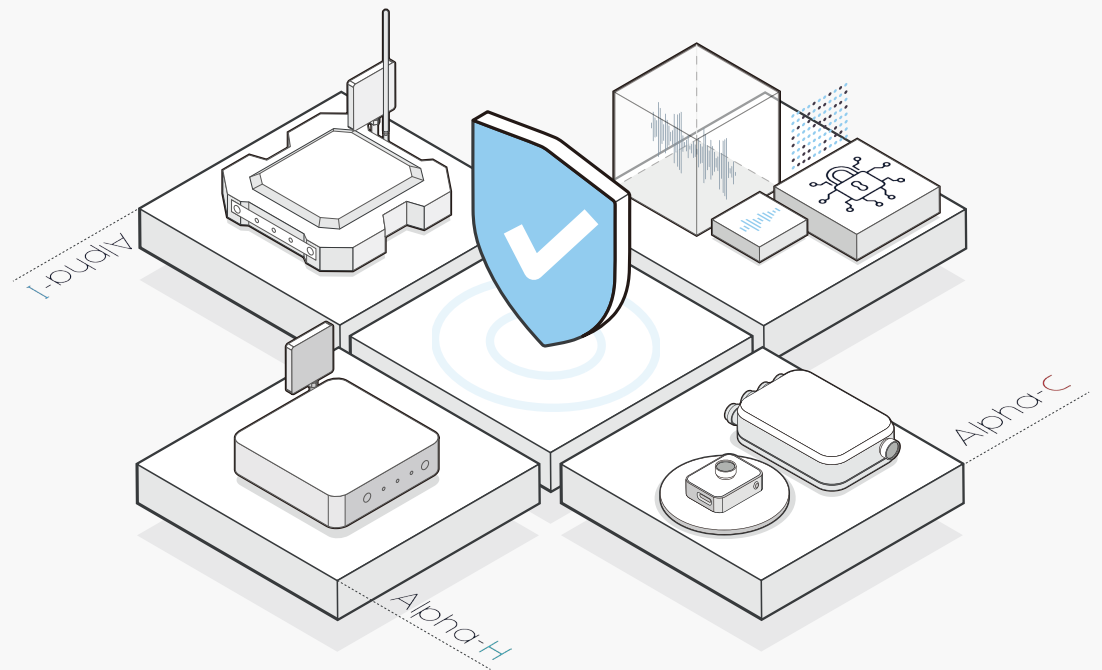


GITSN (주)지슨

기술력으로 범죄를 예방하는
융합 보안 솔루션 기업



본 자료는 주식회사 지스 (이하 “회사”)과 관련하여 기관투자자와 일반투자자들을 대상으로 실시하는 Presentation에서의 정보제공을 목적으로 작성 되었으며 이의 반출, 복사 또는 타인에 대한 재배포는 금지됨을 알려드리는 바입니다.

본 자료의 열람은 위의 제한 사항의 준수에 대한 동의로 간주될 것이며 제한 사항에 대한 위반은 ‘자본시장과 금융투자업에 관한 법률’ 에 대한 위반에 해당될 수 있음을 유념해주시기 바랍니다. 또한, 본 자료의 활용으로 인해 발생하거나 발생할 수 있는 모든 손실에 대하여 ‘회사’ 및 ‘회사’의 임직원과 주주, 자문역 및 기타 이해관계인들은 과실 및 기타의 모든 경우를 포함하여 그 어떠한 책임도 부담하지 않음을 알려드립니다.

본 자료에 포함된 ‘예측정보’는 개별 확인 절차를 거치지 않은 정보들입니다. 이는 과거가 아닌 미래의 사건과 관계된 일체의 사항을 포함하는 것 (별도 ‘예측 정보’ 임을 표기하지 않았다 하더라도)으로 ‘회사’ 및 산업의 향후 예상되는 변화 및 재무의 예상 실적을 의미하는 것입니다. 동 ‘예측정보’ 는 많은 변수에 따라 영향을 받으며, 본질적으로 불확실성을 가지고 있으므로 실제 미래에 나타나는 결과는 ‘예측정보’에 기재되거나 암시된 내용과 중대한 차이가 발생할 수 있습니다.

본 자료는 어떠한 주식의 매입 또는 매도 등 매매의 권유를 구성하지 아니하며, 본 자료의 그 어느 부분도 어떠한 계약 및 약정 또는 투자 결정을 위한 기초 또는 근거가 될 수 없습니다. 또한 본 자료는 어떠한 경우에도 민형사상의 분쟁 및 다툼에 있어서 증거자료로 사용될 수 없음을 알려드립니다.

주식 매입 또는 매도 등 매매와 관련된 모든 투자 결정은 오직 금융감독원 전자공시시스템을 통해 제출한 신고서를 통해 제공되는 정보만을 바탕으로 내려져야 합니다.

Table of Contents

Chapter 1

회사개요

회사소개
지속적 성장을 도모할 수 있는
조직의 안정성
회사연혁
지슨의 포트폴리오
경영성과

Chapter 2

투자포인트

보안 시장의 성장에 따른 동반 성장
기술력 기반 독점 시장 창출
실적의 퀀텀점프
우수한 매출 및 이익 구조
Alpha-V(vehicle) PJT:
차량용 보안사업 전개

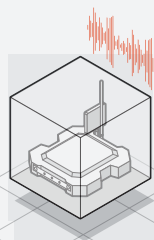
Chapter 3

사업영역 및 기술 경쟁력

무선도청의 종류와 솔루션
무선백도어의 개념과 솔루션
불법촬영의 유형과 솔루션

Prologue

보안 위협의 일상화
지슨's Identity



GITSN (주)지슨

INVESTOR RELATIONS 2025

Prologue

- 01. 보안 위협의 일상화
- 02. 지슨's Identity

GITSN (주)지슨



보안 위협의 일상화, 사회적 리스크로 급부상

‘도·감청’ 대통령실도 뚫렸나...“용산 이전 서두른 탓”

