

AhnLab Policy Center 4.6 for Windows

More security,
More freedom

한눈에 파악하는 보안 상황판

표준제안서



AhnLab

Contents

AhnLab
Policy Center 4.6 for Windows

01

배경

02

AhnLab Policy Center 4.6 for Windows

03

주요 UI

AhnLab

1. 배경

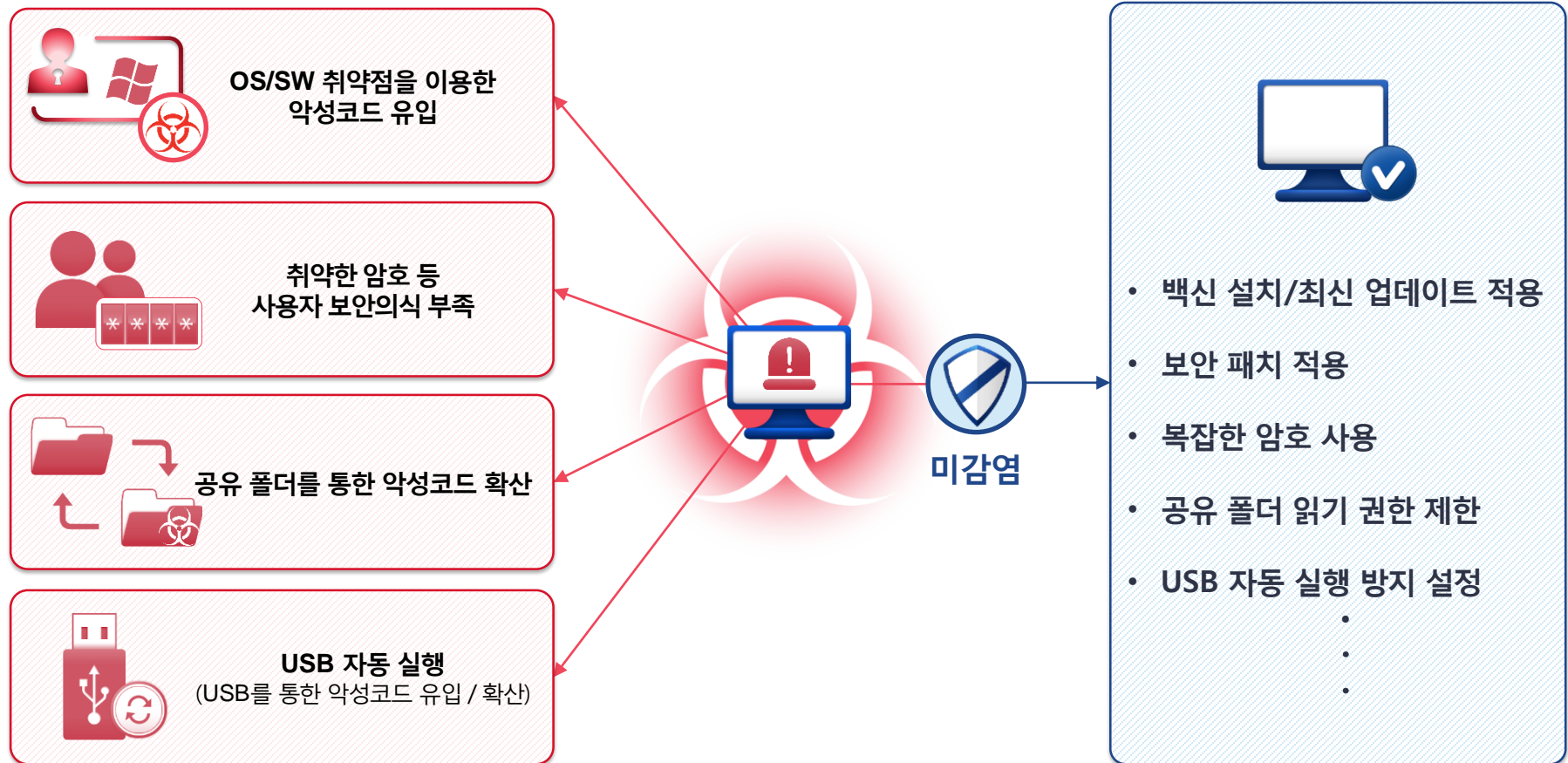
-
1. 엔드포인트를 통한 악성코드 유입 및 확산
 2. 악성코드에 의한 기업 피해 현황

엔드포인트를 통한 악성코드 유입 및 확산

오늘날 악성코드는 기하급수적으로 증가하고 있을 뿐만 아니라 나날이 고도화, 지능화되고 있습니다.

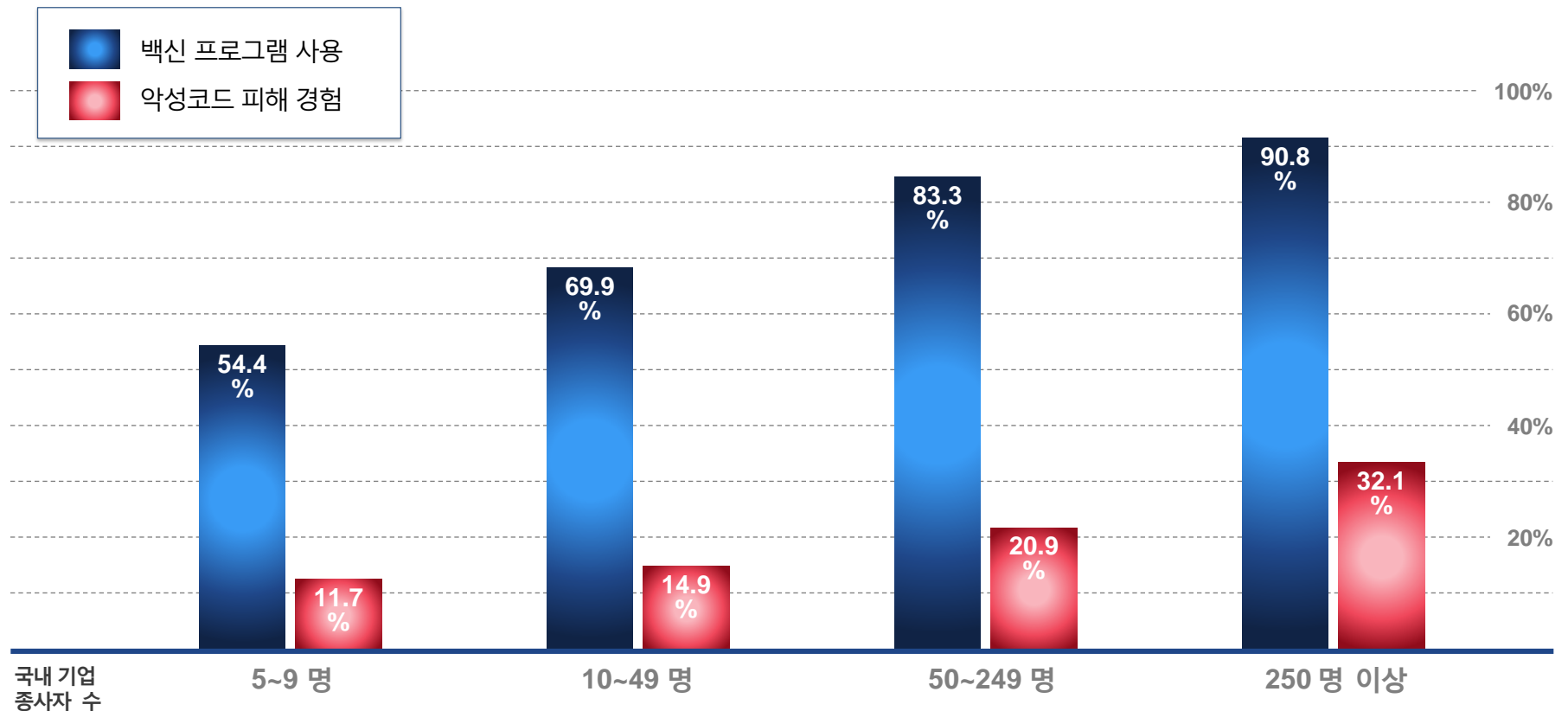
이러한 악성코드는 엔드포인트의 취약한 경로를 통해 기업 내부로 유입됩니다.

