

AI기반 악성 앱 자동 분석 솔루션

OnAppScan 제품소개서

pr@securion.co.kr

2024.10

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

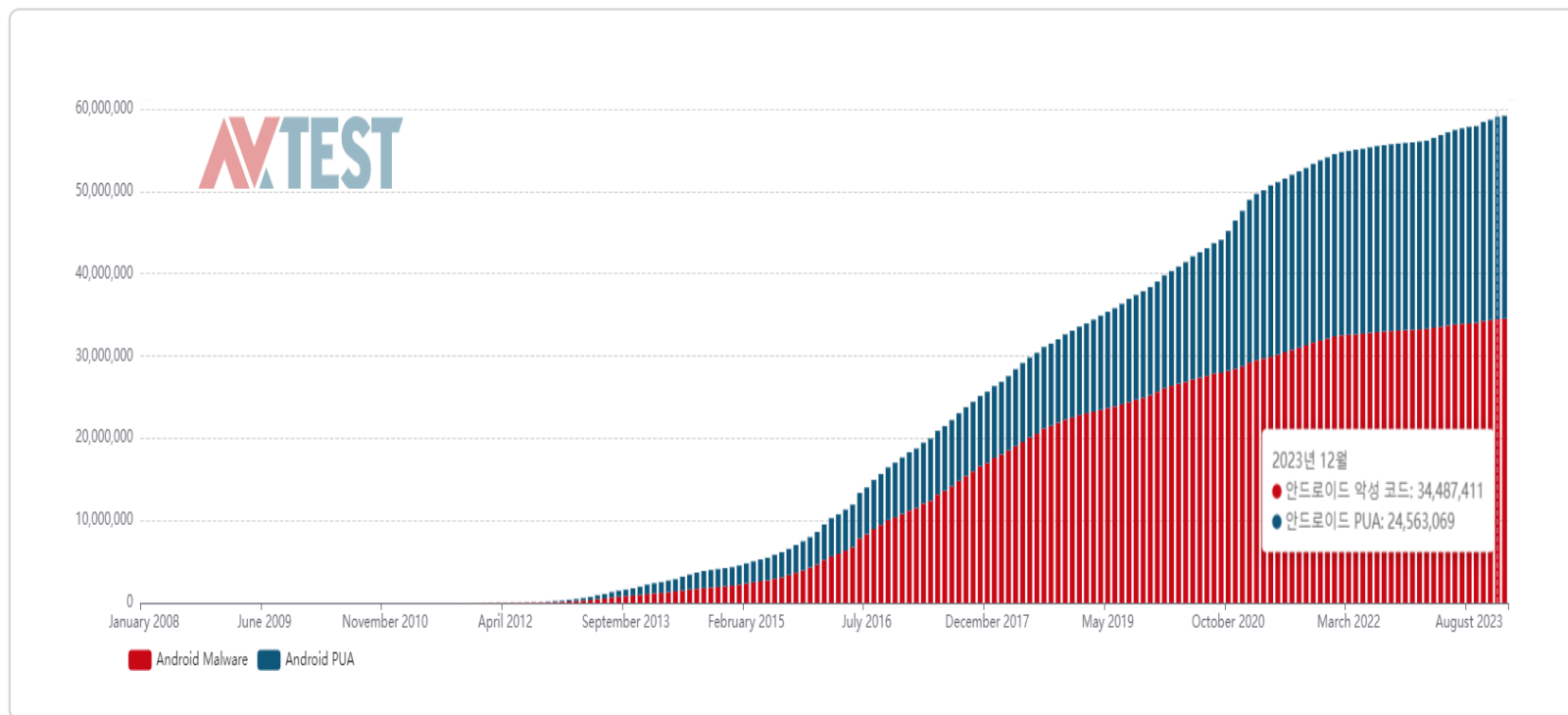
» ㈜시큐리온