기사입력 2023-04-11 08:47 | 최종수정 2023-04-11 09:19

해킹·보안사건 개인 피해액 年 9,800억 원

(2022 한국정보통신보안윤리학회)

보험대리점 해킹으로 1107명 정보 유출...“비밀번호 바꿔야”

등록 2025.05.20 11:23:39 | 수정 2025.05.20 12:10:24

중기업, 해킹 내부 탐지율 31% 불과

(2025 구글클라우드 맨디언트 사이버보안 보고서)

지슨, KB국민銀行에 무선백도어 해킹 탐지 시스템 구축

파이낸셜뉴스 | 김찬미 기자

불법촬영 범죄 2020년 5,032건에서
2024년 7,257건으로 4년간 약 40% 증가

(경찰청 통계)

공공기관 여성 탈의실에 ‘몰카’...수사 시작되자 50대 남성 직원 자수

머니투데이 | 윤혜주 기자

보안 위협 증가로 인한 정부의 보안 예산 확대 추세...

개인정보보호위원회에서 기업·기관의 개인정보보호 예산비중을
2027년까지 전체 IT예산의 최소10%, 2030년까지 15%로 의무화 추진

(2025.05.27 뉴시스)

대통령실 도청 막은 지슨...이번엔 ‘몰카 소탕’ 나섰다

최형창 기자 | 입력 2023.02.06 17:58 | 수정 2023.02.07 00:40

2024년 글로벌 시장에서 대형 보안 기업들의 약진이 두드러져,
시가총액 160억 달러를 넘는 8개 보안 업체 중 7개의 주가가
2024년에 20% 이상 상승

(BankInfoSecurity)

SKT 해킹 후폭풍...정보보호 예산 확대에 뜨는 보안株

배요한 기자 · 2025. 5. 27. 10:11

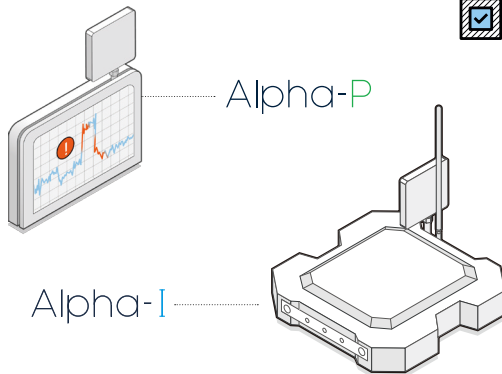
기술로 범죄를 예방하는 융합 보안 솔루션 기업



기술로 범죄를 예방하는 융합 보안 솔루션 기업

도청 보안

공공시장 점유율 98.77%

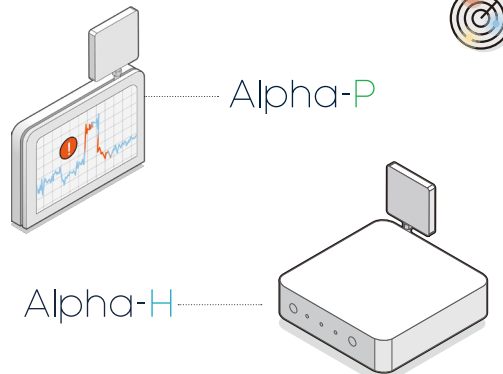


AI 기반 탐지 기술로 집무실, 회의실 등
중요 공간의 무선 도청을 24시간 감지합니다.

- 조달청 우수제품
- 조달청 혁신제품
- 중소벤처기업부 성능인증

무선백도어 보안

시장 점유율 100%

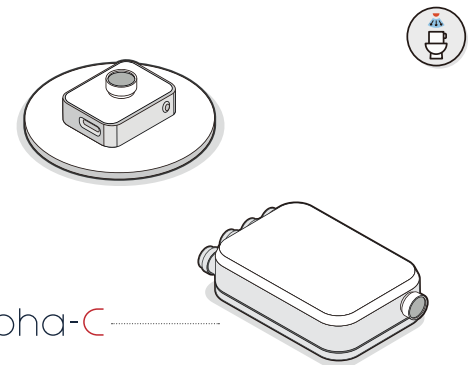


데이터센터와 서버실에 침투한
무선 스파이칩을 탐지해
망분리 체계를 보호합니다.

- 중소벤처기업부 성능인증
- 조달청 벤처창업혁신상품
- 산업통상자원부장관상 표창

불법촬영 보안

공공시장 점유율 60.5%



화장실 등 민감 공간에서
몰카와 칸막이 상단 촬영을
실시간 감지해 범죄를 예방합니다.

