More security,
More freedom

AhnLab TS Engine Suite

2022.05.24

AhnLab

목차

AhnLab

01.
도입 배경

1. 악성코드의 급격한 증가
2. 고도화하고 있는 악성코드
3. 국내 기업의 악성코드 피해 현황
4. 새로운 IT 환경과 보안 위협
5. 내부 인프라에 대한 방역 체계의 필요성

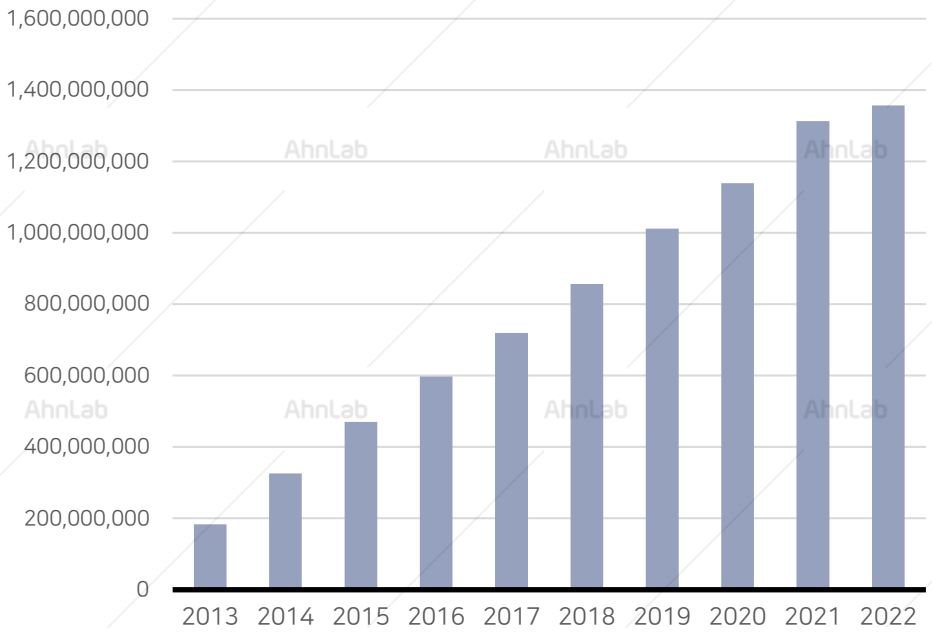
AhnLab

악성코드의 급격한 증가

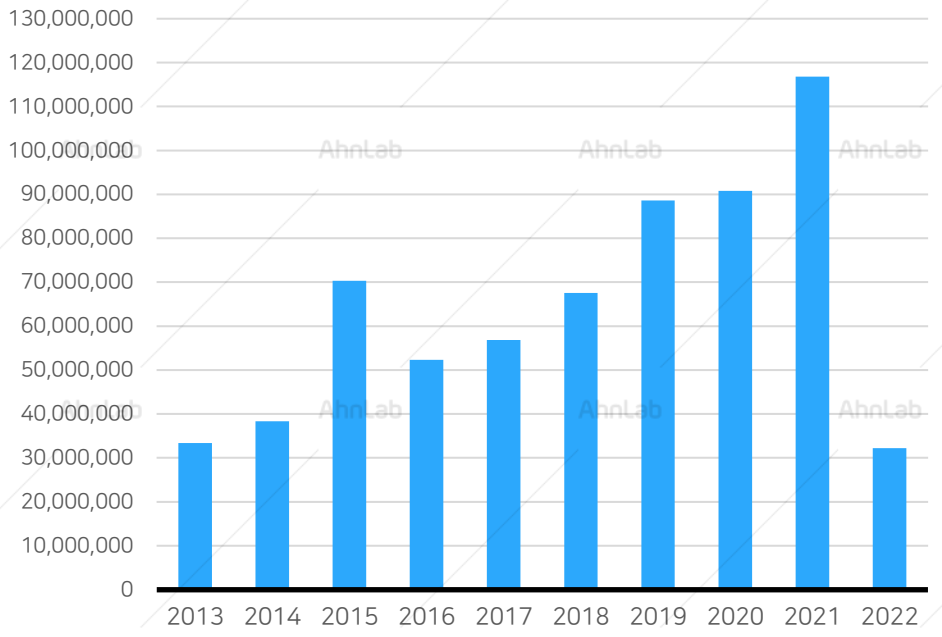
해마다 악성코드의 수는 기하급수적으로 늘고 있습니다. 한 기관에 따르면 매일 45만여 개의
악성코드가 새롭게 발견되고 있습니다. 그만큼 분석 및 대응해야 하는 악성코드의 수가 급격히 늘고 있는 셈입니다.

- 기업의 IT 환경이 발전함에 따라 편의성이 증대됨과 동시에 보안 위협도 높아지고 있음.
- 최근 금전 탈취 목적의 공격이 늘어나고 있으며 악의적 공격도 전문화 · 상업화 되는 추세임.
- 인터넷 등을 통해 악성코드 제작법이 유포, 일반인도 쉽게 악성코드를 만들 수 있어 악성코드는 더 폭증할 것으로 예상됨.

Total Malware



Development of New Malware

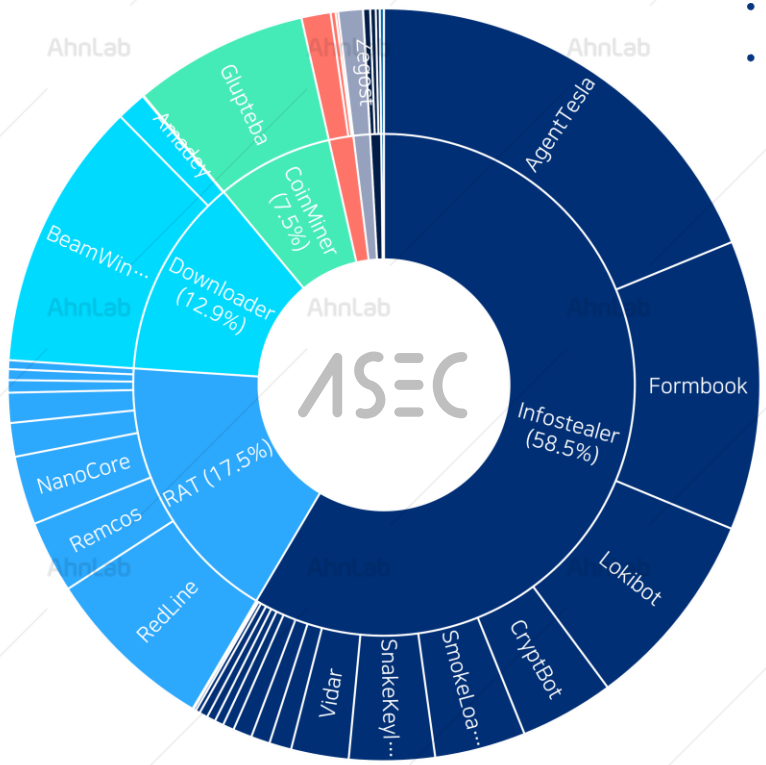


2011~2020년 멀웨어 증가 추이 (2022.05 AV-TEST 자료 참조)

고도화하고 있는 악성코드

2021년에는 악성코드 통계기준 인포스틸러가 71.8%로 1위, 그 다음으로는 RAT (Remote Administration Tool) 악성코드가 19.1%, 다운로더 3.7%, 랜섬웨어 3.3%, 뱅킹 1.7%, 백도어 0.4% 로 집계었습니다.

