More security,
More freedom

AhnLab Patch Management

패치 관리 솔루션의 새로운 기준

표준제안서

AhnLab

CONTENTS

AhnLab

01
제안 배경

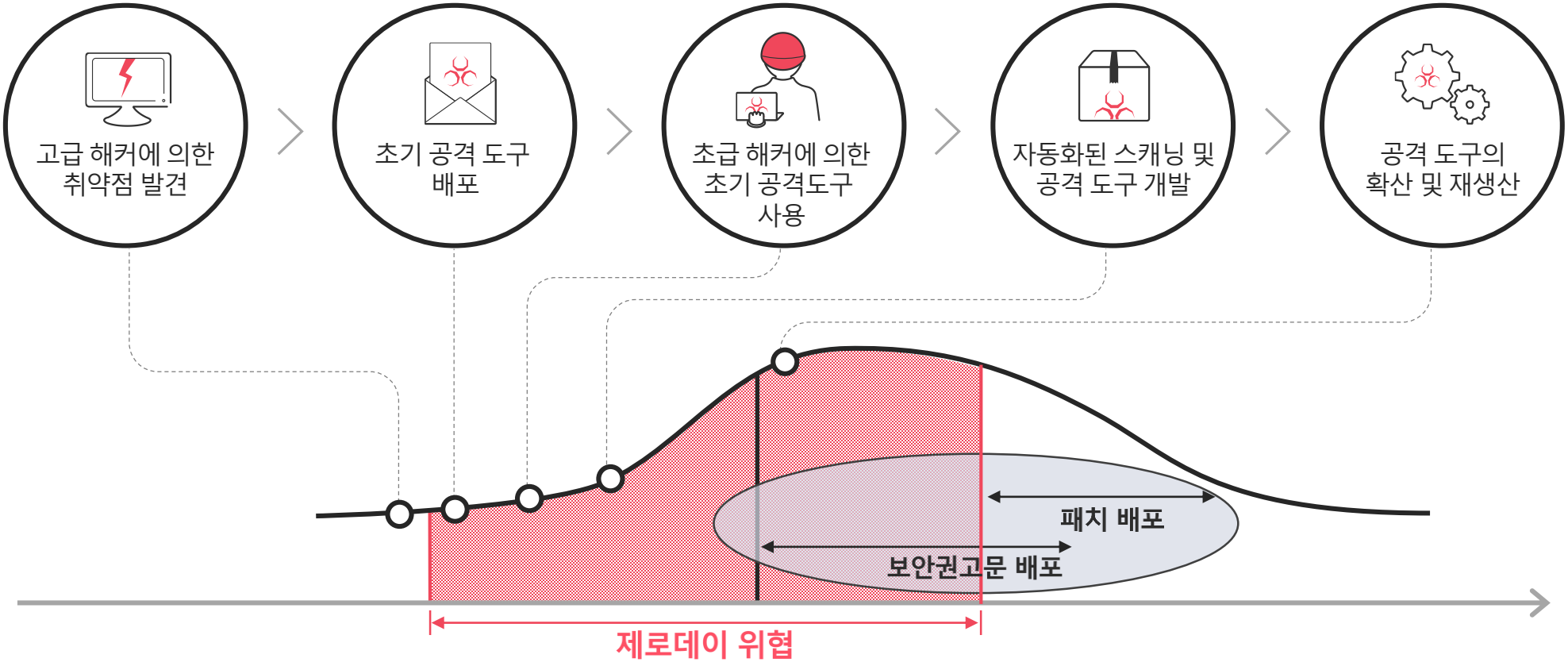
1. 취약점 기반 공격의 다변화 및 고도화
2. 알려진 취약점 기반 공격 증가
3. 패치 관리 미비에 따른 공격 표면 확대
4. 패치 관리 관련 컴플라이언스 강화

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



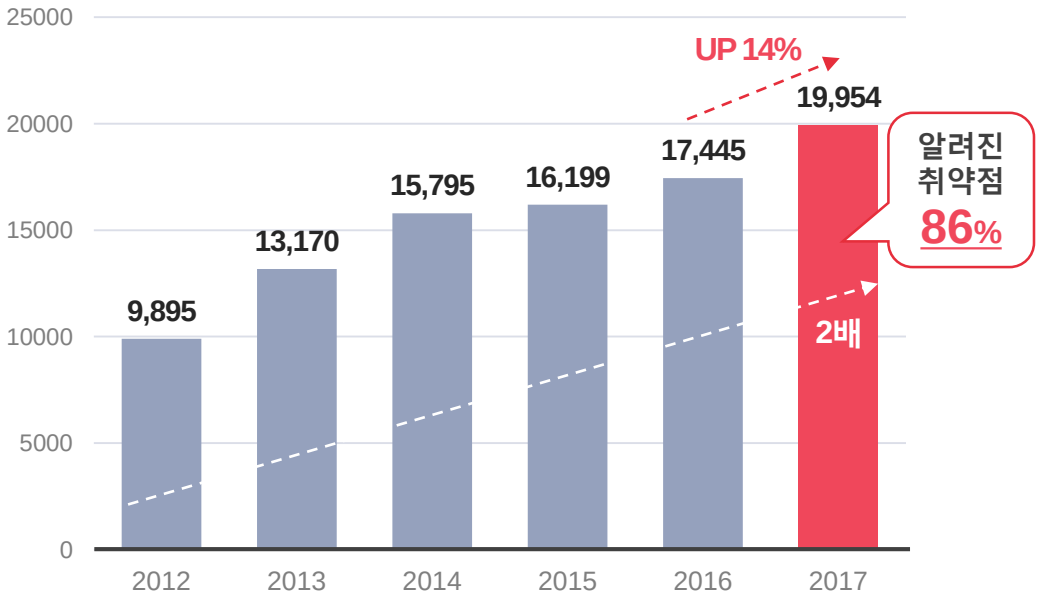
© AhnLab, Inc. All rights reserved.

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.

