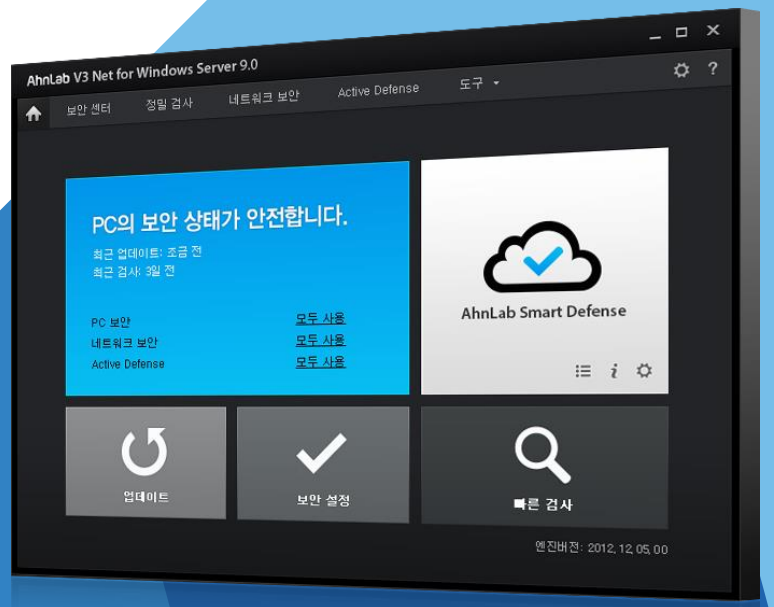
AhnLab

V3 Net for Windows Server 9.0

More security,
More freedom

안정적 서버 운용을 위한 최고의 보안 파트너

표준제안서



AhnLab

AhnLab ENDPOINT SECURITY SOLUTION

Contents

AhnLab
V3 Net for Windows Server 9.0

AhnLab

01.
제안 배경

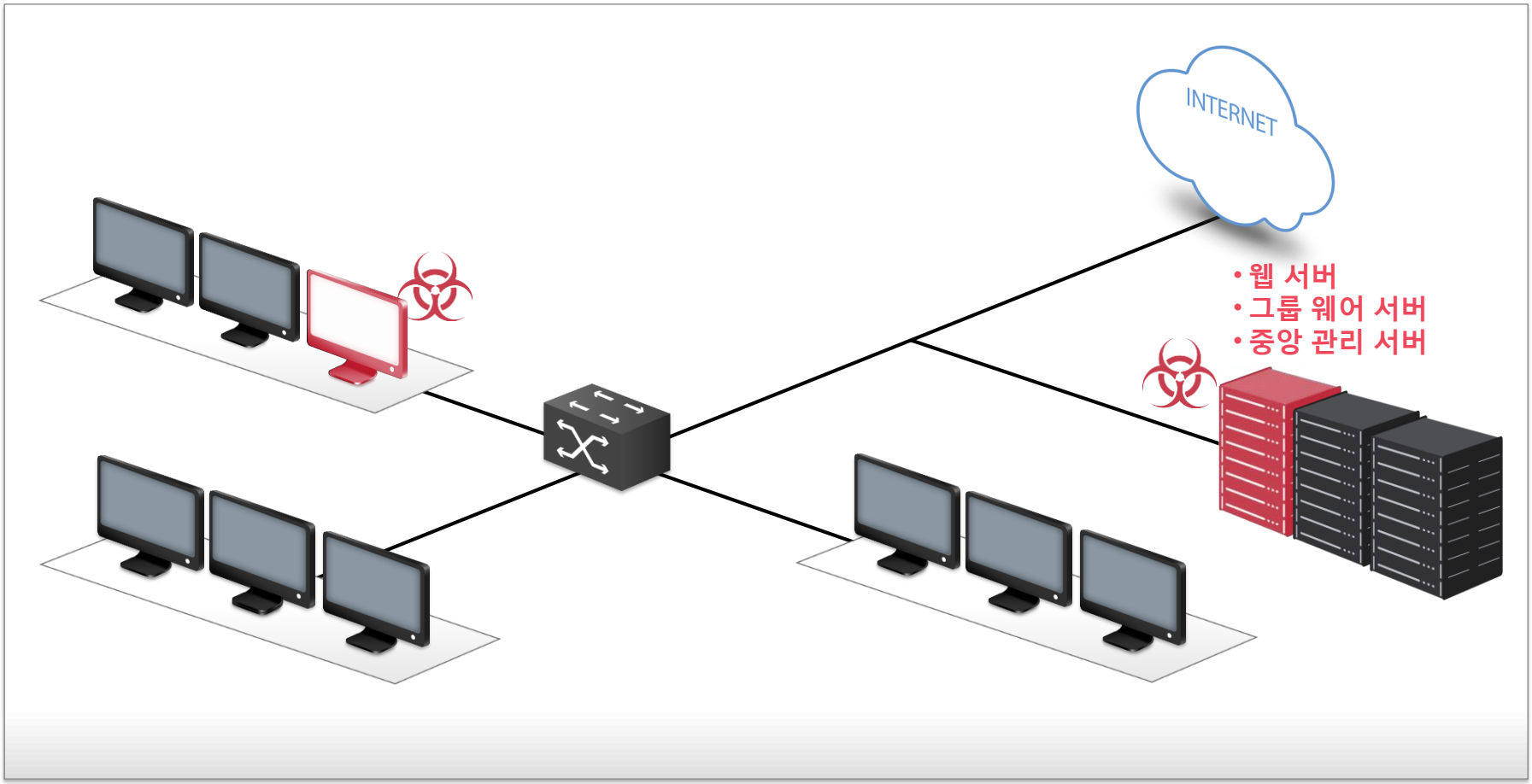
1. 주요 공격 타깃이 된 서버
2. 서버 방역의 중요성
3. 악성코드 위협의 고도화까지
4. 전략적인 서버 방역의 필요성 대두

주요 공격 타깃이 된 서버

최근 기업 서버를 노리는 악성코드 유포가 크게 늘었습니다. 중요한 업무용 데이터들이 집중돼 있는 서버는 악성코드의 공격 목표가 되기 쉬울 수밖에 없습니다.

- 상대적으로 보안이 취약한 서버에 대한 공격 증가
- DB 서버, 웹 서버 등이 내부망 장악의 경로로 이용

- 2011년 N사 금융기관 전산망 사고
- 2013년 3월 네덜란드 웹 호스팅 업체의 서버를 경유한 대규모 DDoS 공격 발생



서버 방역의 중요성

기업의 서버가 감염될 경우 전사적인 피해가 야기될 수 있습니다.

서버의 보안 취약점을 방치할 경우 서버에 저장돼 있는 데이터의 파괴와 유출로 연쇄 사이버 위협이 발생할 수 있습니다.

- 네트워크와 연결된 내부망 PC로 급속한 피해 확산, 비즈니스 중단
- 서버 감염으로 인한 정보 유출

서버가 악성코드에 감염되었을 경우의 피해는 클라이언트 PC와 같을 수 없습니다.

