

AhnLab V3 Internet Security 9.0

More security,
More freedom

진단율, 속도, 사전 방역까지 '차원'이 다르다!

표준제안서



AhnLab

Contents

AhnLab
V3 Internet Security 9.0

- 01 제안 배경
- 02 제품 개요
- 03 도입 효과
- 04 주요 기술
- 05 주요 기능
- 06 지원 OS 확대(Mac OS)
- ※ 별첨

01. 제안 배경

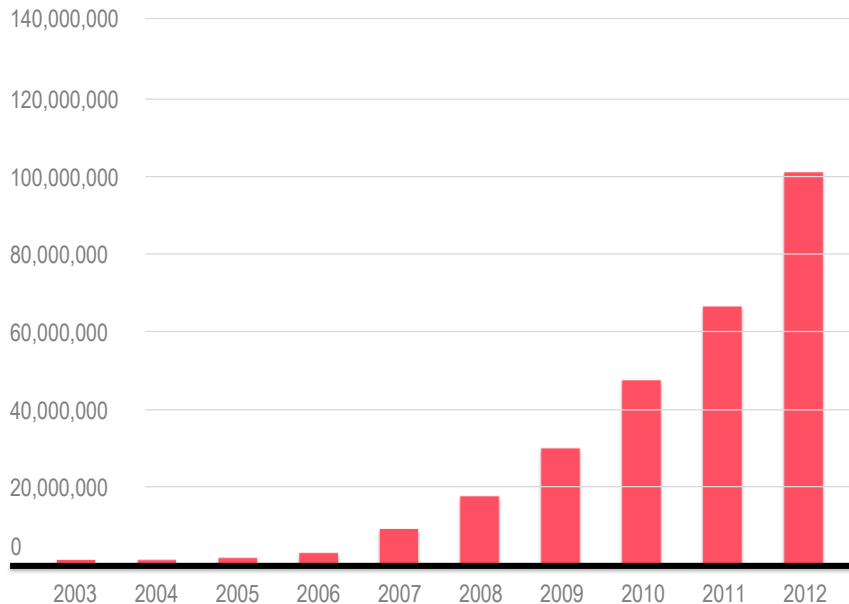
-
1. 악성코드의 급격한 증가
 2. 고도화하고 있는 악성코드
 3. 악성코드 웹 유포도 급증
 4. 국내 기업의 악성코드 피해 현황
 5. 새로운 대응 방안 필요성 대두

1. 악성코드의 급격한 증가

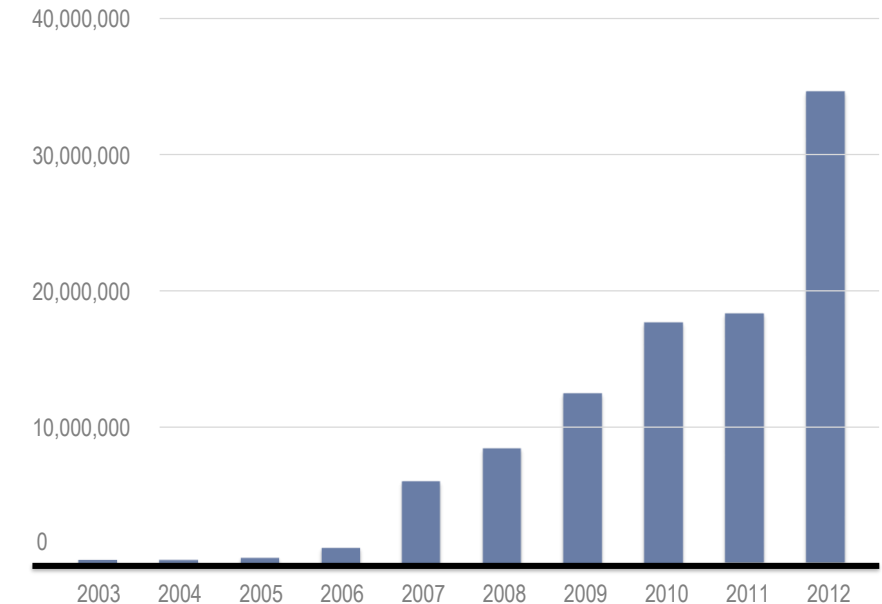
해마다 악성코드의 수는 기하급수적으로 늘고 있습니다. 한 기관에 따르면 매일 20만여 개의 악성코드가 새롭게 발견되고 있습니다. 그만큼 분석 및 대응해야 하는 악성코드의 수가 급격히 늘고 있는 셈입니다.

- 기업의 IT 환경이 발전함에 따라 편의성이 증대됨과 동시에 보안 위협도 높아져
- 최근 금전 탈취 목적의 공격이 늘어나고 있으며 악의적 공격도 전문화·상업화되는 추세
- 인터넷 등을 통해 악성코드 제작법이 유포, 일반인도 쉽게 악성코드를 만들 수 있어 악성코드는 더 폭증할 것으로 예상

Total Malware



New Malware



2003~2012년 멀웨어 증가 추이 (AV-TEST 자료 참조)

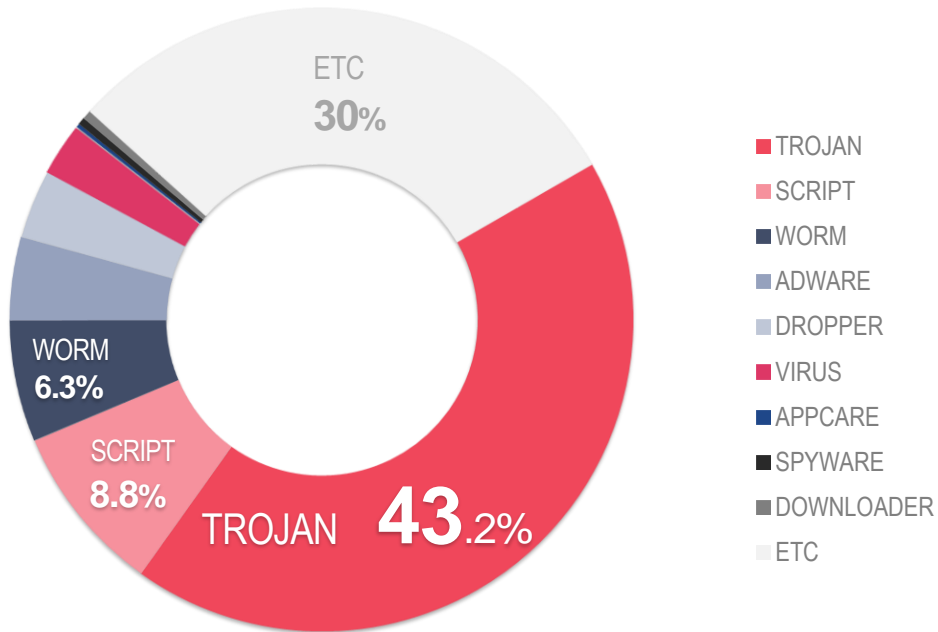
2. 고도화하고 있는 악성코드

특히 2012년에는 악성코드 중 ‘트로이목마(Trojan)’가 43.2%를 차지, 최다를 기록했으며 주로 잠복/은폐한 형태로 유입돼 계정 정보를 유출하거나, 디도스 공격과 같이 타깃 공격에 사용됐습니다.

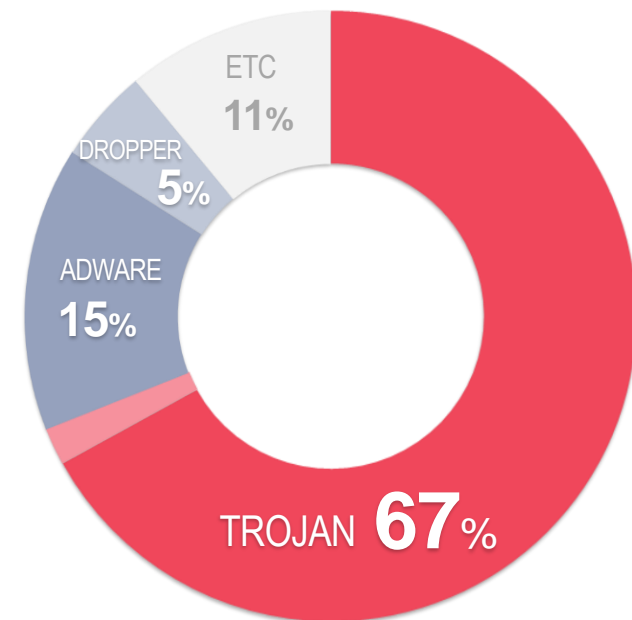
주요 악성코드 유형

1. 악성코드 다단계 공격, 과다 트래픽 발생 악성코드
2. 온라인 뱅킹 트로이목마인 Banki, 패스워드를 노리는 악성코드, 온라인게임핵 변종 악성코드
3. Xerox WorkCenter를 사칭한 악성 메일, Facebook을 사칭한 악성 메일

2012년 악성코드 감염유형



2012년 신규 악성코드 분포



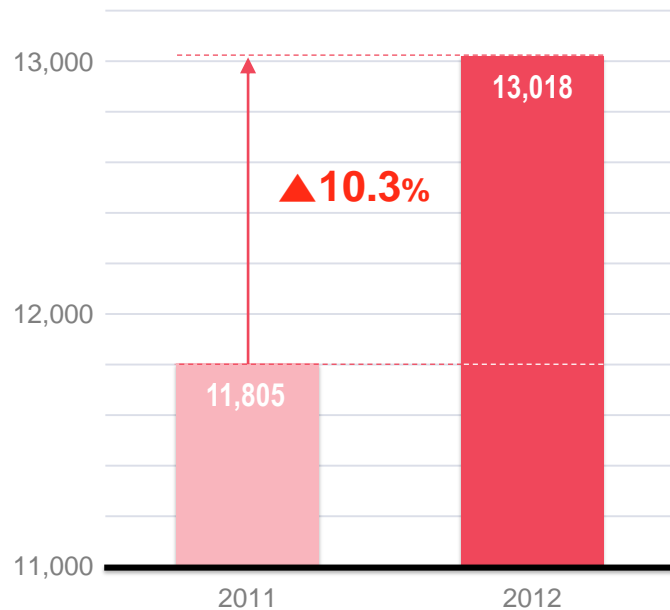
Source : AhnLab ASEC Report

3. 악성코드 웹 유포도 급증

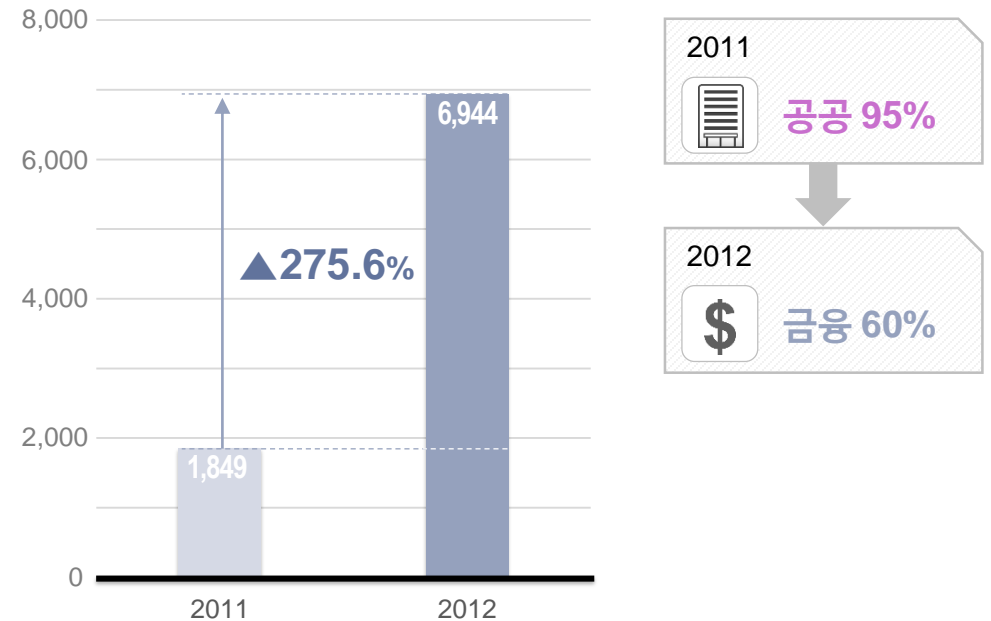
2012년 피싱 사이트는 2011년 대비 275.6%나 증가했고 악성코드 은닉 사이트도 전년 대비 10.3%가 증가했습니다. 무엇보다 피싱/파밍 사이트로 인한 금융 피해 급증하는 양상입니다.