악성코드에 의한 피해를 최소화하기 위해서는 업무용 PC 등 엔드포인트 시스템의 **백신 설치뿐만 아니라 이에 대한 관리가 필수**입니다.



악성코드에 의한 기업 피해 현황

국내 기업 중 80% 이상은 백신(안티바이러스) 프로그램을 사용하고 있음에도 불구하고 일부는 악성코드에 의한 피해를 경험했던 것으로 나타났습니다. 이는 백신만으로는 신속한 진단 및 치료가 어려운 신·변종 악성코드가 증가했기 때문이기도 하지만 백신 설치 이후 최신 업데이트 적용 등 **적절한 관리가 이루어지지 않은 것** 또한 원인이라 할 수 있습니다.



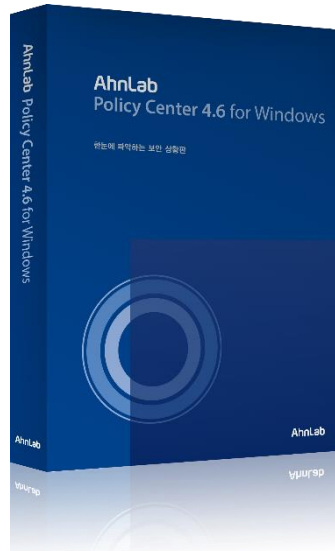
(*출처: 정보화통계집, NIA)

2. AhnLab Policy Center 4.6 for Windows

-
1. AhnLab Policy Center 4.6 for Windows
 2. 개념도
 3. 특징점
 4. 도입 효과
 5. 주요 기능
 6. 제품 구성도
 7. 운영 환경
 8. 경쟁 제품 비교

AhnLab Policy Center 4.6 for Windows

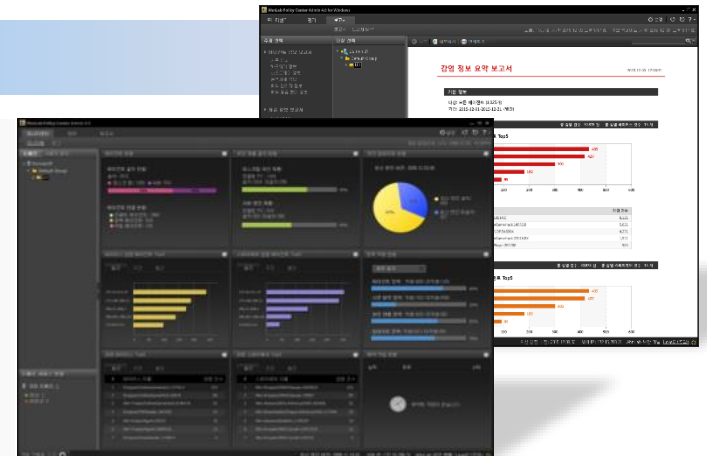
한눈에 파악하는 보안 상황판, AhnLab Policy Center 4.6 for Windows