2021년 악성코드 통계



- Infostealer (58.5%)
- RAT (17.5%)
- Downloader (12.9%)
- Ransomware (1.6%)
- CoinMiner (7.5%)
- Backdoor (1.1%)
- Banking (0.7%)
- Ddos (0.2%)

주요 Top 5 악성코드 행위

- 주로 스팸 메일을 통해 유포되는 인포스틸러 악성코드
- PUP를 통해 다운로드되며, 추가 PUP 또는 악성코드를 다운로드 형태
- MalPe 외형으로 유포되는 랜섬웨어
- 주로 익스플로잇 킷을 통해 유포되는 코인 마이너 또는 인포스틸러 악성코드
- PUP 를 통해 다운로드되며, 추가 정보 탈취 및 추가 악성코드를 다운로드 받는 형태

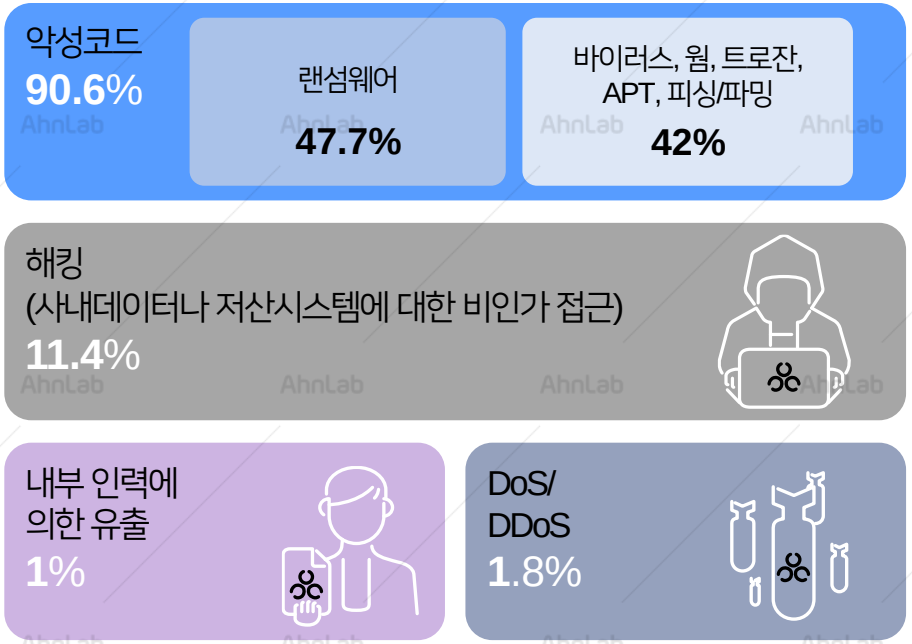
Source : AhnLab ASEC Report2021.01~2021.12)

국내 기업 악성코드 피해 현황

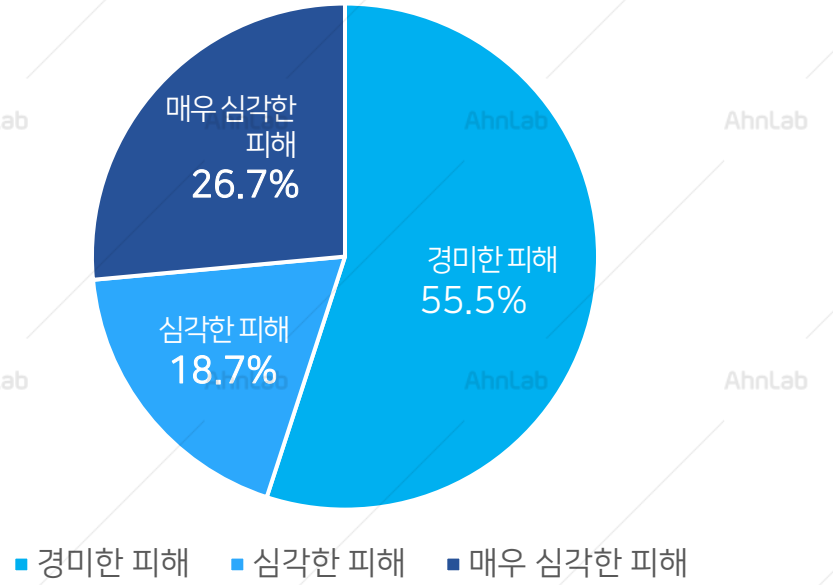
국내 기업의 침해사고는 해마다 증가하는 추세이며, 악성코드 공격은 침해사고 유형 중 가장 많은 비중을 차지 하고 있습니다.
2021년 발생한 랜섬웨어 공격 피해액은 작년대비 102% 증가, 금액은 약 22조로 집계되었습니다. (한국인터넷진흥원)
이제 대다수 기업이 정보보안 문제를 전사적 경영 리스크로 바라보고 있으며, 백신 소프트웨어는 가장 기본적이고 필수적인 정보보안 대책으로 인식되고 있습니다.

- 국내 기업 침해사고 중 악성코드(랜섬웨어, 바이러스, 웜, 트로이목마 등) 공격이 차지하는 비율은 90.6%
- 45.4%가 심각한 피해 또는 매우 심각한 피해를 입었다고 응답

침해사고 경험 유형 (복수응답)



침해사고 피해 심각성 정도



Source : 2021년 정보보호 실태 조사(과학기술정보통신부, KISIA)

새로운 IT 환경과 보안 위협

클라우드 컴퓨팅, 데이터 센터, 콘텐츠 서비스, 모바일 플랫폼 등 기존 PC 환경과는 전혀 다른 IT 환경이 도래함에 따라 다양한 혜택과 더불어 새로운 보안 위협이 증가하고 있습니다. 이에 보안 또한 시스템(System)뿐만 아니라 사용자(User)와 애플리케이션(Application)까지 고려한 접근 방식이 요구되고 있습니다.

