secureletter.

차세대 무선 침입 방지 시스템
DeepTrust AIR

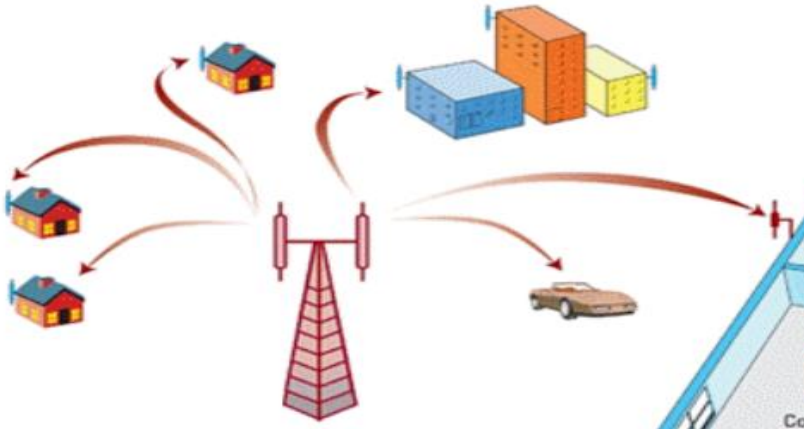
목차

1. 차세대 무선 네트워크와 보안

2. DeepTrust AIR 소개

secureletter.

무선 네트워크 표준

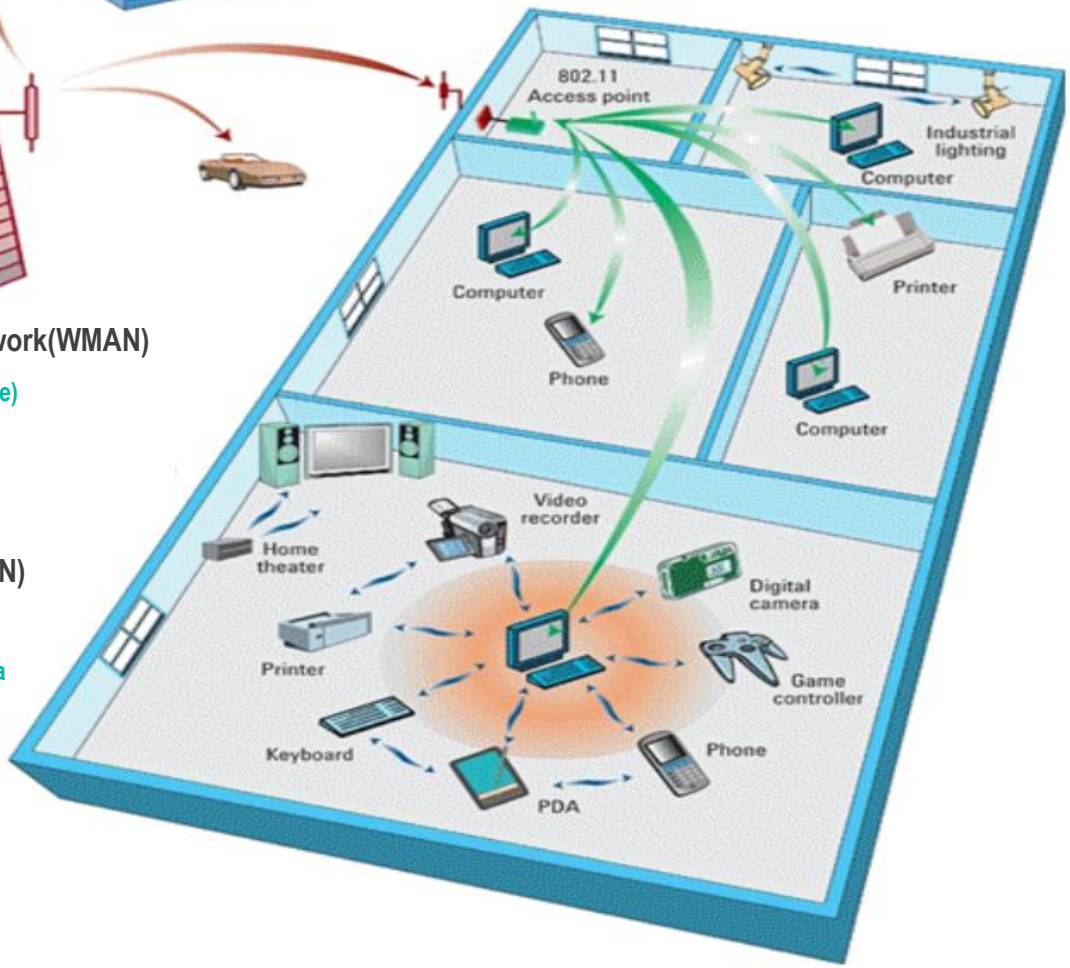


Metro Area Network(WMAN)

