AhnLab V3 for VDI

Agent / Agentless

More security,
More freedom

안정적인 VDI 환경을 위한 확실한 선택

표준제안서

AhnLab

CONTENTS

AhnLab

01
제안 배경

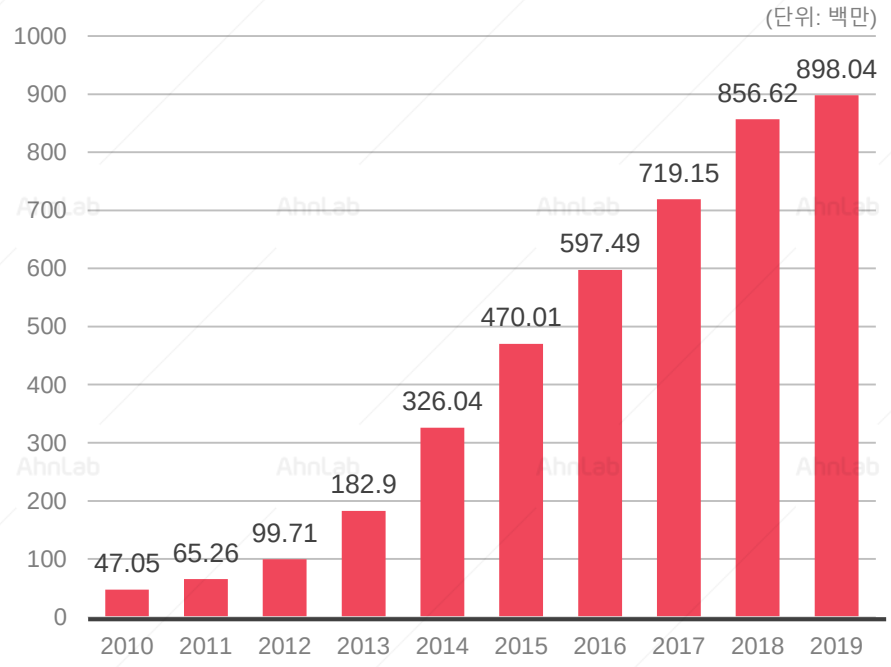
1. 급격한 악성코드 변화
2. 기업의 IT 환경 변화에 따른 보안 위협 증가
3. VDI 전용 보안 솔루션의 필요성

급격한 악성코드 변화

지난 몇 년 간 전 세계적으로 악성코드가 기하급수적으로 증가했습니다. 최근에는 비즈니스 중단 또는 생산성 저하를 야기하는 랜섬웨어와 암호화폐 채굴 악성코드가 늘어나면서 기업에 직•간접적인 위협이 되고 있습니다.

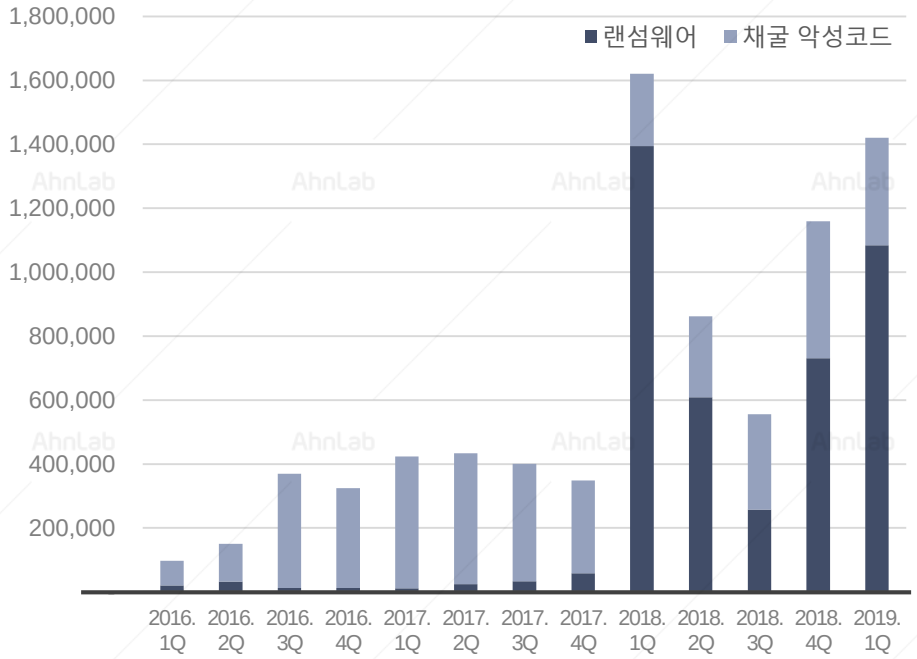
- 악성코드 제작 툴 유포 등으로 악성코드 수의 기하급수적인 증가
- 병원, 공장, 통신업체,웹호스팅 업체, 사회기반 시설 등의 랜섬웨어 감염 사고 발생
- PC 및 서버의 CPU, GPU 성능에 영향을 끼치는 채굴 악성코드 증가

전체 악성코드 추이



(*출처: AV-TEST, 2019년 5월 기준)

랜섬웨어, 채굴 악성코드 추이



(*출처: AhnLab (ASEC), 2019년 5월 기준)

