

# AhnLab V3 Mobile Enterprise

모바일 오피스 관리를 위한 보안 솔루션

표준제안서

More security,  
More freedom



AhnLab

# CONTENTS

---

AhnLab  
V3 Mobile Enterprise

- 01 제안 배경
- 02 AhnLab V3 Mobile Enterprise
- 03 안랩 모바일 위협 대응의 차별점

# 01 제안 배경

---

모바일 보안 위협(1/2) - 모바일 악성코드의 고도화

모바일 보안 위협(2/2) - 내제된 보안 위협

모바일 오피스 보안 위협(1/2) - 환경적 위협

모바일 오피스 보안 위협(2/2) - 주요 보안 위협 유형

모바일 오피스 보안 관리의 필요성 대두

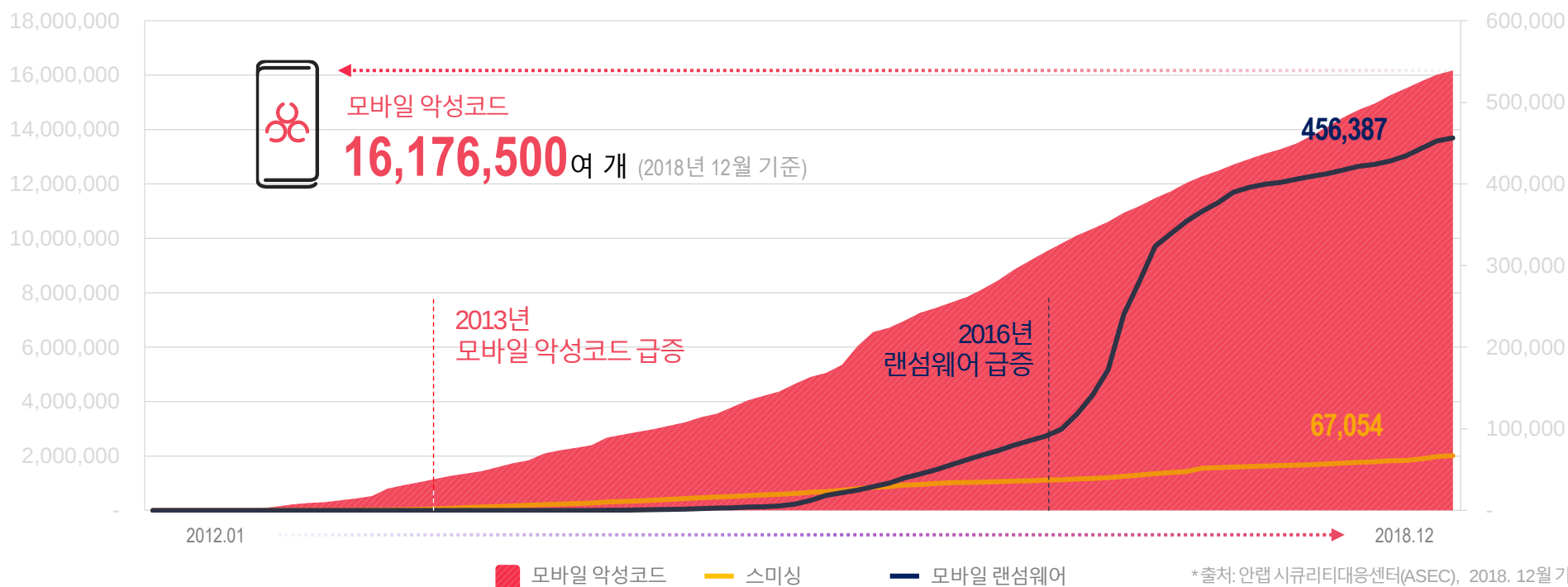
# 모바일 보안 위협(1/2) - 모바일 악성코드의 고도화

2013년부터 전 세계적으로 모바일 악성코드가 급격하게 증가하고 있으며,  
모바일 기기를 노린 랜섬웨어를 비롯해 스미싱 등 모바일 환경에 대한 위협이 고도화되고 있습니다.

