



AI 기반 모바일 안티바이러스 **OnAV**

글로벌 인증 획득 AI 악성 앱 탐지 시스템

2025.01

Contents

1. 제안배경
2. 제품소개
3. 기대효과
4. 적용분야 및 사양
5. 인증 및 수상
6. 특허
7. 레퍼런스



AI based Cyber Security Company

 OnAV

AI 기반 모바일 안티바이러스
OnAV

 OnTrust

모바일·IoT 종합보안 솔루션
OnTrust

 OnAppScan

AI 악성앱 자동분석 시스템
OnAppScan

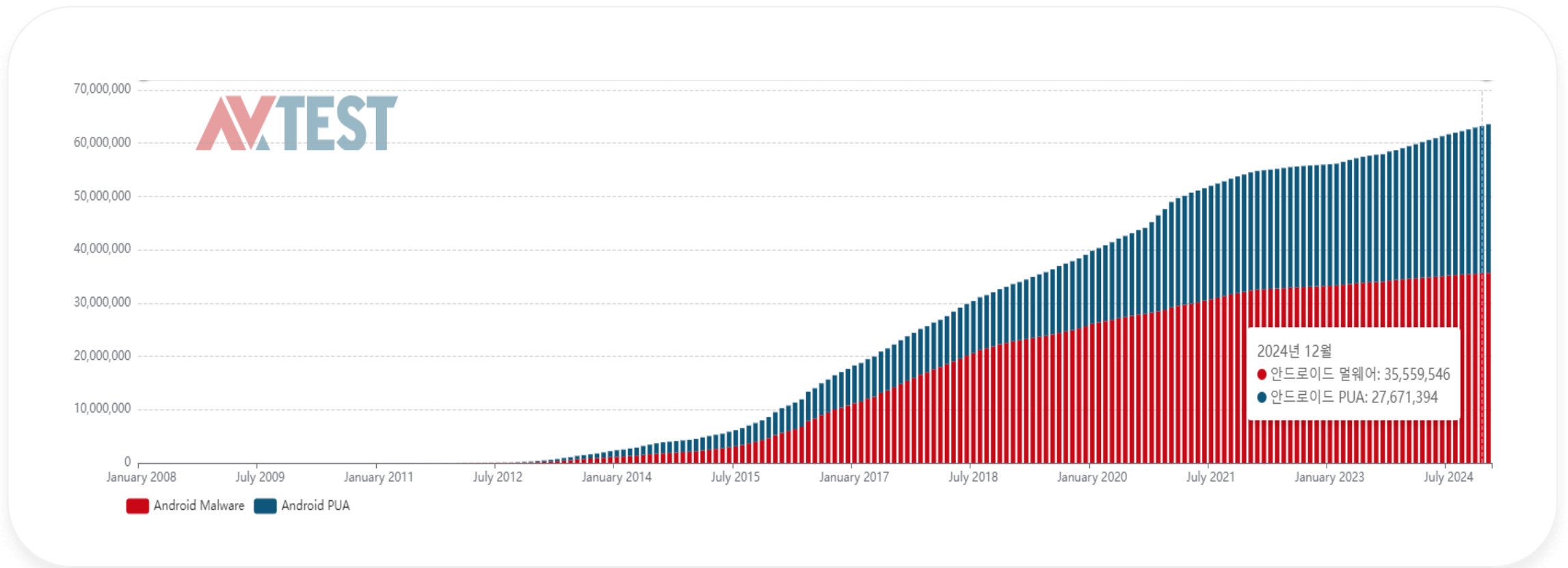
 OnAV for
Linux Desktop

리눅스 OS 안티바이러스
OnAV for Linux Desktop

1. 제안배경 (1) 모바일 위협 증가

안드로이드 악성 앱 및 잠재적 악성앱(PUA) 증가

애드웨어 등 PUA, 악성 행위가 가능한 코드를 숨긴 채 정상 앱으로 가장해 유포

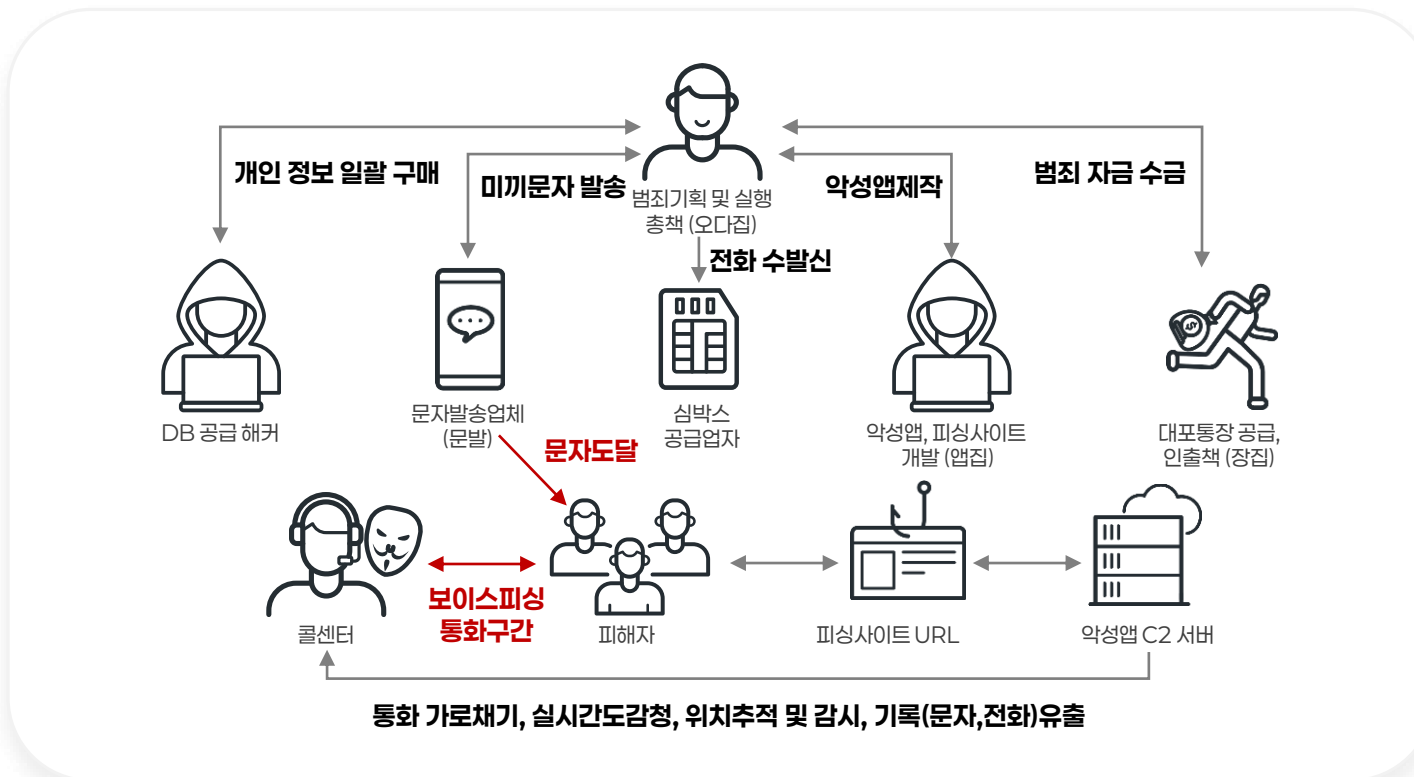


PUA: Potentially Unwanted Application, 주로 애드웨어/ 다운로드 및 브라우저 도구 모음 / 정상 앱과 함께 설치되는 번들웨어, 프록시웨어, 크립토 마이너 등을 포함