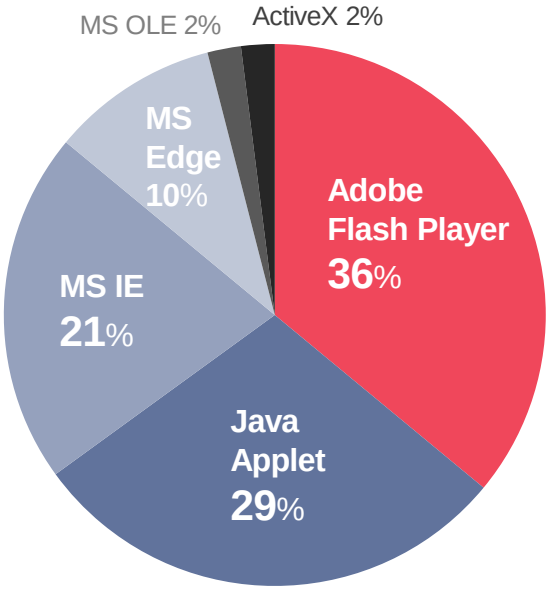
- 2017년 취약점 기반 공격 중 86%가 이미 패치가 배포된 알려진 취약점 활용
- 케르베르 랜섬웨어, 워너크라이 랜섬웨어, 드라이덱스 등 다수의 알려진 취약점 활용한 악성코드 증가
- 어도비의 플래시 개발 중단에 따라 마이크로소프트(MS)의 SW 취약점 악용 증가 추세

글로벌 취약점 보고 현황 (2012-2017)



*출처: Flexera, Vulnerability Review 2018

2018 상반기 국내 SW 취약점 악용 현황



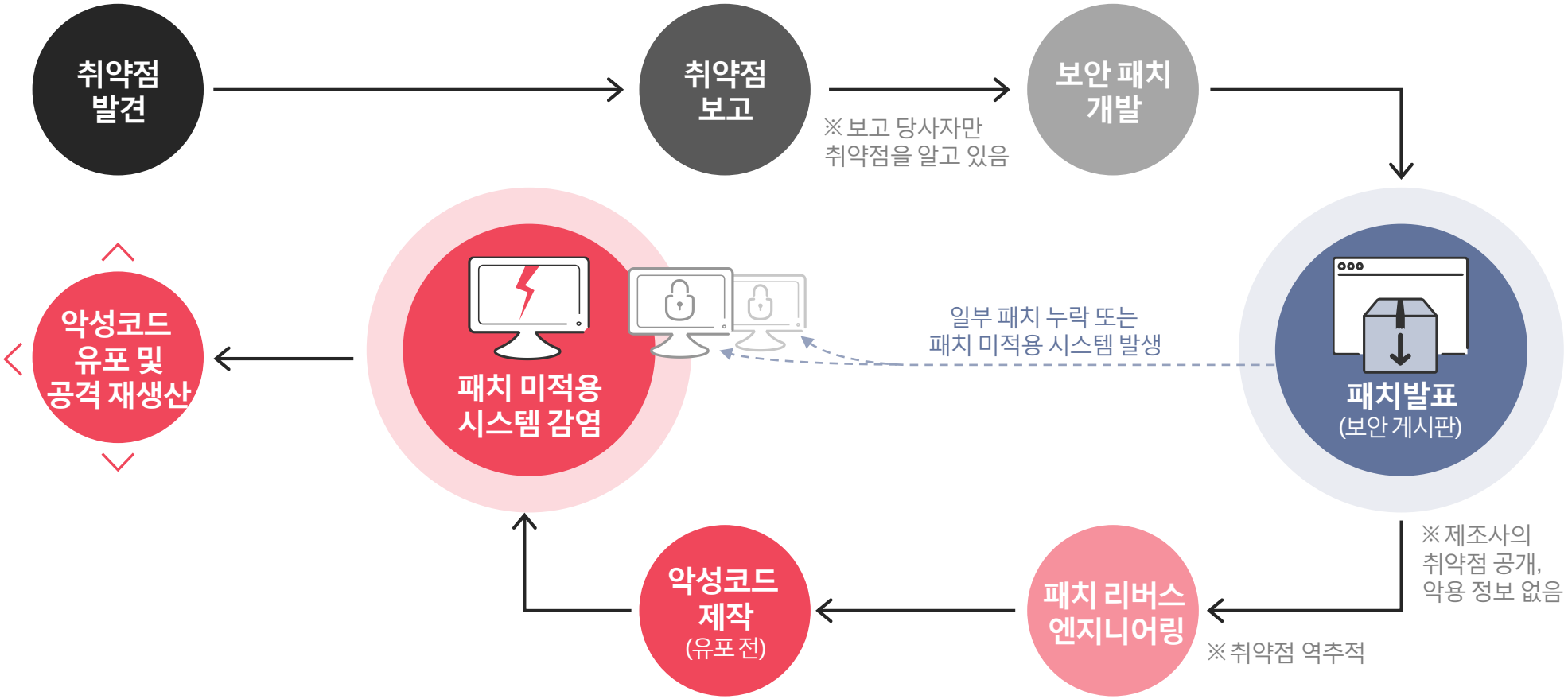
*출처: 한국인터넷진흥원(KISA)

© AhnLab, Inc. All rights reserved.

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 인한 보안 취약점의 누적으로 기업 및 기관의 위협 노출 범위(attack surface)가 확대되고 있습니다.

보안 취약점 이용한 공격 발생 과정



© AhnLab, Inc. All rights reserved.

패치 관리 관련 컴플라이언스 강화

개인정보보호법을 비롯한 다수의 정보 보호 관련 규제가 고도화된 패치 관리를 요구하고 있습니다.
패치 관리와 관련된 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**

© AhnLab, Inc. All rights reserved.

02
AhnLab Patch Management

1. 제품 소개
2. 특장점
3. 주요 기능
4. 도입 효과
5. 구성 방식
6. 운영 환경
7. OS/SW별 상세 패치 지원 현황

AhnLab

AhnLab Patch Management

AhnLab Patch Management는 기업 내 PC의 각종 보안 패치에 대한 실시간 중앙 관리 뿐만 아니라 기업 보안 정책에 위배되는 PC에 대한 정책을 관리할 수 있는 패치 관리 솔루션입니다. 기업 및 기관에서 사용하는 다양한 범위의 패치를 지원하는 것은 물론, 자체 패치랩 기반을 통한 차별적인 패치 안전성과 탁월한 관리 편의성을 제공합니다.

패치 관리 솔루션의 새로운 기준

AhnLab Patch Management

- 패치랩
- 무결성 검증
- 통합 관리 편의성
- 국정원 권고 패치 지원
- 네트워크 대역폭 설정

- ✓ **CC인증 획득**으로 검증된 **강력한 보안성**
- ✓ 안랩의 자체 **패치랩** 및 전담 인력을 통한 **패치 안전성 강화**
- ✓ 엔드포인트 관리 시스템 AhnLab EMS를 통한 **1서버 - 1관리 콘솔 – 1 에이전트 통합 관리 가능**
- ✓ 한글, Adobe 등 **국정원 권고 자동 패치 지원** (*AhnLab Patch Management만 가능)
- ✓ 무결성 검증 등을 통해 **폐쇄망 환경의 패치 관리 지원**
- ✓ **패치 적용 시 사용할 네트워크 대역폭 설정 가능**

© AhnLab, Inc. All rights reserved.

