Extreme AirDefense®

포괄적인 무선 침입 방지 시스템

하이라이트

- 무선 공격을 막기 위한 24x7x365 WLAN 네트워크 모니터링
- 업계 최고의 위협 탐지 라이브러리
- 센서 데이터의 중앙 집계 및 상호 연계, 오탐 최소화
- 다수 제품이 필요한 대규모 배포에 있어서 중앙 집중식 관리
- 공격에 신속하게 대응하는 자동 Rogue 종료 기능을 이용한 Rogue 장치 실시간 탐지, 장치를 물리적으로 제거할 때까지 네트워크 보호
- 평면도에서 Rogue 장치 찾기
- 정책 위반에 기초한 즉시 알림 및 대응을 통한 정책 시행
- 위치 포렌식 등 포렌식 조사의 가시성을 향상시키는 고급 포렌식, 장치가 어디에 있었는지 판단합니다.
- 이상 행동 탐지는 무선 트래픽 모니터링을 통해 조기 경고 표시장치 역할을 합니다.
- 규정 준수 모니터링을 위한 기본 제공 보고서(예: PCI_DSS, SOX, GLBA 등) 또는 Report-Builder를 이용한 맞춤형 보고서 생성
- Liveview는 라이브 네트워크 및 실시간 트래픽 분석을 위한 25개 이상의 요약 그래픽 시각화, 패킷 캡처, 디코딩을 제공합니다.
- 찾기 힘든 간헐적 간섭 출처까지도 모니터링하며 문제를 해결하는 스펙트럼 분석
- 무선 해커의 관점에서 원격 취약성 테스트를 하는 무선 취약성 평가
- BLE 4.0 태그 기반의 잠재적 피싱 공격을 식별하기 위해 예상하지 못한 BT 2.0 장치의 존재를 탐지하는 블루투스 모니터링

제품 개요

무선 연결은 새롭고 강력한 방식으로 통신할 수 있는 독특한 기회를 제공하지만 일련의 취약성, 복잡성, 관리 문제도 발생합니다. 사용자 및 비즈니스에 대한 보안 위험 없이 무선 네트워크를 최대한 활용하려면 정확한 도구 세트가 필요합니다.

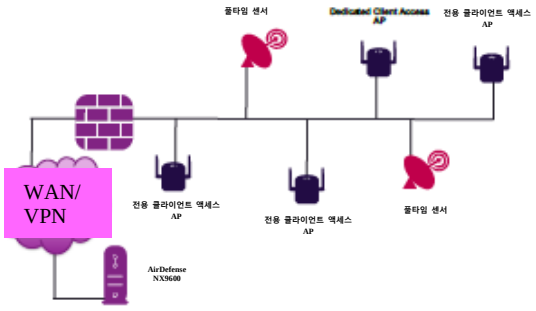
Extreme AirDefense는 무선 LAN 네트워크의 보호, 모니터링, 규정 준수를 단순화합니다. Extreme AirDefense는 연중무휴 24시간 외부 위협으로부터 네트워크를 지속적으로 보호하며, 공격이 발생할 때 IT 직원에게 이를 알려 즉각적인 대응을 가능하게 합니다. 또한 PCI-DSS, Sarbanes-Oxley, HIPAA, GLBA 등의 규정 준수를 지원합니다.

유연성

Extreme AirDefense 시스템은 보안 장치와 함께 전파 모니터링 센서 역할을 하는 일련의 액세스 포인트로 배포됩니다. 이 장치는 하드웨어 장치 또는 가상 장치로 배포할 수 있습니다. 센서들은 전용 센서로 또는 무선 공유 모드로 배포할 수 있습니다. 전용 센서는 가시성 향상을 통해 더 높은 수준의 보안을 제공합니다. 전용 감지(sensing)에는 두 가지 배치 옵션이 있으며, (1) 전체 액세스 포인트를 센서로만 사용하거나 (2) 듀얼 라디오 또는 트라이 라디오 액세스 포인트에서 하나의 액세스 포인트를 센서 전용으로 사용하고 나머지 무선 액세스 포인트는 사용자 데이터 트래픽에 사용하는 것입니다. 무선 공유 모드에서 액세스 포인트는 감지 기능에 하나의 타임 슬라이스를 할당하고 나머지 시간은 데이터 트래픽 제공에 활용합니다. 센서 역할을 하는 Extreme 액세스 포인트는 802.11a/b/g/n/ac 표준을 지원하여 2.4GHz 및 5GHz 대역을 모두 스캔하고 여러 MIMO 스트림을 수신할 수 있습니다.

