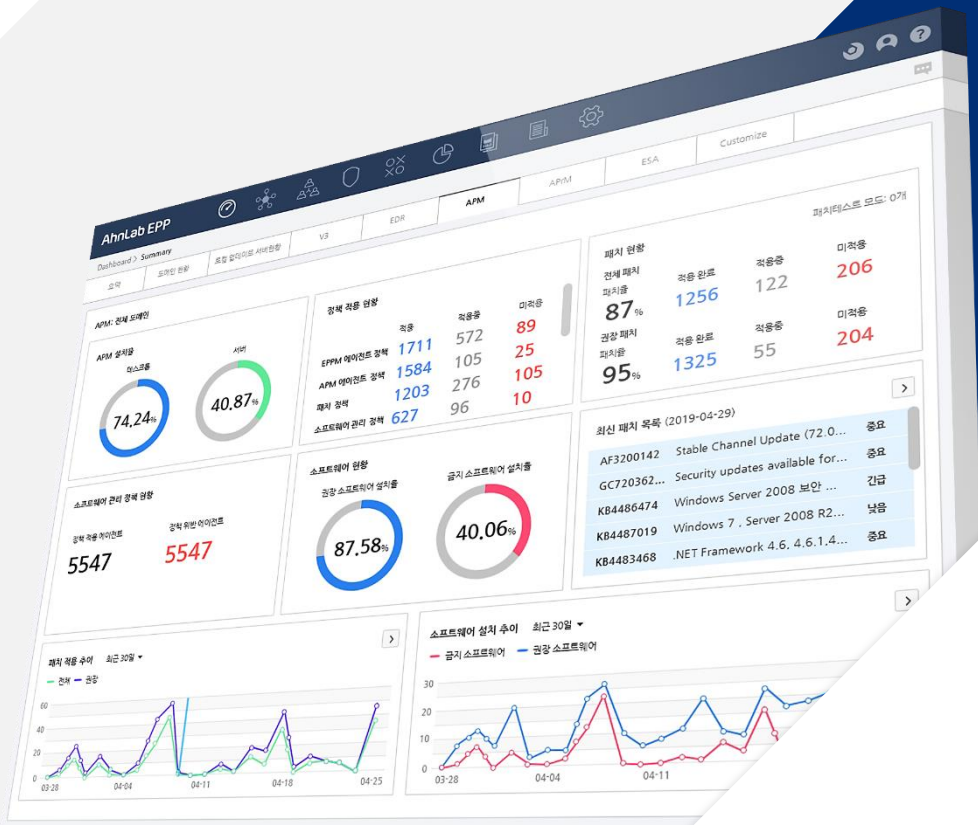
AhnLab

EPP Patch Management

More security,
More freedom

플랫폼 기반의 혁신적인 패치 관리

표준제안서



AhnLab

CONTENTS

AhnLab

01
제안 배경

취약점 기반 공격의 다변화 및 고도화

알려진 취약점 기반 공격 증가

패치 관리 미비에 따른 공격 표면 확대

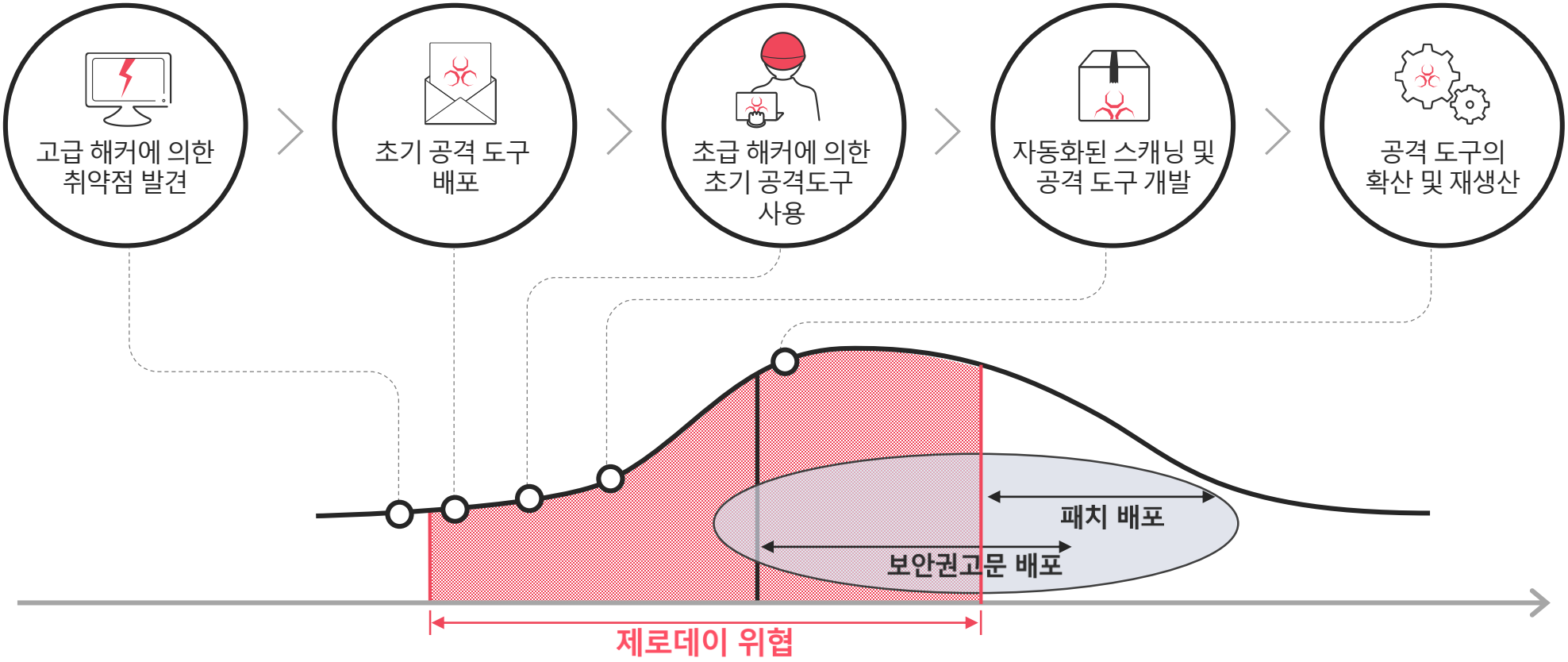
패치 관리 관련 컴플라이언스 강화

취약점 기반 공격의 다변화 및 고도화

전통적인 악성코드는 물론, 최신 랜섬웨어나 지능형 위협(Advanced Persistent Threat)도 운영체제(OS)나 주요 애플리케이션의 취약점을 이용하고 있습니다. 특히 취약점 발견 후 관련 패치가 배포되기 전에 해당 취약점을 이용하는 제로데이 공격(Zero-day Attack)은 막대한 피해를 야기합니다.

- Adobe Flash Player, MS Office, Internet Explorer, Chrome 등 기업 및 기관에서 사용하는 애플리케이션 다양화
- 주요 애플리케이션의 제로데이 취약점 증가 및 이를 이용한 제로데이 공격 증가