모바일 악성코드  
**1,617만 여개**

스미싱 악성코드 **6만 7천여 개** 2012년 하반기부터 증가 추세  
모바일 랜섬웨어 **45만 6천여 개** 2016년 하반기부터 증가 추세

## 모바일 악성코드 증가 추이



# 모바일 보안 위협(2/2) - 내제된 보안 위협

01 제안 배경

가장 개인화된 시스템이자 끊임없이 연결되는 시스템이라는 모바일 기기의 특성은 모바일 시대의 발전 요인인 동시에 위협 요인입니다.

## 연결성

위협 유입·확산 경로로 악용 가능



### Seamless Connection

365일 x 24시간 네트워크 연결  
= 365일 x 24시간 위협 유입 가능

## 개방성

악의적인 애플리케이션 제작 및 유통 가능



### Openness

누구나 앱 제작 및 등록  
= 공격자 앱 제작 및 유포



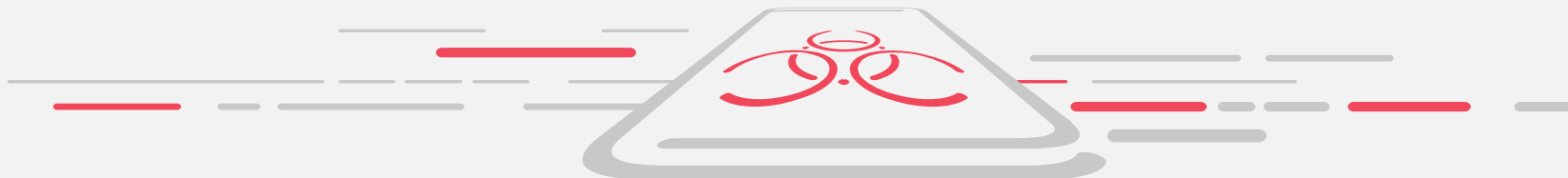
### Device & OS

다양한 모바일 기기와 파편화된  
운영체제 버전에 따른 취약점 관리 한계



### Privacy

가장 개인적인 시스템인  
모바일 기기에 대한 통제 한계



# 모바일 오피스 보안 위협(1/2) - 환경적 위협

업무 효율성 및 생산성 강화를 위해 언제 어디서나 모바일 기기를 이용해 업무를 처리할 수 있는 모바일 오피스(Mobile Office) 도입이 확대되고 있습니다.

