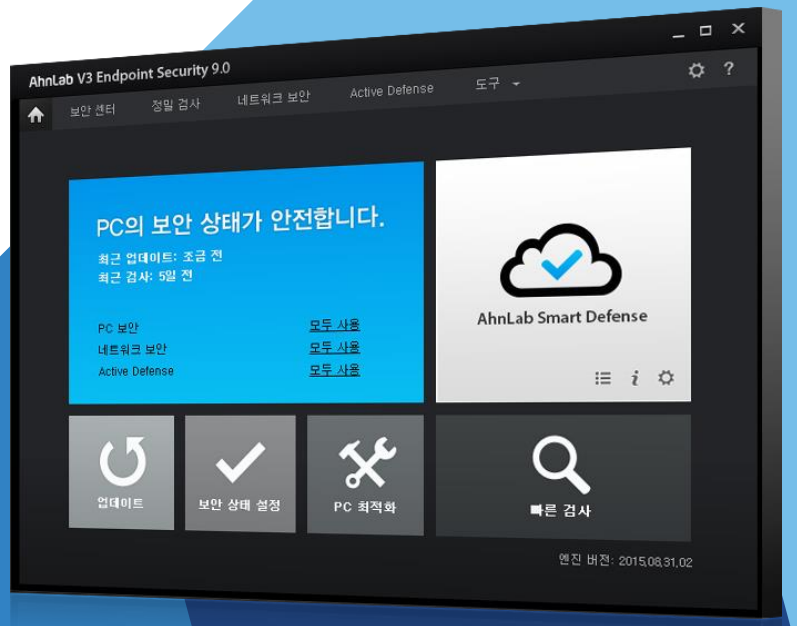
AhnLab

V3 Endpoint Security 9.0

More security,
More freedom

다차원 분석부터 매체제어까지, 엔드포인트 통합 관리 솔루션

표준제안서



AhnLab

AhnLab ENDPOINT SECURITY SOLUTION

Contents

AhnLab
V3 Endpoint Security 9.0

01 제안 배경

02 제품 개요

03 도입 효과

04 주요 기술

05 주요 기능

※ 별첨

AhnLab

01.
제안 배경

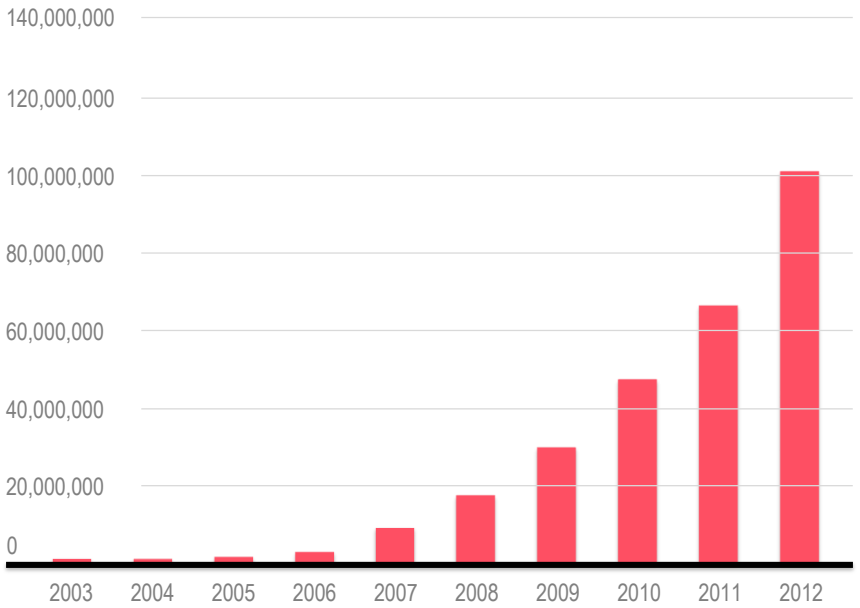
1. 악성코드의 급격한 증가
2. 고도화하고 있는 악성코드
3. 악성코드 웹 유포도 급증
4. 국내 기업의 악성코드 피해 현황
5. 새로운 대응 방안 필요성 대두

1. 악성코드의 급격한 증가

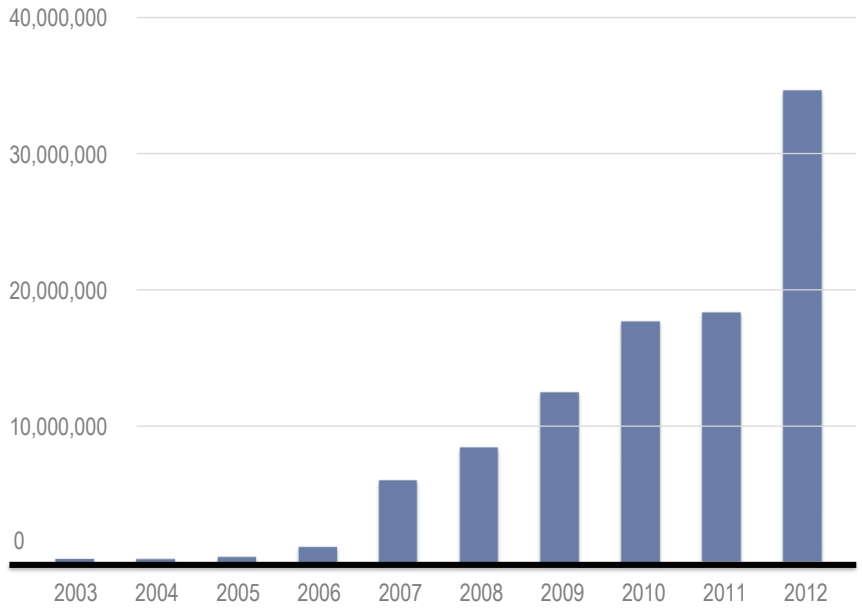
해마다 악성코드의 수는 기하급수적으로 늘고 있습니다. 한 기관에 따르면 매일 20만여 개의
악성코드가 새롭게 발견되고 있습니다. 그만큼 분석 및 대응해야 하는 악성코드의 수가 급격히 늘고 있는 셈입니다.

- 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)

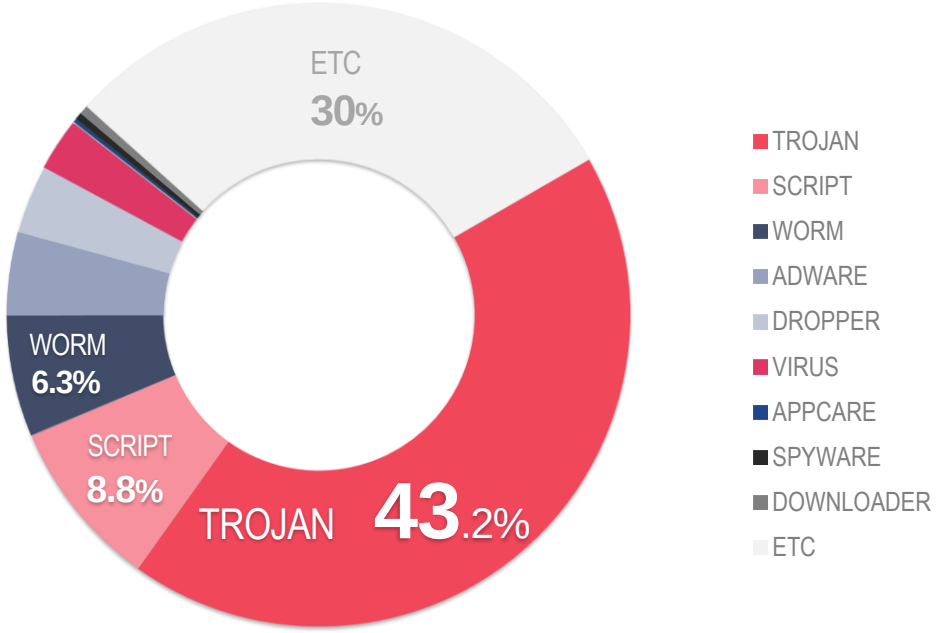
2. 고도화하고 있는 악성코드

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.

