More security,
More freedom

AhnLab
EPP Device Control

기업 인프라 보안를 위한 최적의 장치 제어 솔루션

표준제안서

AhnLab

목차

01
제안 배경

기업 데이터 유출에 따른 리스크

외부 공격의 최초 인입 경로로 악용되는 장치

장치 통제 관련 컴플라이언스

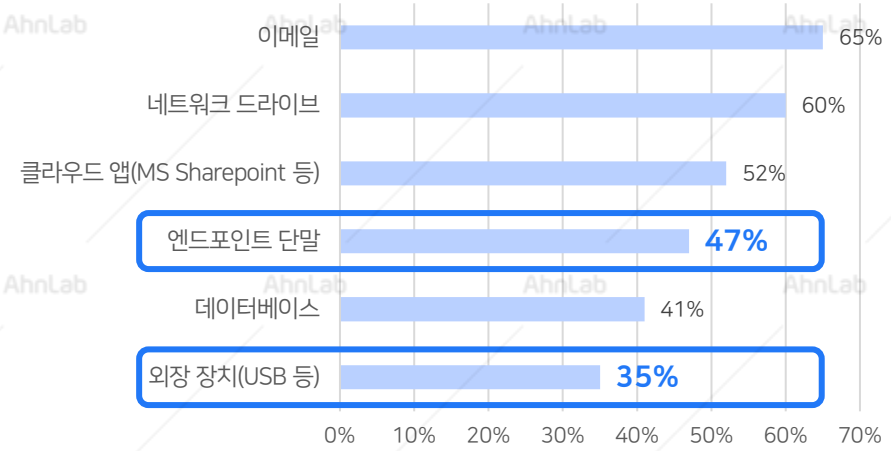
AhnLab

기업 데이터 유출에 따른 리스크

기업 주요 데이터의 상당 수는 관리자가 가시성을 확보하기 어려운 엔드포인트 단말과 외장 장치에 저장되어 있습니다. 데이터 유출을 막기 위해서는 유출에 악용되는 외부 저장 매체에 대한 통제 방안을 구축하고, 사고 발생 시 리스크를 최소화하기 위한 가시성 확보가 필요합니다.

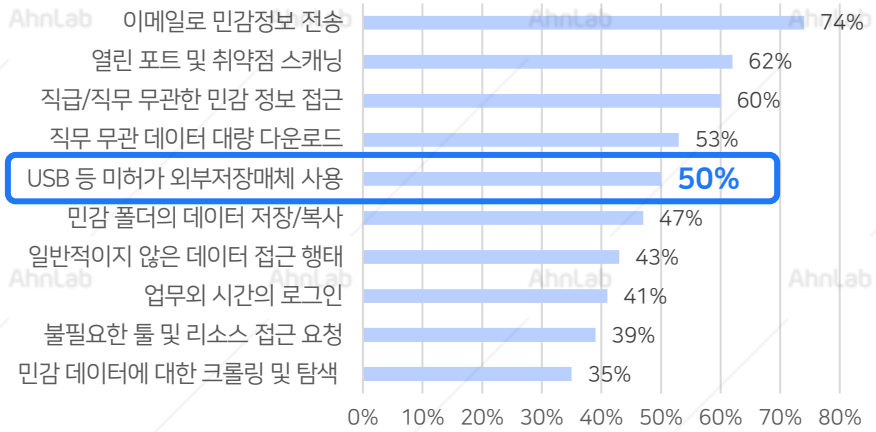
기업의 주요 민감 정보 저장 위치

35% 이상의 기업이 엔드포인트 단말 또는 외장장치에 민감 데이터 보관



악의적 내부자가 데이터 유출 시 시도하는 행위들

50% USB 등 외부 저장 매체를 통한 데이터 유출 시도



출처 : Ponemon Institute 2022 내부자 위협 비용에 대한 글로벌 리포트

데이터 유출 시 **평균 피해 규모 & 복구 기간**

$490만 / 10개월

악의적인 내부자

$446만 / 9개월

사고로 인한 데이터 유출 또는 손실/디바이스 도난

출처 : IBM 2023년 데이터 침해 비용 보고

공격 인입 경로로 악용되는 장치

USB는 오래 전부터 해킹 공격에 악용되어 왔으나, 최근 감염된 USB를 통해 기업 기밀 데이터를 탈취하는 공격 건수가 3배 증가한 것으로 확인되었습니다.
기업은 정상적인 업무 목적의 활용을 보장함과 동시에 악의적인 장치 접근을 막을 수 있도록 보안과 업무 생산성 두가지를 모두 고려해야 합니다.

