모바일·IoT 종합 보안 솔루션

OnTrust 제품소개서

pr@securion.co.kr

2024.10

1. 회사소개

AI based Cyber Security

Mobile·IoT·5G SECaaS Provider

머신러닝 기반 안티바이러스

OnAV

모바일·IoT 종합 보안 솔루션

OnTrust

악성 앱 자동분석 솔루션

OnAppScan

*지원플랫폼: Android, Linux, Gooroom

㈜시큐리온

대표자	유동훈
주력사업	AI기반 사이버 보안기업
주소	서울시 송파구 송파대로 201 송파테라타워2 A동 G129-2 OS-33호
설립일	2019.05.15
전화	02-575-3339
홈페이지	http://www.securion.co.kr/

주요연혁

2024	OnTrust 2024 우수 정보보호기술(제품) 지정
2023	**보이스피싱 악성앱 탐지 특화 OnAppScan V2.0 출시** 시큐리온 ISO9001 품질경영시스템 인증 OnTrust 2023 하반기 정보보호제품 혁신대상 수상
2021	**IoT·모바일 종합보안 솔루션 OnTrust 출시** 유동훈 대표 국가 교육정보화사업 유공 교육부장관 표창
2019	**시큐리온 법인 설립, OnAV/OnAppScan 출시**

2. 제안배경 (1) 위협 현황

모바일 및 IoT에 대한 위협 증가

개인 정보 유출

스마트월패드 해킹으로
700단지 40만 가구 정보 유출

산업 기밀 유출

제조사 정보 유출로 인한
OS 취약점 위협 증가

OS 취약점 공격

스파이웨어 제로데이 공격으로
기기 보안 무력화

OnTrust, 모바일·IoT에서 일어나는 모든 위협 탐지·대응

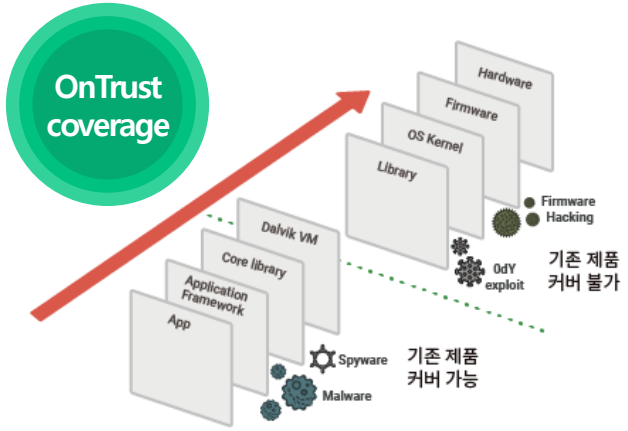
- 제로데이 공격, OS 취약점 공격 등 APP 영역 뿐 아니라 OS 공격도 보호
- 유무선 네트워크 공격 및 카메라·마이크 활용한 녹화, 도감청 대응

AS-IS	OnTrust
불완전한 보호 제로데이 공격 및 OS 취약점 공격 등 대응 불가	**완전한 보호** App과 OS영역 동시 보호
IoT 적용성 낮은 사양에서 업데이트, 모니터링 등 작동 불가	**IoT 적용성** 저사양 IoT 환경에 적합한 초경량 엔진
가시성 확보 단말 위협 현황 파악/대응 불가	**가시성 확보** 위협관리 및 원격관제 기능 제공

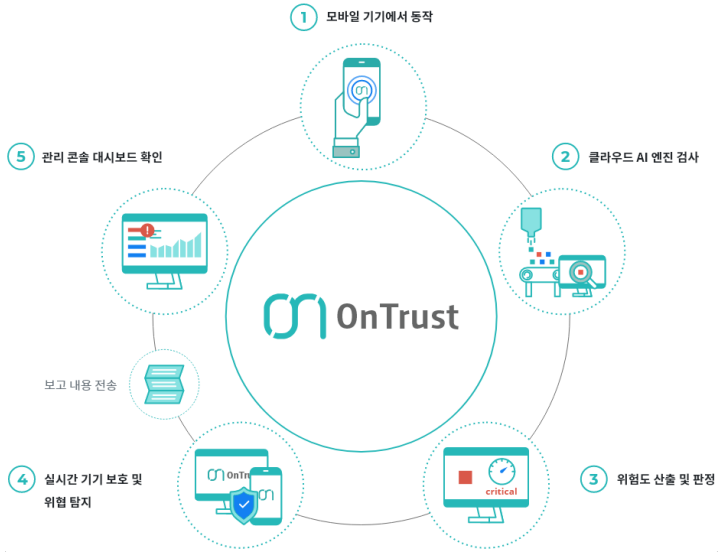
간단한 앱 설치만으로 단말 APP 및 OS 영역 보호

기기 무결성 보장, 악성 앱, 취약점 대응

"OnTrust coverage"