제로데이 공격 라이프사이클

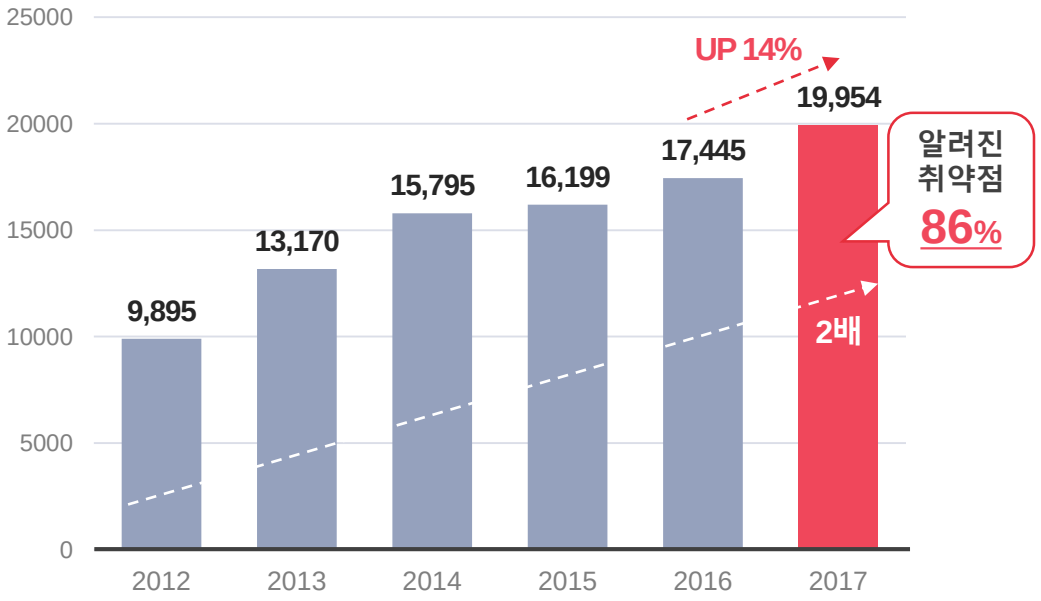


알려진 취약점 기반 공격 증가

최근 발생한 보안 침해 사고는 제로데이 취약점이 아닌 이미 보안 패치가 배포된 알려진 취약점을 활용한 경우가 많습니다.
보안 패치가 배포되어도 실제 기업 및 기관의 패치 적용으로 이어지기까지는 시간이 걸리기 때문에 알려진 취약점을 활용한 다양한 공격이 반복적으로 피해를 야기하고 있습니다.

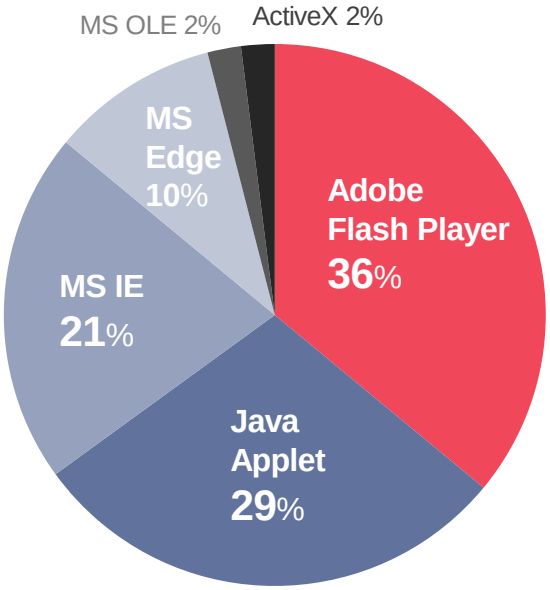
- 2017년 취약점 기반 공격 중 86%가 이미 패치가 배포된 알려진 취약점 활용
- 케르베르 랜섬웨어, 워너크라이 랜섬웨어, 드라이덱스 등 다수의 알려진 취약점 활용한 악성코드 증가
- 어도비의 플래시 개발 중단에 따라 마이크로소프트(MS)의 SW 취약점 악용 증가 추세

전 세계 취약점 보고 현황(2012-2017)



