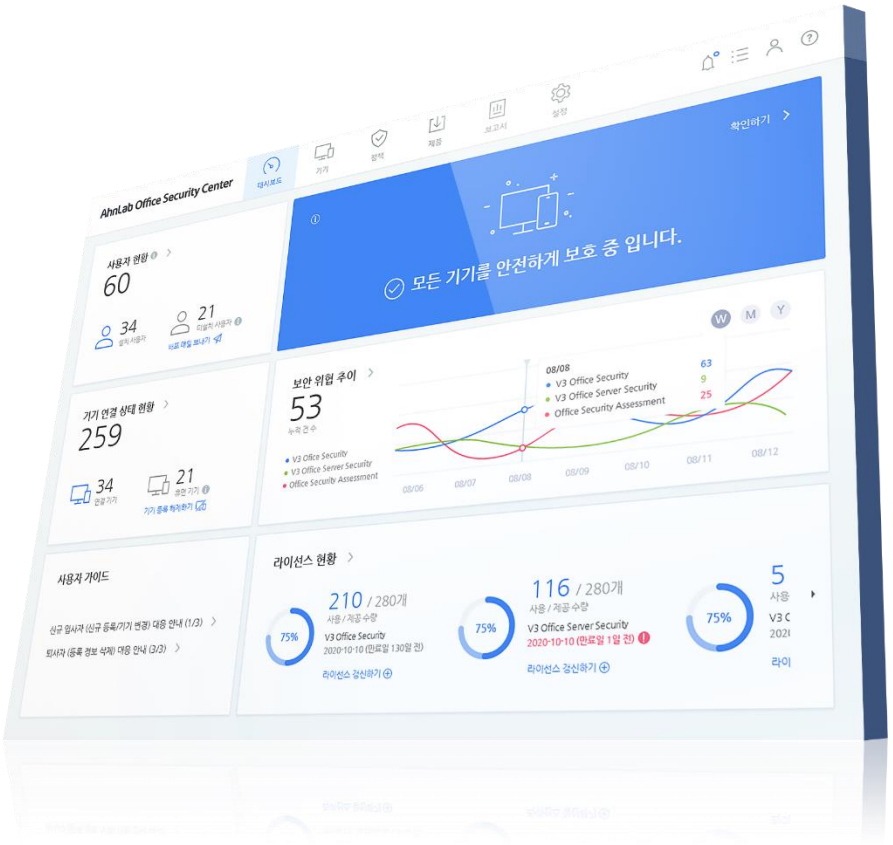
More security,
More freedom

AhnLab Office Security

중소기업을 위한 SaaS형 보안 관리 솔루션

표준제안서



AhnLab

목차

AhnLab
Office Security

AhnLab

01.
제안 배경

1. 업무 환경의 변화
2. 기기 환경의 위협 요소
3. 지속적으로 증가하는 악성코드
4. 침해 위협 노출
5. 보안 관련 현실과 어려움
6. 보안 관리·대응의 필요성

업무 환경의 변화

장소, 시간에 상관없이 정보 공유 및 상호 협력이 가능한 스마트 워크 시대의 도래로 기업 정보 시스템과 직원이 사용하는 정보 자산 환경을 보호하기 위한 대책의 고려가 필요 합니다.
유·무선 네트워크 및 물리적 환경 보안 외에도 스마트한 업무 환경에 사용되는 기기 보안 플랫폼의 보호 대책 마련이 되어야 합니다.

- 업무용 PC가 악성코드에 감염되어 고객 정보나 보고서, 계약서, 매출 자료 등 기업 중요 정보의 유출
- 직원이 카페나 지하철 선반 위에 주요 정보가 저장되어 있는 노트북 가방을 분실 또는 두고 내려 많은 정보 유출
- 재택 근무를 하면서 보안 프로그램을 업그레이드 하지 않아 신종 바이러스에 감염

모바일 업무(Mobility-Workflow) 환경

- 랩톱(Laptop), 모바일 디바이스(Mobile Device)와 같은 이동식 기기를 활용하여 공간 제약없이 실시간 업무 처리
- 기업 외부 업무용 기기의 대한 보안 정책 관리 어려움

홈 오피스 환경

- 자택에서 공간 및 필요한 시설 장비 구비 후 업무
- 외부 기기를 통해 작성된 문서 데이터 등 사내 유입 가능성
- 개인 기기에 대한 보안 정책 관리 어려움

PC방과 같은 외부 환경

- 관리 불가능한 PC 환경에서의 업무 처리
- 외부 기기를 통해 작성된 문서의 사내 유입
- 인터넷 웹 서핑, 이메일, USB 등을 통한 데이터 유입

직장 내 업무 환경

- 직장에서 업무 효율성을 보다 높일 수 있는 시설/환경을 구축하여 자유롭게 근무
- 다양한 업무환경에 따른 유입 위협 확산 및 대응 속도 지연
- PC/Server 개별 자산에 대한 보안 정책 통합 관리 어려움

기기 환경의 위협 요소

스마트워크 업무 환경 전환으로 디바이스 자체에 내재된 취약점 또는 사용 부주의로 다양한 리스크가 발생할 수 있습니다.

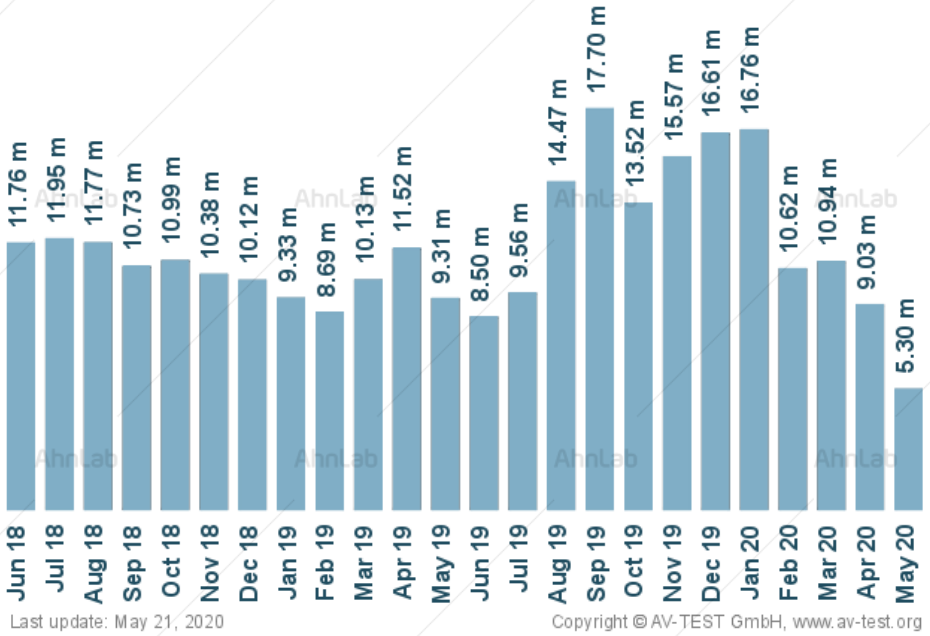
개인정보침해	위치정보 탈취를 통한 개인정보 침해
	카메라, 마이크 등 기기의 하드웨어 자원을 이용한 개인정보 침해
도청	네트워크로 전송되는 데이터 패킷 도청
	Wi-Fi, VoIP 사용 시 음성 및 영상 통화 도청
피싱 및 파밍	악의적인 사이트를 이용한 사용자 정보 입력 유도
	문자 메시지, 이메일 등을 이용하여 악성 애플리케이션 설치 유도
서비스 거부 (DoS/DDoS)	지속적인 통화 연결 및 데이터 전송요청 등을 통한 배터리 소진 및 기기 서비스 거부 공격
	좀비 PC, 좀비 모바일 기기 등을 이용한 내부 서버 대상의 서비스 거부 공격
권한 탈취	기기-내부시스템 간 중간자(Main-in-the-Middle) 공격을 통한 사용자 권한 획득
	SQL Injection 공격을 통한 인증 우회
	악성코드 및 기기 루팅, 탈옥을 통해 관리자(Root) 권한 탈취
	버퍼 오버플로우 공격을 통한 관리자 권한 탈취
	기기와 내부 시스템 간에 맺어진 세션 탈취
악성코드 · 해킹	악의적인 스크립트 실행으로 공격자가 악성코드를 삽입한 웹사이트 접속
	주요 정보가 포함된 문서 및 자료 암호화를 통한 데이터 파괴 (랜섬웨어)
	불필요한 서비스(포트) 사용 취약점
	애플리케이션 소스코드 분석(리버스 엔지니어링)을 통한 취약점 분석
	기기에서 제공하는 네트워크 통신 기능을 사용하여 서버 보안 정책 우회 및 공격 경로로 활용
	기기를 USB 이동 저장매체로 사용하여 악성코드 전파
정보 유출	내부자에 의한 기업 내부 정보자산 유출
	기기 분실, 도난, 양도, 공공장소 사용에 따른 내부정보 유출
	기기 녹음, 녹화, 화면 캡쳐, 메모 기능을 통한 생성·저장된 정보 유출
	비인가 AP를 통한 정보 유출
	키로거(Key Logger) 감염에 의한 사용자 입력정보 탈취
	블루투스 및 Wi-Fi Direct 취약점을 이용한 정보유출
	비인가 애플리케이션 설치에 따른 정보유출
	비인가자의 정보 획득 및 업무처리 기능 접근