- 조달청 혁신제품
- 조달청장 표창
- 한국여성단체협의회 전국여성대회 특별상

특허 기반 독점적 기술을 토대로 HW·SW를 융합
혁신적 고부가가치 제품 개발



하드웨어 기술

- ✔ 광대역 RF 모듈 직접 설계, 생산
- ✔ 초광대역(UWB) 신호 검출 기술

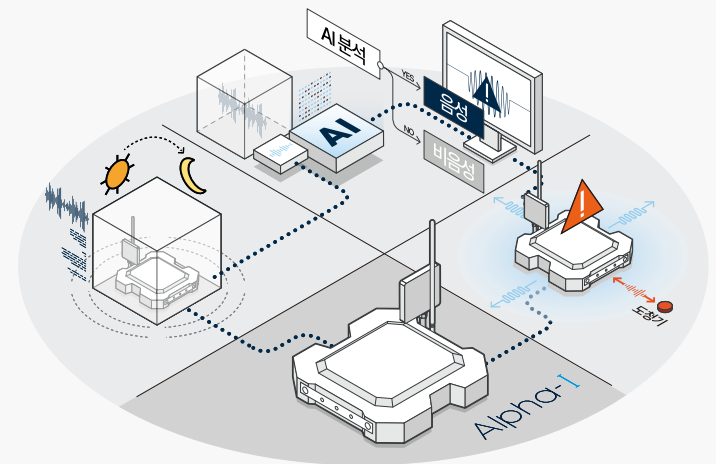
소프트웨어 기술

- ✔ 음성 신호 전송기 위치 식별 기술
- ✔ 비정상·비인가 전파 발생 위치 추정 기술
- ✔ 열원 온도 변화 분석 기술

회사개요

- 01. 회사소개
- 02. 지속적 성장을 도모할 수 있는 조직의 안정성
- 03. 회사연혁
- 04. 지슨의 포트폴리오
- 05. 경영성과

GITSN (주)지슨



스마트 무선도청 상시 방어 시스템

Alpha-1 VIP 집무실, 사무실, 회의실 등 중요 장소에 설치되어 인공지능(AI)으로 첨단 도청을 24시간 자동 탐지

회사개요

회사명	주식회사 지슨
대표이사	한 동 진
설립일	2000년 3월 20일
자본금	86.6억 원
임직원수	104명
사업영역	무선도청탐지, 무선 백도어 해킹 탐지, 불법촬영 탐지 등 융합보안솔루션
주요제품	무선도청, 무선 백도어 해킹, 불법촬영 탐지 시스템
소재지	서울특별시 강남구 개포동 1238-3(형지빌딩)
홈페이지	www.gitsn.com

CEO Profile



한 동 진 대표

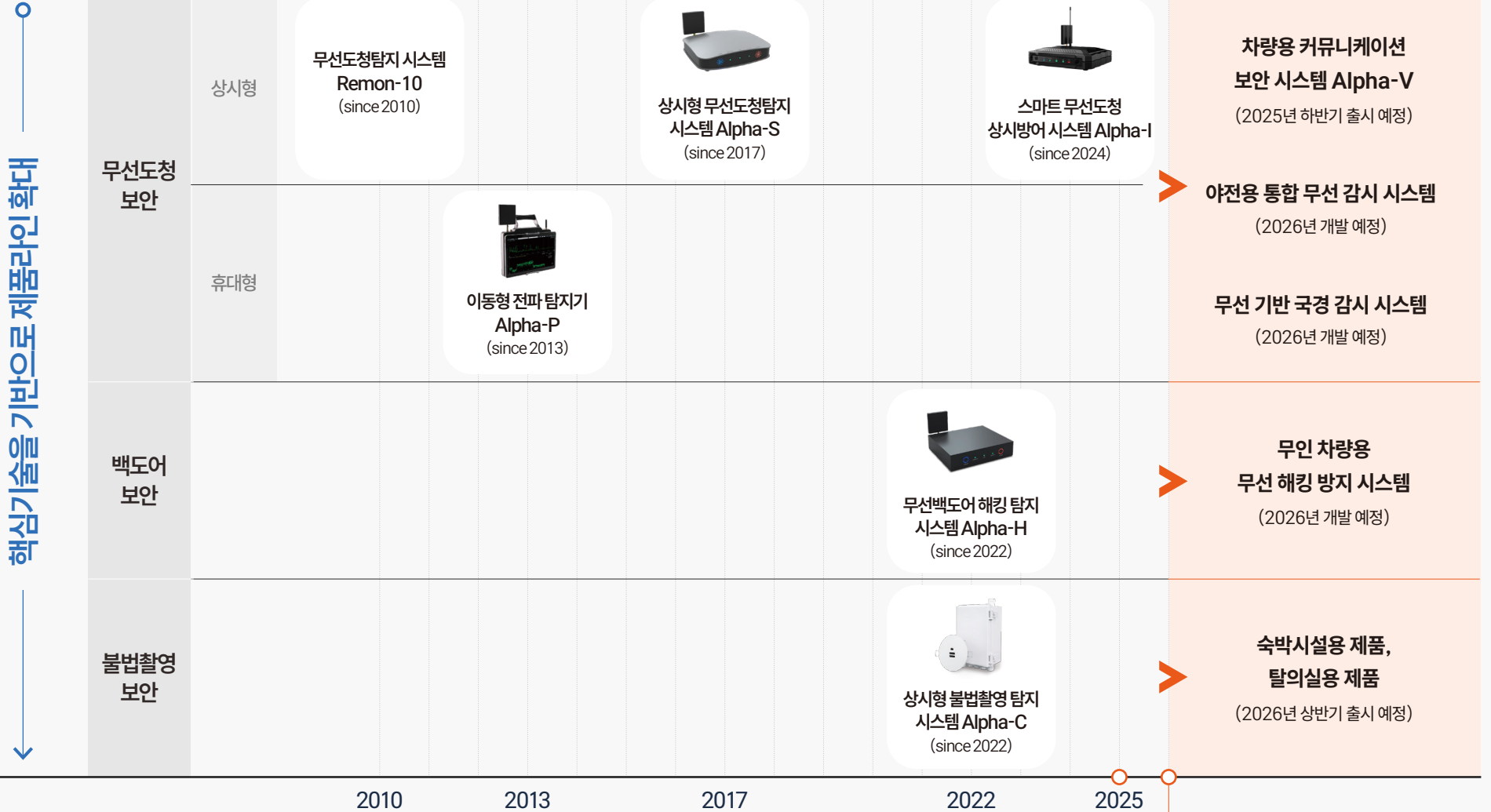
- (주)지슨 대표이사
- 現) 차세대 교통인프라 융합산업연구조합(NTICA) 이사장
- 前) 금융위원회 금융권 망분리 TF 위원
- 前) 국제표준화기구 전문 위원회 (ISO/TC204) 전문위원
- 고려대 전자공학 학·석·박사