서버, 중요 포인트

- 중요한 정보의 관리와 공유를 위해 파일 서버 사용
- 파일 서버는 기업의 정보가 모이고 흩어지는 중요한 포인트에 위치

안전성 중요

- 수많은 PC가 네트워크에 유입/유출되는 상황
- 서버에 접속하는 모든 클라이언트 PC가 안전하다고 판단하기 어려움

기업 생산성에도 직결

- 서버 대책은 기업의 생산성과 직결
- 피해 야기 시 기업의 자산을 효율적으로 보호/서비스 연속성을 보장하기 어려움

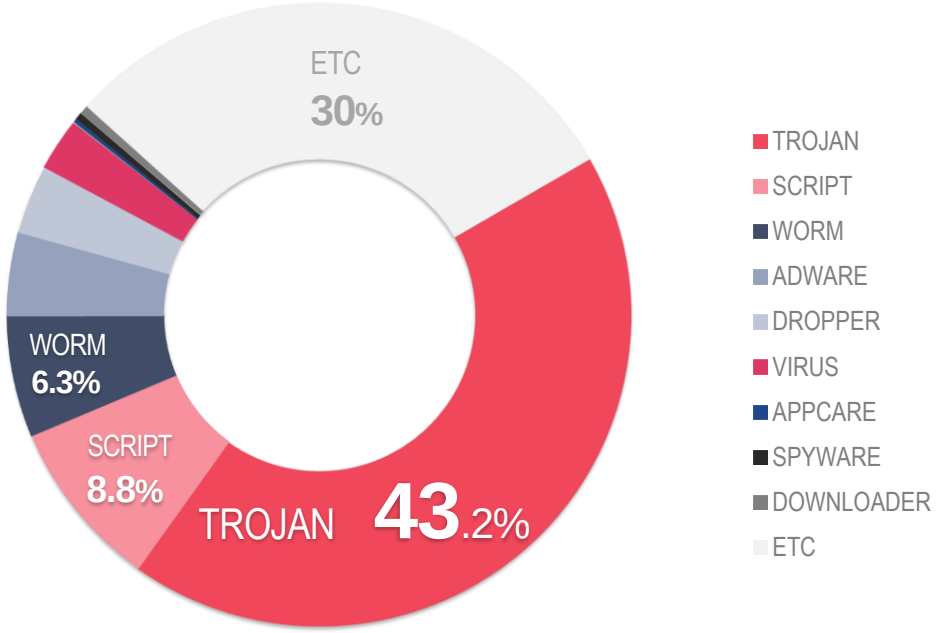
악성코드 위협의 고도화까지

특히 2012년에는 악성코드 중 '트로이목마(Trojan)'가 43.2%를 차지, 최다를 기록했으며 주로 잠복/은폐한 형태로 유입돼 계정 정보를 유출하는 데에 사용됐습니다.

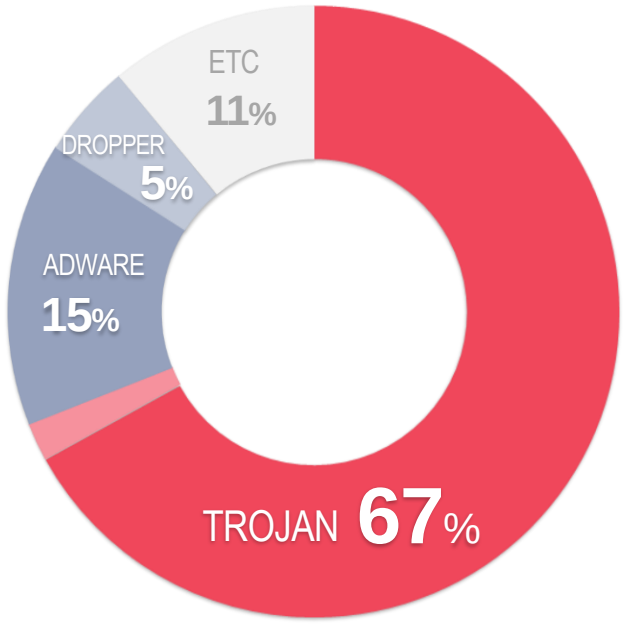
주요 악성코드 유형

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

전략적인 서버 방역의 필요성 대두

다차원 분석 기반 안정적 서버를 위한 최고의 파트너

V3 Net for Windows Server 9.0

서버 방역에 최적화	사전 방역으로 안전한 업무 환경 구축	전사적 보안 정책 수립
서버 관리/활용 극대화	신•변종 악성코드 대응	관리 솔루션 연동 가능

서버 겨냥한 타깃 공격 급증

- 위협 인지 및 방역 어려움
- 업무/비즈니스 마비

악성코드 증가 및 고도화

- 은폐/0-day 취약점
- 사전 탐지/대응 어려움

체계적이고 전문적인 관리 시스템 부재

- 관리 시스템/인력 부족
- 실시간 대응에 취약

02.
제품 개요

AhnLab

V3 Net for Windows Server 9.0 소개

V3 Net for Windows Server 9.0은 다양한 기능을 통해 기업의 정보 자산 보호가 가능하며 특히 다차원 분석 플랫폼이 적용돼 사전 방역과 서버 운영에 효과적입니다.

AhnLab V3 Net for Windows Server 9.0

안정적 서버 운용을 위한 최고의 보안 파트너

다차원 분석 플랫폼 기반의 차별적인 서버 방역

- 다차원 분석 플랫폼 기반의 차별적인 방역(행위/평판, 악성 URL/IP 정보 활용)
- 클라우드 기반의 ASD로 정확한 진단 및 실시간 치료
- Active Defense 기능으로 위협에 대한 가시성 확보, 능동적인 대응 가능