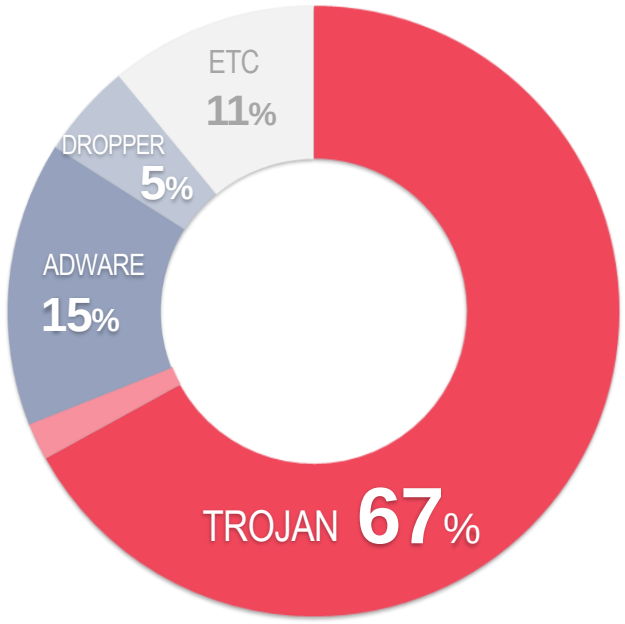
주요 악성코드 유형

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



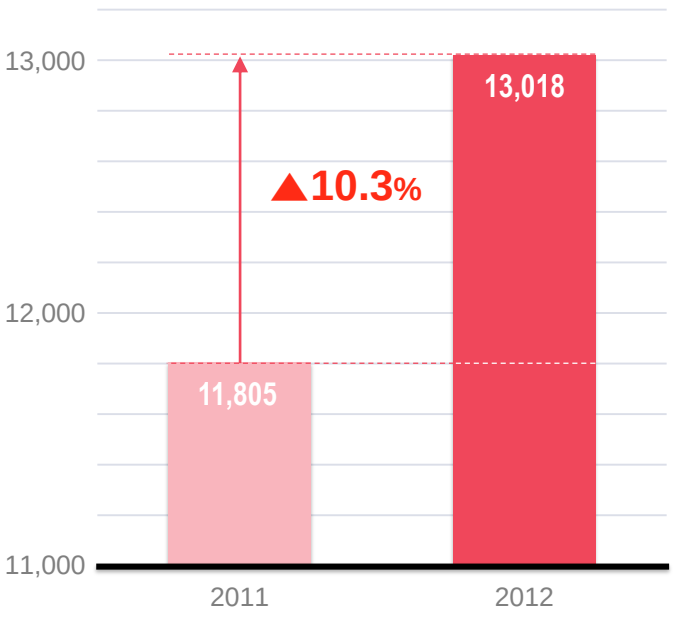
Source : AhnLab ASEC Report

3. 악성코드 웹 유포도 급증

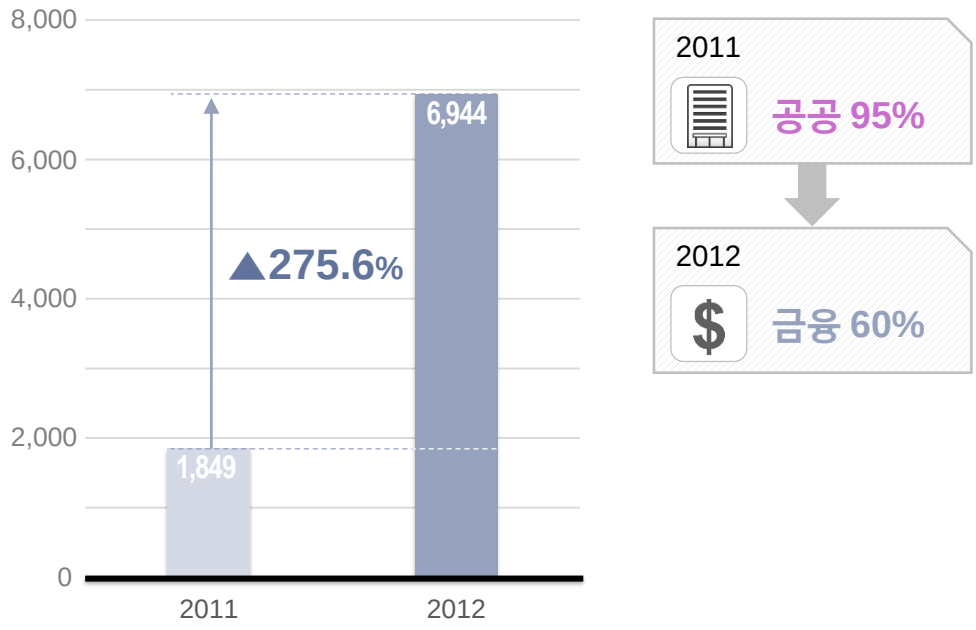
2012년 피싱 사이트는 2011년 대비 275.6%나 증가했고 악성코드 은닉 사이트도 전년 대비 10.3%가 증가했습니다. 무엇보다 피싱/파밍 사이트로 인한 금융 피해 급증하는 양상입니다.

- 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

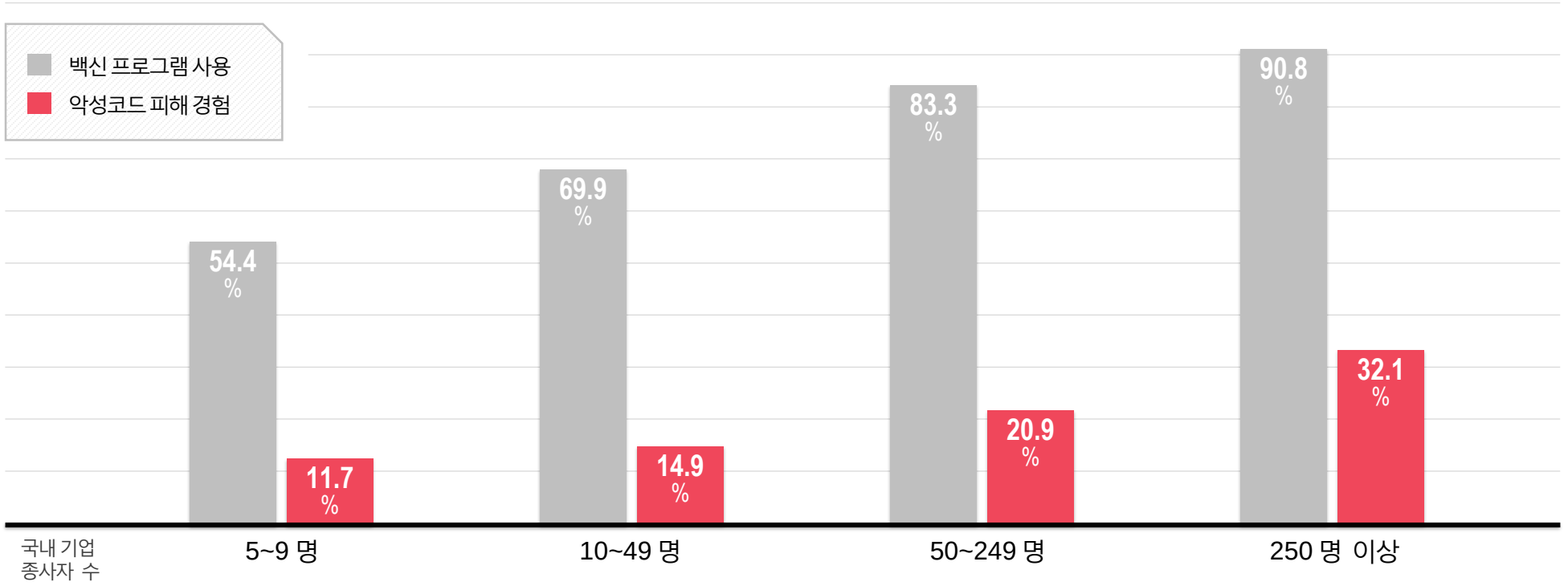


Source : Internet & Security Focus 2013, KISA

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)

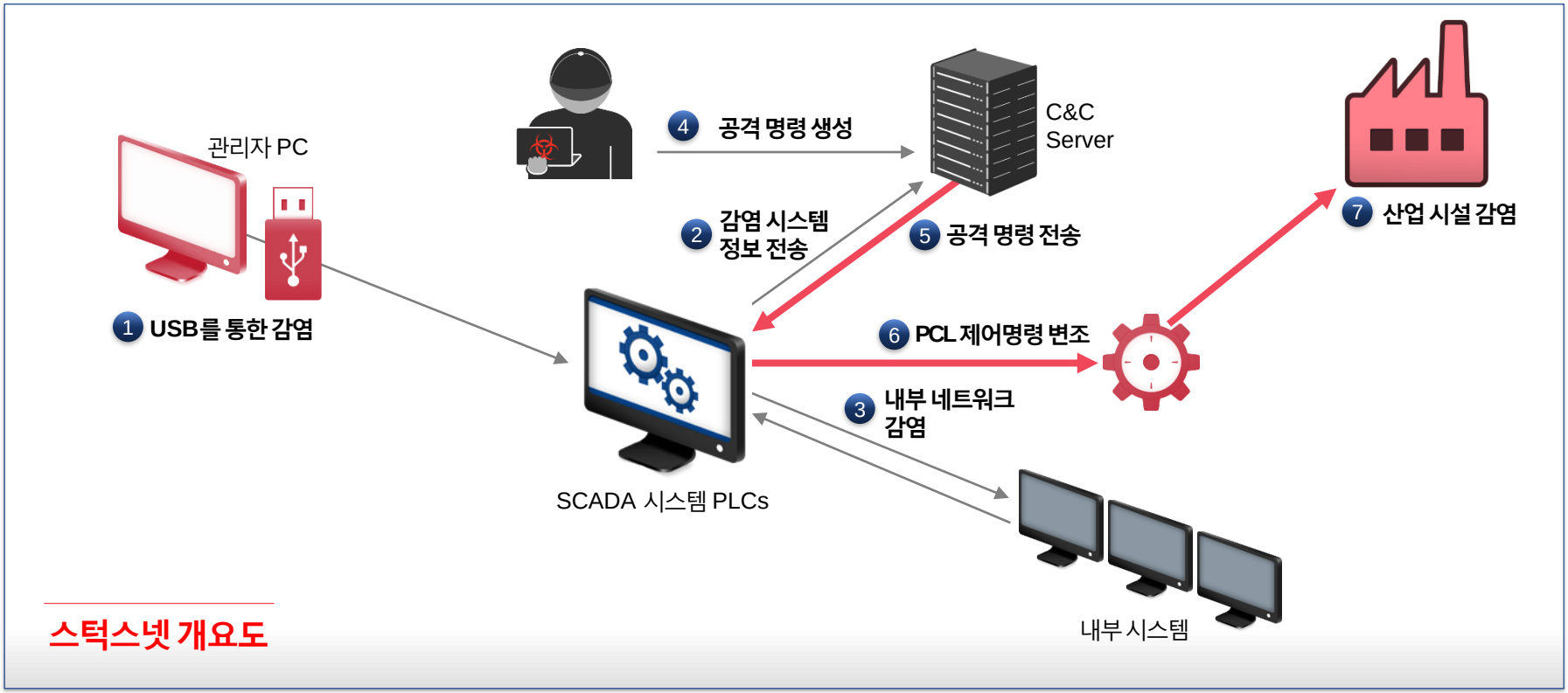


Source : 정보화통계집, NIA

악성코드 유입 경로의 다변화

최근 인터넷과 SNS는 물론이고 사내 PC 사용자가 이용하는 이동형 저장장치를 통한 악성코드 유입이 다수를 이루고 있습니다.