지속적으로 증가하는 악성코드

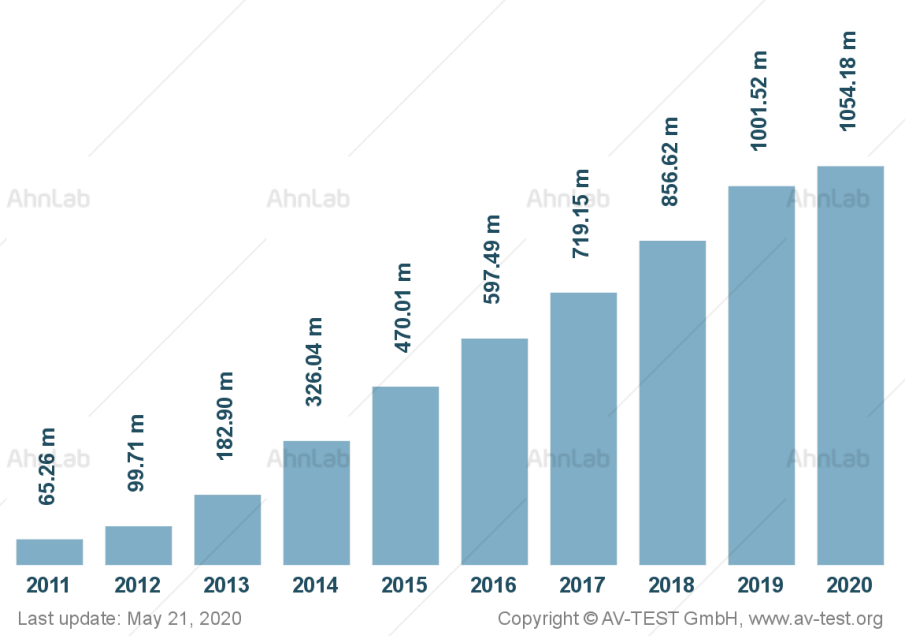
해마다 악성코드의 수는 기하급수적으로 늘고 있으며, 매일 수십만 여 개의 신·변종 악성코드가 새롭게 발견되고 있습니다.
그만큼 분석 및 대응해야 하는 악성코드의 수가 급격히 늘고 있는 셈입니다.

- 기업의 IT 환경이 발전함에 따라 편의성이 증대됨과 동시에 보안 위협도 증가
- 최근 금전 탈취 목적의 공격이 늘어나고 있으며 악의적 공격도 전문화 · 상업화되는 추세
- 인터넷 등을 통해 악성코드 제작법이 유포, 일반인도 쉽게 악성코드를 만들 수 있어 악성코드는 더 폭증할 것으로 예상
- 신종 악성코드는 줄어들고 있으나, 변종 악성코드가 증가함에 따라 전체 악성코드 수는 지속적인 증가 추세

New Malware



Total Malware



As of May 21, 2020
※ Source: AV-TEST GmbH

침해 위협 노출

공격자들은 정보보호 예산과 전문 인력이 부족한 사업체를 타깃으로 공격을 감행하고 있습니다.

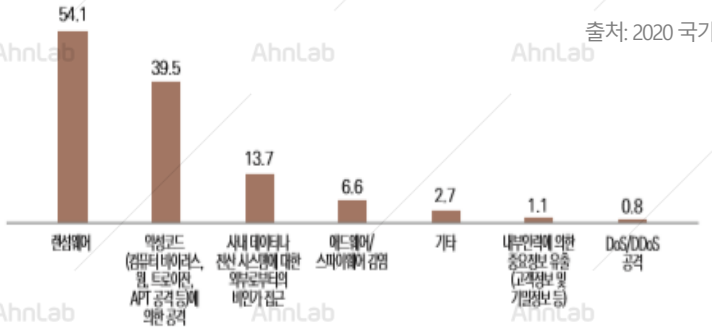
침해사고 경험 사업체 랜섬웨어 **54.1%** > 악성코드에 의한 공격 **39.5%** > 애드웨어/스파이웨어 감염 **6.6%** 등

랜섬웨어 업종별 피해 중소기업 **43%** > 소상공인 **25%** > 대기업 **1%** 등

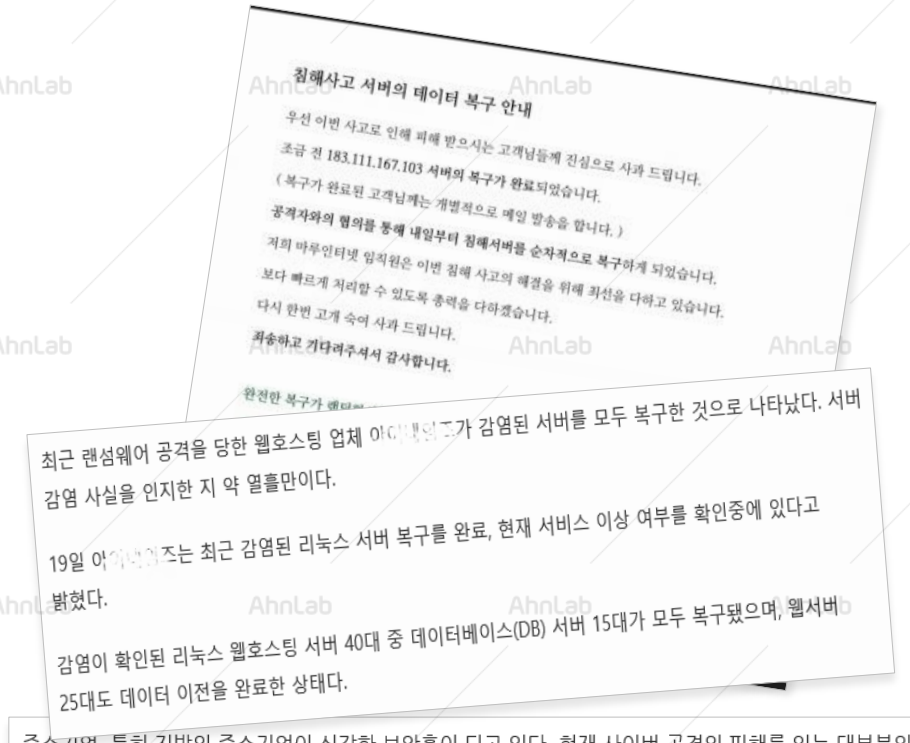
업종별 피해 (개인 / 소상공인 / 중소기업 92%)