특장점

핵심 경쟁력	특장점
패치 관리의 안정성 • **검증된 패치 제공** • **다양한 패치 관리 옵션**	• 안랩 패치랩 검증을 통한 오류 및 문제 발생 가능성 제거 • 각 그룹 환경에 대한 자동 패치 설치 가능 • MS 지원 종료 OS(Windows XP)의 미적용된 패치 및 국정원 취약점 권고 패치 지원 • 폐쇄망 환경 지원을 위한 패치 무결성 검증 및 오프라인 패치 제공 • 백그라운드 설치, 테스트 그룹, 롤백, 재부팅 관리, 네트워크 대역폭 설정 등 다양한 옵션
SW 관리의 가시성 • **HW/SW 현황 관리** • **권고 및 금지 SW 관리** • **현황별 상세 보고서 제공**	• PC별 SW 정보와 SW 설치 PC에 대한 정보 제공 • Client 및 권장 SW에 대한 자동 배포 및 사용자 공지 • 금지 SW 사용에 대한 설치 제어 및 삭제 유도 지원 • 사용자/에이전트/패치/SW/HW 정보 등에 대한 요약 및 상세 보고서 제공 • 패치 진행 상태에 대한 실시간 모니터링
구축, 관리의 편의성 • **시스템 구축 및 관리 편의성** • **보안 관리 편의성**	• 라이선스 추가만으로 솔루션 구축 완료 • 네트워크 환경에 따라 다양한 구조로 적용 가능 • HW, SW, OS, DB에 대한 원스톱 관리 서비스 지원

AhnLab © AhnLab, Inc. All rights reserved.

주요 기능

AhnLab Patch Management는 보안 패치 및 소프트웨어 관리 등 다양한 기능과 편리한 리포트를 제공해 효율적인 보안 관리에 기여합니다.

패치 관리

- 별도의 패치 검증 프로세스 수행 및 오류 보고 패치 별도 관리 지원
- 지원 중단된 Windows XP의 미적용 된 패치 지원
- 국가사이버안전센터 권고 패치 지원 (Adobe, 한글 등)
- 각 PC의 패치 환경에 적합한 패치 등급 선별 후 백그라운드 설치 통해, 관리자 개입 없이 자동 설치
- 기업 환경에 따라 패치 정책 편집 기능(패치 적용 시간, 패치 주기, 패치 적용 대상, 롤백 등)
- 테스트 그룹 및 예외 그룹 설정을 통한 패치 관리 안정성 및 신뢰성 확보

SW 설치/관리

- 권고·차단 SW 등 기업 보안 정책에 위배되는 PC에 대한 정책 관리
- 패치 상태, HW 정보, SW 설치 정보, 패치 대상 SW 정보 등 각 PC별 시스템 상세 정보 조회
- 그룹 정보 / IP 대역별 설치 배포 가능

리포팅 & 모니터링

- 운용 현황을 한눈에 확인할 수 있는 대시보드(Dashboard) 제공
- 사용자 / 클라이언트 시스템/ 패치 / 소프트웨어/ 하드웨어 정보 등에 대한 요약 및 상세 보고서 제공
- 관리 항목에 대한 실시간 현황 보고서 제공으로 변경 내역 및 관리 대상에 대한 편리한 확인 가능
- 패치 진행 상태에 대한 실시간 모니터링
- IP 주소별 네트워크 허용·차단 현황 모니터링 및 통계 그래프 산출

© AhnLab, Inc. All rights reserved.

도입 효과

AhnLab Patch Management는 기업 및 기관의 전체 PC에 대한 실시간 중앙 패치 관리 및 소프트웨어 관리를 통해 기업의 안전한 보안 환경 구축은 물론, 관리 비용 절감 및 업무 효율성 향상에 기여합니다.

AhnLab Patch Management

기업 보안 관리자를 위한 최고의 패치 및 SW관리 솔루션

안전한 엔드포인트 환경 구축

- 취약점을 이용한 악성코드 및 지능형 위협 등에 대한 능동적 대응
- 보안 패치 실시간 적용으로 안전한 업무 환경 확보
- 전체 PC에 대해 기업의 일관된 보안 정책 적용을 통한 보안성 강화

TCO 절감

- AhnLab EMS 기반의 설치 및 운용, 통합 관리를 통해 패치 관리 시스템(PMS) 사용에 따른 구축/운영 비용 최소화
- 보안 패치 미비로 인한 보안 사고 발생을 사전에 방지해 보안 사고로 인한 기업의 비용 손실 감소

SW 관리 효율성 및 생산성 재고

- 기업에서 도입한 SW 설치를 강제함으로써 제품 설치 및 사용률 증대
- 불법 또는 금지 SW 현황 관리를 통한 비용 손실 방지
- 취약점으로 인한 보안 사고 방지로 비즈니스 연속성 보장

© AhnLab, Inc. All rights reserved.

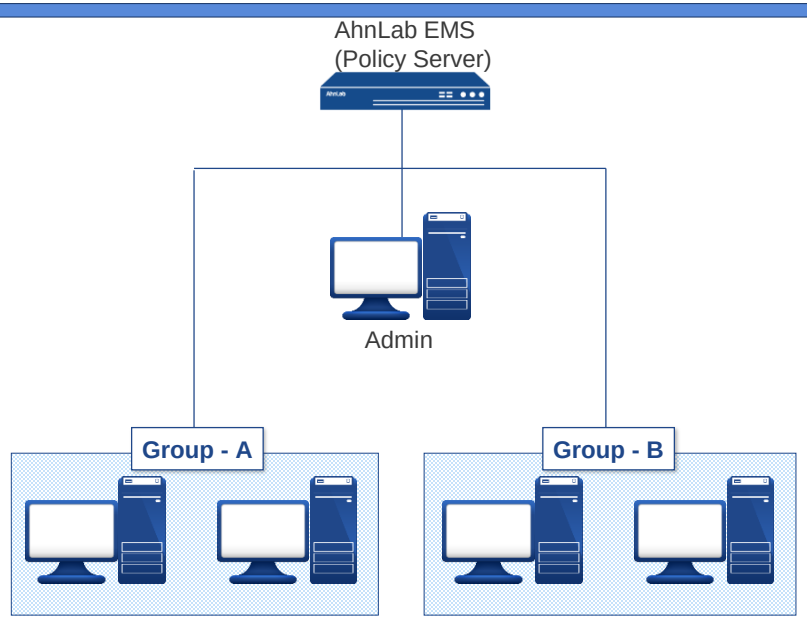
구성 방식

AhnLab Patch Management는 엔드포인트 관리 시스템 AhnLab EMS를 기반으로 기업 및 기관의 환경에 따라 다양한 방식으로 구성할 수 있습니다.