*출처: Flexera, Vulnerability Review 2018

2018 상반기 국내 SW 취약점 악용 현황

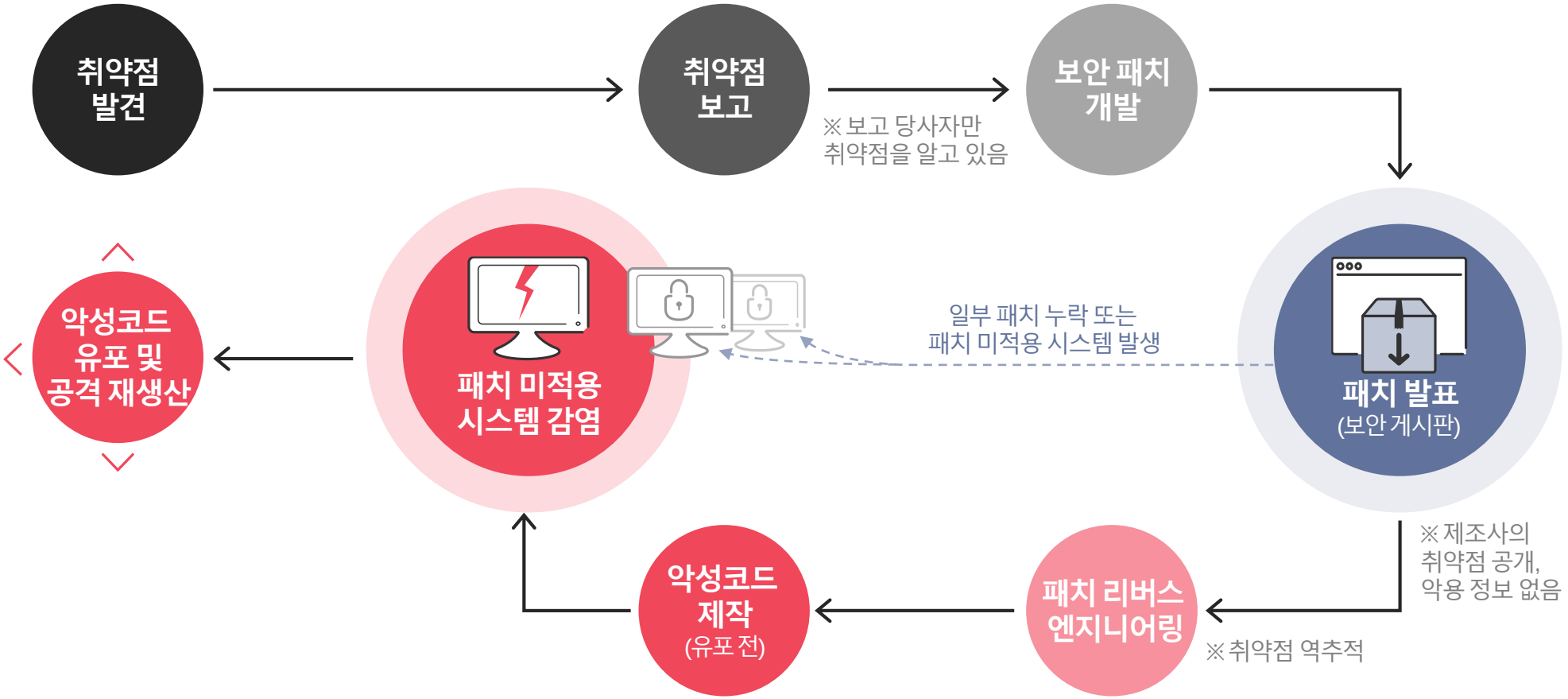


*출처: 한국인터넷진흥원(KISA)

패치 관리 미비에 따른 공격 표면 확대

제로데이뿐만 아니라 알려진 취약점을 이용한 공격이 지속적으로 증가하고 있는 반면, 관련 솔루션 및 프로세스 미비에 따른 패치 적용의 한계와 이로 인해 보안 취약점의 누적으로 기업 및 기관의 위협 노출 범위(attack surface)가 확대되고 있습니다.

보안 취약점 이용한 공격 발생 과정



패치 관리 관련 컴플라이언스 강화

개인정보보호법을 비롯한 다수의 정보 보호 관련 규제가 고도화된 패치 관리를 요구하고 있습니다.
패치 관리 미비에 따른 대내외적인 보안 위협에 대응하기 위해서는 실효성 있는 패치 관리 방안을 마련하는 것이 가장 중요합니다.

주요 정보 보호 관련 규제의 패치 관리 요구 사항

관련 규제	주요 요구 사항
개인정보보호법 (행정자치부 고시, 개인정보의 안전성 확보조치 기준)	<제8조 악성프로그램 등 방지> 개인정보처리자는 악성프로그램 등을 방지·치료할 수 있는 백신 소프트웨어 등의 보안 프로그램을 설치·운영하여야 하며, 다음 각 호의 사항을 준수하여야 한다. 1. 보안 프로그램의 자동 업데이트 기능을 사용하거나, 또는 일 1회 이상 업데이트를 실시하여 최신의 상태로 유지 2. 악성프로그램 관련 경보가 발령된 경우 또는 **사용 중인 응용 프로그램이나 운영체제 소프트웨어의 제작업체에서 보안 업데이트 공지가 있는 경우, 즉시 이에 따른 업데이트를 실시**
전자금융 안전성 제고를 위한 금융전산 보안 강화 종합대책 (금융위원회)	내부 업무용 시스템 인터넷 접속 차단 • **내부망에 설치된 패치 관리, 그룹웨어 등 내부 업무용 시스템은 원칙적으로 외부 인터넷 접속을 차단** - 업데이트용 패치 파일 등 외부에서 파일 전송이 필요한 경우, 관리자가 수동으로 다운로드하고 무결성 검증 및 확인 후 적용
요양기관 개인정보보호 자율점검 (행정자치부, 건강보험심사평가원)	< 제29조 안전조치의무> • 개인정보처리시스템에 백신 프로그램 등 최신의 보안 프로그램을 설치하여 관리 • **보안 프로그램을 정기적(일 1회 이상)으로 업데이트**