출처: 한국랜섬웨어침해대응센터 2028.11

침해사고 경험 유형(복수 응답) – 침해사고 경험 사업체



출처: 2020 국가정보보호백서2020, 2020.05
단위 %



침해사고 서버의 데이터 복구 안내

우선 이번 사고로 인해 피해 받으시는 고객님들께 진심으로 사과 드립니다.

조금 전 183.111.167.103 서버의 복구가 완료되었습니다.

(복구가 완료된 고객님께는 개별적으로 메일 발송을 합니다.)

공격자와의 협의를 통해 내일부터 침해서버를 순차적으로 복구하게 되었습니다.

저희 바루인터넷 임직원은 이번 침해 사고의 해결을 위해 최선을 다하고 있습니다.

보다 빠르게 처리할 수 있도록 총력을 다하겠습니다.

다시 한번 고개 숙여 사과 드립니다.

최송하고 기다려주셔서 감사합니다.

완전한 복구가 [illegible]

최근 랜섬웨어 공격을 당한 웹호스팅 업체 [illegible]가 감염된 서버를 모두 복구한 것으로 나타났다. 서버 감염 사실을 인지한 지 약 열흘만이다.

19일 [illegible]는 최근 감염된 리눅스 서버 복구를 완료, 현재 서비스 이상 여부를 확인중에 있다고 밝혔다.

감염이 확인된 리눅스 웹호스팅 서버 40대 중 데이터베이스(DB) 서버 15대가 모두 복구됐으며, 웹서버 25대도 데이터 이전을 완료한 상태다.

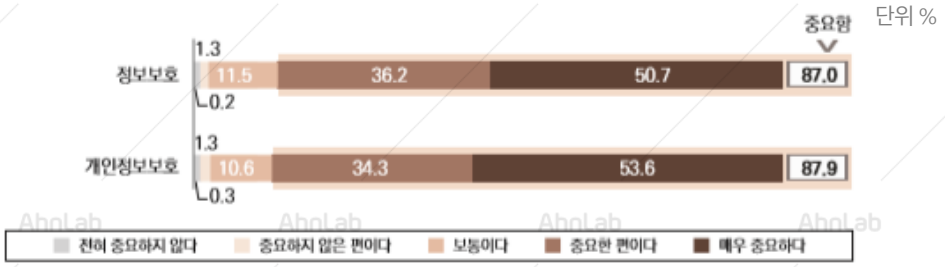
중소기업, 특히 지방의 중소기업이 심각한 보안홀이 되고 있다. 현재 사이버 공격의 피해를 입는 대부분의 기업이 중소규모 기업으로, 보안 투장 예산이 충분하지 않고 전문가를 고용하는 것도 여의치 않으며, 보안에 대한 의지도 높지 않아 중소기업이 주요 공격 타깃이 되고 있다. 또한 중소기업과 협력하고 있는 대기업으로 침투할 통로를 마련하기 위한 목적으로도 중소기업이 공격의 타깃이 되고 있다.

보안 관련 현실과 어려움

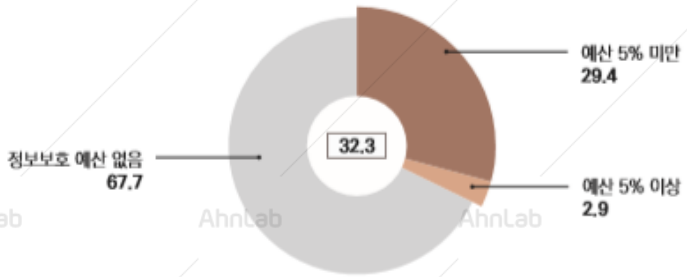
국가정보보호백서에 따르면 국내 사업체의 87.0%가 정보보호의 중요성 인식하고 있습니다.
하지만 정보보호 예산과 전문 인력이 부족한 대다수의 사업체에서는 정보보호 방안을 수립하는데 어려움을 겪고 있습니다.

- 국내 사업체의 12.3%만이 정보보호 조직 운영
- 2018년 1년간 IT 예산 중 정보보호 예산을 편성한 사업체는 32.3%, 67.7%는 정보보호 예산 없음
- 국내 사업체가 정보보호에 대하여 어려움을 느끼는 사항
  : 필요한 정보보호 제품 및 서비스 찾기 어려움(42.5) > 정보보호 예산 확보(38.4%) > 정보보호 전문인력 확보(27.3) 등

정보보호 중요성 인식

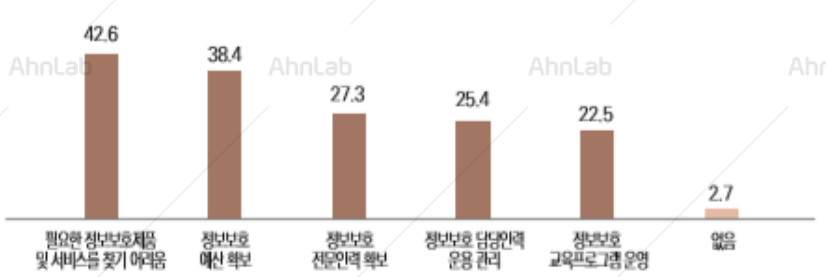


정보보호 예산



정보보호(개인정보보호) 조직 운영

정보보호 애로 사항(복수 응답)



출처: 2020 국가정보보호백서2020, 2020.05

보안 관리·대응의 필요성

01 SMB 취약한 관리 환경

- 공격 대상이 될 수 있음을 자각하지 못함
- 보안 체계 구축에 필요한 시간, 자본, 인력, 교육, 노하우 부족
- 사이버 보안에 대한 수동 / 비공식적 프로세스가 너무 많은 문제
- 사이버 보안 도구의 복잡성을 관리하기 어려워하는 문제

02 보안 관리 전담 부서 부재

- 1인이 본업 외 추가로 보안 관리를 하는 경우가 대부분
- 보안 관리에 투자할 시간적 여유 없음. 시간 / 비용 투자 미흡
- 보안 부서 / 전문 인력 부재
- 보안 의식 / 전문 지식 부족

03 쉽고 간편한 보안 관리 요구

- 세부적 보안 관리/감독이 아닌, 제품 작동이 잘 되는지에 대한 관점
- 입사, 퇴사, 기기 변경/포맷과 같은 이벤트 대응의 어려움
- PC/사용자 정보 수정/삭제 기능 요구 (라이선스 연관)