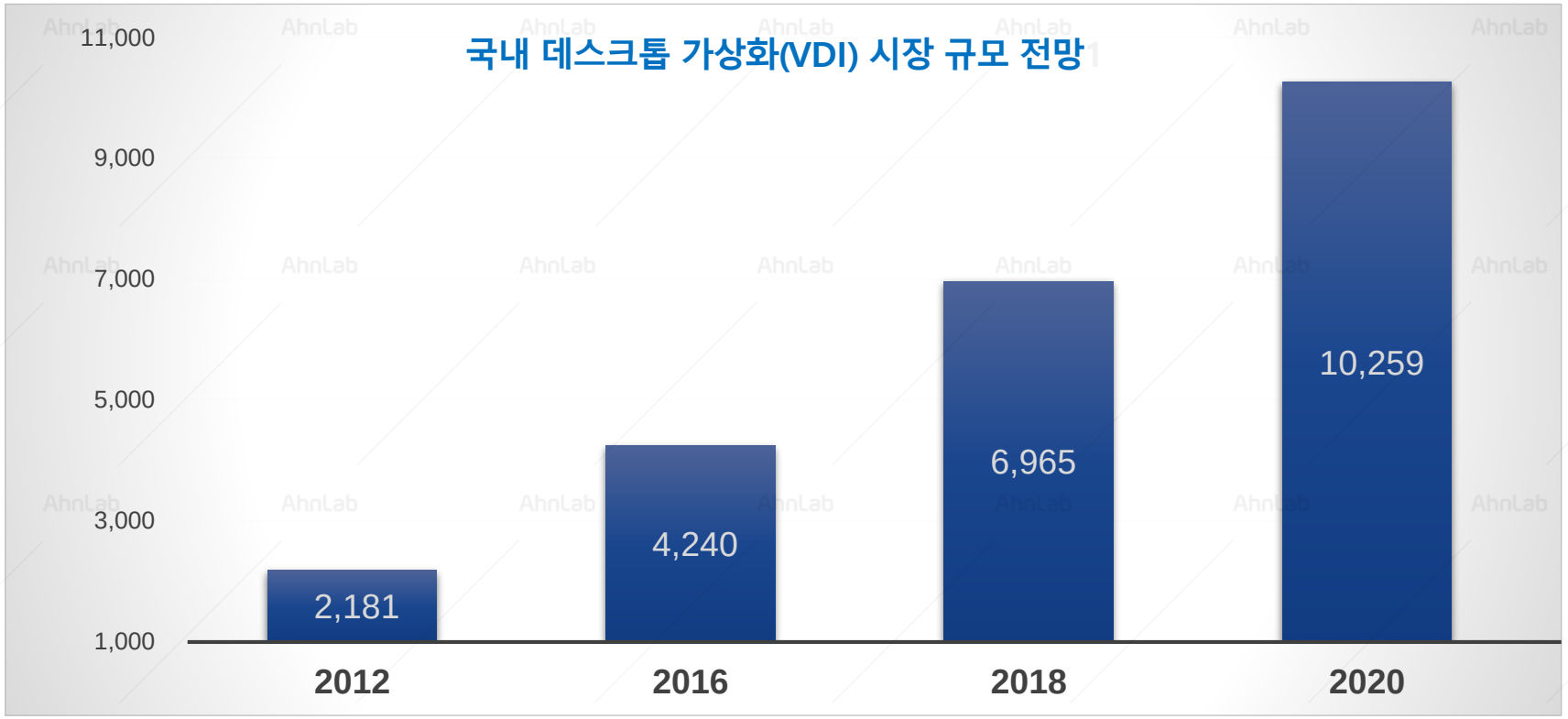
기업의 IT 환경 변화에 따른 보안 위협 증가

최근 비용 절감과 업무 효율화를 위해 클라우드, 가상화 데스크톱(VDI)을 도입하는 기업이 늘어남에 따라 보안 위협 또한 증가하고 있습니다.

- 가상화(VDI, Virtual Desktop Infrastructure) 환경을 업무 시스템에 도입하는 기업 증가
- 리소스 및 비용 효율화 관점에서 VDI를 도입하는 기업이 연평균 30% 이상 늘어날 것으로 전망됨 (CAGR: 36.3%)
- 비즈니스 인프라에서 VDI가 차지하는 비중이 높아짐에 따라 이에 대한 보안 우려 증가

VDI
시장 규모

(단위: 억원)



(*출처: 한국전자통신연구원(ETRI))

VDI 전용 보안 솔루션의 필요성

가상화 데스크톱(VDI) 역시 악성코드 등 기존의 업무 환경과 동일한 보안 위협에 노출되기 쉽습니다. 그러나 시스템 성능 이슈 등 가상화 데스크톱 환경의 특수성 때문에 기존의 보안 솔루션을 도입•운영하기에는 한계가 있습니다.

VDI 시스템에 대한 성능 영향을 최소화한 전용 보안 솔루션 필요

VDI 운영 환경의 특수성

가상화 장비(Virtual Appliance)의 리소스 및 성능 이슈

- 보안 솔루션도 가상화 장비의 공통 리소스(CPU, Memory) 사용
- 엔진 업데이트, 예약 검사에 의한 AV-Storm 우려

VDI 환경에 따른 보안 솔루션 도입 및 운영의 어려움

- VDI 환경의 보안 솔루션 관리 및 정책 설정 제한적
- VDI 환경에 따라 사용자 UI가 없는 경우 존재
- VDI 환경으로의 전환 시 중단 없는 위협 대응 필요

신•변종 악성코드 등 보안 위협 대응의 한계

- 기존 백신의 행위 기반 탐지 기술 활용 제한적
- 증가하는 신•변종 악성코드에 대한 대응 방안 필요

VDI 보안 요구 사항

안정적인 VDI 운영 보장

- 기존 백신의 공통 리소스 사용에 따른 성능 이슈 해소
- VDI 환경의 AV-Storm 방지 및 시스템 영향 최소화를 통한 업무 연속성 유지

최적화된 제공 방식 및 관리 편의성

- 에이전트 방식 및 비에이전트 방식 모두 지원
- 관리자 관점에서의 보안 정책 설정 기능 제공
- AhnLab EPP 및 전용 엔진을 통한 관리

기존 백신과 동일한 수준의 악성코드 대응력

- 시스템 성능 영향을 최소화한 실시간 검사, 예약 검사 등 다양한 기능 제공
- 신•변종 악성코드에 대한 행위 기반 탐지

02
AhnLab V3 for VDI

1. AhnLab V3 for VDI 개요
2. 특장점

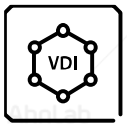
V3 for VDI

AhnLab V3 for VDI는 가상화 데스크톱(Virtual Desktop Infrastructure, VDI) 환경에 최적화된 전용 보안 솔루션으로, 더욱 안정적이며 효율적인 VDI 운영이 가능합니다. 기존의 온프레미스(On-premise) 환경에서 VDI 환경으로의 전환 또는 신규 구축 시에도 기존과 동일한 악성코드 대응이 가능해 비즈니스 연속성 유지에 기여합니다.