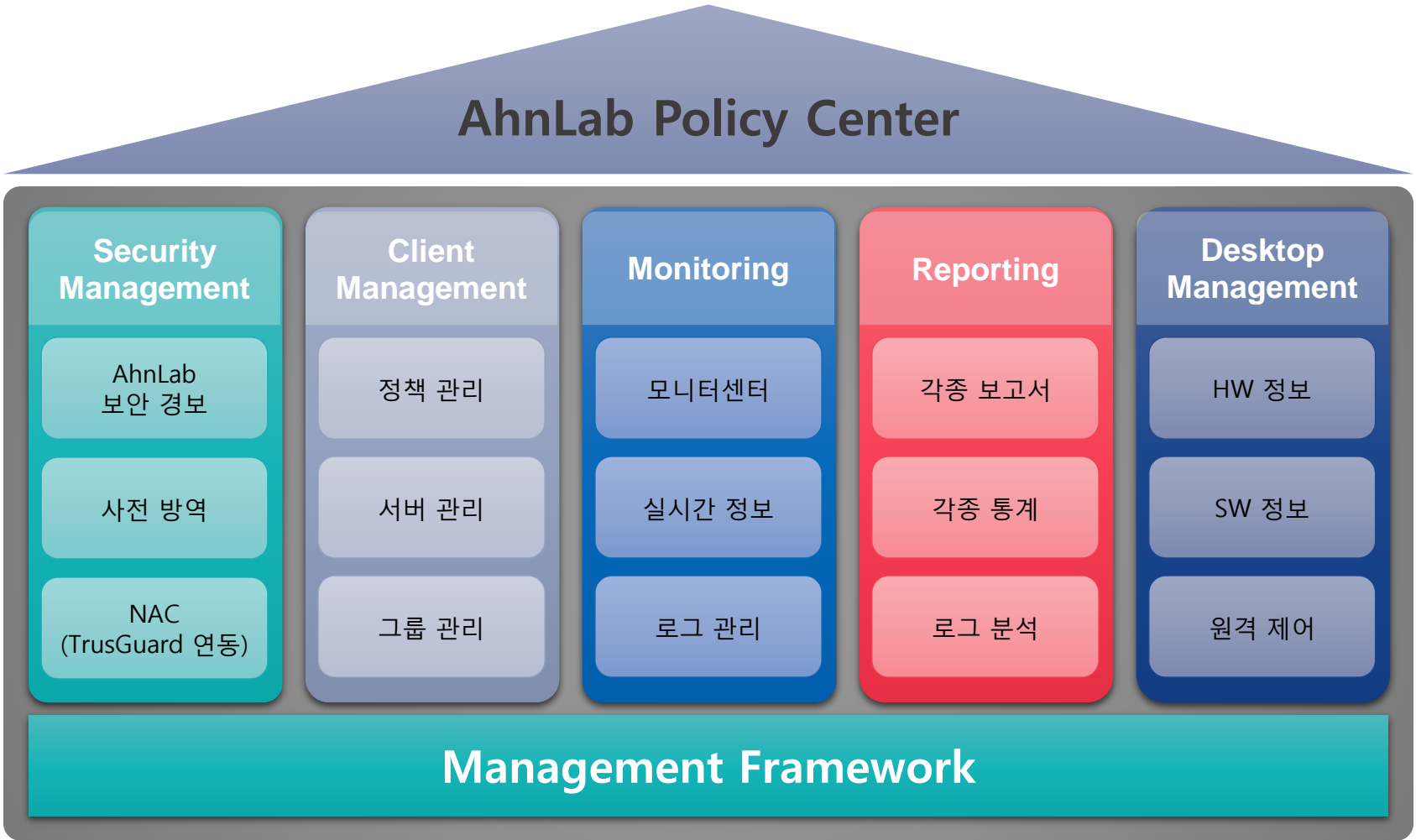
- **AhnLab Policy Center 4.6 for Windows**는 안랩의 Client/Server 보안 제품인 V3 Internet Security 제품군과 V3Net for Windows Server, V3 Net for Unix/Linux Server 제품군을 관리할 수 있는 중앙관리솔루션입니다.
- 기업 보안 정책에 따른 보안 제품 관리 외에, 바이러스 확산 방지를 위한 사전 방역 기능 및 자산 관리와 원격지원과 같은 Desktop Management 기능을 제공함으로써, 기업 내 전체 PC에 대한 제어 및 기업 내 발생 가능한 보안 위협에 효과적으로 대처할 수 있습니다.
- AhnLab policy Center 4.6 for Windows는 기업 내 전산 관리자의 환경과 사용자 분석을 통해 작성된 UX(User eXperience) 설계를 적용하여 혁신적인 관리의 편의성을 제공합니다.

제품 연혁

- **2015. 11 AhnLab Policy Center 4.6 for Windows 발표**
- 2009. 07 AhnLab Policy Center 4.0 발표
- 2008. 06 V3 Internet Security 7.0 Platinum & AhnLab Policy Center 3.0 CC 인증 획득(EAL4)
- 2007. 09 V3Pro 2004 & AhnLab Policy Center 3.0 CC인 증 획득(EAL4)
- 2005. 07 AhnLab Policy Center 3.0 발표
- 2004. 06 AhnLab Policy Center 2.5 발표
- 2003. 06 AhnLab Policy Center 2.0 발표
- 2003. 02 AhnLab Policy Center 1.0 발표
- 2002. 04 V3EDM



개념도



특장점

신뢰성

- 서버와 에이전트 간 실시간 정보 교환으로 정확한 상태 정보 제공
- 상·하위 서버 간 실시간 명령, 정책 수행으로 다양한 정보를 취합
- 통합 도메인 콘솔 구조로 전체 도메인에 대한 제어 및 정보 취합 가능

유연성

- 네트워크 환경에 따라 다양한 구조로 적용 가능
- 인사 DB 연동 표준화로 연동의 유연성 제공

편의성

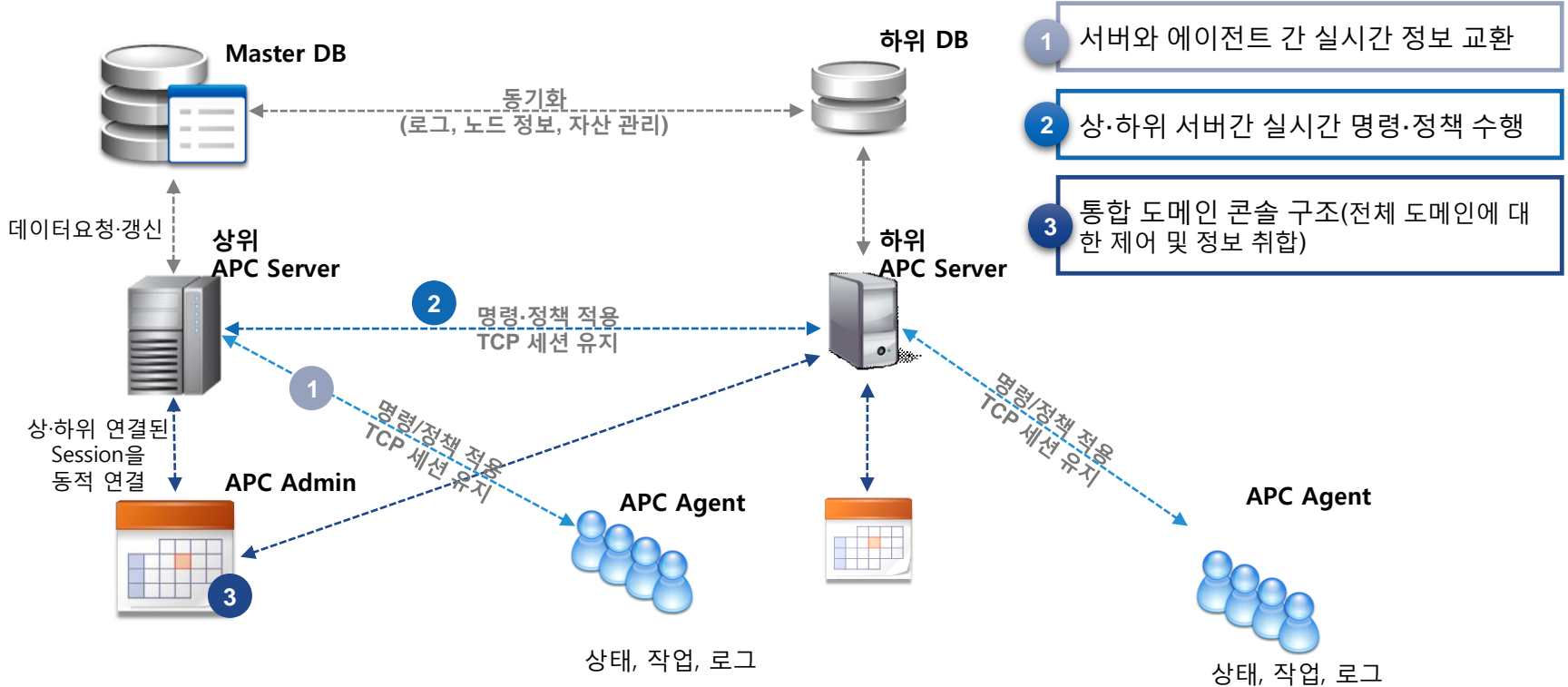
- 사용자 분석을 토대로 작성된 UX(User eXperience) 설계 적용
- 기업 보안 현황을 한눈에 파악할 수 있는 모니터센터 제공
- 작업 관리자를 통한 정책, 명령의 배포 현황 파악

특장점(1)



정책·명령 전달의 정확성과 데이터 신뢰성을 보장합니다.