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/

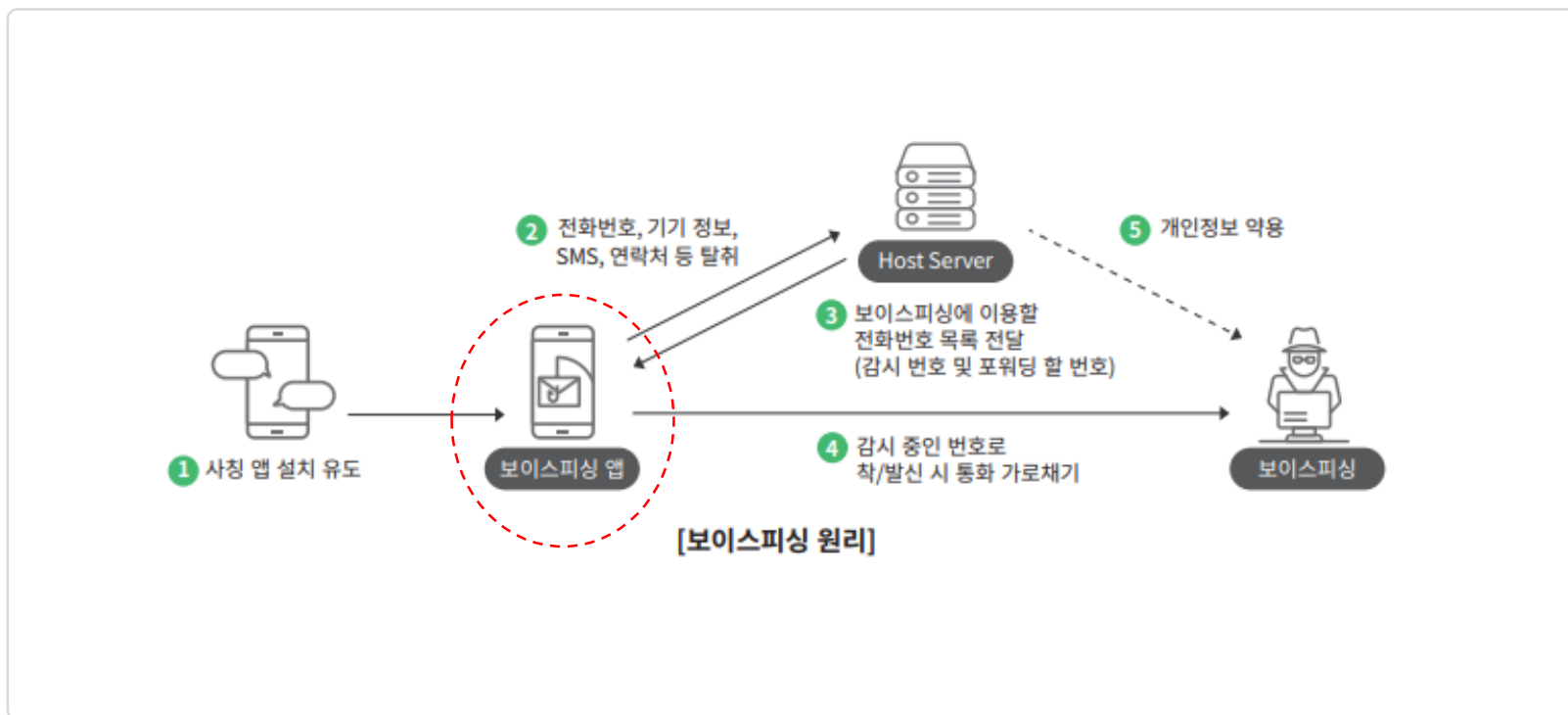
» 주요연혁

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

신·변종 가능성 높은 잠재적 악성앱(PUA) 증가