"운영체제 차이 없이 광범위한 공격대응"



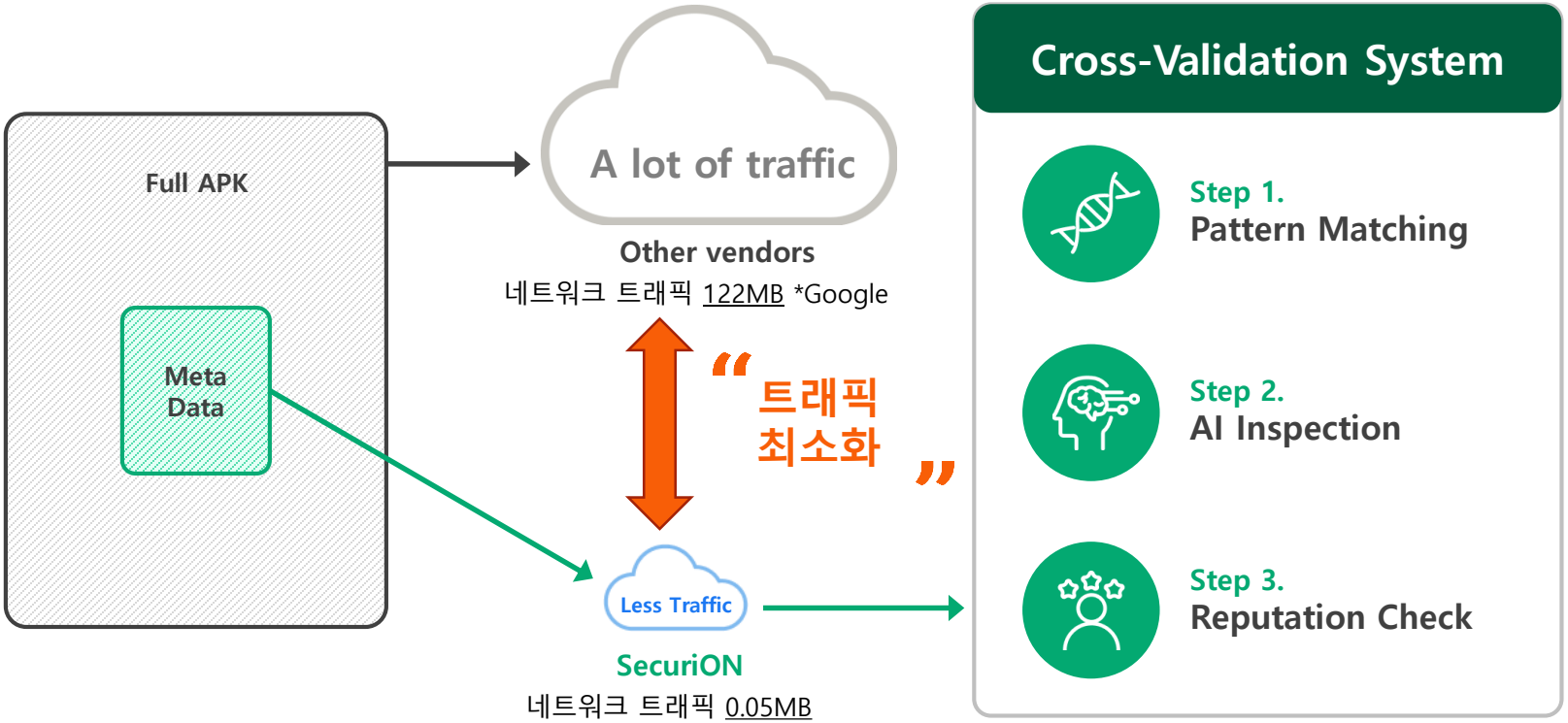
특허 기반 '공격흔적 탐지기술'