다시 활성화되고 있는 USB를 통한 악성코드 공격

러시아의 가마레돈, USB 통해 리틀드리프터 웜 퍼트리고 있어
입력 : 2023-11-21 12:10

악성 USB 통해 퍼지는 소구와 스노위드라이브 멀웨어
입력 : 2023-07-18 12:18

USB 활용한 사이버 공격, 아직 알 수 없는 이유로 급증하고 있어
입력 : 2023-07-19 15:28

USB를 통해 연쇄적인 공격 실시하는 공격자들, 멀웨어 활발히 퍼트려
입력 : 2024-02-01 13:54

USB 장치를 통한 악성코드 공격 사이클

감염된 USB 연결	사용자에 의한 악성 파일 실행	단말 기반 확보 및 악성 행위	다른 USB 드라이브로 확산	목적 달성
	• 메모리 인젝션 및 쉘코드 파일 실행하는 악성 DLL 로딩	• 레지스트리 키 생성 • 호스트 접근 권한 획득 • 메모리 인젝션 • 백도어 삽입	• 호스트 PC에 연결된 새로운 USB 드라이브로 확산	• 데이터 유출

참고 : Mandiant Threat Intelligence, 2023

장치 제어 및 관리 관련 컴플라이언스 강화

개인정보보호법, 정보통신망법, ISMS 인증 기준 등 다수의 정보 보호 관련 컴플라이언스에서 보조 저장 매체에 대한 제어 및 통제 권한을 요구하고 있습니다. 외장 장치를 통한 대내외 보안 리스크를 사전에 예방하고 빠르게 대응하기 위해서는 효과적인 관리 방안을 마련해야 합니다.

주요 정보보호 컴플라이언스의 저장 매체 제어 및 관리 요구 사항

관련 규제	주요 요구 사항
개인정보보호법	• **법 제29조(안전조치의무)** - 개인정보처리자는 개인정보가 분실 · 도난 · 유출 · 위조 · 변조 또는 훼손되지 아니하도록 - 내부 관리계획 수립, 접속기록 보관 등 안전성 확보에 필요한 기술적 · 관리적 및 물리적 조치를 하여야 한다. • 개인정보의 안전성 확보조치 기준 제11조(물리적 안전조치) • 개인정보의 기술적/관리적 보호조치 기준 제8조(물리적 접근 방지)
ISMS/ISMS-P 인증 (정보통신망법, 개인정보보호법)	• **대상** - 서울특별시 및 모든 광역시에서 정보통신망서비스를 제공하는 사업자 - 집적정보통신시설 사업자, 연 매출 또는 세입이 1,500억원 이상인 상급종합병원 또는 재학생 수가 1만명 이상인 학교, - 정보통신서비스 부문 전년도 매출 100억원 이상이거나 직전 3개월 DAU가 100만명 이상인 정보통신서비스제공자 • **인증기준** - 보조저장매체를 통하여 개인정보 또는 중요 정보의 유출이 발생하거나 악성코드가 감염되지 않도록 관리 절차를 - 수립 및 이행하고, 개인정보 또는 중요정보가 포함된 보조저장매체는 안전한 장소에 보관하여야 한다. • **주요 확인사항** **- 외장하드, USB메모리, CD 등 보조저장매체 취급(사용), 보관, 폐기, 재사용에 대한 정책 및 절차를 수립·이행 여부** - 보조저장매체 보유현황, 사용 및 관리실태의 주기적 점검 여부 - 주요 정보시스템이 위치한 통제구역, 중요 제한구역 등에서 보조저장매체 사용 제한 여부 - 보조저장매체를 통한 악성코드 감염 및 중요정보 유출 방지를 위한 대책 마련 여부