중소기업 환경에 최적화된 보안 운영 관리·대응 방안 요구

02.
AhnLab Office Security

1. AhnLab Office Security 개요
2. 솔루션 구성
3. 특장점
4. 제공 환경
5. 기능 구성
6. 주요 화면
7. Management 기능 비교

AhnLab Office Security 개요 (1/2)

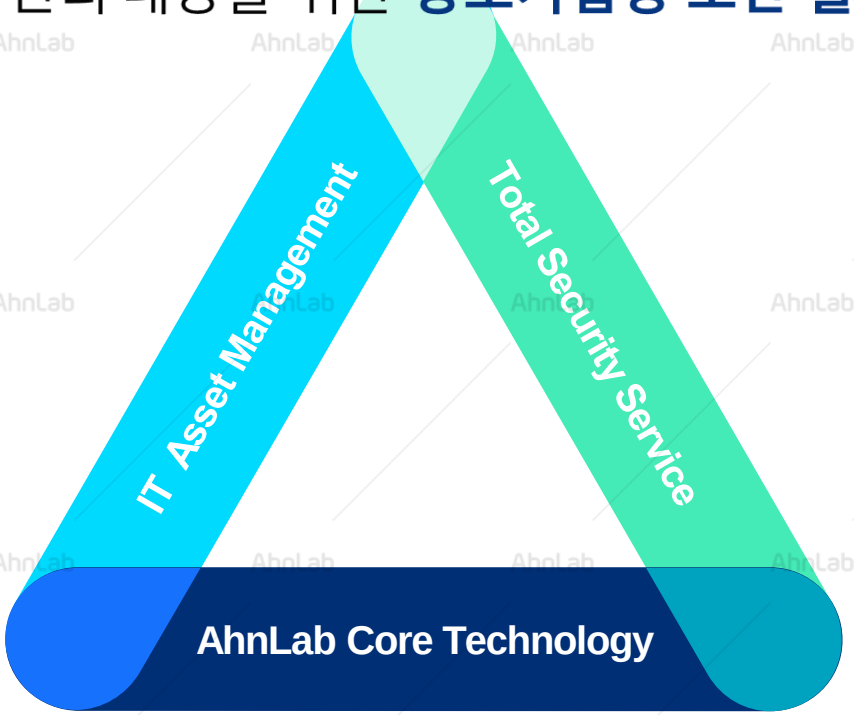
보안 위협을 사전에 예방하고, 위협 발생 시 적절히 대응하기 위해서는 보안 관리 조직 및 관리자가 꼭 필요합니다.
하지만 중소기업에서 **별도의 보안 관리 조직을 운영하기는 쉽지 않은 것이 현실**입니다.
AhnLab Office Security는 멀웨어, 해킹 차단 등 **다양한 보안 위협 예방은 물론, 기업이 보유한 다양한 기기의 보안 상태도 한눈에 관리**할 수 있습니다.

AhnLab Office Security

보안 관리·대응을 위한 **중소기업형 보안 플랫폼**

보안 관리 비용 최소화

사내 보안 관리자 없이
효율적 관리/도입 비용 최소화



보안 관리 효과 증대

긴급한 보안 위협 발생 시
신속한 대응 가능

중소기업 보안 최적화

개별 기기 보호부터
중앙 정책 관리까지 가능

AhnLab Office Security 개요 (2/2)

AhnLab Office Security는
중소기업에 최적화된 SaaS 기반의 보안 솔루션으로,
사내 기기 보안 관리를 합리적인 가격에 이용 가능하며
별도의 보안 관리자 없이도
주기적인 보고서 등을 통해 보다 쉽게
기기 보안 현황을 파악할 수 있습니다.

Devices(Client)

디바이스 보안
- 악성코드 통합 검사
- 행위/평판 기반 진단
- 보안 정책 점검 및 모니터링
- OS/MS Office 보안 패치 점검

네트워크 보안
- 개인 방화벽
- 유해/피싱 웹사이트 차단
- 네트워크 침입 차단
- 행위 기반 침입 차단

클라우드 진단
- ASD 클라우드 진단
- 평판 기반 실행 차단
- 클라우드 자동분석

PC 최적화
- 레지스트리 정리
- 브라우저 캐시 정리
- 프로그램 삭제 관리

AhnLab Office Security

Security Center

모니터링
- 클라이언트 현황
- 사내 기기 보안 위협 현황
- 기기 동작 정보
- 악성코드 감염 정보

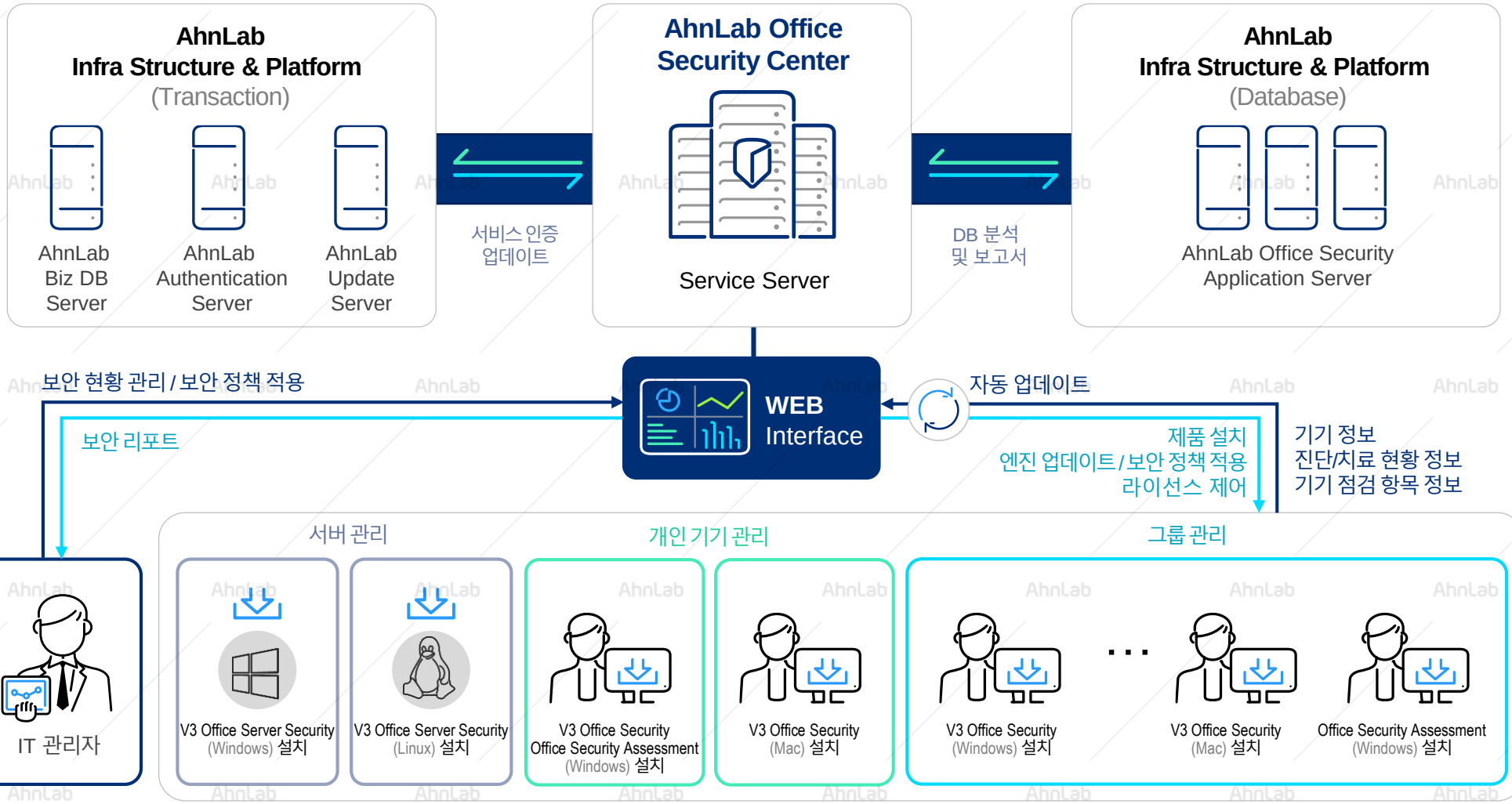
배포 관리
- 기기 배포 관리
- 사원 개별 및 전체 발송
- 사원 그룹 업데이트
- 설치 비밀번호 등 관리