단일 서버 구성

단일 LAN 내에 관리하고자 하는 모든 시스템이 모여있을 경우 구성하는 일반적인 방법

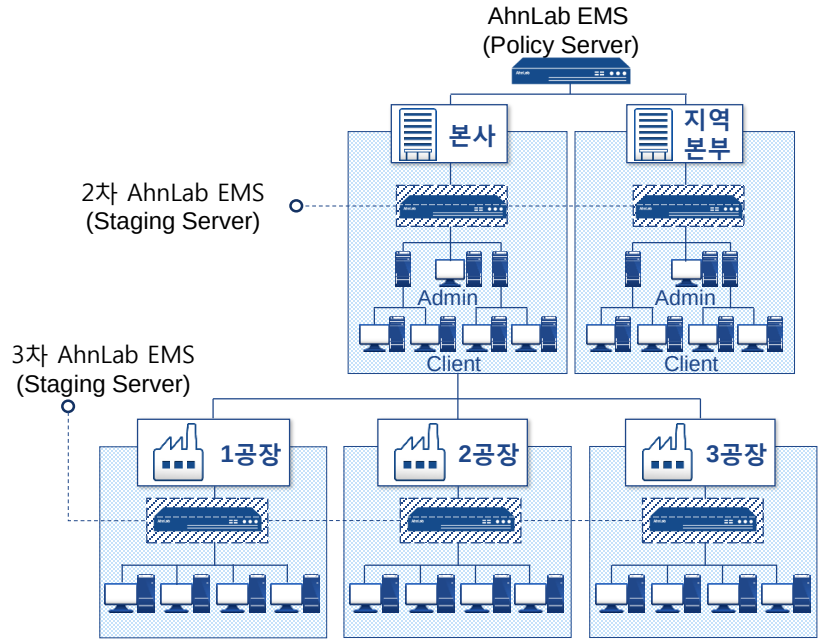
- 1대의 AhnLab EMS가 모든 시스템 관리



다중 서버 구성

관리 조직 및 단위가 계층적으로 분화되어 있고 조직간 연결에 WAN 구간이 있을 경우

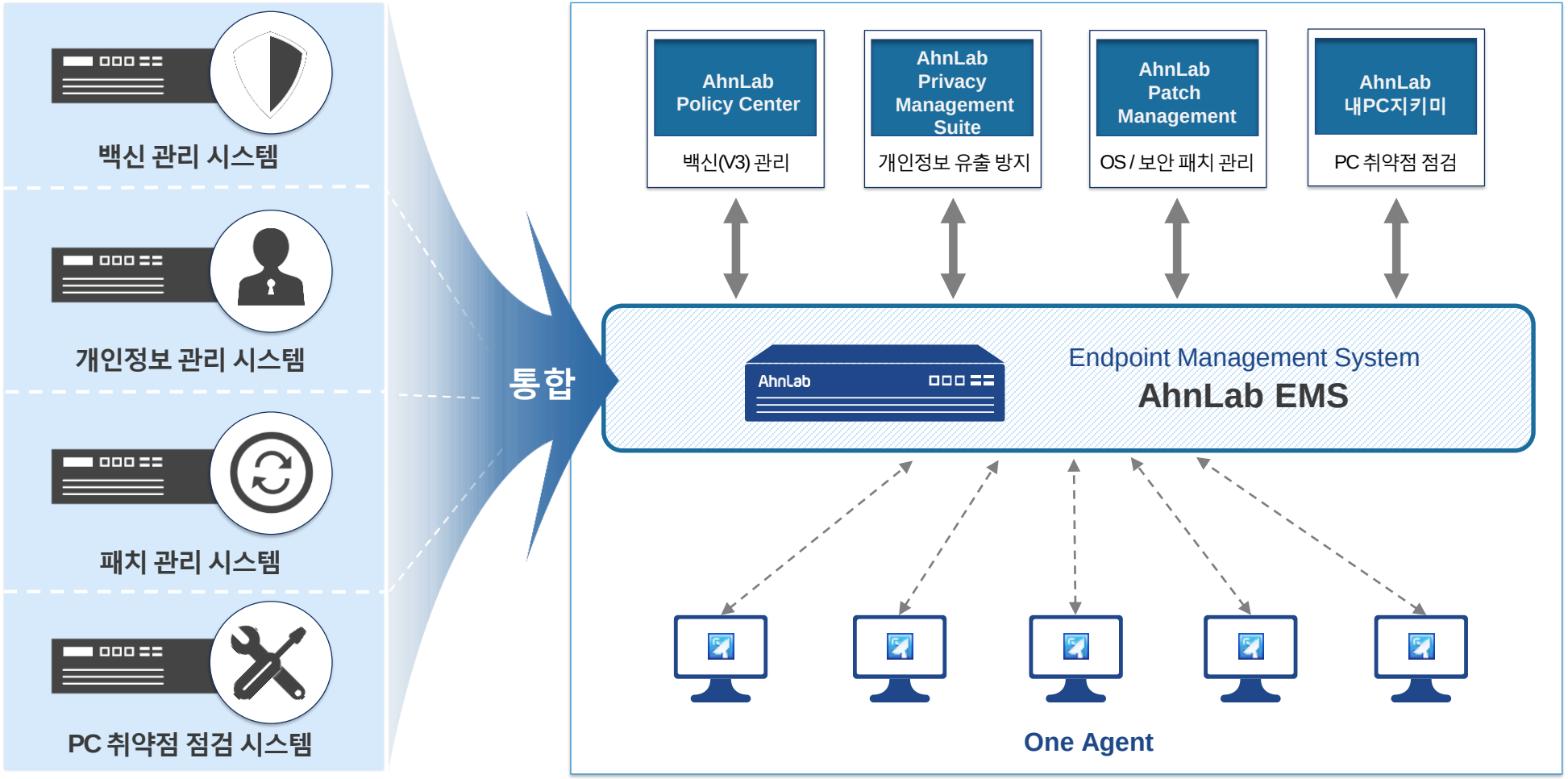
- 1대의 최상위 AhnLab EMS(Policy Server)를 최상위 관리자가 관리
- 다수의 AhnLab EMS(Staging Server)를 단위 조직 관리자가 관리



© AhnLab, Inc. All rights reserved.