1. 제안배경 (2) 위협 대응 난이도 상승

악성 앱 이용 피싱 범죄 생태계, 악성 앱 대량 생산 및 확산에 일조

기존 보안 솔루션 탐지 회피 악성 앱 증가(신·변종 악성 앱, 필터링 우회 공격 기법 등)



최근 보이스피싱·스미싱 범죄 생태계

- 1 텔레그램, 위챗, QQ 내 전문화된 개별 업자와 연계해 범죄 기획 및 실행
- 2 SMS 문자 발송 업체를 통한 대량 발송, 필터링 우회를 통한 높은 문자 도달률
- 3 전문 업체 통한 악성 앱 외주 제작, 피싱 사이트 및 URL 생성, C2 서버 구축
→ 악성 앱 전문 제작자의 지능형 악성 앱 대량 생산 및 배포
→ 누구나 손쉽게 악성 앱 구입, 공격 활용

C2 서버: Command & Control (C&C, 명령 및 제어) 서버 공격자가 공격 대상 장치와 통신을 유지하는 데 사용하며 공격자의 명령을 전달하고 추가 악성코드 다운로드, 데이터 탈취 용도로 사용

1. 제언배경 (3) IoT 확산으로 인한 위협 확대

스마트 홈 및 스마트 시티 환경에 안드로이드 기반 IoT 디바이스 확산 탐지 소요 리소스가 큰 패턴 기반 안티바이러스 솔루션 적용에 어려움



패턴 기반 안티바이러스 탐지 원리

악성 앱
최초 발견

악성 앱 분석
및 패턴 추출

패턴 공유
(up/down)