IEEE 802.16e(Mobile)

Local Area Network(WLAN)

Wi-Fi IEEE 802.11 b / a / g / n / ac / ax



Personal Area Network(WPAN)

- UWB IEEE 802.15.3a
- Bluetooth IEEE 802.15.1.1a
- ZigBee IEEE 802.15.4

차세대 WLAN 표준

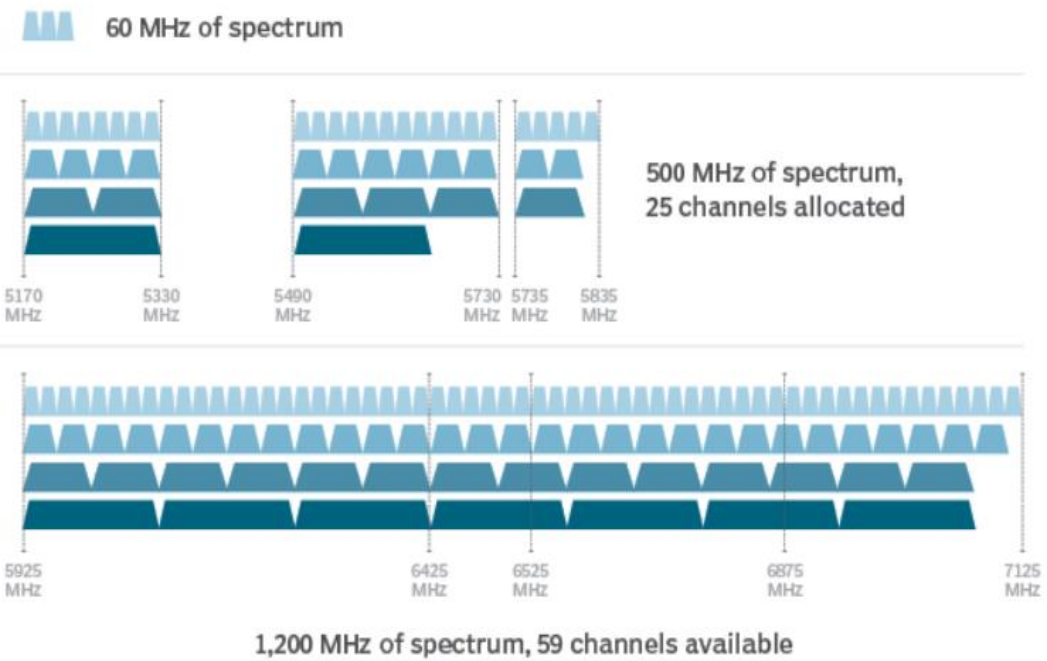
	802.11ac (Wi-Fi 5)	802.11ax (Wi-Fi 6/6E)	802.11be (expected)
Goal	Very High Throughput, Multiple of High-Definition contents delivered, Delivering network with enterprise-class speeds and latencies, High-density environments with scores of clients per AP	High Efficiency Wireless, Multi-user Transmission, Improve overlapping BSS operation in dense environments, Improvement of user experience in dense environments	Extremely High Throughput, Maximum throughput of at least 30Gbps, Improvements to worst-case latency & jitter, Frequency range between 1 & 7.250 GHz
Band(GHz)	2.4 / 5	2.4 / 5 / 6	2.4 / 5 / 6
Bandwidth(MHz)	20, 40, 80, 80+80, 160	20, 40, 80, 80+80, 160	20, 40, 80, 80+80, 240, 160+160, 320
Subcarrier Spacing(kHz)	312.5	78.125	78.125
Modulation	OFDM	OFDM, OFDMA	OFDM, OFDMA
MU-MIMO	downlink	uplink / downlink	uplink / downlink
Maximum Data Rate	6.9 Gbps(Wave2)	9.6 Gbps	46 Gbps
Data subcarrier Modulation	256 QAM	1024 QAM	4096 QAM
Core technology	Downlink Multi-user MIMO	Uplink Multi-user MU-MIMO OFDMA Spatial Reuse	Multi-link Multi AP Beamforming HARQ