서버와 에이전트 간, 서버와 서버 간의 연결 방식 개선을 통해 실시간 상태 정보 및 실시간 데이터 전송

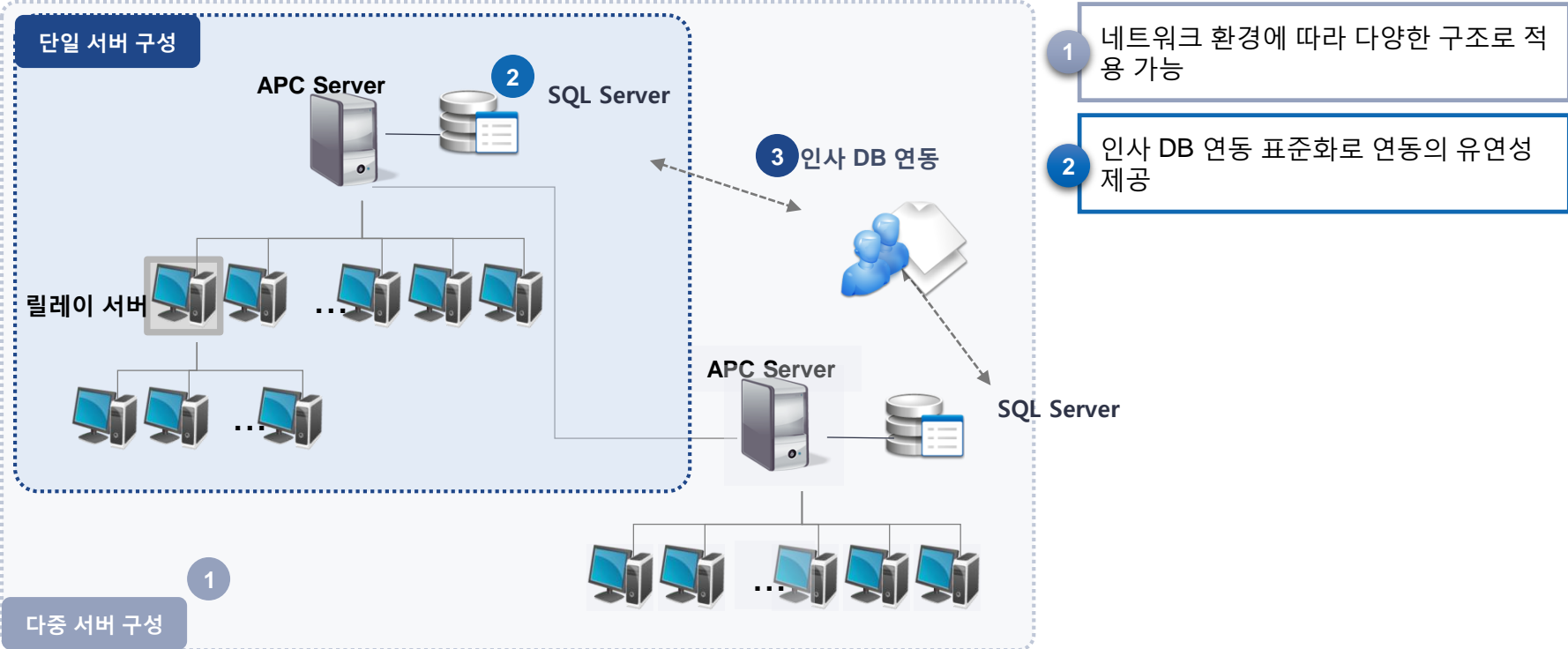


특장점(2)

유연성

기업 내 다양한 환경에 따라 유연하게 적용 가능합니다.

다양한 네트워크 환경에 따른 적용성 강화, 인사 DB 연동으로 기업 환경에 따라 유연하게 적용 가능



특장점(3)



편의성

관리의 편의성을 극대화한 솔루션입니다.

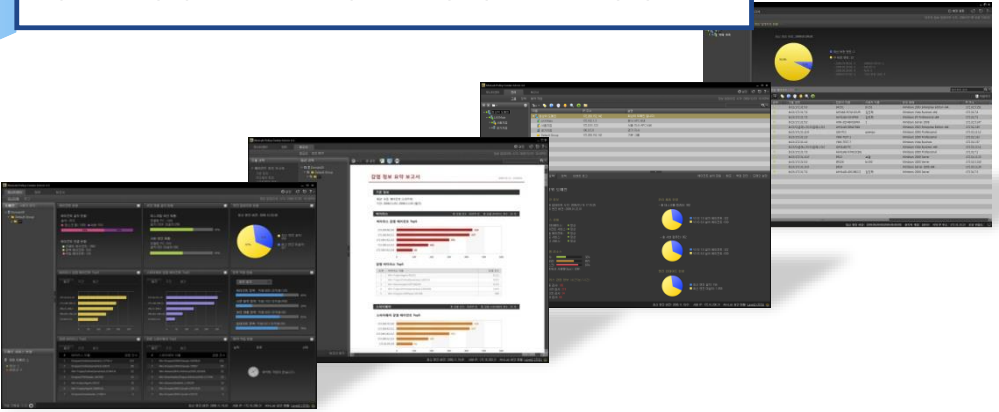
기업 내 전산 관리자의 환경과 사용자 분석을 통해 작성된 UX(User eXperience) 설계 적용으로, 혁신적인 UI 제공