VDI에 최적화, VDI 보안도 역시 V3!

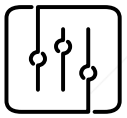
AhnLab V3 for VDI

Agent/Agentless



VDI 전용 엔진으로 시스템 리소스(CPU/메모리) 부담 최소화

- VDI 환경에 최적화된 전용 TS엔진 적용
- SVA(Security Virtual Appliance)에서만 악성코드 검사 및 TS엔진 업데이트 진행
- 각각의 VM에는 ASD엔진, IPS엔진 적용(*V3 for VDI Agent에 한함)



클라이언트 UI 최소화, VDI 환경에서의 중앙관리 최적화

(*V3 for VDI Agent에 한함)

- 클라이언트(Client) UI에서는 주요 기능의 설정 상태 정보만 제공
- AhnLab EPP 기반의 중앙 관리를 통한 효율적인 정책 설정 및 운영

강력한 악성코드 대응을 통한 위협 표면(Attack Surface) 최소화

- 수십억 개의 샘플 DB 및 시그니처 기반의 최신 악성코드 탐지
- 신•변종 악성코드까지 사전에 대응하는 사전 방역
- 다차원 분석 플랫폼 기반의 행위 기반 분석(*V3 for VDI Agent에 한함)

특장점 – VDI 최적화 엔진 적용

VDI 환경에 최적화된 전용 TS엔진을 탑재한 V3 for VDI는 가상화 시스템 성능 저하 없이 악성코드에 대한 강력한 대응 효과를 제공합니다.

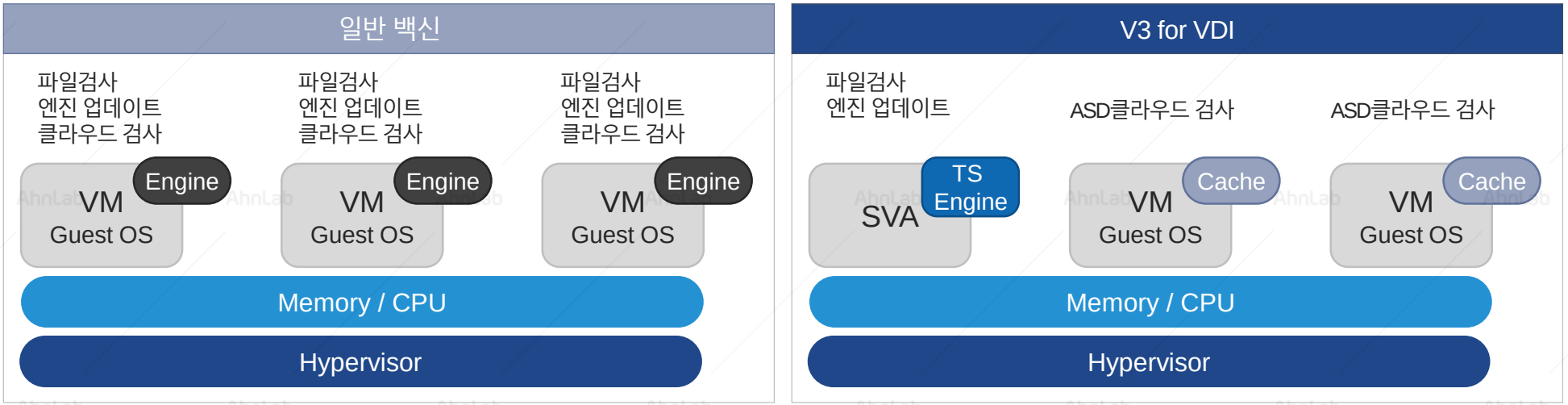
전용 TS엔진 기반의 VDI 환경에 최적화된 악성코드 검사

- 20여 년간 축적된 안랩의 악성코드 대응 기술 및 노하우
- 검사 방식의 이원화: VDI 환경에서는 모든 VM(Virtual Machine)이 아닌 SVA(Security Virtual Appliance)에서만 TS엔진 적용
  - 파일 검사 : SVA에 설치된 TS엔진을 통해 검사 – 각 Guest VM의 Cache 정보 활용
  - 엔진 업데이트 : SVA 에 설치 된 TS엔진 업데이트 - 각 Guest VM은 ASD엔진, IPS엔진만 업데이트

  ※ 참고 : ASD엔진, IPS엔진의 리소스 사용률은 TS엔진의 10% 미만(* V3 for VDI Agent에 한하여 VM에 ASD엔진과 IPS엔진 설치)

VDI 환경에서의 일반적인 백신(Anti-virus) 운영 한계 극복

- 일반 백신: 관리자 정책에 의한 예약 검사 및 엔진 업데이트 수행 시 각 Guest VM의 리소스 사용 집중 → 시스템 부하 발생
- V3 for VDI: 예약 검사 및 TS엔진 업데이트를 SVA에서만 수행 → 시스템 리소스 사용 최소화