보안 관리
- 그룹/제품 별 보안 정책 관리
- 기기 설치 현황
- 그룹/사원 정보 수정
- 사원 기기 상세 정보

보고서
- 기간별 요약 보고서
- 보안 위협 현황 보고서
- 악성코드 감염 현황
- 보고서 메일 설정 및 출력

AhnLab Office Security 솔루션 구성

AhnLab Office Security는 SaaS 기반 인프라를 통해
별도의 서버 구축 및 보안 관리 조직 없이 웹을 통해 손쉽게 사내 기기의 보안 현황을 관리 할 수 있습니다.



특장점 – 중소기업을 고려한 편의성

별도의 관리 서버 구축 및 보안 관리 조직의 운영이 쉽지 않은 중소기업에서도 쉽게 이해하고 사용 가능하도록 지원합니다.
보안 상태에 대한 심플한 정보 구성 및 정책 적용, 개별/통합 명령(원격 검사 및 원격 업데이트) 등이 가능하며
언제 어디서든 한눈에 보안 상태 확인 및 운영 관리가 가능하도록 웹 매니지먼트(Web Management) 환경을 제공하고 있습니다.

언제 어디서든 쉽고 편리한 보안 모니터링 환경
비전문가도 기업 보안 강화 및 운영 관리 효율성 향상

쉽고 간편한 정책 적용

PC, Laptop 보안

- **V3 Office Security** (Windows)
- **V3 Office Security** (macOS)

단말 보안 상태 관리

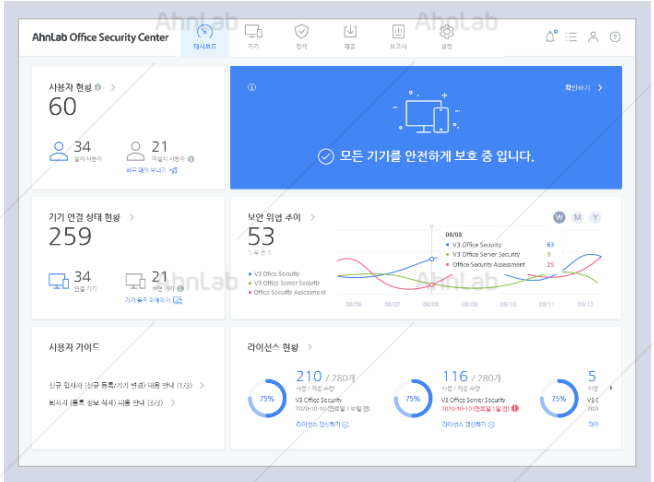
- **Office Security Assessment** (Windows)

(PC 보안 점검 솔루션)

Server 보안

- **V3 Office Server Security** (Windows Server)
- **V3 Office Server Security** (Linux Server)

한눈에 보는 직관적인 대시보드



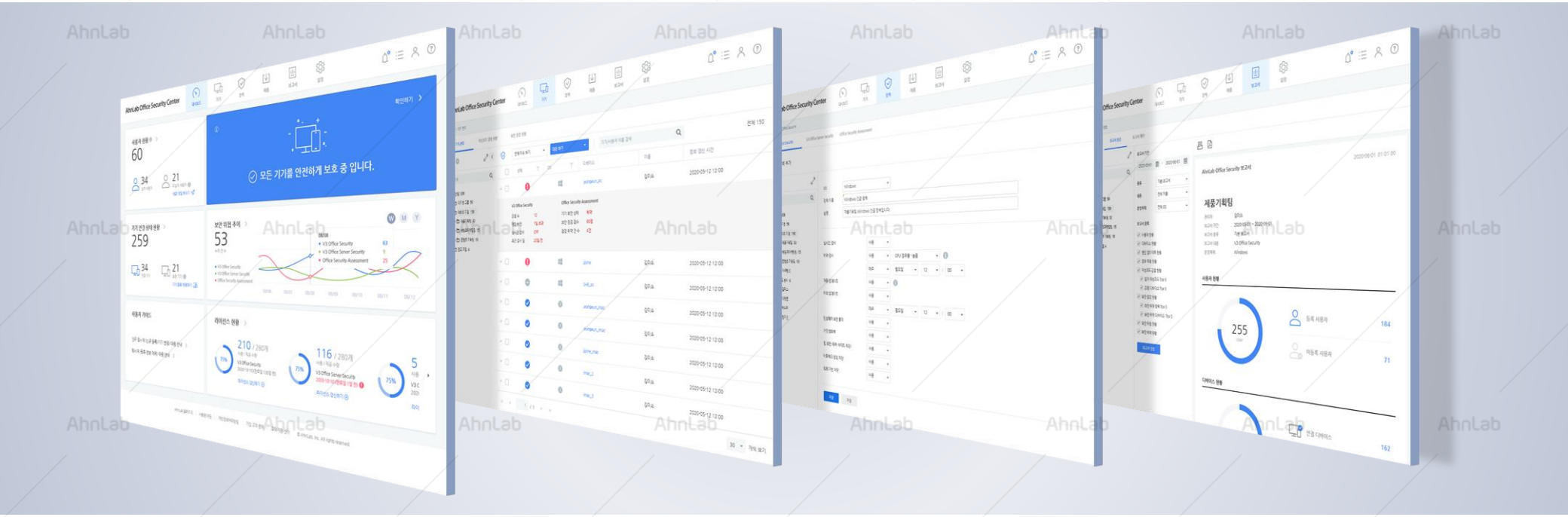
언제 어디서나 편리한 보안 관리

웹 기반 매니지먼트 제공

V3, Office Security Assessment 제품 구매 시
Office Security Center 통합 라이선스 제공

Office Security Center 제공 환경

AhnLab Office Security Center는 언제 어디서든 접속 가능한 웹 기반 매니지먼트 제공으로, 중소기업에 최적화된 관리 메뉴를 제공합니다.