## 모바일 오피스 구성 요소

모바일 기기, 애플리케이션, 무선 네트워크, 업무 관련 내부 시스템

## 모바일 오피스 위협 요소

비인가된 모바일 기기 접근, 애플리케이션 및 플랫폼 취약점, 무선 네트워크 보안 관리, 모바일 기기를 통한 악성코드 유입 등

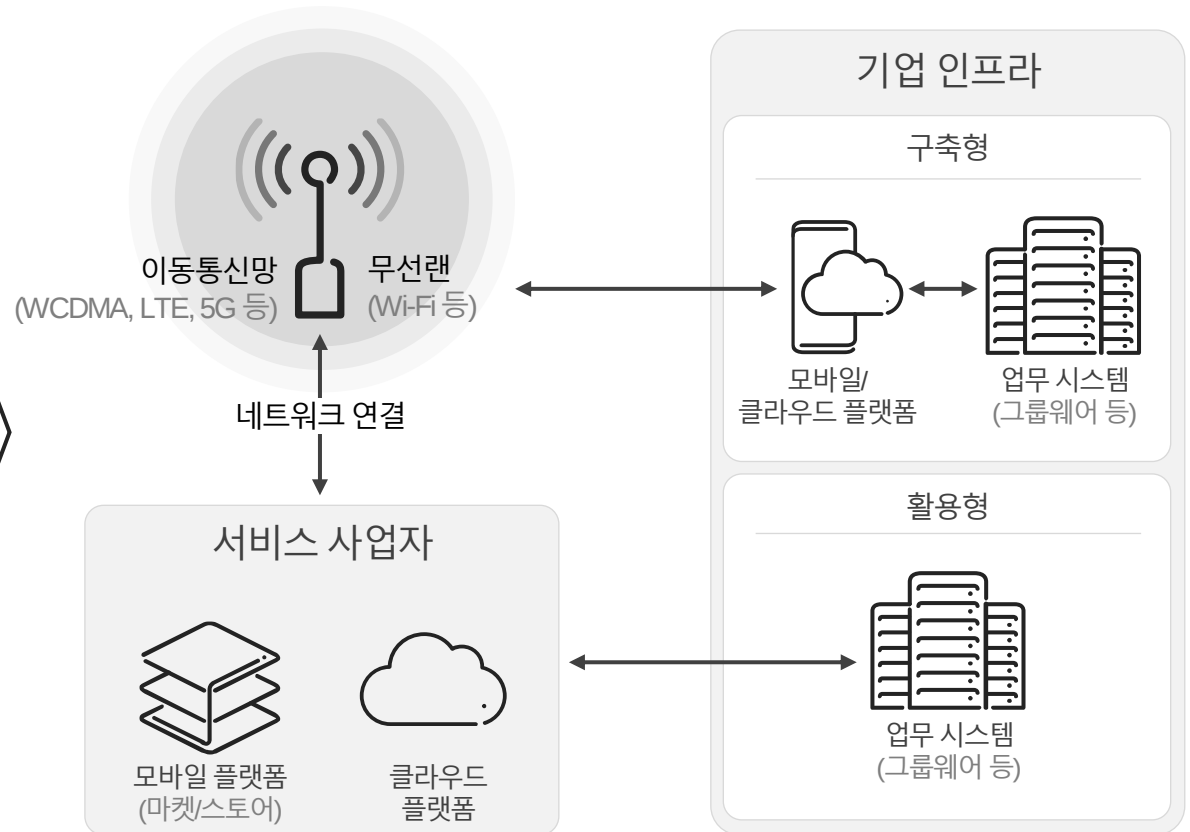
### 모바일 애플리케이션(Application)



### 모바일 기기(Device)



### 모바일 운영체제(Platform)



# 모바일 오피스 보안 위협(2/2) - 주요 보안 위협 유형

모바일 기기에 내제된 요인과 모바일 오피스의 환경적 요인으로 다양한 보안 위협이 발생할 수 있습니다.

| 모바일 보안 위협         | 상세 내용                                                                                                                                                                                                                                                        |
|-------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 개인정보 침해           | 위치정보 탈취를 통한 개인정보 침해<br>카메라, 마이크 등 기기의 하드웨어 자원을 이용한 개인정보 침해                                                                                                                                                                                                   |
| 도·감청              | 네트워크로 전송되는 데이터 패킷 도청<br>mVoIP 사용 시 음성 및 영상 통화 도청                                                                                                                                                                                                             |
| 피싱 및 파밍           | 악의적인 사이트를 이용한 사용자 정보 입력 유도<br>문자 메시지, 이메일 등을 이용하여 악성 애플리케이션 설치 유도                                                                                                                                                                                            |
| 서비스 거부 (DoS/DDoS) | 지속적인 통화 연결 및 데이터 전송요청 등을 통한 배터리 소진 및 기기 서비스 거부 공격<br>зом비 PC, зом비 모바일 기기 등을 이용한 내부 서버 대상의 서비스 거부 공격                                                                                                                                                         |
| 권한 탈취             | 기기-내부시스템 간 중간자(Main-in-the-Middle) 공격을 통한 사용자 권한 획득<br>SQL Injection 공격을 통한 인증 우회<br>기기 루팅, 탈옥을 통해 관리자(Root) 권한 탈취<br>버퍼 오버플로우 공격을 통한 관리자 권한 탈취<br>기기와 내부 시스템 간에 맺어진 세션 탈취                                                                                   |
| 모바일 악성코드·해킹       | 악의적인 스크립트 실행으로 공격자가 악성코드를 삽입한 웹사이트 접속<br>주요 정보가 포함된 문서 및 자료 암호화를 통한 데이터 파괴 (랜섬웨어)<br>불필요한 서비스(포트) 사용 취약점<br>모바일 애플리케이션 소스코드 분석(리버스 엔지니어링)을 통한 취약점 분석<br>기기에서 제공하는 테더링 기능을 사용하여 서버 보안 정책 우회 및 공격 경로로 활용<br>기기를 USB 이동 저장매체로 사용하여 악성코드 전파                      |
| 정보 유출             | 내부자에 의한 기업 내부 정보자산 유출<br>기기 분실, 도난, 양도, 공공장소 사용에 따른 내부정보 유출<br>기기 녹음, 녹화, 화면 캡처, 메모 기능을 통한 생성·저장된 정보 유출<br>비인가 AP를 통한 정보 유출<br>키로거(Key Logger) 감염에 의한 사용자 입력정보 탈취<br>블루투스 및 Wi-Fi Direct 취약점을 이용한 정보유출<br>비인가 애플리케이션 설치에 따른 정보유출<br>비인가자의 정보 획득 및 업무처리 기능 접근 |