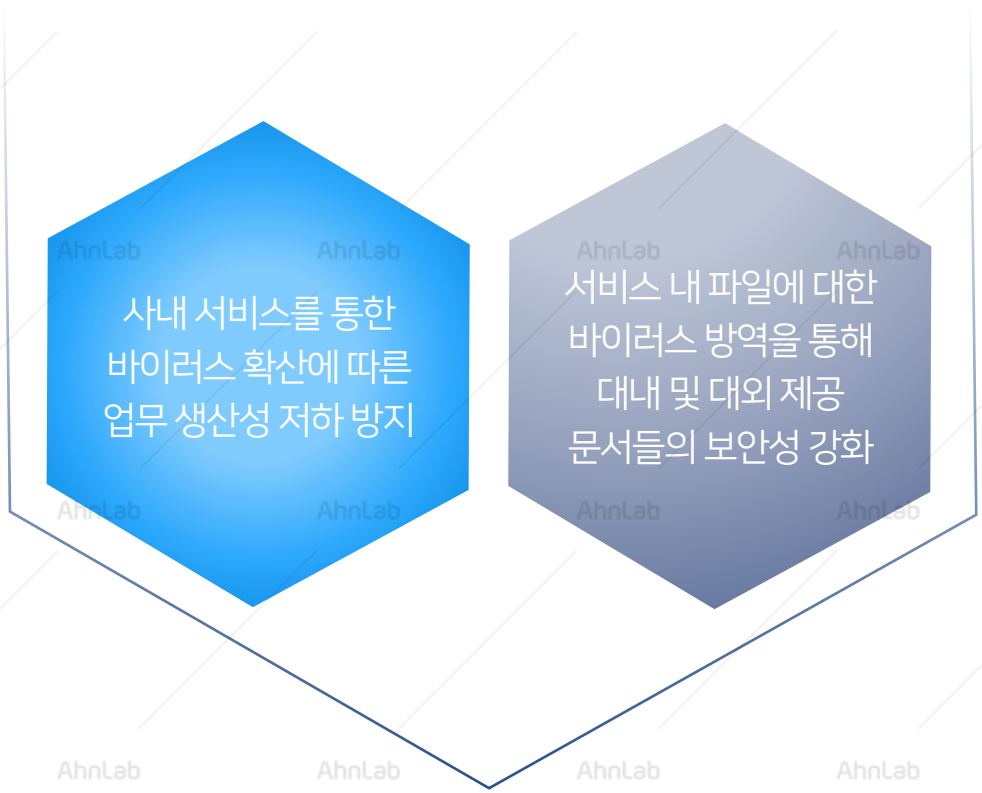
새로운 보안 위협에 대한 대응 요구

보안 위협 변화	• 해커의 공격 포인트 증가 • 스크립트 기반의 공격 등 공격 방식의 다변화	• 멀티 플랫폼에 대한 통합적인 대응 필요 • 손쉬운 연동 및 유지 보수 필요	• 망과 망간의 콘텐츠 보호 필요 • 외부 사용자로부터 인입되는 콘텐츠 검사 필요
기업 IT 환경 변화	• 비즈니스 생산성 향상	• 플랫폼의 다양화	• 비즈니스 연속성 구현
	• 디지털 콘텐츠의 다양화 • 속도의 증가 • 액세스 방법의 다양화	• 클라우드 서비스와 Web OS의 일반화	• 망분리 환경 증가

내부 인프라에 대한 방역 체계의 필요성

기업 내 문서 공유, 업무 시스템 등을 통해 악성코드가 확산되는 것을 방지하기 위해 안전한 악성코드 방역 시스템을 구축이 필수적입니다. 특히 전자문서공유 시스템의 경우, 파일의 업로드/다운로드 시 문서에 대한 보안성을 확보하기 위해 서비스 부하는 최소화할 수 있는 효율적인 방역 체계 구축이 요구됩니다.

내부 인프라에 대한
안전한 바이러스 방역 시스템 구축



02.
AhnLab TS Engine Suite

1.제품 개요

2.주요기능

3. 예상 구조 및 아키텍처

4. AV Engine 필요성

4. 특장점

5. 도입효과

AhnLab

AhnLab TS Engine Suite

연동이 유연한 통합 보안 엔진! AhnLab TS Engine Suite

탁월한 악성코드 탐지/치료

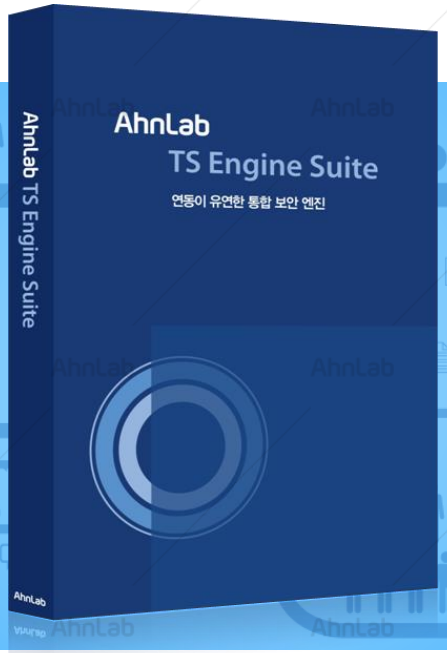
TS Engine Suite은 다각화된 안랩의 악성코드 분석 기술을 통해 최신 악성코드와 스파이웨어를 신속하고 정확하게 탐지하고 치료합니다.

유연한 서비스 연동

다양한 운영체제와 제품 및 서비스에 편리하게 연동 가능한 유연성 및 안정성을 보장합니다.

대외 이미지 제고

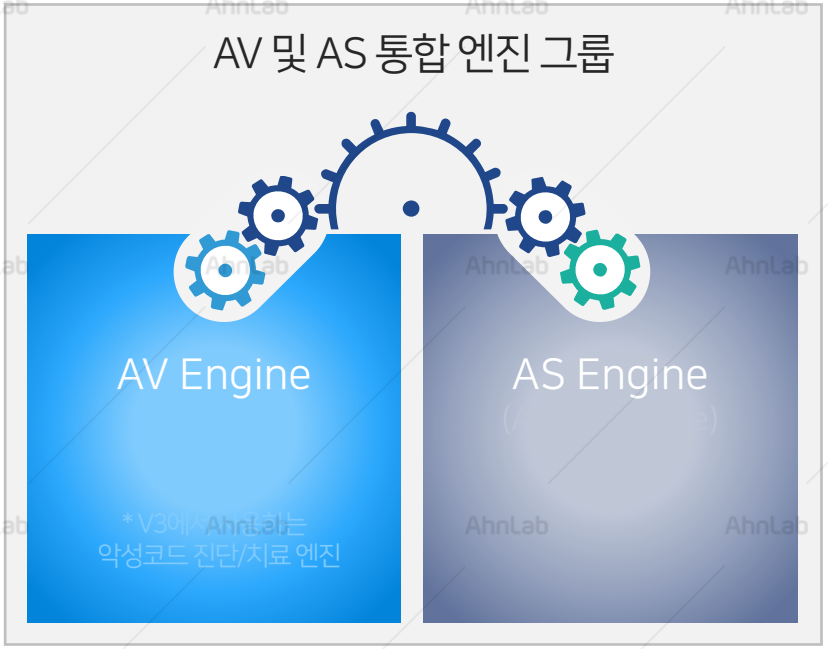
TS Engine은 신 변종 악성코드로 인한 보안 위협 발생 시 신속한 보안 대응이 가능해 악성코드에 의한 피해를 최소화하고 안정적인 비즈니스 구현에 기여합니다.



제품 개요

TS Engine Suite는 안티바이러스(Anti-Virus) 엔진과 안티스파이웨어(Anti-Spyware) 엔진을 통합한 통합 보안 엔진으로, 바이러스, 트로이목마 등의 악성코드뿐만 아니라 스파이웨어, PUP, 피싱 등 다양한 보안 위협에 효과적으로 대응할 수 있습니다.