침해사고 발생 전후 All time 위협관리

공격 흔적 탐지 프로세스

공격	조사	침해사실확인	검증 결과 보고
• 기기 잠금 해제 • OS보호 무력화 • 펌웨어변조 • 원격침입 • 권한상승 • 백도어설치 • 악성앱설치 • 정보유출	• 기기펌웨어 • 파티션상태 • 파일 시스템과 파일 • 프로세스 트리 • 메모리 상태 • 환경 변수 • 프로퍼티 변수 • 각종 보호 모듈	• 시스템 취약점 • 취약점 공격 도구 • 권한상승 공격코드 • 각종 익스플로잇 코드 • 암호화 된 페이로드 • 추가 공격 도구 • 위협적인 앱 • 백도어	

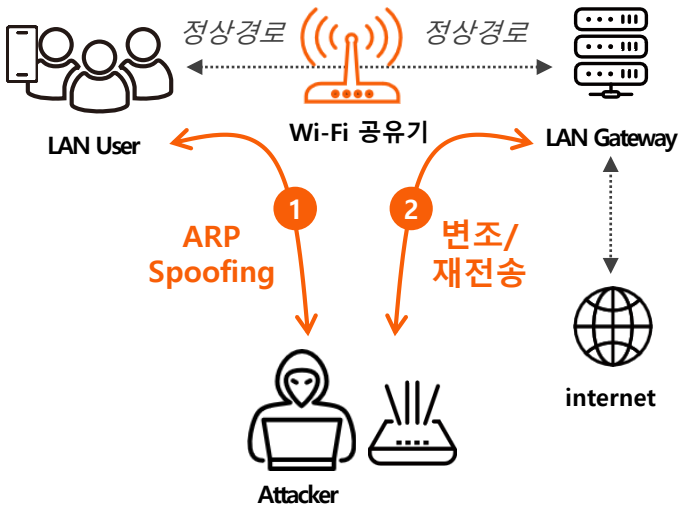
잠재적 악성 앱 탐지 특화 ML 기반 안티 바이러스 엔진 탑재 독자 개발 'CVS' 적용



연결된 유,무선 네트워크 공격 실시간 탐지

각종 스푸핑, MITM 공격에 효과적인 대응 (일반 권한 동작)

Wi-Fi 해킹 기법(MITM) 개념도



ARP (주소 결정 프로토콜) Spoofing 공격 기술

① 가짜 ARP 패킷을 통해 상대방의 데이터 패킷을 중간에서 가로채는 MITM 공격 (Man In The Middle, 중간자 기법)

② 가로챈 데이터를 유출하거나 변조 후 재전송하여 계정 도용 등 불법 행위 가능

OnTrust Network Detection API

01 WLAN_AP_Scan
: 위험한 네트워크 감지

02 DNS_Spoof_Scan
: DNS 스푸핑 공격 탐지

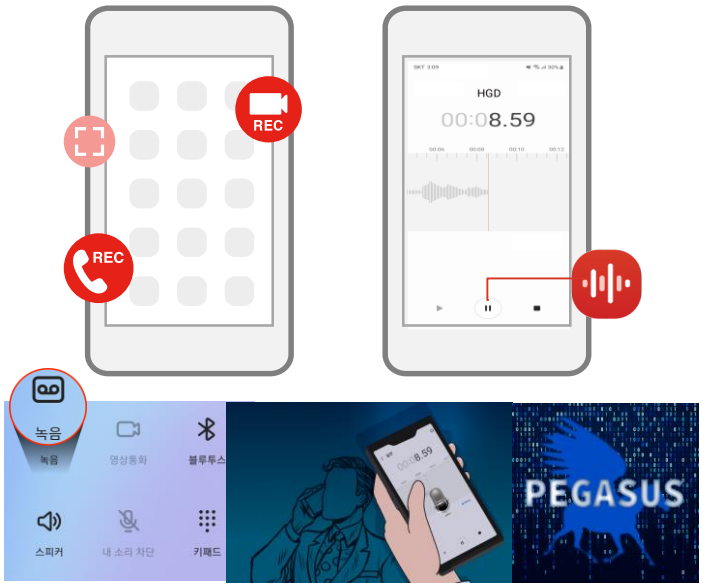
03 MITM_Scan
: 중간자 공격 탐지

04 ARP_Attack_Scan
: ARP 리다이렉트 공격, ARP 캐시 변조 탐지

카메라, 주변 음성, 통화 도감청 탐지 및 실시간 방지

스파이웨어의 레코딩 행위 기반 탐지 및 방지 (일반 권한 동작)