02
AhnLab EPP Patch Management

AhnLab EPP Patch Management 개요

특장점

주요기능

패치지원 SW 상세 현황

도입효과

AhnLab

AhnLab EPP Patch Management

AhnLab EPP Patch Management는 차세대 엔드포인트 보안 플랫폼 기반의 전문 패치 관리 솔루션입니다.
각종 보안 패치에 대한 실시간 관리뿐만 아니라 보안 정책을 위반한 엔드포인트 시스템에 대한 중앙 관리 및 조치 등 탁월한 관리 편의성과 함께 안랩의 자체 패치랩을 통한 차별적인 패치 안전성을 제공합니다.

플랫폼 기반의 혁신적인 패치 관리

AhnLab EPP Patch Management

패치랩

안랩의 자체 패치랩 및
전담 인력을 통한 패치 안전성 강화

통합 관리 편의성

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

무결성 검증

무결성 검증 등을 통해
폐쇄망 환경의 패치 관리 지원

국정원 권고 패치 지원

한글, Adobe 등 국정원 권고 자동 패치 지원
(*AhnLab EPP Patch Management만 가능)

네트워크 대역폭 설정

패치 적용 시 사용할 네트워크 대역폭 설정을 통한
운영 안정성 및 비즈니스 연속성 확보

시스템 하드닝

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

특장점 (1/3) – 패치 관리의 안정성 및 효율성

AhnLab EPP Patch Management는 차별적인 패치 안전성은 물론, 다양한 패치 지원 범위 및 관리 옵션을 제공해 효율적인 패치 관리를 통한 비즈니스 연속성 및 생산성 향상에 기여합니다.

패치 관리의 안정성·효율성 | 소프트웨어 관리 편의성 | 구축·운영 편의성 및 보안 강화

믿을 수 있는 **패치 안전성**

- 안랩의 자체 패치랩을 통해 사전 검증·분석한 안전한 패치 제공
- 패치 검증 프로세스 수행 : 위험도별 패치 및 오류 보고 패치 자동 분류
- 패치 파일의 다운로드 대역폭 제한 설정을 통한 패치 관리 안정성 확보(QoS 보장)
- 폐쇄망 환경 지원을 위한 패치 무결성 검증 및 오프라인 패치 제공

폭넓은 패치 **지원 범위**

- 운영체제(OS) 및 10여종의 소프트웨어 패치 지원
- 지원 종료된 MS의 운영체제(Windows XP 등) 관련 미적용된 패치 지원
- 국정원 취약점 권고 패치 지원(Adobe, 한글 등)

다양한 **관리 옵션**

- 자동화된 패치 관리를 통한 운영 효율성
- 다양한 기업 환경을 위한 유연한 패치 정책 설정
- 테스트 그룹 및 예외 그룹 설정 등을 통한 패치 관리 안정성
- 패치 진행 상태에 대한 실시간 모니터링

전문 서비스를 통한 **운영 안정성**

- 안랩의 전문 인력을 통한 지속적이고 안정적인 지원 서비스
- HW, SW, OS, DB에 대한 원스톱 관리 서비스 지원
- 안정적인 패치 관리 및 보안 운영을 통한 비즈니스 연속성 확보

특장점 (2/3) – 소프트웨어 관리 편의성

AhnLab EPP Patch Management는 패치 관리뿐만 아니라 기업의 효율적인 소프트웨어(SW) 관리를 위한 다양한 기능과 유연한 대시보드 기반의 관리 가시성을 제공합니다.