서버 활용성 극대화를 위한 다양한 기능 제공

- 악성코드 등 위협 발생 시 관리자에게 알림 메일 발송
- 다양한 기업 환경에 최적화

스마트 스캔 기술로 신속•정확한 검사

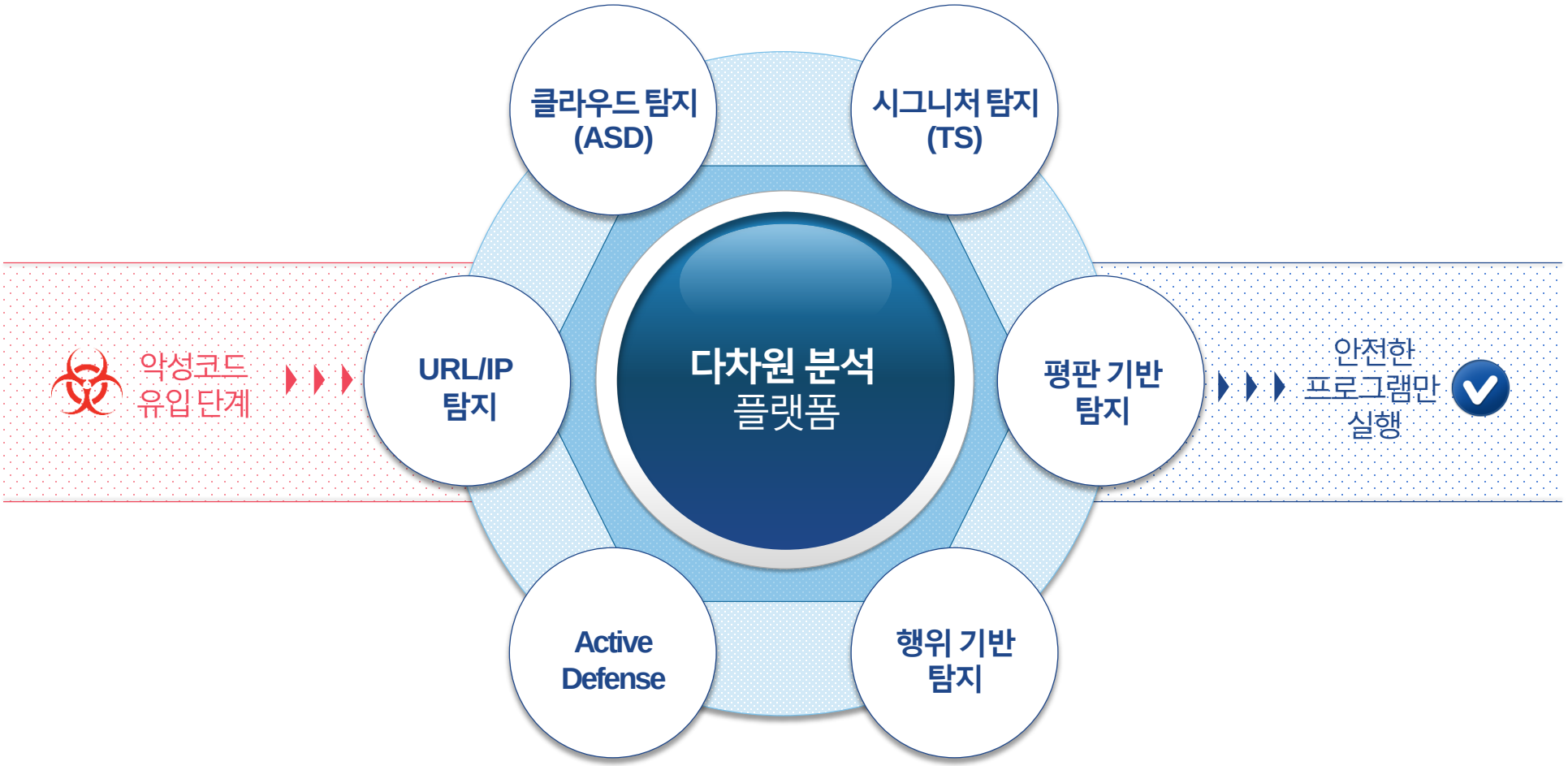
- 최초 1회 검사로 안정성 확보한 파일을 제외하고 검사하는 스마트 스캔(Smart Scan) 기술 적용
- 최대 6배 이상 빨라진 속도로 사용자 편의성 극대화

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 Net for Windows Server 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.



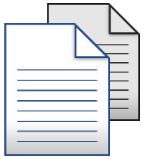
특장점

새로운 진단 기술

- **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

엔진 초경량화 기술 적용

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



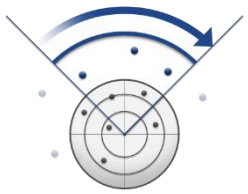
고급 정보 제공

- **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)

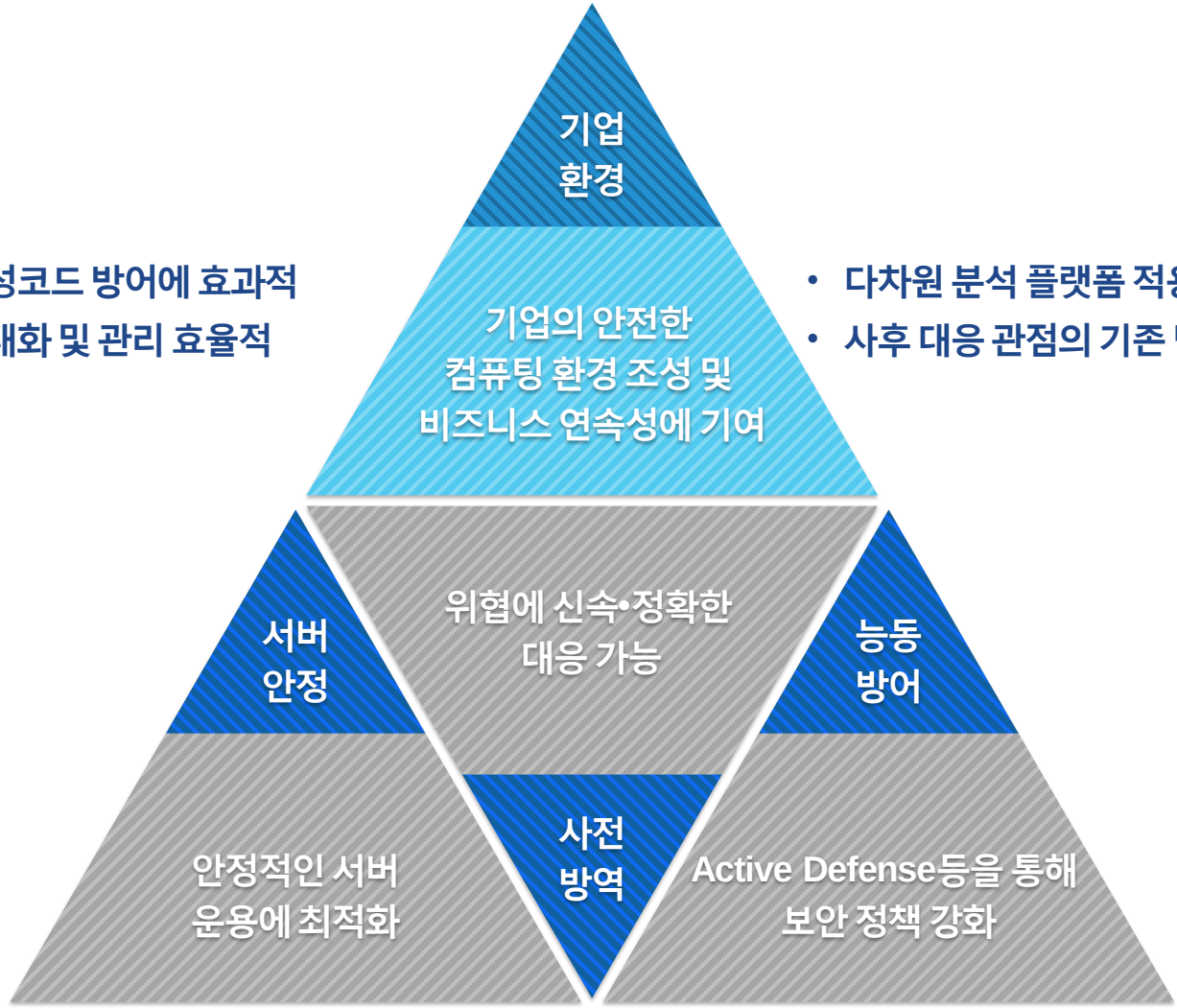
- **스마트 검사 기술 적용**
  - 새로운 파일, 변화된 파일만 검사해 검사 시간과 자원 점유를 단축하는 기술 적용 (수동 검사)
  - 최초 1회 검사는 비슷하나, 이후 6배 정도의 빠른 속도로 검사가 가능

03.
도입 효과

AhnLab

V3 Net for Windows Server 9.0 도입 효과(1)

- 서버 타깃의 악성코드 방어에 효과적
- 서버 활용성 극대화 및 관리 효율적



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

- 한층 강력해진 기능으로 체계적이고 능동적인 대응 체계 구축

V3 Net for Windows Server 9.0 도입 효과(2)

