심플솔루션
SIMPLE SOLUTIONS

빠르게 변화하는 무선통신을 위한 **보안 솔루션**

SECUAIR WIPS



SECUAIR

www.simplest.co.kr

01 SecuAir WIPS 도입 기대 효과

무선 보안 컴플라이언스 준수

- **국가기관, 공공기관** | 국가 정보보안 기본지침, 정보통신보안업무규정, 무선랜 보안 안내서 등을 준수하여 무선랜 환경 구축
- **금융기관** | 전자금융감독규정, 금융회사 정보기술부문 보호업무 모범규준 등을 준수하여 무선랜 환경 구축

국가 정보보안 기본지침 (2021. 11. 1)

제43조(무선랜 보안)
① 각급기관의 장은 내부망을 제외한 정보통신망에서 다음 각 호의 경우와 같이 청사 내에 무선랜(WiFi)을 구축 · 운용할 수 있다.
② 각급기관의 장은 제1항에 따라 무선랜을 구축 · 운용하고자 할 경우 국가정보원장이 배포한 「국가 · 공공기관의 무선랜 구축 및 RFID 보안가이드라인」을 준수하여 보안대책을 수립 · 시행하여야 한다. <개정 2020.7.1.>
③ 제2항에 따른 보안대책을 수립할 경우 제1항 제1호 및 제2호에 따른 무선랜에 대하여는 다음 각 호의 사항을 포함하여야 한다.
6. 무선침입방지시스템 설치 등 침입 차단대책

전자금융감독규정 [시행 2019. 1. 1.] [금융위원회고시 제2018-36호, 2018. 12. 21., 일부개정]

제15조(해킹 등 방지대책)
① 금융회사 또는 전자금융업자는 정보처리시스템 및 정보통신망을 해킹 등 전자적 침해행위로부터 방지하기 위하여 다음 각 호의 대책을 수립 · 운용하여야 한다.
1. 해킹 등 전자적 침해행위로 인한 사고를 방지하기 위한 정보보호시스템 설치 및 운영 ⑥ 금융회사 또는 전자금융업자는 무선통신망을 설치 · 운용할 때에는 다음 각 호의 사항을 준수하여야 한다.<개정 2013. 12. 3.>
2. 무선통신망을 통한 불법 접속을 방지하기 위한 사용자인증, 암호화 등 보안대책을 수립할 것
3. 금융회사 내부망에 연결된 정보처리 시스템이 지정된 업무 용도와 사용 지역(zone) 이외의 무선통신망에 접속하는 것을 차단하기 위한 차단시스템을 구축하고 실시간 모니터링 체계를 운영할 것

SecuAir WIPS 완벽한 무선 WiFi 보안 대책

불법 사용자 사내 접속
- Wi-Fi 비밀번호 유출/탈취
- 사내 불법 AP 설치

사내자료 유출
- 스마트폰 테더링 ↔ 사내 PC
- PC 테더링 ↔ 사내 PC
- 불법 AP ↔ 사내 PC

→ 완벽한 보안 대책 →

SecuAir WIPS 도입 효과



- 불법 AP 및 불법 사용자 무선 접속 탐지, 차단
- 다양항 형태의 불법 테더링 AP 탐지, 차단
- **WI-Fi 6E, 7 탐지, 차단**
- **향후 Future Wi-Fi 탐지, 차단 대응**
- 국가용 보안요안요구사항 V3.0 준수

02 SecuAir WIPS 제품 소개

하이브리드형 무선 위협 대응 SecuAir WIPS

하드웨어 타입



SecuAir Sensor (WIPS)