패치 관리의 안정성·효율성 | **소프트웨어 관리 편의성** | 구축·운영 편의성 및 보안 강화

가시성 기반의 패치 및 SW 관리

- 운용 현황을 한눈에 확인할 수 있는 대시보드(Dashboard)
- 기업 및 기관의 환경에 따라 필요한 정보만 편집해서 볼 수 있는 사용자 정의 대시보드 제공
- 가시성 기반의 효율적인 보안 패치 및 SW 관리

최적화된 SW 관리

- 기업 및 기관의 권고 또는 금지 소프트웨어(SW)의 설치 현황 확인 가능(권장 및 금지 SW 설치 현황)
- 권고·차단 SW 등 보안 정책에 위배되는 PC에 대한 인터넷 접근 차단 및 설치 파일 배포
- 설치된 SW 정보 수집 및 프로세스 차단 관리

편리한 **모니터링** 및 다양한 **리포트**

- 웹 기반의 관리 콘솔을 통한 편리한 모니터링 및 관리
- 사용자/에이전트/패치/SW/HW 정보 관련 요약 및 상세 보고서 제공
- 전체/부서별 패치/SW 설치/정책 적용 현황 보고서
- 운영체제/SW별 패치 현황 보고서
- IP 주소별 인터넷 허용/차단 현황 모니터링 및 통계 그래프 산출
- 각종 보고서 작성 및 CSV 파일로 내보내기 지원

특장점 (2/3) – 구축·운영 편의성 및 보안 강화

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

패치 관리의 안정성·효율성 | 소프트웨어 관리 편의성 | **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
- 패치 관리 및 백신, 개인정보, 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
- 유기적인 패치 관리, 취약 시스템 점검 및 조치, 위협 탐지 및 대응 등을 통한 엔드포인트 시스템 하드닝 효과

주요 기능

구분		상세 내용
패치 관리	패치 정보	- 패치 언어: 한국어, 영어, 중국어(간체) - 패치랩을 통한 사전 검증/분석 - 국정원 권고 패치 지원 - 운영체제 등 10여종 이상 SW패치 지원 - MS 단종 제품(Windows XP)에 대한 미적용 패치 지원 - 패치 심각도/ 오류 보고 패치 분류 제공 - KB 번호 기준의 패치 분류 및 검색 지원
	패치 정책	- 전체/부서/노드별 패치 적용 또는 제외 - 패치 테스트 그룹 운영 - 패치 롤백·백그라운드 설치 지원
	패치 옵션	- 패치 파일 크기 및 다운로드 속도 제한 - 패치 다운로드 금지 시간 설정 - 패치 금지 및 허용 시간 설정, 패치 적용 유예 - 시스템 종료 시 패치 적용 설정 - 패치 적용에 따른 시스템 재부팅 필요 시 사용자 알림 설정 - 패치 실패 시 재시도 지원 - 패치 가능 HDD 용량 설정
	보고서	- 패치 현황 보고서 지원 - 패치 적용 상태 상세 정보 및 점검 기능 - 사용자 정의 보고서 - 각종 보고서 Export(CVS)
	기타	- 인사DB 연동, NAT환경 지원, 사용자 공지 알림 - 대용량 패치 파일 분할 업로드 및 다운로드 제공 - 복수 관리자 지원
소프트웨어 관리	SW 배포	- 콘솔(Console)을 통한 SW 등록·배포 - 백그라운드 자동 설치 지원
	SW 정책	- 금지 및 권고 SW 등록, 설치 현황 정보 제공 - 권고 SW 강제 설치, 금지 SW 삭제 알림 및 유도 - 설치된 SW 정보 수집 및 프로세스 차단 관리
	보고서	- 전체 및 부서별 SW 설치 현황 및 정책 적용 보고서 / 사용자 정의 보고서 / 각종 보고서 Export(CVS)
	기타	- CPU, 메모리 등 하드웨어(HW) 정보 수집