02

AhnLab EPP Device Control

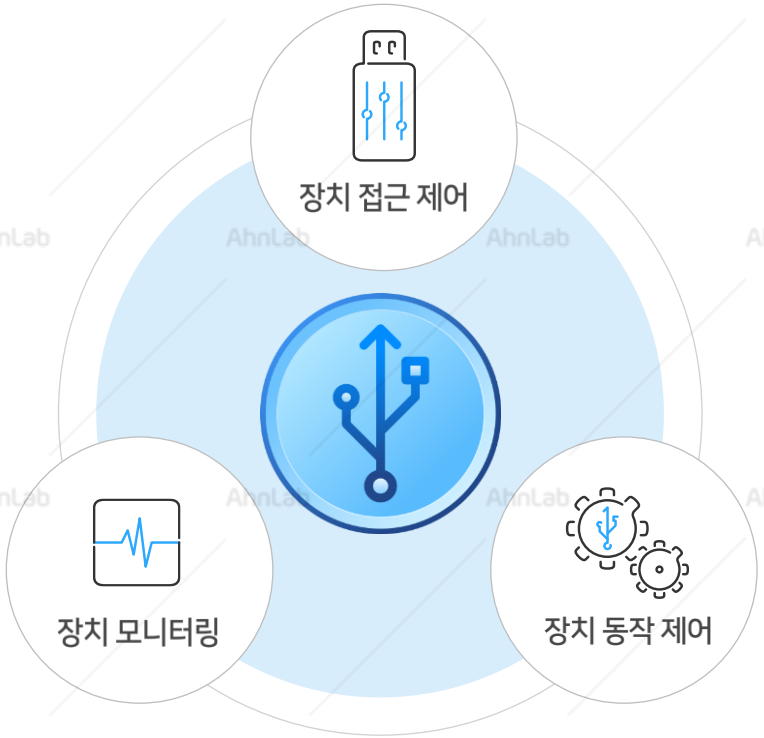
AhnLab

AhnLab EPP Device Control

AhnLab EPP Device Control은 차세대 엔드포인트 보안 플랫폼 기반의 **장치 접근 및 동작 제어 솔루션**입니다.
기업 인프라에 대한 외부 장치의 접근을 제어하고, 연결된 장치로 기업 단말 정보의 이동을 제어함으로써
외부에서 인입되는 악성 위협과 내부에서 기업의 주요 정보가 무단 유출되는 리스크를 원천 차단합니다.

AhnLab EPP Device Control

기업 자산 보호 및 악성 위협 차단



기업 자산에 접근하는 장치의 통합 관리 및 제어

외부 주요 장치의 **접근 차단**과 내부 기업 정보의 **외부 유출**을 제어
업무 필요에 따라 관리자의 **예외 시간대 및 장치 설정** 기능

통합 관리 편의성

차세대 엔드포인트 보안 플랫폼 AhnLab EPP 기반의
단일 매니지먼트, 단일 에이전트를 통한 **통합 관리**

시스템 하드닝

AhnLab EPP 기반의 보안 솔루션 연계를 통한
엔드포인트 **시스템 하드닝**(System Hardening)

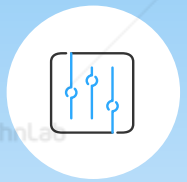
특장점 (1/2) – 제품 안정성 및 쉬운 사용성

AhnLab EPP Device Control은 기업 내외부에서 외장 장치로 인해 발생할 수 있는 보안 리스크를 강력하게 대응하는 동시에 관리자가 간단하게 관리할 수 있는 예외 설정 및 모니터링 기능을 제공합니다.

제품 안정성 및 쉬운 사용성 | 구축·운영 편의성 및 보안 강화

제품 안정성 및 지원 범위

- 누적된 안랩의 노하우를 기반으로 한 15개 이상 장치에 대한 제어 기능 지원
- USB, CD/DVD, WPD 장치 등 주요 업무용 저장 장치에 대한 쓰기 차단 지원
- 클라이언트/서버 OS, 물리/가상 환경* 지원
- 정책 설정 전 내부 장치 사용 현황에 대해 사전 검토할 수 있는 테스트 모드



쉬운 관리 옵션

- EPP 정책 기준 차단 예외 장치 최대 3,000개 등록 및 관리 가능
- 고객사 운영 환경 특성에 따라 장치 제어 금지 시간대 설정 가능
- 그룹별 또는 에이전트 개별 정책 할당을 통한 장치 사용 권한 부여
- 장치별 일시 예외 시간 설정(NEXT)