- 웹 사이트를 통해 유포된 악성코드는 온라인게임핵, 백도어, Banki 등 다수
- 악성코드 제작자의 물량 공세, 2012년 웹을 통해 배포된 악성코드 수만 24만여 건

악성코드 은닉 사이트



피싱 사이트

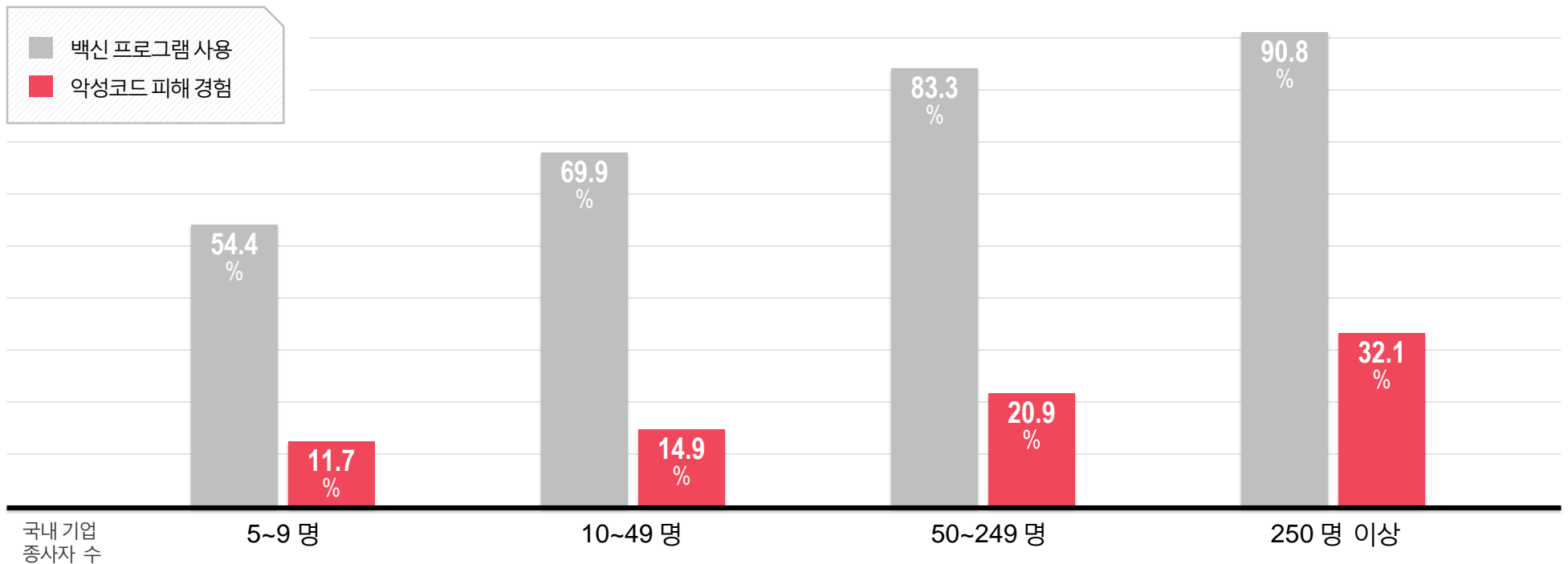


Source : Internet & Security Focus 2013, KISA

4. 국내 기업 악성코드 피해 현황

국내 기업 중 80% 이상은 백신(안티바이러스) 프로그램을 사용한 바 있으나 악성코드 피해 경험이 일부 발생한 것으로 나타났습니다. 이는 기존 시그니처 기반의 백신으로는 신속한 진단 및 치료가 어려운 신·변종 악성코드가 급격히 늘어나고 있음을 의미하는 동시에, 백신조차 사용하지 않는 기업의 피해는 더 클 것임을 짐작하게 합니다.

- 악성코드(바이러스, 웜, 트로이목마 등) 공격으로 인한 기업 피해 2011년 10만 8천여 사업체
- 이 중 피해로 인해 복구 비용이 발생한 비율은 41.8%에 육박(출처: 2012 정보화통계집)



Source : 정보화통계집, NIA

새로운 대응 방안 필요성 대두



사전 방역까지 가능한 V3 Internet Security 9.0

다차원 분석 플랫폼 기반의
사전 방역 효과 제공

평판·행위 기반 분석을 통해
미탐·오탐 최소화

위협의 인지부터 분석, 대응,
리포팅까지
단일 시스템에서 실시간
통합 대응

독보적인 초경량 엔진과
성능으로
사용자 편의성 극대화

- 분석 시간 및 누락 샘플 증가
- 엔진 크기 증가

- 탐지/대응의 어려움
- 사전 관리 부재

- 위협 분석 및
사전 방어 어려움



악성코드 수 폭증



은폐, 제로데이 고도화



타깃 공격/APT

02. 제품 개요

-
1. V3 Internet Security 9.0 소개
 2. 특징점

V3 Internet Security 9.0 소개

기업용 통합 PC 보안 솔루션 V3 Internet Security 9.0은 새로운 진단 기술인 다차원 분석 플랫폼 적용으로 다양한 보안 위협으로부터 기업의 클라이언트 PC를 안전하게 보호하며 사전 방역 기능을 제공해 안전한 컴퓨팅 환경 구축에 기여합니다.

AhnLab V3 Internet Security 9.0

진단을, 속도, 사전 방역까지 '차원'이 다르다!



다차원 분석 플랫폼 기반의 탁월한 진단율

- 다차원 분석 플랫폼 기반의 행위 기반 평판 기반 분석 수행
- 신/변종 악성코드까지 사전에 진단하는 사전 방역기능 제공

스마트 스캔 기술로 신속·정확한 검사

- 최초 1회 검사로 안정성 확보한 파일을 제외하고 검사하는 스마트스캔(Smart Scan) 기술 적용
- 최대 6배 이상 빨라진 속도로 사용자 편의성 극대화

초경량 엔진으로 PC 메모리 사용량 최소화

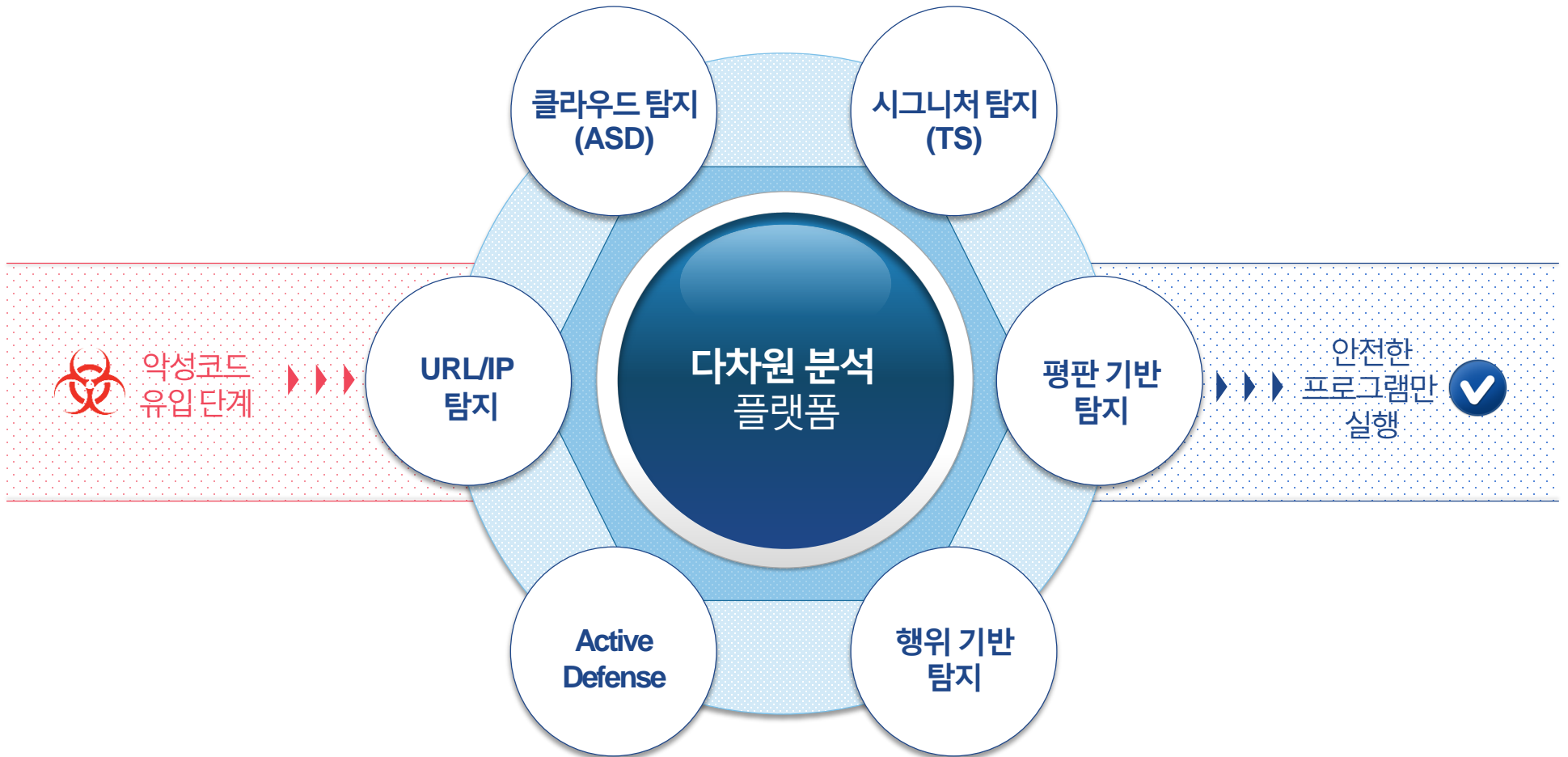
- 안랩의 20여 년 기술 노하우가 응축된 TS Prime 엔진과 클라우드 기반 ASD 엔진 탑재
- 엔진 최적화 기술로 PC 메모리 사용 최소화

쉬운 컬러, 메인 화면에서 문제 한번에 해결

- 선명하고 이해하기 쉬운 컬러로 PC의 보안 상태를 확인
- PC 검사 및 최적화 등 핵심 기능을 메인 화면에서 간단히 이용 가능

특장점

V3 Internet Security 9.0에 적용된 다차원 분석 플랫폼은 6가지 핵심 탐지 기술이 있어 빠르고 정확한 악성코드 분석은 물론 아직 알려지지 않은(0-day) 신·변종 악성코드까지 진단합니다.