User
device 검사

- 악성 앱 분석 시 앱 전체 data 요구
- 정확한 탐지를 위해 패턴이 쌓일 수록 용량이 커짐
- 패턴 파일 송수신에 대량의 트래픽 소요

대부분의 패턴기반 보호 제품은 IoT 적용 불가

현재 국내외 패턴 기반 보안솔루션, 안드로이드 6.0(2015년) 이상 OS버전만 지원

1. 제안배경 (4) 기존 기술의 한계 및 대응 방안

AI 보안 기술로 모바일·IoT 대상 지능형 악성 앱 대응

패턴 기반 솔루션 한계 극복한 초경량·고효율 탐지 엔진 제공

기존 패턴 AV

신·변종 악성 앱 방어 한계
지능화 된 공격에 취약

악성 앱 확산 속도 급증, 신속 대응 불가
패턴 확보를 위한 수동분석 의존도 향상
분석가 업무 과부하 및 분석 시간 지연

디바이스 자원 대량 소모로 인한 성능 저하
불편한 사용자 경험
스마트홈 및 스마트시티 IoT 환경 보호 부적합

SecuriON OnAV

신·변종 악성 앱 탐지 정확도 향상
머신러닝 학습을 통해 지능형 악성 앱 탐지 특화

악성 앱 증가 속도에 발 맞춘 신속 대응
AI 엔진으로 신종/변종 악성 앱도 실시간 탐지
패턴 확보 등 악성 앱 분석 소요 시간 단축

초경량 엔진 구현
가볍고 쾌적한 사용자 경험
저사양 IoT 기기 보호 최적화

Accurate

Real-time

Lightweight

2. 제품소개 (1)개요

글로벌 인증기관 선정 '안드로이드를 위한 최고의 보안 앱' OnAV AI 모바일 안티바이러스 솔루션

검증된 성능과 사용성

- ✓ 악성코드 탐지율 **99% 이상**
- ✓ 앱 설치 다운로드데이터 **1MB 이하**
- ✓ 트래픽 사용율 **1MB 이내**

Secu-ordi 2023년 '최고의 무료 안드로이드 바이러스 백신' 선정

- 프랑스 IT 보안 전문 웹사이트 'Secu-ordi' 자체 진행 글로벌 안티바이러스 솔루션 탐지율 평가
- 22년에 이어 2년 연속 '최고의 무료 안드로이드 바이러스 백신' 선정

AV-TEST 2022년 '안드로이드를 위한 최고의 보안 앱' 선정

- 독일 글로벌 보안제품 성능평가 기관 AV-TEST 진행 내구성 테스트(Endurance Test) 18점 만점 획득
- '안드로이드를 위한 최고의 보안 앱(the Best Security Apps for Android)' 선정

AV-Comparatives 2024년 'AV-Comparatives Awards 2024' 수상

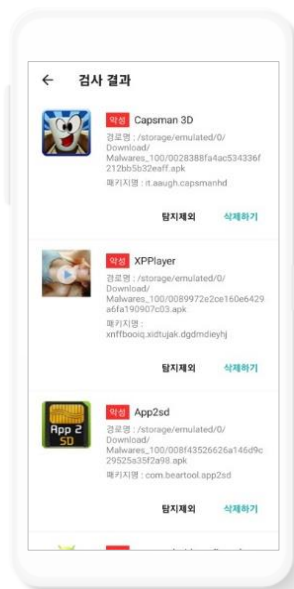
- 오스트리아 글로벌 보안제품 성능평가 기관으로 연1회 글로벌 안티바이러스 솔루션 탐지율 평가
- Securon은 6년 연속 AV-Comparatives의 모바일 보안 테스트에서 성공을 거두고 모바일 보안 상을 수상