모바일 기기 사용 증가 및 모바일 오피스 확대에 따른 기업의 보안 위협을 최소화하기 위해서는 모바일 기기 자체에 대한 보안 관리가 확보되어야 합니다.

## 모바일 오피스 효과

### 생산성 증대

- 현장 중심 업무 수행
- 연속적인 커뮤니케이션
- 정보 접근성 확보
- 즉각적인 대응성 확보

### 업무 시공간 확장

- 시간 비용 절감
- 물리적 장소 제약 해소
- 디바이스 제약 극복

## 모바일 기기 중심의 보안 관리 방안 필요

- 외장 메모리, USB 연결, 카메라 등의 하드웨어 모듈
- 5G, LTE, Wi-Fi, Bluetooth, 테더링(tethering) 등 네트워크 연결
- 사용자가 설치·사용하는 각종 애플리케이션 관리



## 보안 위협 요소

### 기기 위협

- 분실/도난
- 저장 정보 유출

### 네트워크 위협

- 비인가된 접근
- 도청 및 감청

### 플랫폼 위협

- Admin 권한 상승
- 알려진 취약점 공격

### 애플리케이션 위협

- 미검증 애플리케이션 설치
- 악성 애플리케이션 설치

# 02

## AhnLab V3 Mobile Enterprise

---

V3 Mobile Enterprise 개요

특장점 및 도입 효과

주요 기능 및 사용 환경

솔루션 제공 방식

V3 Mobile Enterprise는 기업의 모바일 환경 요구 사항에 최적화된 모바일 오피스 전용 보안 프로그램입니다.

## AhnLab V3 Mobile Enterprise

### 강력한 모바일 위협 대응

- 모바일 악성코드 DB 및 대응 기술 노하우
- 모바일 위협 요소에 최적화된 기능 제공

### 모바일 오피스 최적화

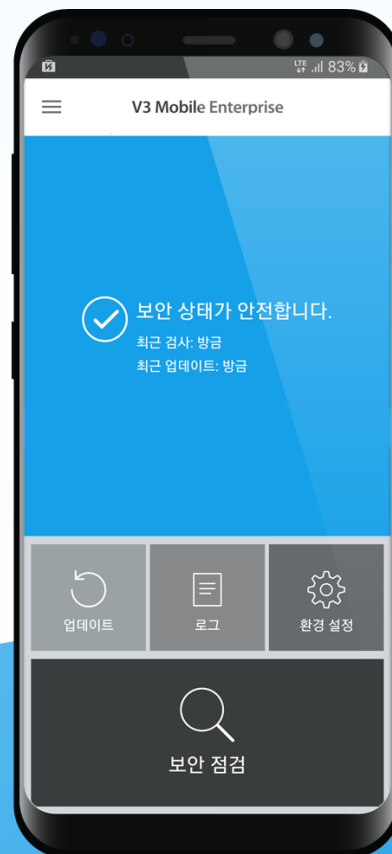
- 기업의 보안 요구 및 모바일 오피스 환경을 다각도로 분석 및 반영

### Global No. 1

- 세계적으로 인정받는 모바일 안티멀웨어 성능

### 효율적인 보안 관리

- 라이선스 적용 단말기 및 MDM 에이전트 연동으로 손쉬운 도입 및 즉각적인 운영
- 보안 사고 발생 시 신속하게 대응 및 조치 가능



# 특장점 및 도입 효과

V3 Mobile Enterprise는 강력한 보안과 구축 편의성을 제공해 기업의 안전한 모바일 오피스 환경 구축에 기여합니다.