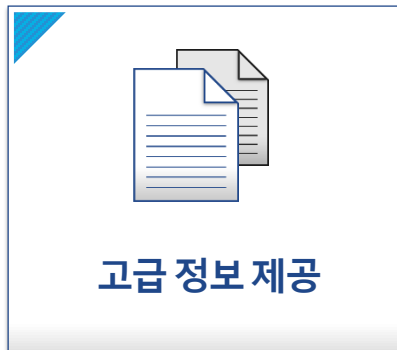
특장점



- 다차원 분석 플랫폼 적용
- ASD(AhnLab Smart Defense) 평판 검사
 - ASD 서버의 평판 정보를 이용해 수동 검사 시 평판이 낮은 파일 진단
- 평판 기반의 프로그램 실행 차단
 - 프로그램의 평판 정보를 통해 안정성이 검증되지 않은 프로그램의 실행 차단
 - 평판 탐지의 예 *발견된 지 20일 이내의 파일로, 전체 사용자 수가 500명 이하일 정도로 극소수가 사용하는 프로그램
*100여 가지의 의심 행위에 대한 탐지



- TS Prime 엔진 적용
 - 엔진 다운로드 사이즈 약 50MB 수준
 - DNA 스캔(Scan)을 통한 리소스 점유율 개선



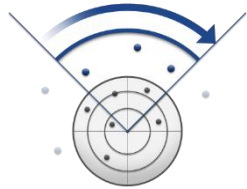
- 파일 분석 보고서
 - 사용자 PC에 생성된 또는 존재하는 파일에 대한 다양한 분석 정보 제공
 - 파일 생성 정보, 기본 정보, 활동 정보, 행위 정보, 평판 정보 등
- 웹사이트 분석 보고서
 - 사용자가 접속한 URL에 대해 ASD 서버의 정보를 이용해 URL에 대한 다양한 분석 정보 제공

특장점



Active Defense

- 시스템에 대한 전반적인 정보 제공 및 이를 통한 룰 정책 생성
 - PC의 프로그램 활동 내역, 클라우드 분석 정보, 평판 정보를 제공
 - 해당 정보를 통해 기업 내 PC의 프로그램 활동 분석 및 차단 룰 정책 적용



진단 영역 확대

- 악성 URL/IP 차단(SiteGuard 대체)
 - 악성코드 유포 URL 접근 차단
 - C&C 등 악성 IP로의 네트워크 접속 차단
- PUS(PUP 유포 등 불필요한 사이트) 접속 차단
- 네트워크의 행위 기반 침입 탐지
 - 기존 시그니처 기반 침입 탐지에 추가
 - 스푸핑이나 이상/과다 트래픽 등 네트워크의 특정 의심 행위를 바탕으로 침입 탐지 및 차단



검사 속도 증가 (수동 검사)

- 스마트 검사 기술 적용
 - 새로운 파일, 변화된 파일만 검사해 검사 시간과 자원 점유를 단축하는 기술 적용 (수동 검사)
 - 최초 1회 검사는 비슷하나, 이후 6배 정도의 빠른 속도로 검사가 가능

03. 도입 효과

-
1. V3 Internet Security 9.0 도입 효과
 2. 입체적 대응 서비스
 3. 전문 고객 지원 프로세스
 4. 통합 보안 시스템 구축

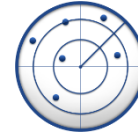
V3 Internet Security 9.0 도입 효과(1)



다차원 분석 플랫폼
적용을 통한 사전 방역



사후 대응 관점의
기존 방식 한계를 극복



Active Defense 적용으로
능동적 보안 가능



다양한 분석 정보를
통한 가시성 확보

행위

탐지를 우회하는 고도화된 악성코드 및
0-day 취약점 대응에 효과적

평판

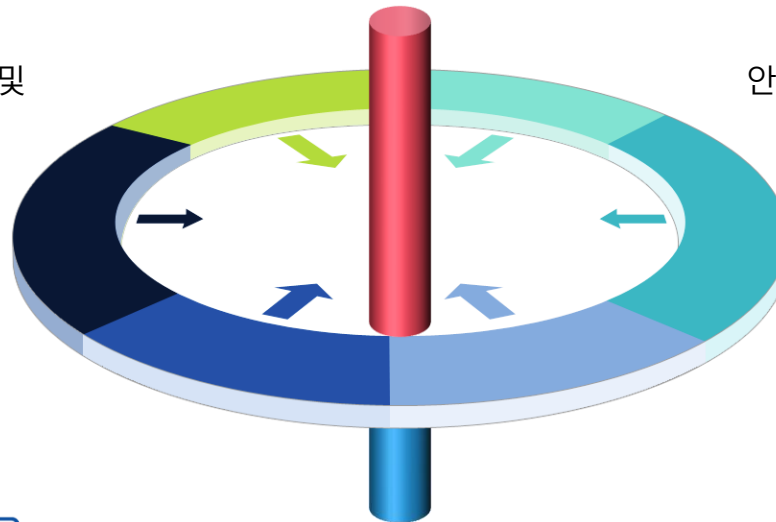
안전 여부가 확인되지 않은 '미진단' 파일 및
프로그램에 대한 잠재적인 위험을
사전 차단

Active Defense

시스템 내부 위협에 대한
가시성 제공

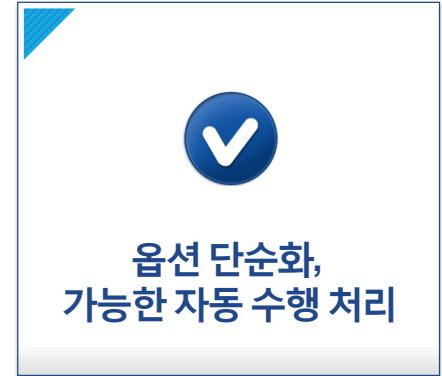
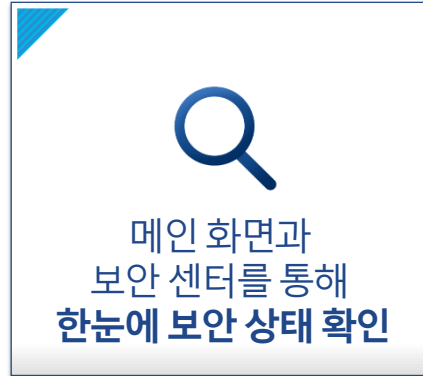
URL/IP

악성 웹사이트/IP 접속을
사전 차단



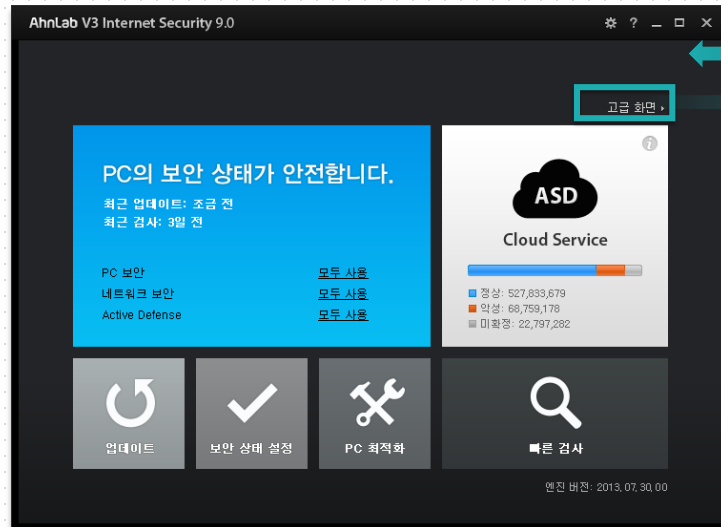
아직 알려지지 않은 위협을 사전에 대응함으로써
기업의 비즈니스 연속성에 기여합니다.

V3 Internet Security 9.0 도입 효과(2)



메인 화면

빠른 검사와 PC최적화 등 일반 사용자 중심의 간편한 구성



보안 센터

PC상태에 대한 상세한 내용 확인 및 세부적인 옵션 설정



사용자가 원하는 모드로 설정
편의성 극대화

V3 Internet Security 9.0 도입 효과(3)



**컬러 변화만으로
직관적인 PC 상태 확인**



**메인 UI 에서
프로세스 진행
(검사/최적화등)**



**메뉴 Depth 최소화,
직관적인 인터페이스**

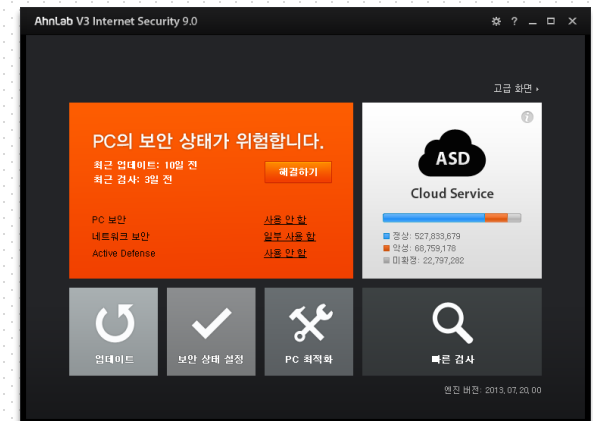
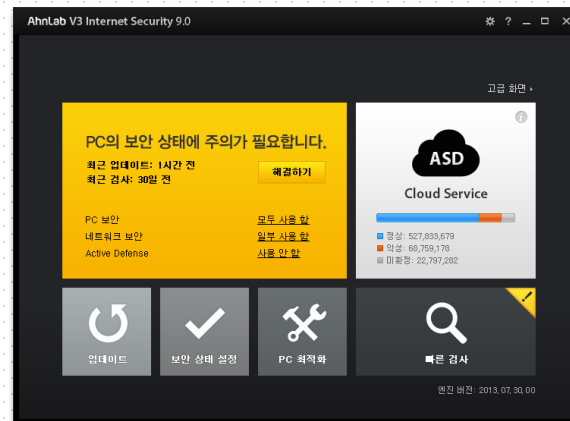
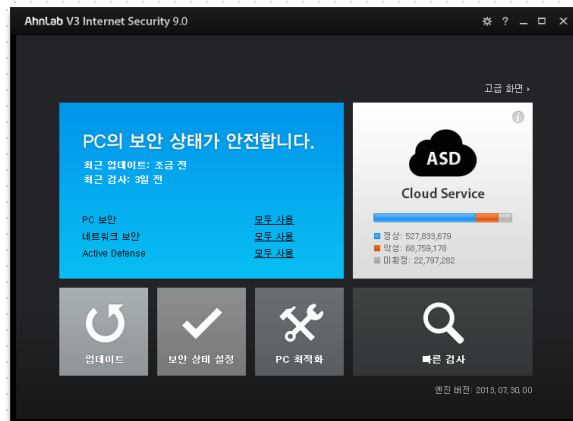


**해결하기 버튼을 통해
원클릭 해결이 가능
(주의/위험으로 나타날 경우)**

안전

주의

위험



- 안전/주의/위험의 색상이 보안 센터에도 연동되어 있어 길잡이(보안 내비게이션) 역할을 합니다.
- 보안 상태가 주의/위험으로 나타날 경우 해결하기 버튼을 통해 원클릭 해결이 가능합니다.

입체적인 대응 서비스

- 안랩의 차별화된 전문 지원 서비스
- 24시간, 365일 깨어 있는 ASEC 대응센터

AhnLab

오랜 기간 쌓아온 악성코드 분석 능력과 대응 경험을 통해
안전한 컴퓨팅 환경 조성 **함께** 기업 비즈니스 연속성에 기여합니다.

안랩은 20여 년간 악성코드를 분석하고 연구해온 전문 기업입니다.

안랩은 지난 1988년부터 악성코드와 바이러스 등에 대한 연구를 시작, 25년여 간 노하우를 축적해왔습니다.
국내 최대 규모의 샘플 DB를 보유하고 있으며 독자적인 기술을 마련해놓고 있습니다.

안랩은 다양한 분야의 기업 고객에게 위협 대응 방안을 제공하고 있습니다.