SecuAir WSE : 관리서버

- 하드웨어 관리서버 제공
- 하드웨어 센서 제공
- 케이블 공사 필요
- 천장에 WIPS센서 설치 필요

소프트웨어 타입



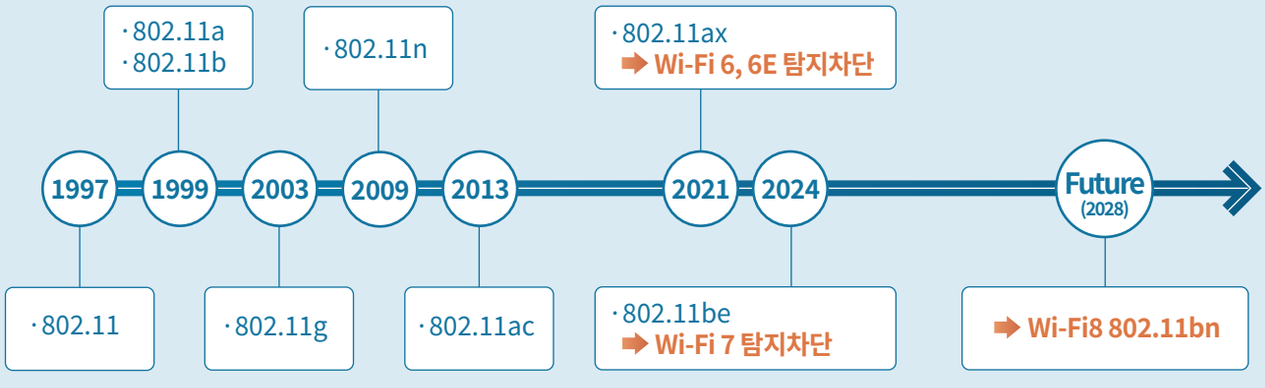
가상 머신 : SecuAir Sensor (WIPS)



SecuAir WSE : 관리서버

- 소프트웨어 관리서버 제공
- 소프트웨어 센서 제공
- 클라우드 지원 제공
- 비용 절감

빠르게 변화하는 무선통신 네트워크 기술 및 보안 이슈



