Ver 1.0.1

More security,
More freedom

AhnLab CPP

하이브리드 환경을 위한 서버 워크로드 보안 플랫폼

표준제안서

AhnLab

목차

01 제안 배경

02 AhnLab CPP

01
제안 배경

1. 클라우드 환경 도입 증가
2. 클라우드 환경에서의 기업 책임 범위
3. 하이브리드 클라우드 환경에서의 통합 관리 필요성
4. 클라우드 환경에서의 네트워크 보안 요구
5. 클라우드 환경에서의 시스템 보안 요구

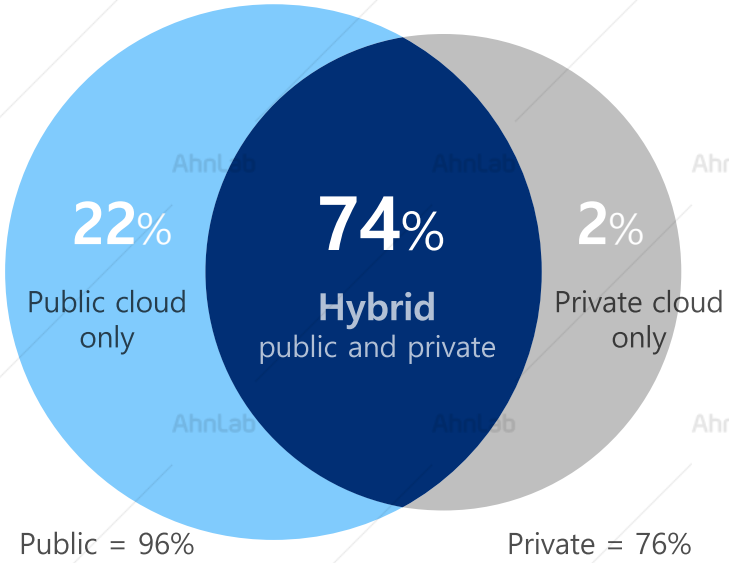
클라우드 환경 도입 증가

클라우드 도입 증가와 함께 비즈니스의 확장성, 안정성 등을 고려하여 하이브리드·멀티 클라우드 전략 채택이 증가하고 있습니다.

- **[해외]** 98% 클라우드 도입(퍼블릭 클라우드 활용: 96%, 멀티 클라우드 사용: 93%)