Wi-Fi 6E 개요

Wi-Fi 6 vs. Wi-Fi 6E

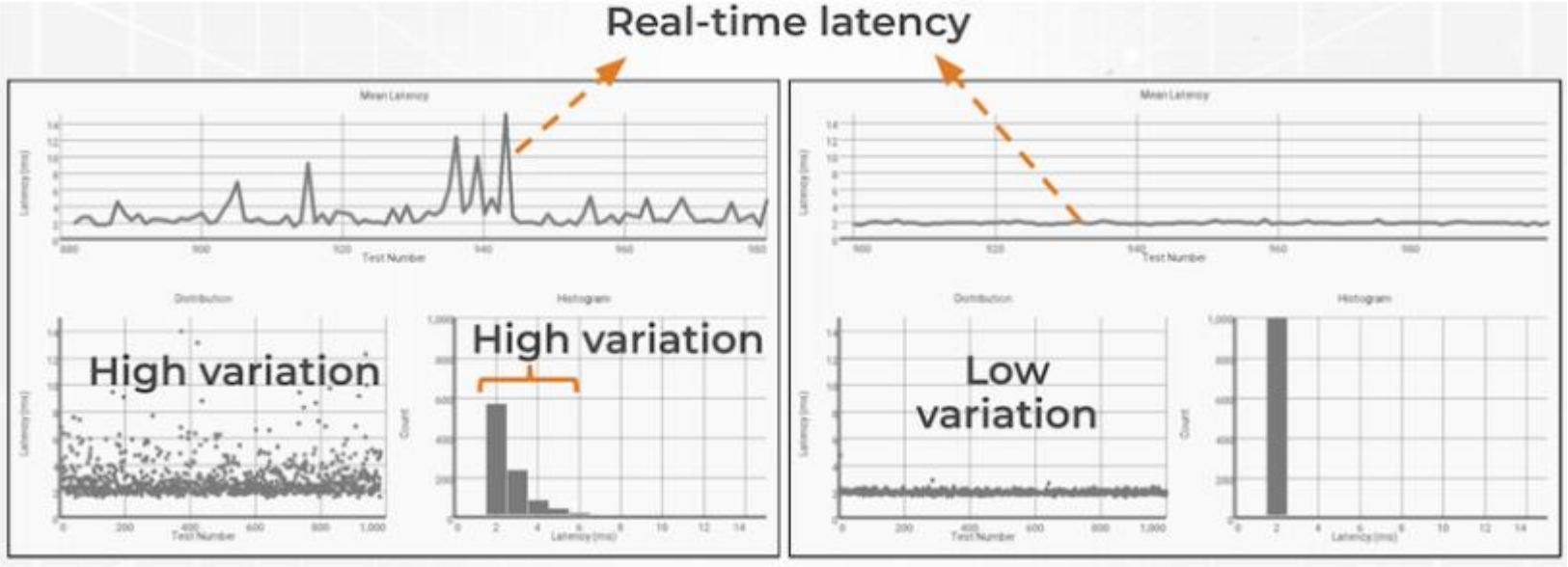
Traditionally, Wi-Fi has operated in the 2.4 GHz and 5 GHz spectrum bands. Wi-Fi 6E operates in the 6 GHz spectrum, providing 1,200 MHz of new spectrum, including 59 new channels at 20 MHz wide, and the potential for various wider channels.

BAND	NUMBER OF CHANNELS	BANDWIDTH PER CHANNEL
2.4 GHz	3	20 MHz
5 GHz	25	20 MHz
	12	40 MHz
	6	80 MHz
	2	160 MHz
6 GHz	59	20 MHz
	29	40 MHz
	14	80 MHz
	7	160 MHz



Wi-Fi 6E 성능

- Mobile AR/ VR gaming
- Deliver efficient gigabit Wi-Fi in smart homes
- low latency Wi-Fi calling
- 4K and 8K streaming
- High-speed tethering
- Real-time gaming
- Connectivity in your car
- Indoor public venues
- Industrial IoT



5GHz 6GHz

차세대 무선 네트워크 보안 과제

- 지향성 전송(Directional Transmission)

  IRS(Intelligent Reflecting Surface)

- 리소스 소모 공격(Resource Depletion Attack)

  Power Saving Mechanism(PSM)

- 중앙 의존형 토폴로지(Centralized Topology)