대시보드 및 보고서

- 장치 제어 현황을 한눈에 확인할 수 있는 대시보드(Dashboard)
- 기업 및 기관의 환경에 따라 필요한 정보만 편집해서 볼 수 있는 사용자 정의 대시보드 제공
- 일정 기간별 기업 내 장치 제어 차단, 예외 허용 등 이벤트 발생 현황을 파악할 수 있는 보고서 제공

전문 서비스를 통한 운영 안정성

- 안랩의 전문 인력을 통한 지속적이고 안정적인 지원 서비스
- 장치 제어 현황 모니터링 및 통제를 통한 비즈니스 연속성 확보

* VM Guest OS에서 장치 인식이 지원되는 경우 限

특장점 (2/2) - 구축·운영 편의성 및 보안 강화

AhnLab EPP Device Control은 차세대 엔드포인트 플랫폼 AhnLab EPP를 기반으로 구축 및 운영 편의성은 물론, 보안 솔루션 연계를 통한 시스템 하드닝(System Hardening) 효과를 제공합니다.

제품 안정성 및 쉬운 사용성 | **구축·운영 편의성 및 보안 강화**

구축 및 확장 편의성

- 라이선스 추가만으로 솔루션 구축 완료 (플러그인 방식)
- 기업 및 기관의 규모, 네트워크 환경에 따라 다양한 서버 구성 가능
- 병렬 구조(Scale Out 방식) 기반의 간편한 서버 추가 및 확장 가능
- 모듈 기반의 유연한 확장성, 관리 편의성 및 운영 안정성

플랫폼 기반의 효율적인 통합 관리

- 차세대 엔드포인트 보안 플랫폼 AhnLab EPP 기반의 단일 에이전트, 단일 관리 콘솔을 통한 운영 부담 최소화
- 백신, 개인정보, 패치 관리, 취약 시스템 점검·조치, 엔드포인트 위협 탐지·대응(EDR) 등 다수의 보안 솔루션 통합 운영 및 관리
- AhnLab EPP 기반의 솔루션 구축 및 관리를 통한 TCO 절감 효과

시스템 하드닝 (System Hardening)

- AhnLab EPP 기반의 다양한 엔드포인트 보안 솔루션 연계를 통한 위협 대응 및 조치
- 확장된 엔드포인트 가시성 확보를 통한 위협 탐지 및 대응 시간 최소화
- 장치 연결 차단 및 쓰기 차단 임시 차단 예외 등의 관리 명령, 규칙을 통한 (검토 예정) 유기적인 대응 및 엔드포인트 시스템 하드닝 효과

주요 기능

<table>
<tr><th colspan="2">구분</th><th>상세 내용</th></tr>
<tr><td rowspan="4">장치 제어</td><td>장치 연결/쓰기 제어 (차단 또는 허용)</td><td rowspan="2">• 주요 장치에 대한 연결/쓰기 차단*
<table><tr><th>USB</th><th>CD/DVD 드라이브</th><th>휴대용 장치(WPD)</th><th>디스크 드라이브</th><th>Bluetooth</th></tr><tr><td>이미징 장치</td><td>PCMCIA</td><td>IEEE 1394</td><td>플로피 디스크</td><td>모뎀</td></tr><tr><td>스마트 카드 리더</td><td>네트워크 어댑터</td><td>COM/LPT 포트</td><td>적외선 포트</td><td>+ 추가 검토 예정</td></tr></table></td></tr>
<tr><td>휴대용 장치 차단 시 충전 허용</td></tr>
<tr><td>장치별 테스트 모드 지원</td><td>• 테스트 모드 설정 시 실제 차단은 하지 않고 차단 로그만 남김 (접근 제어 대상 장치 모두 지원)</td></tr>
<tr><td>업무용 장치 종류 예외 옵션</td><td>• USB 프린터 및 USB 미디어 강제 허용 ON 시 개별 장치를 예외 등록하지 않아도 차단 대상에서 예외</td></tr>
<tr><td>장치 제어 금지 시간대 설정</td><td>• 주요 업무 시간대 등 설정한시간대에는 장치 제어 기능이 일시적으로 동작하지 않음</td></tr>
<tr><td rowspan="4">제어 예외</td><td>장치 접근 차단 예외</td><td>• 장치 인스턴스 경로 기준 최대 3,000개/정책당 설정 가능</td></tr>
<tr><td>EPP 관리 정책에서 설정</td><td>• 관리자가 직접 특정 장치의 인스턴스 경로를 예외 대상으로 추가 가능</td></tr>
<tr><td>장치별 예외 허용 기간 설정 ('24.2H 예정)</td><td>• 관리 정책에 추가 시 혹은 사용자 예외 신청 시 허용 기간 설정 옵션 지원</td></tr>
<tr><td>예외 후 90일 미사용 장치 관리 ('24.2H 예정)</td><td>• 예외 장치 관리를 위한 일정 기간 미사용 장치에 대한 정보 제공</td></tr>
<tr><td rowspan="2">장치 제어 모니터링</td><td>장치 제어 현황 대시보드</td><td>• 장치별 연결 차단 현황
• 장치 연결/쓰기 차단 순위
• 에이전트/장치별 연결 차단 추이</td></tr>
<tr><td>에이전트별 현황</td><td>• EDC 현황
• 최근 30일 내 장치 제어 이력</td></tr>
<tr><td rowspan="2">장치 제어 로깅 및 알림</td><td>장치 제어 케이스별 로깅 ON/OFF</td><td>• 장치 연결 차단 / 차단 테스트 / 예외 허용 로그 (장치 클래스/장치 설명/인스턴스 경로/모드)
• 장치 쓰기 차단 로그 (접근 프로세스/대상 파일)</td></tr>
<tr><td>케이스별 알림 ON/OFF</td><td>• 장치 연결 차단 시 알림
• 시스템 다시 시작 필요 알림
• 장치 쓰기 차단 시 알림 ('24.2H 예정)</td></tr>
<tr><td>장치 제어 관련 보고서</td><td>장치 제어 동작별 현황 보고서</td><td>• 장치 연결 차단, 쓰기 차단
• 장치 제어 예외</td></tr>
</table>