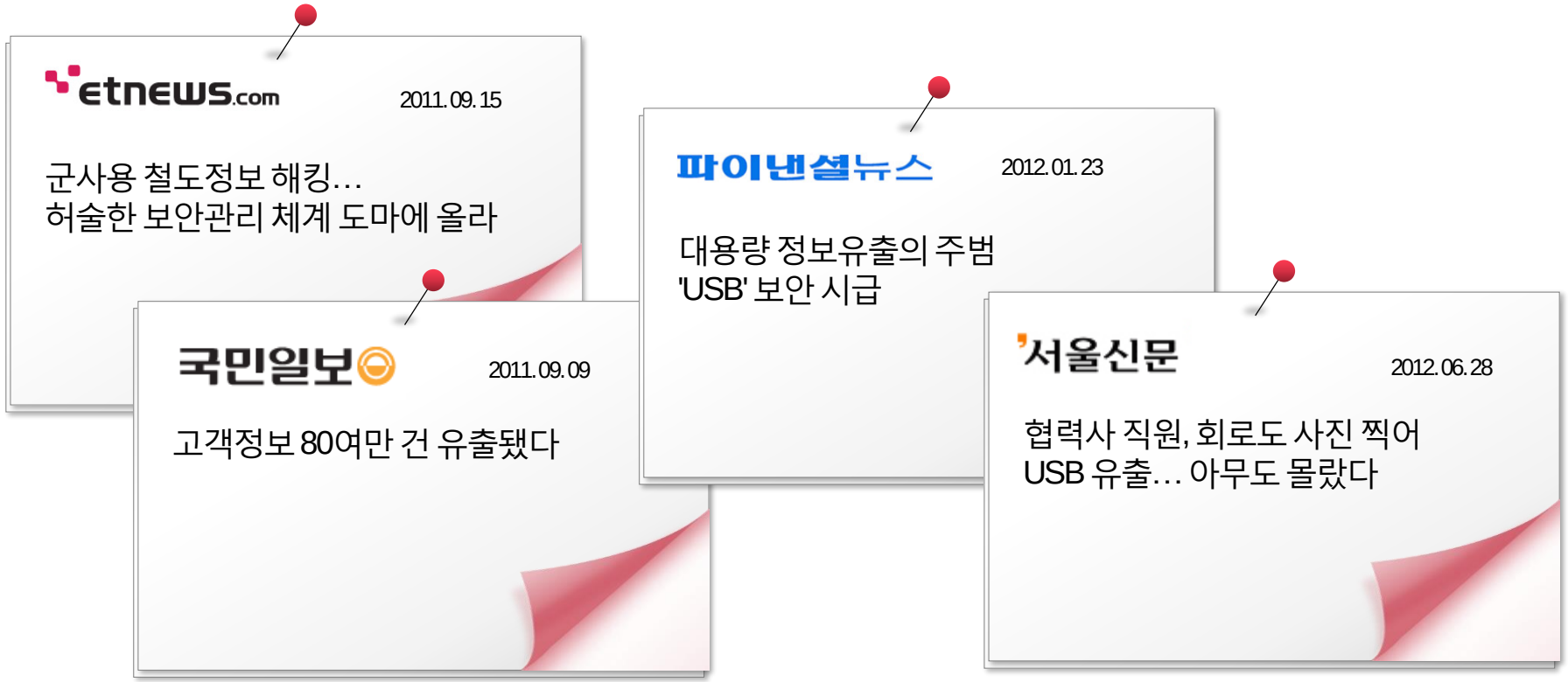
- **2010년 이란 등에서 발견된 '스턱스넷(Stuxnet)'**
  - 기간시설 파괴 목적, 직원들이 사용하는 USB 저장장치 등을 사내에서 연결할 때 침투
- **2012년 서아시아 지역에서 '미니플레임(miniFlame)' 발견**
  - 사회기간 시설망 혹은 기밀에 해당 하는 정보 수집 목적, USB 악용해 침투



내부 정보 유출 위협 증가

기업의 중요한 정보 자산과 대용량 정보가 이동형 저장장치를 통해 외부로 유출된 사례도 다수 발견되고 있습니다.

- **이동형 저장장치에 의한 국내 공공기관 및 기업의 중요 정보 유출 사고 잇따라 발생**
  - 2011년 모 공기업, 직원 과실로 2만6000여 건의 군사용 정보 해킹
  - 모 카드사 80만 명의 고객 정보 유출
  - 3,500만 명 정보가 빠져나간 모 포털 사이트 해킹 사고



체계적인 대응 전략 필요성 대두

매체제어와 사전 방역을 동시에 해결!

V3 Endpoint Security 9.0

매체제어 기능으로 악성코드 유입 차단 중요 정보 자산 유출 방지	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

• 악성코드 탐지/제어 어려움 • 정보 유출 관리 미흡	• 분석 시간 및 누락 샘플 증가 • 엔진 크기 증가	• 탐지/대응의 어려움 • 사전 관리 부재
		
유입 경로 다양화	**악성코드 수 폭증**	**은폐, 제로데이 고도화**

02.
제품 개요

1. V3 Endpoint Security 9.0 소개

2. 특장점

AhnLab

V3 Endpoint Security 9.0 소개

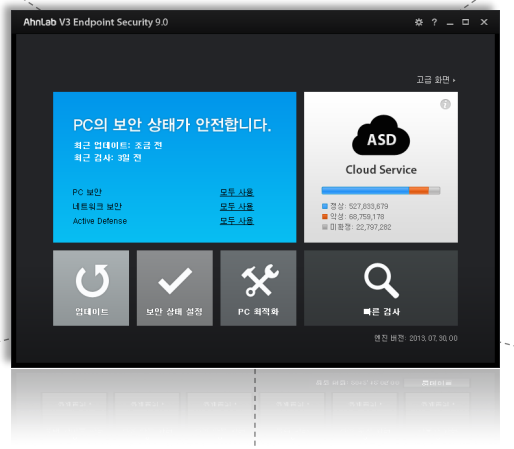
엔드포인트 통합 관리 솔루션 V3 Endpoint Security 9.0은 다차원 분석 플랫폼과 매체제어 기능으로 다양한 경로를 통해 유입되는 악성코드를 원천 차단합니다.

AhnLab V3 Endpoint Security 9.0

다차원 분석부터 매체제어까지

매체제어 기능으로 강력한 보안

- 다양한 경로로 유입되는 악성코드 차단
- USB 저장장치, 디스크 드라이브 등 제어 가능



다차원 분석 플랫폼 기반의 탁월한 진단율

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

스마트 스캔 기술로 신속•정확한 검사

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

초경량 엔진으로 PC 메모리 사용량 최소화

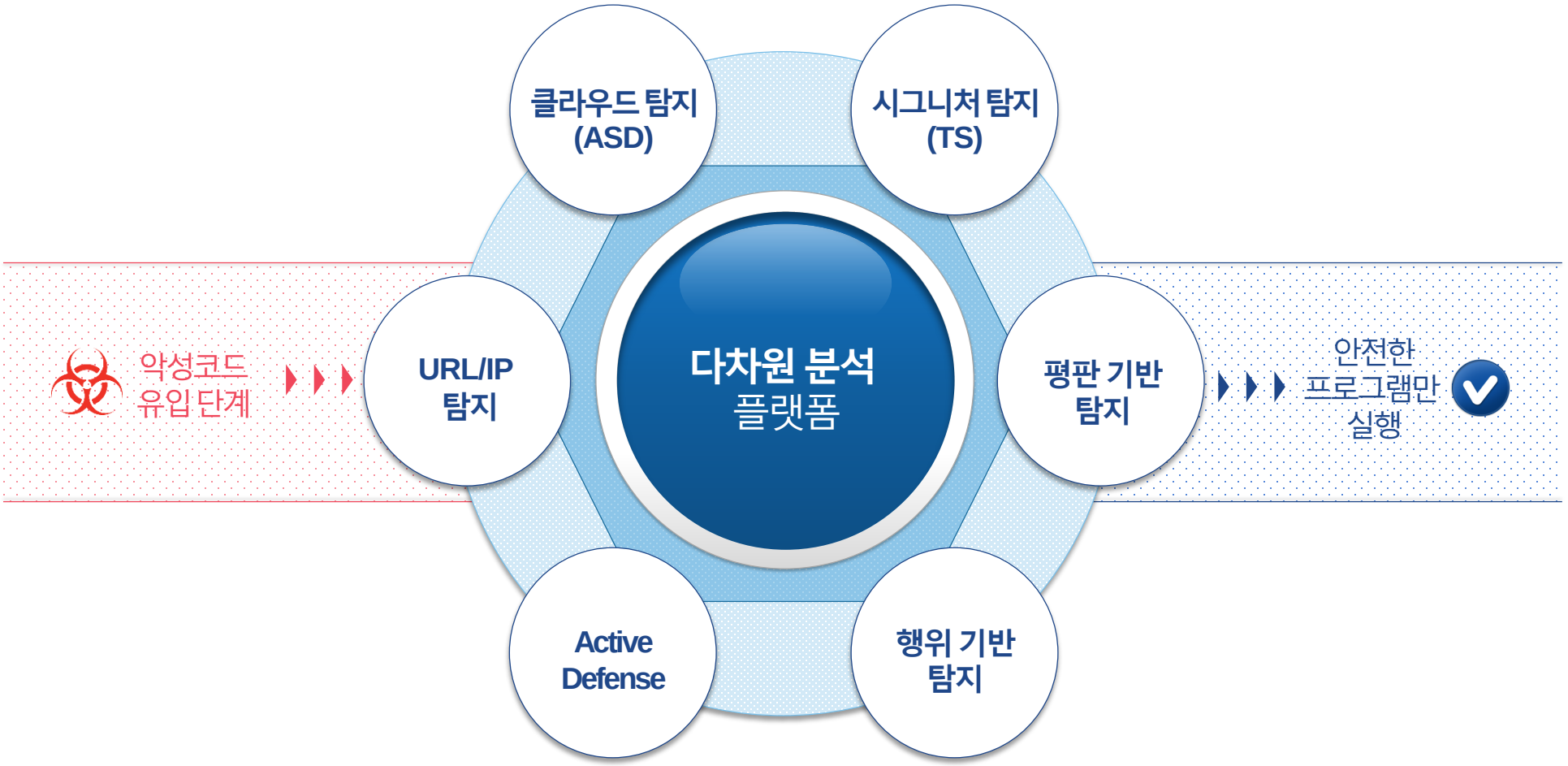
- 안랩의 20여 년 기술 노하우가 응축된 TS Prime 엔진과 클라우드 기반 ASD 엔진 탑재
- 엔진 최적화 기술로 PC 메모리 사용 최소화