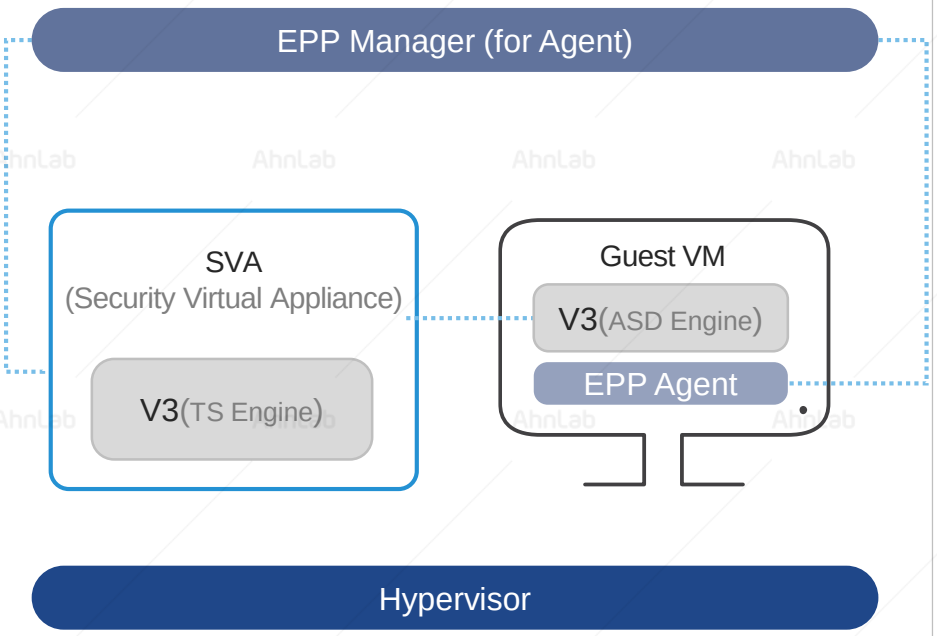


특장점 – 유연한 제공 방식

가상화 환경의 특수성을 다각도로 반영한 V3 for VDI는 고객사 환경에 따라 에이전트(Agent) 방식과 비에이전트(Agentless) 방식으로 제공되며, AhnLab EPP Management와 가상화 전용 TS엔진을 통해 효율적으로 관리할 수 있습니다.

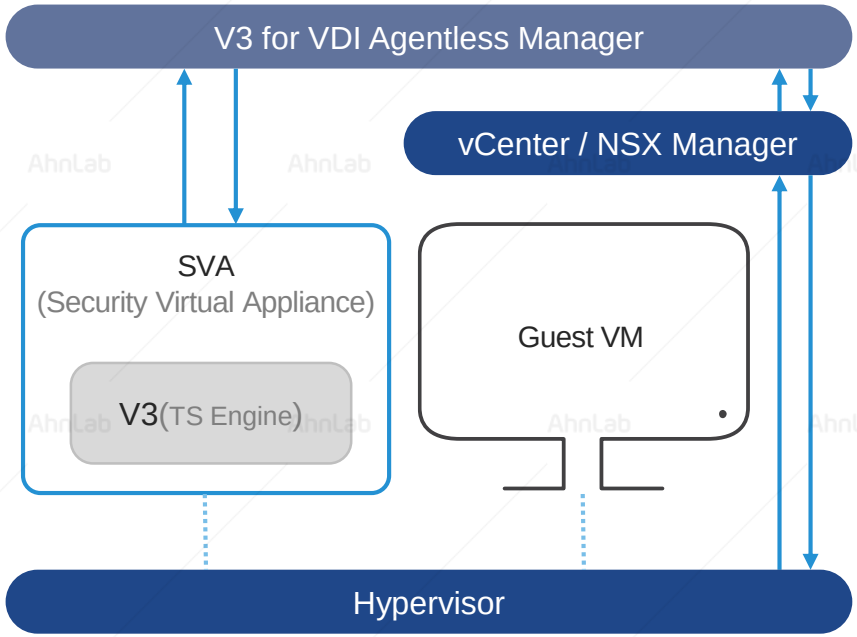
V3 for VDI**(Agent)**

- SVA: TS Engine만 설치
- Guest VM
- - 캐시(Cache) 기능의 경량 백신 및 행위 진단을 위한 ASD 엔진 설치
  - AhnLab EPP 에이전트 설치



V3 for VDI**(Agentless)**

- SVA: TS Engine만 설치
- Guest VM: 설치되는 것 없음



특장점 – 통합 관리 및 위협 대응

V3 for VDI는 차세대 엔드포인트 플랫폼 AhnLab EPP를 기반으로 효율적인 통합 관리가 가능하며, EDR 솔루션 등과의 연계를 통해 더 강력한 위협 대응이 가능합니다. (*V3 for VDI Agent에 한함)

- AhnLab EPP 기반의 통합 관리 및 EDR 연동을 통한 위협 가시성 확보
  - 기존 업무 환경에 VDI 시스템이 추가될 경우에도 AhnLab EPP를 통해 기존에 사용 중인 엔드포인트 보안 관리 솔루션과 통합 관리 가능

특장점 – 관리 강화 및 사용 편의성

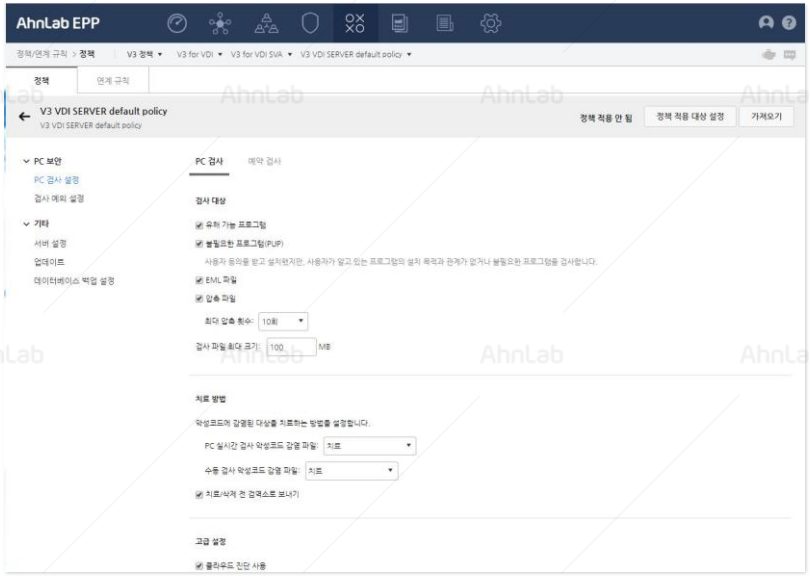
VDI 환경에 최적화된 V3 for VDI를 통해 효율적인 VDI 자산 운용과 보안 관리자의 강력한 보안 정책 적용이 가능합니다.
클라이언트 UI 최적화를 통해 기업의 보안 정책 관련 위험 요소를 사전에 제거하는 효과를 제공합니다. (*V3 for VDI Agent에 한함)

