AhnLab EPP

차세대 엔드포인트 통합 보안 플랫폼

More security,
More freedom

표준제안서

AhnLab

01
제안 배경

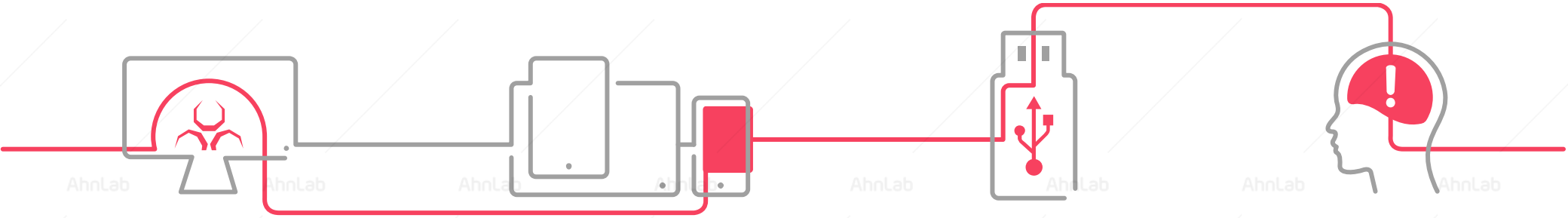
엔드포인트 보안 위협의 다변화·고도화

엔드포인트 보안 관리 범위의 확대

효율적인 위협 관리 및 대응 방안 요구

엔드포인트 보안 위협의 다변화·고도화

엔드포인트는 기업 및 기관의 비즈니스 운영이 이루어지는 영역으로, 중요한 업무용 데이터가 집중되어 있지만 여러 가지 원인에 의해 다양한 보안 위협에 지속적으로 노출되어 있습니다.



신·변종 악성코드 급증

- 랜섬웨어 증가
- 서버 및 모바일 타깃 악성코드 증가

Device 및 OS, SW 다변화

- 다양한 OS 및 SW 이용
- OS 및 애플리케이션 신규 취약점 (제로데이)