## 강력한 모바일 보안

- 세계 최고 수준의 안티멀웨어(Anti-Malware) 엔진 적용
- Root Checker를 통한 Android Platform 변조 여부 탐지
- 최신 엔진 업데이트 및 검사 제어 등 관리자 명령 및 조치 지원
- 20년간 축적된 안랩의 모바일 보안 기술 및 위협 대응 노하우



## 편리한 구축 및 도입

- APK 형태의 설치 방식을 통한 간편한 구축
- 고객사 MDM 솔루션 에이전트에 손쉽게 연동 가능
- 모바일 오피스 시스템 구성 시, 기기 보안 대책 연동 가능
- 기기 보안에 필요한 정책 설정 및 기능에 따라 설계 가능한 유연한 구조



## 비즈니스 효율성 향상

- 쉽고 간편한 디바이스 보안 관리·제어를 통한 보안 업무 부담 해소(\*MDM 연동 시)
- 안전한 모바일 오피스 환경 구축으로 전반적인 비즈니스 효율성 향상



## 체계적인 위협 대응

- 안랩 시큐리티대응센터(ASEC)의 24/7 실시간 보안 위협 모니터링 및 이슈 대응
- 20년간 축적된 모바일 악성코드 대응 노하우 및 전담 조직 운영
- 애플리케이션(App) 수집·분석을 통한 악성코드 대응 체계

## 주요 기능

| 구분                            | 기능          | 내용                                                               |
|-------------------------------|-------------|------------------------------------------------------------------|
| 모바일 악성코드 대응<br>(Anti-Malware) | 기기 검사       | 수동 및 원격 명령으로 빠른/정밀 검사 가능                                         |
|                               | 실시간 검사      | 보안 수준 설정 제어 가능                                                   |
|                               | 외장 메모리      | 설정 시 포함 검사                                                       |
|                               |             | 예약 시간 설정을 통한 예약 검사 제어 가능                                         |
|                               | 엔진 업데이트     | 원격 업데이트, 관리자 설정에 의한 예약 업데이트, 사용자에게 의한 업데이트 지원                    |
| Root Checker                  | 기기 루팅 여부 체크 | 루팅 탐지 기능 탑재                                                      |
| 로그 관리                         | 검사 및 이벤트 로그 | 악성코드 검사 및 이벤트 결과 로그 확인 가능                                        |
| 제품 인증                         | 라이선스 체크     | 라이선스를 통한 제품 활성화 및 인증 유지                                          |
| MDM 연동                        | 인터페이스       | 에이전트(Agent) 연동을 통한 MDM 서버 연동<br>(*Agent와 MDM 서버 페이지는 고객사가 별도 구축) |
|                               | 프로파일        | 에이전트로부터 수신한 MDM 프로파일 및 설정 정책을 통해 제품 기능 설정 제어 가능                  |