- 관리자 관점의 강력한 보안 정책 지원
- 보안 정책 운영 관점의 클라이언트 UI 최적화
  - 클라이언트 PC에서의 백신 정책 변경 불가
  - 직관적인 UI를 통해 최소한의 정보만 제공

관리자 화면

- 관리자 화면에서만 V3에 대한 세부적인 옵션 설정 가능

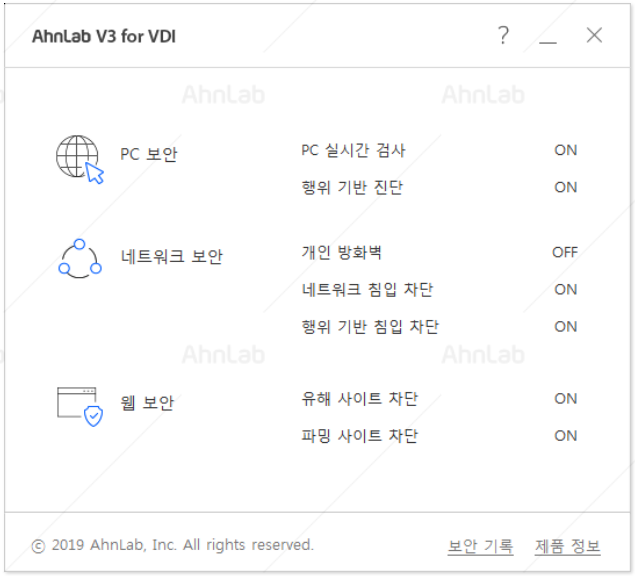
- 사용자 화면에서 설정 불가



사용자 화면

- 심플한 사용자 UI 제공

- 정책 운영 상태만 확인 가능



03
주요 기능 및 사용 환경

1. V3 for VDI Agent
2. V3 for VDI Agentless
3. 타사 제품 비교
4. V3 제품 비교

V3 for VDI Agent

V3 for VDI Agent는 가상화 전용 TS엔진이 적용되어 있으며 엔드포인트 보안 플랫폼 AhnLab EPP를 통해 통합 관리가 가능합니다.

주요 기능

구분	주요 기능	
악성코드 대응	• ASD(AhnLab Smart Defense) 클라우드 네트워크 사용 • 행위 검사(클라우드 행위 검사 포함) • DNA 스캔(Scan) 지원 • 무결성 검사	• 실시간 검사, 사전 검사, 정밀 검사(수동) , 예약 검사 • 제품 보호(보호대상:파일, 프로세스, 레지스트리, 볼륨) • 압축 파일 검사, USB 드라이브 자동 검사 • 악성코드 초기 실행 방지(ELAM), CD/USB 드라이브 자동 실행 방지 • 검사 예외 설정(폴더, 파일, 확장자, 악성코드명 기준)
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) • 신뢰할 수 있는 IP와 차단해야 할 IP 등록 • 공격 IP 임시 차단	• 개인 방화벽 (네트워크 완전 차단, 신뢰 프로그램 판단 기준 설정, 방화벽 정책 목록, 포트 숨김) • 유해 사이트 차단(피싱 사이트 차단, 불필요한 사이트(PUS) 차단) • 파밍 사이트 차단(파밍 사이트 연결 차단)

사용 환경

SVA 권장 사양 (* Guest VM 30대~50대 기준)	
vCPU	4 Core
Memory	8 GB
HDD	64 GB 이상 여유 공간

소프트웨어 요구 사항	
VDI 솔루션	• VMware : ESXi Server 6.0이상, vCenter 6.0 이상 • Citrix : XEN Server 7.1 이상
시스템 운영체제	• Windows 7 / 8 (8.1 포함) / 10 • Windows Server 2008(R2 포함) / 2012 / 2016 /2019 * 상기 OS의 32bit 및 X64 계열의 64bit 지원
지원 언어	한국어, 영어, 중국어(간체)

V3 for VDI Agentless

V3 for VDI Agentless는 VMware NSX에서 제공하는 API를 기반으로 최적화된 보안을 제공합니다.

* VMware NSX API에서 제공하는 기능만 지원 가능

주요 기능

구분	상세 기능
악성코드 대응	• 실시간 검사, 정밀 검사(수동), 예약 검사 • 검사 대상 설정 - 불필요한 프로그램(PUP) • 프록시 서버 지원 • 무결성 검사, DNA 스캔(Scan) 지원 • 압축 파일 검사 • 검사 예외 설정: 폴더, 파일, 확장자, 악성코드명 기준 • ASD(AhnLab Smart Defense) 클라우드 네트워크 사용

사용 환경

V3 for VDI Agentless Manager 권장 사양	
CPU	8 Core 이상
Memory	32 GB
HDD	128 GB 이상 여유 공간