직·간접 경로를 통한 위협 유입

- 이메일, 웹 서핑, USB 등

사용자 부주의

- 보안 패치 미적용
- 보안 정책 위반

수십~수백 개의 PC 및 서버 시스템으로 구성되는 엔드포인트

중요 정보 저장 및 이용
- 보고서, 계약서, 매출분석자료 등

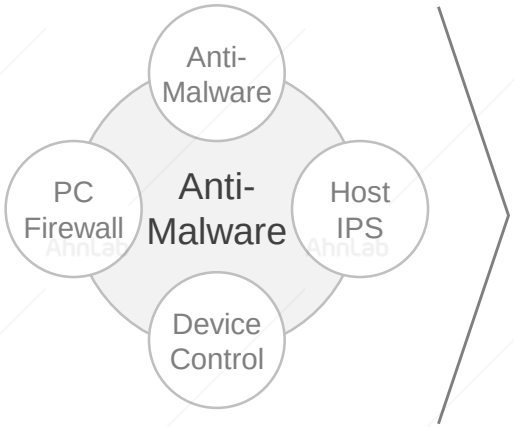
DB, 서버 및 다른 PC에 항시 연결
- 내부 위협 확산 가능성

개인정보 저장 및 이용
- 주민등록번호, 전화번호, 신용카드 번호 등

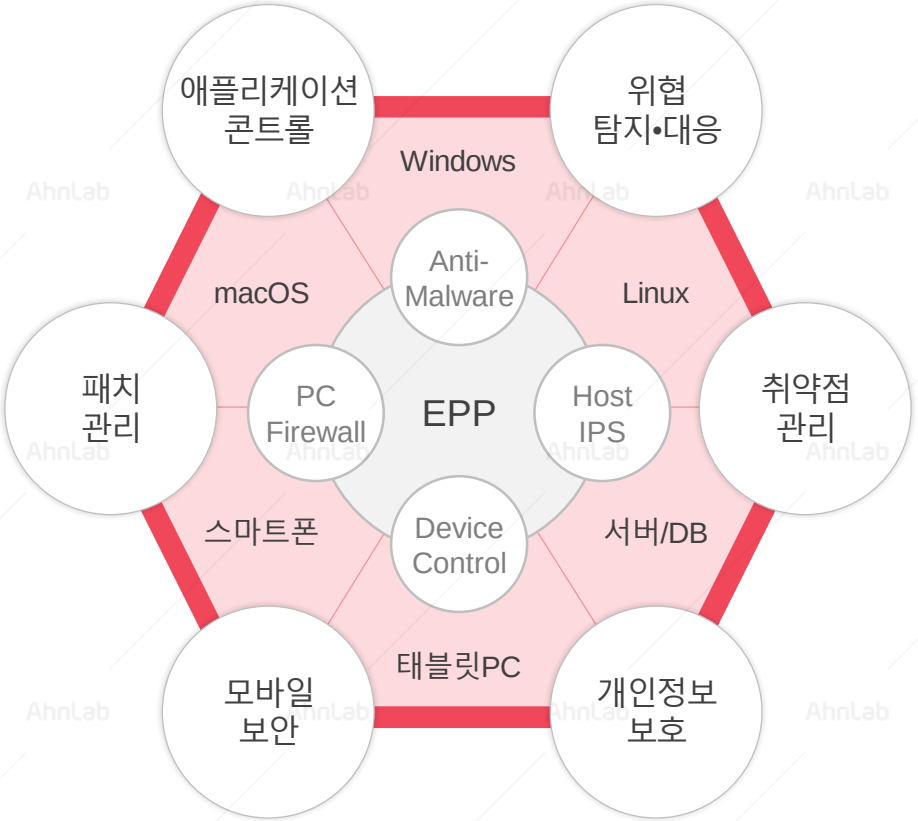
AhnLab © AhnLab, Inc. All rights reserved.

엔드포인트 보안 관리 범위의 확대

엔드포인트 환경 변화와 함께 나날이 증가하는 보안 위협에 대응하기 위해 다수의 보안 솔루션을 도입하면서 기업 및 기관의 보안 운영 및 관리 부담 또한 지속적으로 가중되고 있습니다.



백신(Anti-Malware) 등
개별 보안 제품 중심의
엔드포인트 보안



OS 및 디바이스 다변화에 따른 엔드포인트 보안 영역의 확대

개별 솔루션에 대한
운영 및 모니터링 부담 증가

다수의 솔루션 설치에 의한
인프라 장애

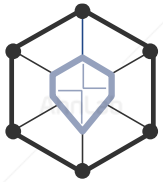
솔루션 안정성 이슈에 따른
보안 운용 중단

AhnLab © AhnLab, Inc. All rights reserved.

효율적인 위협 관리 및 대응 방안 요구

엔드포인트 환경 변화로 인해 보안 관리의 대상 및 범위가 확장됨에 따라
플랫폼 기반의 유기적이며 통합적인 엔드포인트 보안 위협 관리 및 대응에 대한 요구가 늘어나고 있습니다.

플랫폼 기반의 통합적이며 체계적인 위협 관리·대응 필요



다양한 보안 솔루션의 수많은 정보를
신속하게 탐지 및 대응

정확한 정보 전달을 통해
보안 관리자의 반응·대응 시간 최소화

보안 솔루션 및 기능의 유기적 융합을 통한
엔드포인트 위협 가시성 확보

- ✓ 악성코드 **제어 및 대응의 한계**
- ✓ 다양한 위협 경로 **모니터링의 한계**
- ✓ 위협 고도화에 따른 **분석·대응 속도 지연**

다양한 위협 경로
의심/악성 파일 사전 유입 관리 한계

사회공학기법, 표적/지능형 공격
악성코드 감염 및 정보 유출

OS/SW 제로데이 취약점
신·변종 악성코드 증가

AhnLab © AhnLab, Inc. All rights reserved.

02
AhnLab EPP

AhnLab

AhnLab EPP

AhnLab EPP는 다양한 보안 기능의 유기적인 연동 및 통합 운영을 위한 차세대 엔드포인트 보안 플랫폼(Endpoint Protection Platform)으로, 단순 보안 관리를 넘어 통합 플랫폼 기반의 체계적이며 효율적인 엔드포인트 위협 관리 및 대응을 제공합니다.

AhnLab EPP

위협 관리 및 대응 중심의 **차세대 엔드포인트 보안 플랫폼**

최적화된
위협 관리·대응 플랫폼

- 안랩 솔루션의 설치 및 운영에 최적화
- Syslog를 통한 제3자 솔루션(SIEM, 통합로그분석/백업 시스템 등)과의 쉽고 간편한 연동
- 위협 모니터링 및 가시성 제공 - 즉각적인 대응 정책 수립 가능

효율적인
엔드포인트 통합 관리

- 다양한 안랩 엔드포인트 보안 솔루션의 통합 운영 및 관리
- 1개의 에이전트(One Agent), 통합 관리 콘솔(Single Management Console)을 통한 일원화된 보안 운영 및 관리
- 웹(web) 기반의 관리자 콘솔 및 다양한 관리 기능을 통한 운영 편의성

차별적인
비용(TCO) 절감 효과

- 라이선스 비용이 발생하지 않는 리눅스(Linux) OS 지원
- 소프트웨어 솔루션 - 고객사 환경에 따른 유연한 서버 구성 및 확장 가능
- 보안 솔루션 도입 및 관리 비용 효율성 - AhnLab EPP에 라이선스 적용만으로 손쉽게 구축 및 운영 가능

© AhnLab, Inc. All rights reserved.