운영 환경 (1/2)

AhnLab Patch Management는 AhnLab EMS에 설치 시 더욱 안정적인 운용 및 통합 관리가 가능합니다.
AhnLab EMS(Endpoint Management System)는 안랩의 다양한 엔드포인트 보안 솔루션의 효율적인 설치 및 운영에 최적화된 하드웨어 형태의 엔드포인트 관리 시스템입니다.



© AhnLab, Inc. All rights reserved.

운영 환경 (2/2)

AhnLab Patch Management는 엔드포인트 보안 관리 시스템 AhnLab EMS를 기반으로 편리하게 운영할 수 있습니다.

AhnLab Patch Management Admin / Agent 설치 환경

	Admin	Agent
운영체제	Windows XP Professional / Vista / 7 / 8(8.1) / 10 Windows Server 2003(R2포함) / 2008(R2포함) / 2012(R2포함) Windows Server 2016 * 64비트 호환모드 지원	Windows XP(SP3이상) / Vista / 7 / 8(8.1) / 10 Windows Server 2003(SP1이상, R2포함) / 2008(R2포함) / 2012(R2포함) Windows Server 2016 * 64비트 호환모드 지원

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

AhnLab EMS 제품 사양

구분			AhnLab EMS 2000B	AhnLab EMS 5000BR	AhnLab EMS 10000BR
관리 유저(user) 수			2,000	5,000	10,000
소프트웨어	OS		Linux Cent OS 7.5		
	DB		IBM DB2 WorkGroup Server		
하드웨어	CPU (Intel)		Dual Core	Quad Core	Quad Core
	Memory		DDR4 16GB	DDR4 32GB	DDR4 64GB
	HDD		1TB x 1ea. 7200rpm	1TB x 4ea. 7200rpm	2TB x 4ea. 7200rpm
	HDD Bay		1ea.	4ea.	8ea.
	RAID Controller		N/A (미지원)	지원	지원
	NIC	기본 (Default)	10/100/1000 Ethernet 2Ports (Copper)		
		Dual-Ports 1GB Copper	Optional (NIC 최대 1개 추가 가능)	N/A (미지원)	Optional (NIC 최대 1개 추가 가능)
		Dual-Ports 1GB SFP			
		Dual-Port 10GB SFP			

* BR : Raid Controller가 적용되어 있는 라인업(Raid type 1+0)

AhnLab © AhnLab, Inc. All rights reserved.

OS/SW별 상세 패치 지원 현황

구분		상세 버전
운영체제(OS)	Windows Desktop	- Windows XP SP3 / Vista / 7 / 8(8.1) / 10 * 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)
애플리케이션 (Application)	Internet Explorer	- Internet Explorer 7 / 8 / 9 / 10 / 11
	Chrome	- Chrome
	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

© AhnLab, Inc. All rights reserved.

※ 별첨

주요 UI

모니터링 센터

대시보드 – 그룹·에이전트별 상세 모니터링

1 설치·미설치 패치 현황 정보 제공

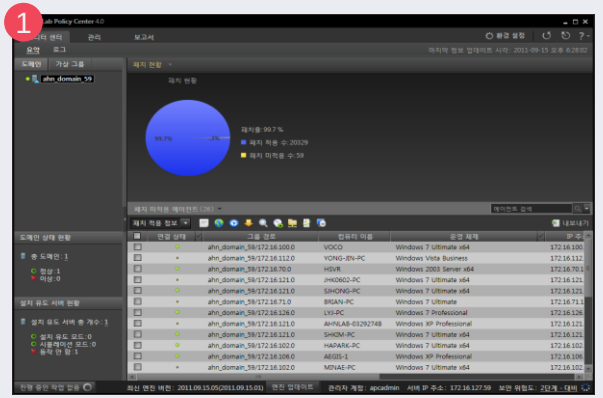
2 권장·금지 SW에 대한 정책 위반·적용 상태 확인

© AhnLab, Inc. All rights reserved.