2. 제품소개 (2)주요기능

AI 검사·패턴 검사·평판 검사 결합해 악성 앱 탐지와 치료, 기기 루팅 검사 기능 제공



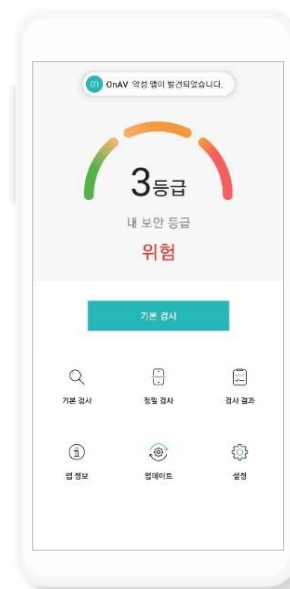
☑ 스마트폰 보안 등급 판정



☑ 기본검사 — 기기에 설치된 앱 검사



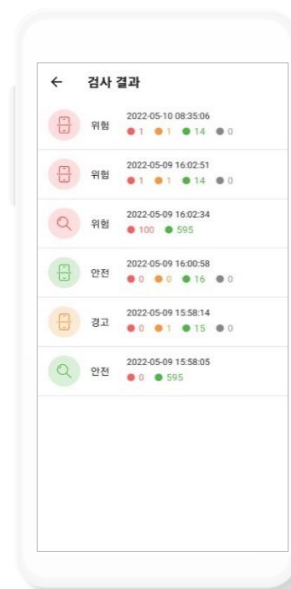
☑ 정밀검사 — 기기에 설치된 앱 검사
저장소 앱 설치파일 검사



☑ 실시간 검사 — 기기에 설치되는 새로운 앱 검사



☑ 야간검사 — 배터리 잔량 90% 이상,
충전 중 일 때 매일 야간마다 정밀 검사

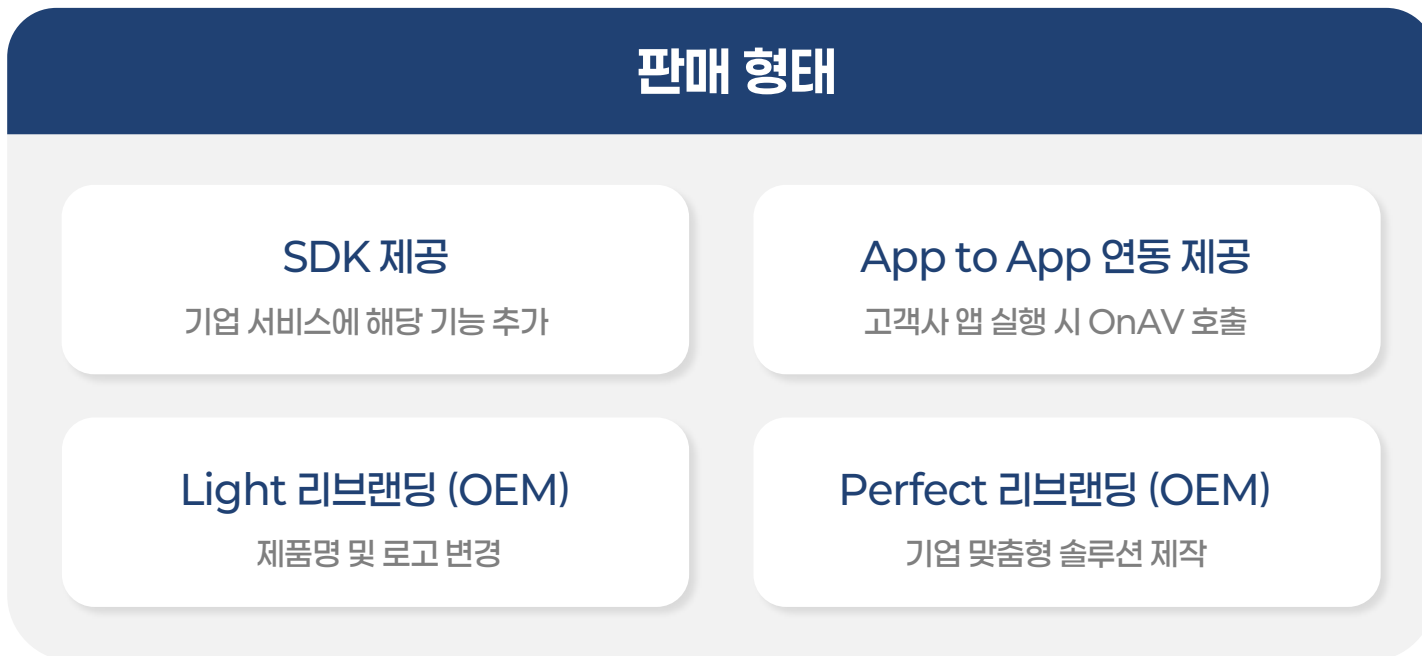


☑ 업데이트 — 최신 패턴 DB 업데이트

2. 제품소개 (3)판매 형태

OnAV, 연간 라이선스(SaaS) 판매

고객 상황에 맞게 다양한 형태로 서비스 제공



보안 기능 통합 방식 별 특징

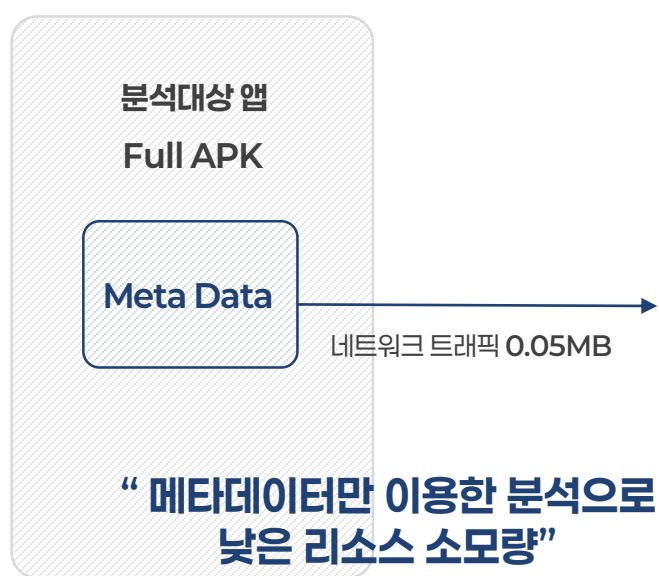
- 1 SDK**