Anti-Virus 엔진과 Anti-Spyware 엔진의 결합으로
악성코드부터 스파이웨어, PUP, 피싱까지 대응 가능

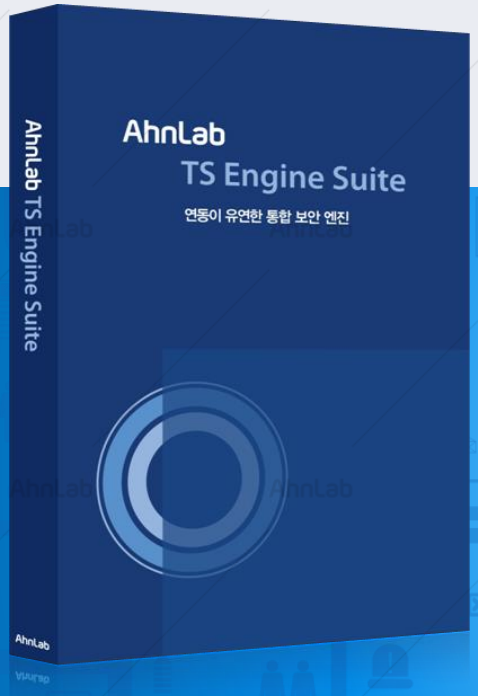


- 용도에 따라 엔진 그룹을 선택적으로 사용
- 통합 진단으로 더욱 빨라진 검사 속도
- 급격히 증가하는 악성코드/보안 위협 대응에 탁월
- 안정적인 시스템 환경 구현

※ PUP(Potentially Unwanted Program) : 사용자가 이해한 프로그램의 설치 목적과 다르거나 불필요하게 설치되어 시스템 부하 또는 사용자 불편을 유발할 수 있는 프로그램

주요 기능 (1/2)

AhnLab TS Engine Suite



- 바이러스, 스파이웨어, 애드웨어와 같은 악성파일 진단
- 윈도우, 유닉스 등 멀티 운영체제 지원, 32bit, 64bit 플랫폼 지원
- AhnLab의 Cloud ASD(AhnLab Smart Defense) 연동, Cloud 진단
- 멀티 프로세스/멀티 스레드를 이용한 다중 검사 지원
- 분산 처리 가능한 클라우드 형 검사 지원
- 사용 환경에 맞춰 검사 옵션 변경 가능
- 시스템에서 발견된 악성파일 현황 등 검사 상태에 대한 정보 제공
- ICAP 서버 지원, Proxy 서버와 연동 통해 HTTP 다운로드 콘텐츠 보안 및 악성 스크립트 실행 방어를 위한 악성 URL 접근 차단
- Milter 서버 지원, 메일 서버(Sendmail, postfix, qmail)와 연동 통한 메일 첨부 파일 및 스팸 검사
- 원격지 파일 검사 지원
- 옵션 및 AhnLab TS Engine Suite 목록 등을 관리하는 중앙 정보 서버(CIS) 기능 지원
  2022년 CIS Console로 제공하는 서버제어 기능 통합 지원 예정

주요 기능 (2/2)

다양한 진단법 탑재

- 시그니처, Gen, Cloud, DNA 등 고도화된 다양한 진단법 탑재
- 악성코드 유형에 따라 최적의 성능과 정확한 진단을 제공하기 위해 특화된 진단법 적용
- 휴리스틱 진단을 통해 신종 악성코드도 신속하게 탐지

콘텐츠/미디어 파일에 대한 강력한 진단

- HWP, PDF, XLS, PPT 등 기밀 정보 유출 사고를 유발하는 콘텐츠형 악성코드 방역
- Office (DOC/XLS/PPT) , HWP, PDF 등 문서 파일 내 악성코드 및 스크립트 진단
- SWF, MIDI, MP4 등 미디어 파일 악성코드에 대한 타사 대비 최고의 진단율 및 성능 제공

클라우드 기반 서비스에 적합한 확장성 제공

- 클라우드 기반 서비스에 적용하는 AV-Engine의 최대 이슈인 AV-Storm을 해결
- VM과 연동하지 않고, 별도 에이전트가 필요 없이 최적의 진단 기능을 제공

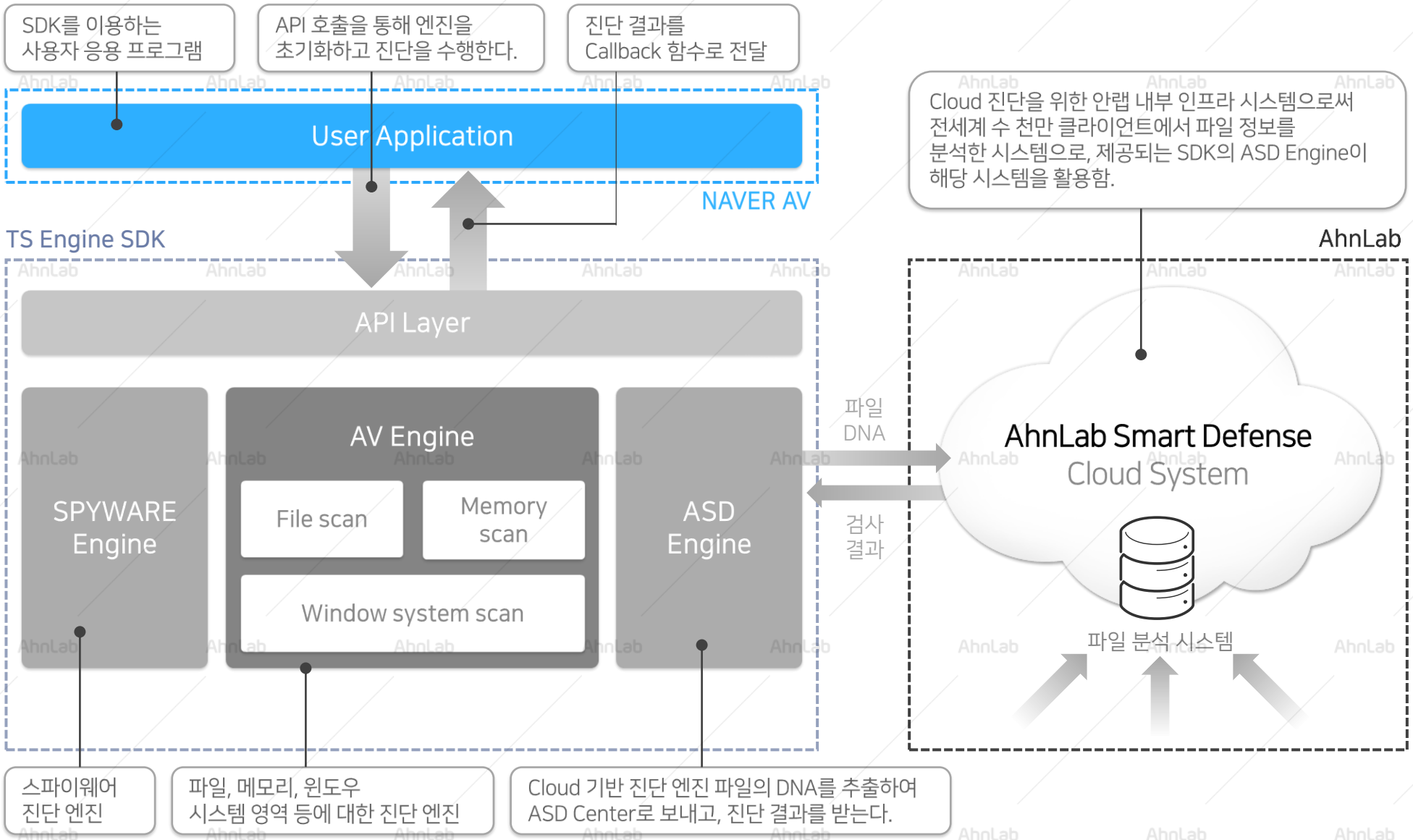
컨테이너 파일에 대한 효율적인 진단

- 압축 파일 검사에 대한 성능 향상
- 압축 파일 전체를 해제하지 않고, 진단 포인트만 해제하여 검사를 진행

멀티 플랫폼(실행파일 포맷)에 대한 악성코드 진단

- PE, ELF 뿐 아니라 Mach, apk 등 모바일 악성코드 통합 진단

예상 구조 및 아키텍처



AV Engine 필요성

AV만 설치하면 서버 보호 끝?