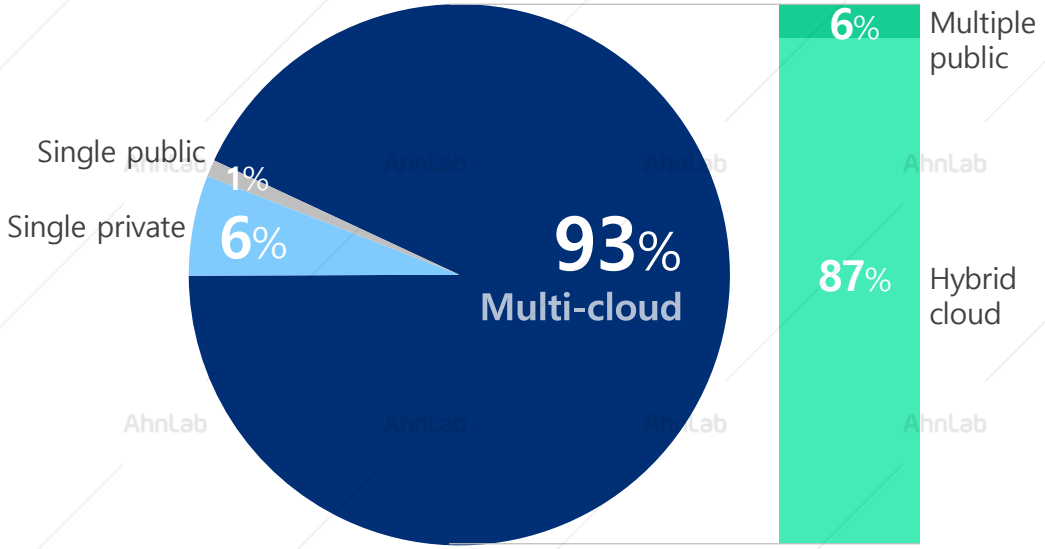
Types of Cloud Used

% of all respondents



Enterprise Cloud Strategy

% of enterprise respondents

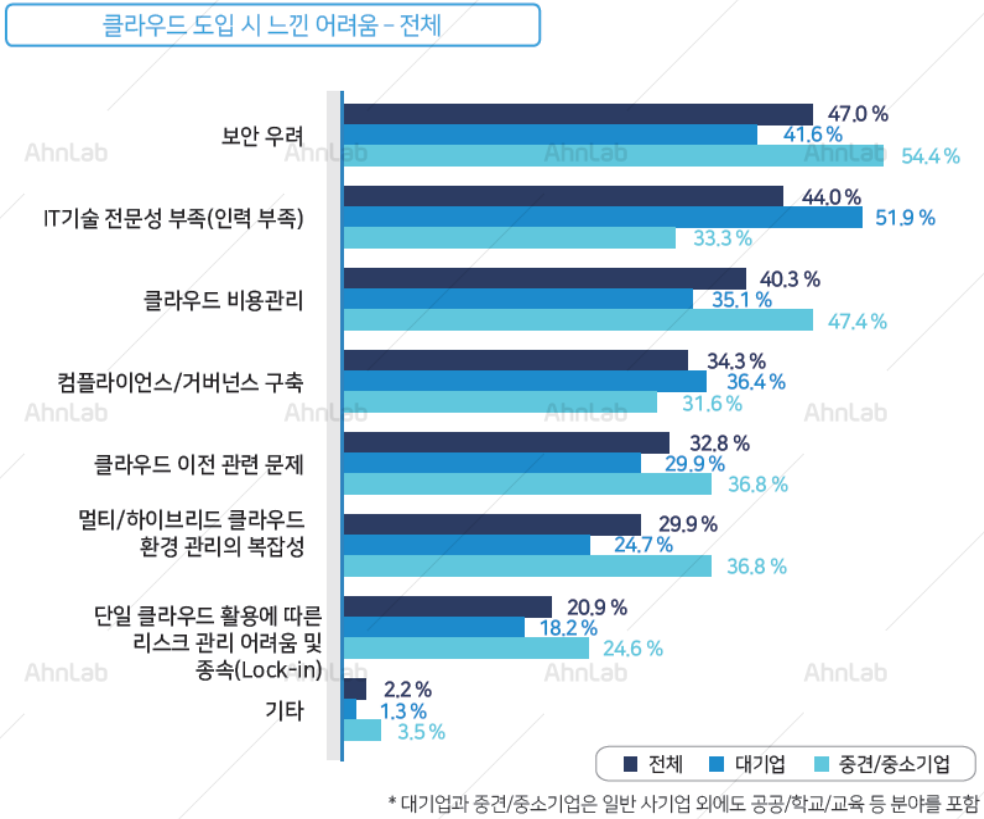


조사 대상: 750개 기업

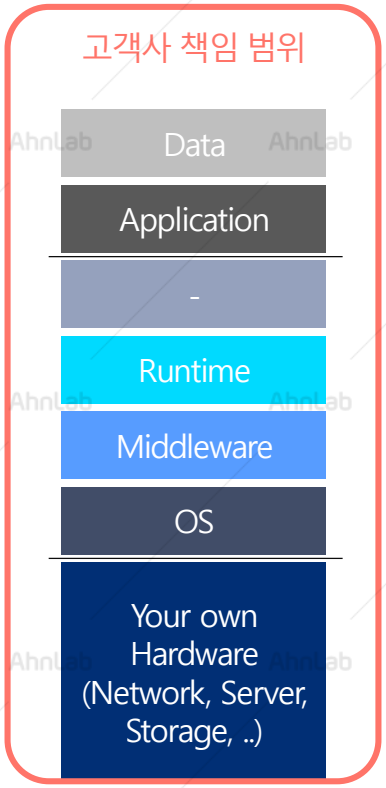
*출처: 플랙세라(Flexera)의 '라이트스케일 2020 스테이트 오브 더 클라우드' 보고서

클라우드 환경에서의 기업 책임

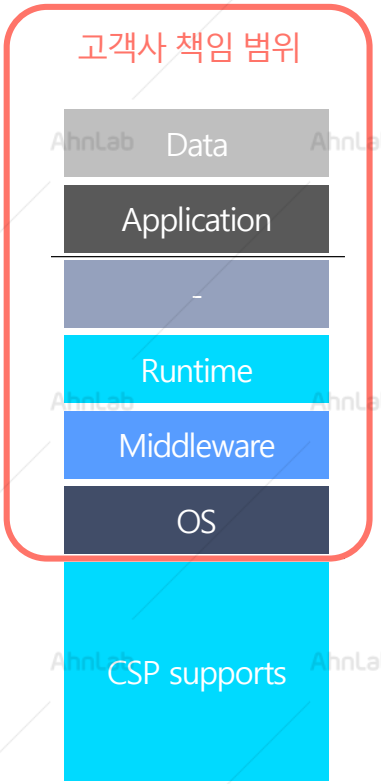
클라우드 환경에서는 보안은 책임 공유 모델(Shared Responsibility Model)로 고객사의 책임은 그대로 존재합니다.



*출처: 베스핀글로벌 – '2019 State of Cloud Adoption in Korea' 보고서



On-premise



Cloud(IaaS)

하이브리드 클라우드 환경에서의 통합 관리 요구

서버 환경 범위가 온프레미스에서 클라우드까지 확장됨에 따라 하이브리드 환경에서의 유기적인 보안 위협 관리 및 대응에 대한 요구가 증가하고 있습니다.

“ 하이브리드 클라우드 환경에서의 **통합 보안 관리 체계 필요** ”

기업 전체 서버 워크로드에 대한
통합 가시성 확보

서비스 제공 환경을 고려한
보안 위협 최소화

서버 워크로드 보안 위협에 대한
신속한 탐지 및 대응

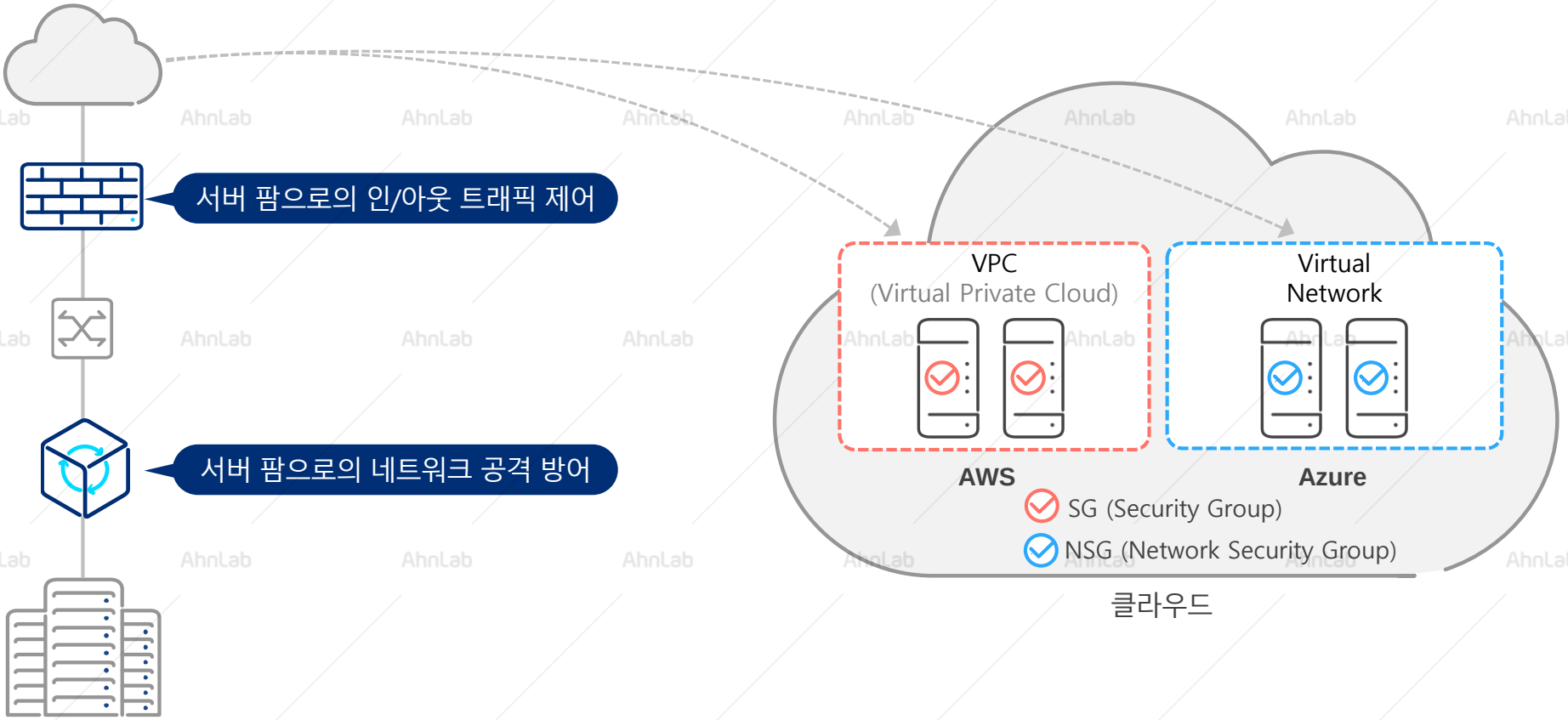
조직 내 자산 범위 증가
온프레미스 뿐만 아니라 클라우드 서버 고려 필요

네트워크 보안 위협 증가
자산으로의 접근 경로 제어 불가

사회공학기법, 표적 · 지능형 공격
악성코드 감염 및 서비스 장애 증가

클라우드 환경에서의 네트워크 보안 요구

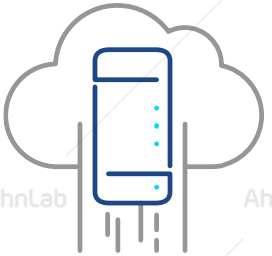
외부에서 내부로의 트래픽에 대한 강력한 제어가 가능한 온프레미스 환경과 다르게
클라우드 환경에서는 서버 워크로드가 고객사가 아닌 CSP 환경 내 존재함으로써 서버 워크로드 자체의 네트워크 보안 필요성이 증가하고 있습니다.