사용자 분석을 토대로 작성된 UX 설계 적용

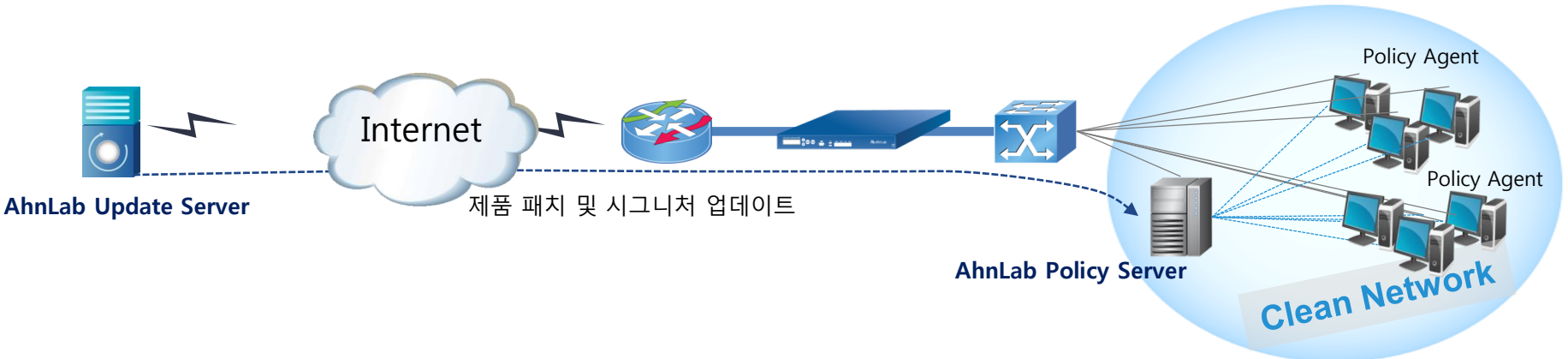
기업 보안 현황을 한눈에 파악할 수 있는 모니터센터

작업 관리자를 통한 정책·명령의 배포 현황 파악



도입 효과(1)

AhnLab Policy Center 4.6 for Windows는 기업의 안전한 보안 환경을 유지합니다!



- 보안 위협 상황 발생 시 신속한 대응
- 일관된 보안 정책 적용, 능동적 보안 관리
- 효율적 자산 관리

AhnLab Policy Center 4.6 for Windows 는 기업의 안전한 보안 환경을 구축하여 **기업의 정보자산 보호 및 비즈니스의 연속성을 확보**해 드립니다.

도입 효과(2)

AhnLab Policy Center 4.6 for Windows는 관리 비용 절감 및 업무 생산성 향상을 실현합니다!

관리 비용
절감

- 중앙 관리로 기업 전체 PC의 보안 제품 관리에 필요한 비용 절감
- PC 관리 및 악성코드 방역 정책의 신속한 적용으로 운용 효율성 극대
- 기업 전체의 PC 보안 관리를 위한 비용 및 시간 투자 감소

업무 생산성
향상

- 기업의 안전한 보안 환경 구축으로 업무 생산성 향상
- 사용자의 보안 인식 부족으로 인한 보안 문제 및 보안 사고 예방
- PC 문제 발생 시에도 중앙 제어로 빠르게 업무 복귀 가능

기업의 대외
이미지 제고

- 기업의 안전한 보안 환경 구축으로 신뢰받는 회사의 이미지 제고
- 안정적인 IT System 운영으로 대외 경쟁력 확보

주요 기능

정보 전달 구조

- 서버와 에이전트 명령/정책 수행 시, TCP Session 연결 방식 구현으로 실시간 정보 교환 및 네트워크 전송 중의 정보 유실 방지

UI 재설계

- 사용자 분석을 토대로 작성된 UX(User eXperience) 설계 적용

통합 도메인 콘솔

- 최상위의 서버에서 다종의 하위 서버 및 에이전트 제어

가상 그룹 관리

- 실제 소속된 그룹 외에, 관리자가 정의한 그룹에 소속된 에이전트들에 대한 관리 기능 (릴레이 서버 그룹, 미설치 그룹, 예외 그룹, 감시 그룹)

담당자 권한 설정

- 사용자정의 관리자 기능 추가로 각 기능별 권한 설정 및 도메인, IP 주소 범위 설정 별 로그인 제한 가능

보안성 강화

- 서버와 서버 간, 서버와 에이전트 간의 통신 구간 전체 암호화, 로그 암호화로 제품의 보안성 강화

작업관리자

- 모든 정책 명령·배포, 예약 작업, 공지사항 등에 대한 진행 사항 표시 및 성공/실패된 에이전트 수 표시

예약 작업

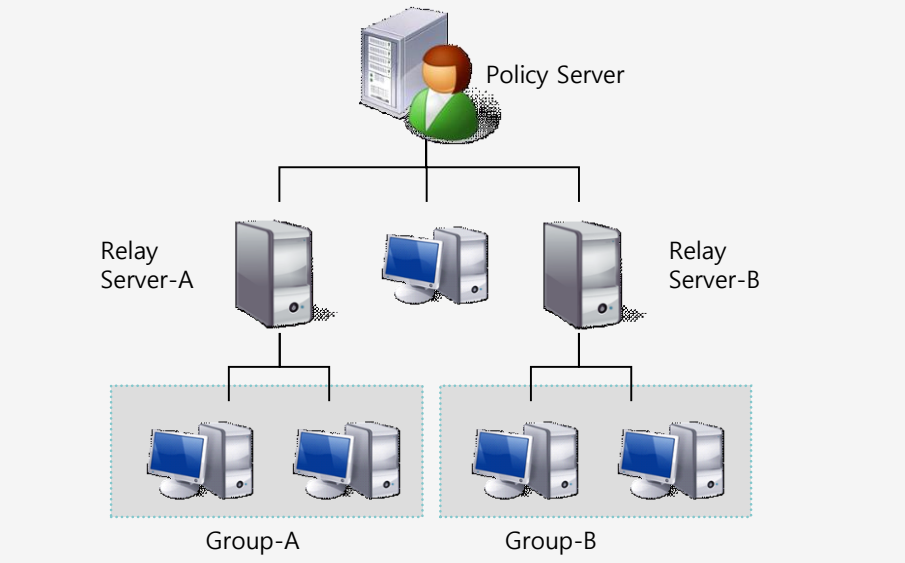
- 예약된 일정에 작업(공지사항, 수동 업데이트, 명령 실행, 정책 배정 등)을 예약 대상에게 배포 가능

