AI기반 악성 앱 자동 분석 솔루션

# OnAppScan 제품소개서

pr@securion.co.kr

2022.04

# AI기반 사이버 보안기업

- 글로벌 인증 AI탐지 시스템과 독자 보안 기술로 모바일·IoT 디바이스 보호

머신러닝 기반 안티바이러스
**OnAV**

IoT·모바일 종합 보안 솔루션
**OnTrust**

악성 앱 자동분석 솔루션
**OnAppScan**

## ㈜시큐리온

- **대표자 :** 이성권(총괄), 유동훈(기술) 각자대표
- **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

**2010** **아이넷캅, 안드로이드 보안 솔루션 개발사업 착수**

**2019** **시큐리온 법인 설립**

'On' Brand 시리즈 라이선스 계약

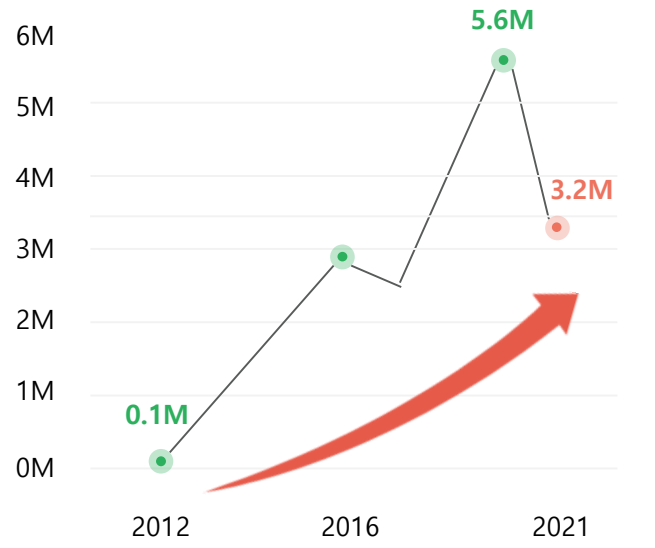
2021 IoT·모바일 종합보안 솔루션 OnTrust 출시

# 2. 제안배경 (1) 모바일 위협 현황

## 신·변종 가능성 높은 잠재적 악성앱 증가

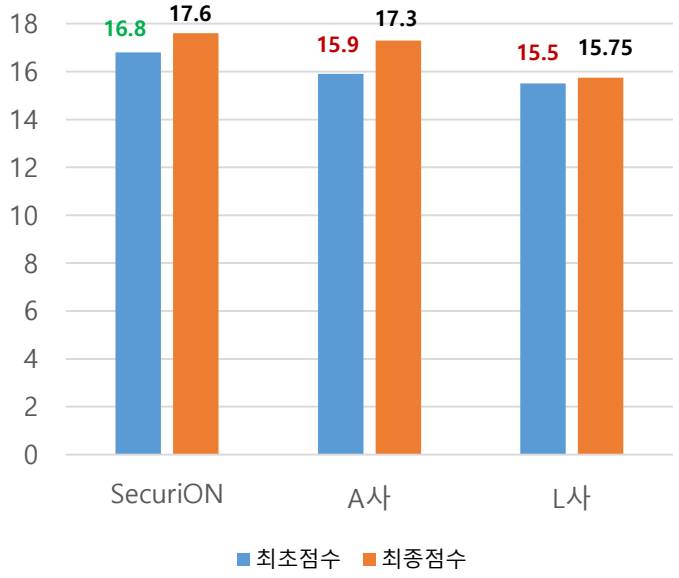
## 시그니처 기반 AV제품 탐지 오류, 전문가의 수동분석으로 보완

### 잠재적 악성앱(PUA) 증가




* AV-TEST 조사

### 국내 AV제품 최초-최종 점수 비교



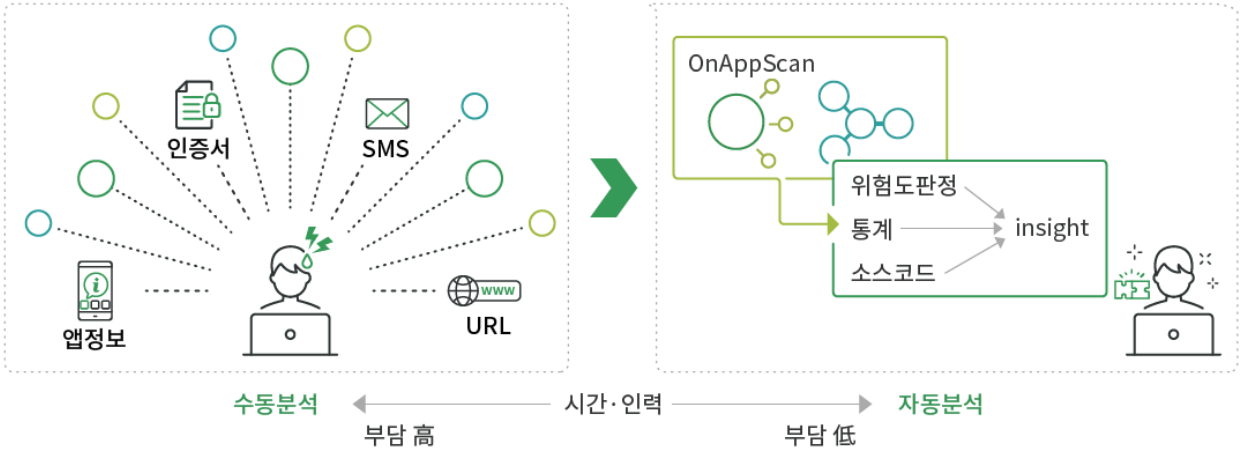

* AV-TEST 조사, 21년 5회 평균

## AI 기반 악성 앱 자동분석 솔루션 OnAppScan

### 신·변종 악성코드 분석 특화, 분석업무 효율화

| Signature AV | | SecuriON OnAV |
|---|---|---|
| 시그니처 기반분석 | 불안정하고 낮은 탐지 정확도<br>전문인력 수동분석 必 | **AI 기반 자동분석 및 위험도 판정**<br>▲ 신변종 멀웨어 탐지율<br>▼ 개인역량 의존도 |
| 분석가 업무부담 | 신·변종 멀웨어 분석 난이도 증가<br>개인역량 의존도 高 | |
| 비효율적 예산운영 | 중급이상 분석인력 인건비 부담<br>분석시간 및 노동력 리소스 高 | **분석업무 및 예산 효율화**<br>✓ 분석인력 인건비 및 시간 리소스 절감<br>✓ 분석기술 내재화 지원 |

