AhnLab ESA

More security,
More freedom

취약 시스템 확인부터 자동조치까지!

표준제안서

AhnLab

CONTENTS

AhnLab

01
제안 배경

엔드포인트 보안 위협의 다양화 • 고도화

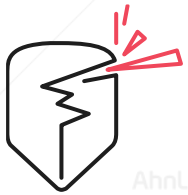
관련 규제 강화 및 보안 관리 부담의 증가

엔드포인트 보안 관리의 과제

엔드포인트 보안 위협의 다양화·고도화

기업의 엔드포인트에 위치한 업무용 PC에는 악의적인 공격자가 금전적, 정치적, 또는 그 외 목적으로 이용할 수 있는 민감한 정보들이 위치하고 있을 뿐만 아니라 다양한 취약점이 존재합니다.

기업 엔드포인트의 위협 요인

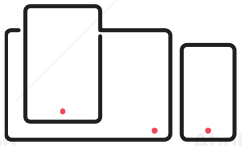


애플리케이션 취약점

OS/애플리케이션 업데이트 미적용

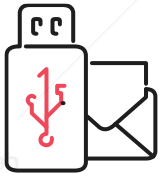
악성코드 감염

신/변종 악성코드 증가



관리 포인트 증가

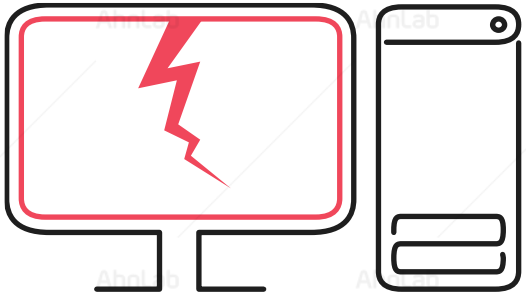
망분리 등



다양한 위협 유입 경로

이메일, 웹 서핑, USB 등

업무용 PC



중요 DB/서버, 다른 업무용 PC 등에 항시 네트워크로 연결됨

중요 정보 저장 및 이용

- 보고서, 계약서, 매출분석자료 등

개인정보저장 및 이용

- 주민등록번호, 전화번호, 신용카드 번호 등

정보 유출 | **시스템 파괴** | **비즈니스 중단** | **대외 이미지 하락**

관련 규제 강화 및 보안 관리 부담의 증가

공공기관에 이어 금융기관 및 일반 기업의 보안 점검에 대한 정보보안 관련 규제가 강화됨에 따라 이제 엔드포인트 보안 점검은 기관 및 기업의 리스크 관리 영역으로 인식되고 있습니다.

공공기관 및 교육기관

'사이버•보안 진단의 날'

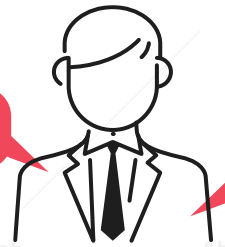
- 매월 세 번째 수요일
- PC취약점, 개인정보 점검 등
- 주기적인 보안 감사
- 망 분리 등 관리 포인트 증가
- 보안 교육 부담

금융기관 및 일반 기업

'정보보안 점검의 날'

- 전자금융감독 규정(제37조의 5)
- 매월 정보보안 점검
- 최신 보안패치 적용 강화
- 임직원 보안의식 제고
- 시스템 외 보안사항 점검
- 보안 감사

복잡하고 광범위한
보안 점검 항목



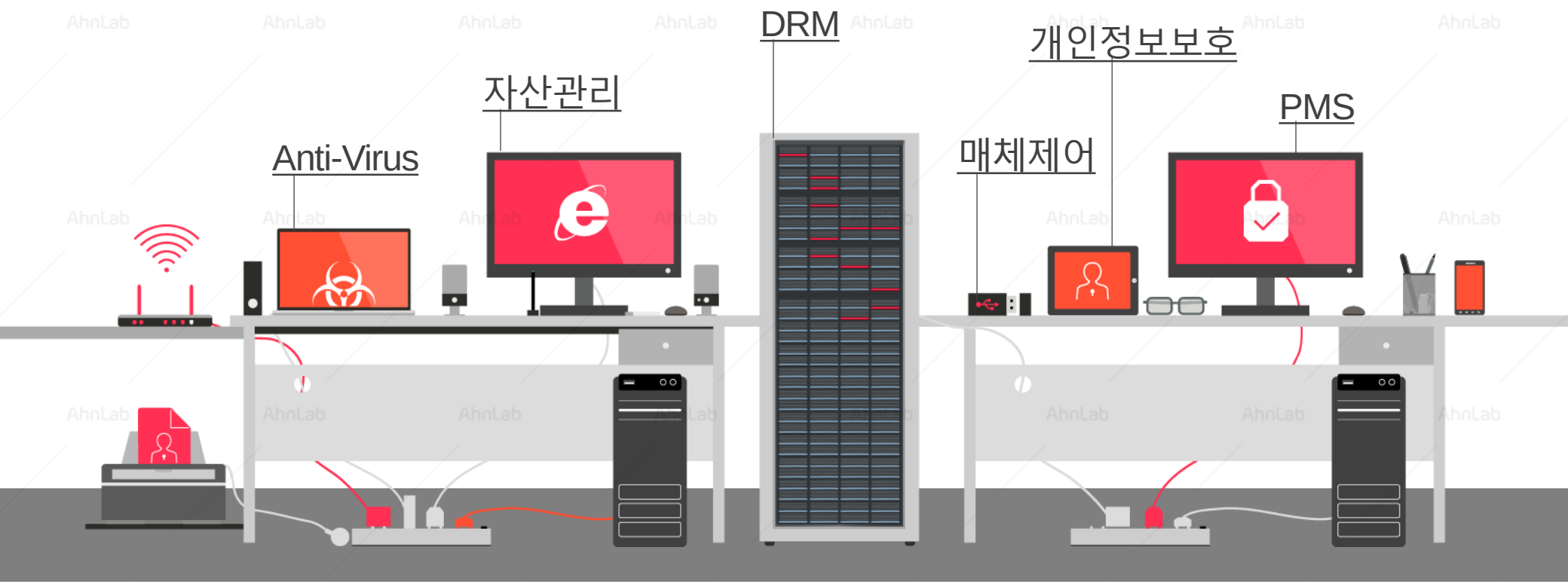
보안 관리자 업무 부담 및 책임 가중

기관 및 기업 임원진의 책임 강화

엔드포인트 보안 관리의 과제

급변하는 IT 환경 변화 및 관련 규제 강화에 의해 보안 관리 범위 및 대상이 늘어남에 따라 다수의 개별 보안 솔루션 도입에 따른 관리와 업무 부담이 증가하고 있습니다.