서버 AV의 보호 영역!

- OS 자체 보호를 위한 '파일 I/O, 프로세스, 메모리'에 대한 악성코드 검사가 주요 목적

하지만 부족한 점은!

- Linux/Unix 등 다양한 운영체제의 개별 정책 및 운영 관리의 불편
- 중요 서버에서 성능 부담인 AV의 실시간 검사 옵션은 대부분 Off, 無의미
- 특히 해외 AV는 클라우드 진단/쿼리가 진단율 핵심이지만 대다수 폐쇄망 환경에서 無의미
- 서버 자체 외 Application, DB 등 영역에 대한 악성코드 검사는 불가

AV 비보호 영역!! 어디에 필요할까?

AV로 보호하지 못하는 영역에 꼭 필요!

- AV가 제어하지 못하는 비보호 영역에서 중요
- DB에 파일이 직접 저장되는 게시판 등이 동작하는 웹서비스/게시판에 업로드 되는 파일 검사, WAS 서비스를 통해 업로드 되는 파일 검사
- C/S환경의 업무 프로그램을 통해 서버 시스템에 파일이 업로드 되는 서비스 전자문서/파일공유시스템 등 서버영역에서 Application을 통해 업로드 되는 파일 검사
- 메일서비스를 제공하는 그룹웨어 그룹웨어(웹포탈)을 통해 첨부되어 발송되는 이메일의 첨부파일 검사

서버 성능 최적화!

- 서버 AV의 실시간 검사 기능으로 인해 발생 할 수 있는 서버 성능 저하를 최소화 하기 위해, Application 레벨에서 엔진 API를 통해 악성코드 사전 검사 및 치료

특장점 - 차세대 방역 기술을 통한 진단력 (1/2)

TS Engine Suite는 DNA Scan, AhnLab Smart Defense 등 독자적인 차세대 방역 기술이 적용돼 탁월한 악성코드 진단 성능을 제공합니다.

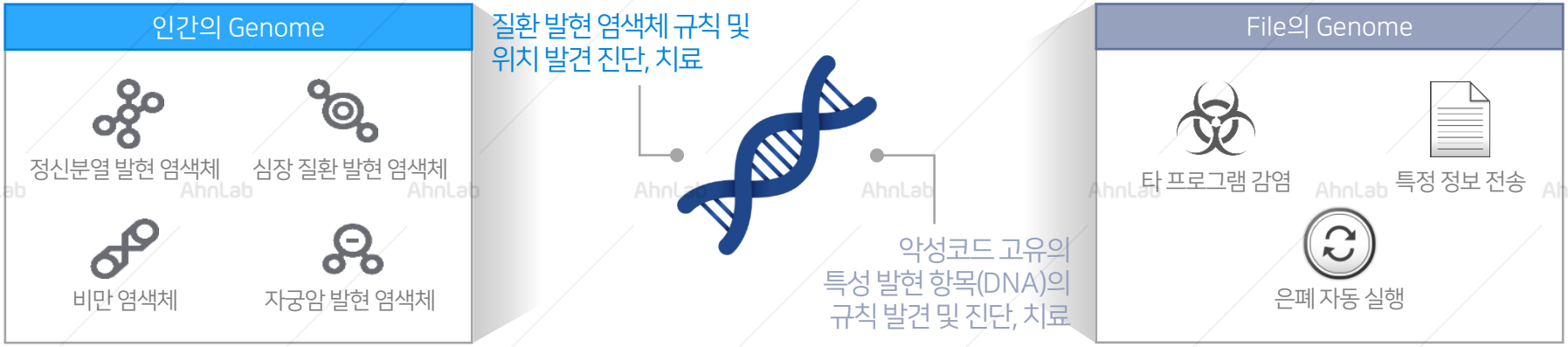
폭증하는 악성코드에 대한 효과적인 대응! DNA Scan 기술

DNA Scan 기술은 수억 개 파일의 특징(DNA)를 추출하고 악성 DNA를 패턴화하여 이와 매칭되는 파일을 검출해 악성코드를 분류하는 기술입니다.
DNA Scan 기술을 통해 오진율과 엔진 사이즈 증가를 최소화할 뿐만 아니라 미발견 악성코드 및 신 변종 악성코드에 대한 사전 대응 효과를 제공합니다.

오진 방지 강화

엔진 사이즈 증가 이슈 해결 (엔진 경량화)