개발도구키트(Software Development Kit)를 통해 고객사 서비스 시스템 내에 보안 기능 구현, 필요 기능 모듈화 및 커스터마이징 용이
- 2 App to app**
보안 앱을 연동하는 방식으로 간편한 기능 구현
고객사 서비스 동작 시 이용 장치와 환경을 실시간으로 보호

2. 제품소개 (4)핵심기술

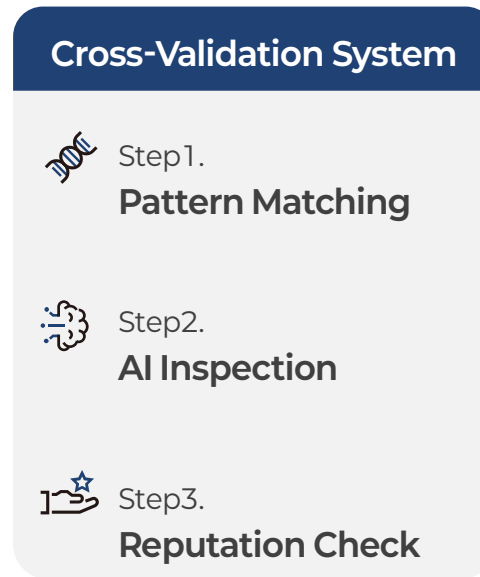
AI 기반 ‘크로스 밸리데이션 시스템(CVS)’으로 탐지 정확도 향상

머신러닝 검사와 패턴 및 평판 검사를 결합해 AI 엔진의 과잉탐지 이슈를 보완

“ 높은 탐지율과 낮은 리소스 소모량 구현 ”



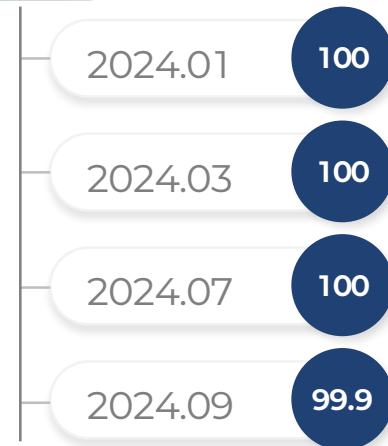
Full APK 이용 G사 엔진 대비 5400분의 1



“ 교차 검증을 통한
탐지 정확도 향상 ”



AV-TEST
Detection rate



3. 기대효과 (1)검증된 AI 보안 기술 도입

글로벌 성능 평가에서 높은 탐지율을 수년간 유지하며 AI 탐지 기술 안정성 입증

“지속적으로 높은 탐지율 유지”