OS/SW별 상세 패치 지원 현황

구분		상세 버전
운영체제(OS)	Windows Desktop	- Windows XP SP3 / Vista / 7 / 8(8.1) / 10/ 10 IoT Enterprise * 상기 OS의 x86/x64 호환 모드 지원
	Windows Server	- Windows Server 2008 (x86/x64) / 2008 R2 (x64) - Windows Server 2012 (x64) / 2012 R2 (x64) - Windows Server 2016 (x64) - Windows Server 2019 (x64)
애플리케이션 (Application)	Web browser	- Internet Explorer 7 / 8 / 9 / 10 / 11 - Chrome - Firefox
	MS Office	- MS Office 2003 / 2007 / 2010 / 2013 / 2016 - 2007 Microsoft Office Suite - Microsoft Office Compatibility Pack - Microsoft Office Proofing Tools Kit 2007 / 2010 - MS Excel Viewer 2003 / 2007 - MS Word Viewer 2003 - MS Power Point Viewer 2003 / 2007 / 2010 - MS Visio Viewer 2007 / 2010
	Adobe Flash Player	- Adobe Flash Player - ActiveX - Adobe Flash Player - Chromium PPAPI
	Adobe ShockWave Player	- Adobe ShockWave Player
	Adobe Reader	- Adobe Reader 9 / 10 / 11 / DC
	Adobe AIR	- Adobe AIR
	JAVA	- JAVA SE Runtime Environment 7/ 8/ 9
	.NET Framework	- .NET Framework 4.5 / 4.6 / 4.7
	한컴오피스	- 한글과컴퓨터 한/글 2007 - 한글과컴퓨터 오피스 2007 - 한컴오피스 한/글 2010 SE+ / 2014 VP / NEO - 한컴오피스 2010 SE+/ 2014 VP /NEO /2018

도입 효과

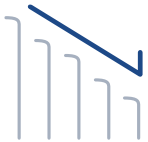
보안 담당자를 위한 최고의 패치 관리 솔루션 AhnLab EPP Patch Management는 기업 및 기관의 실효성 있는 패치 관리는 물론, 시스템 하드닝을 통한 안전한 비즈니스 환경 구축에 기여합니다.

AhnLab EPP Patch Management

패치 관리를 넘어 시스템 하드닝(System Hardening)까지!

더욱 안전한 엔드포인트 환경

- 능동적인 패치 관리를 통해 악성코드 및 지능형 위협 등에 대한 노출 최소화
- 최신 보안 패치의 실시간 적용을 통한 안전한 엔드포인트 환경 확보
- 전사 엔드포인트 시스템에 대한 일관된 보안 정책 적용 및 보안 관리
- AhnLab EPP 기반의 유기적인 보안 솔루션 연계를 통한 시스템 하드닝 및 보안 강화



TCO 절감 효과

- 라이선스 적용 및 병렬 구조(Scale-out) 기반의 간편한 설치 및 확장을 통한 구축 비용 최소화
- SW 관리를 통한 자산 사용률 극대화 및 불법 SW 사용 방지를 통한 비용 절감 효과
- 보안 패치 미비로 인한 보안 사고 방지 및 그에 따른 비용 손실 최소화

관리 효율성 및 생산성 재고

- AhnLab EPP 기반의 패치 및 보안 솔루션 통합 관리를 통한 보안 운영 부담 해소
- 지속적인 전문 지원 서비스를 통한 안정적인 보안 운영
- 안정적인 패치 관리 및 보안 운영을 통한 비즈니스 연속성 확보

03
도입 방식

솔루션 구축 개념도

AhnLab EPP 기반의 구축 및 운영

유연한 서버 구성을 통한 확장

운영 환경

솔루션 구축 개념도

AhnLab EPP Patch Management는 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 Patch Management는 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