AhnLab Office Security Center(Web Management) 주요 기능

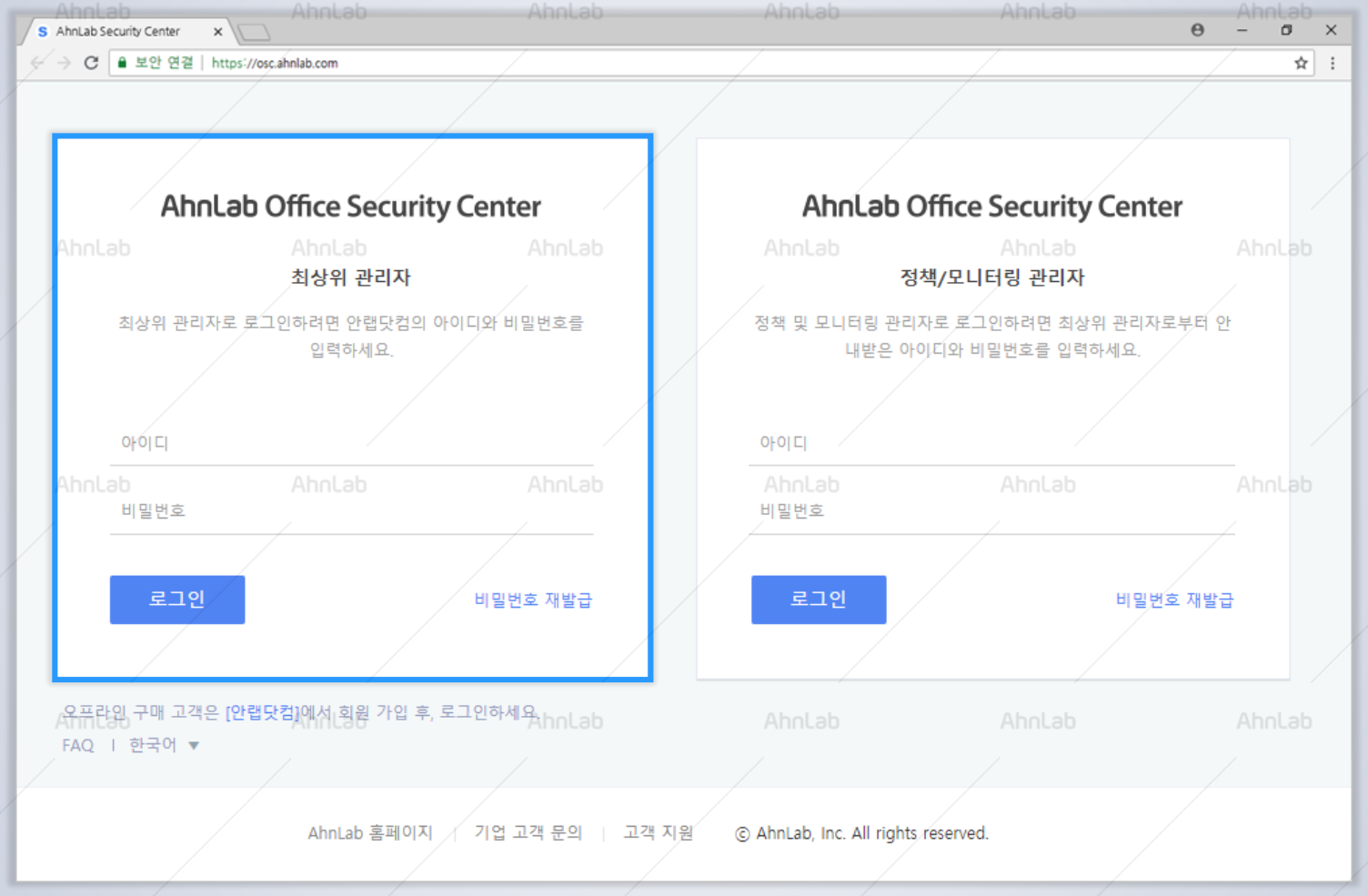
구분	상세 버전
대시보드	기기 보안 상태 및 이슈를 한눈에 확인 가능
라이선스 관리	라이선스 사용기한 및 설치 사용 수량 현황을 확인 가능
기기 관리	그룹/직원 별 PC·Server 상태 확인 및 검사/업데이트 명령 등 제공
제품 설치 관리	관리 대상 기기에 대한 제품 설치 요청 및 현황 파악 가능
보안 정책 관리	관리 대상 기기에 대한 그룹/사용자 별 보안 정책 적용 및 관리 가능
업데이트/패치 관리	안전한 상태 유지를 위한 엔진 업데이트/패치 주기 관리 가능
자동 리포트	항목/주기 설정을 통해 자동으로 현황 리포팅(E-mail) 및 파악 가능

AhnLab Office Security Center(Web Management) 운영 환경

구분	상세 버전
웹 브라우저	Internet Explorer 10 이상
	Microsoft Edge (Chromium) 83 이상
	Chrome 83 이상
	Safari 5.x 이상
지원 언어	한국어, 영어

Office Security Center 주요 화면 (1/10)

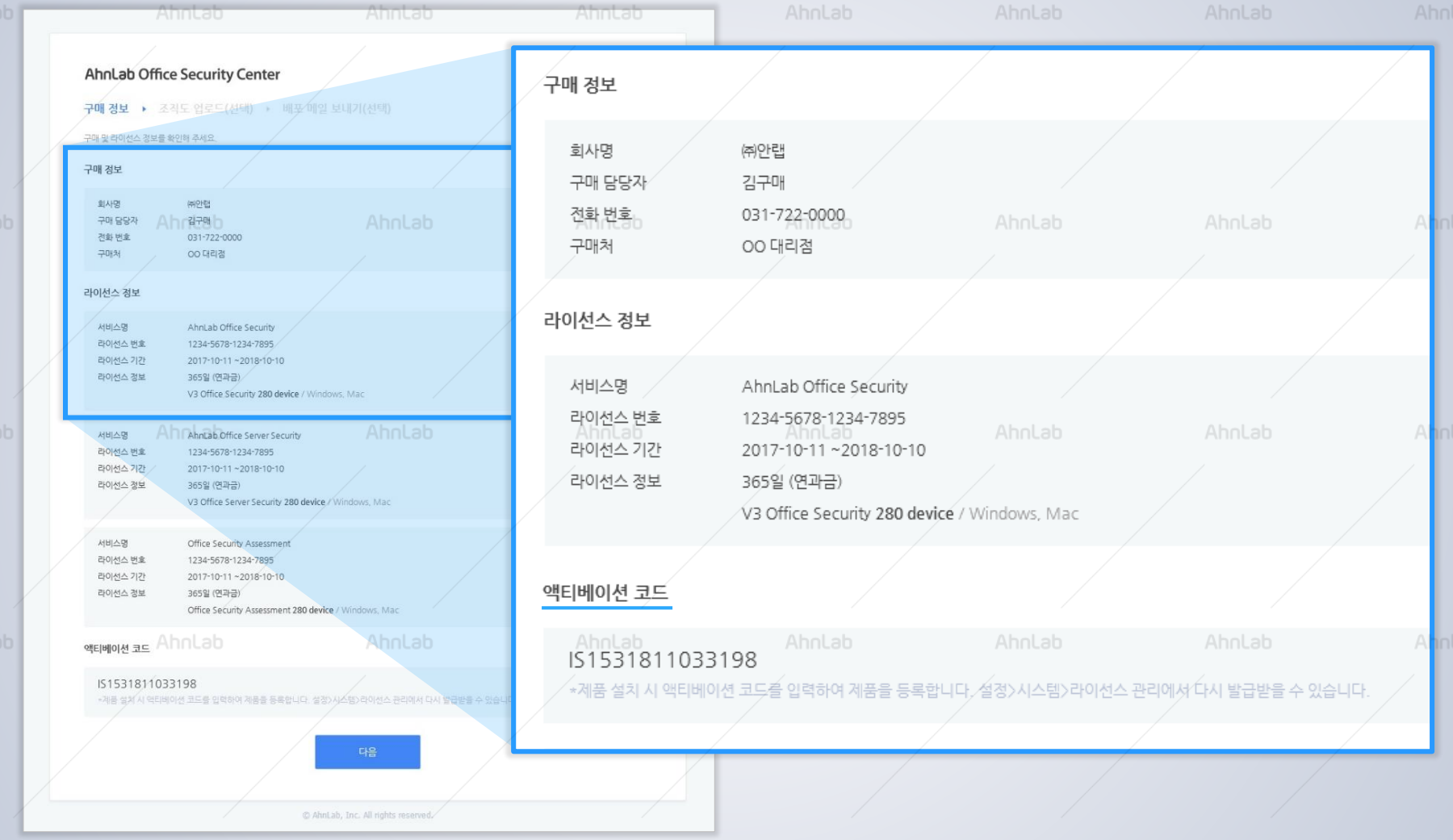
AhnLab Office Security Center 로그인 : V3 Office Security 구매 고객은 안랩닷컴(ahnlab.com) 등록 계정으로 접속 가능 합니다.