03 SecuAir WIPS 특장점

365일 무중단 무선 보안위협 대응

실시간 탐지, 차단을 통한 무선 보안 위협 대응

- 자체 알고리즘을 통한 탐지 시간 최적화
- 탐지되는 즉시 차단 (1초 이내)

관리서버와 통신 장애시 WIPS 단독 동작

- 관리서버와 통신 단절 시 WIPS 단독 동작
- 탐지되는 즉시 차단 (1초 이내)

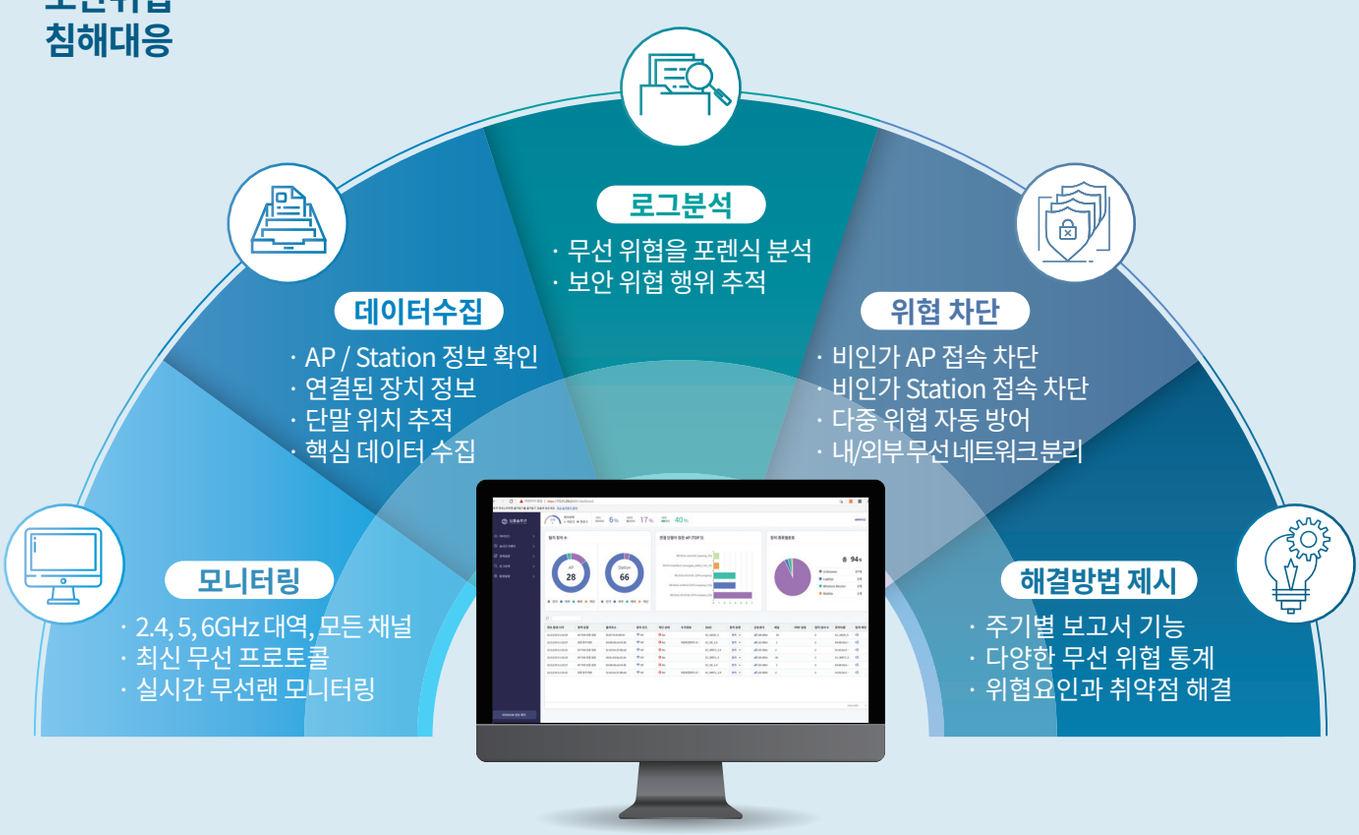
관리서버 이중화 (자동 Fail-Over 지원)