제품 구성도

단일 서버 구성	다중 서버 구성
----------	----------

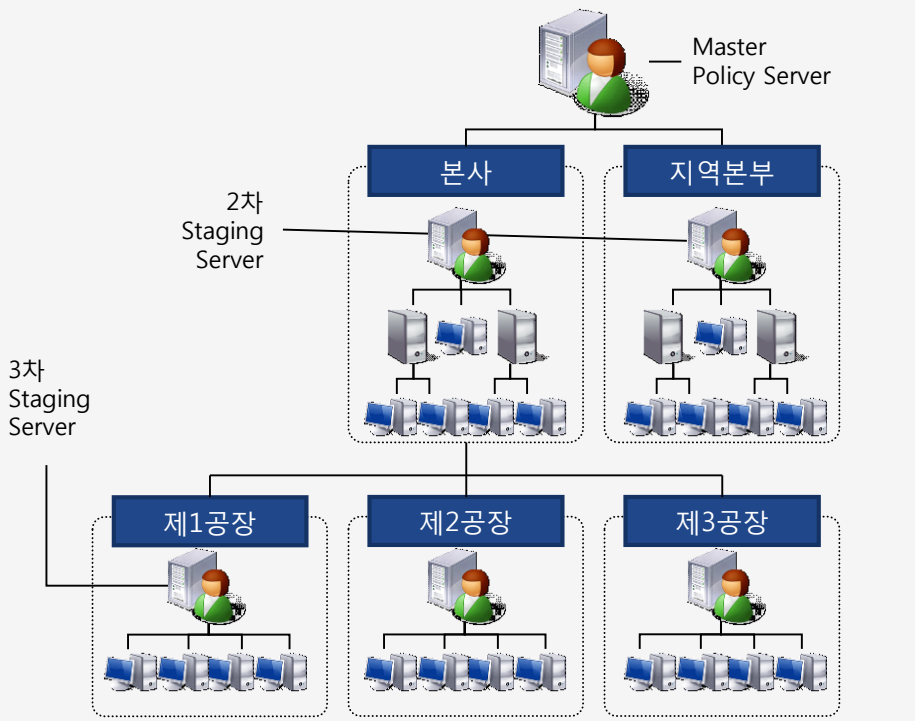
단일 LAN 내에 관리하고자 하는 모든 시스템이 모여있을 때 구성하는 가장 일반적인 방법

- 1대의 Policy Server가 모든 시스템 관리
- 파일 배포 부하 경감을 위해 그룹별 릴레이 서버 구축
- 주 릴레이 서버, 보조 릴레이 서버 지정으로 가용성 확보



관리 조직 및 단위가 계층적으로 분화되어 있고, 조직 간 연결에 WAN 구간이 있을 경우 적용 방법

- 1대의 Master Policy Server를 최상위 관리자가 관리
- 다수의 Staging Server를 단위 조직 관리자가 관리
- 파일 배포 부하 경감을 위해 그룹 별 릴레이 서버 구축
- 주 릴레이 서버, 보조 릴레이 서버 지정으로 가용성 확보



운영 환경

구분		Agent	Admin	Server
필수 구성 요소		<ul style="list-style-type: none"> Internet Explorer 6.0 이상 WinSock 2.0 	<ul style="list-style-type: none"> Internet Explorer 6.0 이상 .Net Framework 3.5 이상 WinSock 2.0 	<ul style="list-style-type: none"> MS SQL Server 2003 이상 MSDE 2000 이상
운영체제		<ul style="list-style-type: none"> Windows Server 2003 / 2008 / 2012 Windows XP Professional / Vista Windows 7 / 8(8.1) / 10 	<ul style="list-style-type: none"> Windows Server 2003 / 2008 / 2012 Windows XP Professional / Vista Windows 7 / 8(8.1) / 10 <p>* Windows 2000 계열은 지원하지 않음</p>	<ul style="list-style-type: none"> - 권장 운영체제 • Windows Server 2003 - 동작 운영체제 • Windows Server 2003 / 2008 / 2012 • Windows 7 <p>* Windows Vista는 지원하지 않음</p>
* 상기 OS의 64비트 호환 모드 지원				
하드웨어	CPU	<ul style="list-style-type: none"> Pentium 233MHz 이상 IBM-PC 호환 컴퓨터 	<ul style="list-style-type: none"> Intel Pentium 1GHz 이상 	<ul style="list-style-type: none"> Intel Pentium 1.5GHz 이상 권장
	Memory	<ul style="list-style-type: none"> 64MB 이상 	<ul style="list-style-type: none"> 1GB 이상 	<ul style="list-style-type: none"> 1GB 이상 권장
	HDD	<ul style="list-style-type: none"> 400MB 이상 	<ul style="list-style-type: none"> 최소 2GB 이상의 여유 공간 	<ul style="list-style-type: none"> 최소 5GB 이상의 여유 공간
	NIC	(해당 사항 없음)	<ul style="list-style-type: none"> 10/100 Ethernet Card <p>* IA64는 지원하지 않음</p>	<ul style="list-style-type: none"> 10/100 Ethernet Card <p>* Policy Server 전용 권장</p>

경쟁 제품 비교

구분		AhnLab Policy Center 4.6 for Windows	H사	S사	E사
관리대상제품	Windows Client AV	○	○	○	○
	Windows Server AV	○	○	○	○
	Unix/Linux Server AV	○	X	X	X
	Personal Firewall	○	○	○	X
서버 간 계층 구조/ 부하 분산/이중화	Staging Server	○	○	○	X
	Relay Server	○	○	X	X
관리자 운영	관리자 권한 레벨 제공	○	○	○	○
	기능별 관리자 권한 제공	○	△	X	X
	IP범위별/시간대별 접근 제어	○	X	X	X
Dash Board 지원	보안 현황 모니터링	○	○	△	△
정책 관리	정책 상속	○	○	-	X
	정책 Import/Export	○	X	X	X
	정책 적용 상태 표시	○	△	X	X
Task 관리	수행 명령의 성공/실패 관리	○	△	△	X
	최근 수행 명령 관리	○	△	X	X
	예약 작업 기능	○	○	X	X
파일 배포	일잔 소프트웨어 배포/실행	○	○	X	○
	실행 파라미터 옵션	○	○	X	○
	OS별 배포 옵션	○	○	X	X
사전 방역	취약 패스워드/공유 폴더 관리	○	○	X	X
	PC Network Threshold	○	X	X	X
Desktop Management	금지사항	○	○	X	○
	원격제어	○	○	X	○
	SW, HW 정보	○	○	X	△
	윈도우 자동 업데이트 제어	○	X	X	X

3. 주요 UI

-
1. 엔드포인트를 통한 악성코드 유입 및 확산
 2. 악성코드에 의한 기업 피해 현황

모니터센터

기업의 보안 상태를 모니터링할 수 있는 현황판으로, 관리자가 필요로 하는 보안 정보를 한눈에 파악할 수 있도록 구성되어 있습니다.