* 일부 장치의 경우 출시 시점에 지원 여부가 변동될 수 있음

도입 효과

기업의 업무 생산성과 보안성 모두를 위한 AhnLab EPP Device Control은 기업 및 기관의 장치 제어를 통한 데이터 유출 방지 및 위협 인입 차단과 더불어, 기업 인프라에 접근하는 디바이스에 대한 가시성을 확보하여 안전한 비즈니스 환경 구축에 기여합니다.

AhnLab EPP Device Control

기업 내·외부 장치를 통한 보안 사고 예방

- 주요 업무용 장치(USB, CD/DVD, 휴대용 장치)를 통한 파일 무단 유출 방지
- 장치 차단 테스트 모드, 장치 차단 금지 시간대 설정 등 기업의 업무 환경 고려
- 그룹별 정책 할당을 통한 대상별, 오프라인 정책을 통한 상황별 장치 제어 동작 가능

보안 이슈 발생 시 리스크 규모 최소화

- 장치 제어를 통한 데이터 유출 사고 방지 및 로그, 이력 관리를 통한 이슈 확인, 리스크 확산 최소화
- 장치 제어 케이스별 로그, 에이전트별 차단 이력을 통해 기업 내 장치 사용에 대한 가시성 확보
- 장치 제어 대시보드를 통한 이상 사용 패턴 모니터링 및 탐지

관리 효율성 및 생산성 재고

- AhnLab EPP 기반의 플러그인과 장치 제어 솔루션 통합 관리를 통한 보안 운영 부담 해소
- EPP 플랫폼 연계 규칙 연동을 통한 AV, EDR 등 제품들과의 시너지 (예정)
- 지속적인 전문 지원 서비스를 통한 안정적인 제품 운영 및 관리

지원 운영 체제

구분		상세 버전
EDC Agent	Windows Desktop	- Windows 8(8.1) - Windows 10 - Windows 11
	Windows Server*	- Windows Server 2012 / 2012 R2 - Windows Server 2016 - Windows Server 2019 - Windows Server 2022
비고		• 상기 OS의 x86/x64 호환 모드 지원 • Windows Server OS는 재부팅 이슈가 있는 기능은 미지원 (현재 휴대용 장치의 쓰기 차단 기능만 해당) • VM Guest OS에서 연결된 장치의 제어가 가능한 경우 지원 가능

03
도입 방식

솔루션 구축 개념도

AhnLab EPP 기반의 구축 및 운영

유연한 서버 구성을 통한 확장

AhnLab

솔루션 구축 개념도

AhnLab EPP Device Control은 차세대 엔드포인트 플랫폼 AhnLab EPP를 기반으로 탁월한 구축 및 운영 편의성과 보안 솔루션 연계를 통한 시스템 하드닝 효과를 제공합니다.