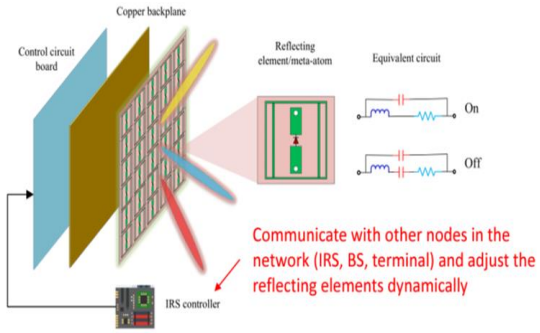
  무선 AP와 STA로 이루어진 중앙 집중적 Star형 토폴로지

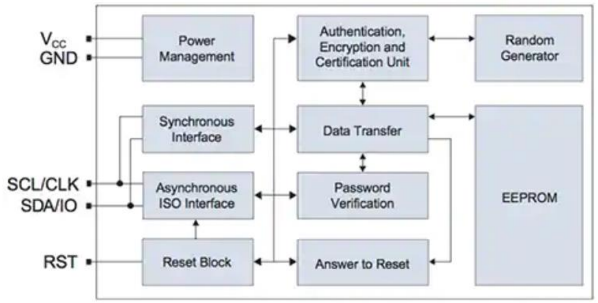
- 위치 기반 서비스(Location-based service, LBS)

  프라이버시 보호 대책

- 지능형 사물인터넷 연결 기밀성 문제

  저전력 장치에서도 기밀성을 보장하는 최적화된 차세대 암호화 알고리즘





Wi-Fi 6E 보안 이슈

■ 새로운 6GHz 비인가 기기

- 개인 사용자용 와이파이 6E AP와 공유기
- 기존 무선 침입 차단 시스템(Wireless Intrusion Prevention System, WIPS)은 주로 802.11 기반 무선 공격, 그리고 6GHz 대역이 아닌 2.4GHz 및 5GHz 주파수 대역의 모니터링과 보호에 초점

■ WPA3와 하위 비 호환

- 6GHz에는 WPA3이 사용되지만 2.4GHz와 5GHz 대역에는 앞으로도 매우 오랜 시간 동안 WPA2가 주로 사용
- *"새로운 기술이 나오면 제조업체들은 취약점 발견 시 업데이트 프로세스에서 기존의 와이파이 기기를 더 이상 포함하지 않을 것이다. 즉, 더 이상 패치를 받지 못하게 된다. 결과적으로 일부 사물인터넷 장비가 제조업체는 물론 기업 자체적으로도 그대로 방치되어 모니터링이나 패치 되지 않는 장비가 회사 네트워크에 남게 되는 위험을 일으킬 수 있다"*

■ OWE 와이파이 6E 취약점

- OWE는 암호화와 데이터 프라이버시를 제공하지만 어떤 형태로든 인증이 없으므로 하이재킹 및 가장 공격 (Impersonation Attacks) 유발

Wi-Fi 6E 보안 해결 방안

1. 아직 와이파이 6E를 구축하지 않았더라도 완전한 6GHz 모니터링 기능으로 WIPS 솔루션을 업그레이드 한다. 6GHz 무선이 있고 하나의 무선으로 3중 주파수 대역 스캔을 제공하는 WIPS 솔루션 센서를 찾아야 한다.

2. 6GHz 대역에서 OWE를 피하고 WPA3-퍼스널(SAE) 또는 WPA3-엔터프라이즈(802.1X)를 사용한다.

3. 보안 리더와 IT 팀을 대상으로 이 문제를 교육해 진지하게 받아들이도록 해야 한다.

4. 네트워크 세그먼트를 사용해 6E가 활성화된 공유기와 기기가 기업 전반에 안전하게 구현되도록 한다. 패치 및 문제에 대한 지원 계약이 분명한 기기만 구입하고, 새로운 기기를 대상으로 구매 라이프사이클에 포함되는 모든 정밀 심사를 실시해야 한다. 이렇게 하면 모든 제조업체 또는 공급업체가 기업의 공급망 관리에 연결된다