클라우드 환경에서의 시스템 보안 요구

클라우드 환경에서는 유동적으로 관리 및 운영되는 서버에 대한 가시성이 매우 중요합니다.
또한 온프레미스 환경과는 달리 사전에 정의된 이미지(애플리케이션)만 사용해 효율성을 향상시키고 안정적인 서버 운영이 가능해야 합니다.

VS



온프레미스		클라우드
필요 자원 사전 정의(변경 어려움)	운영 환경	오토스케일링 · 자원 확장 용이
H/W, S/W, OS, 설치에서 관리까지 모두 관리		사전 정의된 이미지 활용
서버 환경 상이(H/W, S/W , OS 등)		동일 서버 환경 다수(H/W, S/W, OS 등)
서버 목록 고정적	요구 사항	서버 목록 유동적(**서버 가시성 중요**)
서버 환경(S/W) **자산관리 중요**		서버 환경(S/W) 변경 범위가 매우 적음
안정적인 서버 운영 중요		**안정적인 서버 운영 중요**

02
AhnLab CPP

1. 개요
2. 특장점
3. 주요 기능
4. 도입 효과
5. 운영 환경

개요

AhnLab CPP는 서버 워크로드 보호에 필요한 다양한 보안 기능을 유기적인 연동 및 통합 운영 지원하는 보안 플랫폼으로
서버에 대한 체계적이며 효율적인 위협 관리 및 대응을 제공합니다.

“서버 워크로드 중심의 보안 위협 관리 및 대응 플랫폼”

AhnLab CPP

효율적인
서버 통합 관리 및 보안

- 온프레미스와 함께 클라우드(AWS, Azure)에서 운영되는 서버에 대한 통합 관리 지원
- 안랩 서버 보안 솔루션에 대한 유기적인 통합 운영 및 관리 지원

최적화된
위협 관리 및 대응

- 직관적인 대시보드를 통해 보안 위협에 대한 모니터링 및 가시성 제공
- 안랩 서버 보안 솔루션 간 연계 규칙 제공을 통해 조직에 최적화된 위협 대응 체계 지원
- Syslog, 오픈 API 제공을 통해 서드 파티 솔루션(SIEM, 통합로그분석시스템 등)과의 쉽고 간편한 연동 지원

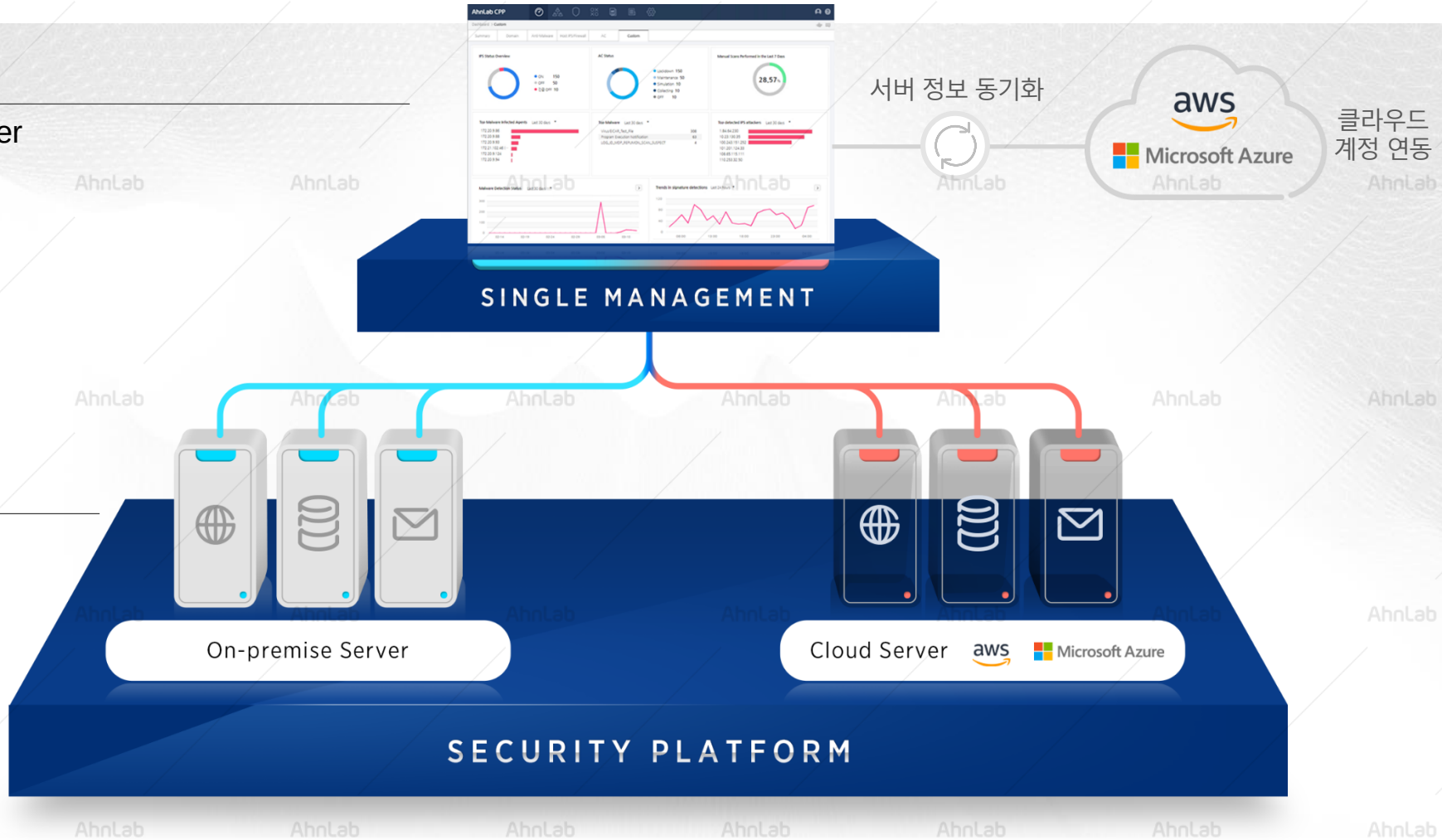
차별적인
비용(TCO) 절감 효과

- 모듈화된 서버 구성 지원으로 고객사 환경에 맞춘 유연한 구성 및 확장 가능
- 업무 특성에 필요한 보안 솔루션 라이선스만 적용함으로써 보안 솔루션 도입 및 관리 비용 효율성 향상

특장점 – 하이브리드 환경에서의 서버 워크로드 가시성

AhnLab CPP는 온프레미스, 그리고 퍼블릭 클라우드(AWS, Azure) 환경의 서버 워크로드에 대한 통합된 가시성을 제공합니다.