특장점 – 단일 에이전트 및 매니지먼트

AhnLab EPP의 단일 에이전트(One Agent), 단일 관리 콘솔(Single Management Console)을 기반으로
백신부터 패치, 개인정보, 보안 취약 시스템 점검 및 조치를 쉽고 간편하게 통합 관리 및 운영할 수 있습니다.

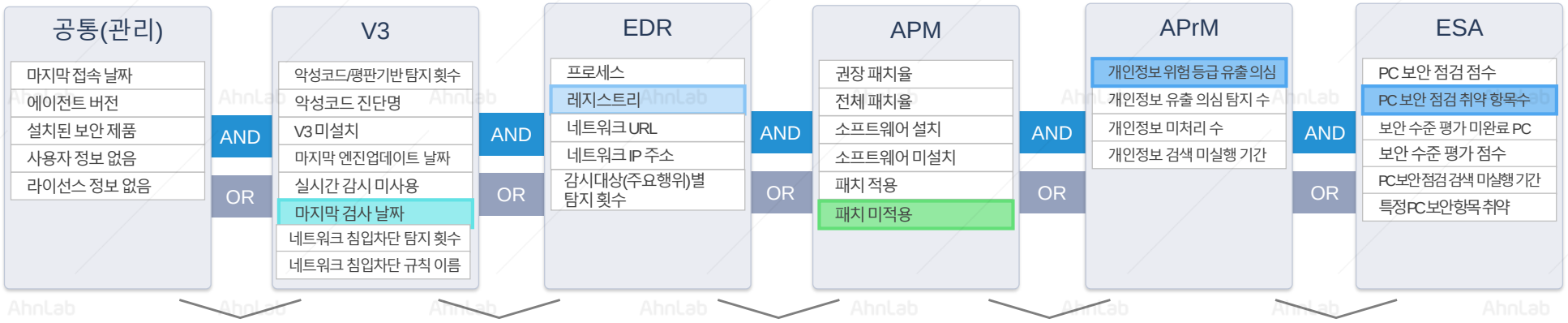
© AhnLab, Inc. All rights reserved.

특장점 – 제품간 연계 정책 설정을 통한 능동적 대응

안랩 엔드포인트 보안 제품간 연계 정책 설정을 통해 조직의 환경에 최적화된 엔드포인트 보안 운영이 가능합니다.

- 엔드포인트 시스템의 취약 상태 여부, 의심 행위 등에 대한 개별 및 연계 정책 설정 가능
- 보안 정책 위반 시스템에 대한 보안 관리자의 주도적•능동적 조치 가능 - 알람, 네트워크 격리, 악성코드 치료, 패치 적용 등

보안 제품 연계 규칙 생성



One Agent

연계 규칙 위반 탐지 시 제품간 대응 규칙 적용

연계 규칙 위반 시스템에 대한 순차적 대응 정책 적용

© AhnLab, Inc. All rights reserved.

특장점 – 모듈 기반의 유연한 확장성 및 운영 안정성(1/3)

AhnLab EPP는 시스템 운영의 안정성과 유연한 확장, 관리 편의성을 제공하기 위해 모듈 방식으로 구성되어 있습니다.

- 모듈별 구성: 로드밸런서(Load Balancer), 파일, 로그, DB, EDR

AhnLab © AhnLab, Inc. All rights reserved.

특장점 – 모듈 기반의 유연한 확장성 및 운영 안정성(2/3)

모듈 기반의 AhnLab EPP는 고객사 환경에 따라 유연하게 구성할 수 있으며, 손쉬운 서버 추가 방식(Scale-out)을 지원해 트래픽 증가 등에 따른 서버 성능 저하를 방지합니다.