- 단일 솔루션들의 상호보완 효과를 위한 일원화된 관리 필요성 대두
- 다양한 엔드포인트 위협 요인에 대한 전반적인 점검 및 관리 방안에 대한 요구
- 본연 업무 수행으로 인한 보안 조치 소홀 및 부담 가중



02
AhnLab ESA

제품 개요

특장점

AhnLab

AhnLab ESA

AhnLab ESA(Endpoint Security Assessment)는 업무용 PC의 보안 상태를 점검하고 자동조치를 통해 엔드포인트의 전반적인 보안 수준을 강화(hardening)하는 취약 시스템 점검 및 조치 솔루션입니다. 업무용 PC의 보안 상태 점검 및 자동 조치를 통해 관리자와 사용자의 업무 부담은 최소화하고 기업의 엔드포인트 보안 수준을 극대화합니다.

- 쉽고 간편한 기능 및 다양한 정책으로 관리자와 사용자의 보안 부담 해소 및 업무 생산성 향상
- 플랫폼 기반의 백신, 패치, 개인정보 통합 관리를 통한 엔드포인트 하드닝(Endpoint Hardening) 효과

AhnLab ESA

원클릭으로
쉽고 간편하게

효율적인 엔드포인트
취약점 관리

관리자와 PC사용자의
업무 효율성 극대화

PC 보안 점검으로 인한 업무 부담 및 리소스 소모 최소화

- 기술적인 지식이 없는 일반 사용자도 손쉽게 PC 보안 상태 확인 및 조치 가능

중앙에서 개별 PC의 보안 상태를 한 눈에 파악

- 사내 모든 PC에 최신 패치 자동 적용
- 통합 매니지먼트로 간편하게 관리 및 보고서 작성 가능

다양한 취약점에 대한 사전 대응 조치 가능

- 타사 대비 최다 점검 항목 지원
- 더욱 안전한 PC 환경 구현

정보보안 관련 규제 대응 및 준수

- 공공기관 '사이버•보안 진단의 날' 의무 규정 준수
- 금융기관 '정보보안 점검의 날' 대응

특장점 – 플랫폼 기반의 엔드포인트 하드닝

AhnLab ESA는 엔드포인트 보안 플랫폼 AhnLab EPP 기반의 연계 정책을 통해 취약 시스템 점검 및 조치부터 악성코드 대응, OS 및 보안 패치 관리, 개인정보 유출 방지 등 기업의 엔드포인트 하드닝(Endpoint Hardening)에 기여합니다.

- AhnLab EPP 기반의 보안 솔루션 연계를 통한 취약 시스템 조치 및 엔드포인트 하드닝 효과

특장점 – 차별화된 점검 항목

AhnLab ESA는 보안 수준 강화를 위한 75개 점검 항목을 제공하고 있으며, 지속적으로 점검 항목을 확대 및 강화하고 있습니다.

점검 항목 75 (점검 항목 63 + 사용자 정의 점검 12)

기본 점검 항목 15

보안 업데이트 **4개**	• 바이러스 백신 설치 및 실행 여부 점검 • 바이러스 백신의 최신 보안 패치 여부 점검 • 운영체제, MS Office의 최신 보안 패치 설치 여부 점검 • 한글프로그램의 최신 보안 패치 설치 여부 점검
패스워드안전성 **2개**	• 로그인 패스워드 안전성 여부 점검 • 로그인 패스워드의 분기 1회 이상 변경 여부 점검
화면보호기, 공유폴더 설정 **2개**	• 화면보호기 설정 여부 점검 • 사용자 공유 폴더 설정 여부 점검
보안 프로그램 설치 **2개**	• USB 자동 실행 허용 여부 점검 • 미사용(3개월) ActiveX 프로그램 존재 여부 점검
관리자 추가 점검 **5개**	• PDF 프로그램의 최신 보안 패치 설치 여부 • 편집 프로그램(MS워드, 한글, PDF) 설치 여부 점검 • 무선랜카드 점검 기능 • 보안USB 설치 여부 점검 기능 • 비인가 프로그램 설치 여부 점검

+

확장 점검 항목 60

계정 설정 점검 **8개**	• 윈도우 자동 로그온 • 장기 미접속 계정 존재 여부 점검 • Guest 계정, Administrator 계정 사용 점검
로컬 보안 정책 점검 **3개**	• 패스워드 최대/최소 사용기간 설정 여부 점검 • Windows 로그온 실패 횟수 초과시 계정 잠금 설정 여부 점검
윈도우 설정 점검 **4개**	• Windows 자동 업데이트 설정 여부 점검 • 사용자 계정 컨트롤(UAC) 사용여부 점검 • 모든 미디어 및 장치 자동실행 설정 점검
네트워크 설정 점검 **12개**	• 원격 데스크톱 포트 변경 • 인터넷 연결 공유 여부 점검 • Hosts 파일 내 비 허용 IP 점검, 비허용 DNS 설정 점검 • 방화벽 사용/ 웹서비스 실행/FTP 서비스 실행 점검
웹 브라우저 설정 점검 **9개**	• IE 자동 암호 입력 여부, 자동 로그인 설정 여부 • IE ActiveX 컨트롤 및 플러그인 실행 점검 • IE 신뢰할 수 있는 사이트 목록의 취약성 점검
기타 점검 항목 **12개**	• 전체 공유권한의 공유 폴더 사용 점검 • 모든 미디어 및 장치 자동실행 설정 점검 • 장치 드라이버 설치 시 서명 점검 • Adobe Flash Player, Adobe Air, JAVA(jre) 최신 보안 패치 여부 점검
사용자 정의 취약점 점검 **12개**	• 검사 항목 관리자 추가 기능

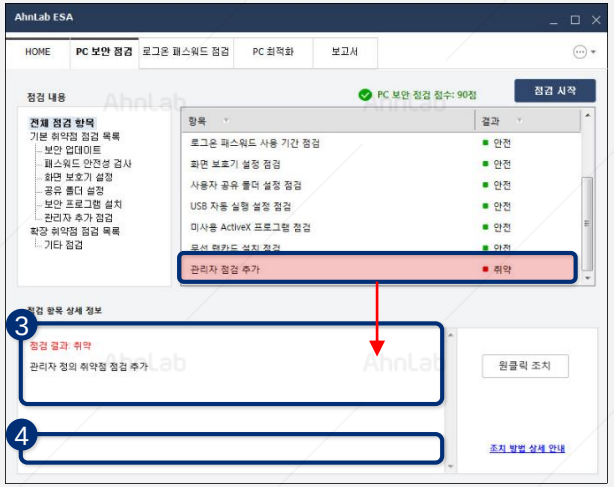
특장점 – 고객사별 커스터마이징

AhnLab ESA는 고객사의 필요에 따라 점검 내역에 표기되는 내용을 편집할 수 있어 더욱 효율적으로 운영 및 관리할 수 있습니다.