- 클라우드 계정 연동을 통해, 오토스케일링(Autoscaling) 되는 워크로드에 대한 자동화된 식별 지원



특장점 – 단일 매니지먼트 · 다양한 보안 기능

플랫폼 기반의 단일 관리 콘솔에서 서버 워크로드 보안 요구사항을 충족하는 다양한 보안 기능을 제공합니다.

CPP Manager

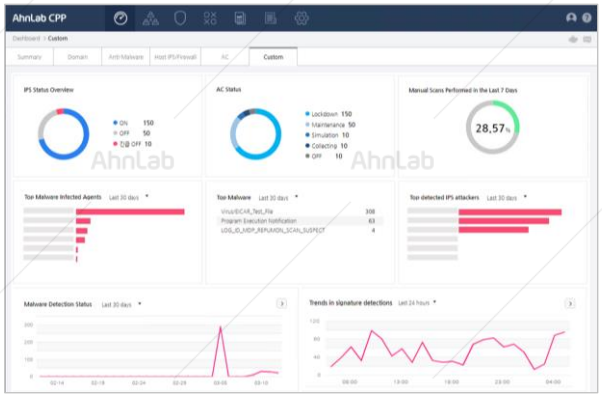
Agent

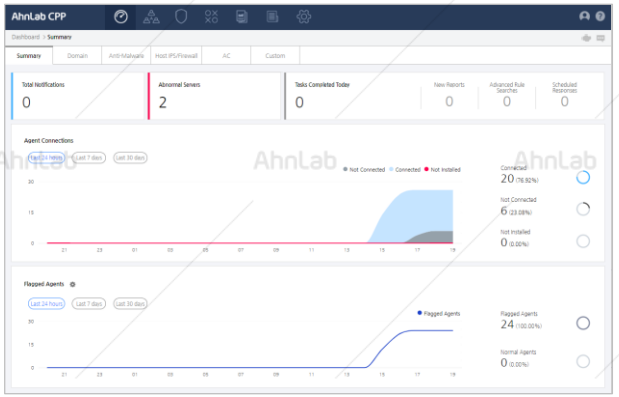
특장점 – 직관적인 가시성 제공

다양한 대시보드, Syslog, 오픈 API 를 통한 외부 솔루션과의 연동을 지원함으로써 위협에 대한 직관적인 가시성 및 대응을 지원합니다.

편리한 사용자 인터페이스를 통한 직관적인 가시성 제공

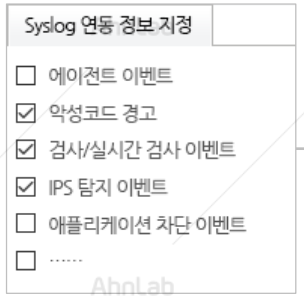
- 다양한 대시보드 지원
- 서버 보안 상태를 한눈에 파악할 수 있는 가시성 제공

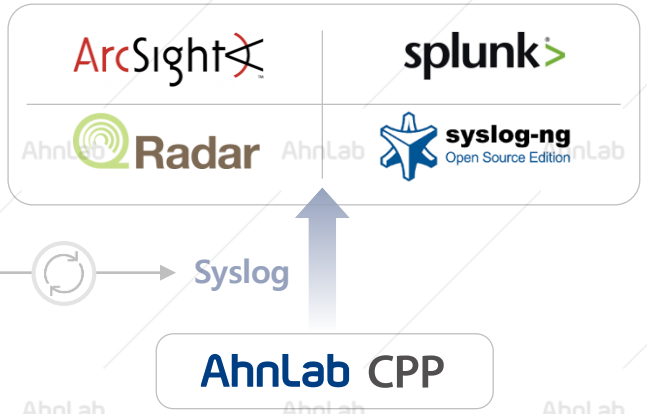




외부 시스템과의 유연한 연동 지원

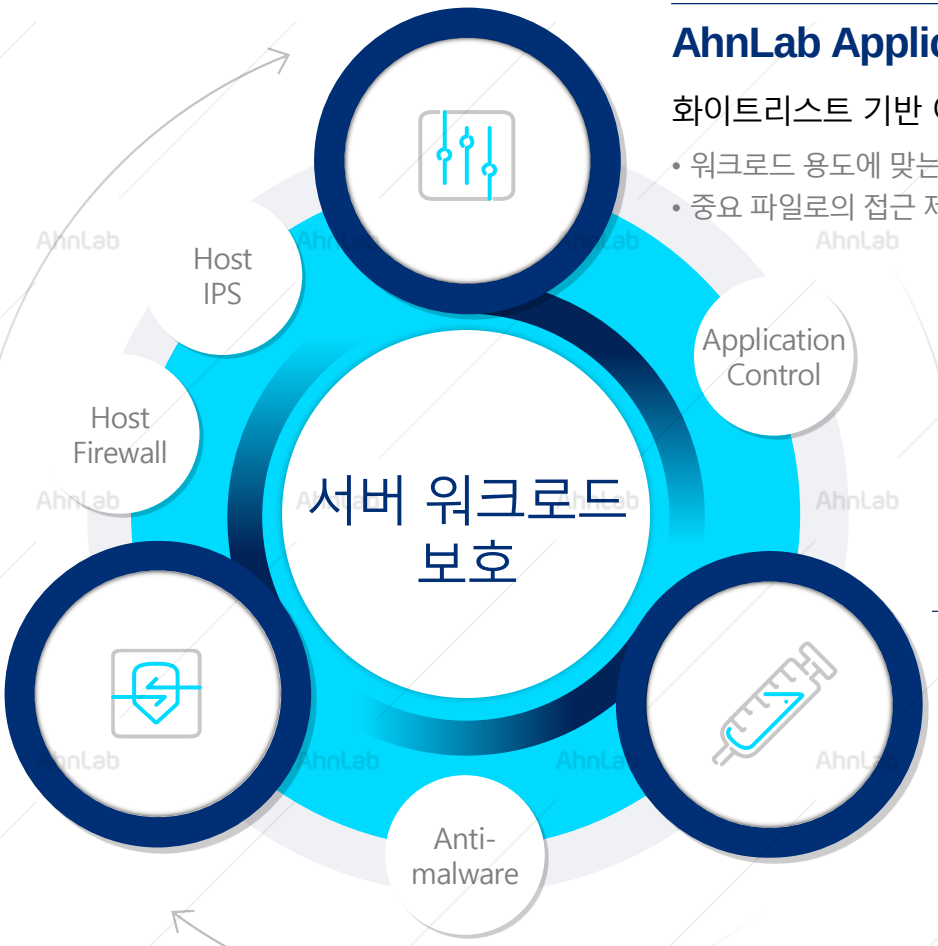
- Syslog, 오픈 API 연동 지원
- 다양한 솔루션(SIEM, ESM 등)과의 원활한 연동을 통해 보안 관제 효과 향상





주요 기능

AhnLab CPP 는 다양한 보안 기능을 기반으로 지능화된 위협으로부터 서버 워크로드를 보호합니다.