사용자 관점의
탁월한 편의성 구현

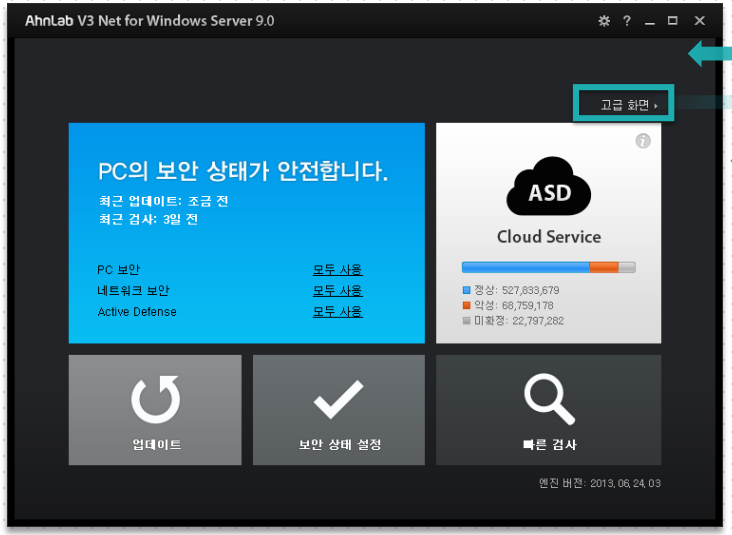
메인 화면과
보안 센터를 통해
한눈에 보안 상태 확인

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 Net for Windows Server 9.0 도입 효과(3)

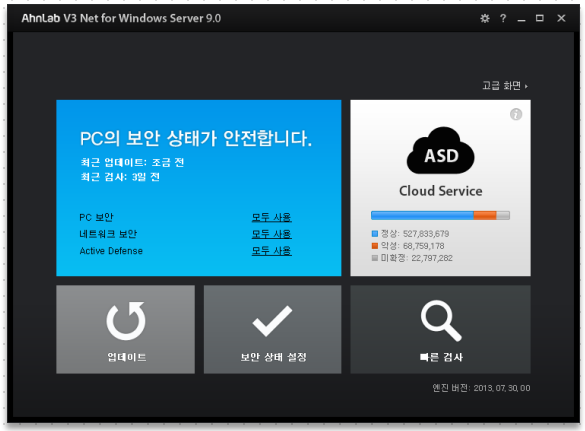
컬러 변화만으로
직관적인 PC 상태 확인

메인 UI 에서
프로세스 진행
(검사/최적화 등)

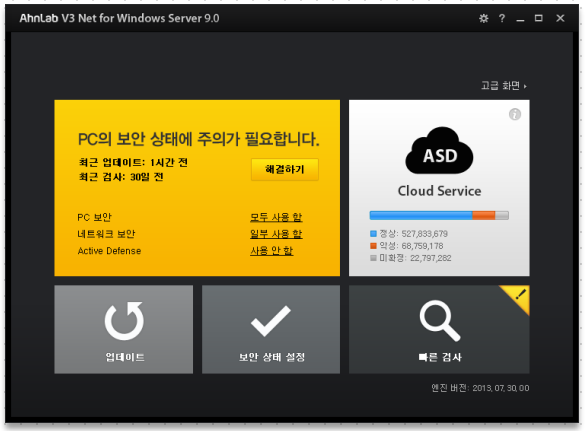
메뉴 Depth 최소화,
직관적인 인터페이스

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

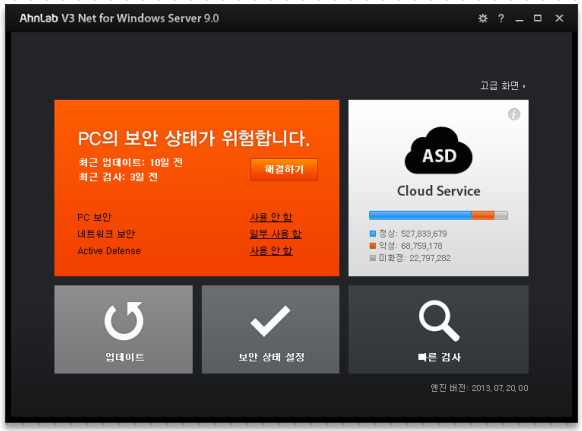
안전



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.

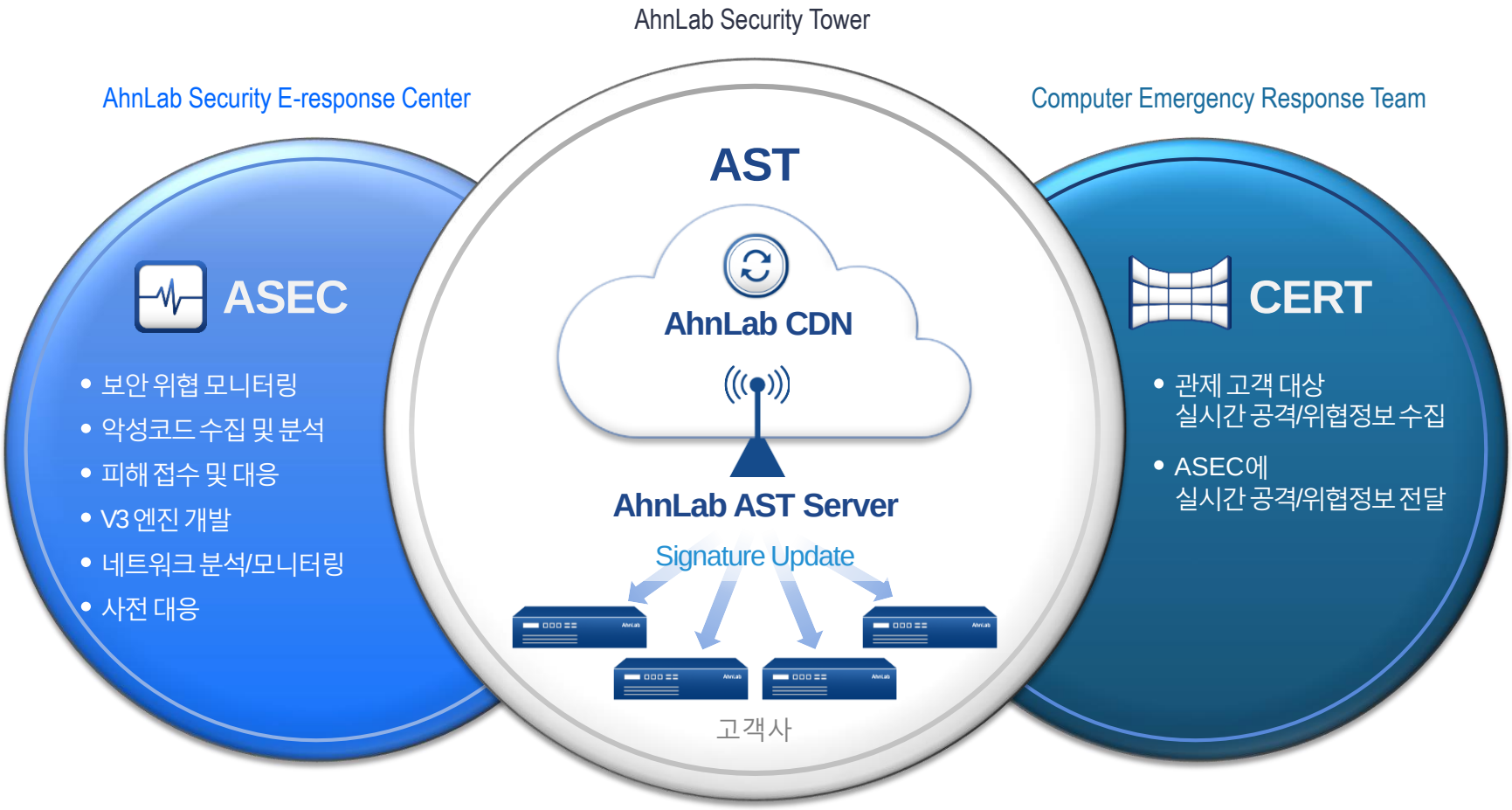
1995년 회사가 설립된 이후 다양한 레퍼런스를 통해 경험을 쌓았습니다.
다양한 기업 환경에서 발생하는 위협을 정확하게 진단해내고 있으며 적절한 대응 방안을 제시하고 있습니다.