## ML 기반 OnAV 엔진 연동 악성 앱 자동 분석 솔루션



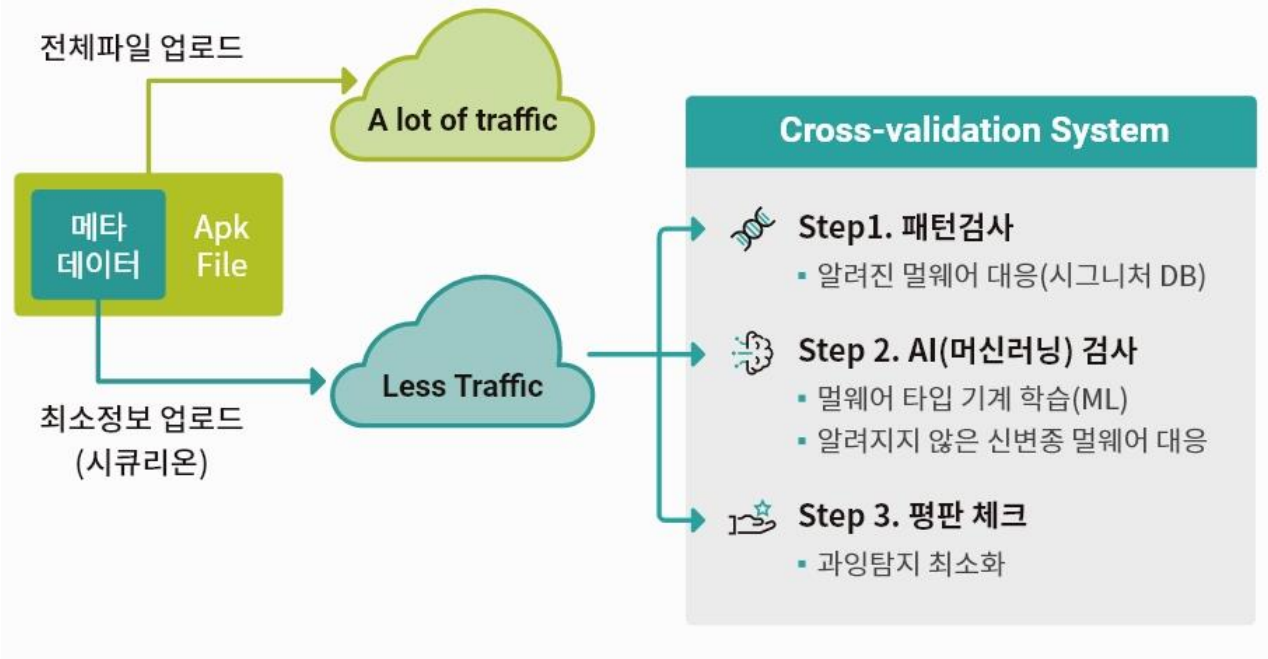

**판매형태**

**Appliance** (일체형 장비) 제공

**클라우드** 서비스 : 관리 콘솔 제공

## 시큐리온 AI 탐지 시스템 'CVS' 적용

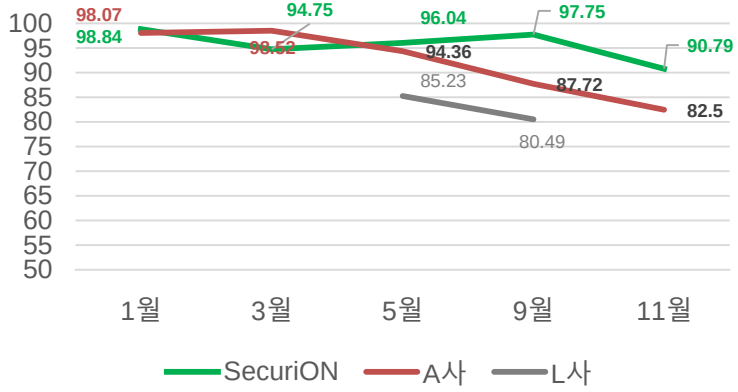
**머신러닝 검사와 패턴 검사, 평판검사 결합해 높은 탐지율 유지**



# 3. OnAppScan 소개 (2) 특장점

## 독보적인 '잠재적인 악성앱(PUA)' 탐지율로 수동분석 업무 최소화

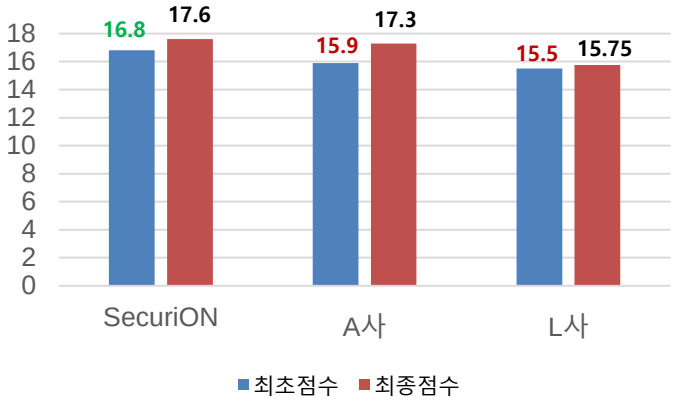
AV-TEST PUA 탐지율 비교 (2021년)