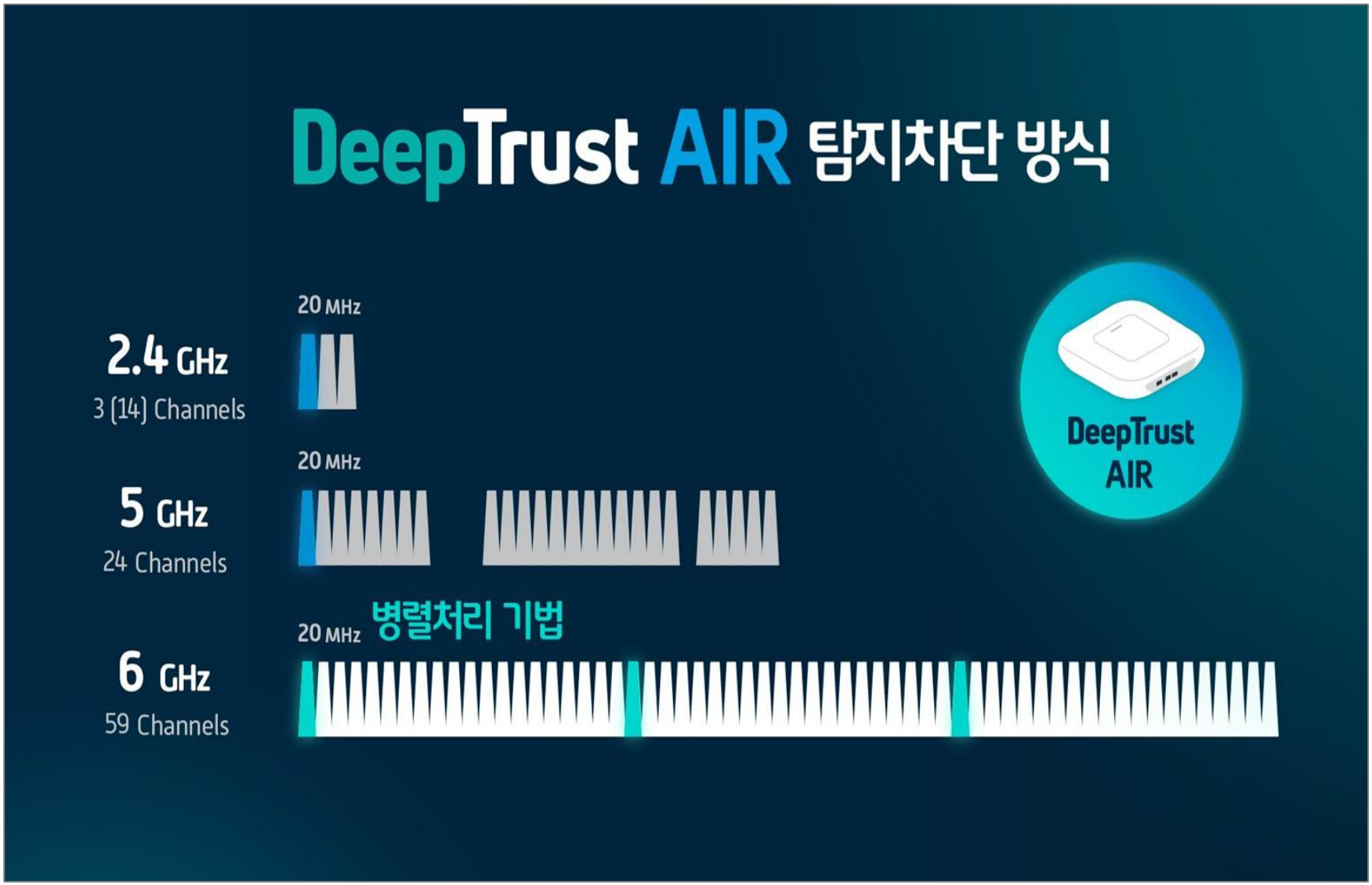
5. 제로 트러스트(Zero Trust) 전략을 고려한다. 제로 트러스트 전략은 강력한 권한 부여/인증 프로토콜을 지원하고 6E 디바이스 침해 이후의 횡적 이동을 제한함으로써 각 기기를 보호하는 데 도움이 될 수 있다.

DeepTrust AIR 개요

기존 WIPS


기존 WIPS 탐지차단 방식
20 MHz
2.4 GHz
3 (14) Channels
20 MHz
5 GHz
24 Channels
WIPS
20 MHz
6 GHz
59 Channels

DeepTrust AIR



WPA 3 개요

	WEP	WPA	WPA 2	WPA 3
Stands for	Wired Equivalent Privacy	Wi-Fi Protected Access	Wi-Fi Protected Access 2	Wi-Fi Protected Access 3
Developed	1997	2003	2004	2018
Security Level	Very Low	Low	High	Very High
Encryption	RC4	TKIP with RC4	AES-CCMP	AES-CCMP AES-GCMP
Key Size	64 bit 128 bit	128 bit	128 bit	128 bit 256 bit
Authentication	Open System & Shared Key	Pre Shared Key & 802.1x with EAP	Pre Shared Key & 802.1x with EAP	AES-CCMP AES-GCMP
Integrity	CRC-32	62 bit MIC	CCMP with AES	SHA-2