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

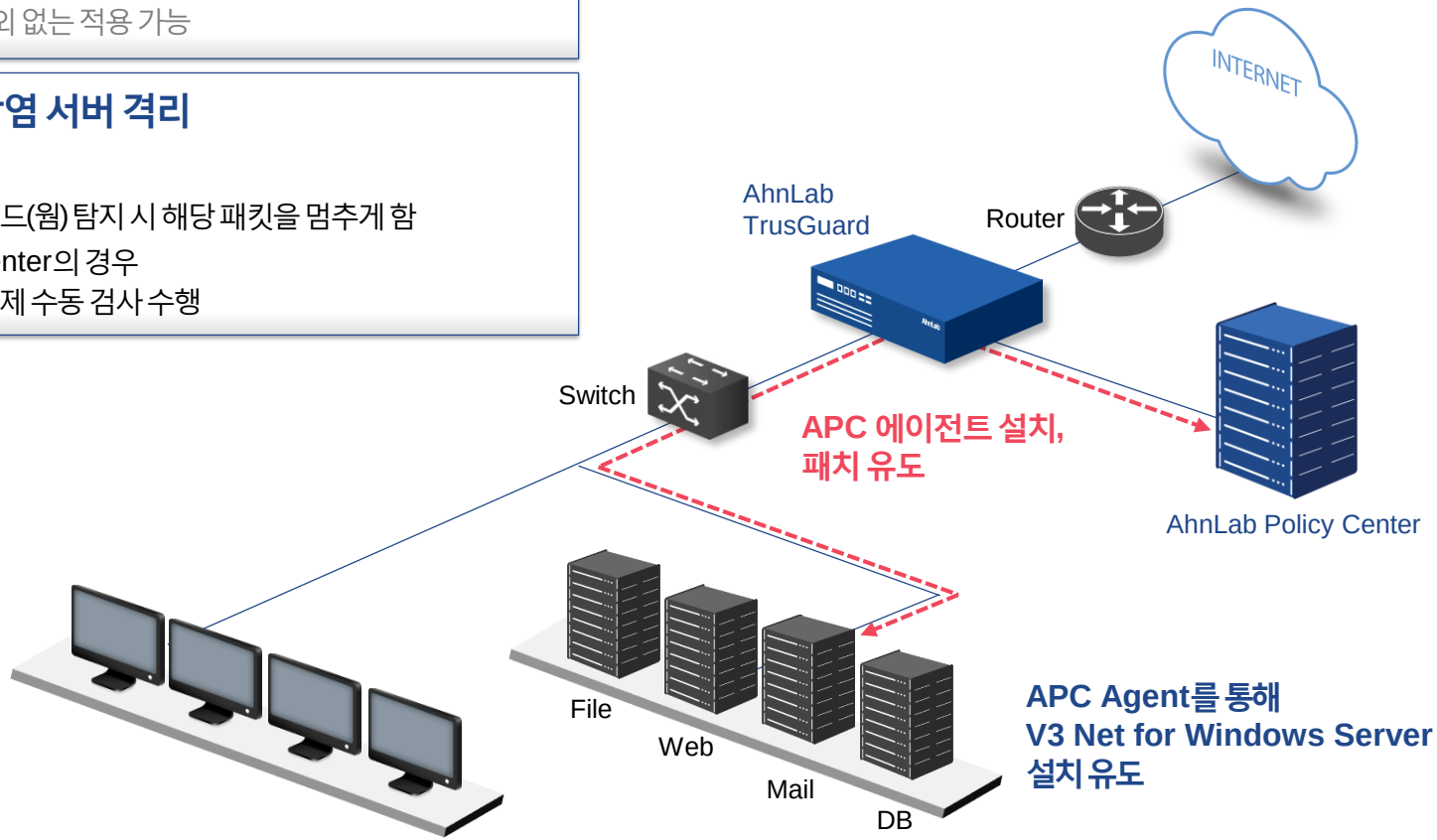
- APC 에이전트 미 설치 PC와 서버의 외부 인터넷 접근 차단
- 에이전트 설치 유도 화면으로 Redirection
- PC와 서버에 APC 에이전트 설치를 유도
  - 보안 정책의 전사 예외 없는 적용 가능

악성코드(웜) 감염 서버 격리

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

API 제공을 통한 관리 솔루션 연계

- 자체적으로 사용하는 보안 관리 솔루션의 경우
- V3 Net 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. 평판 기반 탐지
6. 행위 기반 탐지
7. 액티브 디펜스(Active Defense)

다차원 분석 플랫폼

V3 Net for Windows Server 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)

- 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

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

URL/IP 탐지

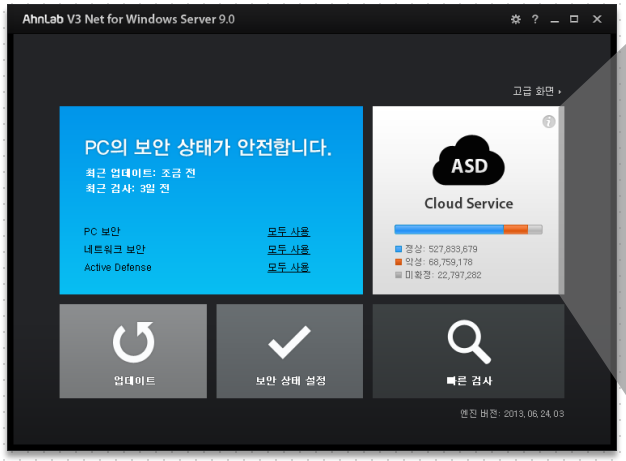
ASD 네트워크를 통해 축적된 웹사이트 및 IP 정보를 통해 악성코드를 유포하는 웹사이트 및 IP로의 접근을 차단하는 기능입니다.
사용자가 웹사이트를 방문할 경우, 이 과정에서 요청되는 모든 URL을 ASD에 질의해 악성으로 판별되면 곧바로 URL 접속을 차단합니다.
또한 웹사이트의 취약점을 통해 유입되는 행위 발견 시, 해당 URL을 ASD에 보고해 악성 행위에 대해 검증, 갱신 업데이트를 진행합니다.

기 능	종 류	내 용
악성 웹사이트 차단	악성URL	홈페이지 변조를 통해 악성 파일을 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.