- 관리 서버 설정 동기화
- 관리 서버 Active 장애 시 Fail-Over 지원

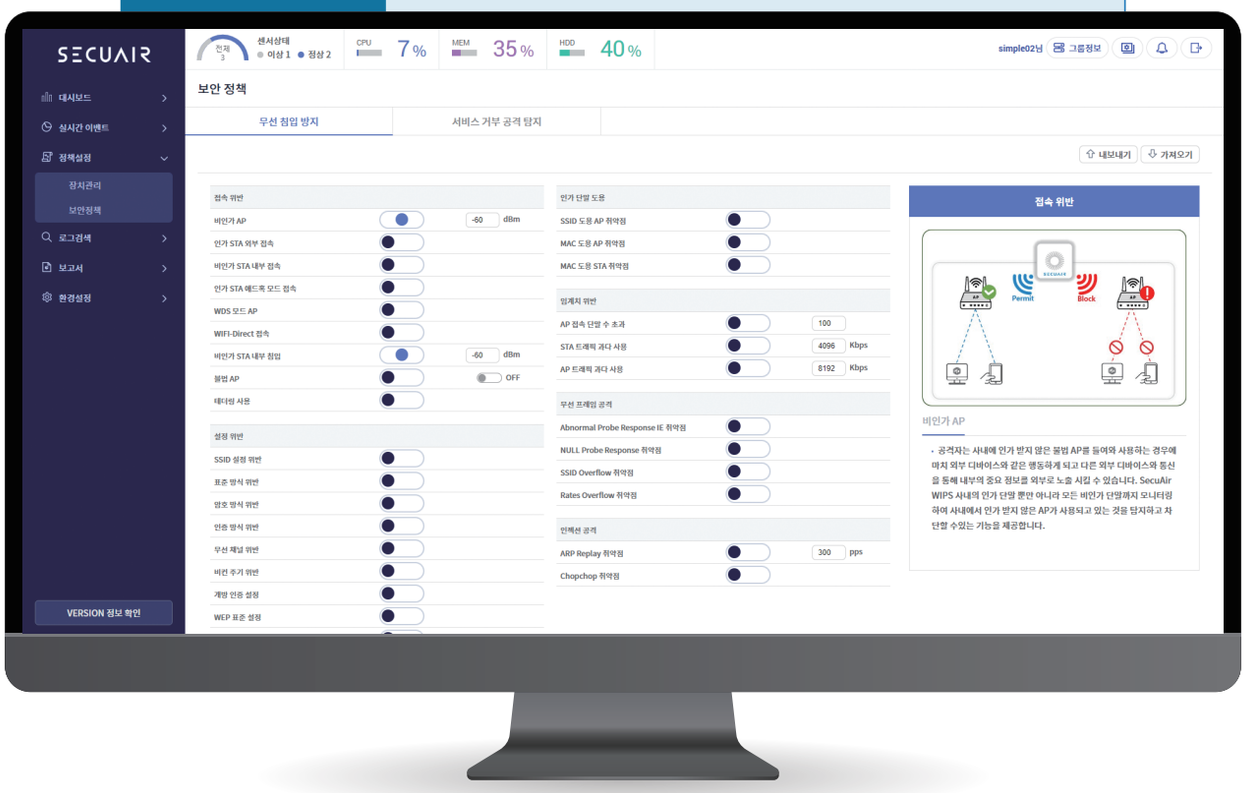
WIPS 무중단 탐지 및 차단

- WIPS 단독 동작 중 재부팅 시 탐지 및 차단

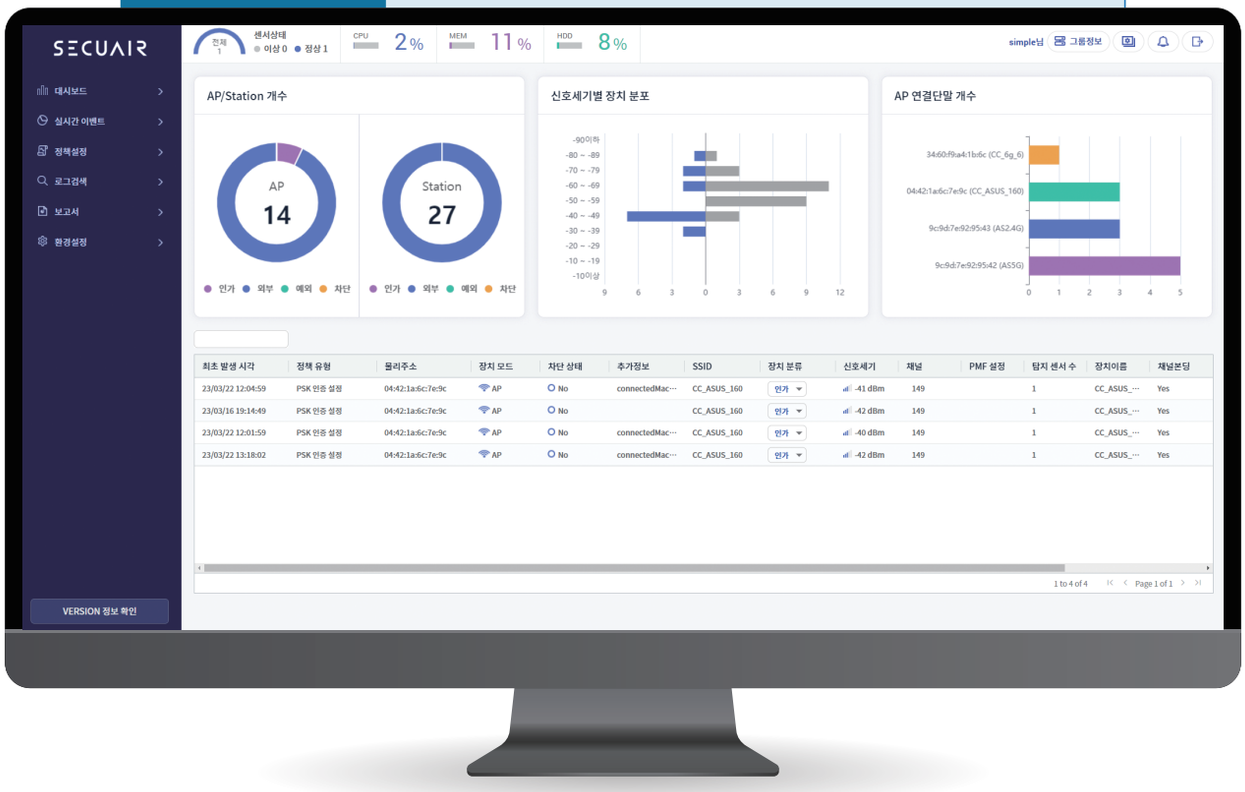
무선 보안위협 침해대응



직관성, 학습성 쉬운 정책 설정, 쉽게 학습, 쉬운 접근, 쉽게 기억

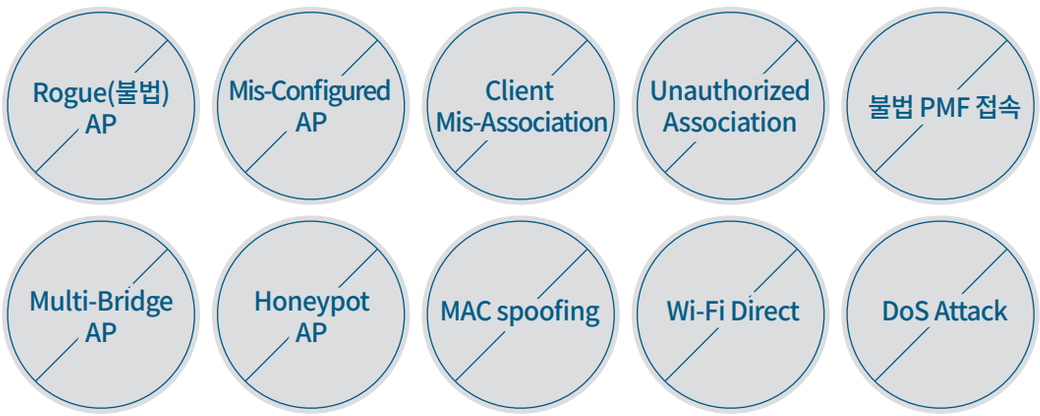


편의성, 가시성 한 화면에서 설정과 로그 조회, 보안정보 시각화



주요기능

SecuAir WIPS V2.0을 통해 탐지 및 차단되는 주요 10대 무선 위협



강력한 무선 제어기술

독자적인 PMF 차단 기능

PMF 차단

- PMF 탐지 시, 자체 로직에 의한 차단
- PMF 연결 단말 차단 기능 수행으로 인한 다른 불법 단말의 차단이 지연되는 이슈 최소화

완전한 센서 독립모드 지원

센서 독립모드

- 관리서버 및 통신 장애 발생시 WIPS의 보안 정책에 대해 센서 스스로 100% 수행
- 센서 단독 동작 중 재부팅 시 탐지 및 차단
- 관리서버 단일화 시 고가용성 보장을 통한 관리서버 추가 비용 절감

무작위(RANDOM) MAC 제어 기능

무작위 (랜덤) MAC 제어 기능

- Wi-Fi 6 이후, 추적 금지 등의 이슈로 무작위 MAC 사용이 기본으로 채택
- 무작위 MAC으로 인한 시스템 과부화 및 서비스 불가 상태 발생
  → 대규모 망 운영에서 나온 문제점 해결 (특허 기술 취득)