AhnLab Application Control

화이트리스트 기반 어플리케이션 제어

- 워크로드 용도에 맞는 어플리케이션만 실행 허용
- 중요 파일로의 접근 제어로, 서비스 안정성 보장

AhnLab Host IPS

네트워크 공격 탐지/방지

- 시그니처 기반 네트워크 침입 공격 탐지 및 차단
- 시그니처 추천 지원
- IP, Port , 프로토콜 기반 통신 제어
- 국가 차단(IP 기반) 지원

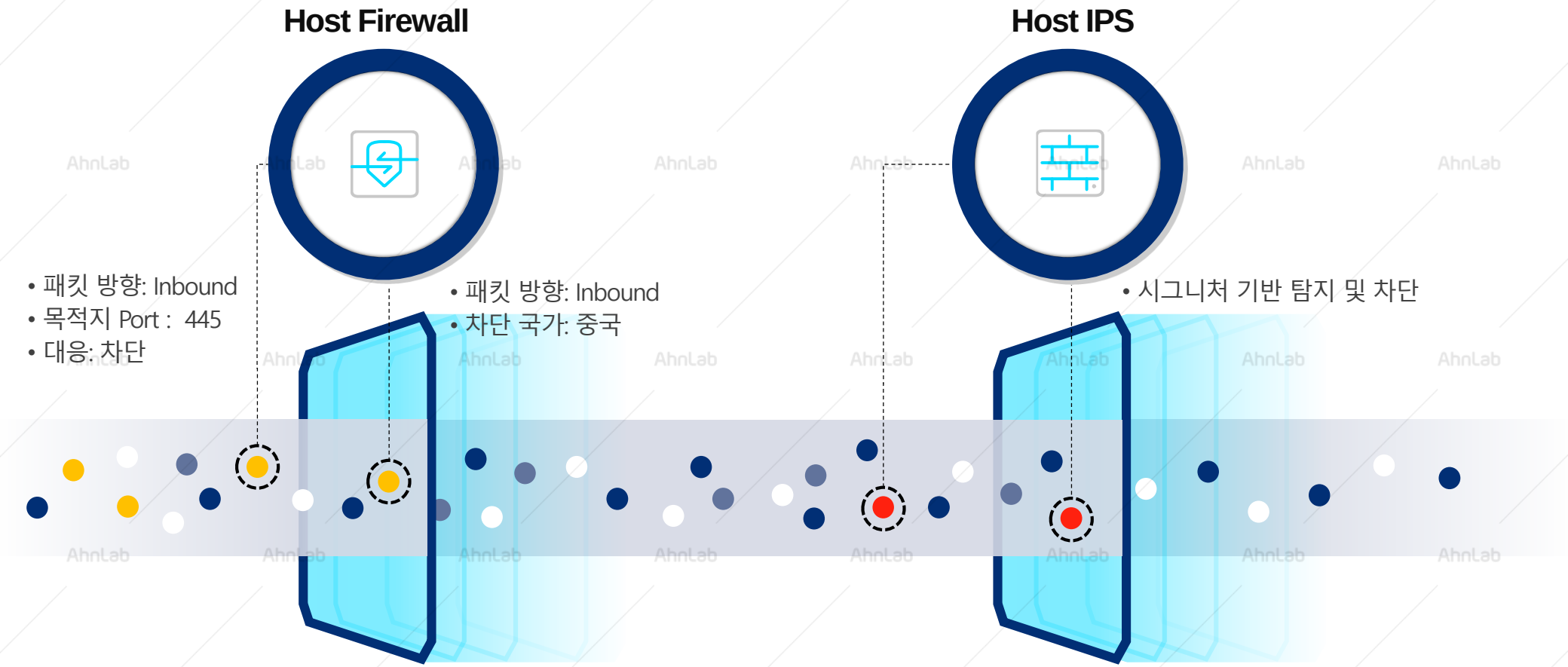
AhnLab V3 Net

악성코드 탐지/대응

- 수동/예약 검사
- 실시간 검사
- 검사 성능/리소스 이슈 최소화

주요 기능 – AhnLab Host IPS (1/6)

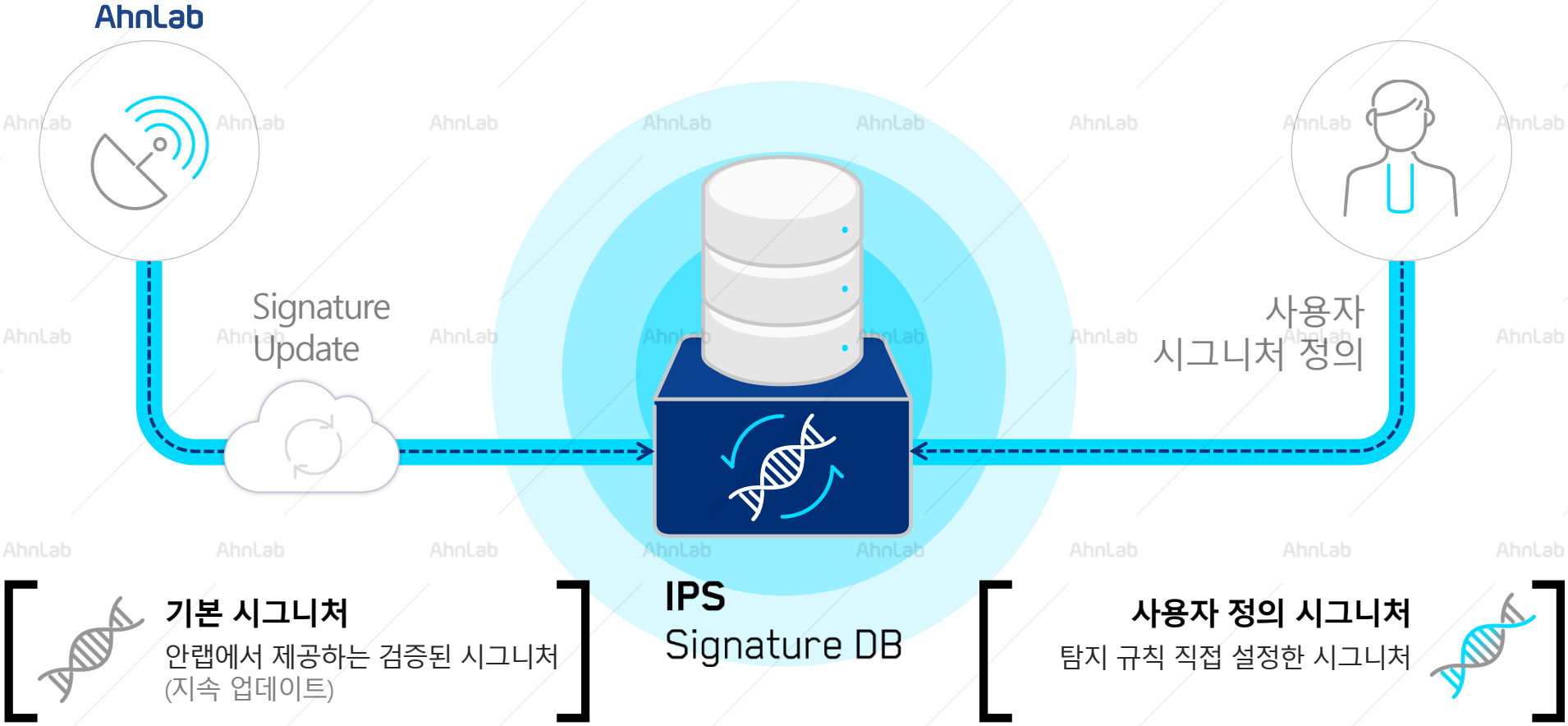
서버 호스트로 인/아웃되는 트래픽을 모니터링하고 네트워크 패킷에 대한 방화벽 기능을 제공합니다.
또한 시그니처 기반 특정 패턴의 트래픽을 탐지해 네트워크 공격으로부터 서버를 안전하게 보호합니다.