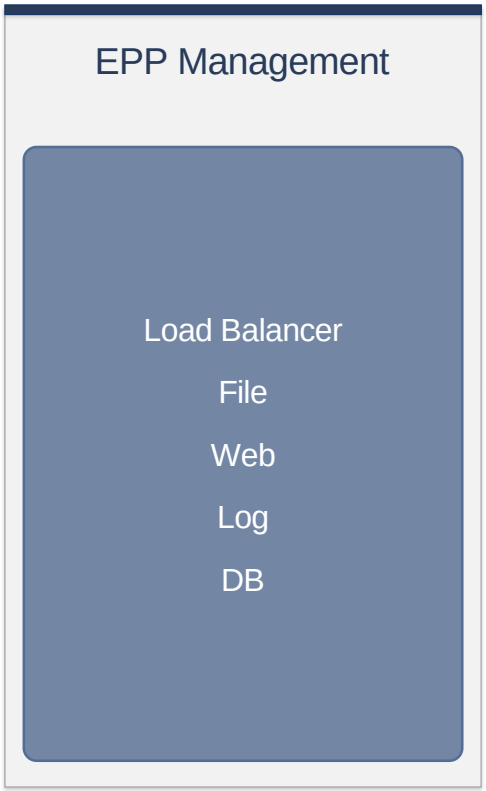
  * EDR 모듈은 EDR 사용 시에만 필요

유연한 서버 구성을 통한 확장

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

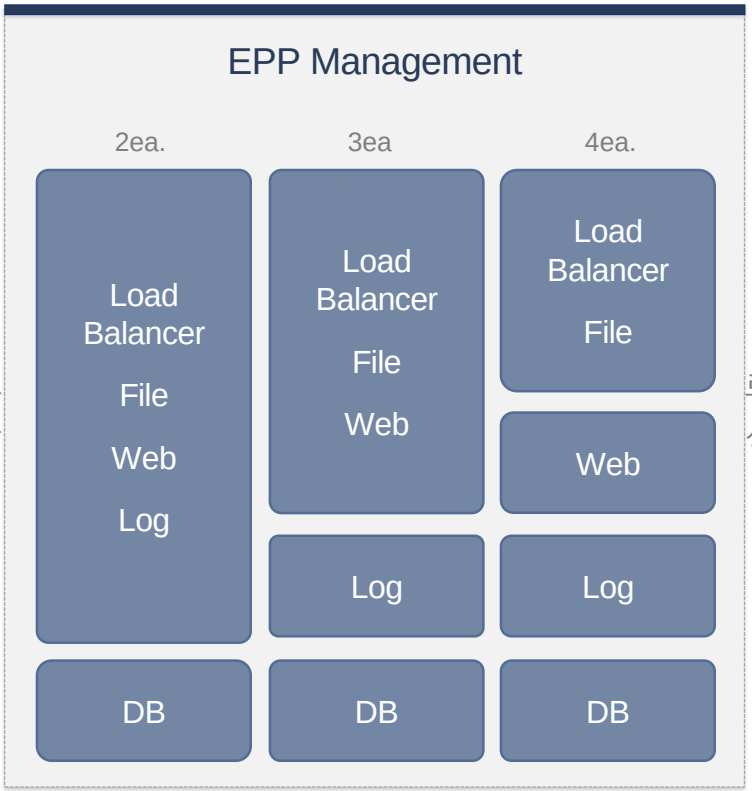
- 최적화된 초기 구축 비용 및 확장 편의성: 사용자 수, 데이터베이스 사용량 등 고객 환경에 따른 시스템 구성
- 에이전트 확대, DB 증가에 따라 모듈별 서버 확장 가능
- Load Balancer / File 서버의 경우 네트워크 별로 확장 구성 가능

구성 1. **올인원** (단일 장비)



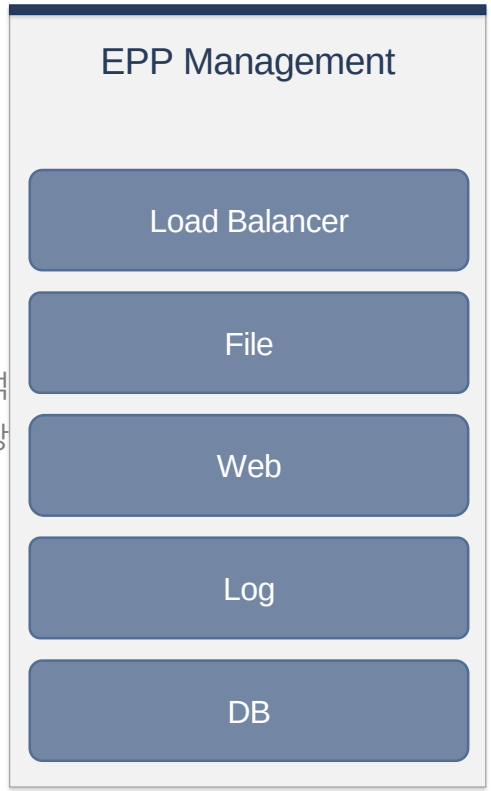
관리·로그
성능 향상

구성 2. **분리형** (개별 장비)



로그·분석
성능 향상

구성 3. **전체 독립형** (개별 장비)



운영 환경

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

- AhnLab EPP Patch Management 에이전트 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
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

※ 원활한 패치 적용을 위해 에이전트와 서버 간의 네트워크 대역폭(Bandwidth)은 최소 32mbps 이상을 권장합니다.

- 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

※ AhnLab EPP Patch Management 사용을 위해 HDD 2개 이상 물리적 분리 구성이 필수입니다.

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 Patch Management

AhnLab