AV-TEST 2022~2024 평가 그래프



AV-TEST 2023 내구성 평가

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

3. 기대효과 (2)안정적 서비스 운영

대규모 서비스 지원 경험 및 노하우 보유 *시큐리온 엔진 탑재 모바일 안티바이러스 누적 다운로드 수 1442만 건

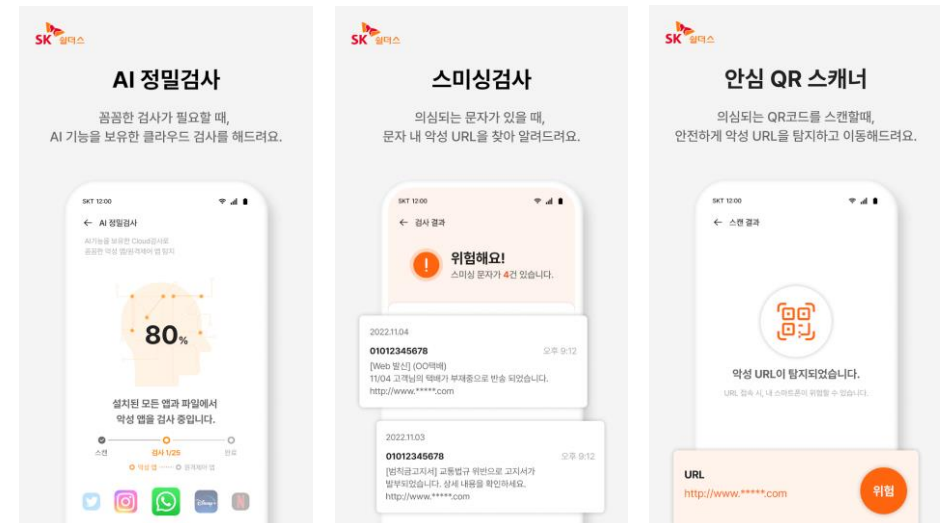
“ 대형 서비스 유지 운영에 필요한 맞춤형 지원 ”

사례

- SKT, 스미싱 피해가 극심하던 2013년 ‘T가드’ 개발,
SKT 고객 대상 선택재 앱으로 제공
- 2021년 SKT ‘T가드’→SK실더스 ‘모바일가드’로 리브랜딩

누적 다운로드 수 1,424만건에 달하는 대규모 서비스로
그에 걸 맞는 지원이 필요

시큐리온은 다양한 고객이 있는 만큼 고객별 수요에 맞춰 검사 기능을 세분화 하거나 최신 보안 기능 개발을 지원하고, 다수의 동시 접속자를 수용할 수 있도록 클라우드 기반 백엔드 서버를 개발하고 구축하는 것을 지원함



3. 기대효과 (3) 이슈 발생시 신속 대응

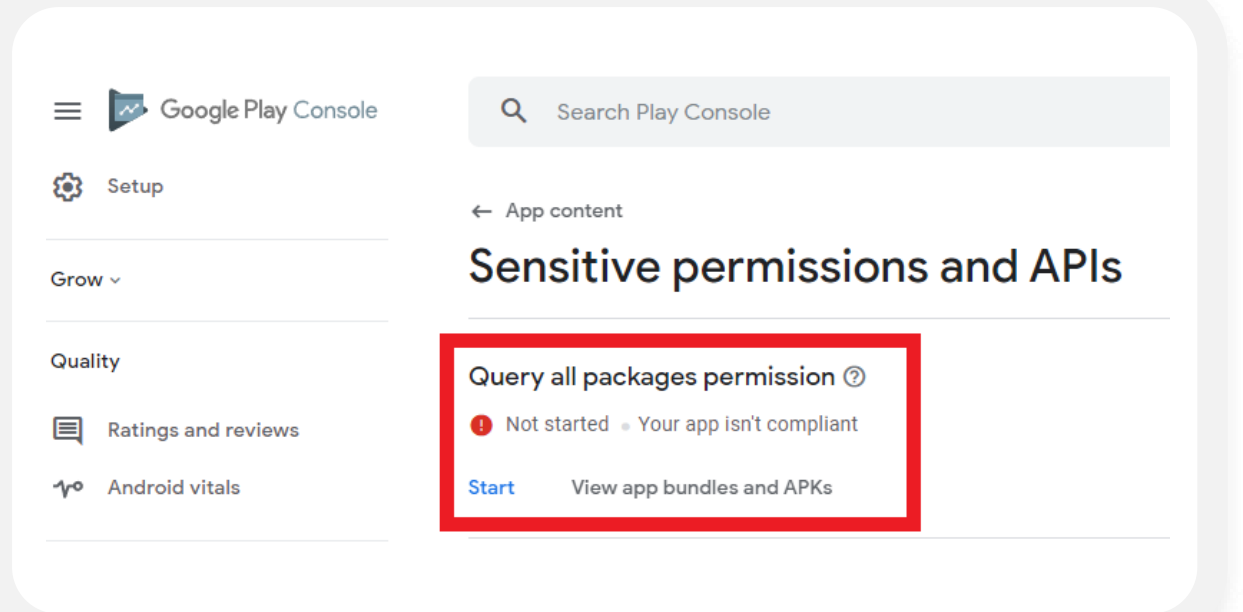
국내 기업 독자 개발 라이선스, 앱 비즈니스 유지를 위한 신속한 이슈 대응 가능