B2G 및 B2B 대상으로 기술영업, 관제, 지속적 매출 확대가 가능한 완비된 조직 보유

대표이사

영업			R&D		
<p>공공사업 7명</p> <p>공공기관, 지자체 전문 영업 / 대형 보안 기업 파트너십 관리</p>	<p>전략사업 10명</p> <p>금융권, 민간기업, 해외 전문 영업 / 사이버 보안 영업</p>	<p>에코시스템 4명</p> <p>영업 파이프 라인 기획, 영업파트너사 선발</p>	<p>HW 11명</p> <p>Embedded, 회로 설계, RF모듈, 금형, 센서</p>	<p>SW 11명</p> <p>Application, Server, UI/UX Design</p>	<p>선행연구 12명</p> <p>차세대 기술 연구, 정부연구과제 (스마트시티, 자율주행 인프라 등)</p>
제조			관리		
<p>제조 7명</p> <p>제품 생산 및 재고 관리 / SCM 및 제품 전수 검사</p>	<p>기술지원 15명</p> <p>제품 설치, 유지보수 및 고객 지원</p>	<p>관제 7명</p> <p>불법촬영 보안 전문인력의 365일 원격 관제 서비스 제공</p>	<p>경영관리 6명</p> <p>회계, 자금, 세무 / 인사, 총무, 컴플라이언스</p>	<p>기획 6명</p> <p>사업, 제품, 경영 기획, PR</p>	

기존 제품 Upgrade로 경쟁사와 격차 지속적 확대, 핵심기술로 신규제품 포트폴리오는 지속적 다변화

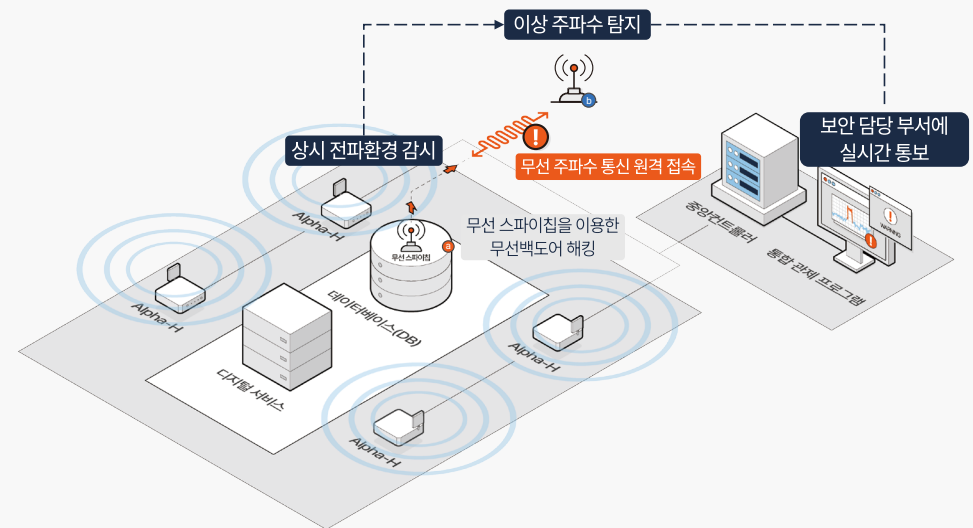


상용화 완료된 제품으로 복수 고객사에 매출 확대

Upgrade Line 개발 중

투자포인트

- 01. 보안 시장의 성장에 따른 동반 성장
- 02. 기술력 기반 독점 시장 창출
- 03. 실적의 퀀텀점프
- 04. 우수한 매출 및 이익 구조
- 05. Alpha-V(vehicle) PJT: 차량용 보안사업 전개



무선백도어 해킹 탐지 시스템

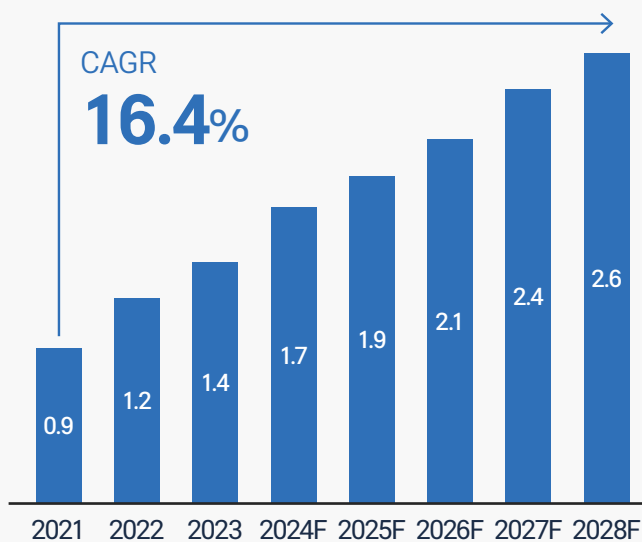
Alpha-H 서버실, 관제실, 집무실 등에 침투되어 망분리 체계를 무력화시키는 무선 스파이칩을 실시간으로 탐지하는 무선백도어 해킹 탐지 시스템

성장하는 보안 시장

보안 시장 성장 추이¹⁾

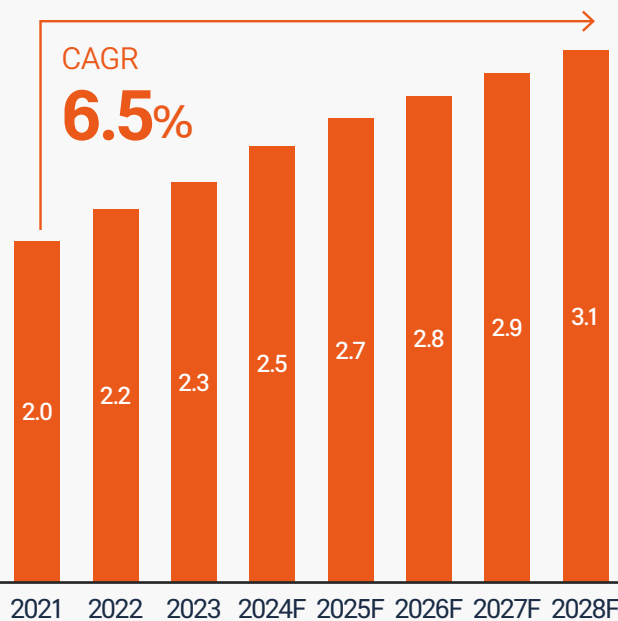
한국 보안시장

(단위: 조원)