시그니처 기반 AV제품 탐지 오류, 전문가의 수동분석으로 보완

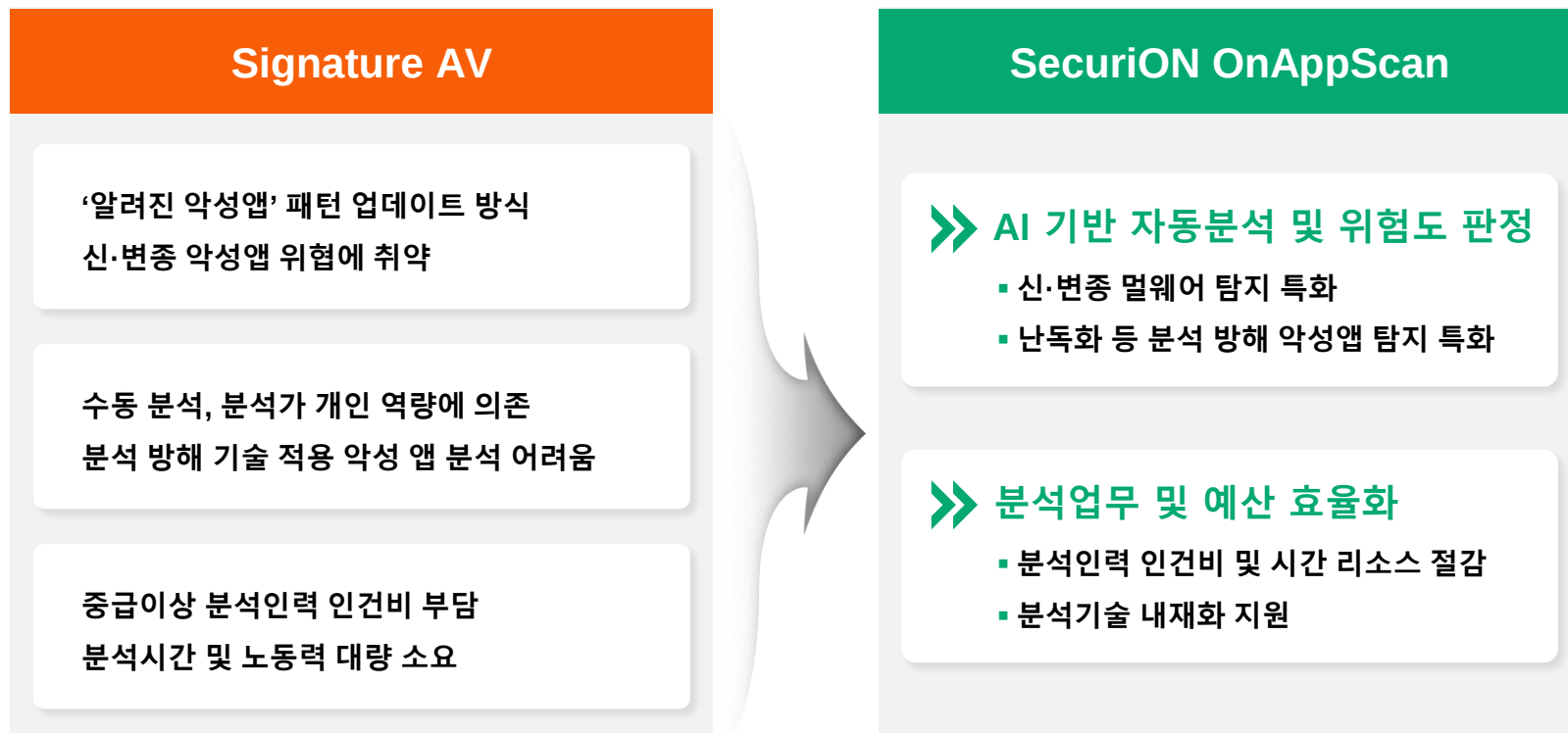


보이스피싱 악성 앱, 난독화·압축 해제 방해 등 분석 방해 기술 탑재 서비스형 난독화(obfuscation-as-a-service·OaaS) 등장