주요 기능 – AhnLab Host IPS (2/6)

자사 전문가와 Network IPS(AIPS)를 통해 이미 국내에서 검증된 수천 개의 IPS 시그니처를 기본 제공합니다.
또한 시그니처에 대한 사용자 정의를 지원, 조직에 필요한 IPS 시그니처를 직접 설정할 수 있습니다.

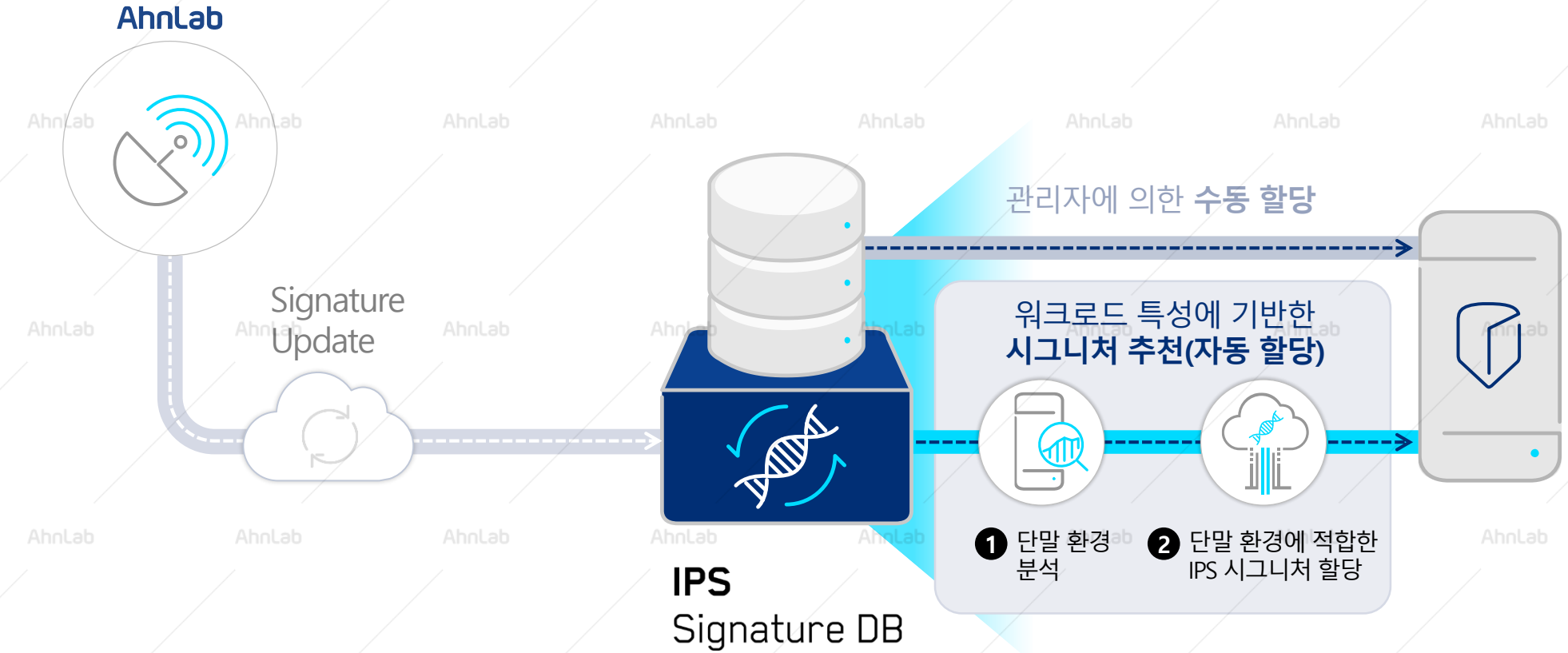
IPS 시그니처 정의 방식



주요 기능 – AhnLab Host IPS (3/6)

서버 워크로드 환경을 분석, 단말의 취약점을 대응할 수 있는 최적화된 IPS 시그니처를 자동 할당 및 추천(Recommendation)합니다.