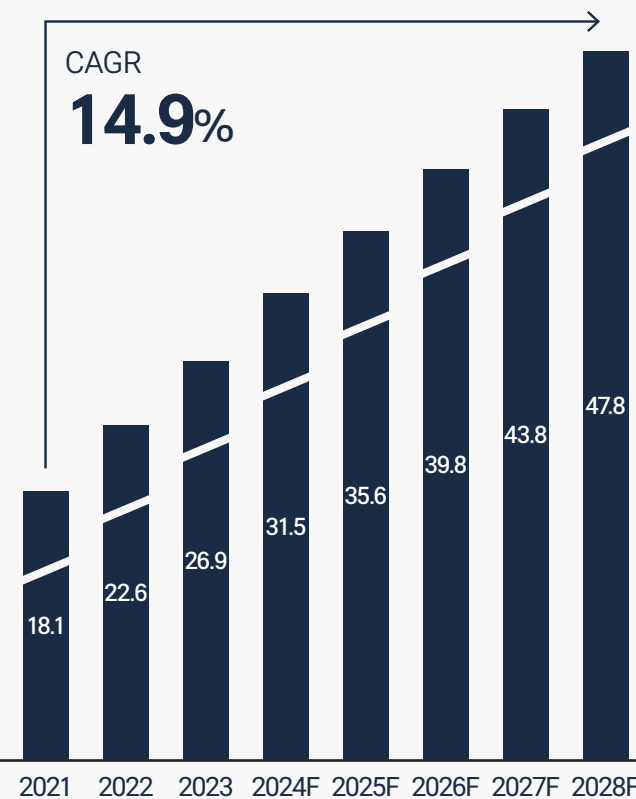
한국 사이버 보안시장

(단위: 조원)



글로벌 보안시장

(단위: 조원)



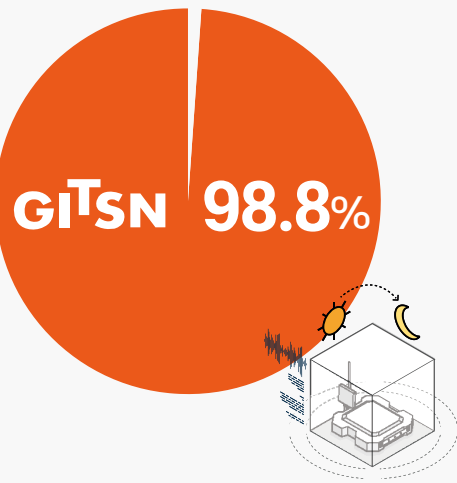
1) 출처: Statista Market Outlook Report-Security south Korea 2024.03.01, :
Statista Market Outlook Report-Security Global 2024.03.01, Statista Market Outlook Report-Cybersecurity - Security Services south Korea 2024.06.01

압도적 점유율과 안정적 장기 매출처 보유

도청 보안¹⁾

무선백도어 보안

불법촬영 보안²⁾



- ✔ 5개년간 243억 원 매출
경찰·검찰·군·의회·외교부·대통령실 등
장기매출처 확보, 대통령실 청와대 복귀 및 세종시 이전에
따른 추가적인 수주 기대

- ✔ 국내유일 공급자로 시장에서 독점적 지위 확보
- ✔ 신시장 초기 독점 중

- ✔ 21대 대통령 대선 공약에 24시간 안전 공중 화장실 조성에
관한 사항 포함 등 범정부적인 관심으로 수요확대가 기대

1) 상시형 도청탐지 공공시장 점유율(금액기준), 출처: 조달정보개방포털·국방전자조달시스템
2) 상시형 불법촬영 탐지 공공시장 점유율(금액기준), 출처: 조달정보개방포털·국방전자조달시스템

뛰어난 기술력과 신뢰를 기반으로 확장되는 레퍼런스

도청 보안

중앙정부, 공공기관, 대기업 등
총 340여 기관/기업에서 도입



대통령실



대한민국 국회



국무총리실



외교부



법무부



국방부



경찰청



서울특별시



경기도



한국은행



금융감독원



한국전력공사

...

무선백도어 보안

국내(13), 해외(5) 등
정부기관, 금융기관 등에서
도입 및 운영 중



국세청



한국수출입은행



한국산업은행



우리은행



신한은행



KB국민은행



삼성 SDS

...

불법촬영 보안

공공(55), 교육기관(39),
민간(15) 등 다양한 기관에서
폭넓게 사용 중



행정안전부
정부청사관리본부



정부청사관리본부
(서울청사관리소)



경찰청



한국철도공사



국립공원공단



서울특별시



울산광역시






한화생명



동원 F&B

...