[HOME 화면]

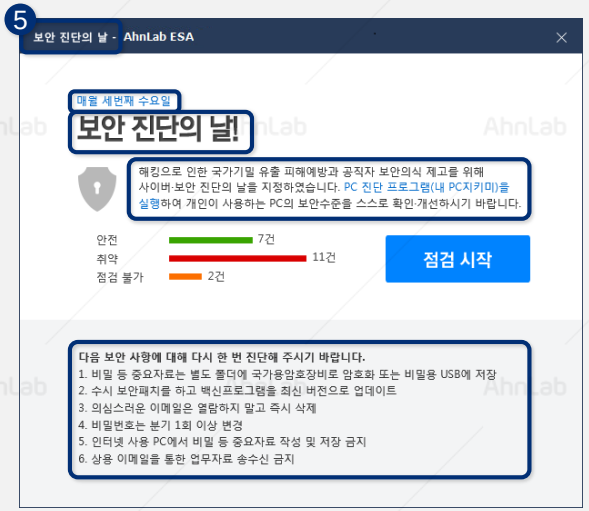
1. 관리자용 안내 문구 삽입 가능
2. 고객사 CI/로고 삽입 가능

[PC보안 점검 화면]



3. 점검 항목별 상세정보 문구 편집 가능
4. 점검 항목 상세정보 영역 내 관리자용 고정 안내 문구 삽입 가능

[보안 진단의 날 팝업]



5. 보안진단의 날 팝업 편집 가능
   - 타이틀, 세부내용 등

특장점 – 탁월한 사용자 편의성

AhnLab ESA는 전문 지식이 없는 일반 사용자도 손쉽게 이해 및 이용할 수 있는 **편리한 사용성**과 **직관적인 UI**를 제공합니다.

편리한 사용성, 직관적인 UI

점검 결과의 '**점수화**',
보안 상태를 **직관적인 색상으로 표현**

별도의 사용자 조작 없이
백그라운드에서의 **자동 조치 가능**

취약 항목에 대한 **One-Click 버튼** 및
조치 방법 안내 지원

AhnLab EPP기반의 **전용 대시보드**
모니터링 • 관리 효율화

03
주요 기능

주요 기능 요약

자동/수동 조치

사용자 참여 유도 기능

보안 점검(설문)

위젯(Widget)

주요 기능 요약

AhnLab ESA는 다양한 기능을 통해 고객사 정책에 따라 모든 개별 PC의 보안 상태를 안전하게 유도 및 관리할 수 있습니다.

75개 '점검 항목'의 선택적 운영 및 배점(점수) 산정	- 기업 환경 및 내부 정책에 따라 '점검 항목' 전체 또는 선택 적용 가능 - 75개 항목으로 기본 점검, 확장 점검, 관리자 지정 점검 항목 구성 - 자동실행 서비스 목록 및 윈도우 시작 프로그램 목록 수집 기능
점검 점수에 따른 네트워크 차단 설정	- 관리자가 '차단 점수' 설정 가능 - 일정한 점수 이상으로 조치 시 차단된 네트워크 자동 재연결 * AhnLab EPP management를 통한 조치
백그라운드(Background) 자동조치	- 자동조치를 통한 보안점수 상승 효과 , 별도의 사용자 조치 없이도 항상 안전 상태 유지 가능 - 비밀번호 재설정 등 사용자 개입이 필요한 항목은 사용자 유도 가능 - 기업의 필요에 따라 간편하게 조치할 수 있는 원클릭(One-Click) 버튼 수동 생성 가능
적극적인 사용자 유도 기능	- 기준 점수 이하인 경우, 바탕화면 상에서 에이전트 '메인 화면' 종료 불가(종료 방지 기능) - 위젯(Widget)을 통한 PC 취약점 점검 현황 상시 알림 - 구체적인 조치 방법 안내 제공(관리자용 텍스트 편집 가능)
PMS 연동 (*안랩에서만 제공 가능)	패치 파일 점검 항목에 최적화 - PMS 연동 조치, 폐쇄망 지원 OS(Windows), IE 및 MS Office, Adobe Flash Player, Adobe Reader, JAVA, HNC(한글) 등의 패치 관리 * AhnLab Patch Management 연동 시

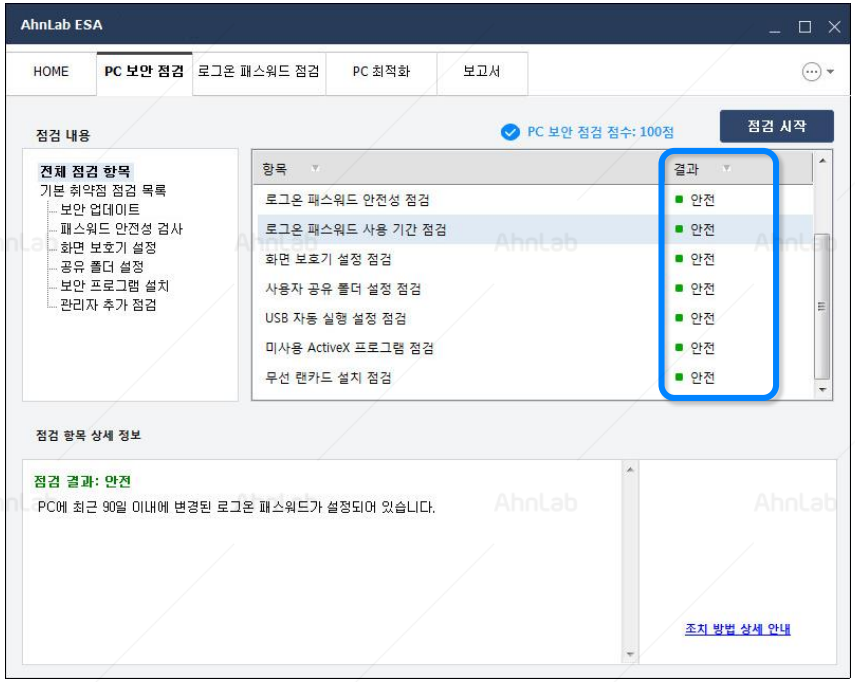
자동/수동 조치

내부 정책에 따라 자동 또는 수동 등의 다양한 조치 기능을 통해 사용자의 부담 없이 쉽고 간편하게 안전한 업무 환경을 구현할 수 있습니다.