- 최소화된 초기 구축 비용 및 확장 편의성: 사용자 수, 데이터베이스 사용량 등 고객 환경에 따른 시스템 구성
- 에이전트 확대, DB 증가에 따라 모듈별 서버 확장 가능 – 단, EDR 통계 서버는 1개 고정, 분석 서버는 확장 가능

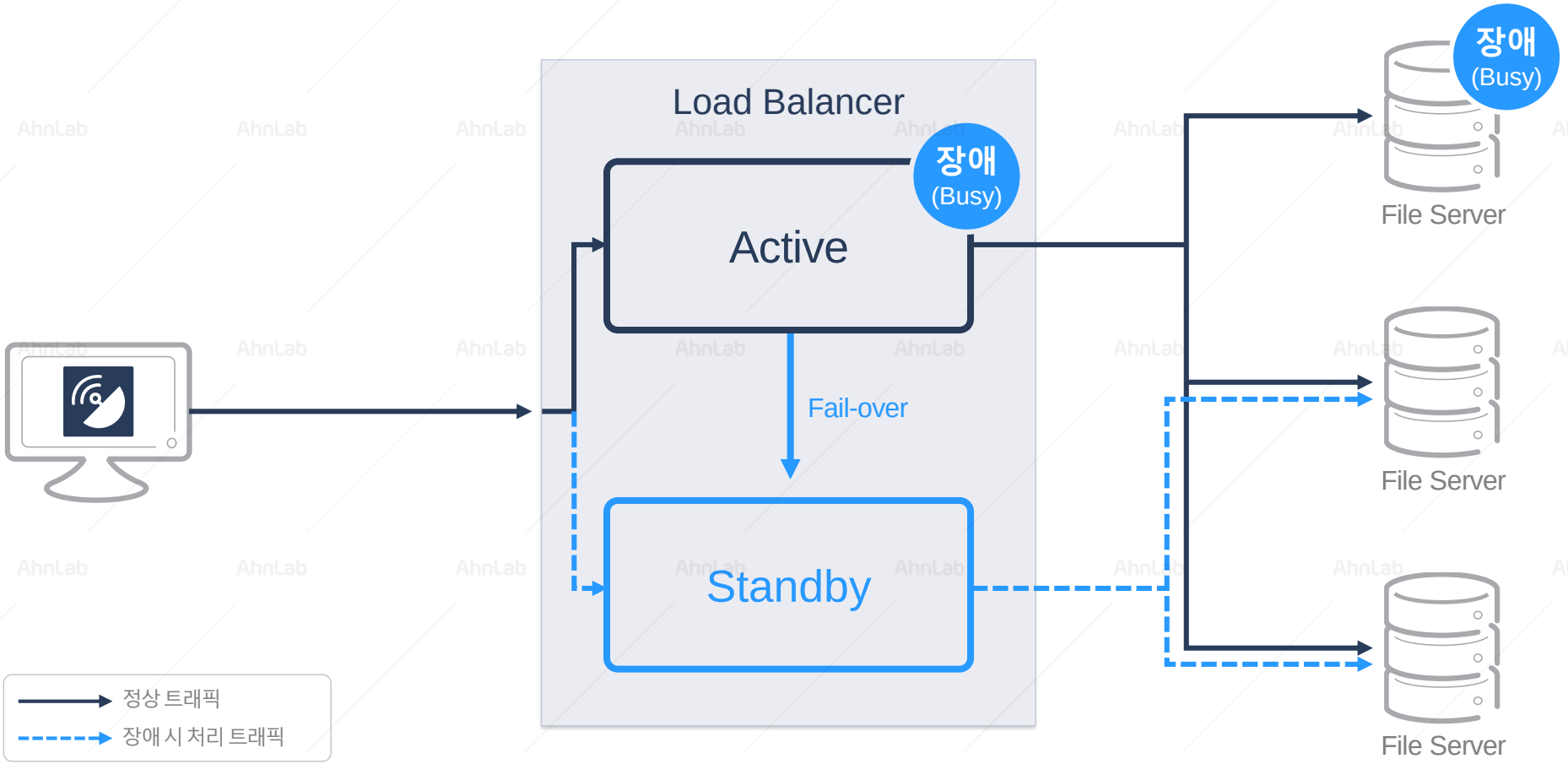
※ EDR 운영을 위한 의심 행위 분석 서버는 물리적으로 분리하여 구성해야 하며, 필요 시 추가 증설이 가능하도록 구성되어 있습니다.

© AhnLab, Inc. All rights reserved.

특장점 – 모듈 기반의 유연한 확장성 및 운영 안정성(3/3)

AhnLab EPP는 모듈간 성능 과부하 방지 및 분산을 위해 로드밸런서(Load Balancer) 기능을 제공합니다.
액티브-스탠바이(Active-Standby) 방식을 통해 로드밸런서 액티브 서버 장애 시에도 스탠바이 서버가 엔드포인트 트래픽을 처리합니다.