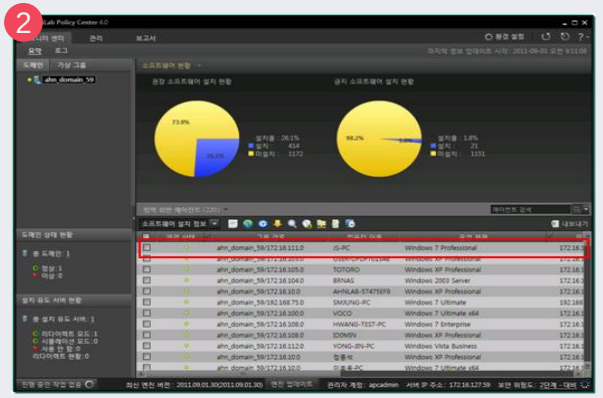
모니터링 센터

대시보드 – 그룹·에이전트별 상세 모니터링

※ 그룹 및 에이전트 별 상세 정보 제공



< 패치 현황 >

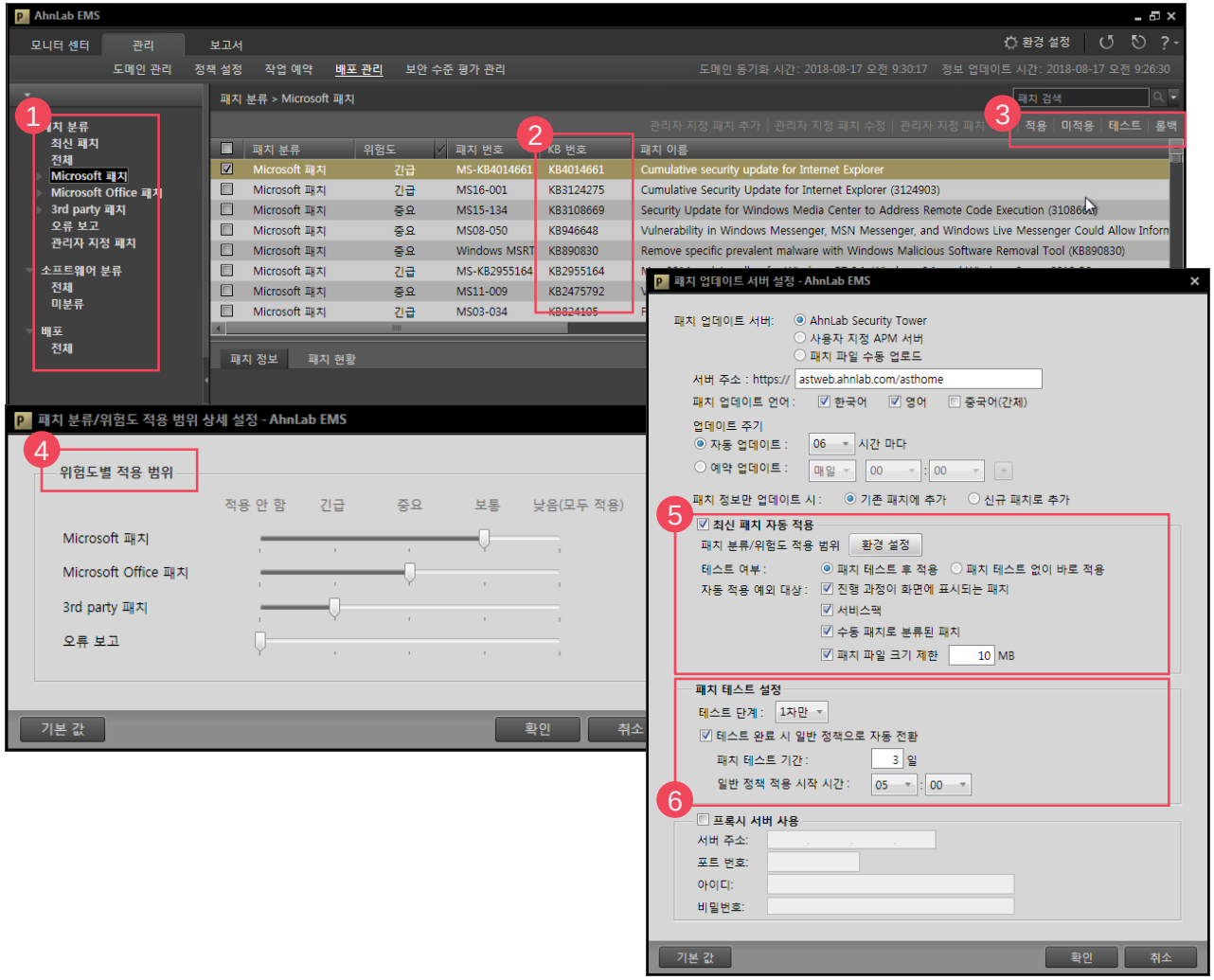


< 소프트웨어 현황 >

© AhnLab, Inc. All rights reserved.

패치 관리 및 정책 적용

패치 관리 – 정책 적용

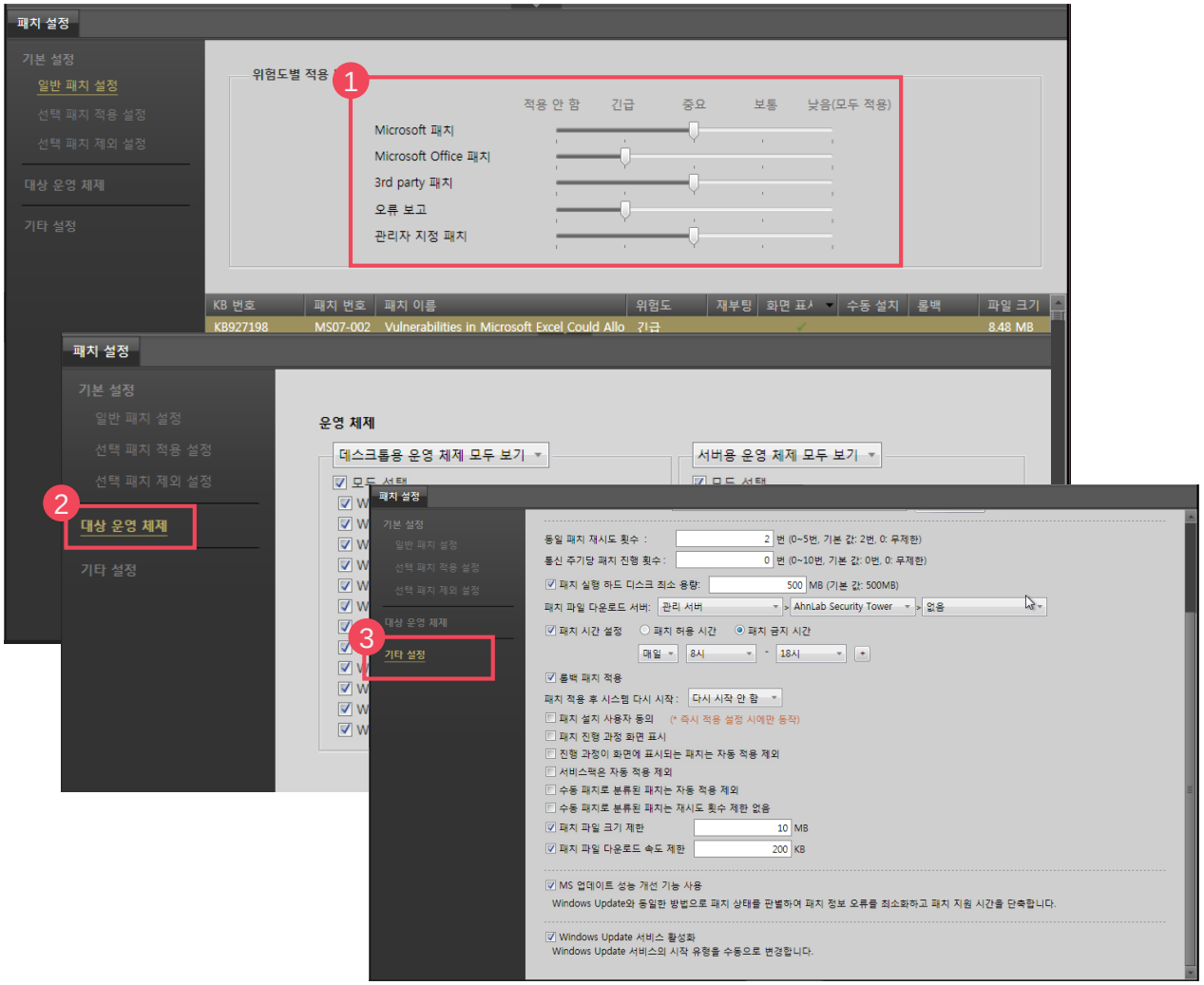


1. MS 제품 및 국정원 취약점 권고 패치 지원
   패치 분류별 카테고리 제공
2. KB번호별 패치 관리
3. 적용, 미적용, 테스트, 롤백 기능 제공
4. 등급별 패치 정책 설정 지원
5. 신규 패치에 대한 업데이트 서버 설정 및
   상세한 자동 패치 적용 옵션 설정 제공
6. 테스트 그룹을 이용한 안정성 검증 지원

© AhnLab, Inc. All rights reserved.