확장성이 큰 아키텍처

최종 사용자 장치의 폭발적 증가와 IoT 장치의 기하급수적인 증가로 인해 무선 보안 시스템이 전파상에 존재하는 장치 수의 엄청난 증가를 따라잡는 것이 중요합니다. Extreme AirDefense 장치는 전체 시스템을 관리하는 단일 그래픽 콘솔을 제공하는 한편 다중 코어 서버와 다중 서버의 여러 코어에 걸친 확장성이 큰 아키텍처를 가지고 있습니다. 패킷 분석은 센서와 장치 간에 분할되어 필수 보안 정보만 장치에 전달하여 센서-장치 간 통신에 사용되는 대역폭 요구 사항을 최소화합니다. 이 장치는 여러 센서에 걸쳐 광범위한 트래픽 및 이벤트 상호 관계를 수행함으로써 수천 개의 센서와 수십만 개의 클라이언트 장치에 확장될 수 있는 정확하고 효율적이며 안전한 모니터링 시스템을 만듭니다.



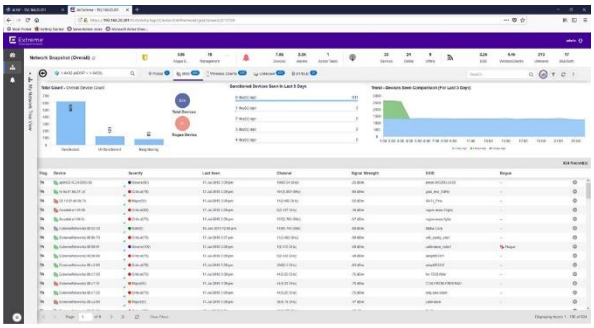
플러그 앤 플레이 기능

AirDefense 는 진정한 플러그 앤 플레이 기능을 통해 사용하기 쉽게 설계되었습니다. 설치 후 몇 분 내에 트래픽을 모니터링할 수 있으며, 무선 LAN 위협에 대한 신속한 대응을 위해 정보를 신속하게 해석하는 도구를 완전히 갖추고 있습니다.

무선 침입 방지

무선 자산의 생산성을 극대화한다는 것은 가능한 가장 강력한 보안 태세를 유지한다는 뜻입니다. AirDefense 보안 및 규정 준수 기능은 무선 네트워크 전반에 걸쳐 원활하게 작동하여 Rogue 장치의 탐지 및 무력화, 정책 시행, 침입 방지, 규정 준수를 보장합니다. 위협 완화 및 정책 시행을 위해 자동화된 도구는 위험에 대한 실시간 대응의 자신감을

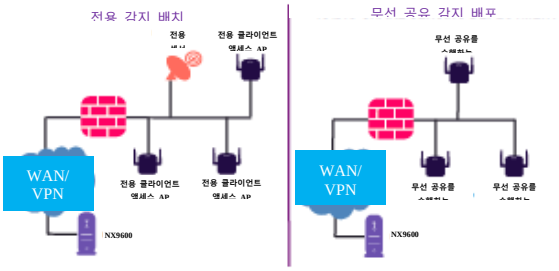
AirDefense Wireless IPS 모듈은 실시간으로 기존 위협 및 제로 데이 위협을 과거 데이터에 비추어 분석하며 무선 취약성과 비정상적인 네트워크 활동을 정확하게 탐지할 수 있습니다. 상황 인식 탐지, 상호 관계 및 다차원 탐지 엔진은 오탐 경보를 최소화합니다. 이 시스템은 광범위한 위협 라이브러리와 사용자가 정의할 수 있는 정책 설정을 통해 무선 보안 위협에 자동 대응하며 네트워크 보안 위험을 최소화할 수 있습니다.