신/변종 악성코드에 대한 사전대응

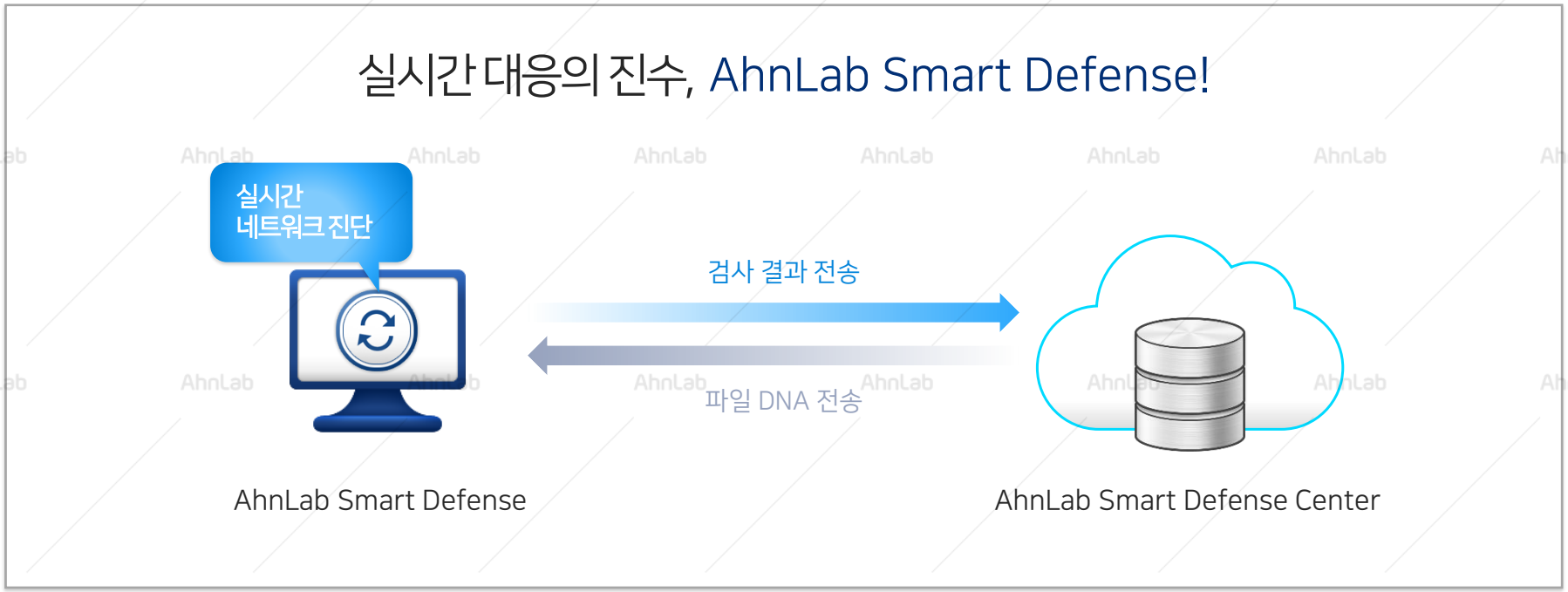


특장점 - 차세대 방역 기술을 통한 진단력 (2/2)

TS Engine Suite은 클라우드(Cloud) 기반의 실시간 악성코드 진단 기술인 AhnLab Smart Defense를 적용해 별도의 업데이트 과정 없이 최신 악성코드를 실시간으로 진단합니다.

클라우드 기반의 ASD 기술 적용으로 최신 악성코드 실시간 탐지 및 진단

※ AhnLab Smart Defense : 수억 개 이상의 파일 유형별 DNA 데이터는 중앙 서버(ASD Center)에서 관리하고 PC에 설치되어 있는 에이전트가 파일의 안전성에 대해 ASD 서버에 문의하면 다양한 분석 기술로 진단한 결과를 실시간으로 답해주는 방식입니다.
기존 악성코드에 대한 모든 데이터(엔진)를 PC로 다운로드 하여 감염 여부를 직접 확인하던 방식과는 차별적인 진단율과 리소스 효율성을 제공합니다.



특장점 - 대용량 처리 및 강력한 성능

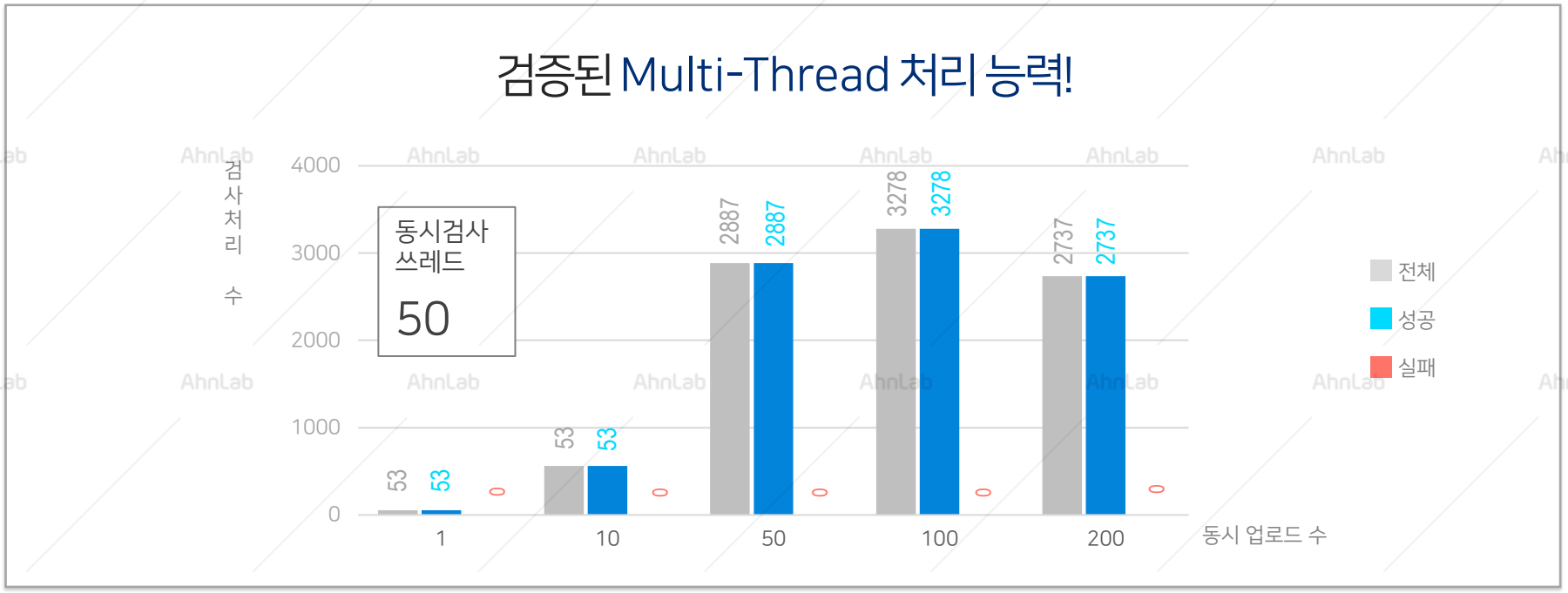
안랩은 기하급수적으로 증가하는 악성코드에 대응하기 위해 DNA Scan 등 다양한 기술의 개발 및 적용을 통해 엔진 경량화와 성능 향상을 동시에 구현하고 있습니다. 특히 Multi-Thread 지원을 통해 다수의 파일에 대한 동시 검사가 가능해 긴급 상황 시, 처리량 과다로 인해 놓치기 쉬운 보안 위협까지 빈틈없이 검사합니다.

Multi-Thread 활용 사례

- 국가기록원 기록물관리 시스템
- KB국민은행 업무포털
- 네이버 백신

Multi-Thread 테스트결과 (*Multi-Thread Module만 테스트)

- 안랩 성능 측정 도구를 이용해 1분 동안 테스트 수행
- 동시에 n명의 사용자가 1초마다 한 개의 파일을 업로드 한 경우, 누락되는 파일 없이 모든 파일에 대해 정상적인 검사 가능



도입효과

TS Engine Suite는 대내외의 다양한 보안 위협으로부터 안전한 기업의 보안 환경을 구축함으로써 업무 생산성 향상 및 비용 절감 효과를 제공합니다.