안전
ASD 분석 결과, 안전한 파일

악성
ASD 분석 결과, 악성 파일

미확정
아직 안전 또는 악성으로 판명되지 않은 파일

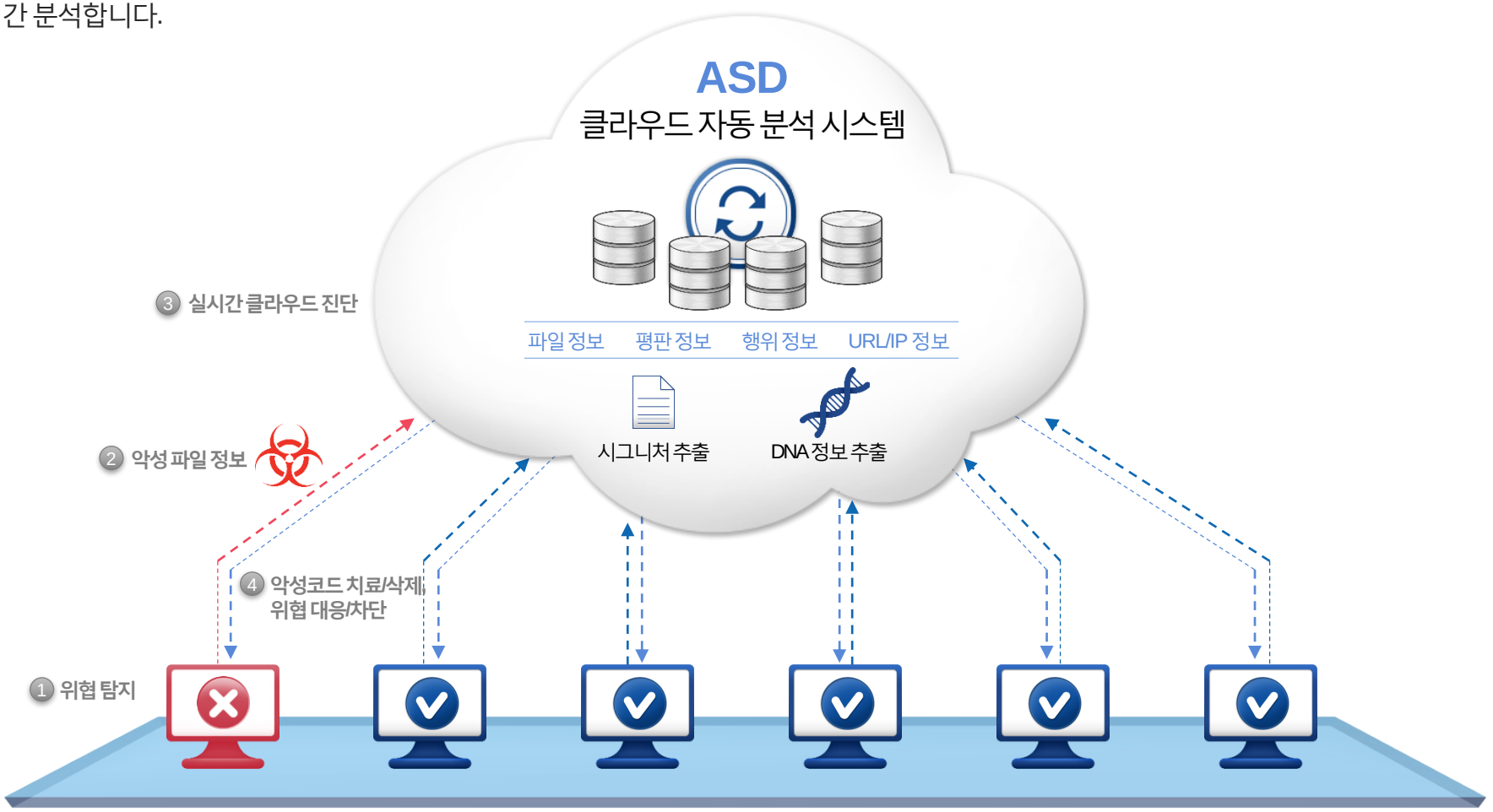
2013. 07. 현재 ASD 보유 DB

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)

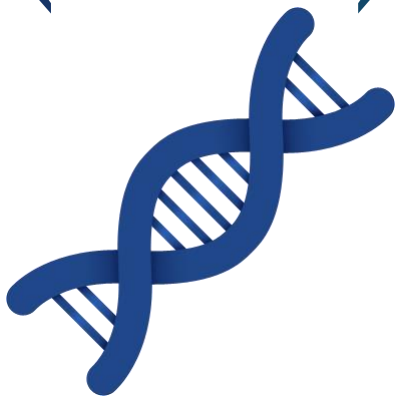
DNA Scan(TS Prime엔진) 기술

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**

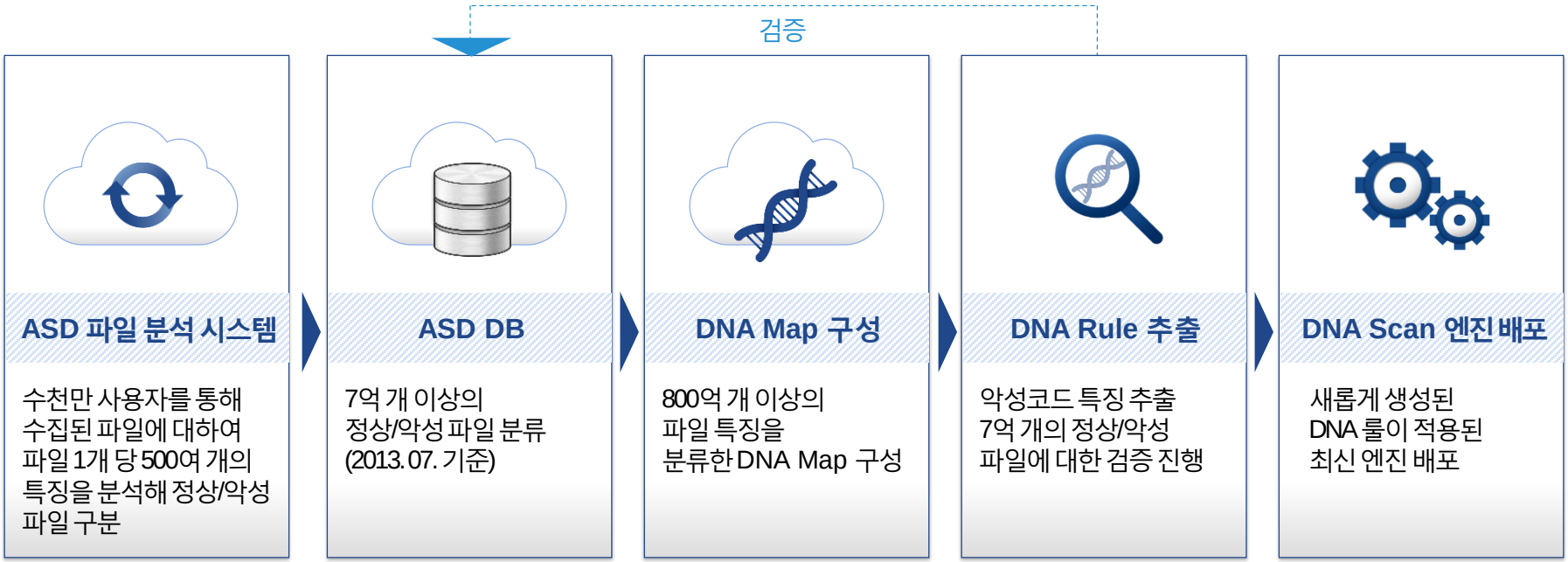
- 타 프로그램 감염
- 특정 정보 전송
- 은폐, 자동 실행

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 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 7억 개 이상의 파일에 대한 검증 후 엔진 반영
  → 타사 대비 휴리스틱 진단법 오진 확률 최소화