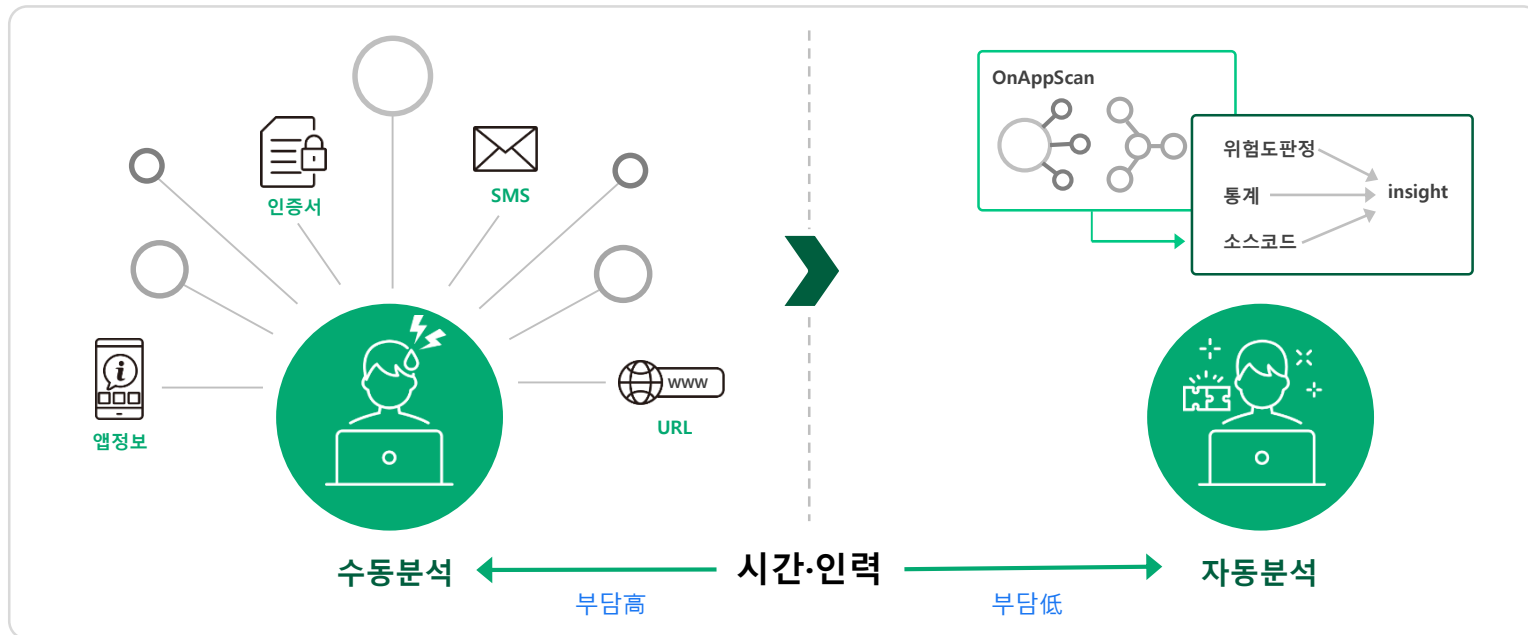
AI 기반 악성 앱 자동분석 솔루션 OnAppScan

‘수동분석→수동판정’ 프로세스, ‘자동판정→수동검증’으로 효율화



3. OnAppScan 소개 (1) 개요

ML 탐지 엔진 탑재 악성 앱 자동 분석 솔루션



판매형태

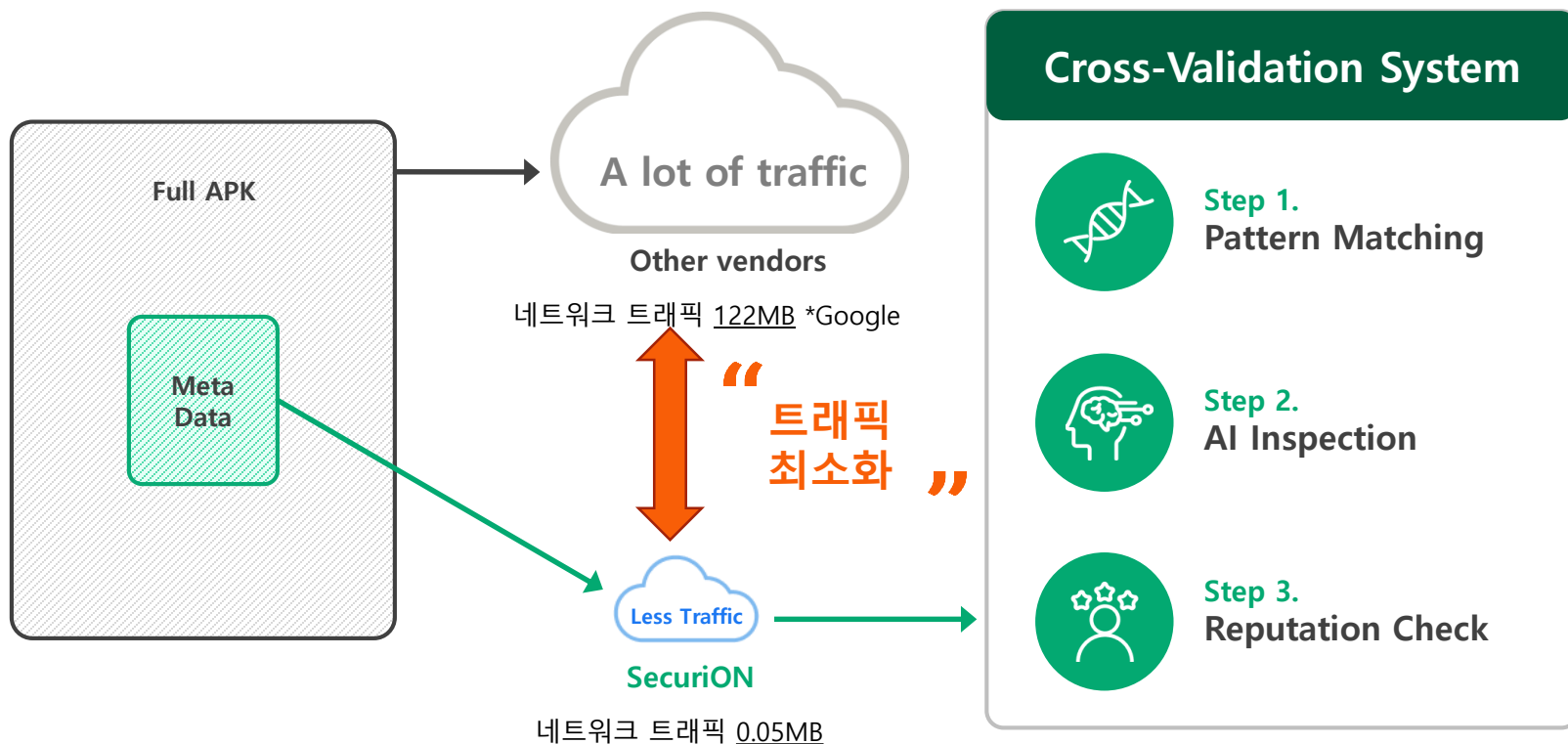
Appliance

(일체형 장비) 제공

클라우드 서비스

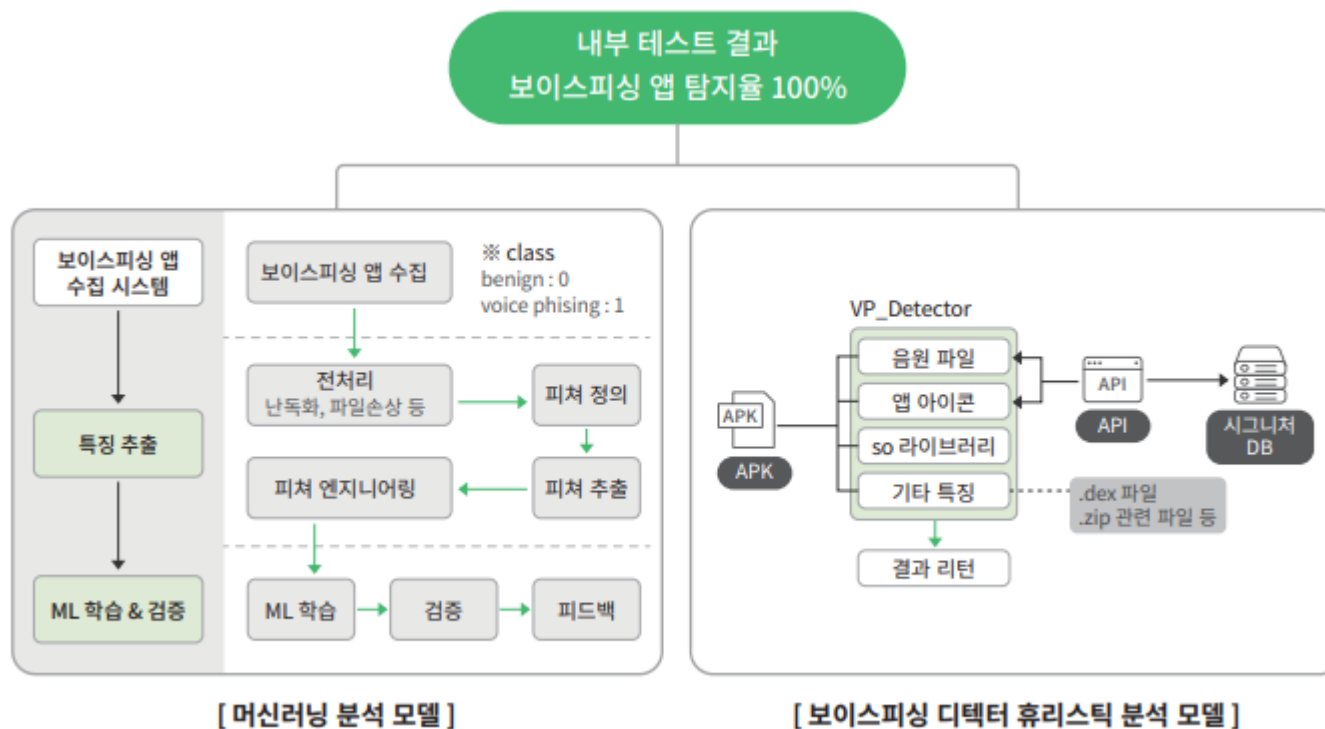
관리 콘솔 제공

시큐리온 AI 탐지 시스템 'CVS', 높은 탐지율과 낮은 리소스 소모량



보이스피싱 악성 앱 특징 추출, AI 및 패턴 기반 탐지 기능 고도화