카메라, 마이크 등 해킹 위협



※ 월패드 카메라 유출 사례, 페가수스 spyware에 의한
음성 도청, 통화 감청 사례 대응

OnTrust MIC/Call Record Detection API

01 Camera_Record_Scan
: 사용 중인 카메라 탐지

02 MIC_Record_Scan
: 사용 중인 마이크 탐지

03 Call_Record_Scan
: 통화 중 녹음 탐지

04 Record_Prevention
: 실시간 도감청 방지

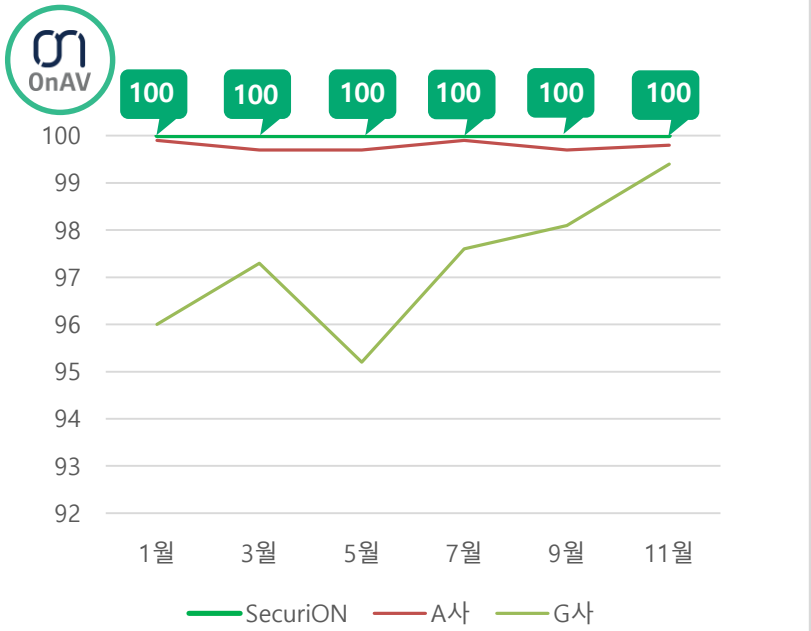
* 하위 Android 4 버전부터 최신 13 버전까지 동일 API 지원

타 보안 제품군 대비 포괄적 보호 제공

✕ 불가 △ 일부 가능 ✓ 가능

기능	시큐리온 OnTrust	A/V 단독	제조사 보호
OS 해킹(취약점) 탐지	✓	✕	△
악성 앱 탐지	✓	✓	✕
기기 무결성 유지	✓	✕	✓
네트워크 공격 탐지	✓	✕	✕
통화 및 음성 도감청 탐지	✓	✕	✕

높은 악성 앱 탐지율 유지 (AV-TEST)