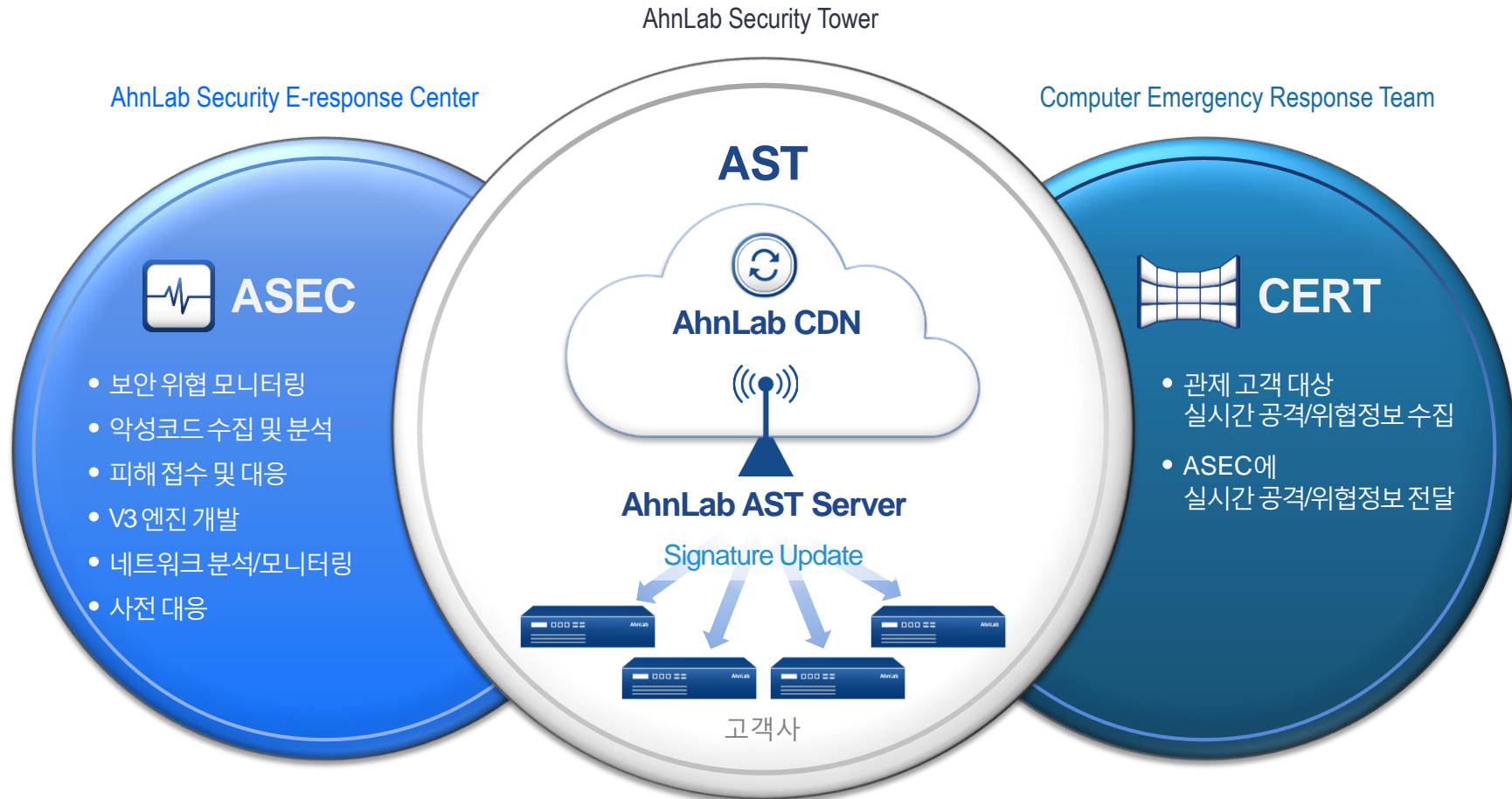
1995년 회사가 설립된 이후 다양한 레퍼런스를 통해 경험을 쌓았습니다.
다양한 기업 환경에서 발생하는 위협을 정확하게 진단해내고 있으며 적절한 대응 방안을 제시하고 있습니다.

안랩은 24시간, 365일 철저한 대응 체계를 가동 중입니다.

24시간 × 365일 ASEC 대응센터의 전문 인력이 위협을 모니터링하며 대응하고 있습니다.
일일 정기 업데이트 및 긴급 업데이트를 수행함으로써 발 빠르게 악성코드에 대처합니다.

전문 고객 지원 프로세스

보안에 대한 오랜 노하우와 경험을 토대로, 체계적이며 전문적인 지원 서비스 제공을 약속합니다.



통합 보안 시스템 구축

- 통합 보안 관리 솔루션인 APC, 네트워크 보안 제품인 TrusGuard 등과 연계 가능
- 간편하면서도 체계적으로 통합 보안 시스템을 구축

보안 정책 강제 적용

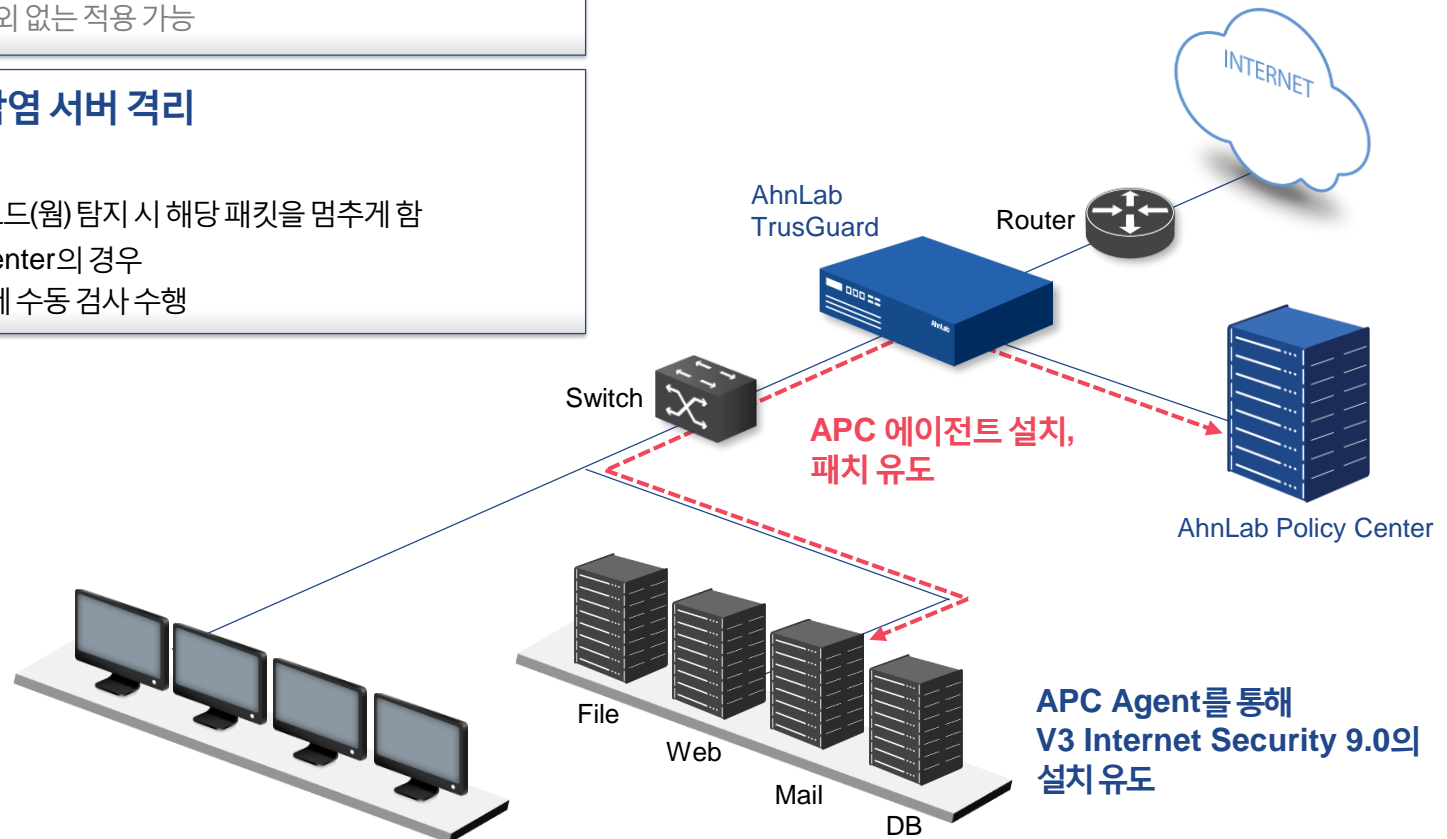
- APC 에이전트 미 설치 PC와 서버의 외부 인터넷 접근 차단
- 에이전트 설치 유도 화면으로 Redirection
- PC와 서버에 APC 에이전트 설치를 유도
- 보안 정책의 전사 예외 없는 적용 가능

악성코드(웜) 감염 서버 격리

- TrusGuard의 경우
- 내부 발송된 악성코드(웜) 탐지 시 해당 패킷을 멈추게 함
- AhnLab Policy Center의 경우
- V3 IS 9.0에서 강제 수동 검사 수행

API 제공을 통한 관리 솔루션 연계

- 자체적으로 사용하는 보안 관리 솔루션의 경우
- V3 IS 9.0의 API 제공으로 설치 여부 및 상태 확인 가능



04. 주요 기술

-
1. 다차원 분석 플랫폼
 2. URL/IP 탐지
 3. 클라우드 기반 탐지
 4. 시그니처 기반 탐지
 5. 행위 기반 탐지
 6. 평판 기반 탐지
 7. 액티브 디펜스(Active Defense)

다차원 분석 플랫폼

V3 Internet Security 9.0에 적용된 다차원 분석 플랫폼은 6가지 핵심 탐지 기술이 있어 빠르고 정확한 악성코드 분석은 물론 아직 알려지지 않은(0-day) 신·변종 악성코드까지 진단합니다.

2. 클라우드 탐지(ASD)

- 8억여 개의 DB정보에서 실시간 확인
- 시그니처 업데이트 없이 실시간 반영

3. 시그니처 탐지(TS)

- DNA Scan으로 다양한 변종 진단
- 최초 발견 파일에 대해 사전 진단

1. URL/IP 탐지

- 악성코드가 PC로 다운로드 되기 전 시그니처 업데이트 없이 실시간 반영

4. 평판 기반 탐지

- 안정성 미확인 프로그램 차단
- 시그니처 없이 사전 방어
- 평판 조건 사용자 선택

6. Active Defense

- 실시간 분석 정보
- 프로그램의 활동내역
- 클라우드 자동 분석

5. 행위 기반 탐지

- 0-day 취약점 원천 차단
- 시그니처 업데이트 없이 사전 진단
- 100여 개의 악의적 행위 패턴 탐지



URL/IP 탐지

ASD 네트워크를 통해 축적된 웹사이트 및 IP 정보를 통해 악성코드를 유포하는 웹사이트 및 IP로의 접근을 차단하는 기능입니다. 사용자가 웹사이트를 방문할 경우, 이 과정에서 요청되는 모든 URL을 ASD에 질의해 악성으로 판별되면 곧바로 URL 접속을 차단합니다. 또한 웹사이트의 취약점을 통해 유입되는 행위 발견 시, 해당 URL을 ASD에 보고해 악성 행위에 대해 검증, 갱신 업데이트를 진행합니다.

기 병	종 류	내 용
악성 웹사이트 차단	악성URL	홈페이지 변조를 통해 악성 파일을 다운로드하게 하는 중간 단계의 URL 최종 악성 파일(PE)를 다운로드하는 URL
	피싱 URL	피싱 웹사이트 URL
불필요한 웹사이트 차단	PUS	불필요한 웹사이트(PUS), 불필요한 프로그램(PUP)의 설치를 유도하거나, 사용자에게 불필요한 사이트로 유도하는 URL
신뢰 웹사이트 예외 처리	신뢰 URL	사용자에 의해 신뢰 사이트로 추가된 URL (이 URL에 대해서는 예외로 처리하여 접속 차단을 하지 않는다)
사용자 정의 웹사이트 차단	사용자 정의	사용자 (V3사용자 또는 APC 관리자)에 의해 입력된 URL



클라우드 기반 탐지(1)

AhnLab Smart Defense(ASD)

ASD(AhnLab Smart Defense)는 클라우드 컴퓨팅 기반의 혁신적인 악성코드 위협 분석 및 대응 기술로, 신·변종 악성코드 및 다양한 보안 위협에 신속·정확하게 대응합니다.