- 내부 보안 정책에 따라 **완전 자동 조치** 또는 **원클릭 수동 조치** 설정 가능
- 취약 항목을 점검 화면에서 즉시, 원클릭으로 손쉽게 조치 가능 – 구체적인 조치 방법 안내 동시 제공

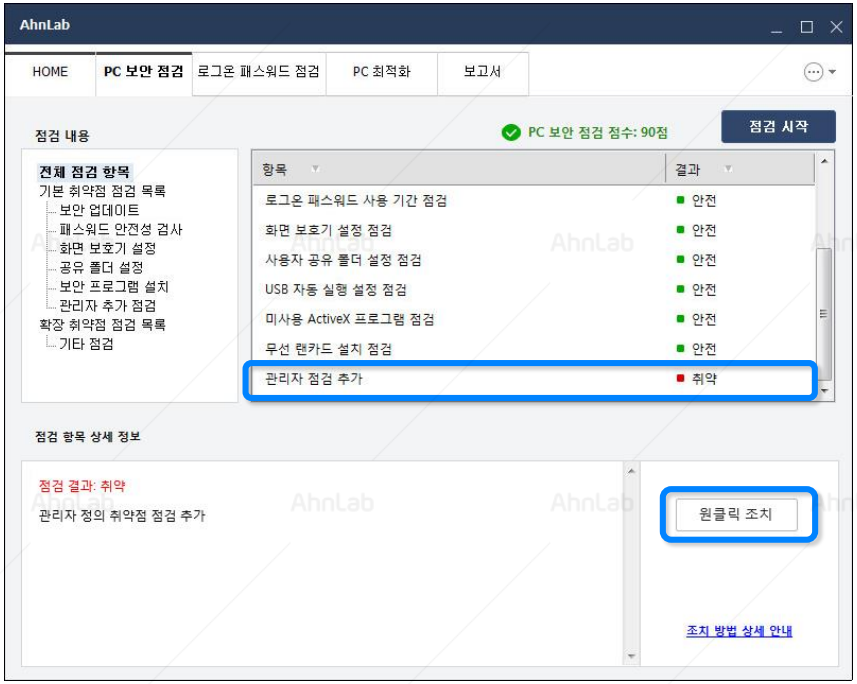
자동 조치(Background)

- 별도의 사용자 조치 및 관리자 개입 없이 항상 '안전' 상태 유지 가능



수동 조치(원클릭 방식)

- 점검 화면에서 사용자가 바로 손쉽게 취약점 조치 가능



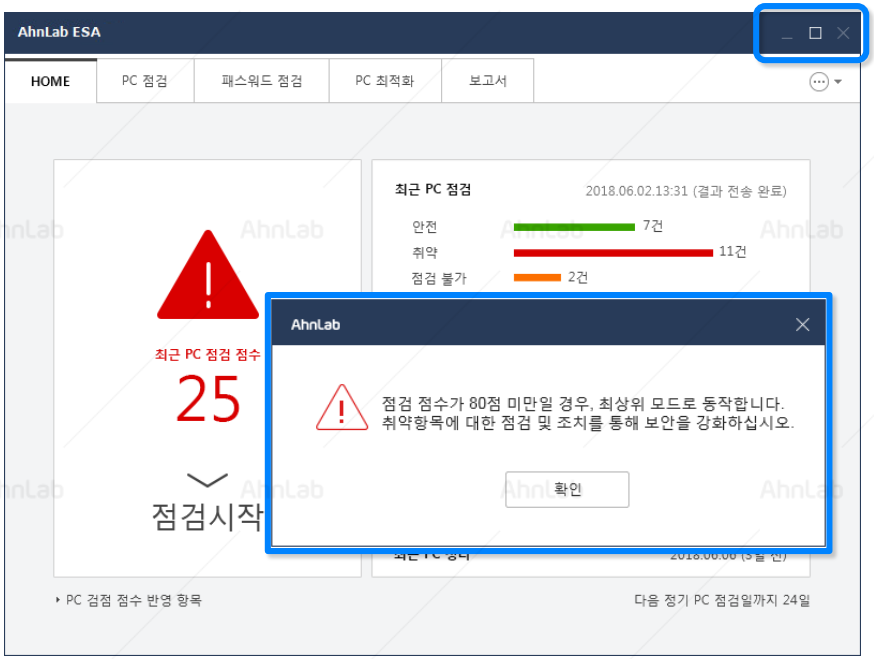
사용자 참여 유도 기능

다양한 사용자 유도 기능을 통해 사내 개별 PC의 보안 수준을 중앙에서 효율적으로 관리할 수 있습니다.

- 사용자 PC의 바탕화면 상에서 'AhnLab ESA' **메인 화면 종료 불가** 설정 가능
- 관리자가 설정한 기준 점수 이하 시 PC의 **네트워크 차단** 가능 - 별도의 NAC 연동 불필요