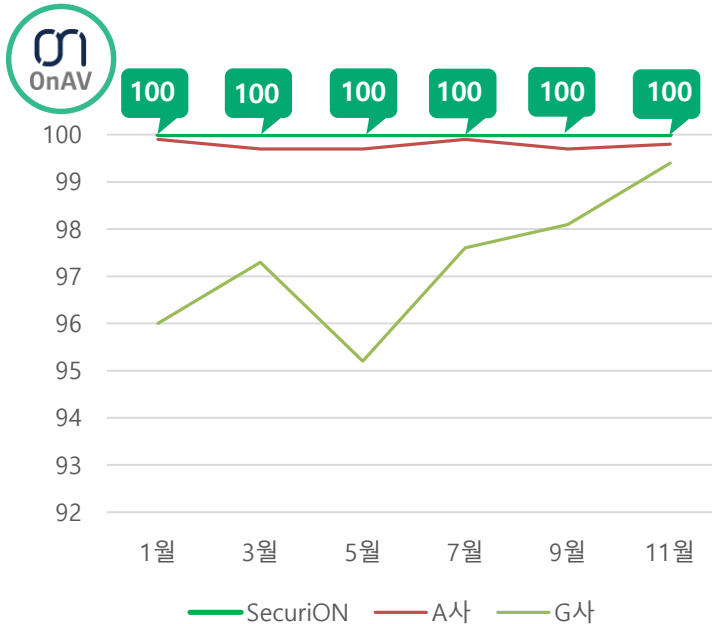
* IITP '휴대폰 단말에서의 보이스피싱 탐지, 예방 기술 개발' 사업 성과물 상용화 제품(관계사 아이넷캡 수행)



3. OnAppScan 소개 (3) 특징점

높은 악성 앱 탐지율로 수동분석 업무 최소화

AV-TEST Detection rate comparison(2023)



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	98.9%	100%
Google	Play Protect	94.9%	98.9%

출처 : AV-Test

분석 방해 기술 적용 보이스 피싱 악성 앱 탐지율 향상

머신러닝 분석모델 테스트 결과 1 *앱 출처: 정상(Playstore), 보이스피싱(2022년 수집)

구분	전체 개수	정탐 개수	오탐 개수	탐지율	전체 탐지율
정상	1500	1500	0	100%	100%
보이스 피싱	2041	2041	0	100%	

머신러닝 분석모델 테스트 결과 2 *앱 출처: 보이스피싱(2023년 8월 수집)

구분	전체 개수	정탐 개수	오탐 개수	전체 탐지율
보이스 피싱	113	113	0	100%

총 수집 앱 139개
피쳐 추출 불가 26개

보이스피싱 디텍터 테스트 결과 *앱 출처: 보이스피싱(2023년 8월 수집)

구분	전체 개수	정탐 개수	오탐 개수	전체 탐지율
보이스 피싱	139	138	0	99.28%

총 수집 앱 139개
피쳐 추출 불가 1개(파일손상)