“마켓 정책 변화 신속 반영 & 서비스 옵션 개발 지원”

사례

2022 구글 플레이스토어
개인정보 정책 강화의 일환으로
'Query all packages permission' 권한을
'민감 정보를 읽어가는 권한' 으로 판단해
다양한 앱이 심사 탈락

시큐리온, 고객사와 협의하여 고객이 직접
보안수준과 보안서비스 제공 방식을 선택하도록 해
해당 이슈 해결



3. 기대효과 (4)긴급 장애 대응 지원

불편 및 장애 대응 상시 접수, 지원



불편접수 채널 운영

전화 및 이메일 상시 접수

긴급 장애 상황 대비한 비상 연락망 운영



장애 상황 등급별 대응

일반/긴급 우선 순위에 따른 대응 조치



결과 보고

불편 사항 대응 결과 이메일 또는 보고서 제공

장애 상황 등급 및 유형에 따른 대응 결과 보고서 제공

	제품 사용방법 안내, 유지보수
담당 부서	(주)시큐리온 기술지원팀
전화	070-4365-5938, 02-575-3339
팩스	02-575-3340
이메일	support@securion.co.kr
평시 운영 시간	10:00 ~ 17:00 (토 · 일 · 공휴일 휴무) *긴급 장애 상황 제외
홈페이지	www.securion.co.kr
무상 유지보수	도입 후 1년간 무상 유지보수 지원
유상 유지보수	도입 1년 이후 유상 유지보수 계약 시 지원

4. 적용 분야 및 사양

모바일·IoT 보안이 필요한 기관 및 기업, 앱 비즈니스 분야

폐쇄망 구축 시 자체 PMS(패턴 및 패치 관리 시스템) 구축 가능

기업/기관 모바일 엔드포인트 보안

기업 서비스에 해당 기능 추가
보안 가이드라인 준수



국방전산정보원

앱 비즈니스 보호

앱 동작 시 이용자 기기 보호
금융/핀테크 등 민감정보 이용 서비스 대상



타 보안 솔루션에 시큐리온 탐지 엔진 탑재

리브랜딩 시 제품명 및 로고 변경
맞춤형 솔루션 제작 / HW 탑재



사용환경 및 사양

구분	OnAV for Endpoint		OnAV for App	
	SDK Stand alone	SDK Cloud	SDK	App
Operating System	Android 4.1(16) +	Android 4.1(16) +	Android 4.1(16) +	Android 5.0(21) +
Service link type	Built in	Built in	Built in	App to App/Web to App
Providing module	AAR file, sample project	AAR file, sample project	AAR file, sample project	Agent sample project
Size	5MB 이내(AAR)	5MB 이내(AAR)	5MB 이내(AAR)	10MB 이내(APP)
Pattern size	7MB 이내	7MB 이내	7MB 이내	7MB 이내
Features	패턴+평판 검사 (Pattern+(ML)Rep) 빠르고 저렴	클라우드 기반 ML 검사 Real time AI 신변종 멀웨어 탐지 특화	Built in 통합 제품 리브랜딩에 적합	App to App 연동 고객사 앱 서비스 동작 시 실시간 보호

5. 인증 및 수상

글로벌 Top 3 인증 및 국내 GS 인증 획득

정보보호제품 성능평가 확인



인증	횟수	내역	비고
AV-TEST	36회	2018년 7/9/11월, 2019년 1/3/5/7/9/11월, 2020년 1/3/5/7/9/11월, 2021년 1/3/5/9/11월, 2022년 3/5/7/9/11월, 2023년 1/3/5/7/9/11월, 2024년 1/3/7/9월, 2025년 1월	연6회 평가 (매 홀수 달)
AV-Comparatives	6회	2019년-2024년	연1회 평가
MRG Effitas	2회	2019년 2분기, 3분기	
SKD Labs	1회	2019년	
PCSL	4회	2018년 3분기, 4분기, 2019년 1분기, 2분기	

정보보호제품 성능평가 확인서



시큐리온 ISO9001 품질경영시스템 인증



6. 특허

핵심기술 국내 IP 확보



리눅스 커널 무결성 검사 및
데이터 복구



현대 단말에서의 악성코드
진단 및 제거



취약점 탐지 아키텍처로 구성된
메모리 관리 기술



취약점 보완을 위한
바이너리 패치 장치



머신러닝 이용 이상거래
탐지 장치 및 그 방법



유사도 기반 악성 어플리케이션
탐지 방법 및 장치



위험도 기반 악성 어플리케이션
탐지 방법 및 장치



악성 어플리케이션
탐지 방법 및 그 장치

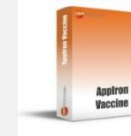
7. 레퍼런스

대표 사례



SK실더스 '모바일가드'