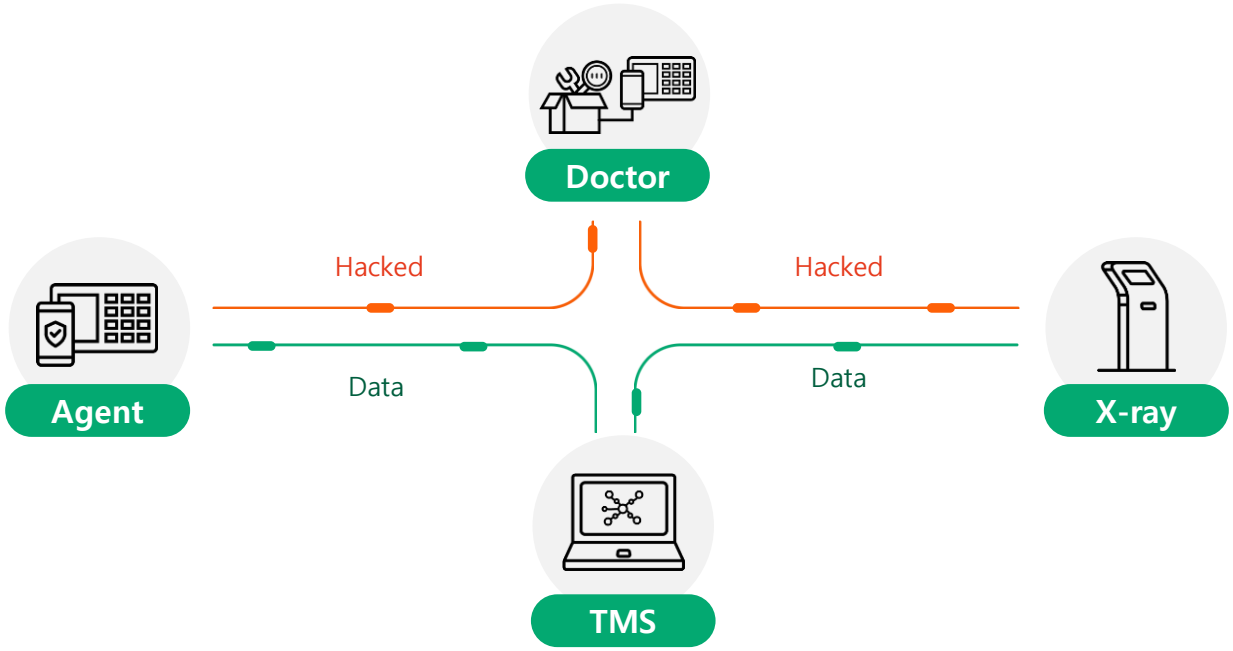
Android security apps in an endurance test
How successfully malware is detected

AV-Test May to October 2023

Manufacturer	Product	Detection Rate Real-Time Testing	Detection Rate Reference Set
SecuriON	**OnAV**	**100%**	**100%**
Avast	Antivirus & Security	100%	100%
AVG	AntiVirus FREE	100%	100%
Bitdefender	Mobile Security	100%	100%
Kaspersky	Plus for Android	100%	100%
Norton	Norton 360	100%	100%
Trend Micro	Mobile Security	100%	100%
Sophos	Intercept X for Mobile	99.9%	100%
Avira	Antivirus Security	99.8%	100%
F-Secure	Total Security & VPN	99.8%	100%
ESET	Mobile Security	99.8%	99.9%
G DATA	Mobile Security	99.6%	100%
McAfee	Mobile Security	99.6%	100%
AhnLab	V3 Mobile Security	99.6%	99.9%
TTB	Antivirus : Mobile Security	99.4%	99.9%
Protected.net	Total AV	96.9%	100%
Google	Play Protect	94.9%	98.9%

• 출처 : AV-Test

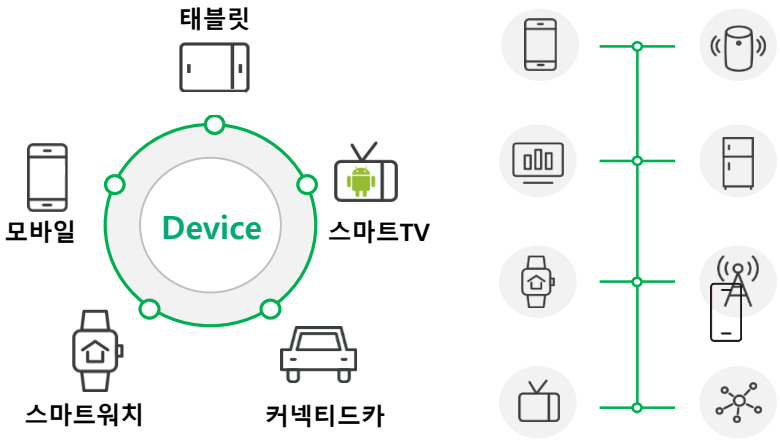
실시간 탐지, 검사, 관제, 복구까지 종합 보안 제공



구분	OnTrust Agent	OnTrust X-Ray	OnTrust Dr	OnTrust TMS
기능	기기 및 OS 시스템 취약점 검사, 앱 악성 여부 검사, 실시간 탐지, 사용자 통계 기능 연계 및 앱 이용 차단 기능 제공	공공 기관 시설, 사옥, 연구소 등 보안 구역 출입 시 기기 및 OS 시스템 취약점 검사, 앱 악성 여부 검사를 신속하게 제공	악성 앱에 감염되었거나 취약점 공격을 받은 기기를 해킹 전 상태로 정상화 할 수 있도록 안전한 복구 기능 제공	종합 관제 서비스를 위해 앱 사용 기기 및 출입 기기 분석 정보와 사용자 통계를 보여주는 대시보드 제공