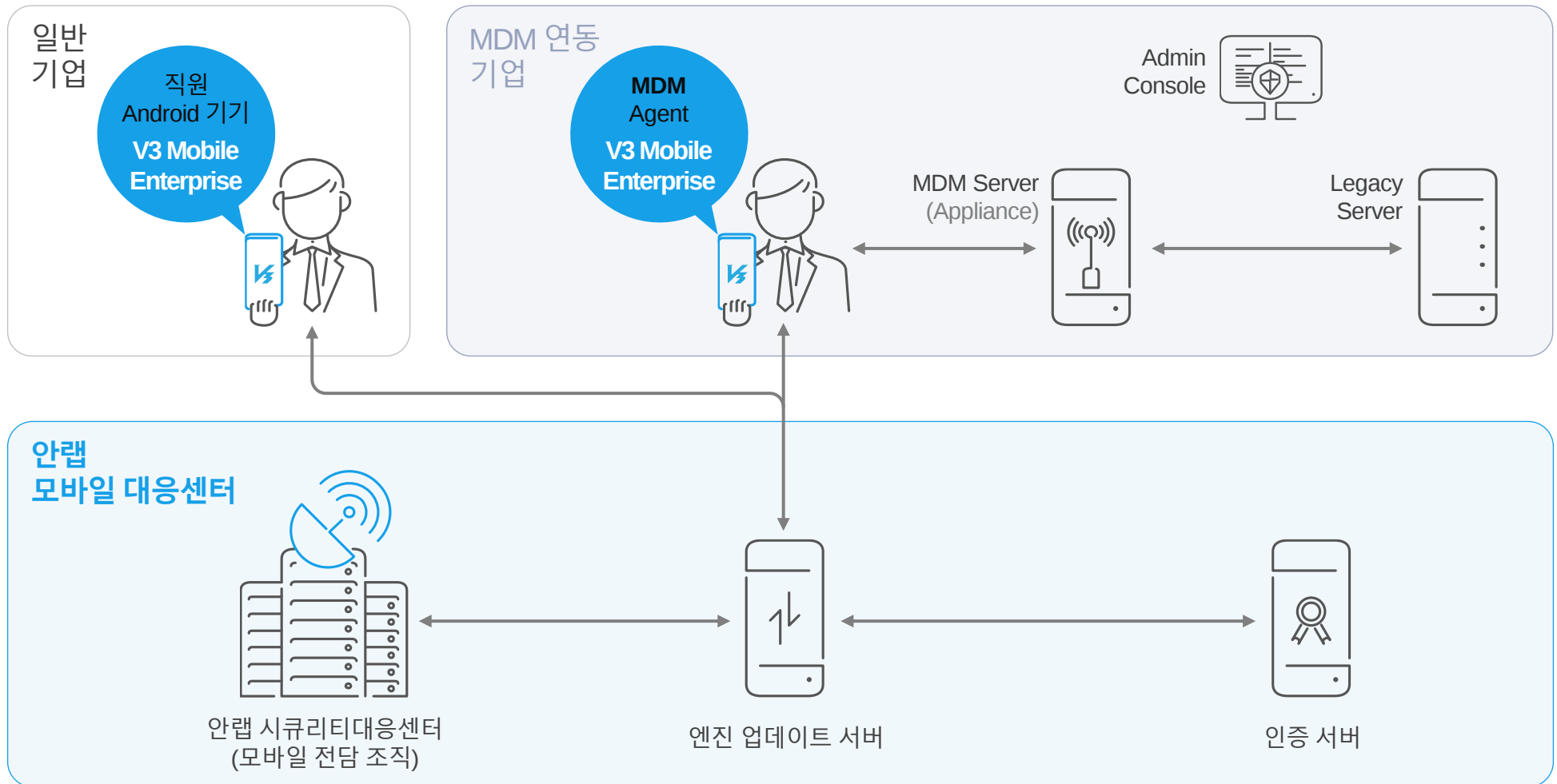
## 사용 환경

| 구분        | 시스템 요구사항               |
|-----------|------------------------|
| 운영체제(플랫폼) | Android version 4.4 이상 |
| 지원 디바이스   | 안드로이드 기반 정품 디바이스       |
| MDM 연동    | MDM Agent 연동 필요        |

# 솔루션 제공 방식

02 AhnLab V3 Mobile Enterprise

V3 Mobile Enterprise는 .apk 형태로 제공되어 기업 내 임직원 단말기에 쉽게 적용할 수 있으며, 고객사에서 사용 중인 MDM과 연동을 통해 쉽게 구축할 수 있습니다.