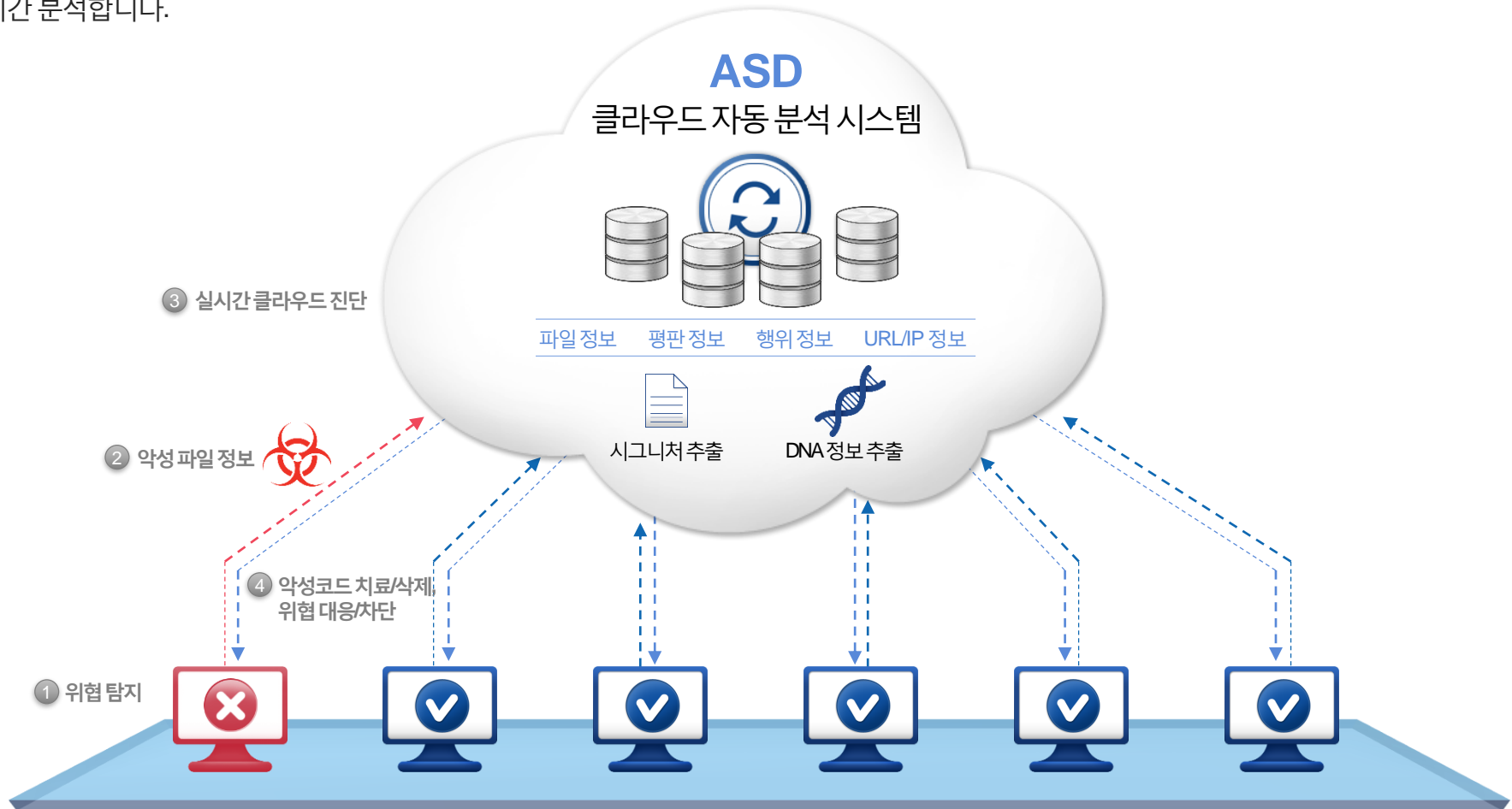
2013. 12. 현재 ASD 보유 DB

800,000,000 (약 8억 개)

수 천만대 PC의 악성코드 정보 모니터링

클라우드 기반 탐지(2)

- **ASD 네트워크**에 연결된 수천만 대의 PC에서 실제 발생한 위협 정보를 실시간 공유해 분석 정확도를 극대화합니다.
- 수억 개 파일의 DNA DB를 통해 신·변종 악성코드를 사전 탐지하고 악성 URL 정보, C&C 서버 IP 정보, 평판 정보로 종합적으로 실시간 분석합니다.



2,000만 명 이상의 사용자로 구성된 ASD 네트워크를 통한
악성코드 정보 실시간 분석 및 대응

시그니처 기반 탐지(1)

DNA Scan(TS Prime엔진) 기술

DNA 스캔(Scan)은 ASD DB에 보유하고 있는 8억 개 이상의 파일을 대상으로 고유 특징을 추출해 인간의 DNA 맵과 같이 파일 DNA 맵을 구성, 이를 통해 신종 및 변종 악성코드를 진단하는 기술입니다.

사람의 Genome

질환 발현 염색체 규칙 및
위치 발견 진단, 치료



정신분열 발현
염색체



심장 질환 발현
염색체



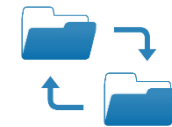
비만
염색체



자궁암 발현
염색체

File의 Genome

악성코드 고유의 특성
발현 항목(DNA)의 규칙 발견 및 진단, 치료



타 프로그램 감염



특정 정보 전송

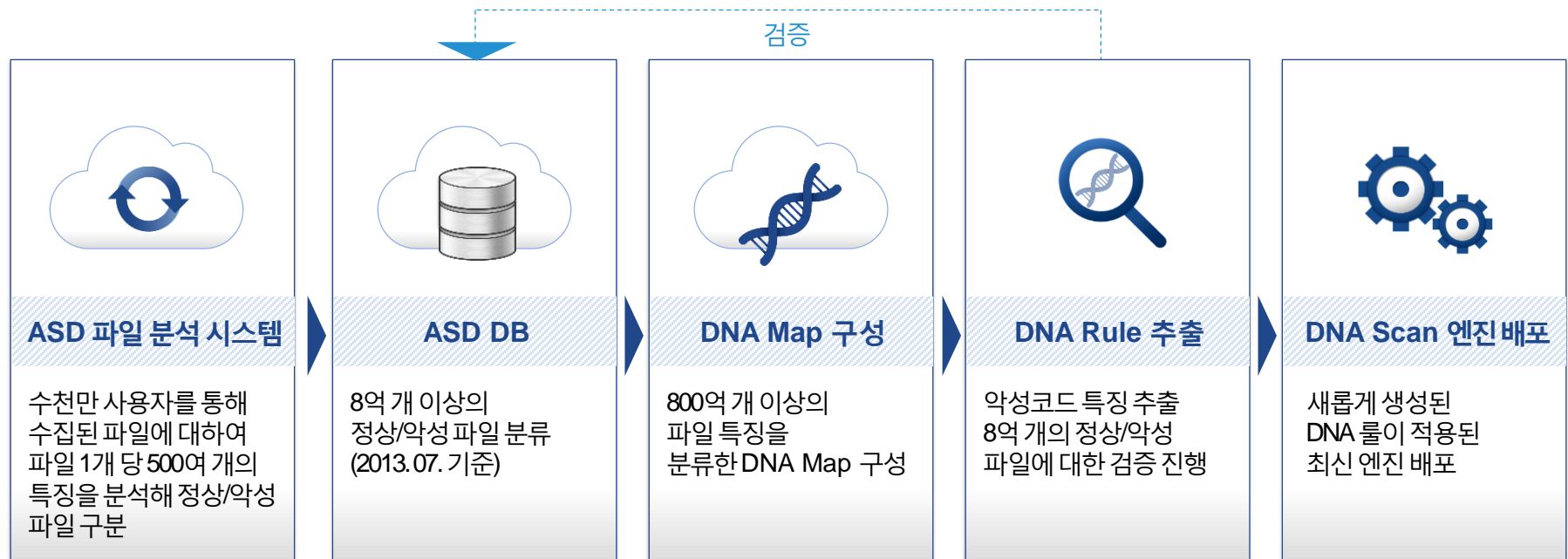


은폐, 자동 실행

시그니처 기반 탐지(2)

ASD 네트워크를 통해 수집된 수억 개의 파일 정보를 분석해 정상 또는 악성 시그니처를 생성 및 매칭, 진단하는 기술입니다. 특히 안랩의 시그니처 기반 탐지 기술은 20여 년 간 축적된 악성코드 분석 노하우를 바탕으로 독자 개발한 TS Prime 엔진을 통해서 ▲안티바이러스 시그니처 ▲안티스파이웨어 시그니처 ▲네트워크 시그니처를 DNA 룰 형태로 제공함으로써 최신 악성코드에 신속하고 정확하게 대응하도록 해줍니다.

- 네트워크 쿼리 없이 엔진 형태로 제공되는 독보적 휴리스틱 진단 제공
→ 완전 폐쇄망 지원(TS Prime 엔진과 함께 제공)
- 분석가의 경험에 의존적인 일반 휴리스틱 진단법과 달리,
ASD 네트워크에 접속하는 수천만 명 사용자 기반의 8억 개 이상의 파일에 대한 검증 후 엔진 반영
→ 타사 대비 휴리스틱 진단법 오진 확률 최소화

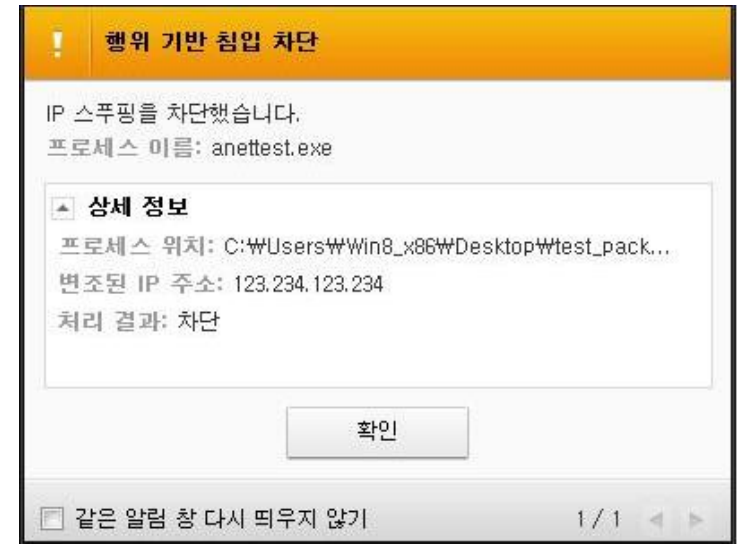
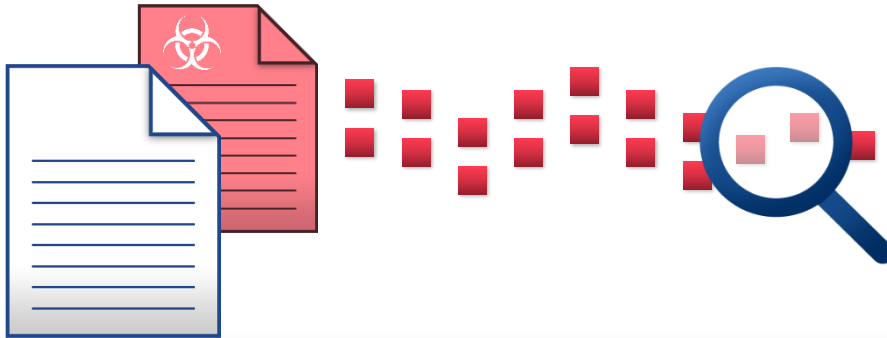


행위 기반 탐지

행위 기반 침입 차단 기능은 패킷의 특정 서명 정보가 아니라, 비정상적인 패킷의 흐름을 모니터링해 이상 여부를 판단하는 기술입니다. 알려지지 않은 네트워크의 위협을 방어하기 위해 알려지지 않은 프로토콜 드라이버 차단을 비롯해 이상 트래픽 차단, IP 스누핑, Mac 스누핑, ARP 스누핑 탐지 등의 기능을 제공합니다.