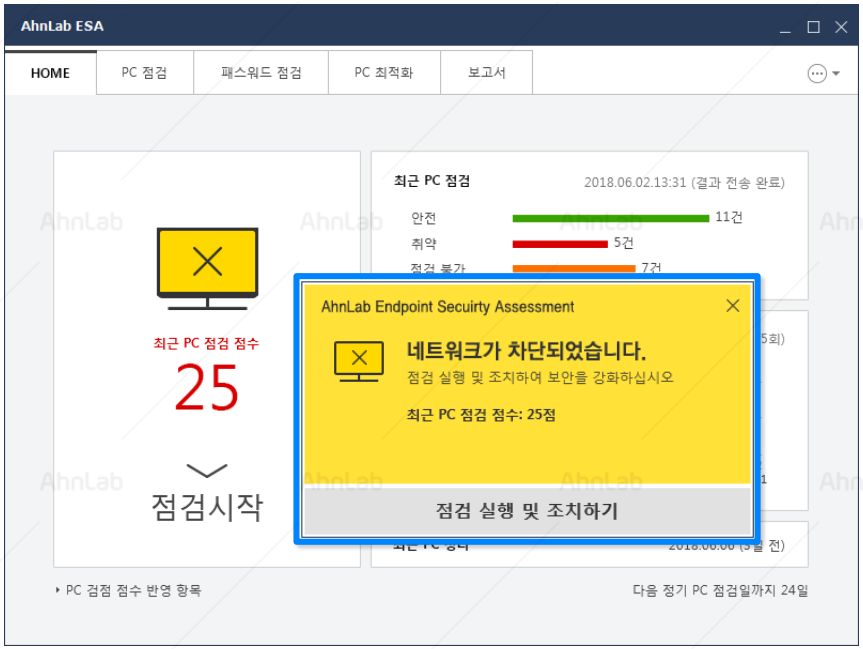
종료 방지 기능

- 기준 점수 이하의 경우 '종료(x)' 버튼 사용 금지
- 조치 시 완료 시 '종료' 버튼 자동 활성화



네트워크 연결 차단

- 기준 점수 이하인 PC의 네트워크 연결 차단
- 조치 완료 시 네트워크 자동 연결



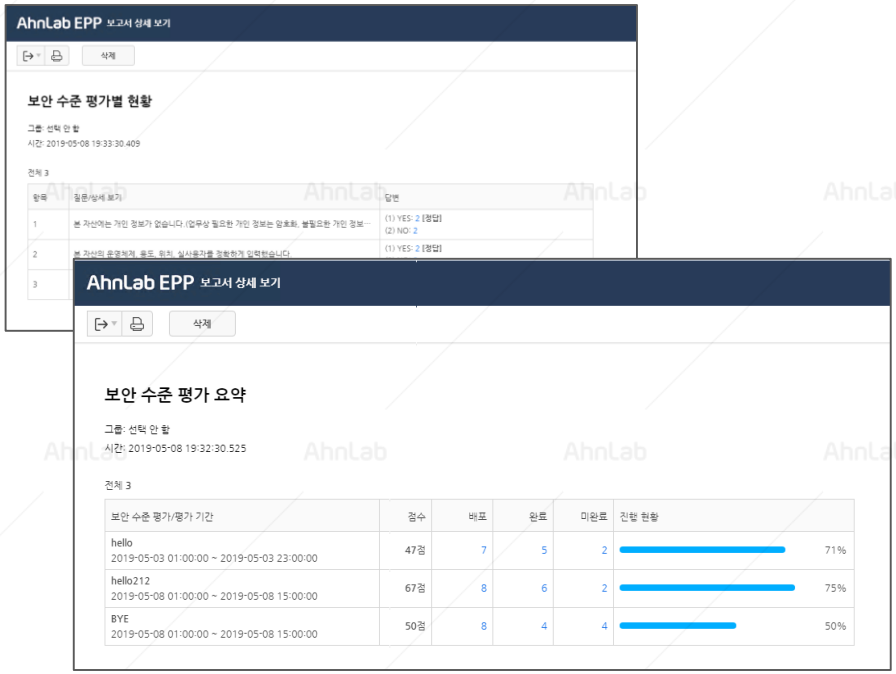
보안 점검(설문 기능)

보안 점검(설문) 기능을 통해 사내 보안 의식 향상 및 보안 사고에 미리 대비 할 수 있습니다.

- 다양한 문제 Pool을 이용해 설문 문항 선택 및 자체적으로 별도 작성 가능 (생성 → 배포 → 현황 관리 → 보고서)
- 각 문항에 따른 배점 적용 / 설문 기간 설정 / 주기적 노출 등 관리 편의성 향상
- 설문 완료 시 배포 / 완료 / 미완료 건수에 대한 모니터링 및 보고서 기능
- **금융위원회 전자금융감독규정의 정보보안 점검 항목 지원**

설문 생성 및 배포

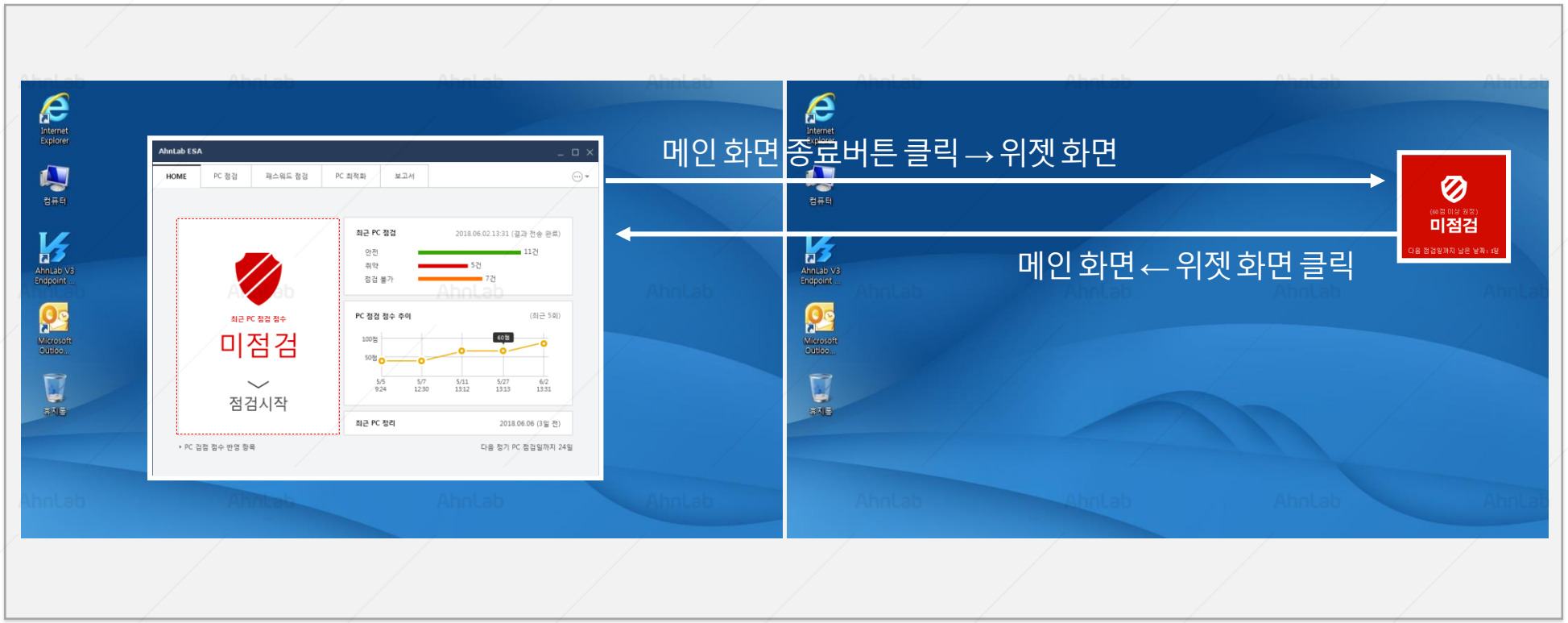
설문 보고서를 통한 통계 수집



위젯(Widget)

위젯(Widget)을 이용한 '상시 알림' 설정을 통해 PC 보안 수준을 향상 및 유지하고 사용자의 보안 인식 제고에 기여합니다.