- SKT 개인용 AV 'T가드' 리브랜딩
- 다운로드 수 1,424만건, MAU 72만명
- 최신 공격 유형 반영 보안 기능 구현

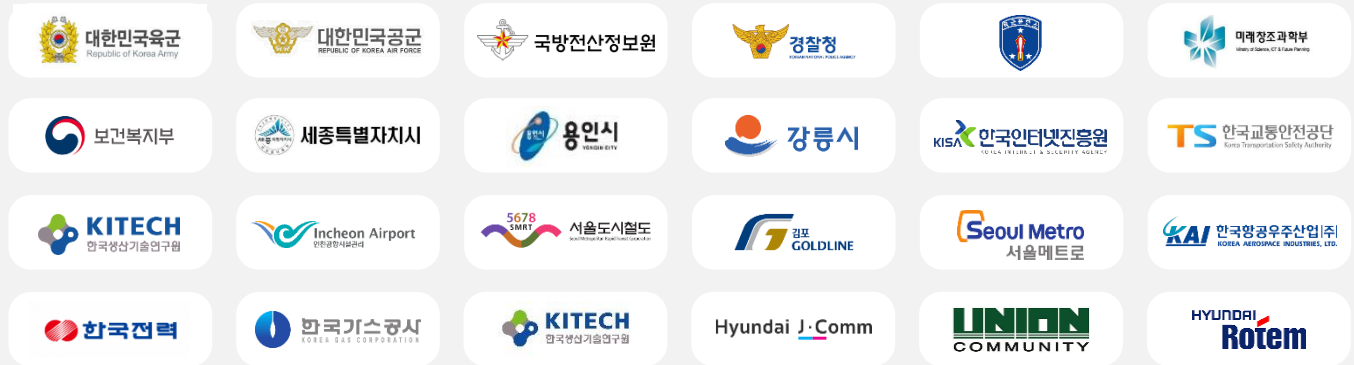


아이티센PNS '앱아이언'

- 고객사 수요 기반 기능 개발
- 기업 및 기관 앱 서비스 30여 개
- 유연한 이슈대응과 안정적 서비스지원

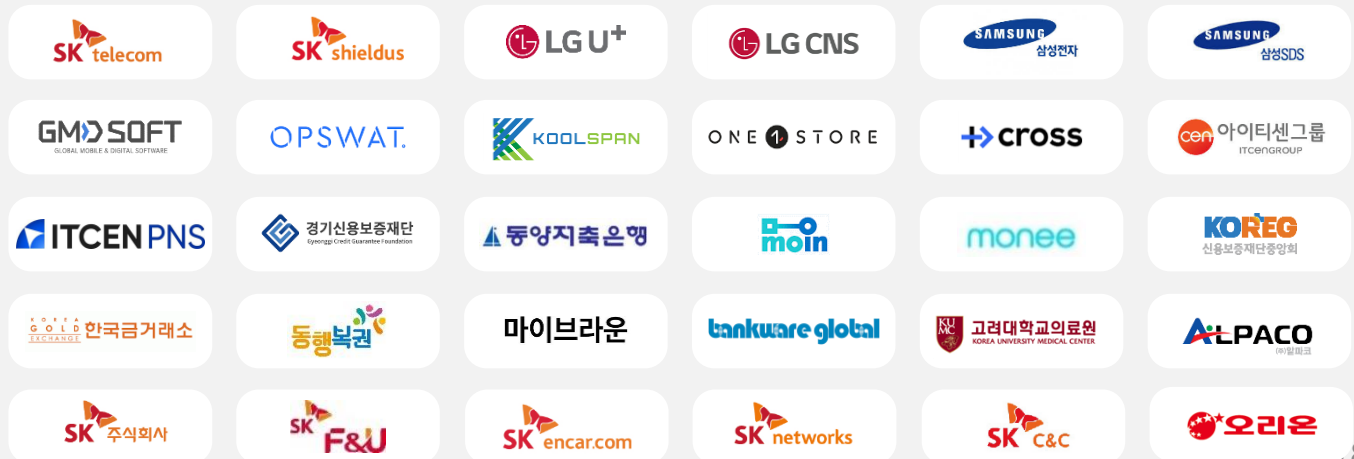
공공 보안

- 1 주요 시설 폐쇄망
- 2 스마트시티
- 3 스미싱 대응



민간 보안

- 1 엔드포인트보안
- 2 앱 서비스 보안
- 3 이용자 단말 보안



Thank you

문의 pr@securion.co.kr