WPA 3 – MFP

802.11w 표준 수정안은 관리 프레임 보호(Management Frame Protection)을 도입 했으며 이 기능은 802.11ac 이후 Wi-Fi Alliance에서 필수
Management Frame Protection은 AP와 스테이션이 키 교환을 협상하고 AP와 스테이션 모두 유효한 키 세트를 가지고 있는 후에 전송되는 관리 프레임에 적용 되며 키 교환 이전에 전송 된 관리 프레임은 비 암호화

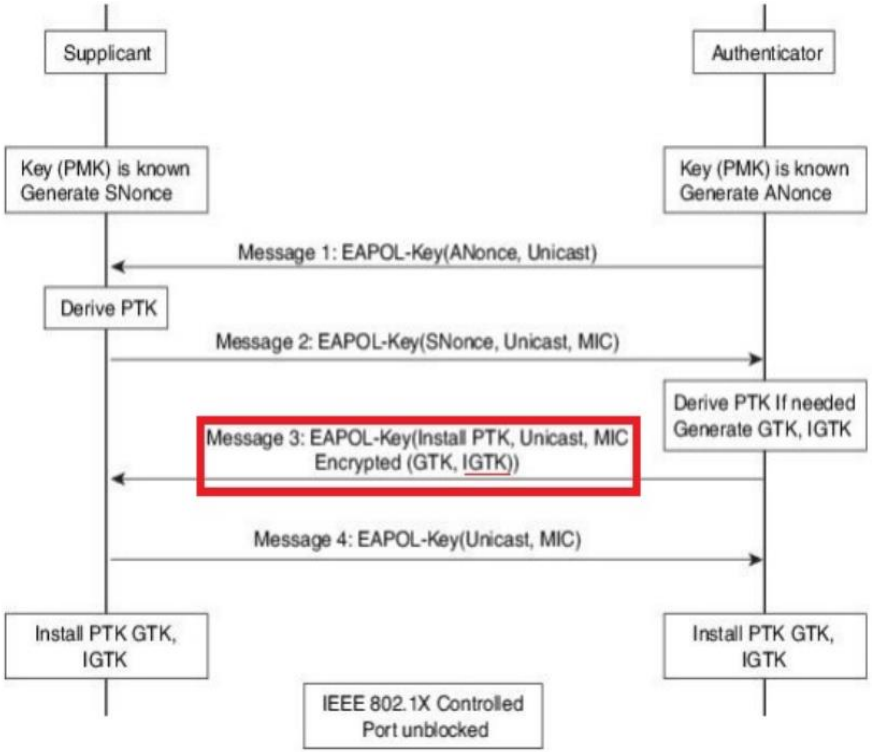
■ 암호화 되지 않는 관리 프레임
- Association frames (request/response)
- Beacon frames
- ATIM
- Authentication frames
- Probe request and response frames
- Spectrum Management action frames

■ 암호화 되는 관리 프레임
- Disassociation frames
- De-authentication frames
- Action management frames

Management Frame Protection은 MIC과 새 알고리즘(BIP-Broadcast Integrity Protocol) 의하여 생성 되어 무결성 검사를 제공하는 새로운 IGTK (Integrity Group Temporal Key)를 도입

DeepTrust AIR – MFP (or PMF)

- PMF 기능을 실행한 비인가 AP 탐지/차단 기법 국내 최초 특허 보유
- PMF 비인가 단말의 탐지 및 선별적 차단 지원




특허증
CERTIFICATE OF PATENT
특허 제 10-2102835 호
Patent Number
출원번호 제 10-2019-0034193 호
Application Number
출원일 2019년 03월 26일
Filing Date
등록일 2020년 04월 14일
Registration Date
발명의 명칭 Title of the Invention
WIPS 센서
특허권자 Patentee
시큐어레터 주식회사(110111-*******)
서울특별시 강남구 역삼로 223, 2층(역삼동, 대사빌딩)
발명자 Inventor
유용수(840128-*******)
서울특별시 영등포구 경인로114가길 14(영등포동1가,레텐어반) 518호
위의 발명은 「특허법」에 따라 특허등록원부에 등록되었음을 증명합니다.
This is to certify that, in accordance with the Patent Act, a patent for the invention has been registered at the Korean Intellectual Property Office.
2020년 04월 14일
특허청장
COMMISSIONER,
KOREAN INTELLECTUAL PROPERTY OFFICE
박 원주
특허청
Korean Intellectual Property Office

802.11w PMF 차단 기법에 대한 특허 보유
(특허 제 10-2102835호)