- 플러그인(plug-in) 방식 - 라이선스 적용만으로 간편하게 구축 및 다수의 보안 제품과 통합 운영 가능

AhnLab EPP 기반의 구축 및 운영

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

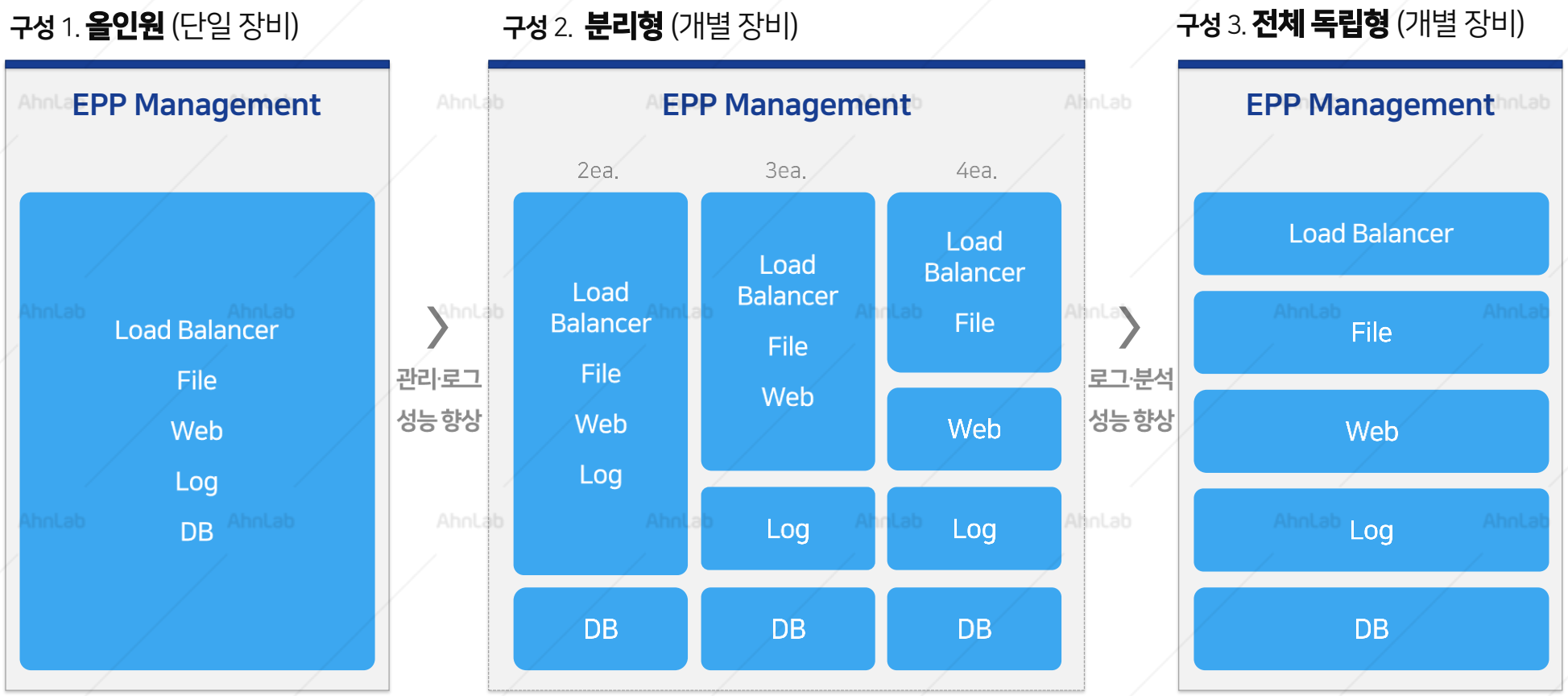
- **AhnLab EPP 모듈 구성: 로드 밸런서, 파일, 로그, DB**

  * EDR 모듈은 EDR 사용 시에만 필요

유연한 서버 구성을 통한 확장

AhnLab EPP 기반으로 운영하는 AhnLab EPP Device Control는 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



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
EPP Device Control

AhnLab

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