*서버 구축 시 추가 비용 발생

디바이스 종류와 환경에 맞는 검사방식 지원



- **지원 대상**
  - 스마트폰, 태블릿, 월패드, TV, 워치, 차량 등
- **신속검사 기능 제공**
  - 앱 설치 없이 기기 연결로 신속검사 가능
  - Kiosk 및 전문가용 분석박스 지원
- **적용산업**
  - 단말에서 중요 정보를 다루는 산업
  - 정부기관, 코인거래소, 개인정보취급산업

검사방식

앱 설치를 통한 검사 (마켓을 통한 설치)	PC 연결을 통한 자동 검사 (응용 프로그램 동작 방식)	키오스크 연결을 통한 신속 검사 (부스 H/W 제공)	분석 및 복구 장비 (박스 H/W 제공)

모바일·IoT 엔드포인트 보안 관제 및 보안구역 관리

VIP 스마트폰 해킹탐지 및 복구

기업 및 기관 모바일 엔드포인트 위협 관리

기기에서 탐지된 위협을 관리자가 통합 콘솔에서 모니터링

기존 관리 플랫폼/도구 연동 지원(SIEM, EDR)

특수 목적 모바일·IoT 디바이스 보안

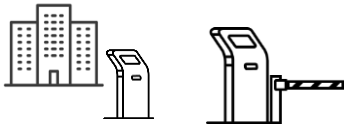
특수 목적에 따라 관리되는 단말 그룹의 OS 및 APP 영역 보안

EX) 아파트 월패드, 국가재난망, 교육용(보급) 단말, 의료용 단말 등

보안구역 모바일 기기 출입관리

보안 시설 출입자를 대상으로 소지 단말 스캔, 악성코드 유입 차단

EX) 사옥, 연구소, 대외비 자료 보관실, 군부대, VIP 전용 출입구역 등



해킹 단말 정상 복구

해킹 탐지부터 단말 복구까지 대외비 복구 시스템 구축

EX) 국가/기업 기밀 보유자(군/검/경, 방산업체, C레벨 경영진 등)

EX) VIP 대상 대외비 업무 수행 업체(로펌, 컨설팅 에이전시 등)

4. 인증 및 수상

시큐리온 AI탐지 시스템(OnAV) 글로벌 Top 3 인증 획득

독일 | 오스트리아 | 영국 | 대한민국 | 중국 | 중국

OnTrust 2023 하반기
정보보호제품 혁신대상 수상

OnTrust, OnAV for Gooroom
한국지능정보사회진흥원 인증

OnTrust 2024
우수 정보보호 기술(제품) 지정

시큐리온 ISO9001
품질경영시스템 인증

시큐리온 OnTrust
중소기업기술마켓 인증

5. 특허

핵심기술 국내 IP 확보

1. 리눅스 커널 무결성 검사 및 데이터 복구
2. 휴대 단말에서의 악성코드 진단 및 제거
3. 취약점 탐지 아키텍처로 구성된 메모리 관리 기술
4. 취약점 보완을 위한 바이너리 패치 장치