단말 인증 기능

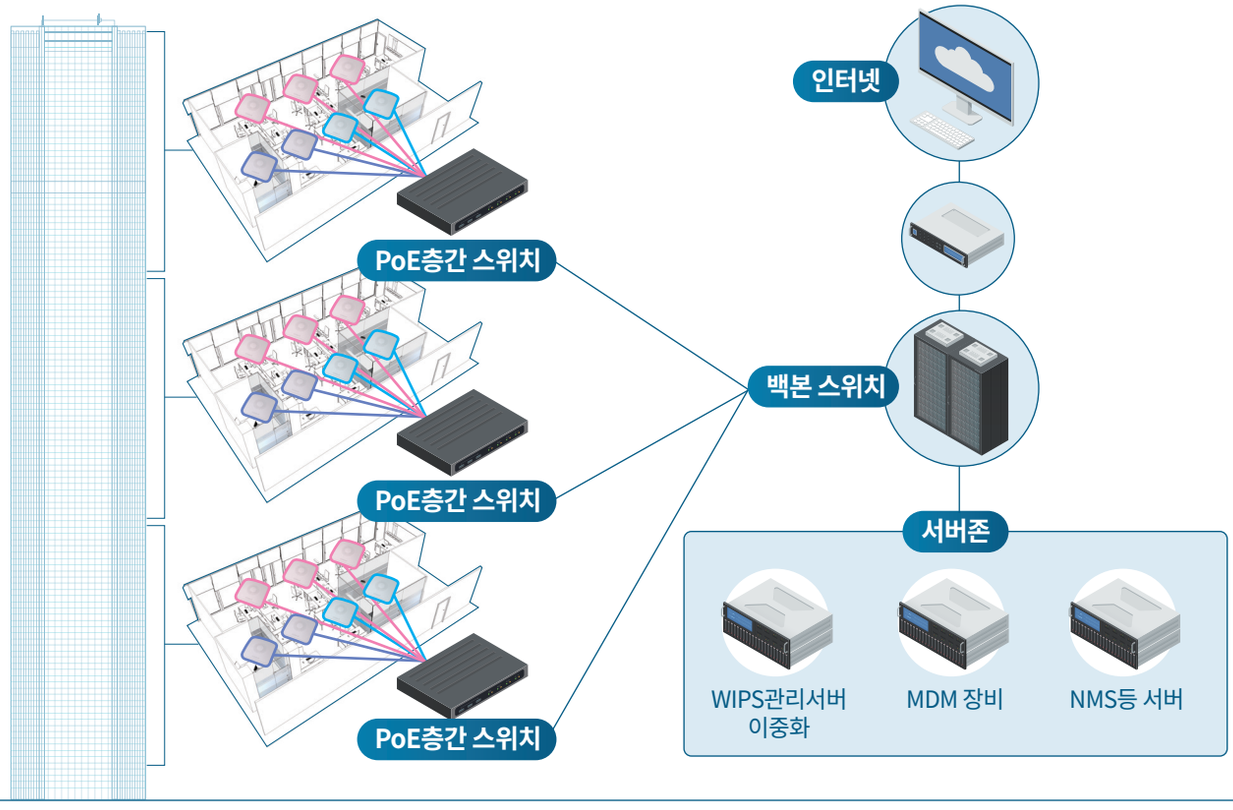
다양한 시스템과의 인증 연동을 위한 API 제공

- 인증단말 정보 연동할 수 있는 API 제공
- 인증서버 연동 위한 커스터 마이징 제공

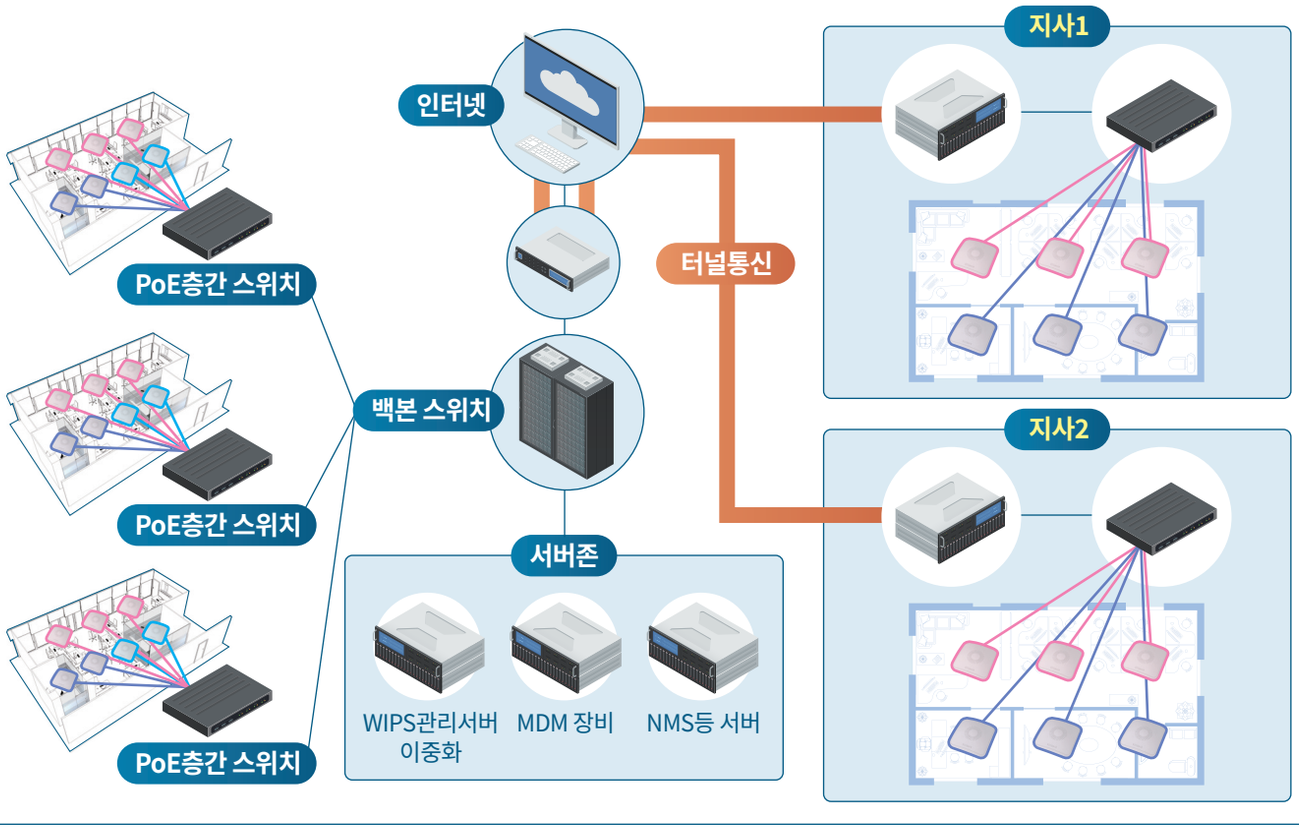
무작위 MAC 자동 인증

- 무작위 MAC, 클라우드 환경 고려하여 자동인증 서버와 어플리케이션 제공
- Wi-Fi 보안 권고사항 무작위 MAC 환경 고려한 인증 제공

구성 방안 지사가 없는 고객



구성 방안 지사가 있는 고객



Hardware Specification

모델명	SecuAir Sensor 100
Wireless Standard	· 802.11 a/b/g/n/ac/ax/be 지원 · Wi-Fi 6E (6GHz), Wi-Fi 7 지원
Wireless Security	· 802.11w 탐지 / 차단
H/W	· Quad-core 1.2GHz · Memory : 512M · Flash memory : 256 MB
Wi-Fi Antenna	· 2.4GHz / 5GHz / 6GHz
Interface	· 10/100/1000 BASE-T * 2, Console * 1
Power Supply	· PoE(802.3af/at), DC 12V Adapter · 소모 전력 : ≤ 15.4W
Size & Weight	· 크기 : 195(H)×195(W)×35(D)mm · 중량 : 450g (본체)
Temperature	· 동작 : 0~50°C, 저장 : -10~60°C