보안 강화	• 악성코드로 인한 피해 방지 • 엔진 자동 업데이트 및 악성코드 방역 정책의 신속한 적용 가능 • 사용자 보안 인식 부족으로 인한 보안 사고 예방
업무 생산성	• 안정적인 IT 시스템 운영 가능 • 고객사 솔루션 및 인프라에 간편하게 연동 가능해 운영의 안정성과 편리성 제공
비용 절감 효과	• 악성코드 감염으로 인한 시스템 또는 데이터 복구 비용 최소화 • 기업 전체 PC의 보안 관리를 위한 비용 및 시간 투자 감소
대외 이미지 제고	• 신뢰성 및 안정적인 전산 자원으로 대외 경쟁력 확보 • 검증된 안랩의 엔진 도입을 통해 신뢰할 수 있는 기업 이미지 강화

03.
적용사례

1.웹게시판/웹포탈 연동

2.파일서버/스토리지 연동

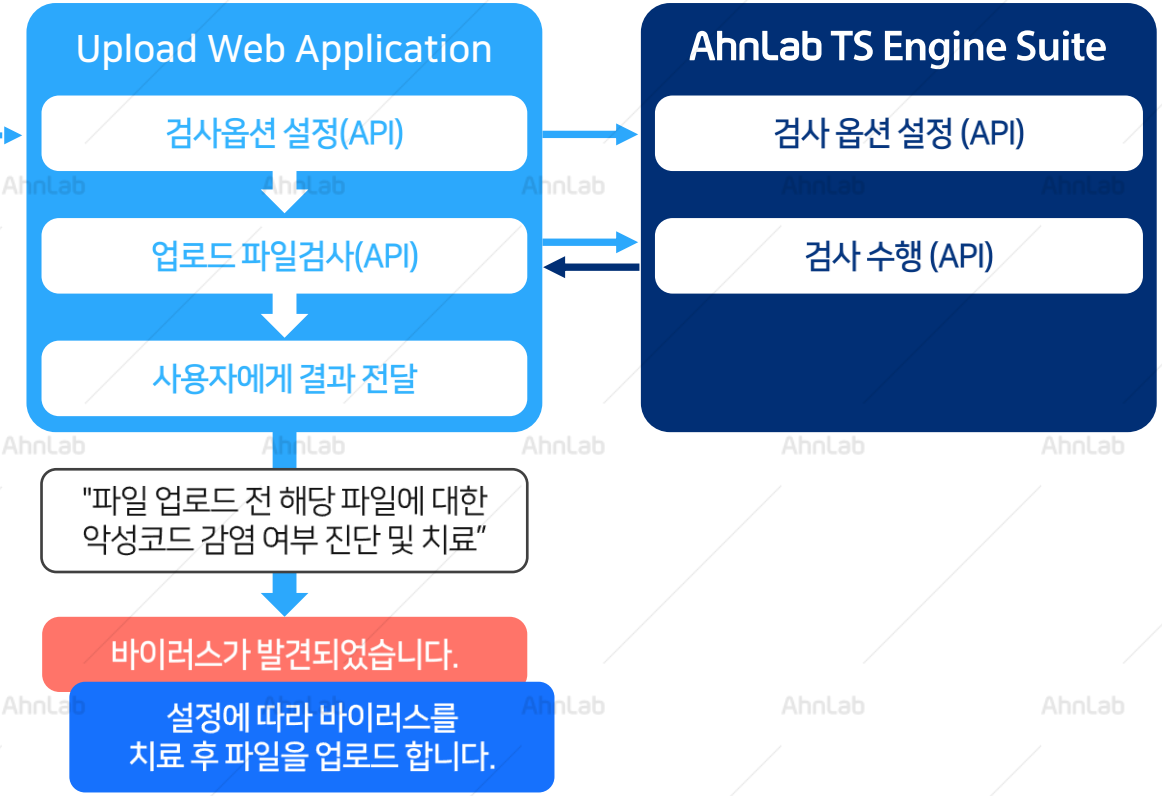
3.그룹웨어/대외 서비스 연동

4.응용프로그램 연동

AhnLab

적용 사례 1) 웹게시판/웹포탈 연동

웹 게시판 형태의 자료실/스토리지 등 사용자가 파일을 업로드 시,
해당 파일에 대한 악성코드 감염 여부를 판단하여 진단 및 치료하고 안전한 파일만 업로드 할 수 있습니다.



적용 사례 2) 파일서버/스토리지 연동

WAS를 통해 고객 또는 직원이 문서 및 자료를 서버로 업로드 하거나 다운로드 할 때, 악성코드 감염 여부를 판별합니다.
이를 통해, 감염 여부가 확인된 정상 파일만을 서버에 저장할 수 있도록 합니다.

사용자
문서 및 자료 업로드/다운로드

"파일 업로드 전 해당 파일에 대한 악성코드 감염 여부 진단 및 치료"

파일서버/WAS
감염여부가 확인된 정상 파일만 저장

Upload Web Application

- 검사옵션 설정(API)
- 업로드 파일검사(API)
- 사용자에게 결과 전달

AhnLab TS Engine Suite

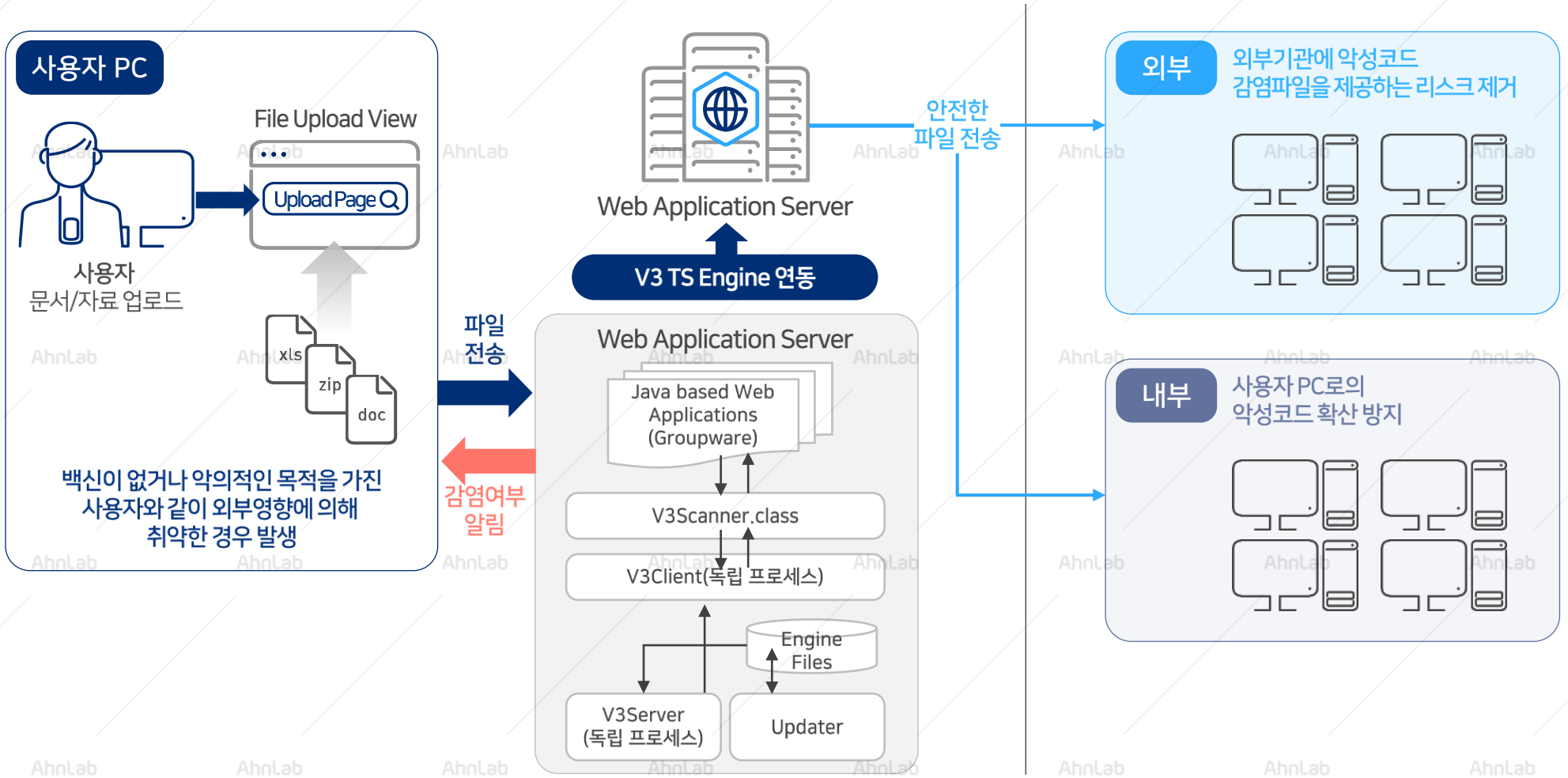
- 검사 옵션 설정 (API)
- 검사 수행 (API)