Rogue 탐지 및 완화

AirDefense 는 전용 탐지와 무선 공유 탐지 작동 모드를 모두 지원합니다. 전자에서는 추가 액세스 포인트가 24x7 스캔을 수행하는 전용 센서 역할을 합니다. 무선 공유 모드에서는 액세스 포인트가 주로 데이터를 제공하고 정기적으로 채널에서 벗어나 다른 채널의 위협을 모니터링합니다. 이 모드에서 액세스 포인트는 인프라 채널에서 데이터를 제공하는 동시에 탐지도 수행합니다. 전용 탐지는 전파의 가시성을 향상시킵니다. 이 시스템은 탐지된 데이터 및 광범위한 상관 관계를 이용해, 유선 네트워크에 연결된 진정한 Rogue 를 식별하여 이를 인접 액세스 포인트에서 분리하고 오탐을 최소화합니다. 일단 Rogue 가 식별되는 경우, 이 시스템은 무선 종료, Rogue 가 연결된 액세스 이더넷 스위치의 포트를 찾아 비활성화하거나 ACL 을 사용하는 등 다양한 기술을 통해 Rogue 억제를 수행할 수 있습니다.

심어주며, 효과적인 보안 태세를 갖추고 있다는 마음의 평화를 선사합니다.



보안 정책 관리

관리자는 네트워크에서 시행해야 하는 보안 정책을 AirDefense를 통해 정의할 수 있습니다. 시스템이 정책 위반을 탐지하면 경보가 발생합니다. 이 시스템에는 관리자에게 이메일 보내기, syslog 또는 snmp 트랩 생성, 자동 원격 패킷 캡처 개시, 스펙트럼 분석 시작 등 경고에 기초해 특정 작업을 트리거하도록 구성할 수 있는 경고 작업 관리자가 있습니다.

Rogue 탐색

AirDefense 센서는 Rogue 액세스 포인트와 클라이언트를 찾아 평면도에 해당 위치를 표시할 수 있습니다. 이는 IT 직원이 Rogue를 찾고 연결을 끊는 것을 돕습니다.

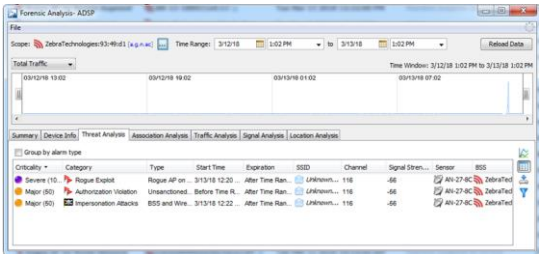
보고 및 규정 준수

AirDefense는 네트워크 보안 및 정책 준수 영역에서 광범위한 보고 기능을 제공합니다. AirDefense에는 보안, 인프라, 인벤토리, 규정 준수 등의 영역에서 몇 가지 기본 제공 보고서가 있습니다. 또한 관리자가 AirDefense 데이터베이스에서 제공하는 필드를 선택하여 맞춤형 보고서를 생성하는 Report Builder도 갖추고 있습니다. 사용자 정의 보고서는 그런 다음 사전 정의된 보고서처럼 나중에 사용할 수 있습니다.

이 모듈에는 WIP 라이선스가 필요합니다.

고급 포렌식

포렌식은 보안의 핵심입니다. 감사의 경우, IT 직원은 과거에 발생한 관심 대상 시간 간격 동안 행해진 네트워크 활동 데이터를 분석하고 추출할 수 있어야 합니다. 관심 항목에는 특정 액세스 포인트에 연결된 클라이언트 식별, 특정 대상에 대한 통신, 관심 장치들 간에 교환되는 데이터 트래픽의 양, 이러한 교환이 발생한 일시 등이 포함될 수 있습니다. 이러한 분석은 조직이 타깃 공격에 노출된 기간을 판단하고 감사를 지원하는 사실 데이터를 제공하는 것을 지원합니다. 고급 포렌식 모듈은 관리자가 무선 환경을 지속적으로 모니터링하는 기능을 제공하고, 포렌식 조사 및 네트워크 성능 문제 해결 지원에 필요한 데이터 및 분석 도구를 제공합니다.



필요한 증거의 캡처

고급 포렌식을 이용해 관리자는 몇 개월에 걸친 의심되는 장치의 활동에 초점을 맞출 수 있으며, 무선 활동의 분 단위 세부 정보를 검토하기 위해 드릴다운할 수도 있습니다. 시스템은 1분 단위로 식별된 각각의 무선 장치에 대해 300개 이상의 데이터 포인트를 저장하며, 나중에 분석할 수 있도록 광범위한 데이터를 제공합니다. 분석에 사용할 수 있는 높은 수준의 세분화된 정보는 관리자가 장기간에 걸쳐 발생하는 공격 패턴을 탐지하고 해결할 수 있도록 하는 포렌식 기능과 동일한 소스에서 행해지는 반복 공격에 대해 개별적인 별도의 사건으로 대응하는 것의 차이를 표시합니다. 이러한 강력한 포렌식 기능은 더 효율적인 네트워크 관리를 지원하고 규정 준수와 전반적인 보안 태세를 개선함으로써 비즈니스 운영을 개선합니다.