패치 관리 및 정책 적용

패치 관리 – 정책 적용



1. 위험도별 적용범위 설정
   그룹 정보 및 재부팅, 수동 설치,
   화면 표시 등에 대한 상세 패치 정보 제공

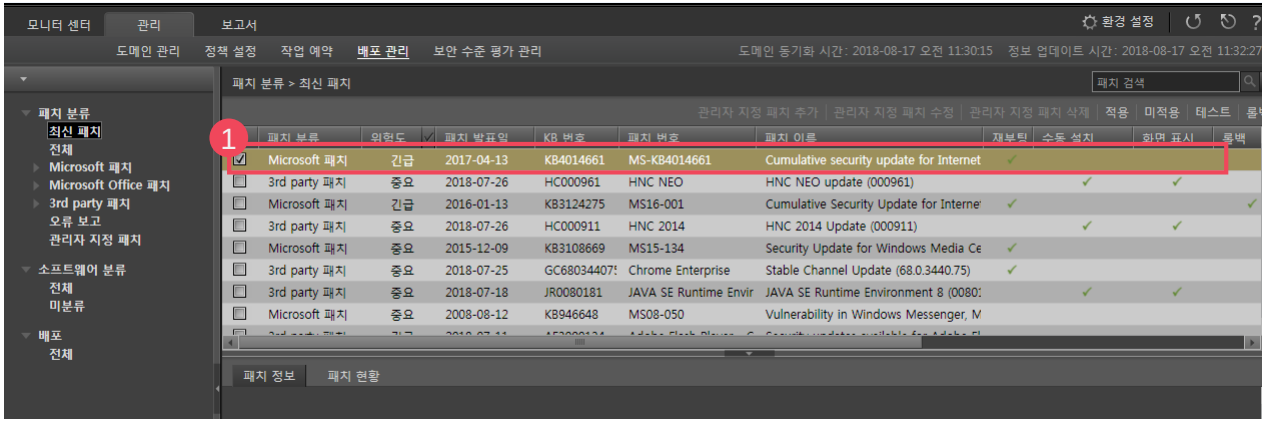
2. 대상 운영체제 별 선택
   → Windows XP 이상 미적용 패치 제공

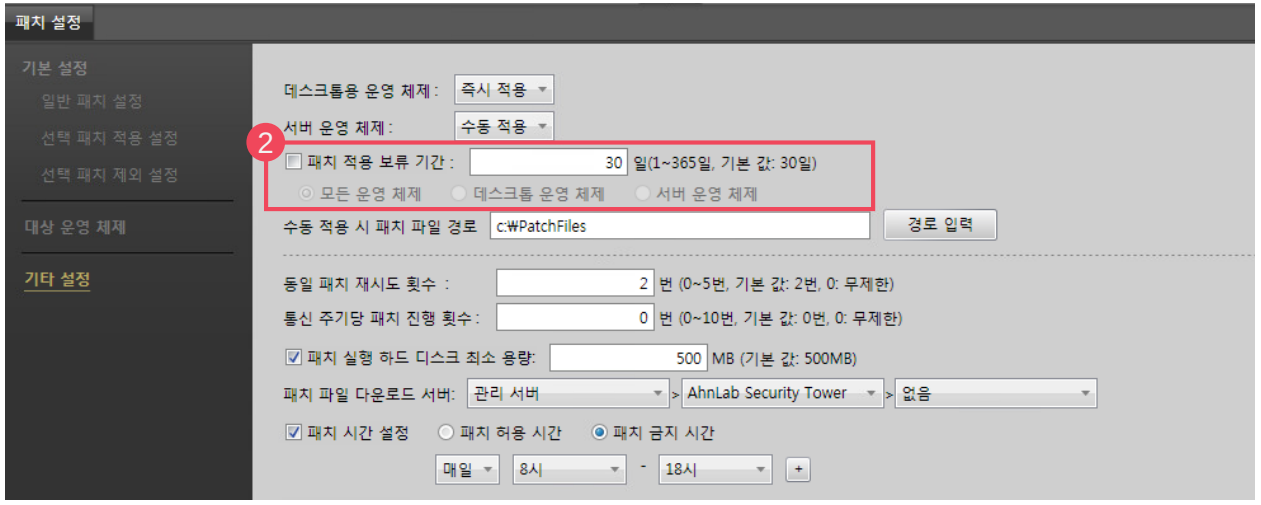
3. 각 그룹에 적용할 패치 정책 설정
   → 재시도 횟수, 주기당 패치 수, 디스크 용량,
   패치 금지 시간, 패치 롤백, 동의창 설정,
   UI 표시 여부 등

© AhnLab, Inc. All rights reserved.

패치 관리 및 정책 적용

패치 관리 – 패치 적용 유예 기능





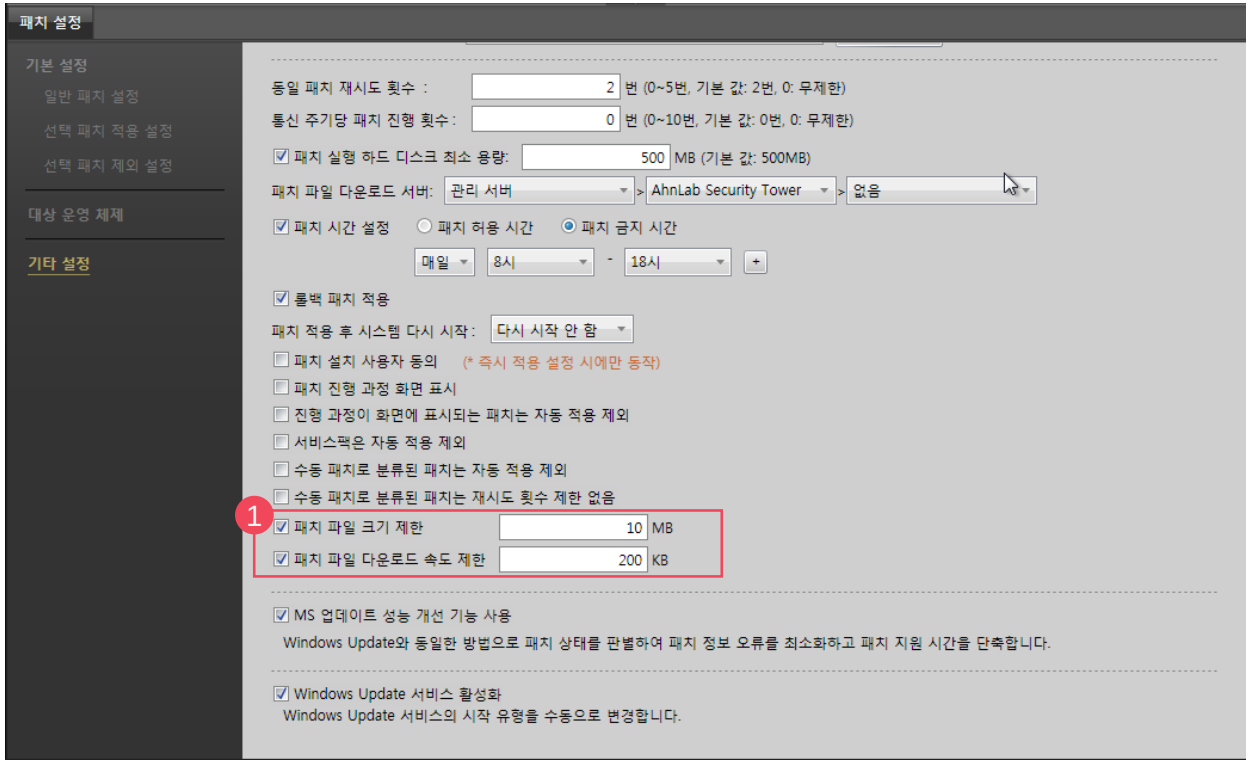
1. 권고 상태의 패치들에 대해 패치 발표일 기준 특정 기간 이후의 패치들에 대해서만 적용 (패치 발표 이후, 안정성이 확인 된 패치에 대해서만 적용)