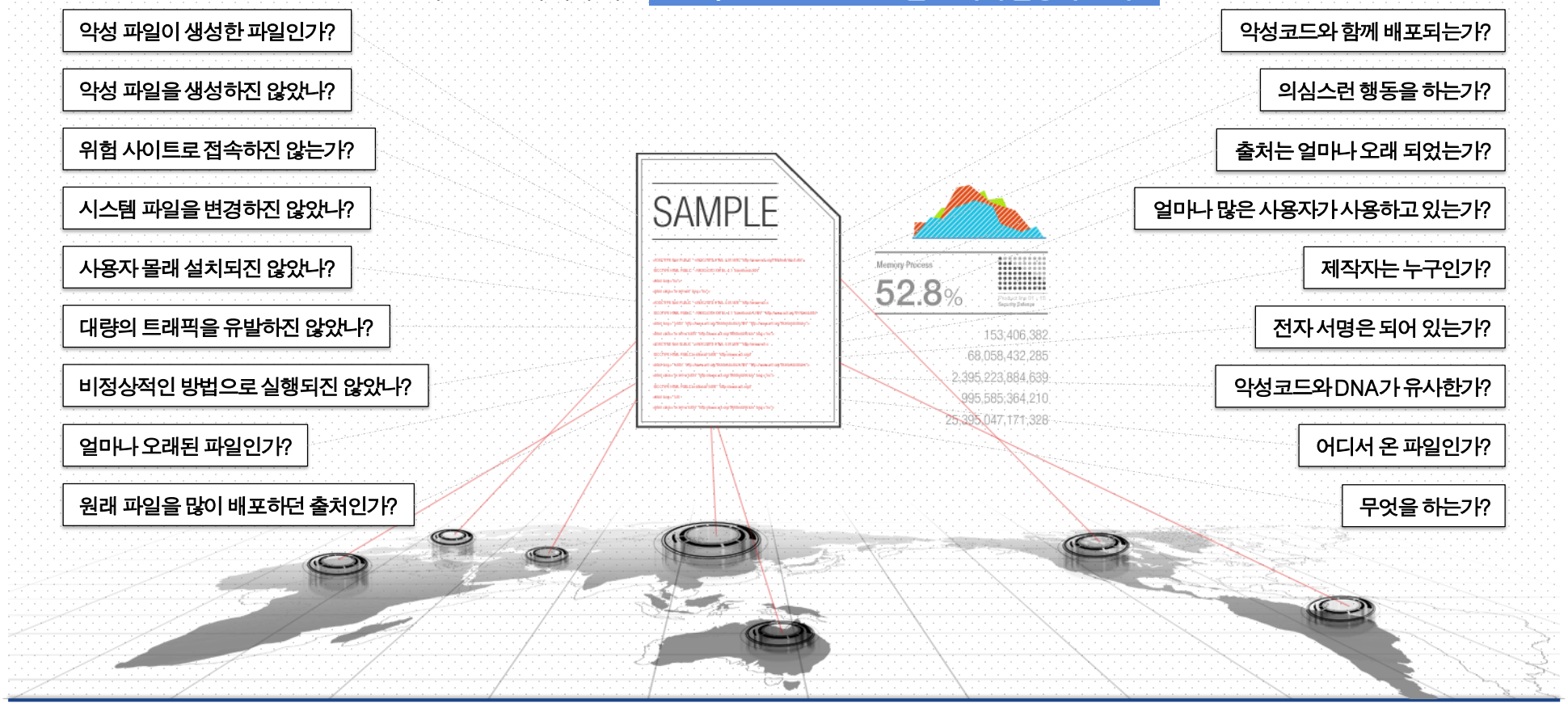


평판 기반 탐지(1)

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

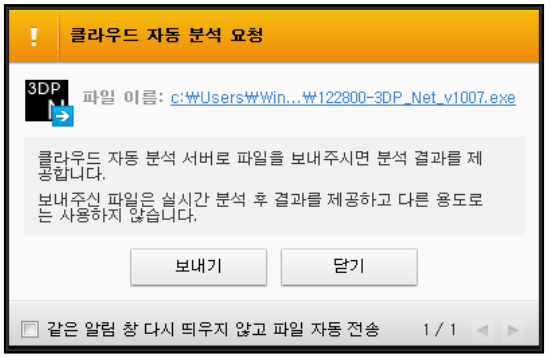
파일(샘플)의 출처와 샘플의 나이, 샘플 사용자 수, 제작 목적, 제작자 정보 등
해당 샘플 자체가 아닌 **샘플과 연관된 모든 정보를 분석에 활용하는 기술**



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

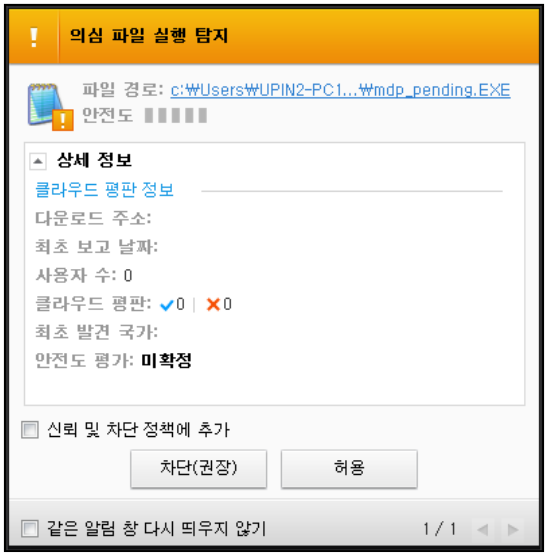


평판 기반 프로그램의 실행 차단

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

※ 평판 탐지의 예시

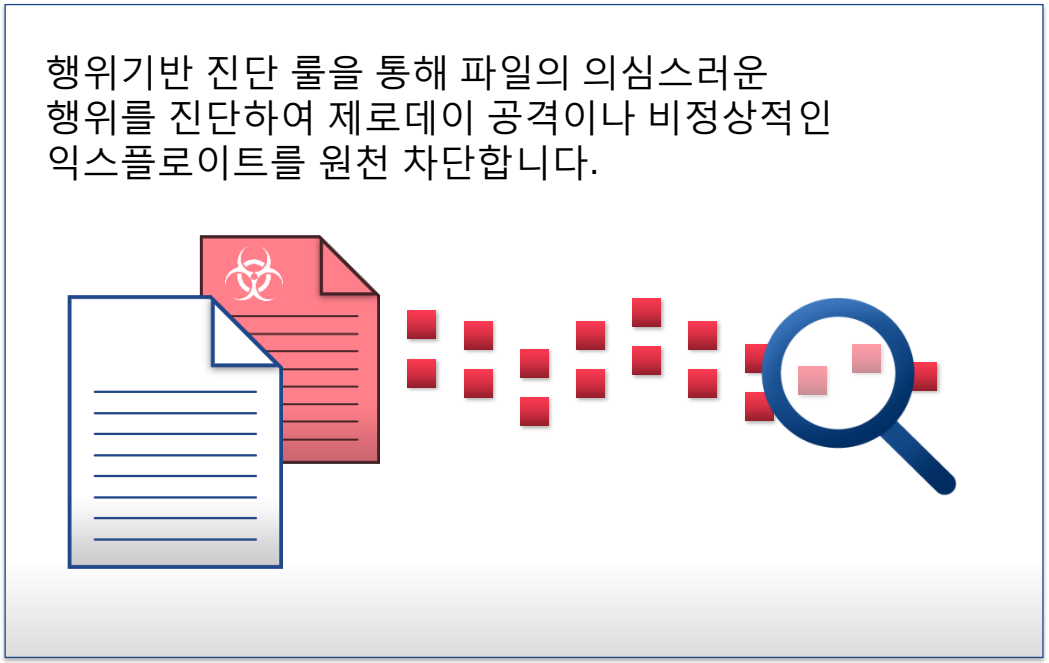
- 최초 발견된 지 20일 이내의 파일로, 사용자 수가 극히 적은(500명 이하) 프로그램
  * 100여 개의 의심 행위에 대한 탐지를 실시함