규정 준수 간소화

AirDefense 고급 포렌식 모듈은 HIPAA, GLBA, Sarbanes-Oxley(SOX), 그리고 VISA CISP 등의 PCI(Payment Card Industry) 데이터 보안 표준과 같은 많은 규정 및 국방부에서 요구하는 매우 정확한 과거 데이터를 유지관리합니다. 따라서 조직의 규정 준수(그리고 규정 준수 증명)가 자동화, 일상화됩니다.

여기에는 다음과 같은 기능이 포함됩니다.

- 과거 연관성 분석
- 과거 트래픽 분석
- 과거 채널 분석
- 과거 위치 추적 및 로밍 궤적

문제 해결 도구

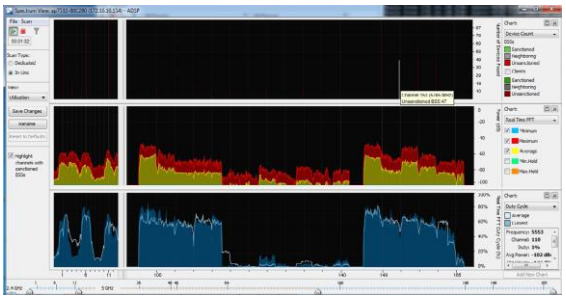
무선 통신은 이동성을 위해 설계되었습니다. 불행하게도, 매우 매력적인 바로 그 기능으로 인해 문제 해결이 매우 어려워졌습니다. 사용자가 왔다가 가고, 장치는 연결되었다가 떠나고, 간섭 소스는 여기 저기를 옮겨 다닙니다. 네트워크 연결, 활용, 가용성에 영향을 미치는 수많은 요인을 계속 추적하는 것은 힘든 작업입니다. 포렌식 모듈에서 보관되는 과거 데이터는 더 이상 작동하지 않을 수도 있는 과거에 보고된 사건을 해결하기 위한 도구를 제공합니다. 이 시스템은 식별된 각 무선 장치에 대해 채널 활동, 신호 특성, 장치 활동, 트래픽 흐름 등 분당 300개 이상의 데이터 포인트를 수집합니다. 이 동적 데이터베이스를 사용하여 네트워크 사용 추세를 차트로 나타내고, 이상 징후를 식별하며, 용량 계획을 지원할 수 있습니다.

이 모듈에는 고급 포렌식 라이선스가 필요합니다.

스펙트럼 분석

무선 네트워크는 무선 전화기, 무선 카메라, 전자레인지 등 많은 장치와 동일한 2.4GHz 및 5GHz 비면허 주파수 대역에서 작동합니다. 이러한 장치는 WLAN에 간섭을 일으킬 수 있으며 네트워크 성능에 영향을 줄 수 있습니다. 종종 모르는 사이에 여러 소스가 간섭하고 문제가 간헐적으로 발생하므로 문제 해결이 어렵기 때문에 일반적으로 실시간으로 수행되어야 합니다. 스펙트럼 분석 모듈은 이러한 유형의 간섭 문제를 해결하는 비용 효율적인 솔루션을 제공합니다.

스펙트럼 분석 모듈은 Extreme WLAN 인프라(전용 센서 또는 액세스 포인트)를 사용하여 가능한 간섭 소스를 식별/분류하며 무선 네트워크에 미치는 영향을 파악합니다. 이 모듈은 간섭 소스가 탐지되는 경우 네트워크 관리자에 대한 경고를 생성합니다. 이것은 특화된 하드웨어 없이 무선 네트워크의 물리적 계층을 볼 수 있게 하는 소프트웨어 전용 솔루션입니다. 찾기 어렵고 간헐적인 간섭 소스라 할지라도 사용하기 쉬운 그래픽 인터페이스를 통해 모니터링하고 문제를 해결할 수 있습니다. 실시간 스펙트로그램을 볼 수 있기 때문에 가능한 문제를 식별하고 무선 성능을 즉시 개선하기 위해 필요한 조치를 취하는 데 도움이 됩니다. 탐지는 중앙 콘솔에서 수행하므로 IT 직원이 간섭 원인을 판단하기 위해 현장을 방문할 필요가 없습니다.