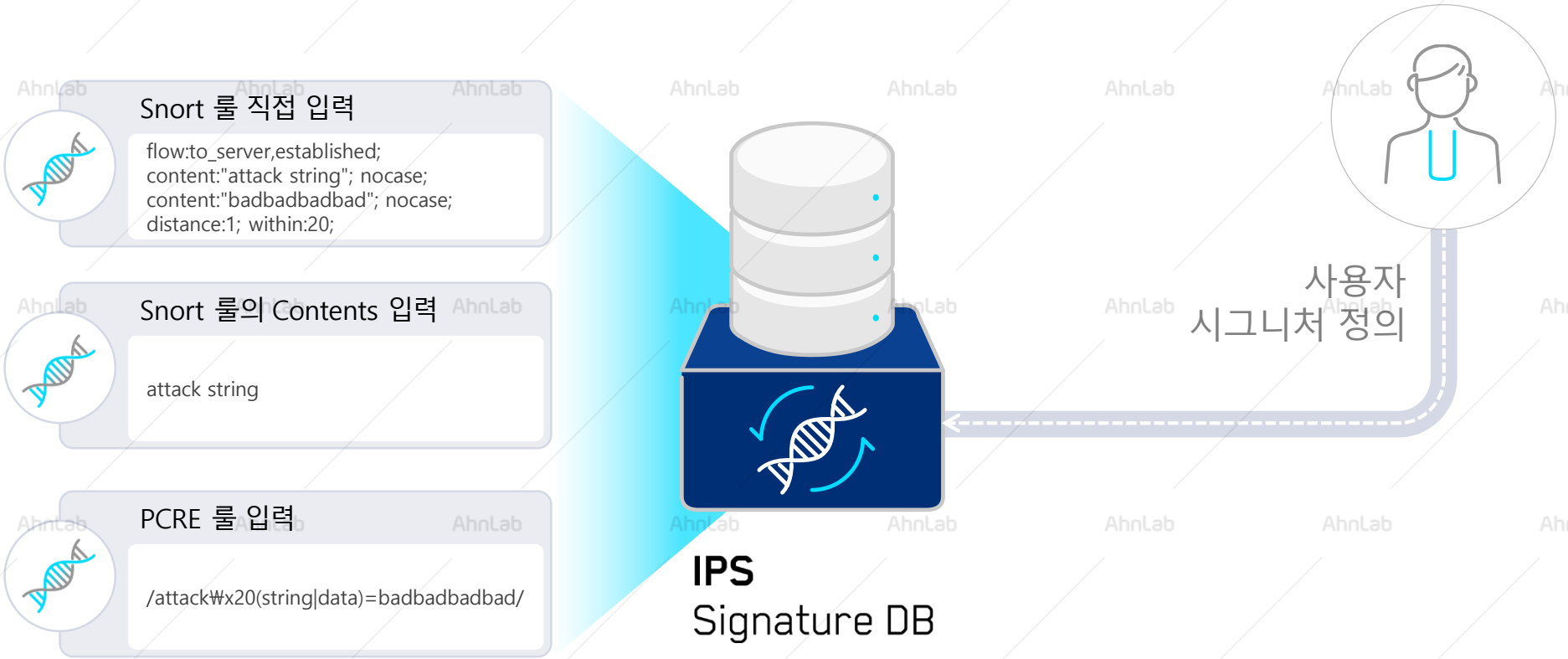
IPS 시그니처 할당 방식



주요 기능 – AhnLab Host IPS (4/6)

IPS 시그니처 사용자 정의 시 Snort, PCRE 지원으로 보다 손쉬운 설정을 지원합니다.
또한 PCRE 패턴 탐지 시 하이퍼스캔(hyperscan) 기반 고속 패턴 매칭 지원으로 보다 빠른 탐지가 가능합니다.

사용자 정의 시그니처 - 패턴 입력 방식



주요 기능 – AhnLab Host IPS (5/6)

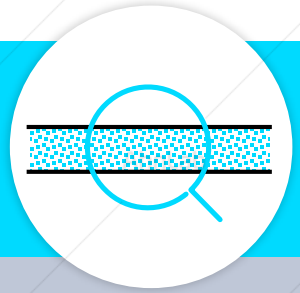
출발지 또는 목적지 IP, Port, Protocol 에 기반한 방화벽 기능을 지원합니다.
또한 특정 지정된 국가로 들어오거나 나가는 트래픽에 대한 선별적인 차단을 지원합니다.

- 지속 업데이트되는 geoIP DB 와 함께 사용자 정의 지원을 통해 보다 신뢰할 수 있는 국가 식별 지원
- HTTP의 경우 XFF(X-forward-for) 인식 지원으로 출발지 IP 에 대한 식별 지원

주요 기능 – AhnLab Host IPS (6/6)

서비스 가용성을 고려한 다양한 네트워크 엔진 모드를 제공합니다.

- Inline 모드와 함께 서비스 가용성을 고려하여 Tap 모드와 Bypass 모드 지원



Inline 모드

정책 기반 탐지 및
차단 모드

호스트로 인/아웃되는
통신 모니터링

방화벽 정책에 따른
IP/Port 통신 차단

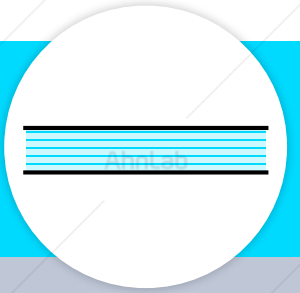
IPS 시그니처 기반 이상 트래픽
탐지 및 차단

Tap 모드

통신 지연 없이
정책 위배/이상 트래픽 탐지 모드

호스트로 인/아웃되는
트래픽을 복사

통신 지연 없이
복사된 트래픽에 대한 방화벽 및
IPS 시그니처 기반 탐지만 수행



Bypass 모드

서비스 장애 등
비정상 환경을 고려한 운영 모드

트래픽에 대한 검사 및 제어를
수행하지 않음

방화벽 정책 및
IPS 시그니처 진단
모두 미동작

주요 기능 – AhnLab V3 Net (1/2)

다수 고객 및 글로벌 인증 기관을 통해 이미 검증된 V3 Net 을 활용해 고도화되는 위협으로부터 서버 워크로드를 안전하게 보호합니다.

정확하고 신속한 서버 방역

- 실시간 검사 기능을 통한 모니터링 가능
- 독보적인 엔진으로 신속하고 정확한 바이러스 진단 및 치료 지원
- 다양한 다중 압축 파일 검사 및 치료 지원

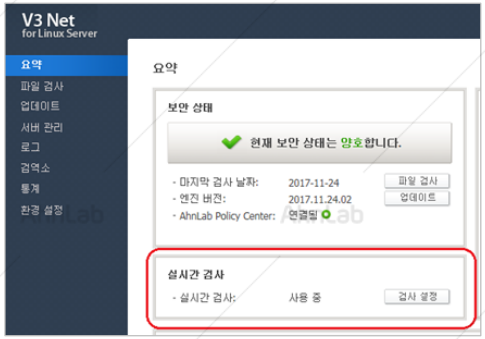
서버 활용성 극대화를 위한 다양한 기능 제공

- 수동 검사와 함께 예약 검사 기능 제공
- 지정된 시간에 수행하는 엔진 예약 업데이트 기능 제공

관리자 편의를 고려한 효율적인 관리 기능

- 검사 예외 설정 기능으로 효율적인 방역 정책 적용
- 바이러스 검사 및 치료에 대한 다양한 리포트 제공

주요 기능 – AhnLab V3 Net (2/2)



다양한 운영 환경에 대한 실시간 검사 지원

- Windows OS 뿐만 아니라 Linux OS 에서도 악성코드에 대한 실시간 검사 지원
- 실시간 검사 시 치료 여부에 대한 설정 지원(치료, 치료 안함 등)

서비스 제공이 중요한 서버 환경을 고려해 다양한 보안 기능 제공

- 예약 검사 시 주요 경로 지정, 자동 치료 여부, CPU 점유율 설정 지원
- 검사 예외 폴더 및 확장자, *예외 악성코드 설정 지원
- 검사 로그, 이벤트 로그, 검역소 크기 제한 설정 지원

※ 실시간 검사는 모든 리눅스 커널을 지원하지는 않으며, 지원하지 않는 환경에서는 단말에서 관련 정보를 표시합니다.

* 검사 예외 설정은 플랫폼별로 제공 방식이 상이합니다.

주요 기능 – AhnLab Application Control (1/3)

사전에 정의된 서비스만 운영되는 클라우드 워크로드에 효과적인 보안을 제공합니다.
신뢰된 프로세스만 실행 허용함과 동시에 중요 폴더/파일에 대한 접근 제어를 통해 보다 강력한 보안 효과를 제공합니다.