SVA 권장 사양	
vCPU	2 Core 이상
Memory	2 GB
HDD	16 GB 이상 여유 공간

소프트웨어 요구 사항	
VDI 솔루션	• VMware NSX : ESXi Server 6.5 이상/ vCenter 6.5 이상/ NSX Manager 6.4 이상 * VMware NSX만 지원
시스템 운영체제	• Windows 7 / 8 (8.1 포함) / 10 • Windows Server 2008(R2 포함) / 2012 / 2016 * 상기 OS의 32bit 및 X64 계열의 64bit 지원
지원 언어	한국어, 영어

타사 제품 비교 (Agent/Agentless)

기능 구분	AhnLab		T 사		S 사		K 사	
	Agent	Agentless	Agent	Agentless	Agent	Agentless	Agent	Agentless
실시간 검사	O	O	O	O	O	O	O	O
수동/예약 검사	O	O	O	O	O	O	O	O
행위 기반 진단	O		O		O		O	
압축 파일 검사	O	O	O	O	O	O	O	O
유해 사이트 차단	O		O		O		O	
개인 방화벽	O		O		O		O	
악성 웹/피싱 차단	O		O		O		O	
네트워크 침입차단 (IPS)	O		O		O		O	
검사 예외 설정	O	O	O	O	O	O	O	O
로그/검역소	O	O	O	O	O	O	O	O
Stable 엔진	O	O						

자사 제품 비교

V3는 20여 년간 축적된 안랩의 악성코드 대응 기술과 노하우가 적용된 글로벌 수준의 안티멀웨어(Anti-malware) 솔루션입니다.
다양한 V3 제품 중에서 VDI 환경에 최적화된 V3 for VDI를 통해 효율적이며 효과적인 가상화 환경 보호가 가능합니다.

구분	일반 V3	V3 for VDI	
		Agent	Agentless
VDI 환경 지원	• VMware • Citrix • KVM	• VMware • Citrix (* KVM, Hyper-V는 추후 반영 예정)	• VMware Only (* Agentless는 VMware NSX만 지원함)
장점	• 모든 가상화 솔루션에서 사용 가능 • V3의 모든 기능 운영	• 하이퍼바이저 종속성 적음 • 행위 기반 진단 지원 • 가벼운 리소스 운용 • AhnLab EPP 기반의 통합 운영 가능	• VMware NSX를 통한 자동 격리 – VMware 환경에 최적화 • VM에 백신이 설치되지 않음 - 관련 리소스 사용 없음
단점	• 모든 VM에 TS엔진, ASD엔진 설치 - 예약 검사 및 엔진 업데이트 이슈 • 엔진 업데이트 시 리소스 사용으로 인한 성능 저하 가능성 – 불필요한 리소스 사용	• 일반 V3 대비 일부 기능 제약	• VMware NSX만 지원 • 파일 검사 및 진단만 가능 (행위 기반 진단 불가능) • 클라이언트 UI 없음 • 전용 Management 지원

04
주요 기술 및 대응 체계

1. 다차원 분석 플랫폼
2. 클라우드 기반 탐지
3. 시그니처 기반 탐지
4. 입체적인 대응 서비스
5. 전문 고객 지원 프로세스

다차원 분석 플랫폼

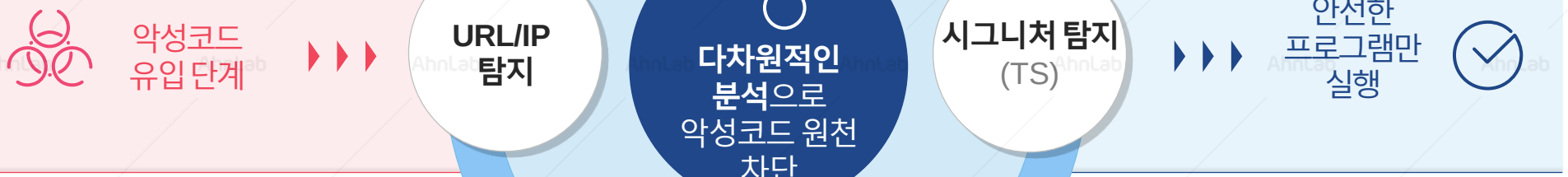
V3 for VDI는 안랩의 독자적인 다차원 분석 플랫폼(Multi-dimensional Platform)의 핵심 기술을 기반으로 VDI 환경에서도 빠르고 정확한 악성코드 탐지를 제공합니다. (* V3 for VDI Agent에 한 함)

URL/IP 탐지

- 악성코드가 PC로 다운로드 되기 전 시그니처 업데이트 없이 실시간 반영

클라우드 탐지(ASD)