- 관리자 정책 옵션에 따라 사용자 PC의 바탕화면 상시 알림(위젯) 제공
- 메인 화면을 통한 다양한 정보 알림 - 점수 현황 , 관리자 권장 점수, 다음 점검 일자, 최근 5회 점수 그래프, PC 정리 날짜 정보 등
- 사용자의 보안 인식 제고 및 능동적인 참여 유도 효과



04
도입 효과

'사이버•보안 진단의 날' 준수

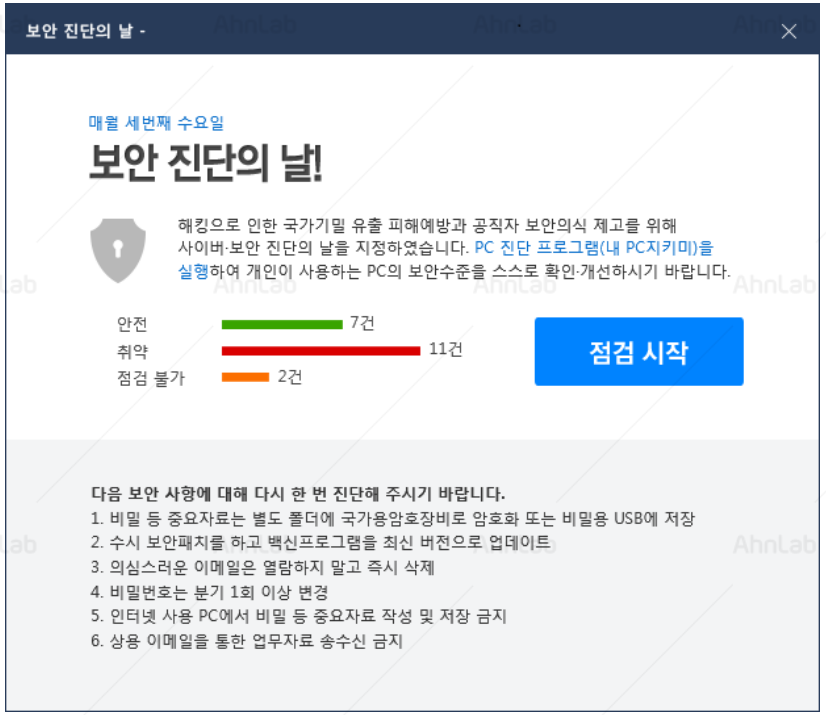
'정보보안 점검의 날' 대응

강력한 엔드포인트 통합 관리

'사이버·보안 진단의 날' 준수

안랩은 AhnLab ESA와 전문적인 서비스를 통해 '사이버•보안 진단의 날' 준수를 위한 보안 프로그램의 안정적인 운영 및 관리를 지원합니다.

- 자동/강제 조치, 사용자 참여 유도 등의 기능을 통해 '사이버•보안 진단의 날'에서 요구하는 보안 수준 달성 가능
- 다양한 보고서 기능 등 보안 담당자의 부담 해소 및 관리 효율성 극대화
- "안랩 제품에 의한 결과를 내PC지키미의 점검 결과로 인정한다" - 국가보안연구소(2013.08)



매월 세번째 수요일 '사이버 • 보안 진단의 날' 의무화

- 공공기관, 교육기관, 금융기관 대상
- 매월 PC 취약점 점검 및 개인정보 점검 등 보안 활동 실시

<관련 규정>

국가정보원 '국가정보보안 기본지침' 제16조
안전행정부 '정보통신보안업무규정' 제11조
교육과학기술부'보안업무규정시행세칙'제63조

해킹 등 사이버 공격으로부터
정보 자산 보호 및 전 직원 보안 의식 제고

NSRI 국가보안기술연구소

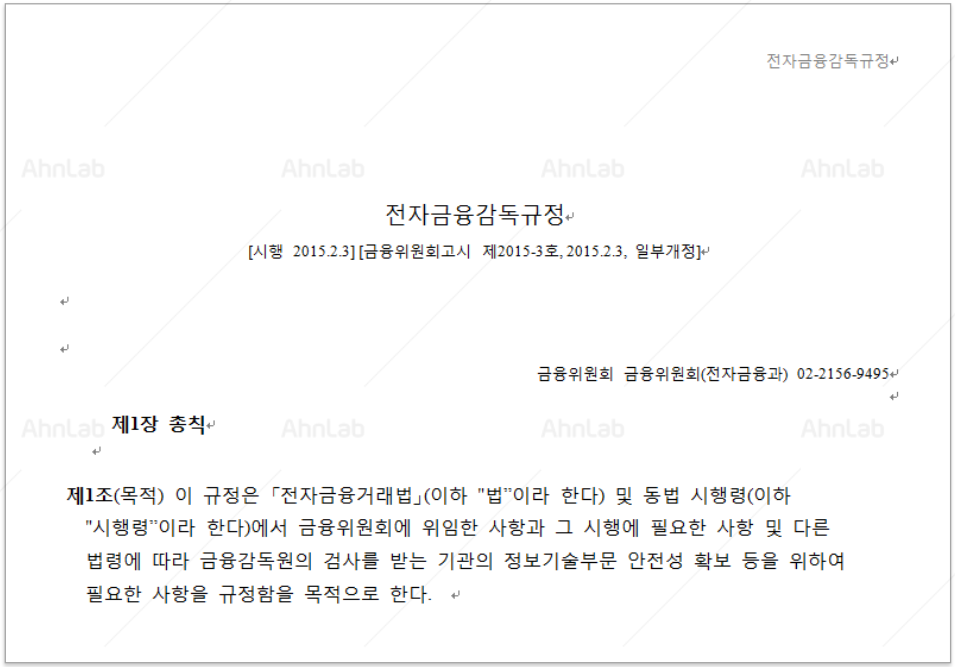
AhnLab, 국가보안기술연구소 선정 공식
'내PC지키미 협의체'

'정보보안 점검의 날' 대응(1/2)

AhnLab ESA를 통해 전자금융감독규정에서 요구하는 보안 점검 항목을 쉽고 편리하게 관리 및 조치할 수 있어 효율적인 '정보보안 점검의 날' 준수 및 대응이 가능합니다.