통합 도메인 콘솔

보안 위험도 정보 제공

작업 진행 현황 파악

The screenshot shows the AhnLab Policy Center Admin 4.6 for Windows interface. The dashboard is divided into several sections:

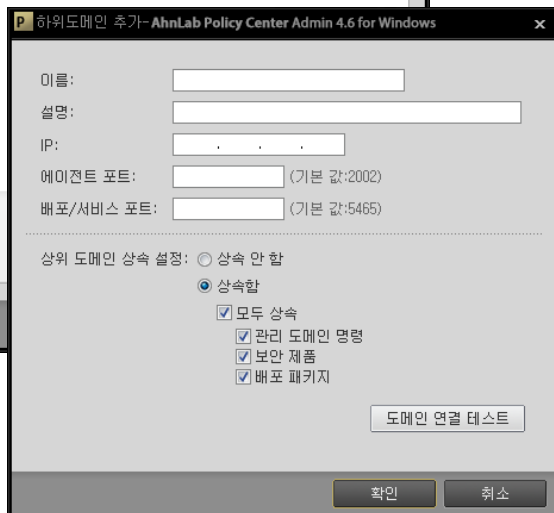
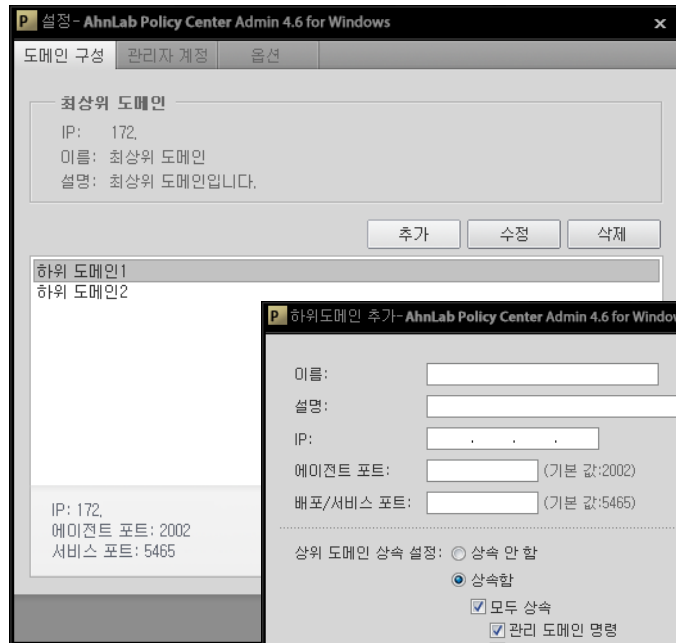
- 도메인 (Domain):** A tree view on the left shows the domain structure, including 'Domain01' and 'Test Domain'.
- 에이전트 현황 (Agent Status):** Displays the status of installed agents, including a bar chart showing 56% (1320) installed and 44% (510) not installed.
- 보안 제품 설치 현황 (Security Product Installation):** Shows the status of security products installed on desktops and servers, with 45% completion for both.
- 엔진 업데이트 현황 (Engine Update Status):** Includes a pie chart showing the distribution of engine versions (321 latest, 660 old).
- 바이러스 감염 에이전트 Top5 (Virus Infection Agent Top5):** A horizontal bar chart showing the top 5 infected agents.
- 스파이웨어 감염 에이전트 Top5 (Spyware Infection Agent Top5):** A horizontal bar chart showing the top 5 infected agents.
- 정책 적용 현황 (Policy Application Status):** A bar chart showing the application status of various policies, such as Agent Policy (85%), Incident Response Policy (23%), Security Product Policy (82%), and Update Policy (78%).
- 감염 바이러스 Top5 (Infected Virus Top5):** A table listing the top 5 detected viruses.
- 감염 스파이웨어 Top5 (Infected Spyware Top5):** A table listing the top 5 detected spyware.
- 에약 작업 현황 (Quarantine Task Status):** A table showing the status of quarantine tasks.
- 도메인 상태 현황 (Domain Status Status):** A summary of domain status, showing 4 domains, 3 warnings, and 1 error.
- 작업 진행 중 (Task In Progress):** A button to view the progress of tasks.

A red alert box in the bottom right corner displays the following information:

AhnLab 보안 경보
 Win-Trojan/Downloader.374651
 위의 바이러스가 공격해 퍼지고 있습니다.
 보안 위협에 각별히 주의하십시오.
 상세보기

도메인 관리

모니터센터 상단의 '환경설정' 메뉴를 통해 도메인을 손쉽게 추가할 수 있으며, '도메인 상태 현황' 메뉴를 통해 총 도메인들의 상태를 확인 할 수 있습니다.



도메인 이름	IP	최신 패치 적용	DB크기(MB)	서비스 상태			시스템 리소스				부유 엔진 버전	상태 업데이트
				에이전트	판술	로그	CPU	Memory	HDD	Traffic		
최상위 도메인	172.200.152.142	✔ 적용 4.6.3.12	34MB	●	●	●	18%	60%	75%	95Mbps	2015.12.09.03	2015/12/09 1
Main	172.102.1.3	⚠ 미적용 4.6.3.23	156MB	●	●	●	12%	15%	13%	25Mbps	2015.12.09.01	2015/12/09 1
서울 지점	172.0.51.123	⚠ 적용 중...(상세)	985MB	●	●	●	27%	35%	36%	84Mbps	2015.12.08.01	2015/12/08 1
경기 지점	196.0.5.8	✖ 적용 실패(상세)	453MB	●	●	●	34%	89%	56%	10Mbps	2015.12.07.01	2015/12/07 1

도메인 서비스 상태 표시

그룹 관리

도메인 하단의 그룹 관리를 위한 기능으로, 도메인 상태 요약 및 정책 배정 현황 파악이 가능합니다.

그룹 추가/삭제

The screenshot displays the AhnLab Policy Center Admin 4.6 for Windows interface. The main window shows a table of domain groups with columns for Name, IP Address, and Description. Below the table, there are tabs for '도메인 상태 요약' (Domain Status Summary), '정책' (Policy), and '이벤트 로그' (Event Log). The '도메인 상태 요약' tab is active, showing detailed information for the '최상위 도메인'.

이름	IP 주소	설명
최상위 도메인	172.16.200.5	최상위 도메인 입니다.
Main	172.102.1.3	본사 APC 서버
서울 지점	172.0.51.123	서울 지사 APC 서버
경기 지점	196.0.5.8	경기 지사
기본 그룹	기본 그룹	기본 그룹

도메인 요약 정보, 정책 배정 현황 파악

최상위 도메인

도메인 정보

- 상태 업데이트 시간: 2015/12/09 17:17:30
- 보유 엔진 버전: 2015.12.09.03

서비스 상태

- 데이터베이스: ● 정상
- 에이전트 서비스: ● 정상
- 콘솔 에이전트: ● 정상
- 배포 서비스: ● 정상
- 로그 서비스: ● 정상

시스템 리소스

- CPU: 32%
- 메모리: 65%
- 디스크: 87%
- 네트워크 사용량(bps): 324K

바이러스 감염 정보 (최근5분/1시간)

- 수동 검사: 105
- 실시간 검사: 219
- 인터넷 검사: 34
- 기타 검사: 66

관리 제품 현황

- 총 데스크톱 컴퓨터: 1320
- V3 IS 7.0 설치 에이전트: 224
- V3 IS 8.0 설치 에이전트: 1096

총 서버 컴퓨터: 510

- V3 IS 7.0 설치 에이전트: 347
- V3 IS 8.0 설치 에이전트: 163

엔진 업데이트 현황

- 최신 버전 엔진: 854
- 구 버전 엔진: 420

작업 진행중 ○ 최신 엔진 버전: 2015.12.09.03 서버 IP: 172.16.200.31 AhnLab 보안 레벨: Level2(주의)

정책 관리

관리하는 대상 보안 제품(V3 Internet Security, V3Net for Windows Server, V3 Net for Unix/Linux Server) 및 agent, 사전 방역 등의 정책을 설정합니다.