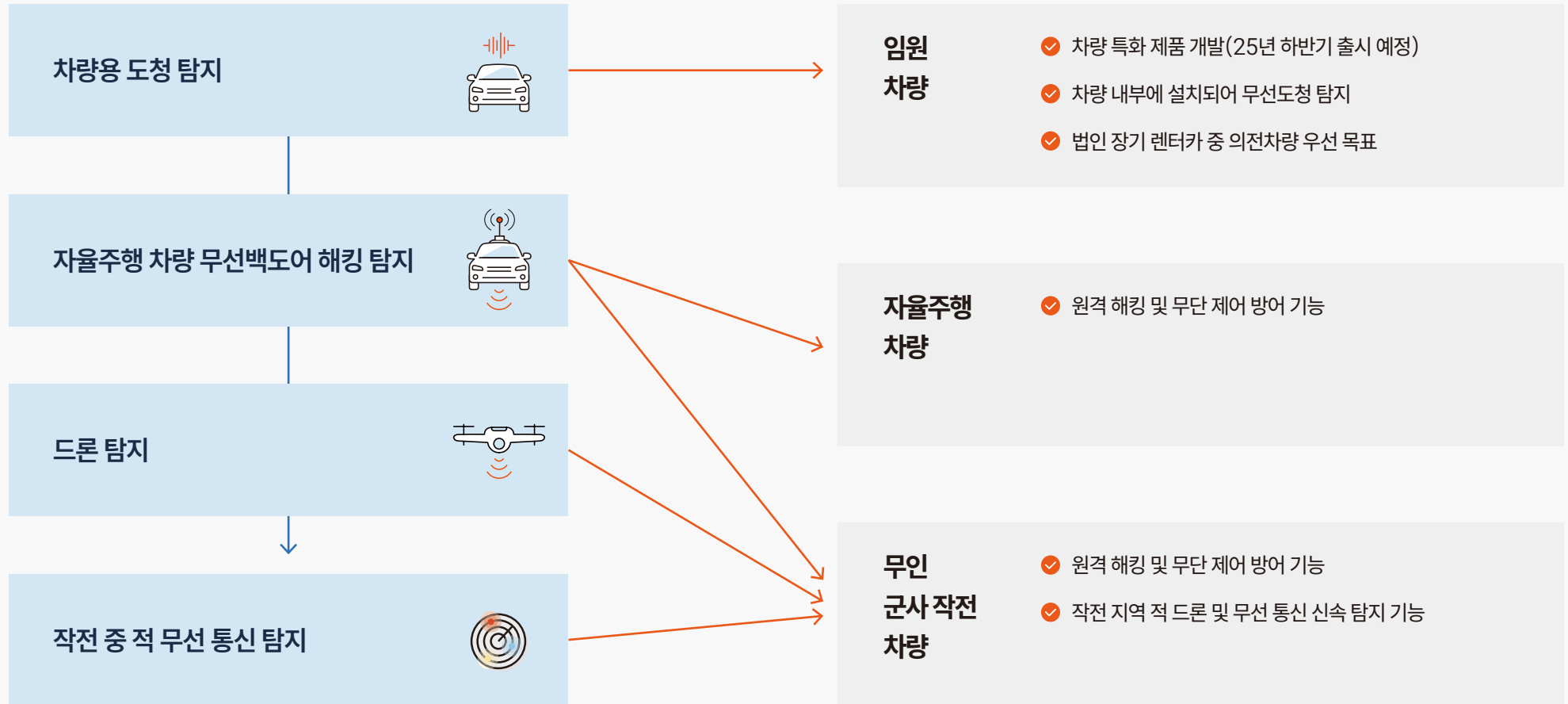
보안 사고로 인한 사회적 이슈 증가 및 제도 개선에 따른 수요 급증

	사회적 이슈	제도 개선
 <p>도청 보안</p>	<ul style="list-style-type: none"> ☑ 용산 대통령실 도청 의혹 ☑ 대통령실 청와대 복귀 및 세종시 이전 추진 	<ul style="list-style-type: none"> ☑ 국가 정보보안 기본 지침(2023.01.31 개정)에 따라 공공기관은 도청 보안이 필수 의무 ☑ 도청방지기 내용연수 단축(10년 → 8년)으로 26년부터 연간 25%의 수요 증가 효과 기대 
 <p>무선백도어 보안</p>	<ul style="list-style-type: none"> ☑ SKT 해킹사고 후 각 기업의 보안분야 투자 증대 ☑ 금융기관 무선백도어 해킹우려에 금감원의 대응책 마련 → 우리·신한·KB 등 주요은행을 포함한 금융권 85곳: 당사 무선백도어 보안 시스템 도입 완료 또는 도입 협의 중 	<ul style="list-style-type: none"> ☑ 무선백도어 해킹 위협 지속으로 24년 법제화: 「정보통신망이용촉진및정보보호등에관한법률」 일부개정 → 정보통신망의 정상적인 보호·인증절차를 우회하여 정보통신망에 접근할 수 있도록 하는 프로그램이나 기술적 장치 등을 금지 
 <p>불법촬영 보안</p>	<ul style="list-style-type: none"> ☑ 불법촬영 범죄 증가에 따른 사회적 관심도 증가 → 공공 불법촬영 보안제품은 상시형 중심으로 전환되면서 급속하게 성장 중(22년 2.9억 원 → 24년 27.1억 원) 	<ul style="list-style-type: none"> ☑ 「공중화장실 등에 관한 법률」, 서울시 조례, 경기도 조례 등을 통해 불법촬영 점검 체계 구축 및 대응책 마련 의무화 ☑ 대통령 대선공약: 24시간 안전 공중 화장실 조성 공중화장실 상시형 불법촬영 탐지 시스템 단계적 확대 