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

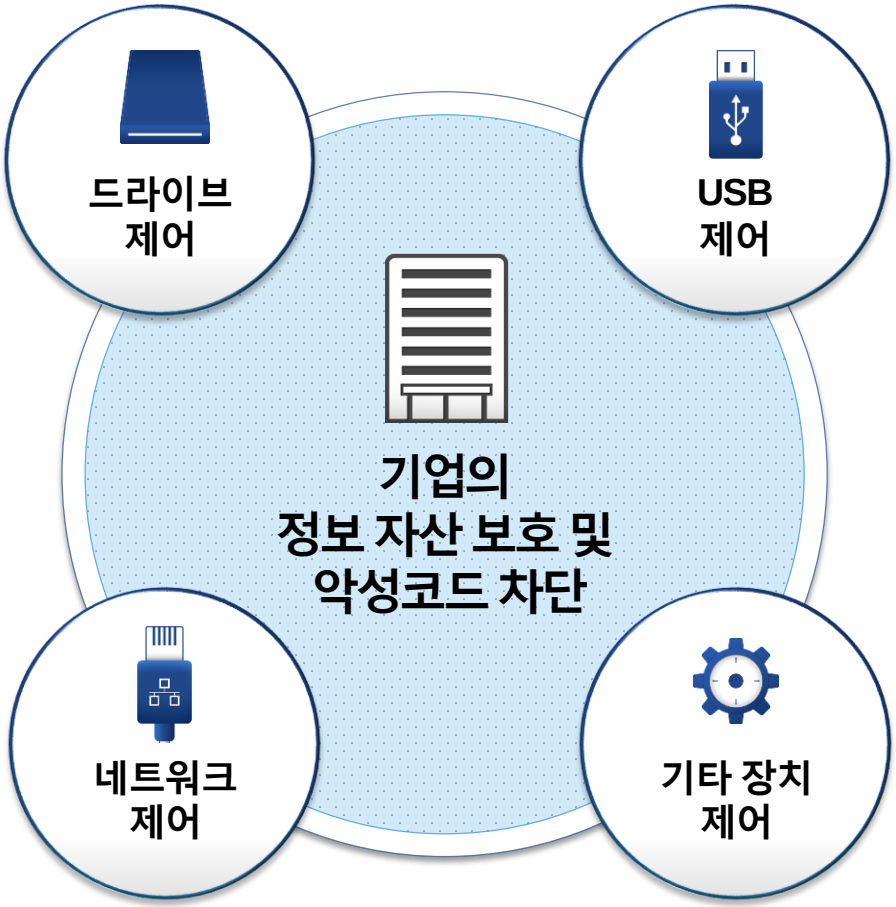
V3 Endpoint Security 9.0에 적용된 다차원 분석 플랫폼은 6가지 핵심 탐지 기술이 있어 빠르고 정확한 악성코드 분석은 물론 아직 알려지지 않은(제로데이) 신•변종 악성코드까지 진단합니다.



특장점

엔드포인트 통합 관리 솔루션 V3 Endpoint Security 9.0은 USB 제어, 네트워크 제어, 드라이브 제어 등 매체제어 기능을 제공해
다양한 경로로부터 유입되는 악성코드를 차단하여 기업의 정보 자산을 안전하게 보호 합니다.

- 디스크 드라이브
- 모뎀
- 플로피 디스크 드라이브
- CD/DVD 드라이브
- 스마트 카드 리더



- USB 저장장치 사용
- USB 저장장치 접근 로깅

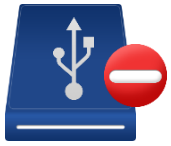
- 유선 네트워크
- 무선 네트워크
- 외장 네트워크 어댑터

- IEEE1394(FireWine)
- PCMICA 어댑터
- 적외선 장치
- 블루투스 장치
- COM/LPT 포트

특장점

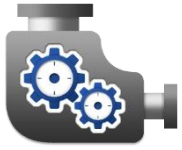
새로운 진단 기술

- **다차원 분석 플랫폼 적용**
- **ASD(AhnLab Smart Defense) 평판 검사**
  - ASD 서버의 평판 정보를 이용해 수동 검사 시 평판 수준이 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



- **매체제어 기능 제공**
- **APC/APC Appliance 연동 시**

- USB 저장장치를 비롯해 다양한 이동형 저장장치에 대한 통제/제어 가능
- 악성코드의 사내 유포 사전 방지
- 중요 정보의 외부 유출 방지



엔진 초경량화 기술 적용

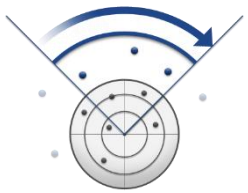
- **TS Prime 엔진 적용**

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

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

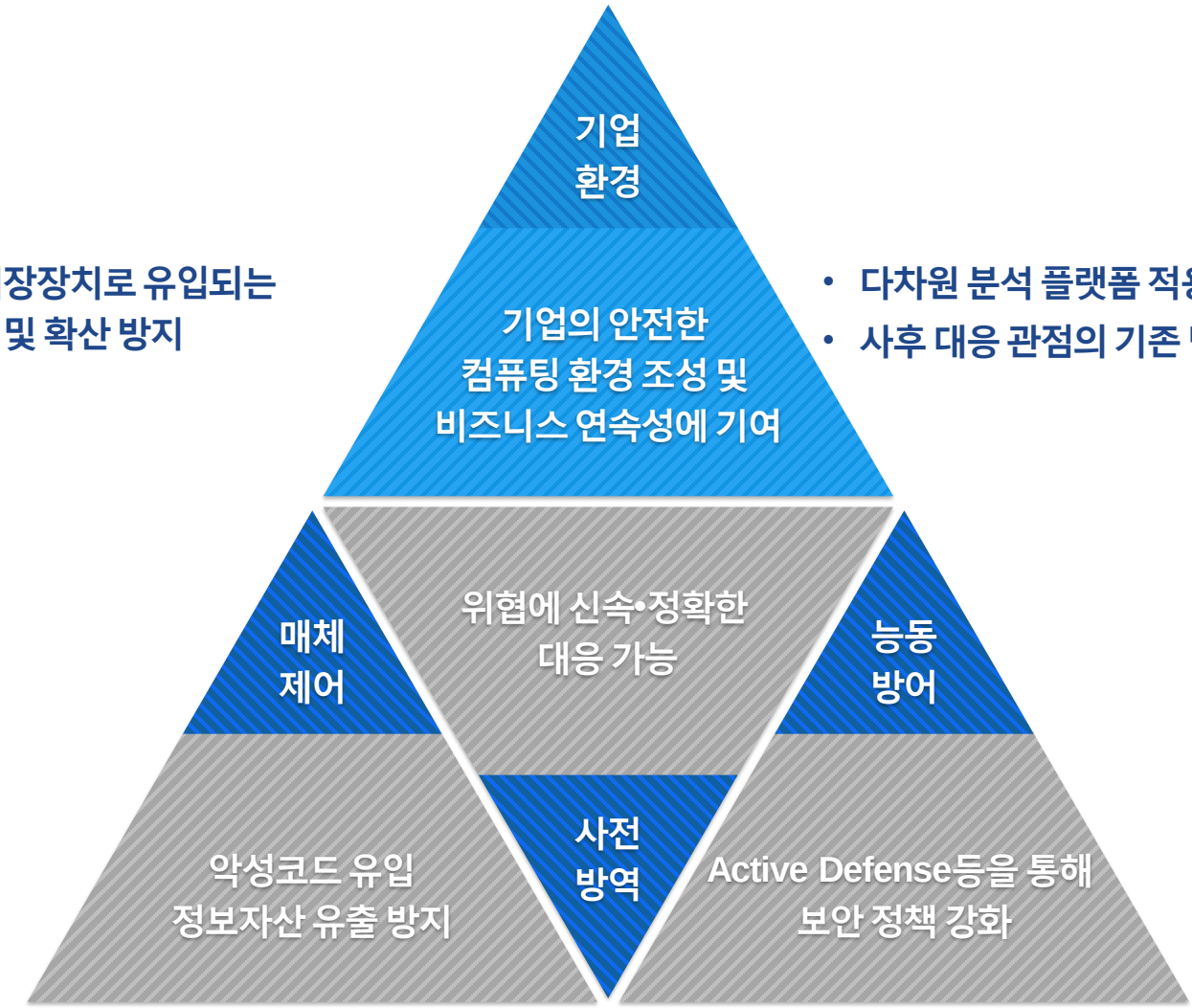
03.
도입 효과

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

AhnLab

V3 Endpoint Security 9.0 도입 효과(1)

- 각종 이동형 저장장치로 유입되는 악성코드 차단 및 확산 방지



- 다차원 분석 플랫폼 적용을 통한 사전 방역
- 사후 대응 관점의 기존 방식 한계를 극복

- 한층 강력해진 기능으로 체계적이고 능동적인 대응 체계 구축

V3 Endpoint Security 9.0 도입 효과(2)

사용자 관점의
탁월한 편의성 구현

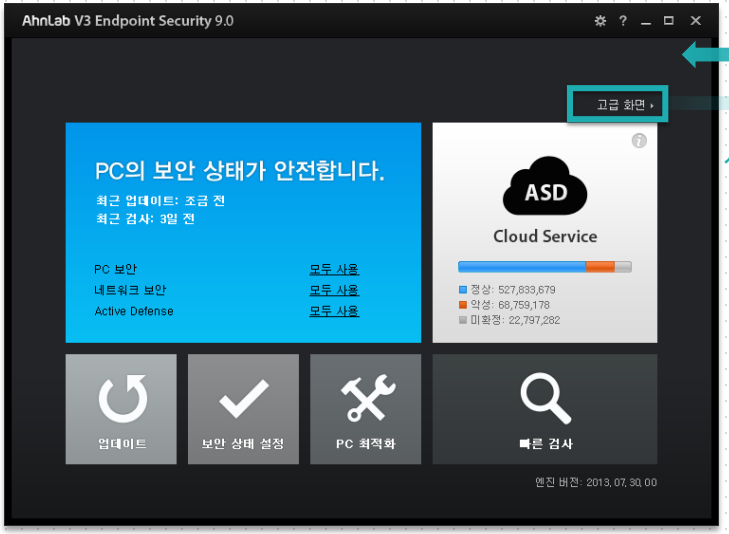
메인 화면과
보안 센터를 통해
한눈에 보안 상태 확인

신속하고
능동적인 대응 가능

옵션 단순화,
가능한 자동 수행 처리

메인 화면

빠른 검사와 PC최적화 등 일반 사용자 중심의 간편한 구성



사용자가 원하는 모드로 설정
편의성 극대화

보안 센터

PC상태에 대한 상세한 내용 확인 및 세부적인 옵션 설정

V3 Endpoint Security 9.0 도입 효과(3)