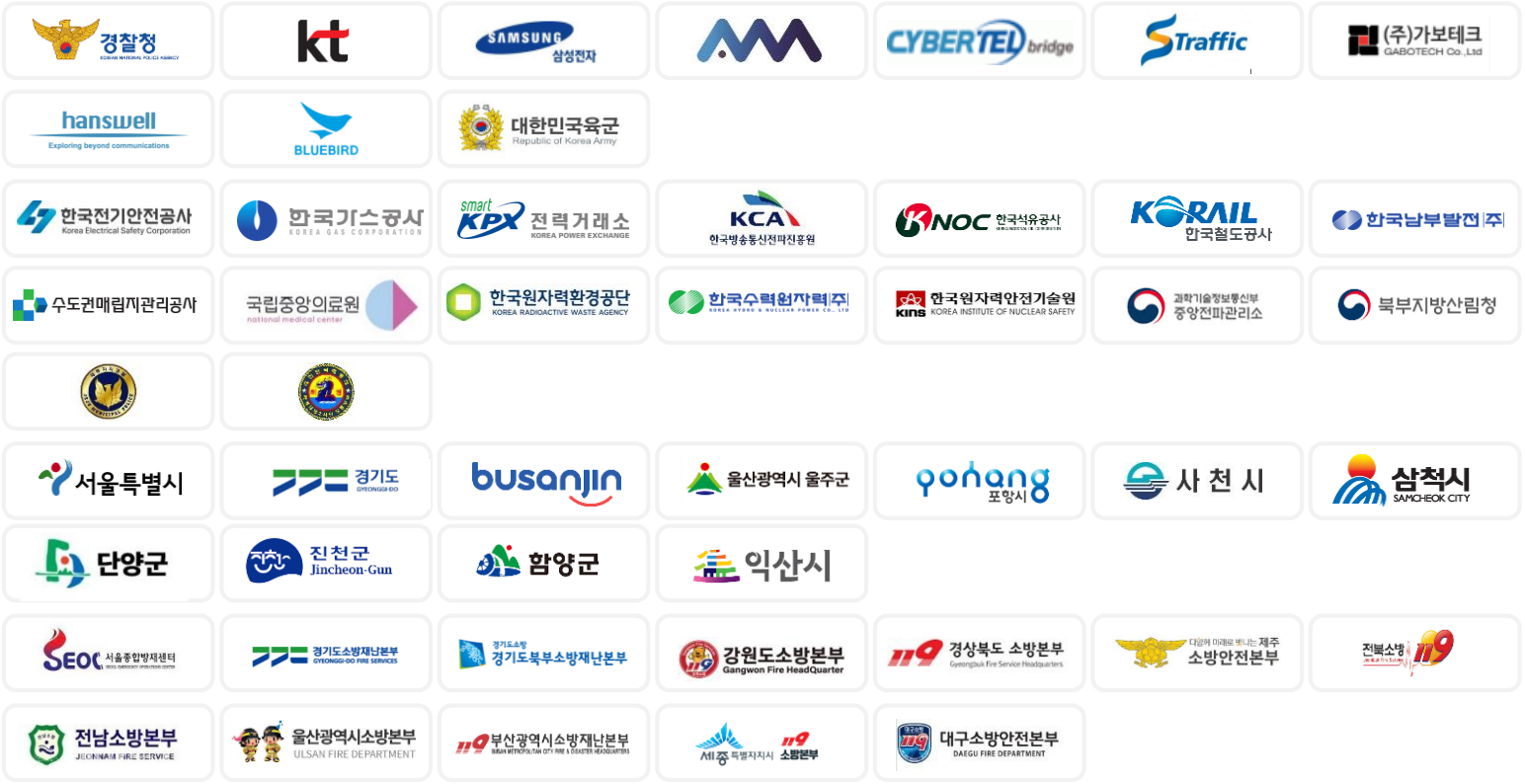
6. 레퍼런스

국가재난안전통신망

글로벌 서비스 기기 무결성 검사

모바일 스마트워크 보안

국가재난안전통신망



6. 레퍼런스

공공


대한민국육군
Republic of Korea Army
대한민국공군
REPUBLIC OF KOREA AIR FORCE
국방전산정보원
경찰청
미래정조과학부
보건복지부
세종특별자치시
용인시
강릉시
한국인터넷진흥원
한국교통안전공단
KITECH
한국생산기술연구원
Incheon Airport
서울도시철도
김포 GOLDLINE
Seoul Metro
서울메트로
한국항공우주산업㈜
한국전력
한국가스공사

민간


SK telecom
SK networks
SK C&C
SAMSUNG 삼성전자
SAMSUNG 삼성SDS
LG U+
아이티센그룹
ONE STORE
SK F&U
cross
monee
한국금거래소
KOREG
신용보증재단중앙회
경기신용보증재단
동양지축은행
moin
SK shieldus
SK 주식회사
SK encar.com
시큐센
secucen
오리온
GMD SOFT
OPSWAT.
KOOLSPAN
고려대학교의료원
ALPACO

감사합니다

서울시 송파구 송파대로 201 송파테라타워2 A동 G129-2 OS-33호
T : 02-575-3339 F : 02-575-3340 W : www.securion.co.kr