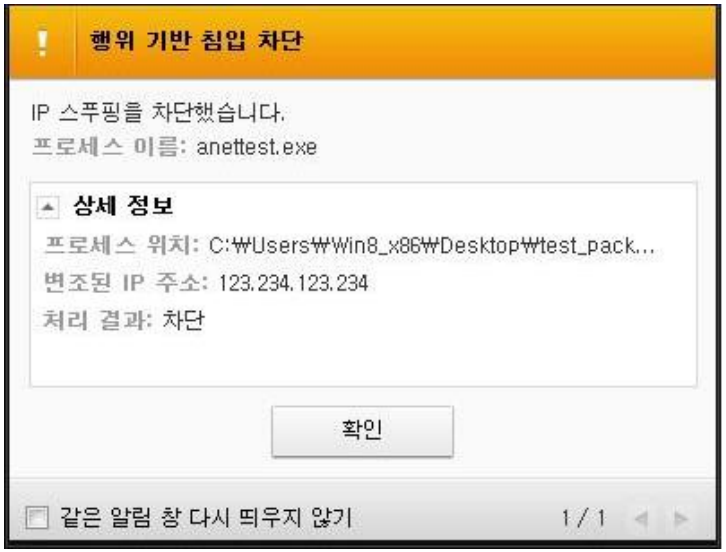


행위 기반 탐지

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

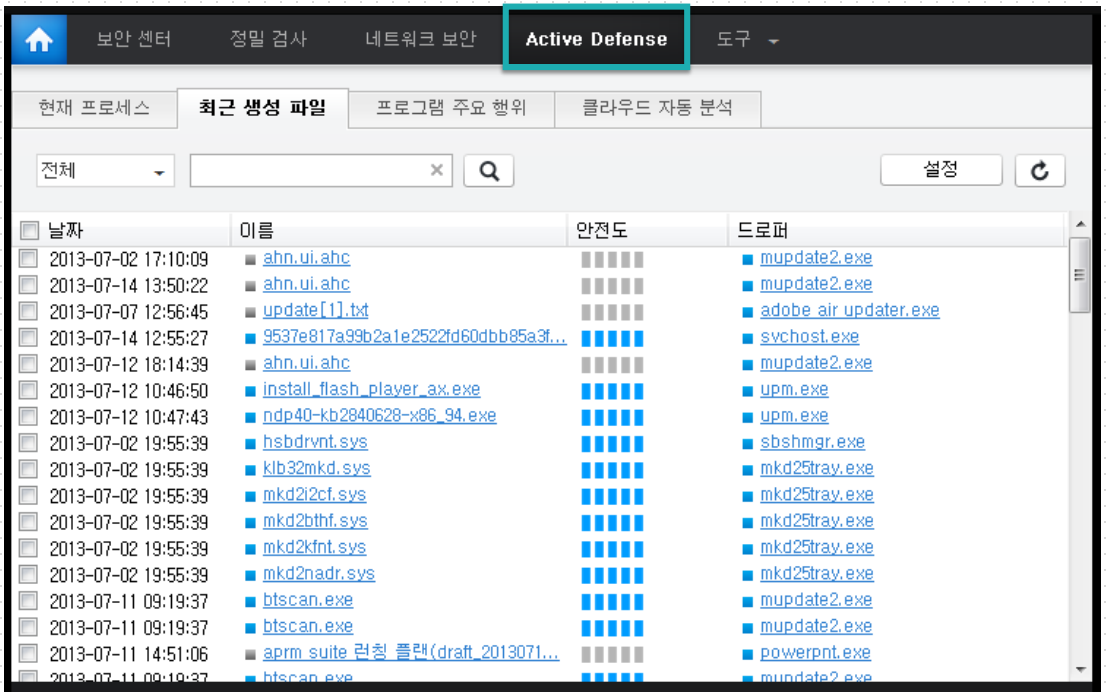




액티브 디펜스(Active Defense)

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

AhnLab

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
Active Defense	• 동작 중인 프로세스 확인, 최근 생성된 파일 확인, 프로그램 활동 내역 확인, 클라우드 자동 분석 결과 확인 • 신뢰/차단 프로세스 목록 관리

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

기능/성능 비교표

구분	AhnLab		Hauri	ESTSoft	Kaspersky	Avast	Symantec	McAfee
	V3 Net for Windows Server 7.0	V3 Net for Windows Server 9.0	ViRobot Windows Server 3.5	알약 3.0 Server Edition	Anti-Virus for Windows Servers Enterprise Edition	Endpoint Protection Suite Plus	Endpoint Protection 12.1.2	VirusScan Enterprise 8.8
클라우드 기반 엔진	X	O	X	X	O	O	O	X
압축파일 검사	O	O	O	O	O	O	O	O
감염되기 쉬운 파일 검사	O	O	O	O	O	O	O	X
CD/USB 자동실행 방지	X	O	O	O	O	X	O	X
휴리스틱 진단	O	O	O	O	O	O	O	O
PUP 검사	X	O	O	O	O	O	O	X
평판 기반 차단	X	O	X	X	O	O	O	X
클라우드 자동 분석	X	O	X	X	O	O	O	X
알림 메일	O	O	O	X	O	O	O	O
포트 차단	O	O	O	O	X	X	O	O
Active Defense	X	O	X	X	X	X	X	X
빠른 검사(Smart Scan)	X	O	X	O	O	O	O	O
현황판(Dashboard)	X	O	X	X	O	O	X	O
다운로드 파일 평판 분석	X	O	X	X	O	O	O	X
HIPS(스푸핑)	X	O	X	X	O	O	O	O
Stable 엔진 사용 기능	O	O	X	X	X	X	X	X

시스템 요구 사항

시스템 사양

운영체제	항목	권장 사양	최소 사양
Windows Server 2003 SP2 이상(R2 포함)	CPU	800MHz 이상	700MHz 이상
	Memory	512MB	256MB
Windows Server 2008 (R2 포함)	CPU	2GHz 이상	1GHz 이상
	Memory	1GB	512MB
Windows Server 2012 (R2 포함)	CPU	2GHz 이상	1GHz 이상
	Memory	2GB	1GB
공통 사항	HDD	500MB 이상	
	지원 언어	한국어, 영어	

※ 해당 OS가 지원하는 모든 32bit CPU와 x64 계열의 64bit CPU를 지원합니다. (IA 64계열 제외)

※ 별첨

AhnLab
V3 Net for Windows Server 9.0

제품 연혁

AhnLab

※ 별첨

V3 Net for Windows Server 제품 연혁

- **2013. 07.** **V3 Net for Windows Server 9.0**
- 2008.06. V3 Net for Windows Server 7.0
- 2004.11. V3 Net for Windows Server 6.0
- 2002. 05. V3 Net for Windows Server SE
- 1999. 04. V3 Net for NT 3.0
- 1997. 09. V3 Net for NT 1.0

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 Net for Windows Server 9.0

AhnLab