- 25억여 개의 DB정보에서 실시간 확인
- 시그니처 업데이트 없이 실시간 반영



행위 기반 탐지

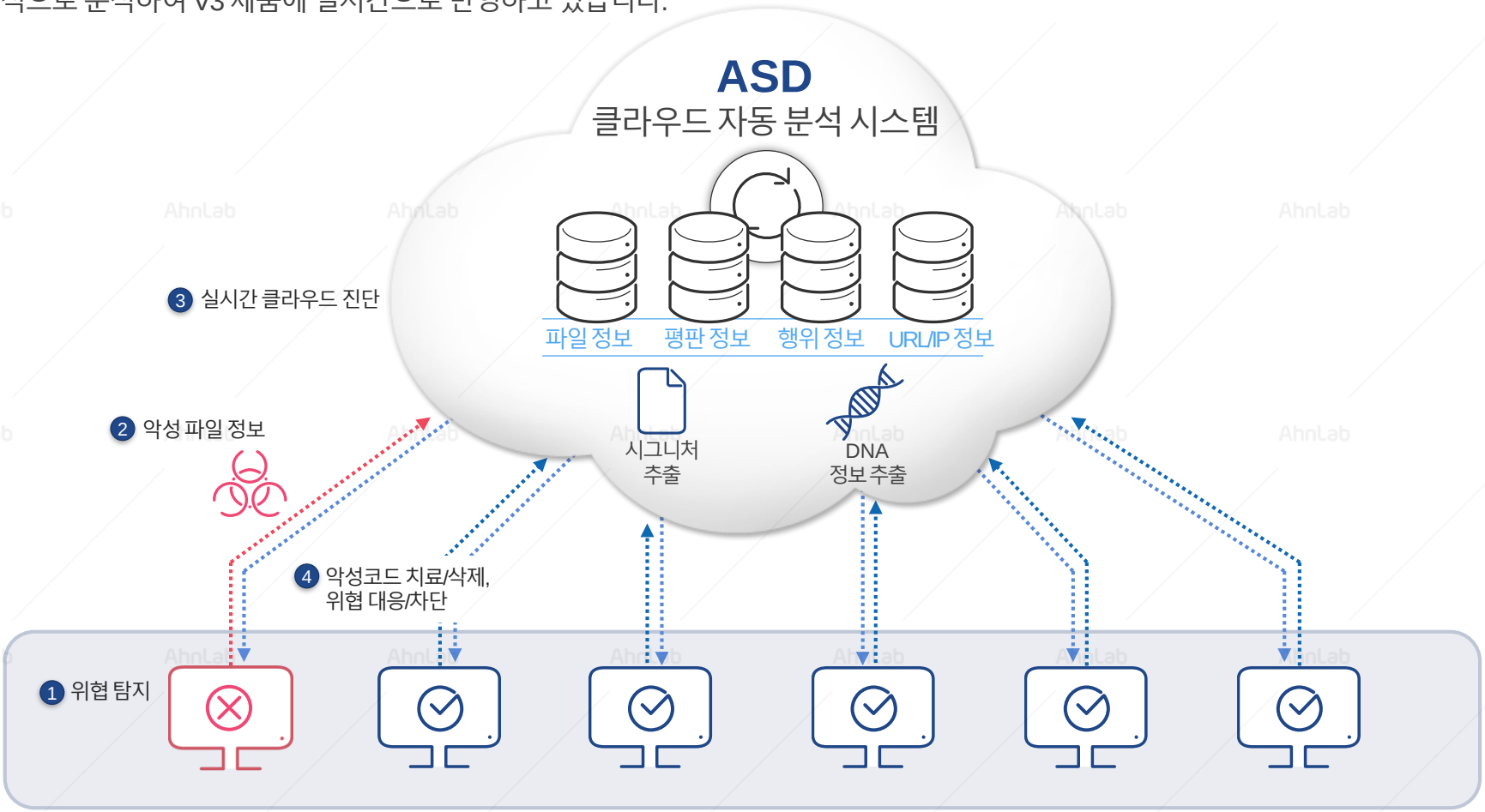
- 제로데이 취약점 원천 차단
- 시그니처 업데이트 없이 사전 진단
- 1,000 여 개의 악의적 행위 패턴 탐지

시그니처 탐지(TS)

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

클라우드 기반 탐지

안랩은 ASD 네트워크에 연결된 수천만 대의 PC에서 실시간으로 공유되는 실제 위협 정보를 기반으로 V3 제품의 악성코드 탐지 정확도를 극대화합니다. 또한 클라우드 기반 자동 분석 시스템인 ASD를 통해 악성코드뿐만 아니라 악성 URL 정보, C&C 서버 IP 정보, 평판 정보를 종합적으로 분석하여 V3 제품에 실시간으로 반영하고 있습니다.

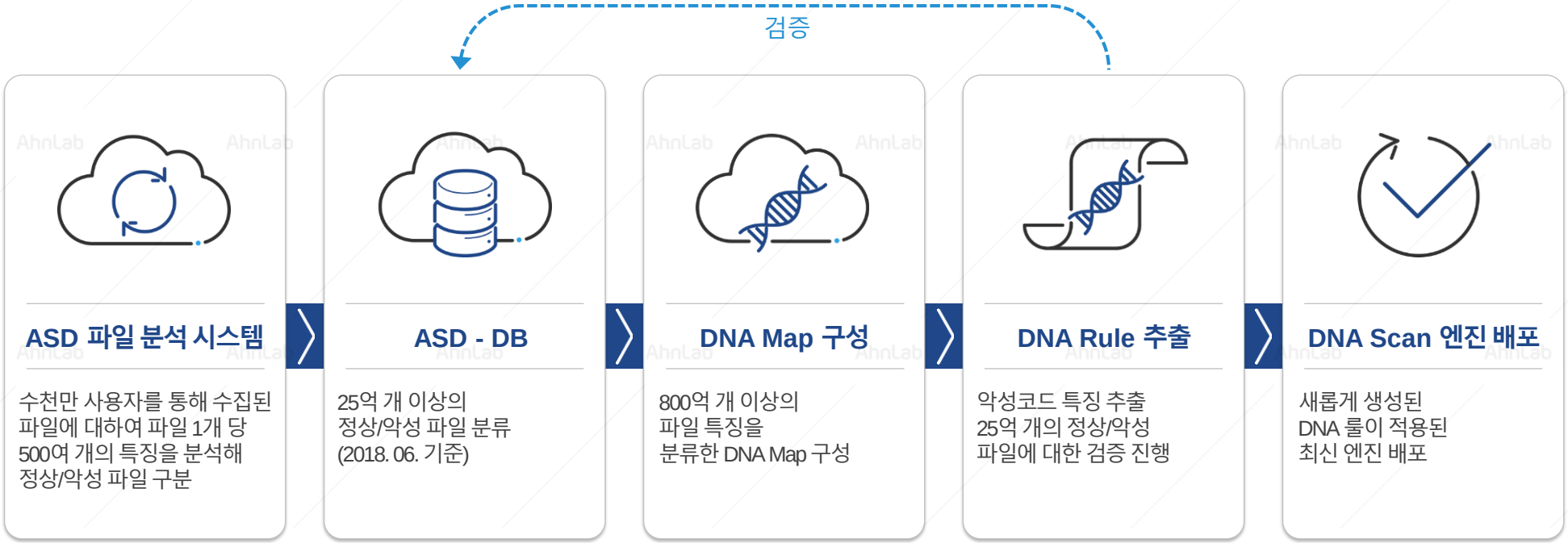


수천만 명 이상의 사용자로 구성된 ASD 네트워크를 통한
악성코드 정보 실시간 분석 및 대응

시그니처 기반 탐지

20여년 간 축적된 악성코드 분석 노하우를 바탕으로 안랩이 독자적으로 개발, V3에 탑재된 TS 엔진은 ▲안티바이러스 시그니처 ▲안티스파이웨어 시그니처 ▲네트워크 시그니처를 DNA 룰 방식으로 제공해 최신 악성코드에 신속하고 정확한 대응이 가능합니다.