- 각 모듈 서버에 대한 주기적인 모니터링을 통해 병목 현상 방지
- 장애 발생 시 트래픽 분산 처리를 통해 정상 서버를 통한 안정적인 시스템 운영



AhnLab © AhnLab, Inc. All rights reserved.

특장점 – 동적 UX 기반의 사용자 편의성

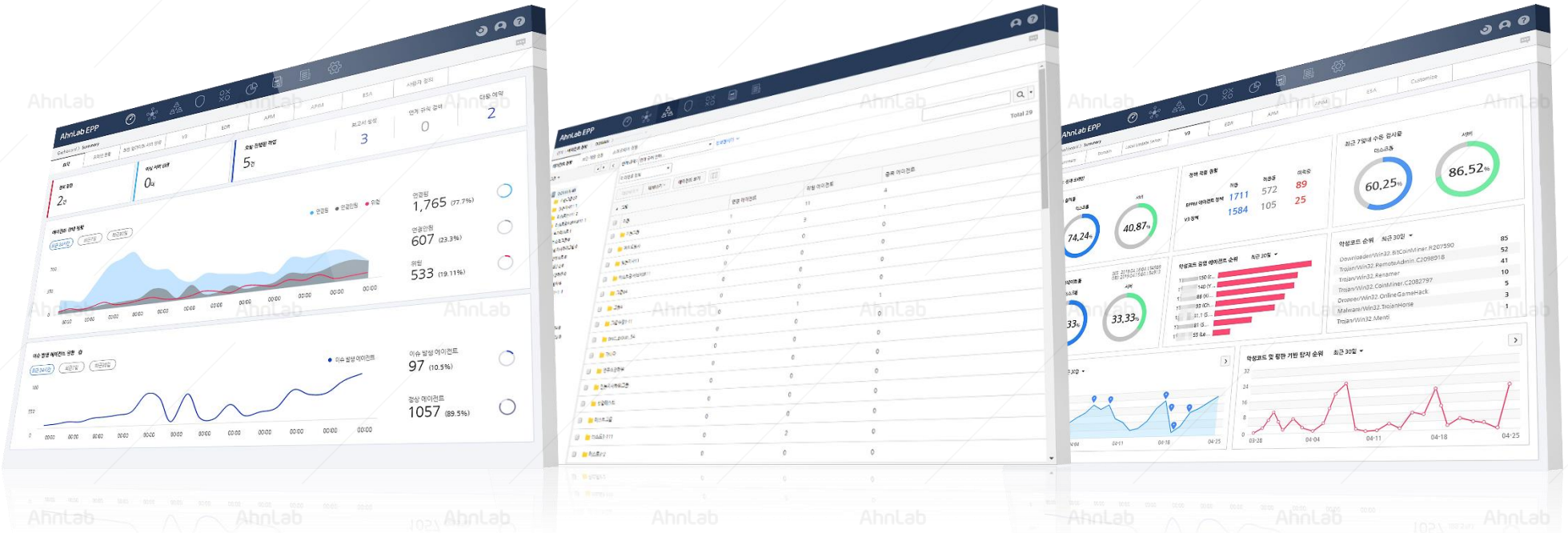
AhnLab EPP는 보안 관리자의 편의성을 강화하기 위해 웹 기반의 관리 콘솔과 최적화된 다양한 관리 메뉴를 제공합니다.
또한 동적 UX 기반의 직관적인 대시보드를 통해 한눈에 파악할 수 있는 엔드포인트 가시성을 제공해 효율적인 위협 관리 및 대응이 가능합니다.