MTBF	· 70,000 시간 이상

모델명	SecuAir 관리서버 50	SecuAir 관리서버 100	SecuAir 관리서버 200	SecuAir 관리서버 500
CPU	Intel® 4 core, 3.7GHz	Intel® 4 core, 3.7GHz	Intel® 8 core, 2.6GHz	Intel® 8 core, 2.8GHz
Memory	16G	32G	64G	128G
Storage	SSD 480GB	SSD 480GB	SSD 480GB * 2 (RAID)	SSD 480GB * 3 (RAID)
	HDD 2T	HDD 2T	HDD 4T * 2 (RAID)	HDD 4T * 4 (RAID)
Interface	2x1Gbe	2x1Gbe	2x1Gbe	2x1Gbe
Power Supply	Redundant Power (450W)	Redundant Power (450W)	Redundant Power (450W)	Redundant Power (800W)
Size	1U	1U	1U	2U
Sensor(max)	50	100	200	500

* 관리서버 500 상위모델 및 소프트웨어 타입은 별도 문의

심플솔루션
SIMPLE SOLUTIONS

㈜심플솔루션은 쉬운 보안, 간결한 보안,
명확한 보안을 모토로 항상 고객과 함께합니다.



Unit 201, 2F Metamorpho Bldg, 89, Seongsuil-ro, Seongdong-gu, Seoul, Republic of Korea, 04790
+82-2-2135-3735 simple@simplest.co.kr www.simplest.co.kr