# 03

## 안랩 모바일 위협 대응의 차별점

---

세계 최고의 모바일 악성코드 대응력

안랩 악성코드 대응 프로세스

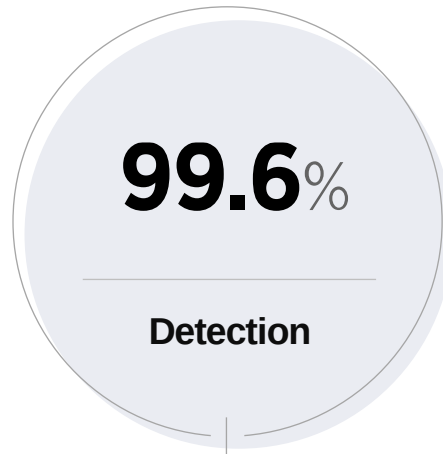
# 세계 최고의 모바일 악성코드 대응력

안랩의 모바일 안티멀웨어 엔진(V3 Mobile Security)은 세계 최고 수준의 모바일 악성코드 대응 역량을 인정받고 있습니다.

글로벌 보안 제품 평가 기관 AV-TEST의 모바일 부문 평가에서  
**전회 인증 획득, 평균 진단율 99% 기록**



2013년 1월부터 부터  
2019년 1월 현재까지 진행된  
총 37회 테스트 전회 통과



실시간 악성코드  
진단율  
평균 99.6%



악성코드 진단율을 포함한  
보안 성능  
평균 5.8점 (6.0 만점)



배터리 등 시스템 자원 소모 및  
메모리 사용률 등 사용성  
평균 5.8점 (6.0 만점)

최근 1년 평균 (2018년 1월~2019년 1월)

## ※ AV-TEST란?

AV-TEST(<http://www.av-test.org>)는 전 세계 주요 보안 제품을 평가하여 인증을 부여하는 기관입니다.

AV-TEST의 모바일 부문은 최신 악성코드 탐지 성능을 평가하는 진단율(Protection) 외에도 사용성(Usability), 부가 기능(Features) 등을 기준으로 평가하며, 안랩의 V3 Mobile Security는 전 세계 주요 모바일 보안 솔루션 10개 중 최상위권 성적을 유지하고 있습니다.

# 안랩 악성코드 대응 프로세스

악성코드 분석 전문가로 구성된 안랩 시큐리티대응센터(ASEC)의 4단계 위협 대응 프로세스를 기반으로 악성코드 및 침해 시도(해킹)에 강력하게 대응합니다.



AhnLab Security Emergency response Center

1단계 접수



2단계 분석



3단계 1차 대응



4단계 2차 대응

신·변종 바이러스,  
해킹 사고 접수

바이러스.  
해킹 툴 수집

상황 분석

1. 국내·외 피해 조사, 예측
2. 프로그램 용도
3. 바이러스·해킹 발생 시점 및 행동 분석

샘플 분석

1. 샘플 입수·분석
2. 분석 리포트 제출
3. 대응 방식 결정
4. 대응 일정 확정

엔진 대응

1. 바이러스·해킹 툴 대응 엔진 제작
2. 엔진 업데이트

추가 공격 대응 준비

1. 변종 바이러스·해킹 툴 모니터링
2. 고객 응대 확대

모듈 변경

1. 변종 바이러스 엔진 추가 등록
2. 해킹 툴 방지 모듈 개발
3. 제품 업데이트

※ ASEC(AhnLab Security Emergency response Center)

안랩에서 운영하는 비상 대응 조직으로, 바이러스 및 보안 위협의 24시간 감시, 신속한 대응 및 지속적인 연구를 수행하여 고객사의 중요 정보 자산 및 비즈니스 연속성을 보호하여 고객사의 대외 신뢰도 강화에 기여합니다.

---

㈜안랩

경기도 성남시 분당구 판교역로 220 (우) 13493

대표전화: 031-722-8000 | 구매문의: 1588-3096 | 전용 상담전화: 1577-9431 | 팩스: 031-722-8901 | [www.ahnlab.com](http://www.ahnlab.com)

© AhnLab, Inc. All rights reserved.

More security,  
More freedom

## AhnLab V3 Mobile Enterprise

AhnLab