전자금융감독규정 제37조의 5 (정보보호최고책임자의 업무)

정보보호최고책임자는 정보보안점검의 날을 지정하고,
임직원이 금융감독원장이 정하는 정보보안 점검항목을 준수했는지 여부를 매월 점검하고,
그 점검 결과 및 보완 계획을 최고경영자에게 보고하여야 한다.



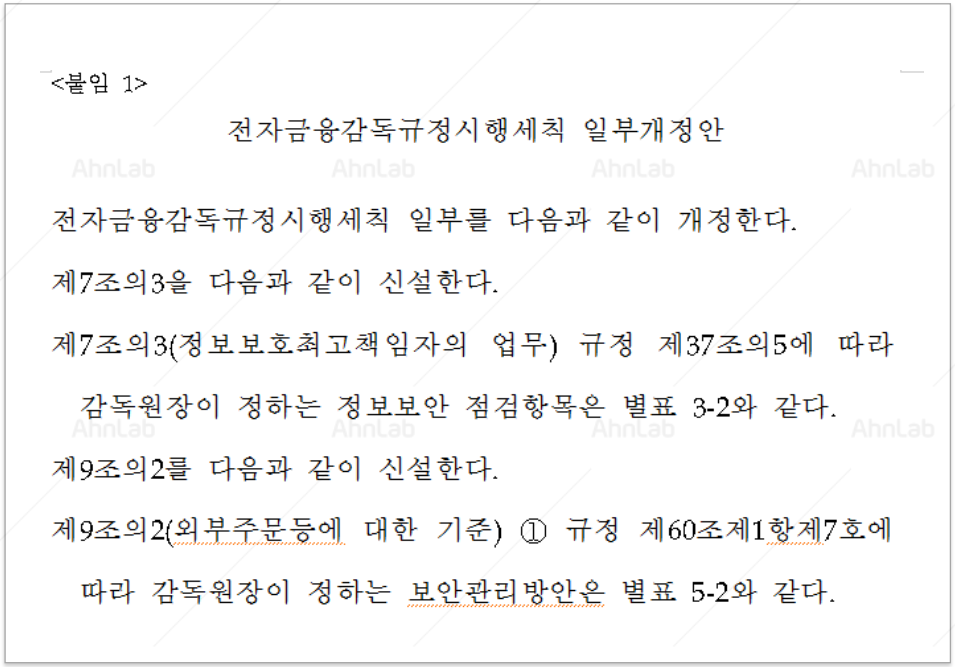
전자금융감독규정

[시행 2015.2.3] [금융위원회고시 제2015-3호, 2015.2.3, 일부개정]

금융위원회 금융위원회(전자금융과) 02-2156-9495

제1장 총칙

제1조(목적) 이 규정은 「전자금융거래법」(이하 "법"이라 한다) 및 동법 시행령(이하 "시행령"이라 한다)에서 금융위원회에 위임한 사항과 그 시행에 필요한 사항 및 다른 법령에 따라 금융감독원의 검사를 받는 기관의 정보기술부문 안전성 확보 등을 위하여 필요한 사항을 규정함을 목적으로 한다.



<붙임 1>

전자금융감독규정시행세칙 일부개정안

전자금융감독규정시행세칙 일부를 다음과 같이 개정한다.

제7조의3을 다음과 같이 신설한다.

제7조의3(정보보호최고책임자의 업무) 규정 제37조의5에 따라 감독원장이 정하는 정보보안 점검항목은 별표 3-2와 같다.

제9조의2를 다음과 같이 신설한다.

제9조의2(외부주문등에 대한 기준) ① 규정 제60조제1항제7호에 따라 감독원장이 정하는 보안관리방안은 별표 5-2와 같다.

'정보보안 점검의 날' 대응(2/2)

AhnLab ESA를 통해 전자금융감독규정에서 지정한 정보보안 점검항목을 통합 관리할 수 있습니다.

- 'PC 취약점 점검' 및 오프라인 '보안 점검'을 함께 관리함으로써 정보보안 점검 항목 준수 가능
- 다양한 보고서 기능으로 매월 최고책임자에게 보고해야 하는 관리자의 업무 효율화

종료 방지 기능

-AhnLab ESA 점검 항목으로 지원

- 예: 개인별 사용자계정과 비밀번호 부여 여부
  → 로그인 패스워드 안정성 여부 점검

네트워크 연결 차단

-PC 취약점 외 오프라인 점검항목도 통합 운영 가능

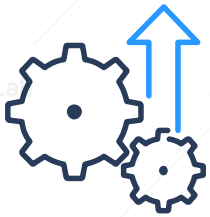
- 예: 전산자료 및 전산 장비의 반출·반입 통제 여부
  → 단말기 외부 반출 시 관리 대장을 기록·보관 합니다.(예/아니오)

강력한 엔드포인트 통합 관리

플랫폼 기반의 AhnLab ESA통한 취약 시스템 조치 및 고객 주도의 능동적 보안 실현

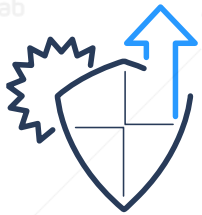
관리비용 절감

- 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
- 안랩 제품간 연계정책을 통한 통합보안 강화