직관적이고 편리한 모니터링 환경을 통한
관리 효율성 향상 및 보안 강화

간편한 정책 적용

**사용자 정의 및
제품별 대시보드**

차별적인 동적 UX

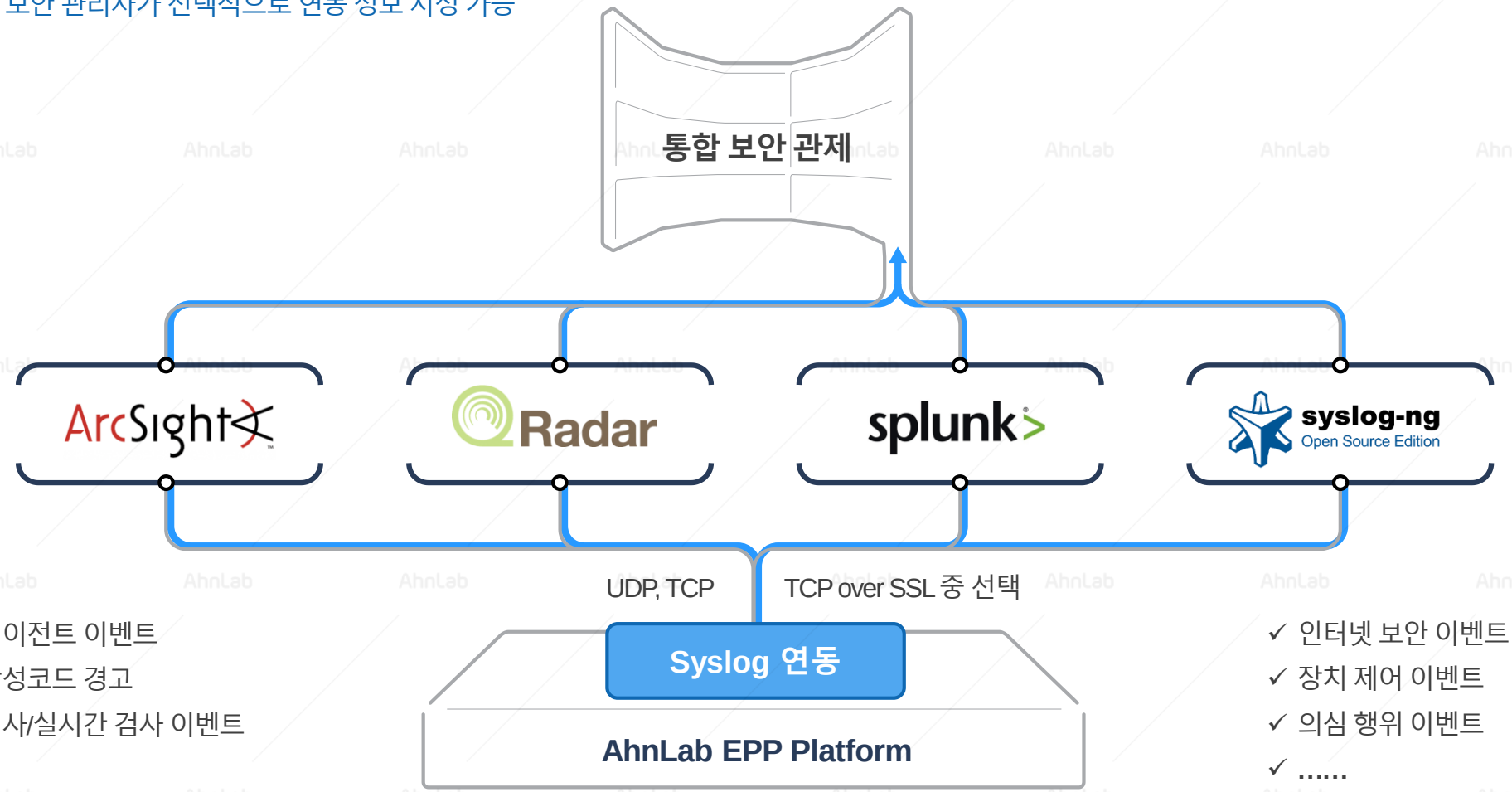


© AhnLab, Inc. All rights reserved.

특장점 – Syslog를 통한 외부 솔루션 연동

AhnLab EPP의 자동화된 Syslog 연동 기능을 통해 다양한 타사 솔루션(SIEM, ESM, 통합 로그)과 원활하게 연동 가능합니다.
다양한 솔루션 연동을 통해 풍부한 위협 인텔리전스를 확보하고 보안 관제 효과를 극대화할 수 있습니다.