DeepTrust AIR – WPA 3 Enterprise

세계 최고 성능 및 스케일

- 최대 규모 레퍼런스
  LGU+ 300만 AP /1,300만 user 이상 연동
- PEAP기준 70,000 APM(타사 유사 장비 15,000APM)
- 국정원 CC 인증(EAL 2 등급) 획득

검증된 안정성

- 700여개 사이트에서 검증된 기술
- 독자적인 구축 방법론과 KNOW-HOW
- 클러스터링 : 인증 서버간 다중 병렬 연동 지원

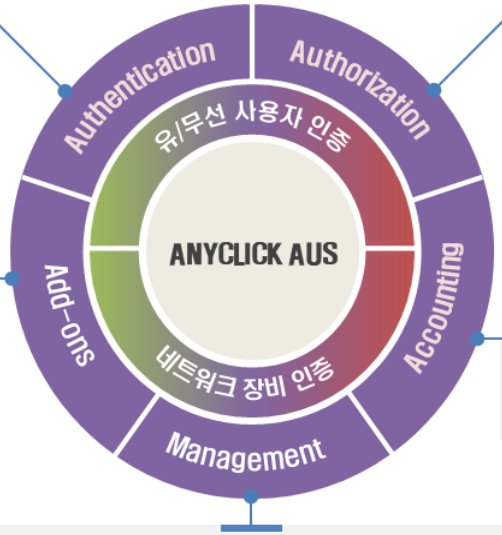
다양한 인증 환경 지원

- OTP TWO FACTOR 인증 지원
- 다중 DB 연동 및 DB별 사용자 정책 개별 적용
- 사용자 인증
  ID+MAC, ID+NAS, HDD Volume 인증 지원
- 가상화 계정 지원으로 DB 연동 환경에서도
  사용자 개별 정책 적용 지원

Anyclick AUS는 IEEE802.1x 표준을 지원하는 RADIUS 인증서버

802.1x 환경에서 유/무선 사용자 인증과 네트워크 장비 인증 지원

- 사용자 ID 등록 여부 체크
- 사용자의 비밀번호 정합성 체크
- Network 장비의 secret 키 정합성 체크



- 어떤 네트워크 사용이 가능한지 체크
  - 무선 SSID 및 VLAN 등.
- 어떤 네트워크 사용 권한이 있는지 체크
  - Administrator : 관리자 권한 (Read & Write)
  - Monitoring : 관제 권한 (Read Only)

인증 외에 부가적인 기능 포함

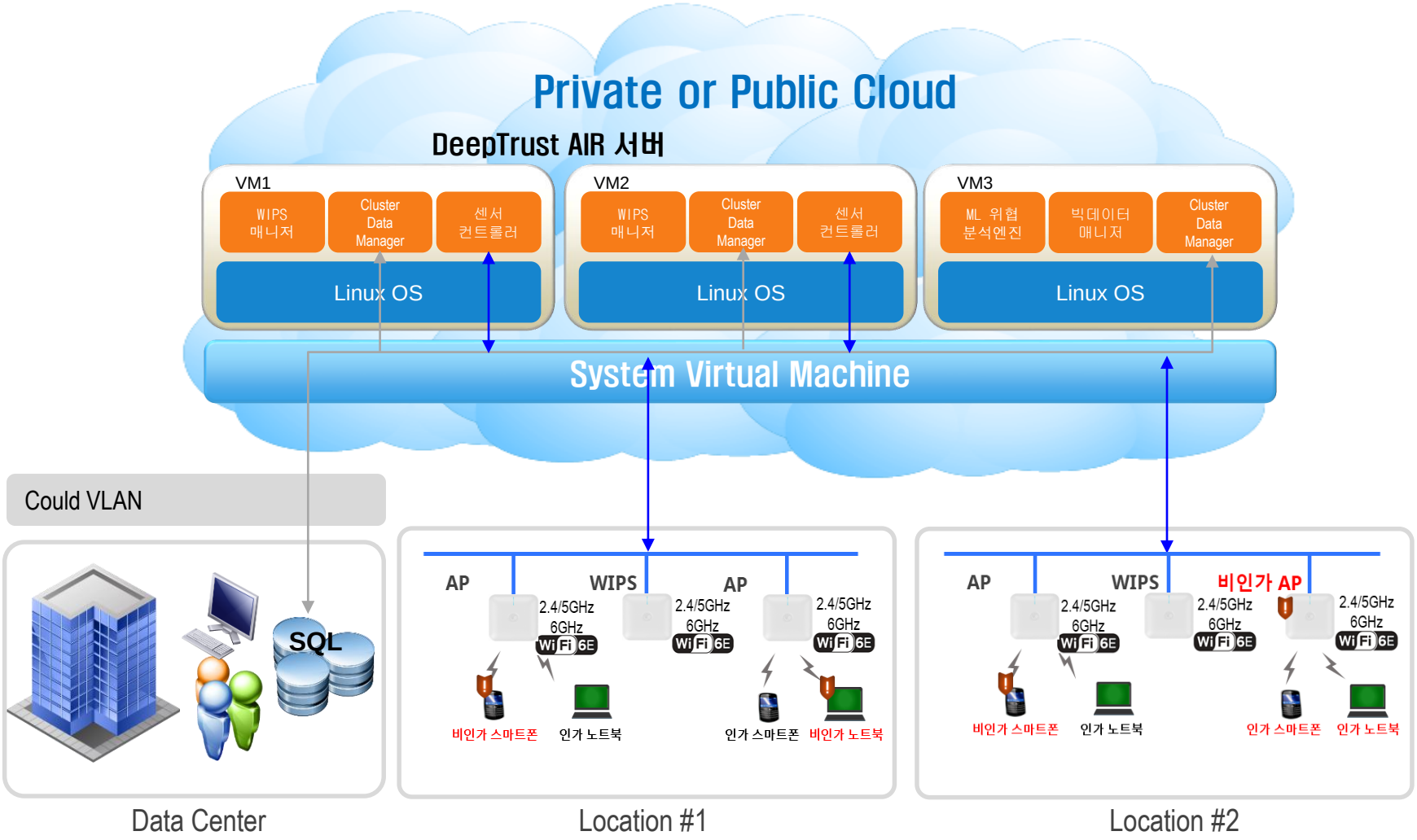
- DHCP 서버 기능
- Proxy 서버 기능
- Captive Portal의 External 페이지 서버 기능