- 시스템 파일명 변경/시스템 파일의 이름을 변경하는 프로세스 진단
- 문서, 자바 취약점을 통한 PE 생성
- 웹 브라우저 취약점으로 PE다운로드/웹 브라우저의 취약점을 통한 프로세스 실행
- 보안 설정 변경 후 인젝션 등

행위기반 진단 룰을 통해 파일의 의심스러운 행위를 진단하여 제로데이 공격이나 비정상적인 익스플로이트를 원천 차단합니다.

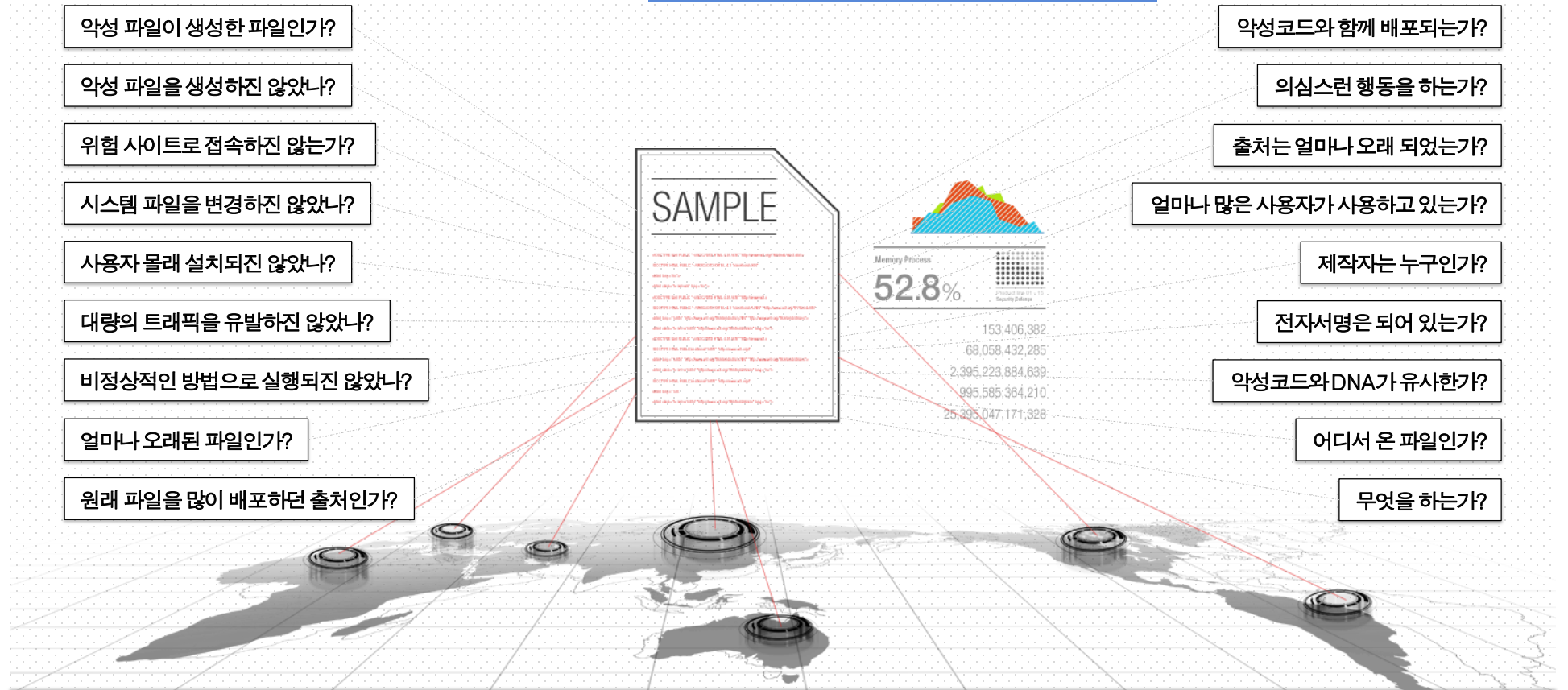


평판 기반 탐지(1)

평판 기반 기술은 기본적으로 평판이 낮은(=평판이 좋지 않은) 프로그램을 통제하는 데에 활용됩니다.
 새로 만들어진 악성코드는 제작자가 불분명하고 출처가 불확실하며, 사용자가 거의 없기 때문에 평판이 낮을 수 밖에 없습니다.
 기업에서 별도로 사용하고 있는 프로그램은 화이트리스트 처리하여 안정성을 확보 할 수 있습니다.

평판 기반 탐지

파일(샘플)의 출처와 샘플의 나이, 샘플 사용자 수, 제작 목적, 제작자 정보 등 해당 샘플 자체가 아닌 **샘플과 연관된 모든 정보를 분석에 활용하는 기술**

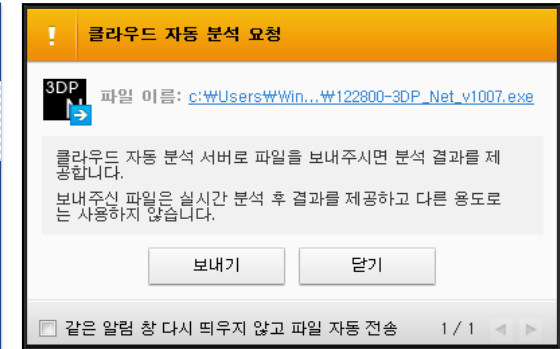


평판 기반 탐지(2)



클라우드(ASD) 평판 검사

- ASD 서버의 평판 정보를 이용해 검사 시 평판이 낮은 파일을 진단
: 사용자의 PC에서 ASD에 존재하지 않는 파일이 발견되는 경우, 이를 ASD클라우드에 전송(설정 옵션 활용)
- 클라우드에 전송된 파일은 정적/동적 분석을 통해 악성 여부를 판단, 반영
- ASD의 악성코드 탐지 차단 기능에 적용돼 실시간 탐지 및 수동 검사에도 활용

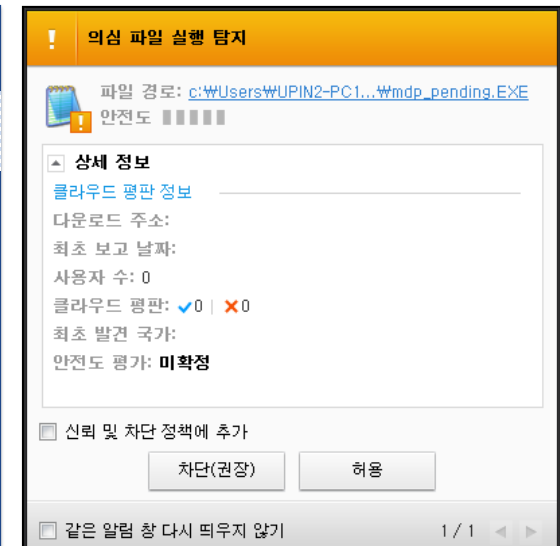


평판 기반 프로그램의 실행 차단

- 사용자의 PC에서 프로그램이 실행될 때 악성으로 판정되진 않았으나 프로그램의 평판 정보를 통해 안정성이 검증되지 않은 프로그램의 경우 실행을 차단

※ 평판 탐지의 예시

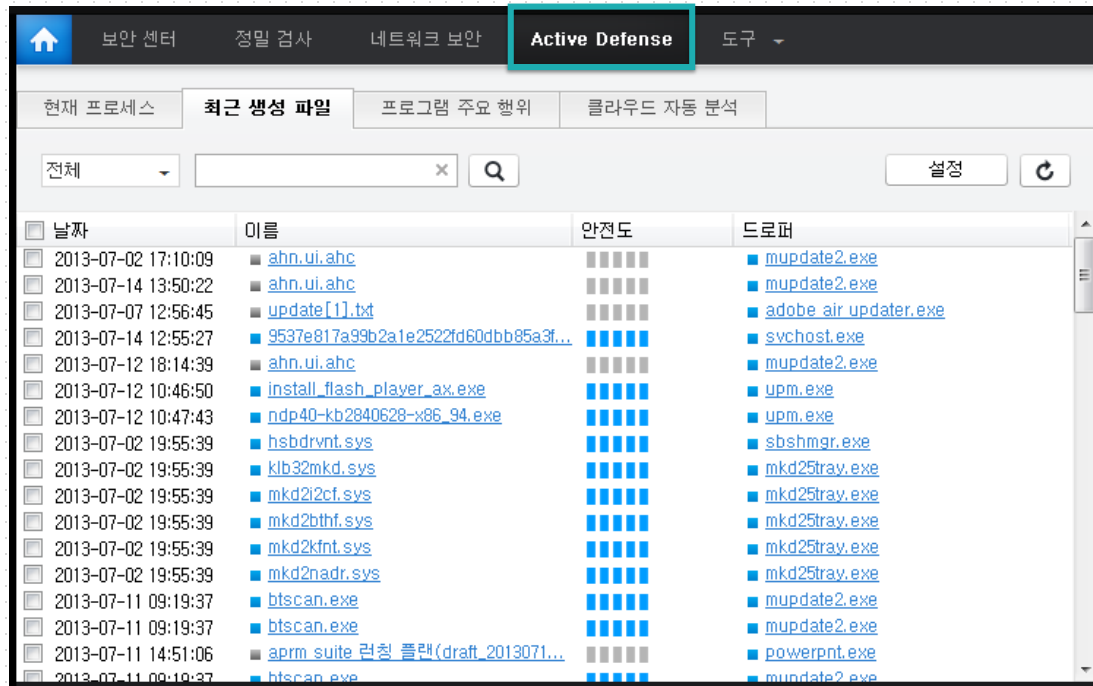
- 최초 발견된 지 20일 이내의 파일로, 사용자 수가 극히 적은(500명 이하) 프로그램
* 100여 개의 의심 행위에 대한 탐지를 실시함



액티브 디펜스(Active Defense)

사용자 PC 내에서 발생한 행위 정보와 이슈가 될 수 있는 파일들을 필터링해 의심스러운 파일과 그 행위에 대해 사용자에게 정보를 제공하는 기술이자 기능으로, 위협에 대한 가시성을 제공함으로써 능동적인 대응이 가능하도록 돕습니다.

- **프로그램 활동 내역 정보 제공**: 특정 프로세스가 어떤 행위를, 어떻게 하는지 가시성 확보
- **동작중인 프로세스**: 실행되고 있는 전체 프로세스 중 의심스러운 프로세스만을 취합해 사용자에게 정보 제공
- **최근 생성 파일**: 최근 생성된 파일 중 의심 파일만을 필터링해 정보 제공
- **차단 및 신뢰를 사용자가 직접 적용 가능**



05. 주요 기능

-
1. 주요 기능 요약
 2. 기능/성능 비교표
 3. 시스템 요구 사항

주요 기능 요약

<p>Anti-Virus/ Anti-Spyware</p>	<ul style="list-style-type: none"> • ASD(AhnLab Smart Defense) 클라우드 네트워크 사용 • 스마트 스캔(Smart Scan) 기술 적용 • 행위/평판 검사(클라우드 행위/평판 검사 포함) • 액티브 디펜스(Active Defense) 적용 • DNA 스캔(Scan) 지원 • PC 실시간 검사, 수동(정밀) 검사, 예약 검사 기능(사용자예약 검사 우선) • 시작 프로그램 감시, 실행 중인 프로세스, 메모리 검사 기능 • 제품 보호 기능(자동 재시작, 보호대상 설정(파일, 프로세스, 레지스트리, 볼륨)) • 실시간 감시 자동 재시작/부트타임 실시간 검사 기능 • 중요 시스템 파일 보호, 부트 타임 제품 보호 사용 • 불필요한 프로그램 검사(PUP), 유해 가능 프로그램 검사 • 압축 파일 검사, USB 드라이브 검사, 공유 폴더 해제 후 검사 • 악성코드 초기 실행 방지, CD/USB 드라이브 자동 실행 방지/제품 감염 여부 검사
<p>네트워크 보안</p>	<ul style="list-style-type: none"> • 서명 기반 네트워크 침입 차단(허용/차단 IP 사용, 공격자 IP 임시 차단) • 행위 기반 네트워크 침입 차단(Unknown Protocol Driver 방어, 이상 트래픽 방어, IP/MAC/ARP 스푸핑 방어) • 포트 차단(포트 차단 방식, 예외 포트 사용, 포트 차단 규칙 관리) • 신뢰할 수 있는 IP와 차단해야 할 IP 등록 • 악성코드 확산 시 네트워크 긴급 차단 • 공격 IP 임시 차단 • 개인 방화벽(네트워크 완전 차단, 신뢰 프로그램 판단 기준 설정, 방화벽 정책 목록, 포트 숨김) • 유해 웹사이트 차단
<p>Active Defense</p>	<ul style="list-style-type: none"> • 동작 중인 프로세스 확인, 최근 생성된 파일 확인, 프로그램 활동 내역 확인, 클라우드 자동 분석 결과 확인 • 신뢰/차단 프로세스 목록 관리