- Syslog UDP 및 TCP, TCP over SSL 동시 지원
- 보안 관리자가 선택적으로 연동 정보 지정 가능



✓ 에이전트 이벤트
✓ 악성코드 경고
✓ 검사/실시간 검사 이벤트

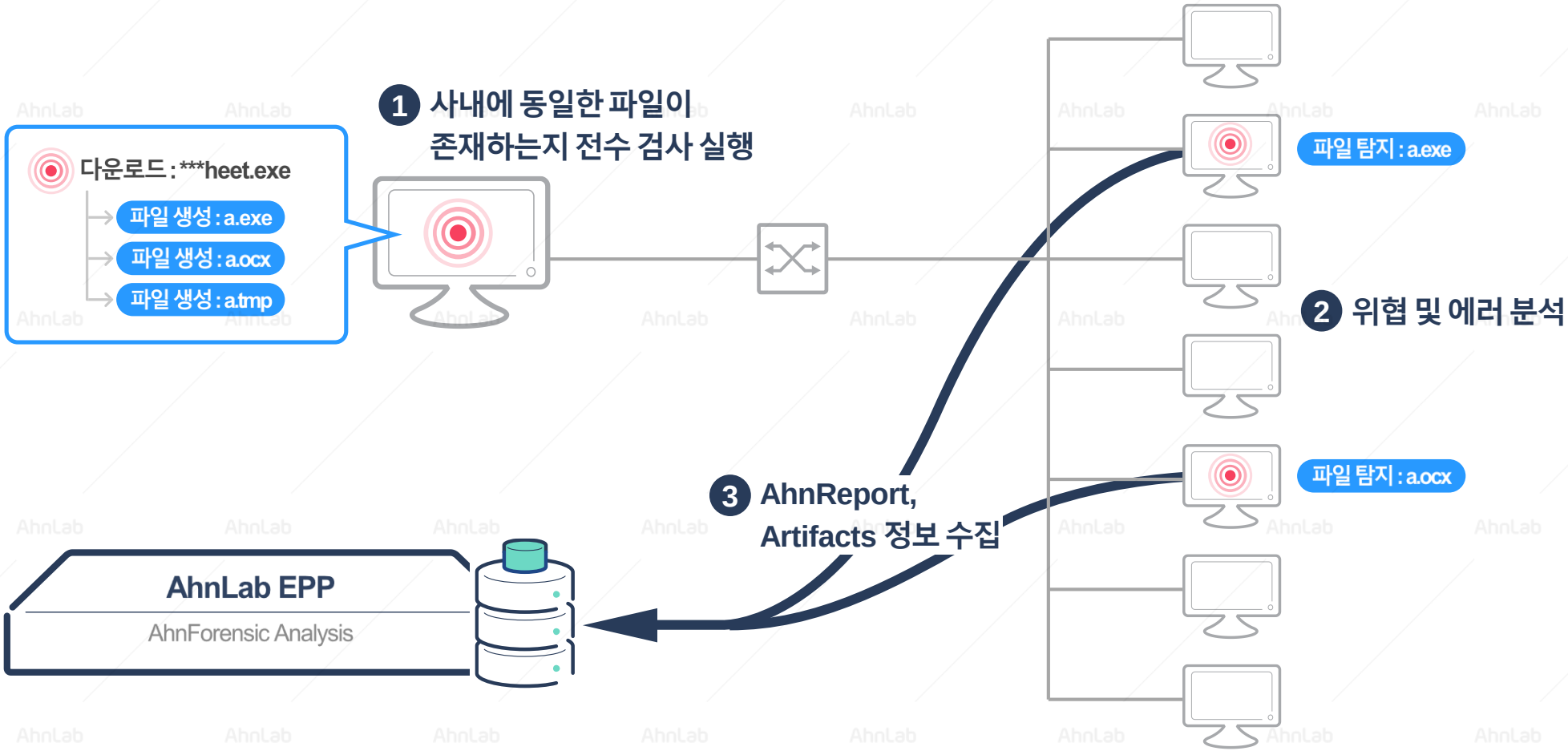
✓ 인터넷 보안 이벤트
✓ 장치 제어 이벤트
✓ 의심 행위 이벤트
✓ .....

AhnLab © AhnLab, Inc. All rights reserved.

특장점 – 엔드포인트 위협 정보 자동 수집

엔드포인트의 의심 단말 분석 및 에이전트를 통한 위협 정보 자동 수집 기능을 이용해 악성코드 위협에 더욱 효과적으로 대응할 수 있습니다.

- 자동 AhnReport 수집 및 뷰어 제공
- AhnLab EDR을 통한 파일 전수검사 및 아티팩트(Artifacts) 정보 수집 가능
- 수집된 위협 정보는 안랩 프로페셔널 서비스 연계를 통해 추가 분석 가능 – 상세 분석 보고서, 대응 가이드 제공 가능



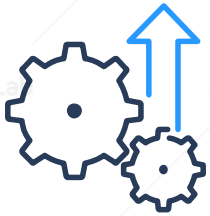
AhnLab © AhnLab, Inc. All rights reserved.