3. OnAppScan 소개 (3) 특징점

정확도 높은 ML 기술로 앱 위험도 산출 및 악성행위 판정 악성 여부 판정 근거 '연관 앱 정보' 당사 단독 제공

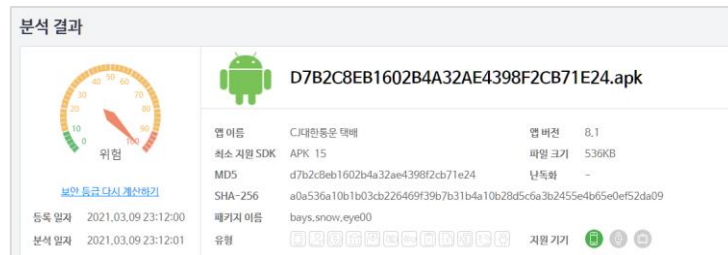
제품기능비교 *OnAppScan은 글로벌제품(V/T, AMAAAS, SandDroid, JOE-sandbox)의 150% 수준의 기능 제공

구분	자체판정		앱 분석					위험도 분석				연관 앱 정보			리소스 뷰어
	점수	등급	앱 정보	난독화 여부	인증서 정보	매니 페스트	유출지 정보	행위 정보	권한	String	API	동일 인증서	유출지	유사도 분석	
OnAppScan	O	O	O	O	O	O	O	O	O	O	O	O	O	O	O
Malwares.com	O	X	O	X	O	O	△	X	X	X	X	X	X	X	X
Hybrid-analysis	O	O	O	X	O	O	X	△	O	X	X	X	X	X	X
AMAAAS	O	X	X	X	X	X	X	X	△	X	X	X	X	X	X
Koodous	X	O	O	X	X	X	X	X	X	X	X	X	X	X	X
AVC UnDroid	O	X	O	X	X	O	X	X	O	X	O	X	X	X	X
Intezer Analyze	X	O	O	△	X	X	X	X	X	X	X	X	X	X	X
JOE Sandbox	O	O	O	X	X	O	O	O	X	X	△	X	X	X	X

동적 분석 없이도 실시간 판정 성능 보장

3. OnAppScan 소개 (4) 주요기능 및 UI

악성코드의 위험도 및 악성 행위에 대한 직관적 UI



AI 통한 위험도 산출

동일한 인증서를 사용하는 다른 앱

파일명	SHA-256
검진모아 com.opera.simi	b7dfdb6e8d1d17d47c6932eafc355a06e0ddc
Chrome m.mo.ry	10f57aed20847104b66b8d0e5579a97d9b8d
농협은행 com.google.vclue	39339320b9a2b61839fffd692a326074db1d6

분석대상 악성 앱과
동일 인증서 사용 앱 목록
→ 동일 인증서로 악성코드를 유포하는
집단(그룹) 추정 가능

Manifest 정보

권한

항목	설명
android.permission.CALL_PHONE	통화
android.permission.INTERNET	네트워크 소켓 연결 허용
android.permission.MODIFY_PHONE_STATE	전화 상태(power on, mmi 등)를 수정
android.permission.READ_PHONE_STATE	전화 상태를 읽을수 있도록 허용
android.permission.RECEIVE_SMS	SMS 메시지 수신(모니터링, 기록, 처리 기능) 허용
android.permission.SEND_SMS	SMS 메시지 전송 허용

악성코드가 주로 요구하는
권한 및 행위에 대한
위험도와 통계 정보 제공

고객 니즈에 따라 클라우드 또는 어플라이언스 제공

클라우드 기반 서비스

- 시큐리온 클라우드 서버를 통해 자동분석 서비스
- 별도의 내부 솔루션 구축 비용이 없고
계정 별 이용량에 따른 비용 부과로 예산 절감

페쇄망 기반 서비스

- Appliance 제공으로 고객사 내부 분석 시스템 구축
- 기본시스템 분석 서비스 외
평판검사/AI검사/패턴DB검사 유료 라이선스 제공

구분	OnAppScan appliance
Server OS	Linux
WAS / DB / JDK	NginX 1.10 / Postgres 9.5 / openjdk-8
CPU / Disk / Memroy	1 CPU / 1TB / 32GB
Client Browser	-크롬 38~79(Stable), 80,81,82 -파이어폭스 72(Stable), 73,74 -오페라 66(Stable), 67,68 -IE 11(Edited) -엣지 44(EdgeHTML Stable), 81,82(Chromium Beta, Canary) -사파리 12(모하비), 13(Developer Preview)