※ AhnLab Office Security Center(osc.ahnlab.com)는 솔루션 구매 후, 안랩닷컴(ahnlab.com) 회원가입 계정을 통해 로그인 사용이 가능 합니다.

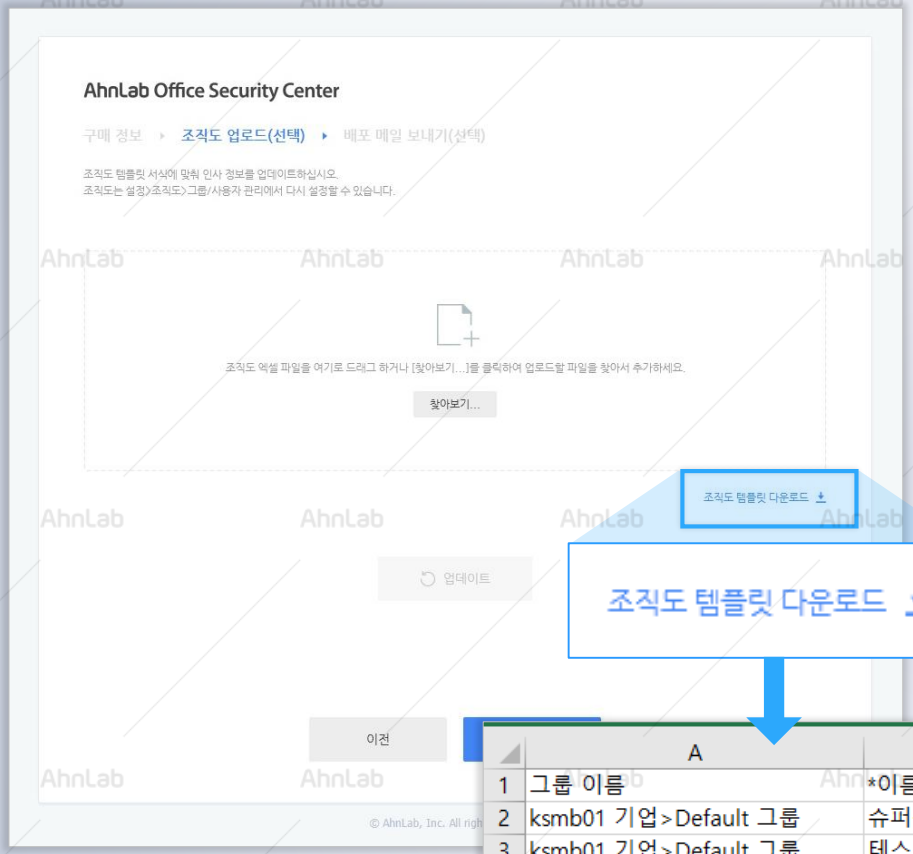
Office Security Center 주요 화면 (2/10)

솔루션 구매 정보 확인 : 솔루션 구매 라이선스 정보 및 제품 설치를 위한 '액티베이션 코드' 확인

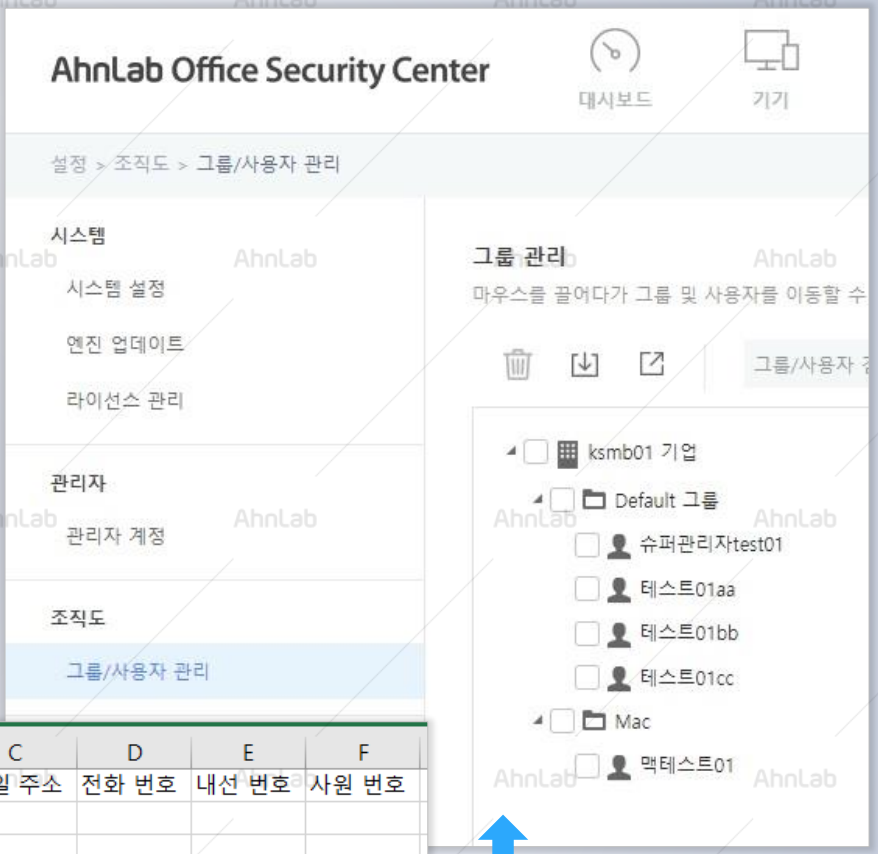


Office Security Center 주요 화면 (3/10)

기업 조직도 업로드(선택) : 템플릿 구성을 참고하여, 조직도 작성 및 업로드 합니다. 이후 작성 및 재설정 가능 합니다.