- 네트워크 쿼리 없이 엔진 형태로 제공되는 독보적 휴리스틱 진단 제공
- 분석가의 경험에 의존적인 일반 휴리스틱 진단법과 달리,
  ASD 네트워크에 접속하는 수천만 명 사용자 기반의 25억 개 이상의 파일에 대한 검증 후 엔진 반영
  → 타사 대비 휴리스틱 진단법 오진 확률 최소화



입체적인 대응 서비스

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

AhnLab

20여 년간 축적된 악성코드 분석 능력과 대응 경험을 통해
안전한 컴퓨팅 환경 조성과 함께 기업 비즈니스 연속성에 기여합니다.

안랩은 30년간 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.

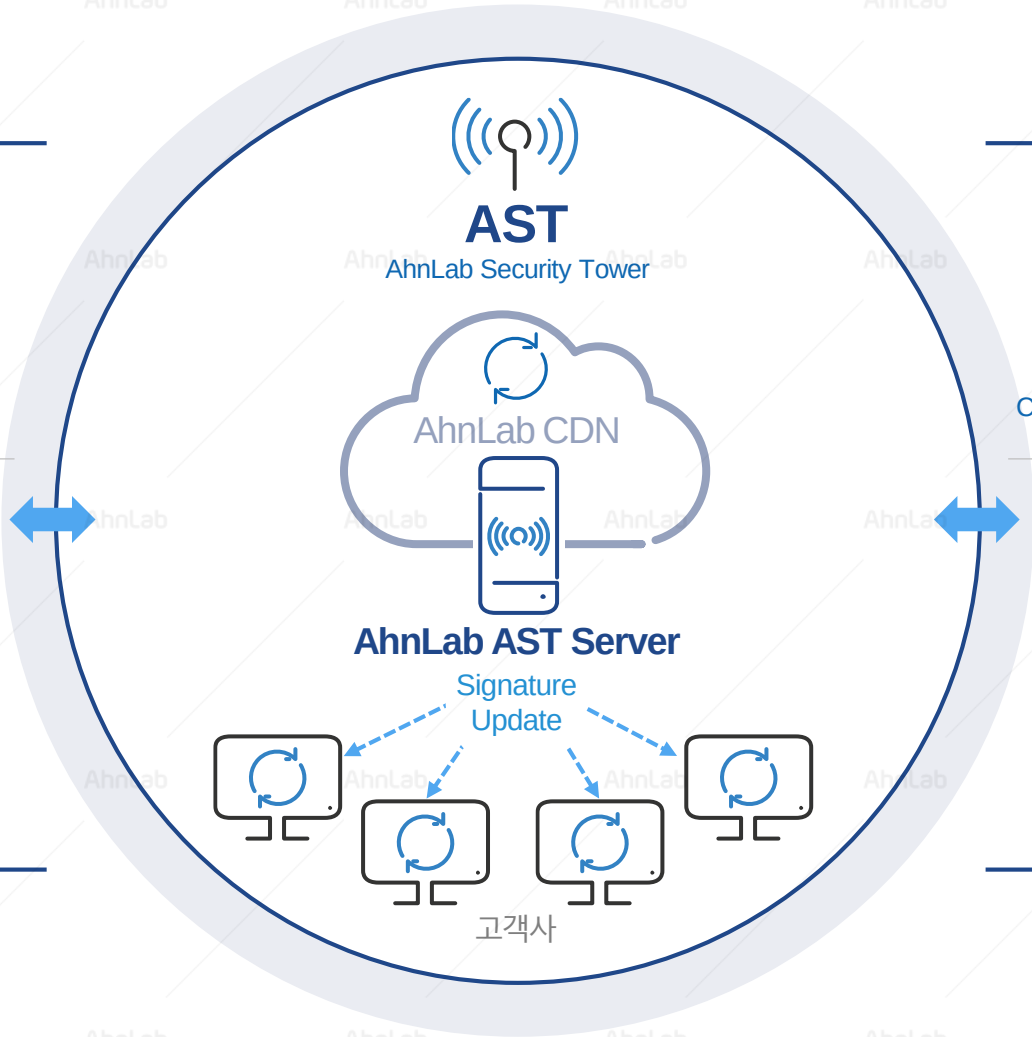
24시간 × 365일 ASEC 대응센터의 전문 인력이 위협을 모니터링하며 대응하고 있습니다.
일일 정기 업데이트 및 긴급 업데이트를 수행함으로써 발 빠르게 악성코드에 대처합니다.

전문 고객 지원 프로세스

위협 분석 및 대응에 대한 오랜 노하우와 경험을 토대로 체계적이며 전문적인 지원 서비스 제공을 약속합니다.

ASEC
AhnLab Security E-response Center

- 보안 위협 모니터링
- 악성코드 수집 및 분석
- 피해 접수 및 대응
- V3 엔진 개발
- 네트워크 분석/모니터링
- 사전 대응



CERT
Computer Emergency Response Team

- 관제 고객 대상 실시간 공격/위협정보 수집
- ASEC에 실시간 공격/위협정보 전달

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 for VDI

AhnLab