2. 유예된 패치들은 패치 대상에서 제외되어 관리 (유예 기간이 지난 후 관리 대상으로 적용)

© AhnLab, Inc. All rights reserved.

패치 관리 및 정책 적용

패치 관리 – 패치 다운로드 파일크기 제한 및 속도 제한 설정 기능



1 패치 다운로드 시,
패치파일 크기제한, 다운로드 속도 제한 설정

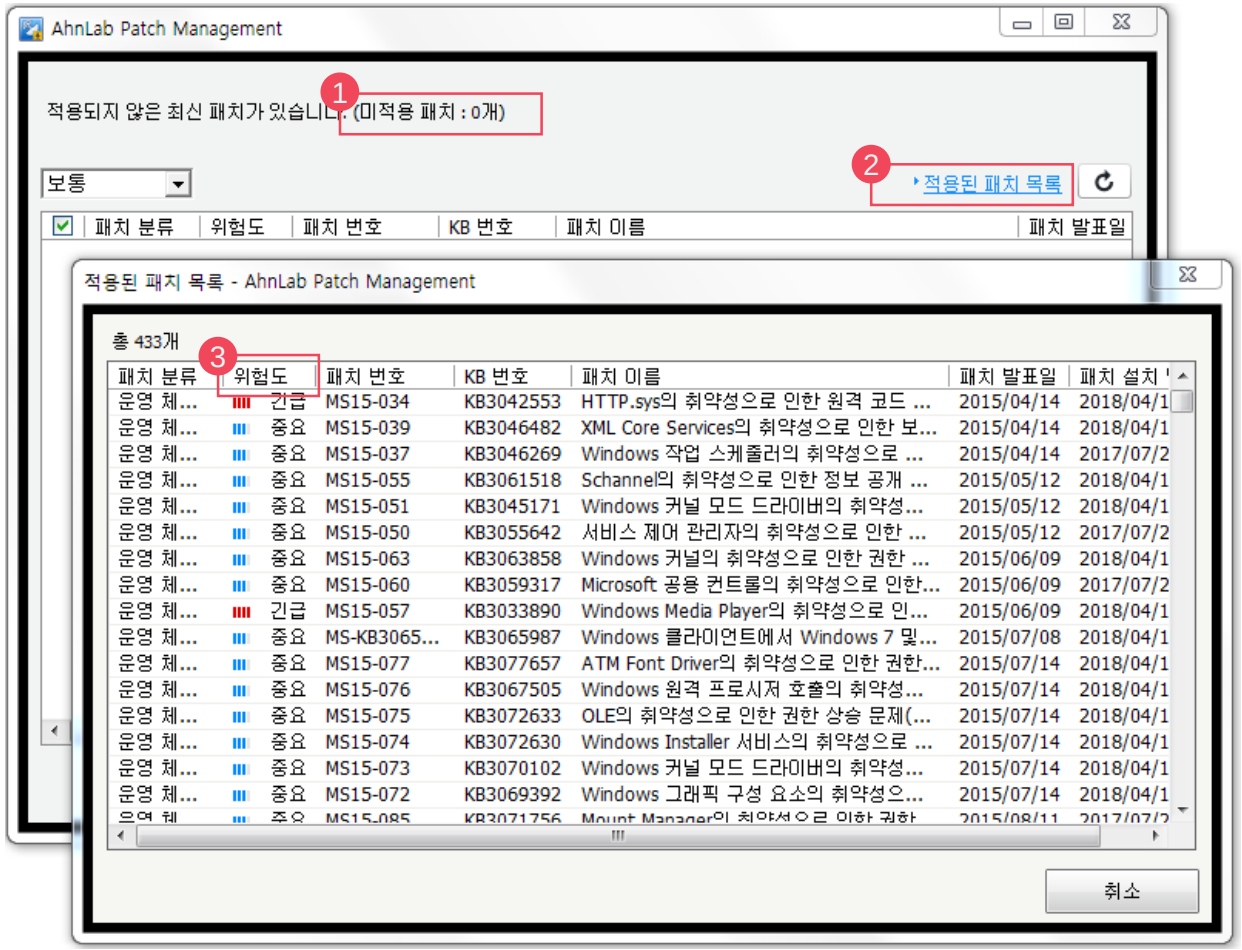
1) 파일크기
- 기본값: 10MB

2) 다운로드 속도제한
- 기본값 : 200 KB/s
- 설정 가능 범위 : 100 ~ 1024 KB/s

© AhnLab, Inc. All rights reserved.

패치 정보 보기 (Agent)

패치 적용/미적용 상태 목록



1 적용 대상 패치 개수 표시

2 적용된 패치 목록 제공

3 위험도 필터 제공

AhnLab © AhnLab, Inc. All rights reserved.

소프트웨어 관리

소프트웨어 등록·관리 – 정책 적용

1. 소프트웨어 분류 기능 제공
2. 소프트웨어 그룹 "추가·수정·삭제" 지원
3. 소프트웨어 설치 현황 정보 제공

© AhnLab, Inc. All rights reserved.

소프트웨어 관리

소프트웨어 등록·관리 – 정책 적용

1. 정책에 반영될 소프트웨어 그룹 설정 지원

2. 권장·금지 소프트웨어 옵션 지원
   * 권장 : 미제어, 알림, 배포
   * 금지 : 미제어, 알림, 인터넷 제어

© 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 Patch Management

AhnLab