바이러스가 발견되었습니다.

설정에 따라 바이러스를 치료 후 파일을 업로드 합니다.

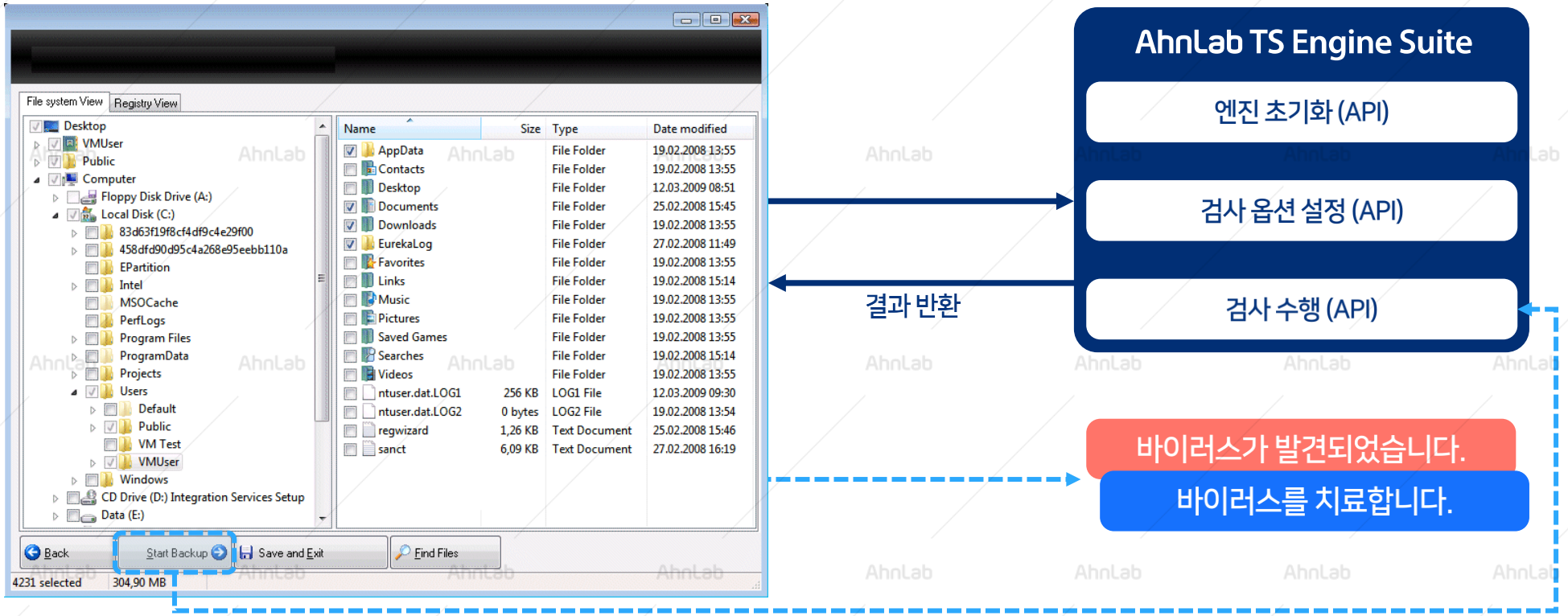
적용 사례 3) 그룹웨어/대외 서비스 연동

그룹웨어에 내부 직원의 파일 업로드 시, 대외 서비스에 고객이 파일 업로드 시, 악성코드와 정상파일을 체크하여
WAS에는 정상파일만 업로드 할 수 있습니다.



적용 사례 4) 응용프로그램 연동

응용프로그램에서 직접 특정 파일에 대한 악성코드 감염 여부 진단 및 치료가 가능합니다.



04.
별첨

1.주요인증

2.레퍼런스

AhnLab

주요 인증

안랩은 CC 인증, GS 인증을 비롯해 AV-TEST, AV-Comparatives, ICSA, VB100, Check Mark 등 국내외 주요 인증을 획득했습니다.

안티멀웨어 국제인증

AV-TEST
AV-Comparative
ICSA Labs
VB 100
Checkmark

CC(Common Criteria) 인증

V3 제품군
엔드포인트 보안 관리 제품군
AhnLab MDS
네트워크 제품군(TrusGuard 시리즈) 외 다수

GS(Good Software) 인증

V3 제품군
엔드포인트 보안 관리 제품군
AhnLab Safe Transaction
AhnLab Online Security 외 다수

정보보호관리체계 인증

ISMS
(Information Security Management System)
PIMS
(Personal Information Management System)

ISO / IEC 27001:2005

Information Security Managing Service
Information Security Consulting Service

레퍼런스

TS Engine은 공공/금융/기업 등 다양한 산업 분야에 걸쳐 도입 및 운영되는 등 시장에서 안정성이 입증된 통합 보안 엔진입니다.

금융감독원 | kakao | IBK기업은행 | ebay
SAMSUNG | KB | KORAIL | kt
KICA 한국정보인증 | 대법원 SUPREME COURT OF KOREA | KEB 하나은행 | Kdn 한전KDN
중앙선거관리위원회 | DTaQ 국방기술품질원 Defense Agency for Technology and Quality | SAMSUNG 삼성SDS | koscom
충청북도 CHUNGCHEONGBUK-DO | 대전광역시 DAEJEON METROPOLITAN CITY | DAEGU 대구광역시 DAEGU METROPOLITAN CITY | 안산시
행정안전부 | 검찰 PROSECUTION SERVICE | 거제시 GEOJE-SI | Incheon Airport

More security,
More freedom

㈜안랩
경기도 성남시 분당구 판교역로 220 (우) 13493
대표전화 : 031-722-8000 | 구매문의 : 1588-3096 | 전용상담전화 : 1577-9431 | 팩스 : 031-722-8901 | www.ahnlab.com

AhnLab TS Engine Suite

AhnLab

www.ahnlab.com
www.facebook.com/AhnLabSP
www.youtube.com/user/OfficialAhnLab