이 모듈은 AirDefense 10.1 이상 릴리스의 WIP 라이선스와 함께 포함되어 있습니다. 이전 릴리스에서는 고급 스펙트럼 분석 라이선스가 필요합니다.

무선 취약성 평가

AirDefense 무선 취약성 평가 모듈은 무선 보안을 원격으로 테스트하는 특허 기술을 사용합니다. 이를 통해 관리자는 자동으로 액세스 포인트에 로그온하여 무선 해커의 관점에서 취약성을 테스트할 수 있습니다. Extreme 센서는 무선 침투 테스트를 수행함으로써 취약성이 악용되기 전에 이를 사전에 식별하므로 위협 관리를 개선하고 시스템을 안전하게 유지할 수 있습니다.

원격 및 자동

현재 관행에는 관리자가 취약성을 식별하기 위해 기존 취약성 평가 도구와 간헐적인 현장 무선 평가를 결합하는 것이 포함됩니다. 수동 테스트와 관련된 시간 및 비용 때문에 대부분의 조직은 일반적으로 네트워크 위치의 작은 샘플만 스캔하여 잠재적으로 취약성을 놓칠 가능성이 있습니다. AirDefense 무선 취약성 평가 모듈의 원격 테스트 기능은 수동 테스트 및 현장 방문의 필요성 및 관련 비용을 없앱니다. 스캔은 자동으로 실행되거나 요청에 따라 실행되도록 구성할 수 있으므로 강력한 네트워크 보안 태세를 유지하면서 PCI DSS 등의 규정 준수 요구 사항을 충족할 수 있습니다.

광범위한 검색을 통해 방화벽 및 무선 스위치 정책의 유효성을 검사할 수 있으며, 이와 동시에 시스템의 유선 측에 있는 자산에 대한 잠재적 진입 경로를 식별/제어할 수 있습니다. 사용자 지정이 가능한 블랙리스트를 사용해, 무선 네트워크에서 액세스해야 하거나 액세스하지 않아야 하는 특정 네트워크와 장치를 타깃팅할 수 있으므로 민감한 데이터를 보호할 수 있습니다.
무선 취약성 평가(WVA) 라이선스가 필요합니다.

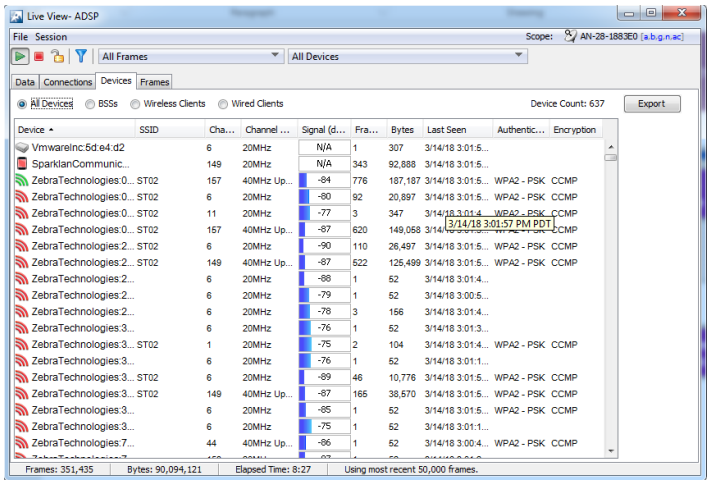
Liveview

Extreme AirDefense의 Liveview 모듈은 무선 트래픽 분석을 실시간으로 수행하는 도구를 제공합니다. Liveview를 사용하면 관리자가 센서를 스니퍼로 바꾸고 전파에서 보이는 전체 레이어-2 프레임을 캡처할 수 있습니다. 그런 다음 개별 필드를 분류하는 기능이나 다른 패킷 분석 도구(예: Wireshark)로 가져오기 위해 pcap 파일로 저장하는 기능을 통해 패킷 캡처를 Liveview UI에서 볼 수 있습니다. 원격 패킷 캡처는 최대 5개의 센서를 동시에 지원합니다.

이와 별도로, Liveview는 데이터 분석, 장치 분석, 연결 분석, 프레임 분석 등에 관해 위의 데이터에서 파생된 25개 이상의 요약 시각화를 제공하며, 이는 원격 패킷 캡처 기능 이상의 것입니다.