도입 효과

AhnLab EPP를 통한 쉬운 보안, 고객 주도의 능동적 보안 실현

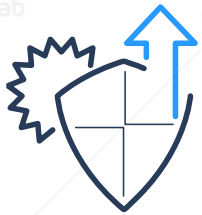
관리비용 절감

- 비용 부담이 없는 Linux OS, DB 지원을 통해 관리 비용 절감 효과
- 통합 관리를 통한 운영 인력 비용 절감 및 관리 효율성 극대화
- 편리한 통합 운영을 통한 개별 솔루션 도입 효과 극대화
- 유연한 구성 방식을 통해 서버 확장에 따른 관리 부담 최소화



업무 생산성 향상

- 중앙 제어(통합 콘솔)를 통한 신속한 사고 대응 및 업무 부담 최소화
- 중앙 관리에 필요한 시스템 설치•운영 • 관리 부담 해소
- 안전한 보안 환경 구축으로 업무 연속성•생산성 향상



보안 사고 대응력 향상

- 엔드포인트 위협 가시성 확보 및 통합 관리를 통한 효율적인 보안 운영 가능
- SIEM/통합 로그 분석 시스템 연동을 통한 보안 관제 효과 증대
- EDR 연동을 통한 엔드포인트 위협 수집 및 분석 강화로 보안 사고 대응력 향상

© AhnLab, Inc. All rights reserved.

운영 환경(권장 하드웨어 사양)

- AhnLab EPP Agent 설치 환경

구분	상세 버전
운영체제	Windows XP SP3 / Vista / 7 / 8(8.1) / 10 / 10 IoT Enterprise Windows Server 2003 SP1 이상 (R2 포함) Windows Server 2008 / 2012 – 공통 사항: R2 포함 Windows Server 2016 / 2019 *상기 OS의 64bit 호환 모드 지원 macOS Sierra(10.12), macOS High Sierra(10.13)
지원 언어	한국어, 영어, 중국어(간체), 일본어

- AhnLab EPP Management 운영 환경

구분	상세 버전
웹 브라우저	Internet Explorer 11 이상 Chrome 최신 버전
지원 언어	한국어, 영어, 중국어(간체), 일본어

- AhnLab EPP 권장 하드웨어 사양

구분		관리 에이전트 수						
		최대 300개	최대 1,000개	최대 5,000개	최대 10,000개	최대 15,000개	최대 30,000개	최대 50,000개
CPU		4	4	8	16	16	16	16
메모리		32G	64G	64G	128G	192G	256G	384G
HDD	기본	500G	500G	1TB	1TB	1TB	1TB	2TB
	APM 사용 시	1TB	1TB	1TB	1TB	1TB	1TB	1TB

* APM 사용 시: HDD 2개 이상 물리적 분리 구성 필수, 에이전트와 서버간 네트워크 대역폭 최소 32mbps 이상 권장

- AhnLab EDR 서버 사양

구분		관리 에이전트 수						
		최대 300개	최대 1,000개	최대 5,000개	최대 10,000개	최대 15,000개	최대 30,000개	최대 50,000개
CPU		4	4	8	16	16	16	16
메모리		32G	64G	64G	128G	256G	384G	512G
HDD	기본	2TB	2TB	4TB	4TB	8TB	8TB	16TB

* 의심 행위 분석(EDR) 로그 데이터 저장을 위한 Raid 구성은 검색 속도 등을 고려하여 Raid 1+0 권장

AhnLab © AhnLab, Inc. All rights reserved.

※ 별첨

‘2019 올해의 엔드포인트 보안 기업’ 선정

'2019 올해의 엔드포인트 보안 기업' 선정

※별첨

안랩은 엔드포인트 보안 분야에서의 기술력, 시장 점유율 등을 인정받아 글로벌 리서치 기관인 프로스트 앤 설리번(Frost & Sullivan)이 주최한 2019 Frost & Sullivan Korea Best Practices Award에서 '올해의 엔드포인트 보안 기업'으로 선정되었습니다.

2019 프로스트 앤 설리번 베스트 프랙티스 어워드

2019 Frost & Sullivan Best Practices Award
South Korea Endpoint Security Vendor of the Year

2019년 11월 14일

"안랩은 멀티OS, 멀티 클라우드 등 기업 환경 변화와 요구에
최적화된 엔드포인트 보안 솔루션을 제공하고 있다.
복잡한 엔드포인트 환경을 안랩의 단일 에이전트와 단일 관리 콘솔을
통해 대한 효과적으로 보호할 수 있다."

Kenny Yeo
Associate Director and Head of Asia-Pacific Cyber Security
Frost & Sullivan

© AhnLab, Inc. All rights reserved.

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, Inc. All rights reserved.

AhnLab EPP

AhnLab