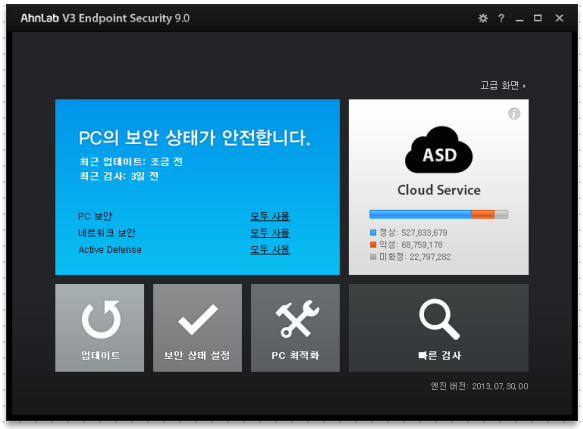
컬러 변화만으로
직관적인 PC 상태 확인

메인 UI 에서
프로세스 진행
(검사/최적화 등)

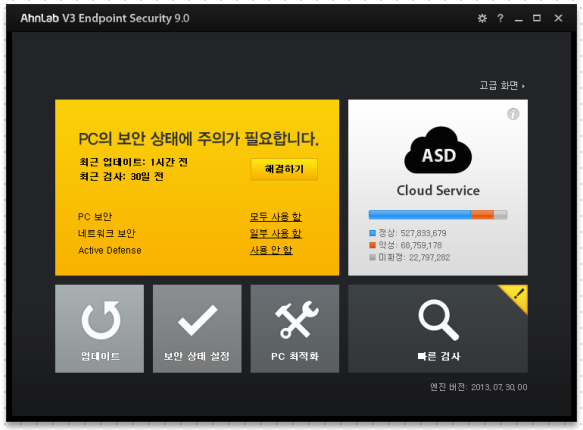
메뉴 Depth 최소화,
직관적인 인터페이스

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

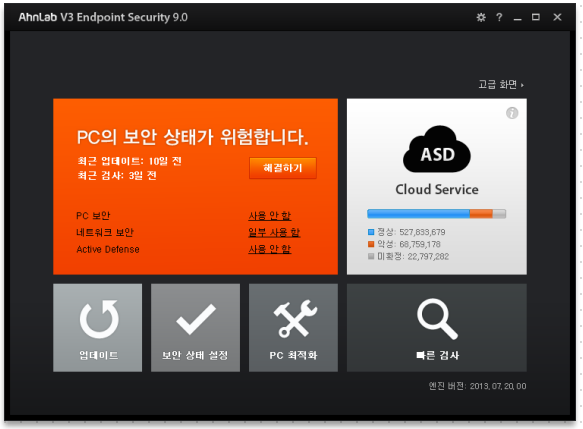
안전



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 조성과 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.

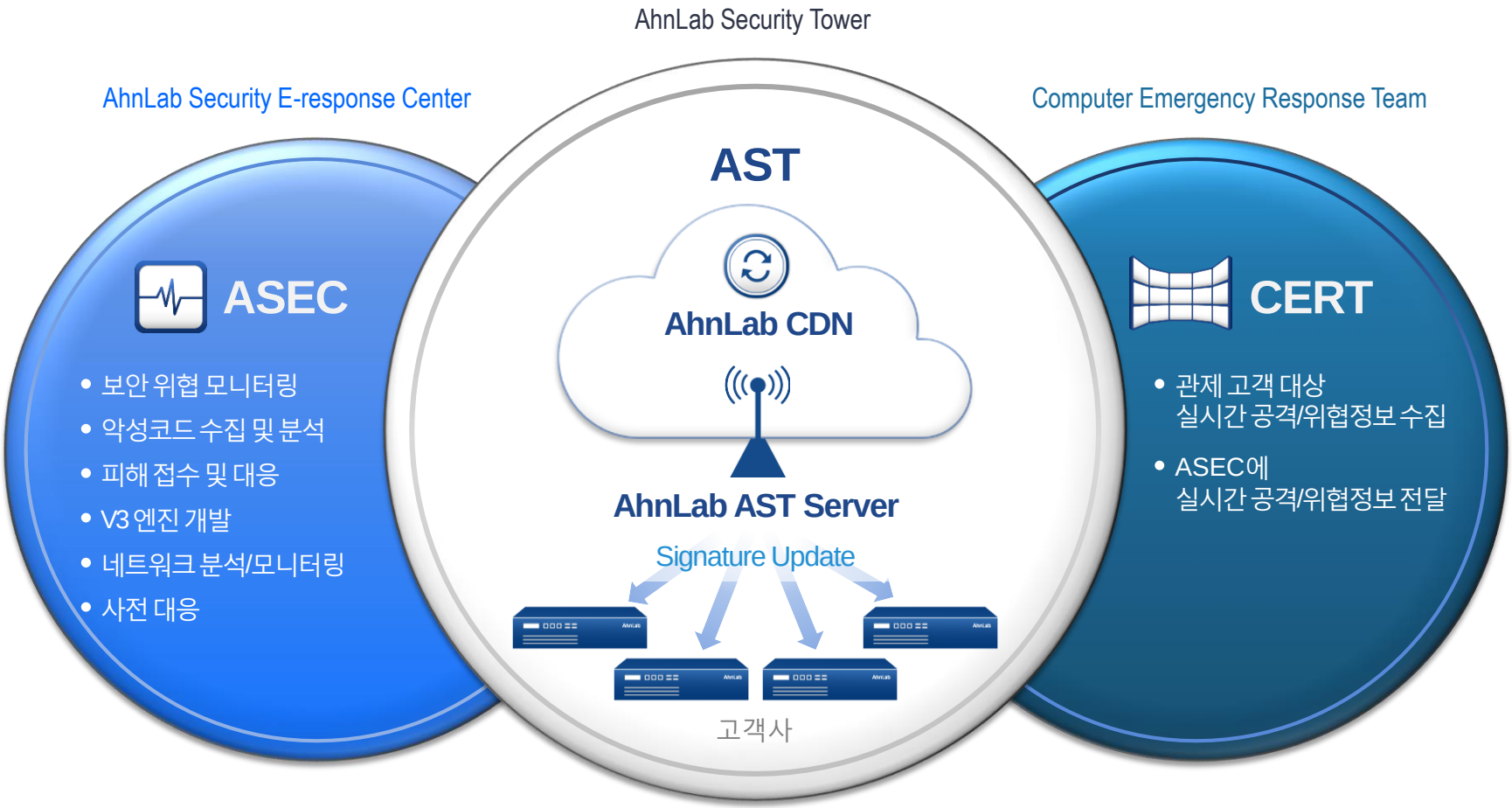
1995년 회사가 설립된 이후 다양한 레퍼런스를 통해 경험을 쌓았습니다.
다양한 기업 환경에서 발생하는 위협을 정확하게 진단해내고 있으며 적절한 대응 방안을 제시하고 있습니다.

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

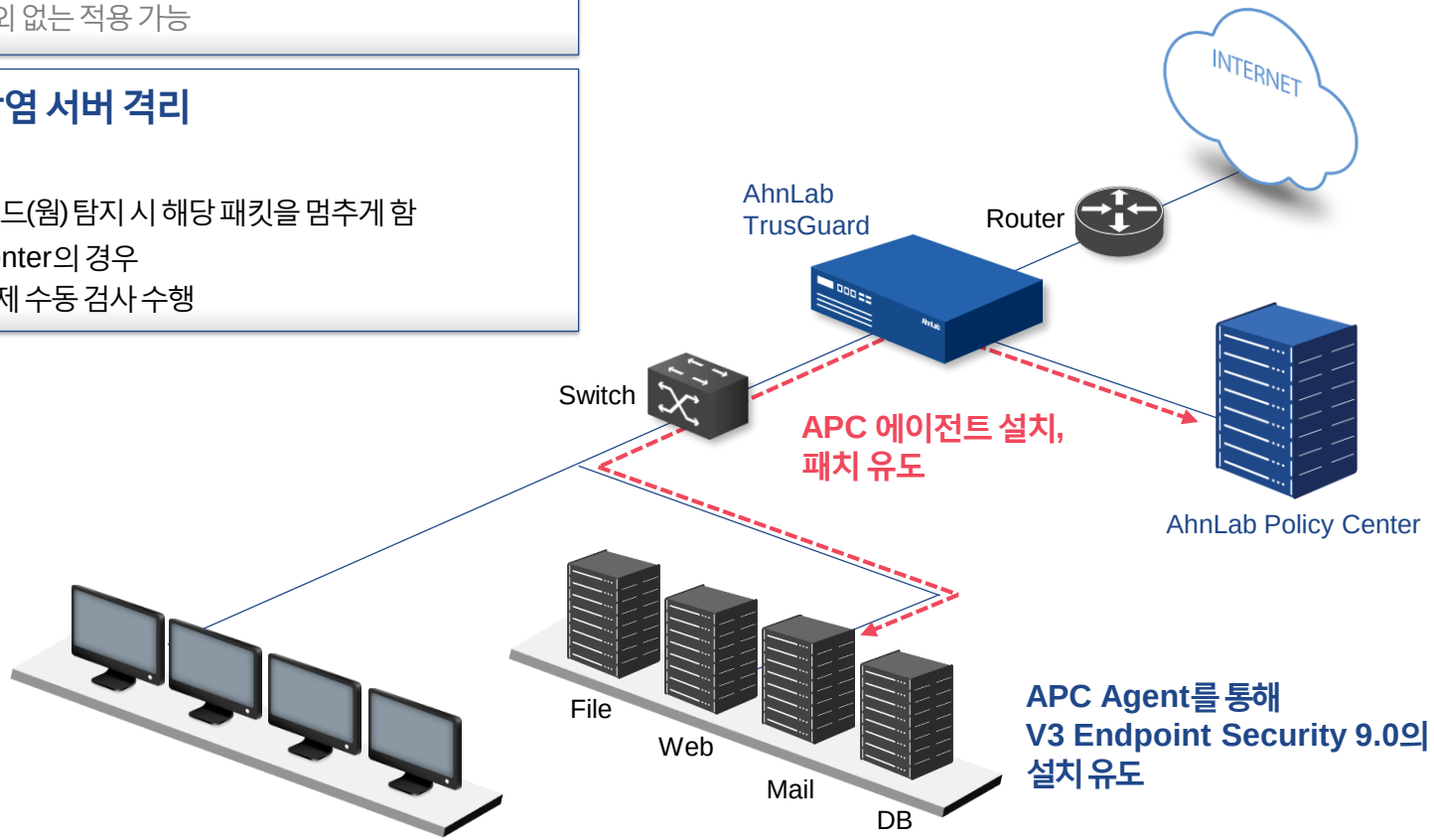
- APC 에이전트 미 설치 PC와 서버의 외부 인터넷 접근 차단
- 에이전트 설치 유도 화면으로 Redirection
- PC와 서버에 APC 에이전트 설치를 유도
  - 보안 정책의 전사 예외 없는 적용 가능

악성코드(웜) 감염 서버 격리

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

API 제공을 통한 관리 솔루션 연계

- 자체적으로 사용하는 보안 관리 솔루션의 경우
- V3 ES 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 Endpoint Security 9.0에 적용된 다차원 분석 플랫폼은 6가지 핵심 탐지 기술이 있어 빠르고 정확한 악성코드 분석은 물론 아직 알려지지 않은(제로데이) 신•변종 악성코드까지 진단합니다.