화이트리스트 기반 실행 및 접근 제어

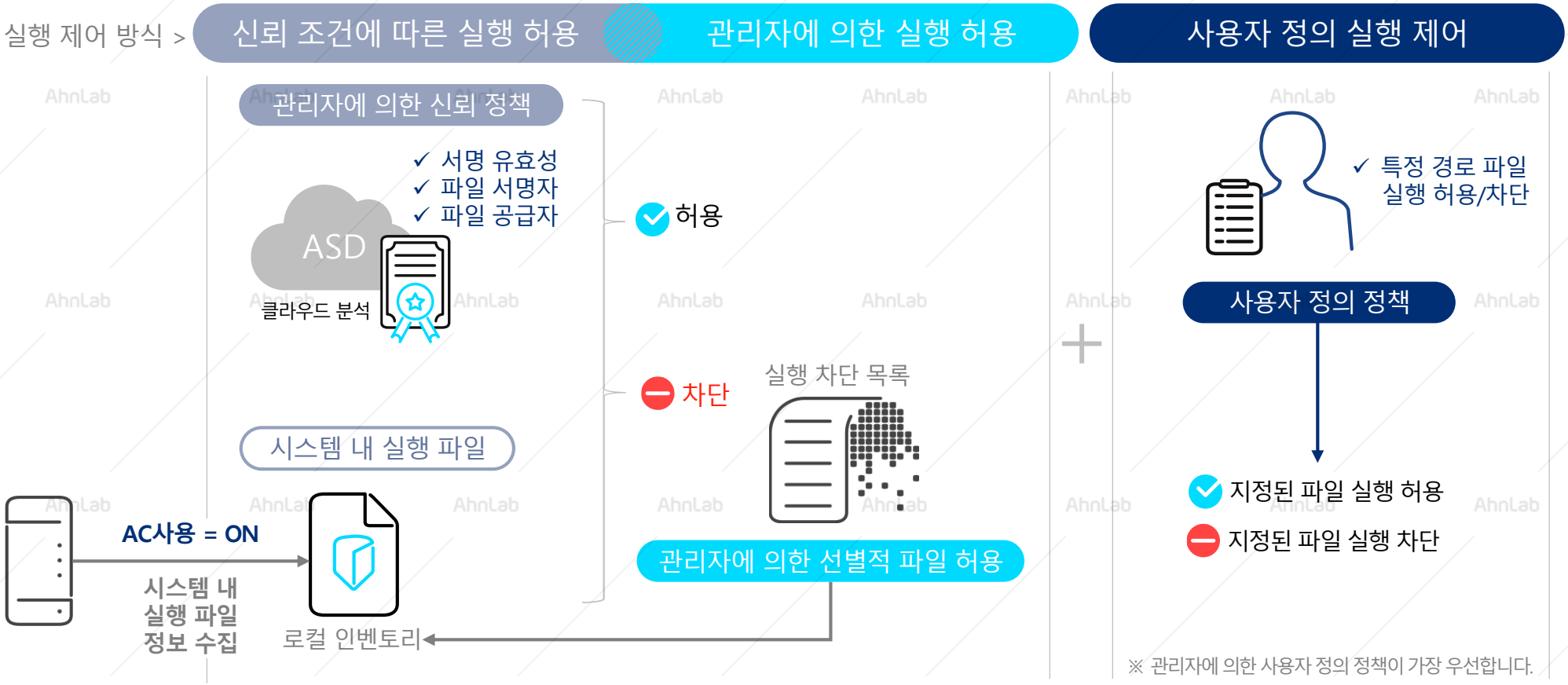
허용된 애플리케이션에
대한 실행만 허용하며
그 외 애플리케이션 실행 차단

중요 폴더 및 파일은
특정 프로세스에 의해서만
접근 허용 지원

주요 기능 – AhnLab Application Control (2/3)

관리 편의성과 서버 가용성을 함께 고려한 실행 제어를 제공합니다.

- 실행 허용 목록에 시스템 파일 자동 등록과 함께 차단된 파일에 대한 관리자 선별적 허용 지원
- 신뢰 파일에 대한 실행 허용과 함께 사용자 정의 정책으로 특정 경로 파일에 대한 예외적인 차단 및 허용 지원



주요 기능 – AhnLab Application Control (3/3)

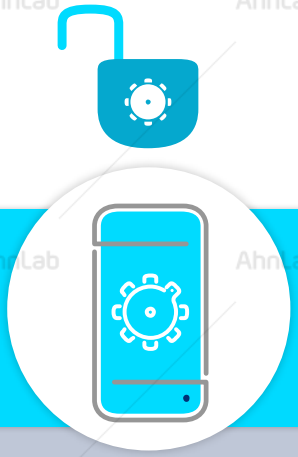
다양한 운영 모드 지원을 통한 안정적인 서비스 운영에 기여합니다.

Maintenance 모드

OS/프로그램 업데이트 등
시스템 중요 변경을 위한 모드

유지보수 모드 동안
변경된 실행파일 정보는
허용 목록에 자동 등록

지정된 기간 후,
Lockdown 모드로 자동 변경



Simulation 모드

정책에 따른 탐지 및
설정한 정책 적절성 판단을 위한 모드

정책에 위배된 이벤트에 대한
차단 없이 탐지만 수행

지정된 기간 후,
Lockdown 모드로 자동 변경

Lockdown 모드

정책에 따른
보안 운영 모드

허용된 또는 신뢰된 프로그램만
실행 허용.
그 외 프로그램은 실행 차단

기본 동작 모드

도입 효과

AhnLab CPP는 하이브리드 클라우드 환경에서의 효율적인 서버 워크로드를 보호함으로써 기업의 비즈니스 연속성을 지원합니다.

안전한 보안 환경 구축

- 온프레미스와 클라우드 서버에 대한 통합 관리 및 일원화된 보안 관리 지원
- 기업 내 서버에서 발생하는 보안 위협에 대한 통합된 가시성 확보
- 다양한 대시 보드 및 제품간 연계 규칙을 통해 보다 빠른 대응 지원
- SIEM, 통합 로그 분석 시스템 연동을 통한 보안 관제 효과 증대

업무 연속성 확보

- 시스템 안정적인 운영 지원으로 업무 연속성 및 생산성에 기여
- 불필요한 통신, 애플리케이션에 대한 차단으로 잠재적인 위협 요소 사전 제거
- 다양한 모드와 함께 예외처리 지원으로 시스템 운영에 최적화된 정책 설정 지원

관리비용 절감

- 온프레미스와 클라우드 서버에 대한 통합 관리 지원으로 효율적인 보안 운영 가능
- 플랫폼 기반에서 보안 솔루션 통합 운영으로 업무 부담 최소화 및 연계 규칙을 통한 도입 효과 극대화
- 서비스 특성에 맞춘 선별적 보안 적용으로 솔루션 도입 비용 절감 효과

운영 환경

Manager

구분		최소 권장 사양
하드웨어	CPU	4 이상
	Memory	16 GB 이상
	HDD	200 GB 이상
운영체제		CentOS 7.3 ~ 7.7(x86_64)
콘솔(브라우저)		Internet Explorer 11 이상, Chrome 최신 버전

Agent

구분		최소 권장 사양
운영체제	Windows Server	• Windows Server 2012(R2 포함) • Windows Server 2016 • Windows Server 2019 • Windows Server v1809, 1903, 1909
	Linux Server	• CentOS 7 • RHEL 7 • Ubuntu 16.04(x64) • Amazon Linux 2

※Anti-malware는 AhnLab V3 Net for Windows Server, Linux Server 소개 페이지를 참고바랍니다.

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 CPP

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

AhnLab