4. 인증 및 수상

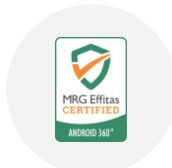
시큐리온 AI탐지 시스템(OnAV) 글로벌 Top 3 인증 획득



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

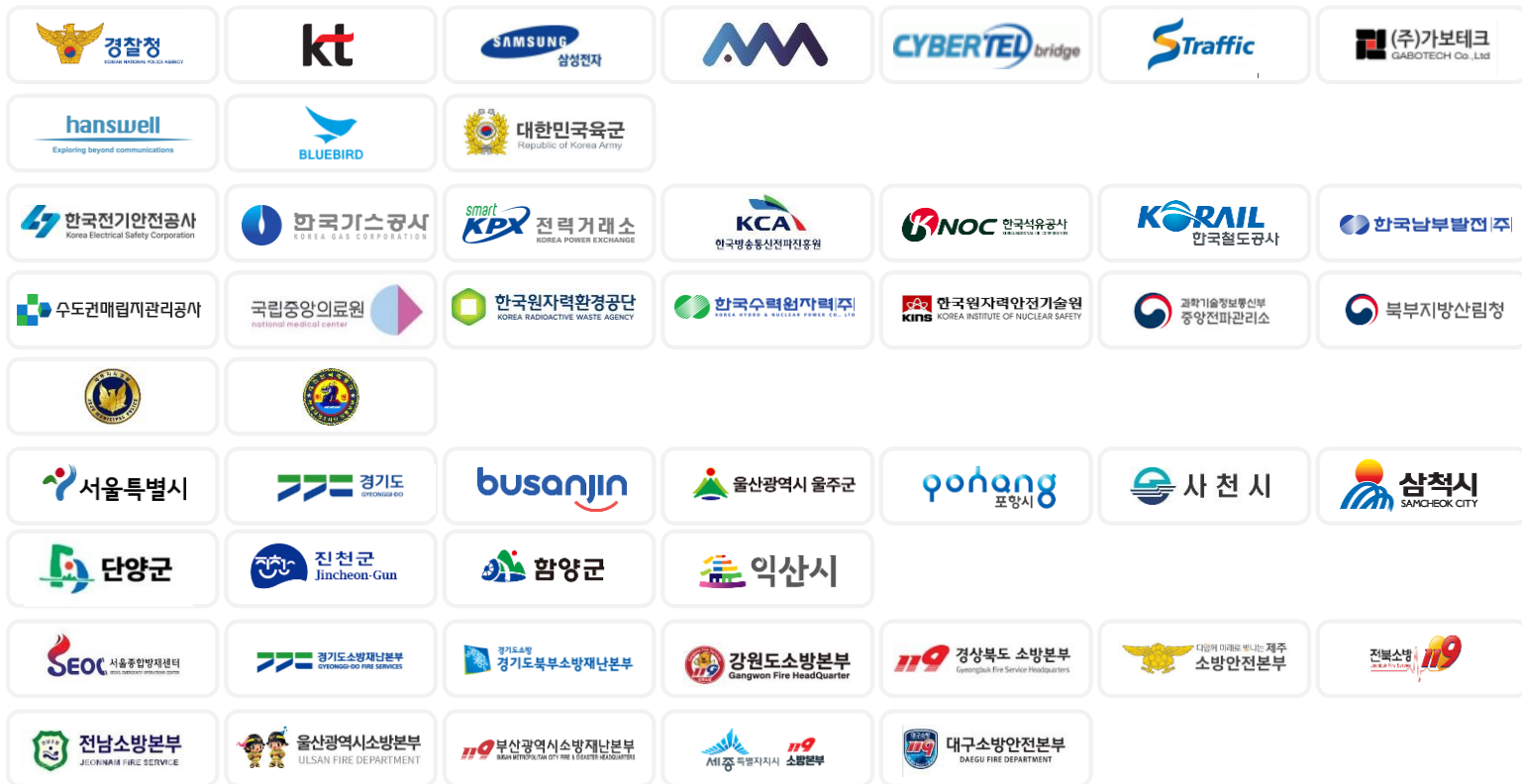
6. 레퍼런스

마켓 침투 악성 앱 제거
ONE 1 STORE

보이스피싱 고객 피해 방지
LG유플러스

사이버 침해대응 본부
KISA 한국인터넷진흥원
KOREA INTERNET & SECURITY AGENCY

국가재난안전통신망



6. 레퍼런스

공공



민간



감사합니다

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