2. 클라우드 탐지(ASD)

- 약 7억여 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

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

URL/IP 탐지

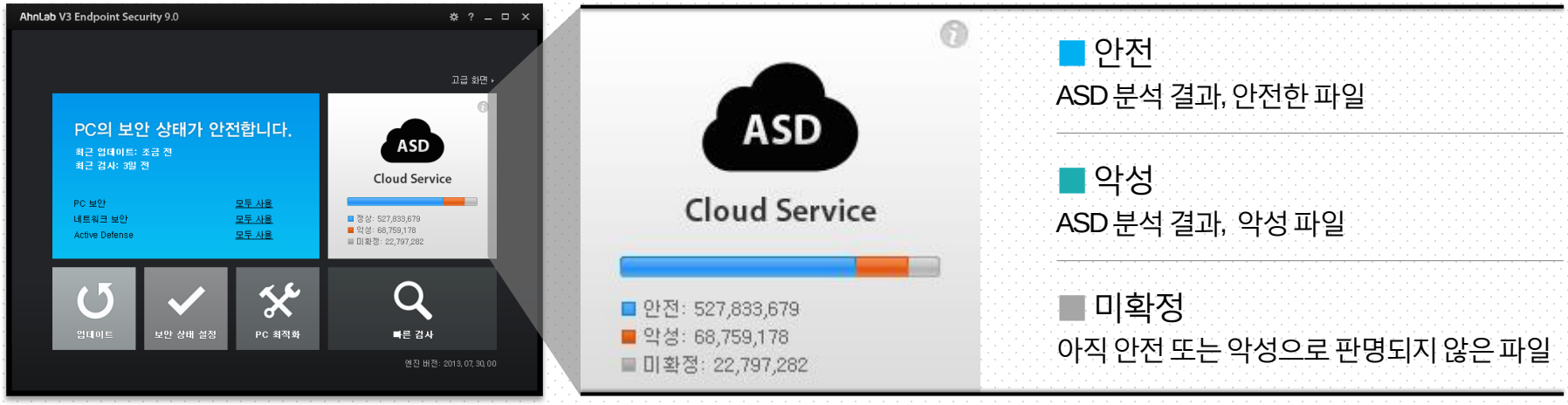
ASD 네트워크를 통해 축적된 웹사이트 및 IP 정보를 통해 악성코드를 유포하는 웹사이트 및 IP로의 접근을 차단하는 기능입니다.
사용자가 웹사이트를 방문할 경우, 이 과정에서 요청되는 모든 URL을 ASD에 질의해 악성으로 판별되면 곧바로 URL 접속을 차단합니다.
또한 웹사이트의 취약점을 통해 유입되는 행위 발견 시, 해당 URL을 ASD에 보고해 악성 행위에 대해 검증, 갱신 업데이트를 진행합니다.

기 능	종 류	내 용
악성 웹사이트 차단	악성URL	홈페이지 변조를 통해 악성 파일을 다운로드 하게 하는 중간 단계의 URL
		최종 악성 파일 (PE)를 다운로드 하는 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.



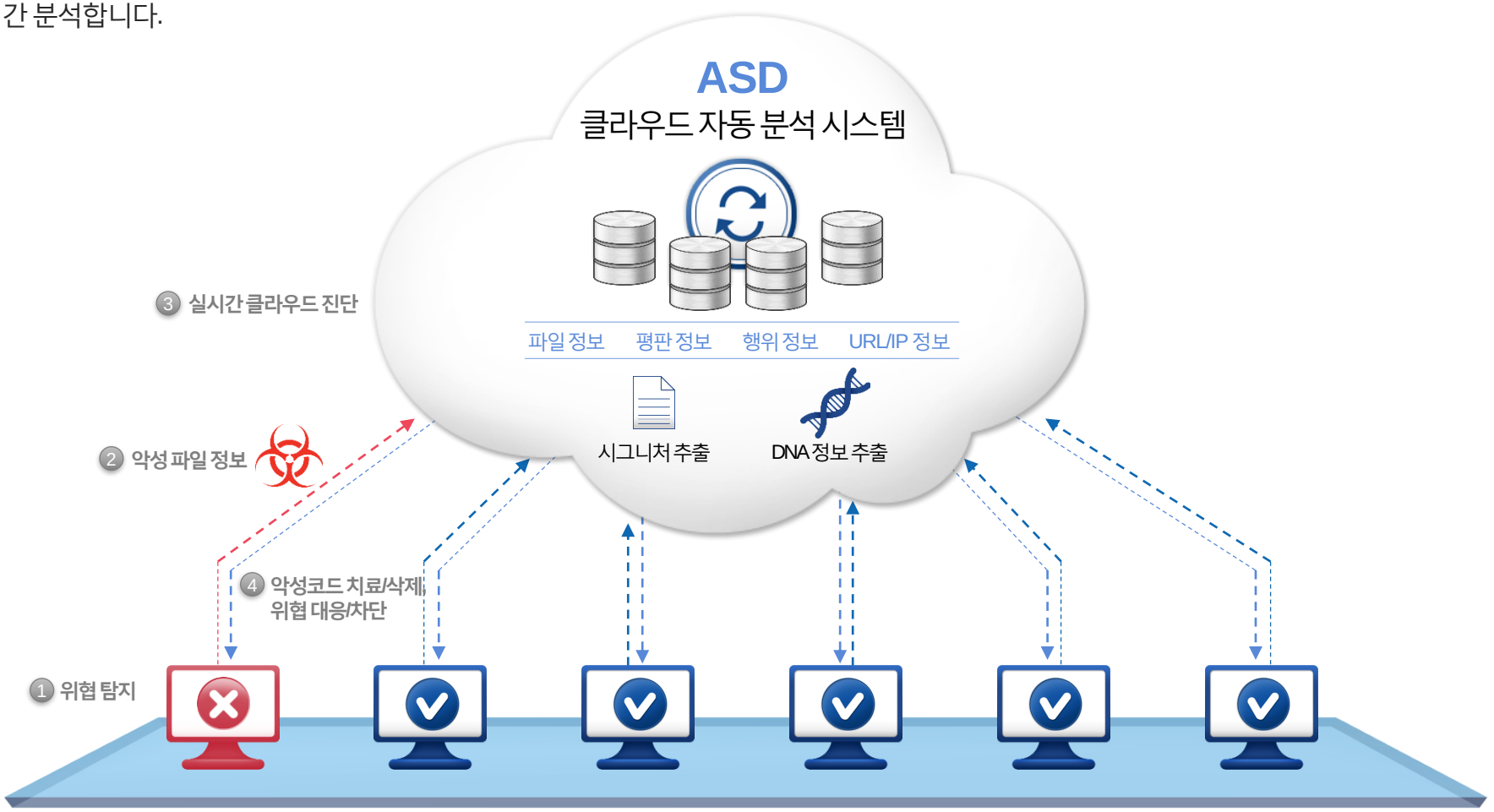
2013. 07. 현재 ASD 보유 DB

700,000,000 (약 7억 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)

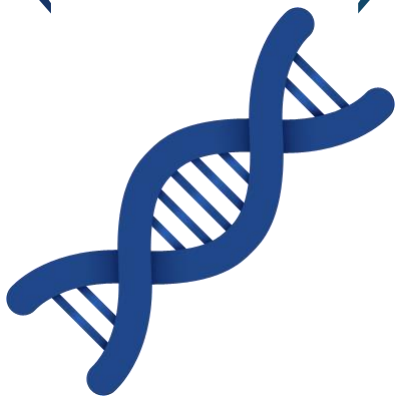
DNA Scan(TS Prime엔진) 기술

DNA 스캔(Scan)은ASD DB에 보유하고 있는 7억 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**

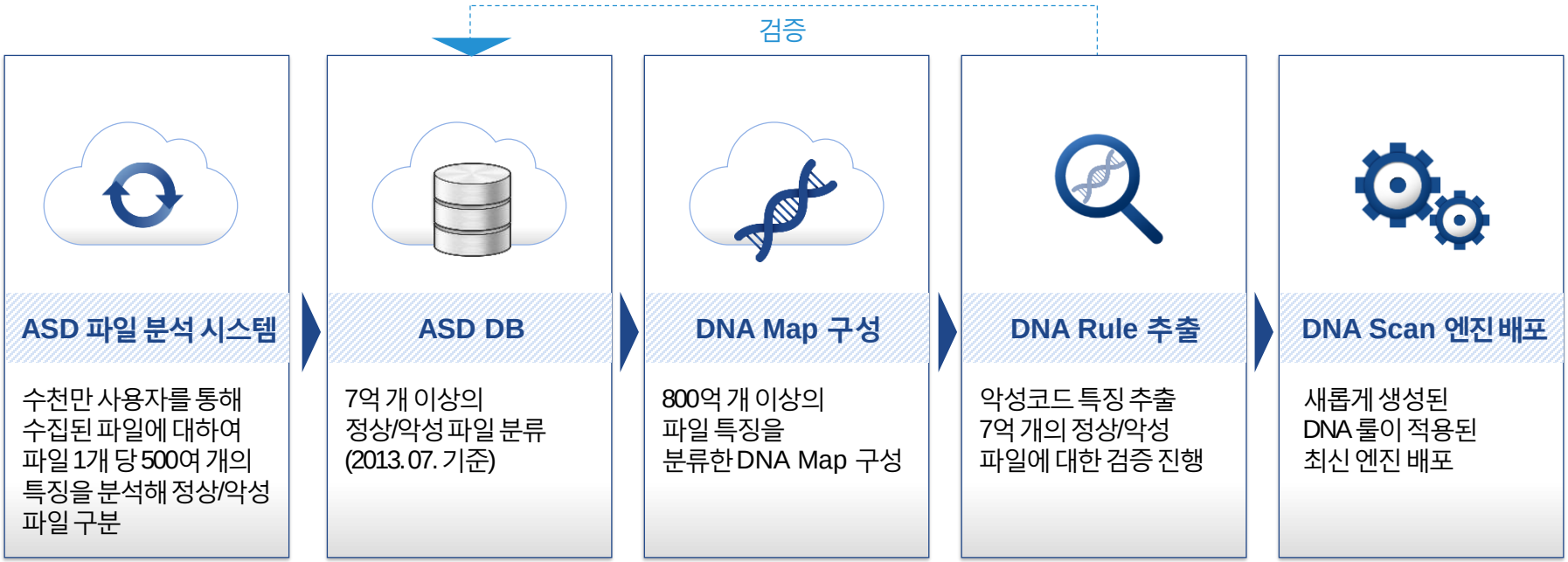
- 타 프로그램 감염
- 특정 정보 전송
- 은폐, 자동 실행

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 20여년 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.