→ 잠재적인 악성앱(PUA),
알려지지 않은 신·변종 악성앱일 가능성 高

→ ML기술 시큐리온과 타사 사이에 큰 차이 존재

AV-TEST 최초/최종 점수 비교 (21년 5회평균)




→ 18점 만점 기준 최초/최종 점수

→ 최초·최종 결과 차이 적을수록
인력 리소스 절감

# 3. OnAppScan 소개 (3) 특장점

## 정확도 높은 ML 기술로 앱 위험도 산출 및 악성행위 판정

## 악성 여부 판정 근거 '연관 앱 정보' 당사 단독 제공

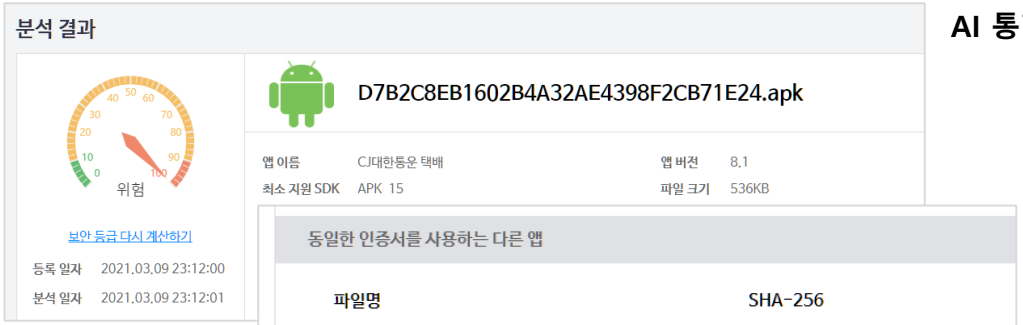
**제품기능비교** *OnAppScan은 글로벌제품(V/T, AMAAAS, SandDroid, JOE-sandbox)의 150% 수준의 기능 제공