독보적 무선 보안 기술 기반 차량용 보안 사업 전개 : 자체 투자 + 정부 지원 사업 활용으로 개발 효율성 향상

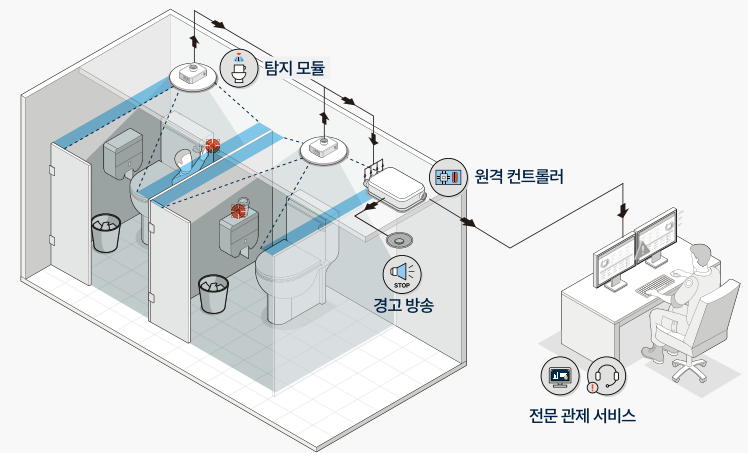
지스만이 구현 가능한 무선 보안 기능

적용 대상



사업영역 및 기술 경쟁력

- 01. 무선도청의 종류와 솔루션
- 02. 무선백도어의 개념과 솔루션
- 03. 불법촬영의 유형과 솔루션



상시형 불법촬영 탐지 시스템

Alpha-C 모든 유형의 몰래카메라에 대응이 가능하고,
칸막이 차단 촬영 행위도 감지하는 상시형 불법촬영 보안 솔루션

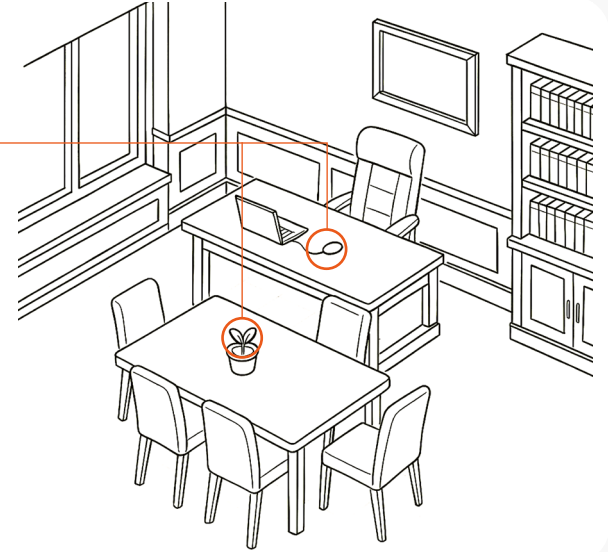
발전하는 도청기술에 완벽하게 대응하는 솔루션

무선도청

무선주파수(RF) 송신방식의 도청기를 사용한 도청

도청기의 종류

- 초소형** 5mm에서 최대 동전크기
- On/Off형** 외부에서 원격으로 On/Off를 조정해 탐지를 회피
- 위장형** 일상용품에 숨겨진 위장형 도청기
- UWB도청기** 넓은 주파수 범위 사용, 짧은 전송 시간과 낮은 전력 수준으로 탐지의 어려움



GITSN's solution

Alpha-I

집무실, 회의실, VIP실 등
중요 장소에 설치되어
최첨단 무선도청 위협을 탐지



24/7 상시탐지



UWB통신 탐지



AI도청 음성 판별



도청기 위치 탐지



다수의 단말기 통합 관제



8GHz RF탐재

세계 최고 수준의 상시형 도청탐지 시스템

초광대역(UWB)전파 분석

- ✔ 일반 휴대형·상시형 무선도청 탐지 수단으로는 탐지 대응이 어려운 UWB 주파수 영역 탐지
- ✔ 해외 6개국 특허 획득 (미국, 중국, EU, 이스라엘, 러시아, 파키스탄)
- ✔ 모방난이도 AA (국제특허법률사무소 24.04)

도청기 존재 유무 확인

- ✔ AI 도청 음성 판별 기술
데이터의 특징점을 머신러닝으로 학습하여 음성과 비음성을 구별
- ✔ 도청기위치 탐지 기술
비가청영역의 고주파를 방사하여 도청탐지기 설치 공간 내 도청기 존재여부 자동 판별

RF 모듈 설계

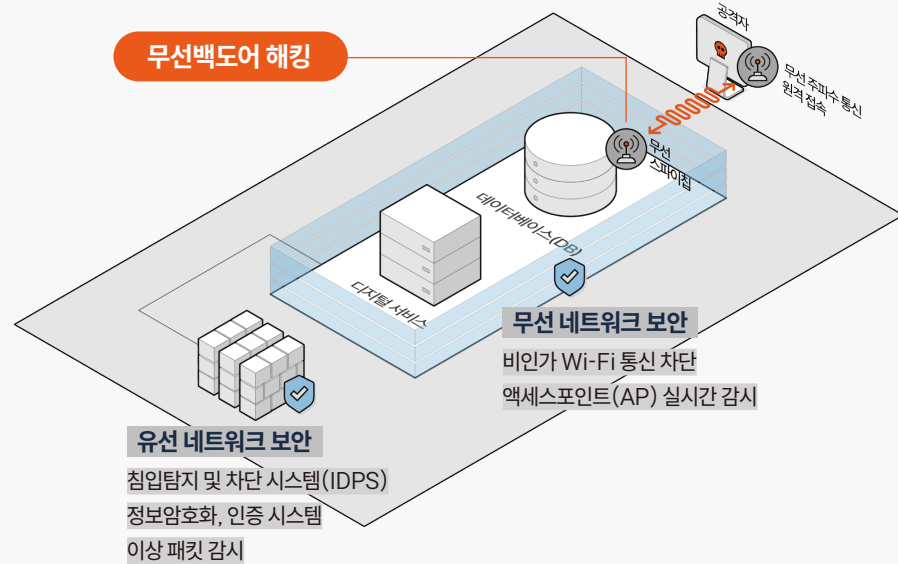
- ✔ 최대 8GHz까지 도청 탐지 범위를 넓혀 Wi-Fi 6E, Wi-Fi 7 기반 첨단도청 장치 탐지 가능

제조사(제품명)	제품사진	출시연도	탐지대역	수신감도	탐지 시간	무인 자동 판별	UWB 탐지	핵심 부품
지스 (Alpha-I)		2024	25kHz ~8GHz	-100~ -10dBm	0.3초 이내	○	○	자체 개발
G社		2019	25kHz ~6GHz		미공개			
K社		2020	25kHz ~6GHz		3초 이내	X	X	외주 수입
K社		2023	20kHz ~6GHz	-60~ -10dBm	3초 이내			

가장 발전된 형태의 해킹에 대비하는 최고의 솔루션

무선백도어 해킹

내부망으로 분리된 서버 등에 무선스파이칩을 심어 불법으로 무선 연결통로를 확보한 후, 무선통신을 통한 원격접속으로 데이터를 탈취하거나 시스템을 붕괴시키는 신종 해킹 위협