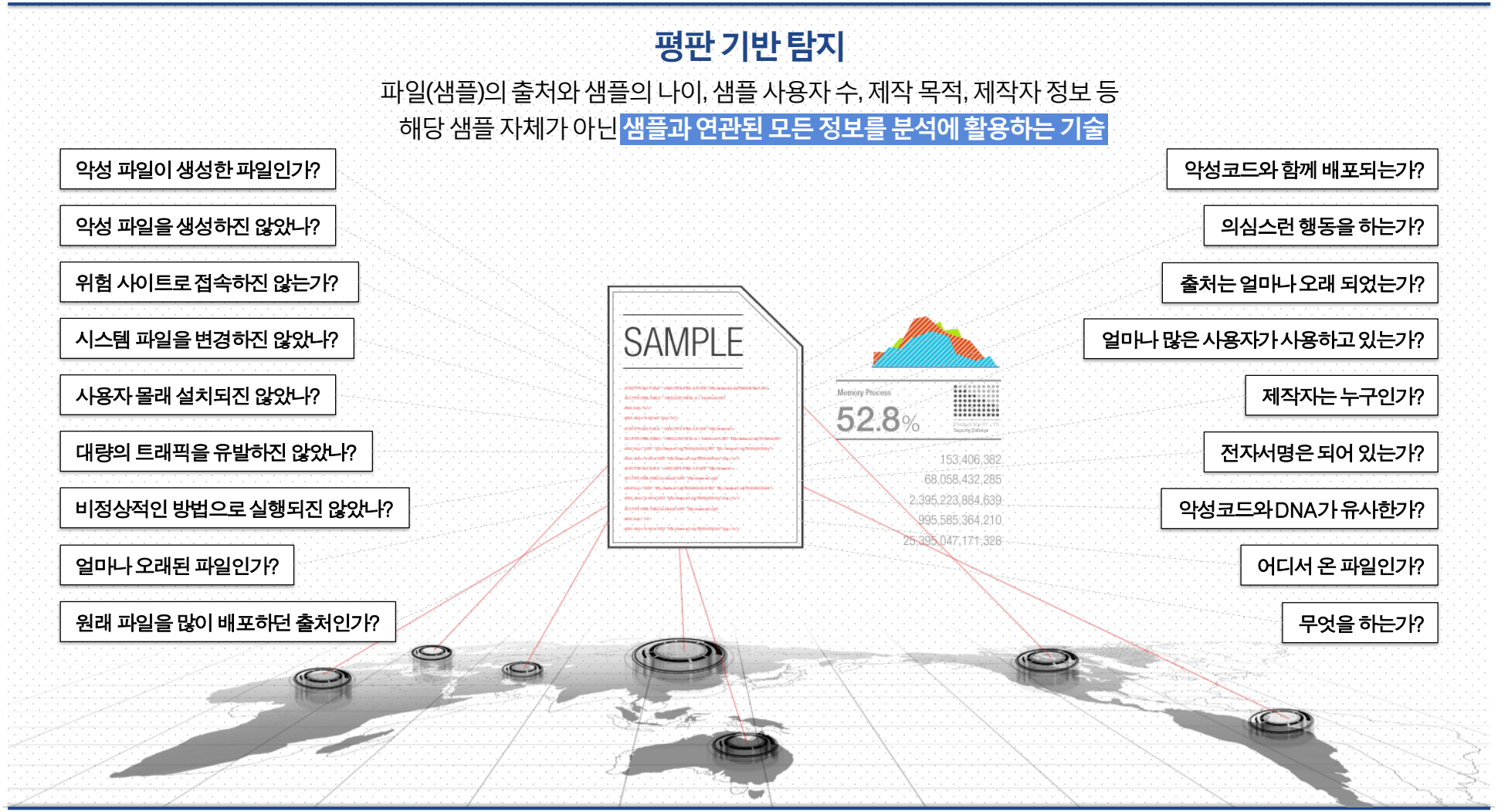
- 네트워크 쿼리 없이 엔진 형태로 제공되는 독보적 휴리스틱 진단 제공
  → 완전 폐쇄망 지원(TS Prime 엔진과 함께 제공)

- 분석가의 경험에 의존적인 일반 휴리스틱 진단법과 달리,
  ASD 네트워크에 접속하는 수천만 명 사용자 기반의 7억 개 이상의 파일에 대한 검증 후 엔진 반영
  → 타사 대비 휴리스틱 진단법 오진 확률 최소화



평판 기반 탐지(1)

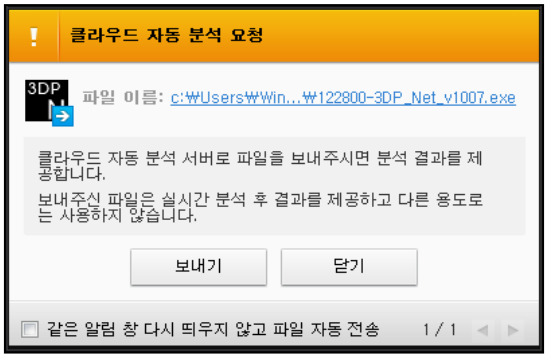
평판 기반 기술은 기본적으로 평판이 낮은(=평판이 좋지 않은) 프로그램을 통제하는 데에 활용됩니다.
새로 만들어진 악성코드는 제작자가 불분명하고 출처가 불확실하며, 사용자가 거의 없기 때문에 평판이 낮을 수 밖에 없습니다.
기업에서 별도로 사용하고 있는 프로그램은 화이트리스트 처리하여 안정성을 확보 할 수 있습니다.



평판 기반 탐지(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

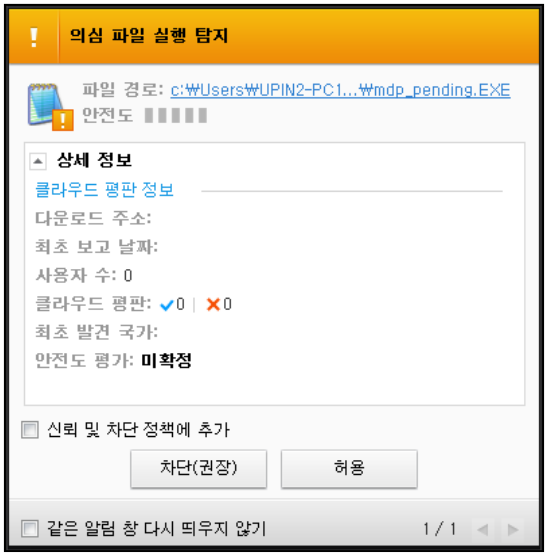


평판 기반 프로그램의 실행 차단

- 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)의 프로그램
  * 100여 개의 의심 행위에 대한 탐지를 실시함

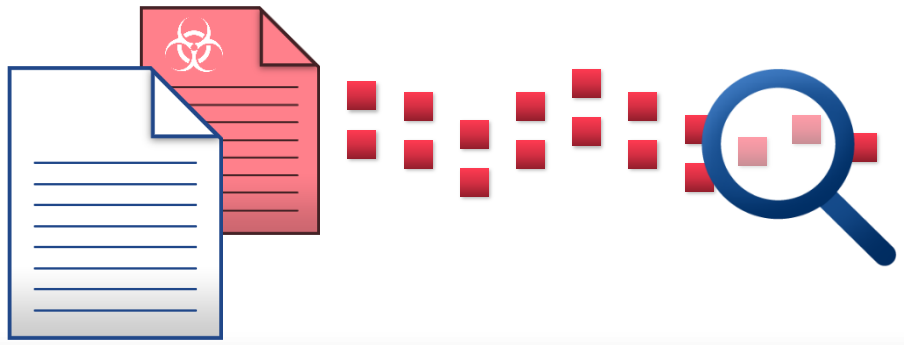


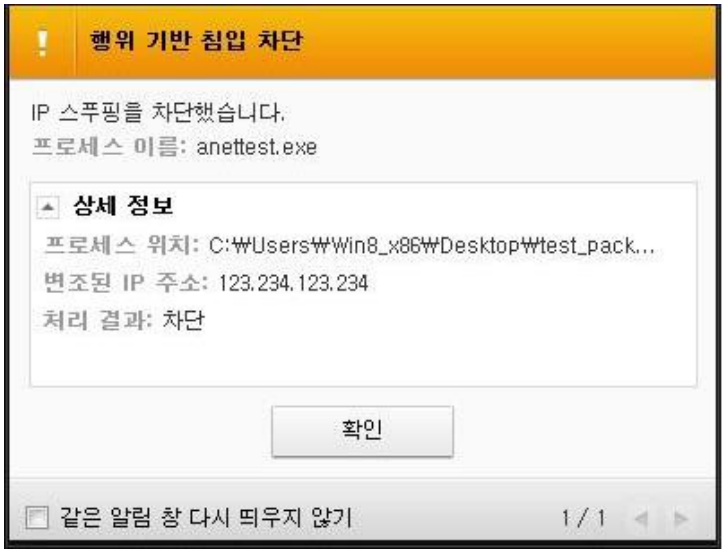
행위 기반 탐지

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 스푸핑,
Mac 스푸핑, ARP 스푸핑 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.