| 구분 | 자체판정 | | 앱 분석 | | | | | 위험도 분석 | | | | 연관 앱 정보 | | | 리소스 뷰어 | 동적 분석 |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| | 점수 | 등급 | 앱 정보 | 난독화 여부 | 인증서 정보 | 매니페스트 | 유출지 정보 | 행위 정보 | 권한 | String | API | 동일 인증서 | 유출지 | 유사도 분석 | | |
| OnAppScan | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ |
| Malwares.com | ✓ | ✗ | ✓ | ✗ | ✓ | ✓ | △ | ✗ | ✗ | ✗ | ✗ | ✗ | ✗ | ✗ | ✗ | ✗ |
| Hybrid-analysis | ✓ | ✓ | ✓ | ✗ | ✓ | ✓ | ✗ | △ | ✓ | ✗ | ✗ | ✗ | ✗ | ✗ | ✗ | ✓ |
| AMAaaS | ✓ | ✗ | ✗ | ✗ | ✗ | ✗ | ✗ | ✗ | △ | ✗ | ✗ | ✗ | ✗ | ✗ | ✗ | △ |
| Koodous | ✗ | ✓ | ✓ | ✗ | ✗ | ✗ | ✗ | ✗ | ✗ | ✗ | ✗ | ✗ | ✗ | ✗ | ✗ | ✗ |
| AVC UnDroid | ✓ | ✗ | ✓ | ✗ | ✗ | ✓ | ✗ | ✗ | ✓ | ✗ | ✓ | ✗ | ✗ | ✗ | ✗ | ✗ |
| Intezer Analyze | ✗ | ✓ | ✓ | △ | ✗ | ✗ | ✗ | ✗ | ✗ | ✗ | ✗ | ✗ | ✗ | ✗ | ✗ | ✗ |
| JOE Sandbox | ✓ | ✓ | ✓ | ✗ | ✗ | ✓ | ✓ | ✓ | ✗ | ✗ | △ | ✗ | ✗ | ✗ | ✗ | ✓ |

동적분석 없이
실시간 탐지성능 보장

# 3. OnAppScan 소개 (4) 주요기능 및 UI

## 악성코드의 위험도 및 악성 행위에 대한 직관적 UI 제공




AI 통한 위험도 산출

분석대상 악성 앱과

동일 인증서 사용 앱 목록

→ 동일 인증서로 악성코드를

유포하는 집단(그룹) 추정 가능


악성코드가 주로 요구하는

권한 및 행위에 대한

위험도와 통계 정보 제공

## 고객 니즈에 따라 클라우드 또는 어플라이언스 제공

### 클라우드 기반 서비스

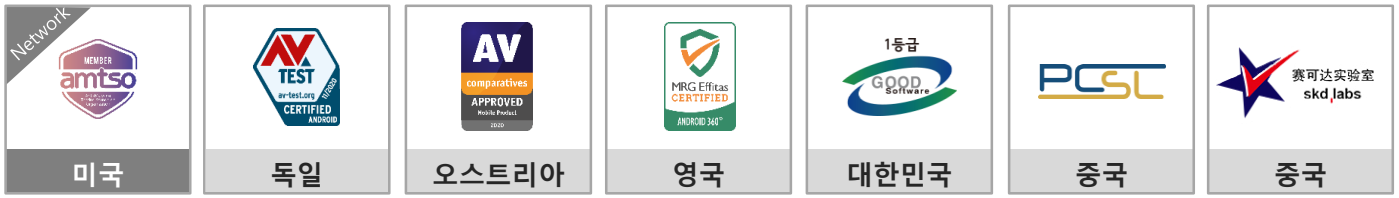
- 시큐리온 클라우드 서버를 통해 자동분석 서비스
- 별도의 내부 솔루션 구축 비용이 없고
  계정 별 이용량에 따른 비용 부과로 예산 절감

### 폐쇄망 기반 서비스

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

| 구분 | OnAV 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<br>-파이어폭스 72(Stable), 73,74<br>-오페라 66(Stable), 67,68<br>-IE 11(Edited)<br>-엣지 44(EdgeHTML Stable), 81,82(Chromium Beta, Canary)<br>-사파리 12(모하비), 13(Developer Preview) |

## 글로벌 Top 3 인증 획득




## 주요 레퍼런스

SK telecom, SK networks, SK encar.com, SK C&C, SK infosec, SK 주식회사, SK shieldus

SAMSUNG 삼성SDS, SAMSUNG 삼성전자, NSOK, F&U, 오리온, cen 시큐센 secucen, cen 아이티센 ITCEN

미래창조과학부, 보건복지부, 5678 행복미소 서울도시철도, Seoul Metro 서울메트로, 김포 GOLDLINE

세종특별자치시, 강릉시, 한국가스공사, 한국전력, KOREA GOLD EXCHANGE 한국금거래소

고려대학교의료원 KOREA UNIVERSITY MEDICAL CENTER, ALPACO, OPSWAT., cross, moin

# 감사합니다

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