기능/성능 비교표

구분	AhnLab		Hauri	ESTSoft	Kaspersky Lab		Avast	Symantec	McAfee
	V3 Internet Security 8.0	V3 Internet Security 9.0	ViRobot Internet Security 2011	알약 3.0	Endpoint Security for Business - Core (한글판)	Endpoint Security for Business - Core	Endpoint Protection Suite Plus	Endpoint Protection 12.1	VirusScan Enterprise 8.8
클라우드 기반 엔진	○	○	X	○	○	○	○	○	X
압축 파일 검사	○	○	○	○	○	○	○	○	○
신.변종 악성코드 분석	○	○	○	○	○	○	○	○	○
감염되기 쉬운 파일 검사	○	○	○	○	○	○	X	○	X
EML 파일 검사	○	○	○	○	○	○	○	○	○
CD/USB 자동실행 방지	○	○	○	○	○	○	X	X	X
휴리스틱 진단	○	○	○	○	○	○	○	○	○
PUP 검사	○	○	○	○	○	○	○	○	X
평판 기반 차단	X	○	X	X	○	○	X	○	X
클라우드 자동 분석	X	○	X	X	○	○	○	○	X
Active Defense	X	○	X	X	X	X	X	X	X
빠른 검사(Smart Scan)	X	○	X	○	○	○	○	○	X
현황판(Dashboard)	X	○	X	X	X	X	○	X	X
다운로드 파일 평판 분석	X	○	X	X	X	X	X	○	X
HIPS(스푸핑)	X	○	X	X	X	○	○	○	○
Stable 엔진 사용 기능	○	○	X	X	X	X	X	X	X

기능/성능 비교표

구분	AhnLab		Hauri	ESTSoft	Kaspersky Lab		Avast	Symantec	McAfee
	V3 Internet Security 8.0	V3 Internet Security 9.0	ViRobot Internet Security 2011	알약 3.0	Endpoint Security for Business - Core (한글판)	Endpoint Security for Business - Core	Endpoint Protection Suite Plus	Endpoint Protection 12.1	VirusScan Enterprise 8.8
클라우드 기반 엔진	○	○	X	○	○	○	○	○	X
압축 파일 검사	○	○	○	○	○	○	○	○	○
신.변종 악성코드 분석	○	○	○	○	○	○	○	○	○
감염되기 쉬운 파일 검사	○	○	○	○	○	○	X	○	X
EML 파일 검사	○	○	○	○	○	○	○	○	○
CD/USB 자동실행 방지	○	○	○	○	○	○	X	X	X
휴리스틱 진단	○	○	○	○	○	○	○	○	○
PUP 검사	○	○	○	○	○	○	○	○	X
평판 기반 차단	X	○	X	X	○	○	X	○	X
클라우드 자동 분석	X	○	X	X	○	○	○	○	X
Active Defense	X	○	X	X	X	X	X	X	X
빠른 검사(Smart Scan)	X	○	X	○	○	○	○	○	X
현황판(Dashboard)	X	○	X	X	X	X	○	X	X
다운로드 파일 평판 분석	X	○	X	X	X	X	X	○	X
HIPS(스푸핑)	X	○	X	X	X	○	○	○	○
Stable 엔진 사용 기능	○	○	X	X	X	X	X	X	X

시스템 요구 사항

1. 하드웨어 요구 사항

구분	시스템 요구사항
CPU	Intel Pentium 4 1GHz 이상
메 모리	512MB 이상
HDD	300MB 이상의 여유 공간
지원 언어	한국어, 영어

2. 소프트웨어 요구 사항

제품명	운영 체제
AhnLab V3 Internet Security 9.0	Windows XP SP2 이상 Windows Vista SP1 이상 Windows 7 Windows 8 (8.1 포함) Windows 10 Windows 10 IoT Enterprise * 32비트와 X64 계열의 64비트 CPU 지원

06. 지원 OS 확대(Mac OS)

1. Mac 악성코드 및 국내 PC 환경의 변화
2. AhnLab V3 for Mac
3. AhnLab V3 for Mac 특징점 -APC 통합 운영
4. AhnLab V3 for Mac 주요기능 요약
5. AhnLab V3 for Mac 시스템 요구 사항

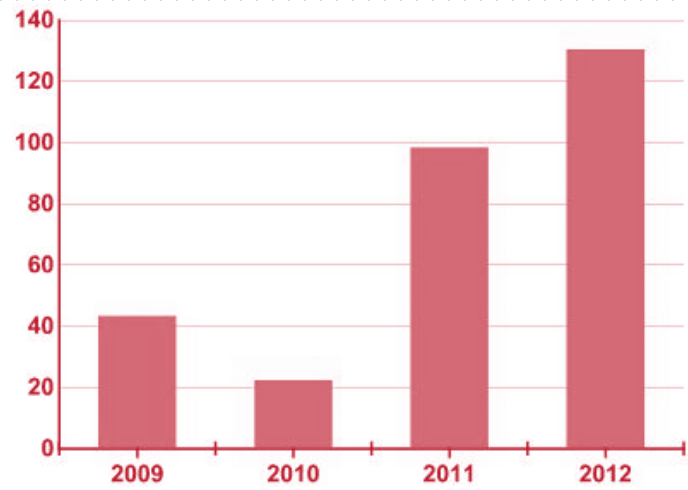


Mac 악성코드 및 국내 PC 환경의 변화

전 세계적으로 OS X(Mac OS) 사용자가 증가함에 따라 이를 노리는 악성코드 또한 급증하고 있습니다.
 한편 국내 OS X 사용 비율은 전체 OS의 2.8%(2013.08 기준)를 차지하고 있습니다.
 이는 윈도8 점유율과 비슷한 수치이며 윈도98, 윈도2000, 윈도ME 사용자 비율의 합한 것보다 높은 수치로,
 기업 내 OS X에 대한 보안 대책 마련이 필요합니다.

[주요 맥(Mac) 악성코드 동향]

- 2011년 전년 대비 6배, 2012년은 전년대비 1.3% 등 맥 악성코드의 기하급수적인 증가
- 2012년 OS X를 대상으로 한 'Flashfake' 악성코드 등장, 전 세계 약 70만대의 Mac PC 감염
- 대표적인 맥 악성코드 'FakeCo'는 전체 Mac PC 감염의 52% 차지, 비디오 코덱 설치 파일로 위장하여 개인정보 탈취
- 아직까지 OS X용 백신 보급이 상당히 더딘 편으로, 맥 악성코드 유입 시 대처에 한계(윈도 OS와 달리 OS X용 무료 백신은 보급되지 않음)



< OS X용 악성코드 추이 >

순위	이름	%
1	Trojan.OSX.FakeCo.a	52%
2	Trojan-Downloader.OSX.Jahlav.d	8%
3	Trojan-Downloader.OSX.Flashfake.ai	7%
4	Trojan-Downloader.OSX.FavDonw.c	5%
5	Trojan-Downloader.OSX.FavDonw.a	2%
6	Trojan-Downloader.OSX.Flashfake.ab	2%
7	Trojan-FakeAV.OSX.Defma.gen	2%
8	Trojan-FakeAV.OSX.Defma.f	1%
9	Exploit.OSX.Smld.b	1%
10	Trojan-Downloader.OSX.Flashfake.af	1%

< OS X 악성코드 Top 20 >

(*출처 : Kaspersky Lab)

AhnLab V3 for Mac

AhnLab V3 for Mac은 기업용 맥 OS(OS X) 전용 안티바이러스 솔루션입니다.
 맥 OS에 최적화된 V3 for Mac은 맥 OS를 노리는 다양한 악성코드 대응이 가능합니다.
 또한 엔드포인트 중앙관리 솔루션 AhnLab Policy Center 및 AhnLab Policy Center Appliance 연동을 통해 쉽고 간편하게 관리할 수 있습니다.



**APC 연동을 통한
관리 편의성**



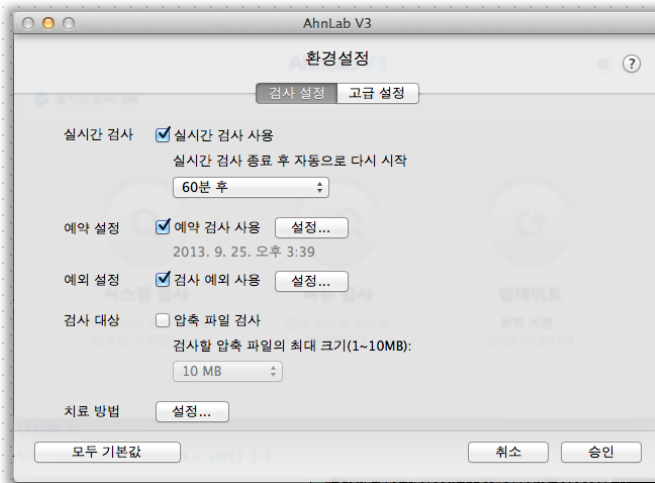
**V39.0 등에 적용된
TS Prime 엔진 적용**



한국어, 영어 지원



**Mac 최적화 UI로
탁월한 사용성 구현**

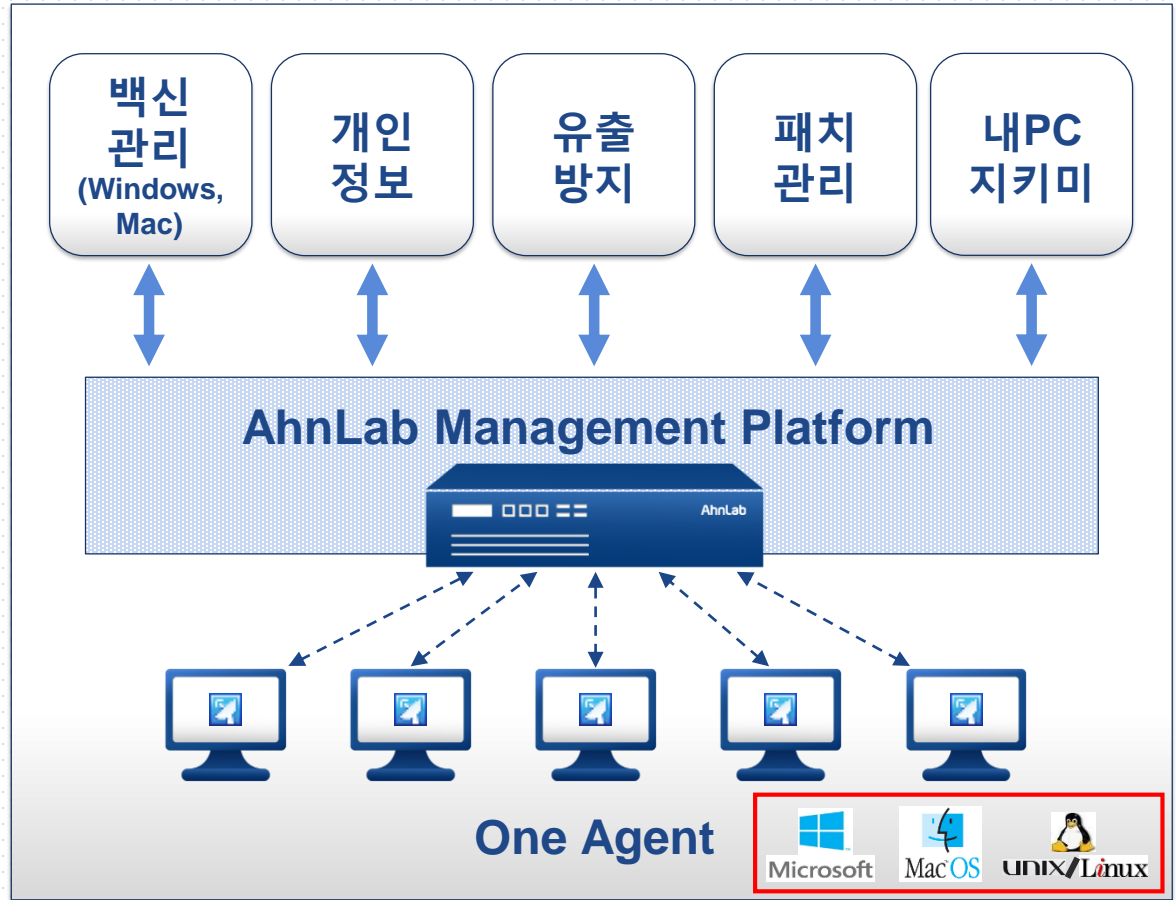


AhnLab V3 for Mac 특징점

AhnLab V3 for Mac는 맥용 백신 중 최초로 중앙관리 솔루션 연동되어 탁월한 관리 편의성을 제공합니다. 엔드포인트 중앙관리 솔루션 AhnLab Policy Center Appliance와의 연동을 통해 백신관리(V3), 패치관리(AhnLab Patch Management), 개인정보보호(AhnLab Privacy Management)를 하나의 Agent, 하나의 플랫폼으로 통합 운영 및 관리할 수 있습니다.