요약하면, Liveview는 중앙집중식 위치에서 관리할 수 있는 뛰어난 원격 문제 해결 및 데이터 분석 기능을 제공함으로써 문제가 발생하는 동안 이를 포착할 수 있게 하는 동시에 기술자 현장 파견과 관련된 높은 운영 비용을 없앱니다.

Liveview 모듈에는 WIP 라이선스가 필요합니다.



블루투스 모니터링

Extreme AirDefense는 블루투스 장치에 대한 액티브 모니터링을 수행할 수 있습니다. 이 기능을 사용하려면 블루투스 하드웨어가 내장된 액세스 포인트 모델이 필요합니다. 이 기능은 네트워크에 블루투스 프로토콜을 사용하여 무단 액세스를 허용할 수 있는 구멍을 열려고 시도하는 블루투스 스키머(skimmer) 탐지에 유용합니다. 또한 Extreme AirDefense는 BLE 4.0 프로토콜을 이용해 Google Eddystone 또는 Apple iBeacon 지원 태그에서 URL/UUID 광고를 수신할 수도 있습니다. 이렇게 하면 피싱 공격 시작을 위한 길을 여는 무단 URL을 광고할 수 있는 태그를 탐지하는 데 도움이 됩니다. 허용된 URL(예: 조직의 자체 도메인 이름을 포함하는 URL)을 필터링하도록 허용 목록을 구성할 수 있으며, 이와 동시에 승인되지 않은 URL에 대한 경고를 트리거할 수 있습니다.

이 기능은 WIP 라이선스와 함께 포함되어 있습니다.

중앙 집중식 관리

AirDefense 장치는 센서 구성 및 센서 펌웨어 관리 등 수천 개의 센서에 걸친 관리를 중앙 집중화합니다. 장치상의 소프트웨어 아키텍처는 여러 코어에 분산되어 있는 여러 엔진을 활용하지만 중앙 UI 인터페이스는 단일 창을 제공하여 내부적으로 분산되어 있는 시스템의 성질을 관리자로부터 숨깁니다.

둘 이상의 장치가 필요한 대규모 배포의 경우 AirDefense CMC(AirDefense Centralized Management Console) 모듈은 여러 장치 데이터에 대한 집계 보기 및 구성 변경을 위한 단일 지점을 제공합니다. CMC는 보안 이벤트 모니터링 간소화, 관리 자동화, 네트워크 문제 해결 시간 단축을 통해 생산성을 향상시킵니다.

이 모듈에는 다중 장치 배포를 위한 CMC 라이선스가 필요합니다.

라이선스

라이선스		
기능	**전용 센서 부품 번호**	**무선 공유 센서 부품 번호**
무선 침입 방지(WIP)	AD-SNFL-P-1	AD-FLRS-P-xx
고급 포렌식	AD-FESN-P-1	AD-FERS-P-1
무선 취약성 분석(WVA)	AD-VASN-P-1	제공되지 않음
중앙 집중식 관리 콘솔(CMC) (다중 장치 배포에만 필요함)	AD-CMC-P-1	
장치 플랫폼 라이선스(1차 서버/VM에만 필요함)	SP-SWSV-P-1	
장치 사양		
하드웨어 장치	NX-9600-100AD-WR – (2,500개의 전용 센서 또는 3,000개의 무선 공유 센서 지원). 상세 내용은 NX 9600 wspecsheet 참조	
가상 장치 지원	다음 하이퍼바이저에서 지원됨 • VMWare EXSi 5.5 이상 • Xen 4.1.2 이상	
클라이언트 콘솔 사양		
추천 시스템	Windows 7 Enterprise 또는 Windows 10 Enterprise에서 2GHz 이상의 프로세서, 1GB 이상의 RAM, 2GB 이상의 디스크 공간	
브라우저	크롬, 파이어폭스, 인터넷 익스플로러	
센서 지원 사양		
지원되는 액세스 포인트 모델	WING 액세스 포인트: AP 7632, AP 7662, AP 7612, AP 8432, AP 8533, AP 7522, AP 7532, AP 7562 익스트림 무선 액세스 포인트: AP 39XX 참고: 각각의 액세스 포인트 모델에 대한 기능 지원은 릴리스 정보를 참조하시기 바랍니다.	