정책 Export / Import

정책 배정 현황

정책 상세 설정

The screenshot displays the AhnLab Policy Center Admin 4.6 for Windows interface. The left sidebar contains a navigation tree with the following structure:

- 에이전트(1)
 - 기본 정책
 - 기본 정책_2
- 사전 방역(1)
 - 기본 정책
- 데스크탑용 제품(2)
 - V3 IS 7.0 (1)
 - 기본 정책
 - V3 IS 8.0 (1)
 - 기본 정책
- 서버용 제품(2)
 - V3 Net 6.0 (1)
 - 기본 정책
 - V3 Net 7.0 (1)
 - 기본 정책

The main content area shows the configuration for the selected policy '기본 정책_2'. It includes a '배정 현황' (Assignment Status) section with a pie chart and the following data:

- 성공: 123
- 실패: 23
- 적용중: 55

Below the chart are tabs for '에이전트 일반 설정', '제품 설치 설정', and '제품 업데이트 설정'. The '에이전트 일반 설정' tab is active, showing the following settings:

- 관리 대상 제품 설정** (Managed Product Settings):
 - V3 IS 7.0
 - V3 IS 8.0
 - V3 IS 9.0
 - V3 ES 9.0
 - V3 Net 6.0
 - V3 Net 7.0
 - V3 Net 9.0
- 주기 설정** (Cycle Settings):
 - 정책 다운로드 주기: 240 (10-1440분)
 - 에이전트 패치 주기: 1440 (1-9999분)
 - 필레미 서버 패치 주기: 1440 (1-9999분)
 - 에이전트 정보 업로드 주기:
 - 관리 대상 보안 제품 정보: 240 (1-480분, 기본 값:240)
 - 하드웨어 자산 정보: 1440 (10-1440, 기본 값:1440)
 - 소프트웨어 자산 정보: 1440 (5-1440분, 기본 값:1440)
- 시간 동기화** (Time Synchronization):
 - 상위 서버와 시간 동기화

At the bottom of the configuration area, there are buttons for '기본 값' (Default), '확인' (OK), and '취소' (Cancel).

예약 작업

예약된 일정에 따라 작업(공지사항 발송, 수동 업데이트, 명령 실행, 정책 배정 등) 내용이 배포되도록 설정합니다.

The screenshot displays the '예약 작업' (Scheduled Task) configuration window in AhnLab Policy Center Admin 4.6. The window is divided into several sections:

- 예약 작업 리스트 (Scheduled Task List):** A table at the top showing a list of tasks. The first task is highlighted:

주기	종류	이름	설명	대상	상태
매일 [20:00]	수동 업데이트	수동 업데이트 하기	매일 지정된 시각에 수동 업데이트 예약 작업	특정 조건으로 대상 선택	!! 대기중
- 예약 작업 선택 및 일정 설정 (Task Selection and Scheduling):** A panel on the left for configuring the task details:
 - 이름: 수동 업데이트 하기
 - 설명: 매일 지정된 시각에 수동 업데이트 예약 작업
 - 주기: 매일, 20:00
 - 제품 선택: V3 IS 7.0, V3 IS 8.0, V3 Net 6.0, V3 Net 7.0
 - 대상 선택: 패치 파일, 엔진 파일
- 예약 작업 적용 대상 (Task Application Targets):** A panel on the right for selecting target environments:
 - 예약 대상: 그룹 트리에서 대상 선택, 특정 조건으로 대상 선택
 - 조건 선택: OS
 - Desktop: Windows98SE, Windows ME, Windows NT Workstation 4.5 SP5, Windows2000 Professional, Windows XP Home/Professional, Windows Vista
 - Server: Windows NT Server 4.0 SP5, Windows 2000 Server, Windows 2003 Server, Windows 2008 Server

보고서

DB에 등록되어 있는 각종 기록 정보를 이용하여 내용별 보고서를 제공합니다.

보고서 예약 기능

보고서 템플릿

사용자 정의 보고서

The screenshot displays the 'AhnLab Policy Center Admin 4.6 for Windows' interface. The left sidebar contains a tree view of report templates under the '보고서' (Reports) tab. The main area shows a preview of a '감염 정보 요약 보고서' (Infection Information Summary Report) for the date 2015-12-09 17:16:51. The report includes sections for '기본 정보' (Basic Information), '바이러스' (Virus), and '스파이웨어' (Spyware). The '바이러스' section features a horizontal bar chart showing the top 5 infected agents and a table listing the top 5 infected viruses. The '스파이웨어' section also features a horizontal bar chart showing the top 5 infected agents.

감염 정보 요약 보고서 2015-12-09 17:16:51

기본 정보

대상: 모든 에이전트 (1,025개)
기간: 2015-12-01-2015-12-31 (월간)

바이러스 총 감염 건수: 30,878 건 총 감염 바이러스 갯수: 15 개

바이러스 감염 에이전트 Top5

IP	감염 건수
172.100.56.210	435
172.100.54.211	427
172.100.152.212	301
172.100.12.213	182
172.100.152.214	95

감염 바이러스 Top5

순번	바이러스 이름	감염 건수
1	Win-Trojan/Agent.9514.C	8,121
2	Win-Trojan/OnlineGameHack.14552.B	5,021
3	Win-Downloader/LOP.546304	4,231
4	Win-Trojan/OnlineGameHack.22016.BX	1,521
5	Win-Dropper/3WPlayer.267208	985

스파이웨어 총 감염 건수: 30,878 건 총 감염 스파이웨어 갯수: 15 개

스파이웨어 감염 에이전트 Top5

IP	감염 건수
172.100.75.210	435
172.100.42.211	427
172.100.162.212	301
172.100.32.213	182
172.16.24.214	95

최신 엔진 버전: 2015.12.09.03 서버 IP: 172.16.200.31 AhnLab 보안 레벨: Level2(중위)

㈜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
Policy Center 4.6 for Windows

More security,
More freedom

AhnLab