통합



AhnLab V3 for Mac 주요 기능

구분	기능		비고
PC검사	PC 실시간 검사(모든 파일)	빠른 검사(중요폴더 검사)	실시간 검사 (프로그램 실행 시 프로세스검사)
	수동 검사(폴더/파일)	폴더 선택 검사	지정된 디스크 및 폴더에 존재하는 악성코드 검사 및 치료
		사용자 목록 검사(최대50개)	사용자가 미리 저장한 폴더 목록에 대해서 검사 및 치료
		압축 파일 설정	압축 파일 크기 제한(기본값: 10MB), 다중 압축 지원 안 함
		치료방법 설정	그대로 두기 / 치료하기 / 삭제하기 (실행중인 파일도 프로세스 종료 후 삭제)
	예약 검사		한 번만/매일/매월/매주
	사전 검사		실행 중인 모든 process에 대해서 바이러스/스파이웨어 검사 PC실시간 검사 시작 시, PC 검사 및 예약 검사 시작 시 수행
	검사 예외 설정	폴더/파일 대상(최대 50개 등록)	특정 폴더에 대해서 바이러스/스파이웨어 검사를 하지 않도록 제외
	V3 감염 여부 검사		검사/치료 프로그램 자체가 악성코드에 감염되었는지를 검사/치료
	제품 보호		제품의 기능 동작을 중지, 방해 할 목적으로 제품에서 사용하는 파일에 대한 접근 차단
검역소	검역소		악성 코드를 치료할 때 삭제/변경되는 파일 정보를 백업, 필요시 복원 가능
로그	로그		검사 기록, 이벤트 기록 (날짜, 카테고리, 레벨, 기능 이름, 내용, 상세정보)
업데이트	업데이트	3시간 단위 체크	엔진 및 제품 패치, 업데이트
기타	APC 배포를 이용한 설치		

AhnLab V3 for Mac 시스템 요구 사항

1. 하드웨어 요구 사항

구분	시스템 요구사항
CPU	Intel CPU Only
메 모리	1GB 이상
HDD	300MB 이상의 여유 공간
지원 언어	한국어, 영어

2. 소프트웨어 요구 사항

제품명	운영 체제
AhnLab V3 for Mac	MAC OS X 10.9~ 10.11 macOS 10.12 ~ 10.15

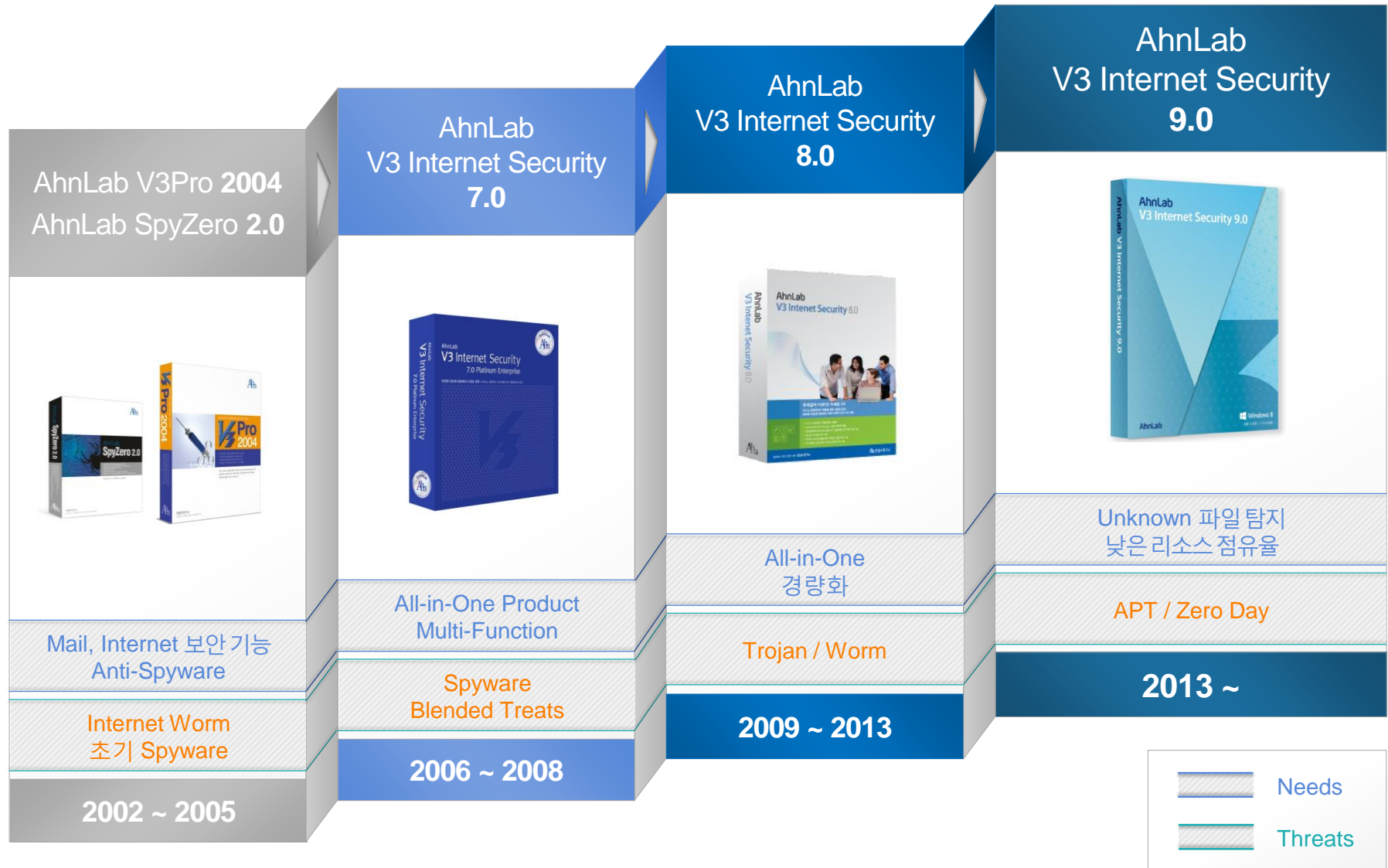
※ 별첨

AhnLab
V3 Internet Security 9.0

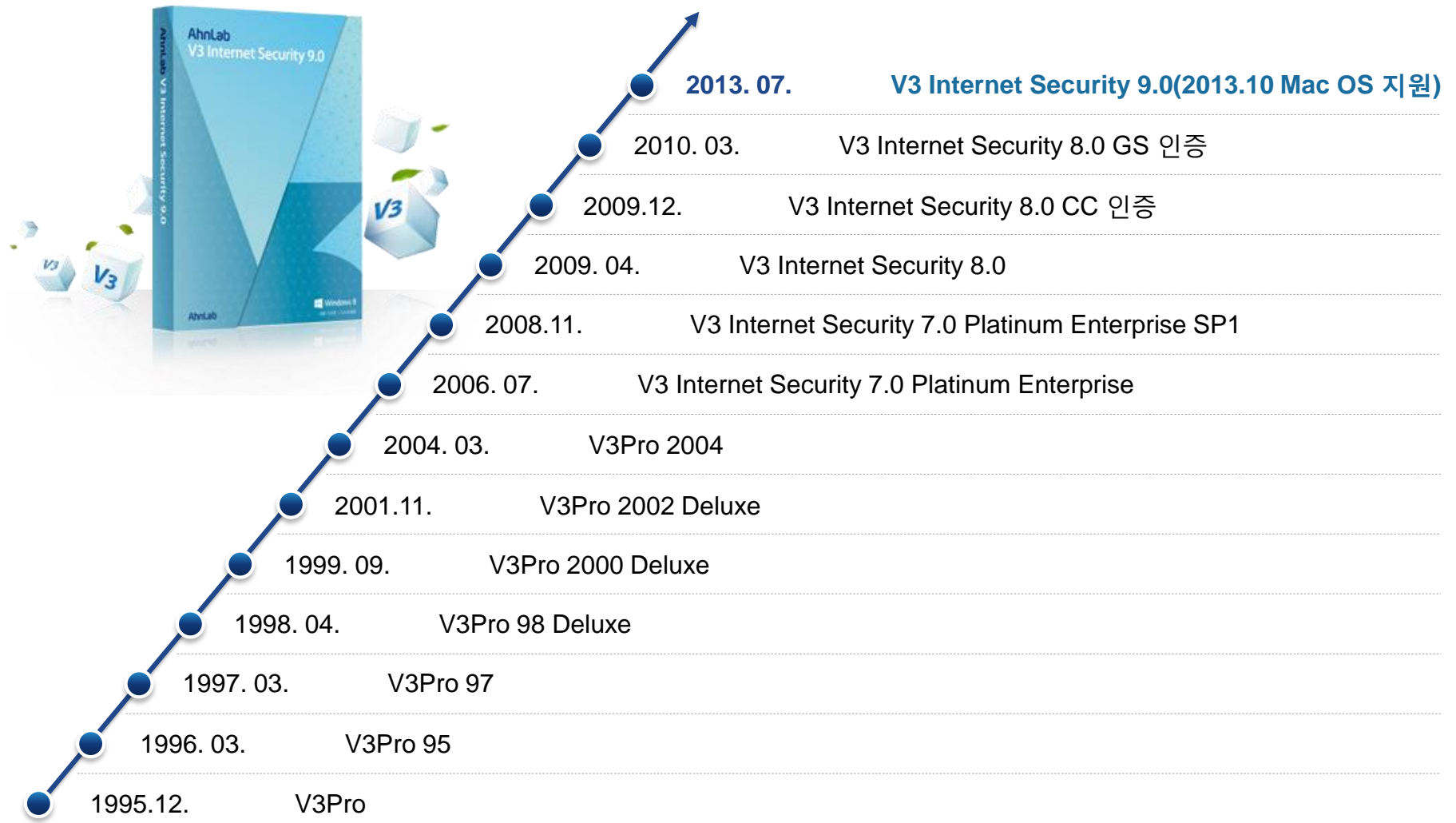
—
제품 연혁

AhnLab

V3 Internet Security 제품 연혁



V3 Internet Security 제품 연혁



㈜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

© AhnLab, Inc. All rights reserved.

AhnLab
V3 Internet Security 9.0

**More security,
More freedom**

AhnLab