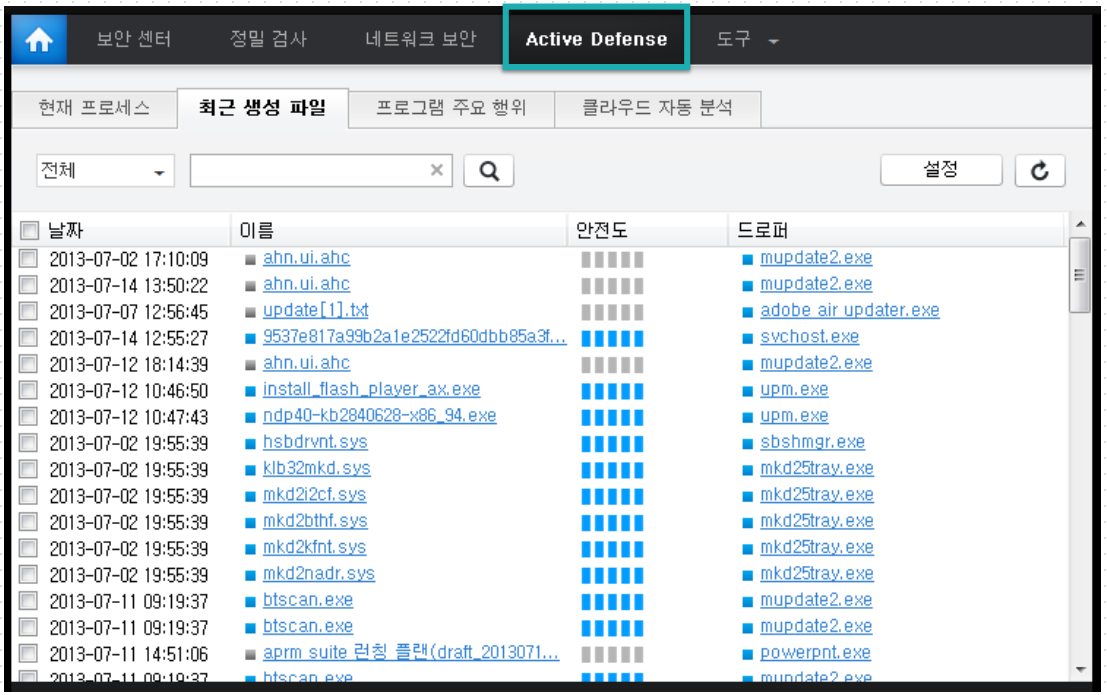




액티브 디펜스(Active Defense)

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(1)

Anti-Virus/ Anti-Spyware	• 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(사용자 예약 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
네트워크 보안	• 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
매체제어	• USB 저장장치, 유•무선 네트워크, 디스크 드라이브, 모뎀 등 관리 가능 • IEEE1394(FireWine), PCNCIA 어댑터, 적외선 장치, 블루투스 장치, COM/LPT 포트 등

주요 기능(2)

보안센터	• 해결하기 기능 지원 • 네트워크 보안 상태 확인(현재 PC의 방화벽 차단, IPS 차단, 웹사이트 검사, 웹사이트 차단 건수 확인) • 클라우드 보안(파일 검사 수, 악성 파일 차단 건 수 확인) • 시그니처 보안(시그니처 수, 파일 검사 수) • 평판 기반 실행 차단(의심 파일 실행 탐지 건 수, 허용/차단 건 수 확인) • 행위 기반 진단(악성 행위 차단 건 수 확인) • Active Defense(미확정 파일 건 수, 사용자 차단 건 수, 사용자 미처리 건 수 확인)
웹 보안	• 피싱 URL 차단 • 불필요한 웹사이트(PUS) 차단 사용
PC 도구	• PC 최적화(레지스트리 , 인터넷 익스플로러, 시스템, 프로그램, 윈도우 탐색기 청소) • PC 관리(프로그램 관리, ActiveX 관리, 툴바 관리) • 파일 완전 삭제 • 로그/검역소(이벤트 로그, 진단 로그, 검역소)
업데이트 & 패치	• 최신 업데이트 파일 및 패치 파일 존재 여부 확인 • 스마트 업데이트를 이용한 업데이트 및 패치 제공 • 로그오프 시에도 자동 업데이트 가능 • 업데이트 주기 확인 후 PC상태 표시
Active Defense	• 동작중인 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 Endpoint 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	O	O	X	O	O	O	O	O	X
압축파일 검사	O	O	O	O	O	O	O	O	O
신.변종 악성코드 분석	O	O	O	O	O	O	O	O	O
감염되기 쉬운 파일 검사	O	O	O	O	O	O	X	O	X
EML 파일 검사	O	O	O	O	O	O	O	O	O
CD/USB 자동실행 방지	O	O	O	O	O	O	X	X	X
휴리스틱 진단	O	O	O	O	O	O	O	O	O
PUP 검사	O	O	O	O	O	O	O	O	X
평판 기반 차단	X	O	X	X	O	O	X	O	X
클라우드 자동 분석	X	O	X	X	O	O	O	O	X
매체제어	X	O	X	O	O	O	X	X	X
Active Defense	X	O	X	X	X	X	X	X	X
빠른 검사(Smart Scan)	X	O	X	O	O	O	O	O	X
현황판(Dashboard)	X	O	X	X	X	X	O	X	X
다운로드 파일 평판 분석	X	O	X	X	X	X	X	O	X
HIPS(스푸핑)	X	O	X	X	X	O	O	O	O
Stable 엔진 사용 기능	O	O	X	X	X	X	X	X	X

시스템 요구 사항

1. 하드웨어 요구 사항

구분	시스템 요구사항
CPU	Intel Pentium 4 1GHz 이상
메 모 리	512MB 이상
HDD	300MB 이상의 여유 공간
지원 언어	한국어, 영어
매체제어	APC (4.0/ 4.6) /APC Appliance /AhnLab EMS 연동 시

2. 소프트웨어 요구 사항

제품명	운영 체제
AhnLab V3 Endpoint 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

AhnLab
V3 Endpoint Security 9.0

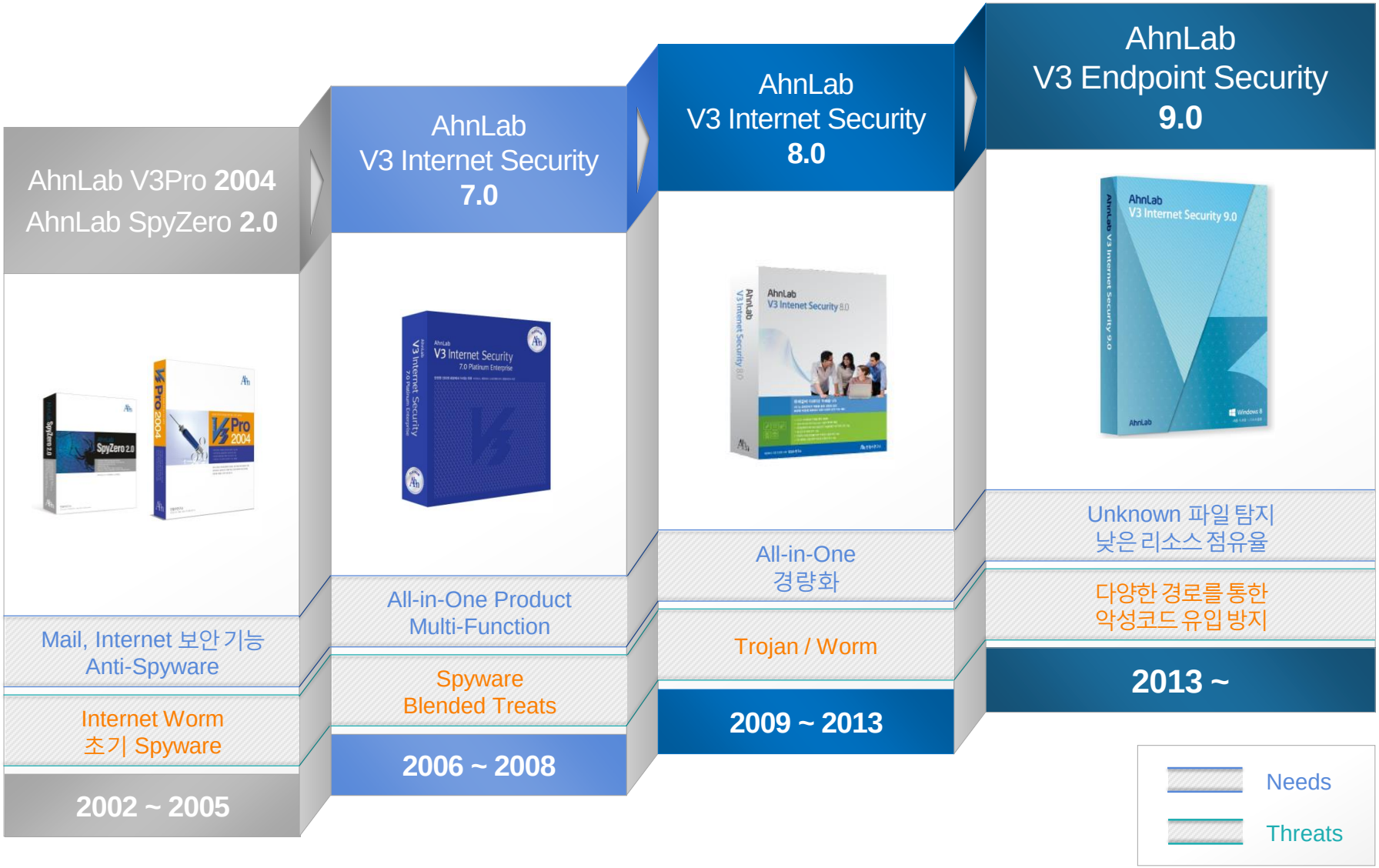
별첨

제품 연혁

AhnLab

※ 별첨

V3 Internet Security 제품 연혁



※ 별첨

V3 Endpoint Security 제품 연혁

- **2013. 07.** **V3 Endpoint Security 9.0**
- **2013. 07.** **V3 Internet Security 9.0**
- 2010. 03. V3 Internet Security 8.0 GS 인증
- 2009.12. V3 Internet Security 8.0 CC 인증
- 2009. 04. V3 Internet Security 8.0
- 2008.11. V3 Internet Security 7.0 Platinum Enterprise SP1
- 2006. 07. V3 Internet Security 7.0 Platinum Enterprise
- 2004. 03. V3Pro 2004
- 2001.11. V3Pro 2002 Deluxe
- 1999. 09. V3Pro 2000 Deluxe
- 1998. 04. V3Pro 98 Deluxe
- 1997. 03. V3Pro 97
- 1996. 03. V3Pro 95
- 1995.12. V3Pro

More security,
More freedom

㈜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
V3 Endpoint Security 9.0

AhnLab