GITSN's solution

Alpha-H

데이터센터, 전산실, 관제실, 집무실 등에 설치되어 망분리 체계를 무력화시키는 무선 스파이칩을 실시간 탐지



24/7 상시탐지



UWB통신 탐지



다수의 단말기 통합 관제



금융권PoC다회수행



서버, 데이터센터 등 대규모 도입 공간을 고려한 '무선 스파이칩 위치 추정' 특허기술 적용

모방할 수 없는 기술력으로 국내 유일 공급자 지위 확보

신호원 위치추적 기술

- ✔ 신호원 위치 추정을 통한 무선백도어 해킹 탐지 기술 (2021 특허등록)
- ✔ 주요 은행 주관 성능 시험통과 후 각 IDC에 적용

PoC 협업

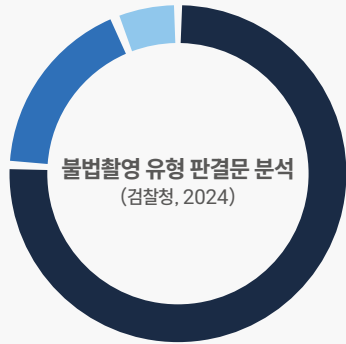
- ✔ 다수 기관 · 장기간 PoC 및 파일럿 테스트를 통해 안정성 확보
- ✔ 금융권 보안성 심의 체크리스트 41개 항목에 부합하는 유일한 제품

현실적으로 불가능한 역설계

위험요소	난이도 상승 요인	
<ul style="list-style-type: none"> ✔ 하드웨어 분석 ✔ 회로설계 이해 ✔ 특수 부품 사용 ✔ 소프트웨어 복제 ✔ 소스코드 접근 ✔ 복제 인력 및 장비 ✔ 복제 성공 후 유지 	<ul style="list-style-type: none"> ✔ 회로추적의 어려움, 해석의 복잡성 ✔ 분석시간 증가, 전문성 요구 ✔ 펌웨어 없이 분석 불가 ✔ 코드분석의 난이도, 역컴파일 한계 ✔ 시간·노력·기술 요구 ✔ 인건비·장비 비용 ✔ 복제품 무력화·완전복제 불가능 	<p style="text-align: center;">높은 기술적·경제적 진입장벽으로 역설계가 불가능</p>

모든 형태의 불법촬영을 탐지하는 통합 솔루션

불법촬영의 유형



침입형
76%

설치형
18%

기타
6%

설치형

일회용품, 분실물, 시설물 등으로
위장한 초소형 몰카로
기기 색출 및 범인 적발이 어려움



침입형

칸막이 상단 등에 숨어
직접촬영



GITSN's solution

Alpha-C

설치형 및 침입형의 모든 유형의 불법촬영을
탐지할 수 있는 통합 솔루션



24/7 상시탐지



전문 관제 서비스



몰카 선별 분석 알고리즘을 통해
모든 유형의 몰래카메라 탐지

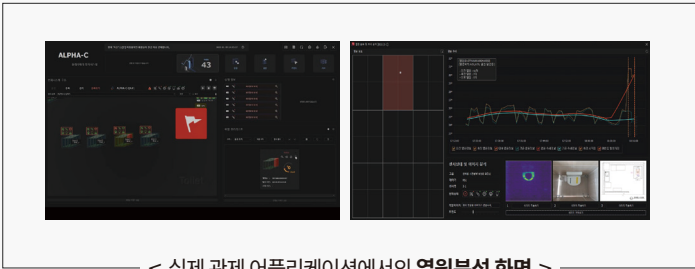


레이저 센서 이용,
칸막이 상단의 촬영 행위 실시간 감지

우수한 기술력 기반으로 국내 유일 모든 유형의 불법 촬영 탐지

열원분석을 통한 불법촬영 기기 탐지

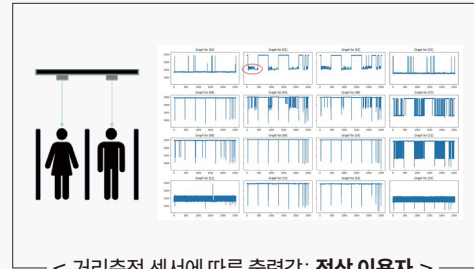
- 시계열 열환경 분석을 통해 정상적인 열원과 불법촬영 기기로부터 발생하는 이상 열원을 구분하여 불법촬영 기기 색출



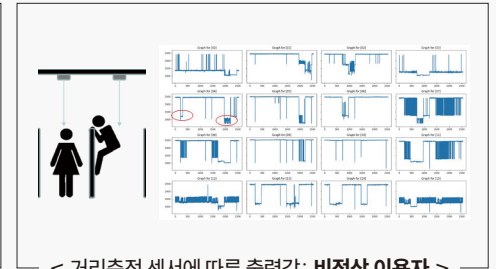
< 실제 관제 어플리케이션에서의 열원분석 화면 >

정상·비정상 이용자 구분 기술





- 거리 측정 센서의 출력값으로 정상이용자와 이상이용자를 구분 가능
- 국내 유일 설치형 카메라 뿐만 아니라 숨어서 찍는 침입형 불법촬영도 대응 가능



< 거리측정 센서에 따른 출력값: 정상 이용자 >



< 거리측정 센서에 따른 출력값: 비정상 이용자 >

제조사	제품사진	기반기술	탐지대상	불법촬영 기기 세부 위치파악	24/7 상시탐지
지سن (Alpha-C)		온도변화 및 레이더 기반 탐지	모든유형 탐지	○	○
U社		이상행동 탐지기반	침입형만 탐지	X	○
I社		무선랜 탐지기반	Wifi 송출형만 탐지	X	○
N社		무선랜 탐지기반	Wifi 송출형만 탐지	X	○

GITSN (주)지스