIPS 또는 사용자 지원 액세스 포인트를 지원할 수 있습니다.
  - Mobility Services Engine은 오직 하나의 WCS 인스턴스만으로 관리됩니다. 따라서 전반적인 네트워크 확장 설계 시 이를 고려해야 합니다.
  - 단일 WCS 인스턴스는 여러 무선 네트워크 서비스 엔진을 동시에 관리할 수 있습니다.

라이센스 및 주문 정보

Cisco Unified Wireless Network Version 5.2 이상에 탑재되어 있는 Cisco Adaptive WIPS는 Cisco Mobility Services Engine에서 허가 받은 소프트웨어 기능 세트입니다. 표 6은 Adaptive WIPS에서 사용할 수 있는 모든 라이센스 수준을 나타냅니다. 이러한 라이센스 수준은 Adaptive WIPS를 실행하는 데 필요한 액세스 포인트에 따라 변경될 수 있습니다. 예를 들어, 5개의 액세스 포인트와 25개의 액세스 포인트를 합치게 되면 Adaptive WIPS를 30개의 액세스 포인트에서 실행하기 위한 라이센스가 제공됩니다.

표 6. Cisco Adaptive Wireless IPS 소프트웨어 라이센스

부품 번호	설명
AIR-WIPS-AP-5	Adaptive WIPS 소프트웨어 라이센스: 5개의 시스코 모니터-모드 액세스 포인트 지원
AIR-WIPS-AP-25	Adaptive WIPS 소프트웨어 라이센스: 25개의 시스코 모니터-모드 액세스 포인트 지원
AIR-WIPS-AP-100	Adaptive WIPS 소프트웨어 라이센스: 100개의 시스코 모니터-모드 액세스 포인트 지원
AIR-WIPS-AP-500	Adaptive WIPS 소프트웨어 라이센스: 500개의 시스코 모니터-모드 액세스 포인트 지원
AIR-WIPS-AP-2000	Adaptive WIPS 소프트웨어 라이센스: 2000개의 시스코 모니터-모드 액세스 포인트 지원

서비스 및 지원

시스코 시스템즈는 고객의 성공을 위해 다양한 서비스 프로그램을 제공합니다. 이러한 혁신적인 서비스 프로그램은 수준 높은 인력, 프로세스, 고객지원 툴 및 파트너의 기술력이 어우러진 것으로서 높은 고객 만족도를 실현합니다. 시스코는 다양한 서비스를 통해 여러분의 네트워크 투자를 보호하고 네트워크 운영을 최적화하며, 새로운 애플리케이션에 대비하여 네트워크 인텔리전스 및 비즈니스의 성능을 확장할 수 있도록 도와드립니다. 시스코 서비스에 대한 자세한 내용은 시스코 기술 지원 서비스(Cisco Technical Support Services) 또는 시스코 고급 서비스(Cisco Advanced Services)를 참조하십시오.

추가 정보

Cisco Adaptive WIPS 정보: http://www.cisco.com/go/WIPS.
Cisco Self-Defending Network 정보: http://www.cisco.com/go/SDN.
Cisco Mobility Services Engine 정보: http://www.cisco.com/go/MSE.
Cisco Unified Wireless Network 정보: http://www.cisco.com/go/wireless.

Americas Headquarters
Cisco Systems, Inc.
San Jose, CA

Asia Pacific Headquarters
Cisco Systems (USA) Pte. Ltd.
Singapore

Europe Headquarters
Cisco Systems International BV
Amsterdam, The Netherlands

Cisco has more than 200 offices worldwide. Addresses, phone numbers, and fax numbers are listed on the Cisco Website at www.cisco.com/go/offices.

Printed in USA C78-501388-01 03/09