05
도입 방식

AhnLab EPP 기반의 구축 및 운영

유연한 서버 구성을 통한 확장

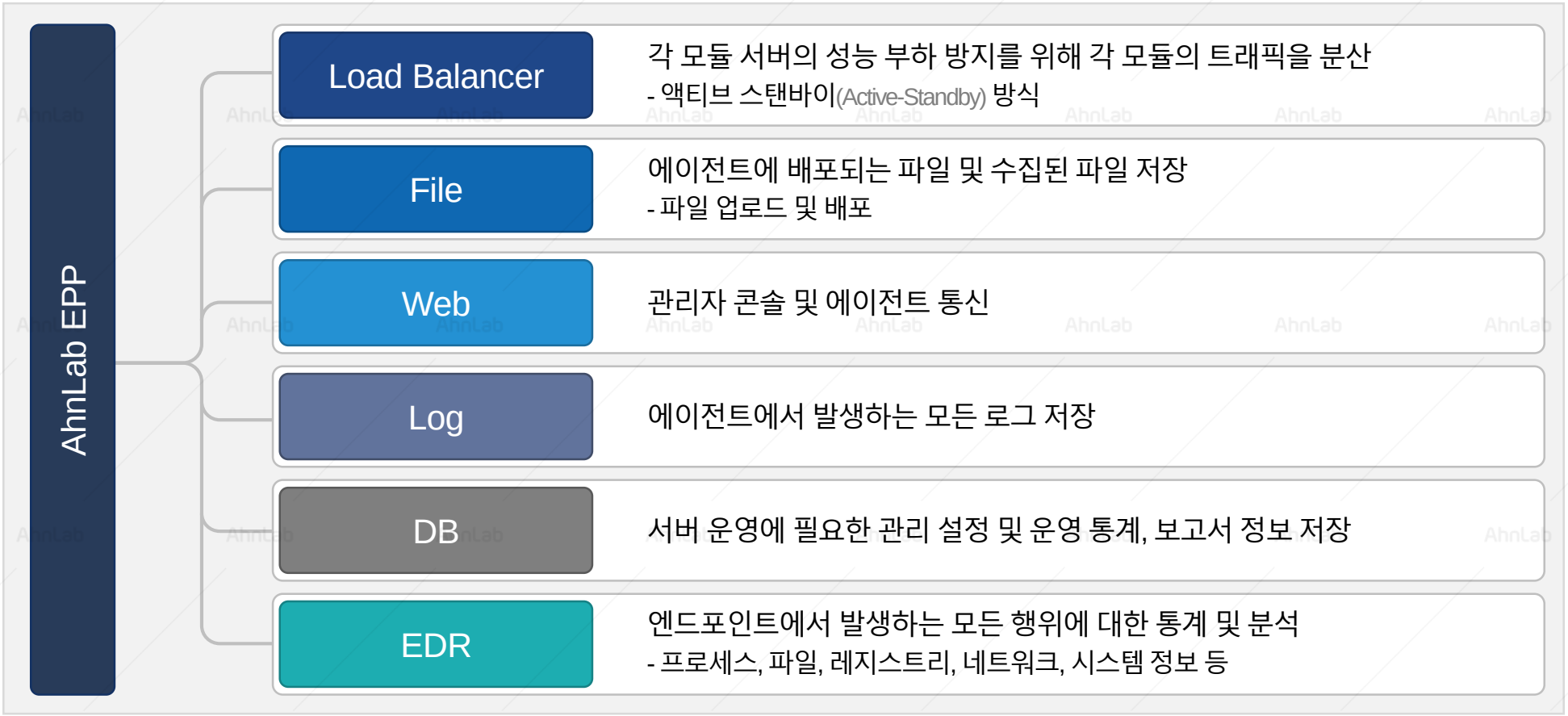
운영 환경

AhnLab EPP 기반의 구축 및 운영

AhnLab ESA는 모듈 방식으로 구성된 차세대 엔드포인트 플랫폼 AhnLab EPP를 통해 간편하게 구축 및 운영할 수 있으며, 필요 시 유연하게 확장할 수 있습니다.

- AhnLab EPP 모듈 구성: 로드 밸런서, 파일, 로그, DB

  * EDR 모듈은 EDR 사용 시에만 필요

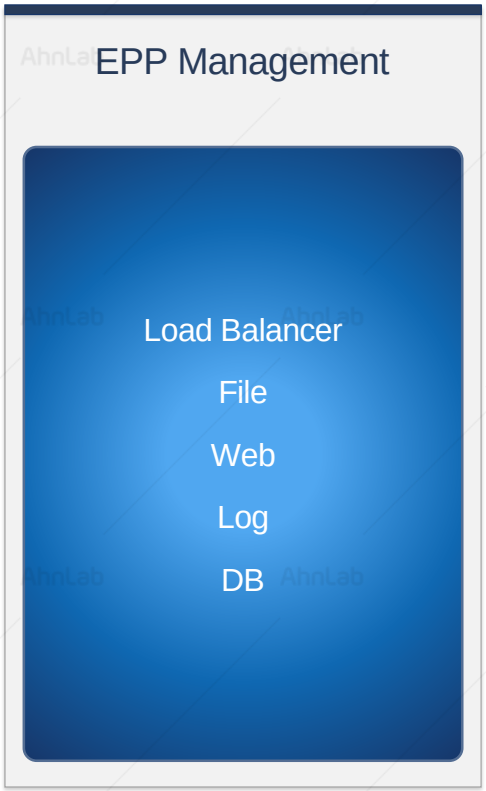


유연한 서버 구성을 통한 확장

AhnLab EPP 기반으로 운영하는 AhnLab ESA는 고객사 환경에 따라 시스템을 유연하게 구성할 수 있는 다양한 옵션을 제공합니다.

- 최적화된 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
- Load Balancer / File 서버의 경우 네트워크 별로 확장 구성 가능

구성 1. **올인원** (단일 장비)

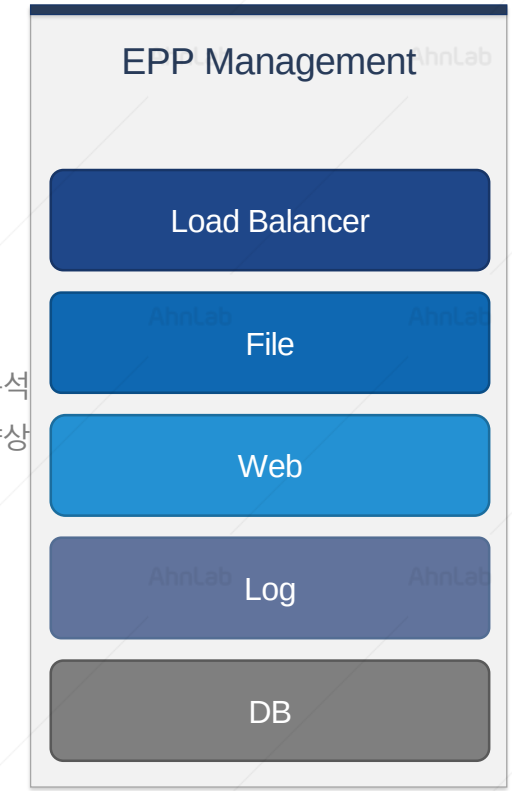


관리·로그
성능 향상

구성 2. **분리형** (개별 장비)

로그·분석
성능 향상

구성 3. **전체 독립형** (개별 장비)



운영 환경

AhnLab ESA는 차세대 엔드포인트 보안 플랫폼 AhnLab EPP Management를 기반으로 효율적인 통합 관리를 제공합니다.

- AhnLab ESA 에이전트 설치 환경

구분	상세 버전
운영체제	Windows XP SP3 / Vista / 7 / 8(8.1) / 10 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
지원 언어	한국어, 영어, 중국어(간체), 일본어

- 관리 콘솔(AhnLab EPP Management) 운영 환경

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

- 권장 서버 하드웨어 사양 (AhnLab EPP Management 설치 환경)

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

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 ESA

AhnLab