- 장비에 Log-In & Log-Out 시간 기록
- 사용 트래픽 기록

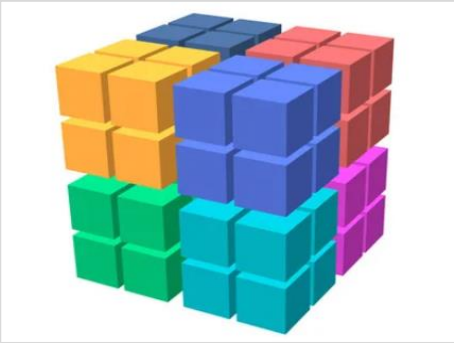
- 사용자 계정 및 장비 관리
- 권한 및 정책 관리
- 접속 이력 관리 및 통계/리포트

secureletter.

DeepTrust AIR – 클라우드 아키텍처



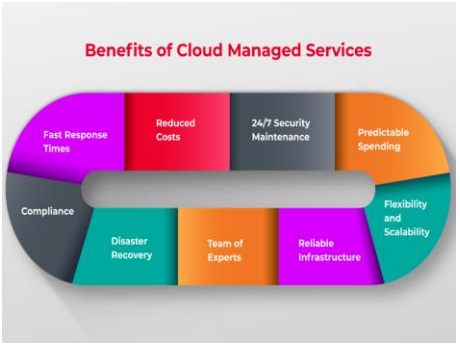
DeepTrust AIR – 주요 기능



손쉬운 분류 및 관리

효율적인 탐지 차단

편리한 운영과 낮은 TCO



클라우드 기반 관리

체계적인 보고서

정밀한 위치 추적

주요 레퍼런스

■ 금융/기업

KEB하나은행 | 한화디펜스 | IBK투자증권 | 신한은행 | 아주캐피탈 | 교보라이프플래닛생명 | 한화에스테이트

한화투자증권 | 우아한형제들 | SK m&service | KDB캐피탈 | 카카오페이증권 | 한국무역보험공사 | 신한아이타스

■ 공공/교육/의료

한국교통안전공단 | 중소벤처기업부 | 문화재청 | 경남도청 | 육군본부 | 부산대표도서관

건강보험심사평가원 | 강원랜드 | 지역난방공사 | 광물자원공사 | 한국장학재단 | 서울상수도사업본부

경찰병원 | 국립마산병원 | 동산의료원 | 한국중부발전 | 한국서부발전 | 한국동서발전

한국남동발전 | 육군3사관학교 | 세종시교육청 | 충청남도교육청 | 인천광역시교육청 | 동덕여자대학교

화성시청 | 질병관리본부 | 한국전자통신연구원 | 항공우주연구원 | 농촌진흥청 | 과학기술정보통신부

secureletter.

Q&A