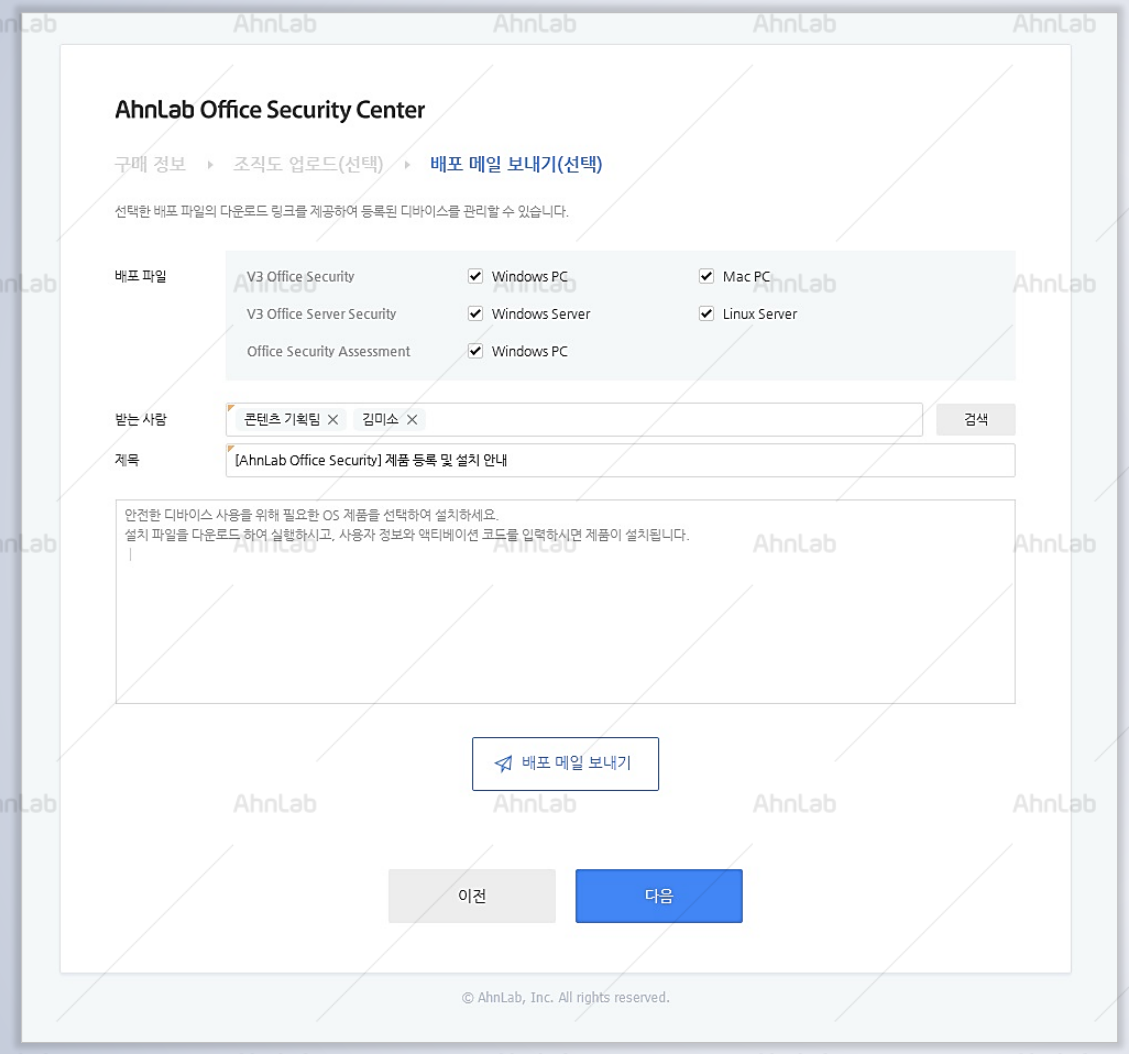


	A	B	C	D	E	F
1	그룹 이름	*이름	*메일 주소	전화 번호	내선 번호	사원 번호
2	ksmb01 기업>Default 그룹	슈퍼관리자test01				
3	ksmb01 기업>Default 그룹	테스트01aa				
4	ksmb01 기업>Default 그룹	테스트01bb				
5	ksmb01 기업>Default 그룹	테스트01cc				
6	ksmb01 기업>Mac	맥테스트01				
7						
8						



Office Security Center 주요 화면 (4/10)

사용 제품 사내 배포 하기 : 구매 라이선스 해당 제품 내에서 선택 대상 그룹 또는 직원에게 설치 요청 이메일을 발송 할 수 있습니다.

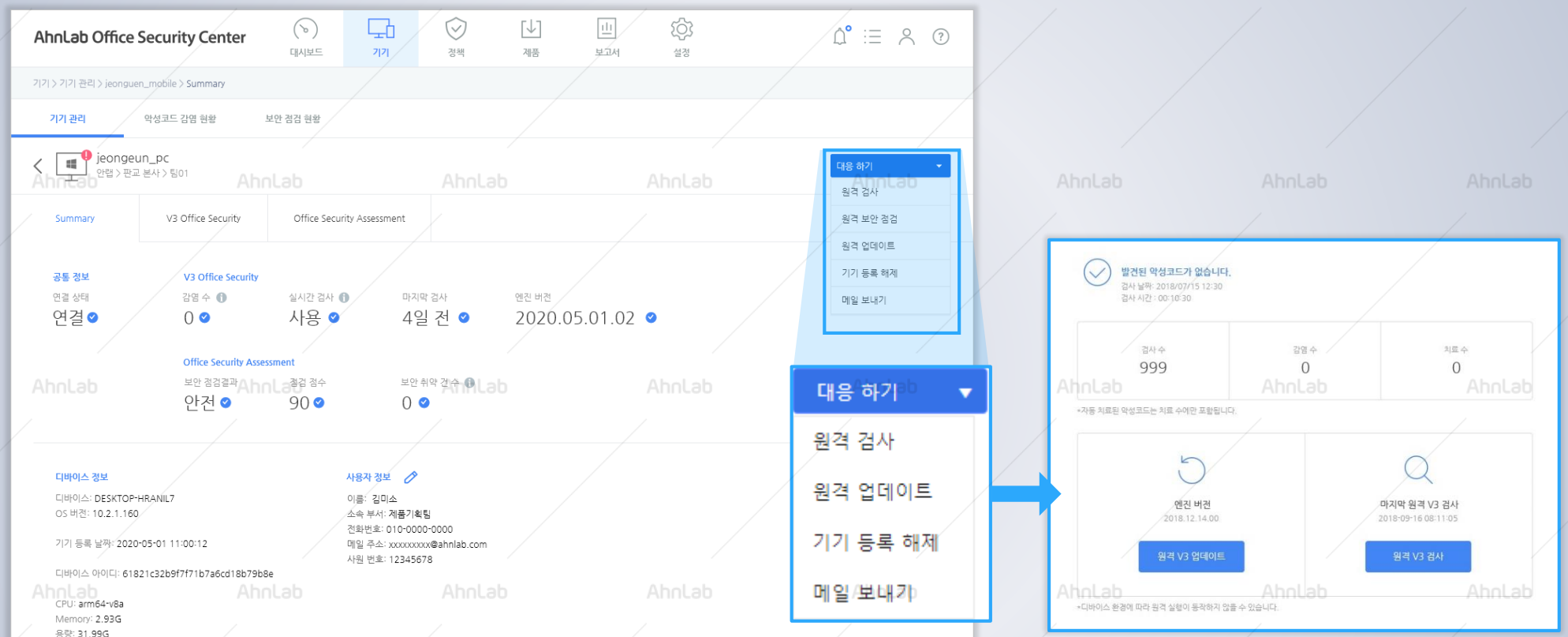


Office Security Center 주요 화면 (5/10)

Dashboard : 솔루션 설치 현황 / 기기 연결 현황 / 위협 현황 및 위협 추이 / 라이선스 현황을 한눈에 확인 및 조치 가능 합니다.

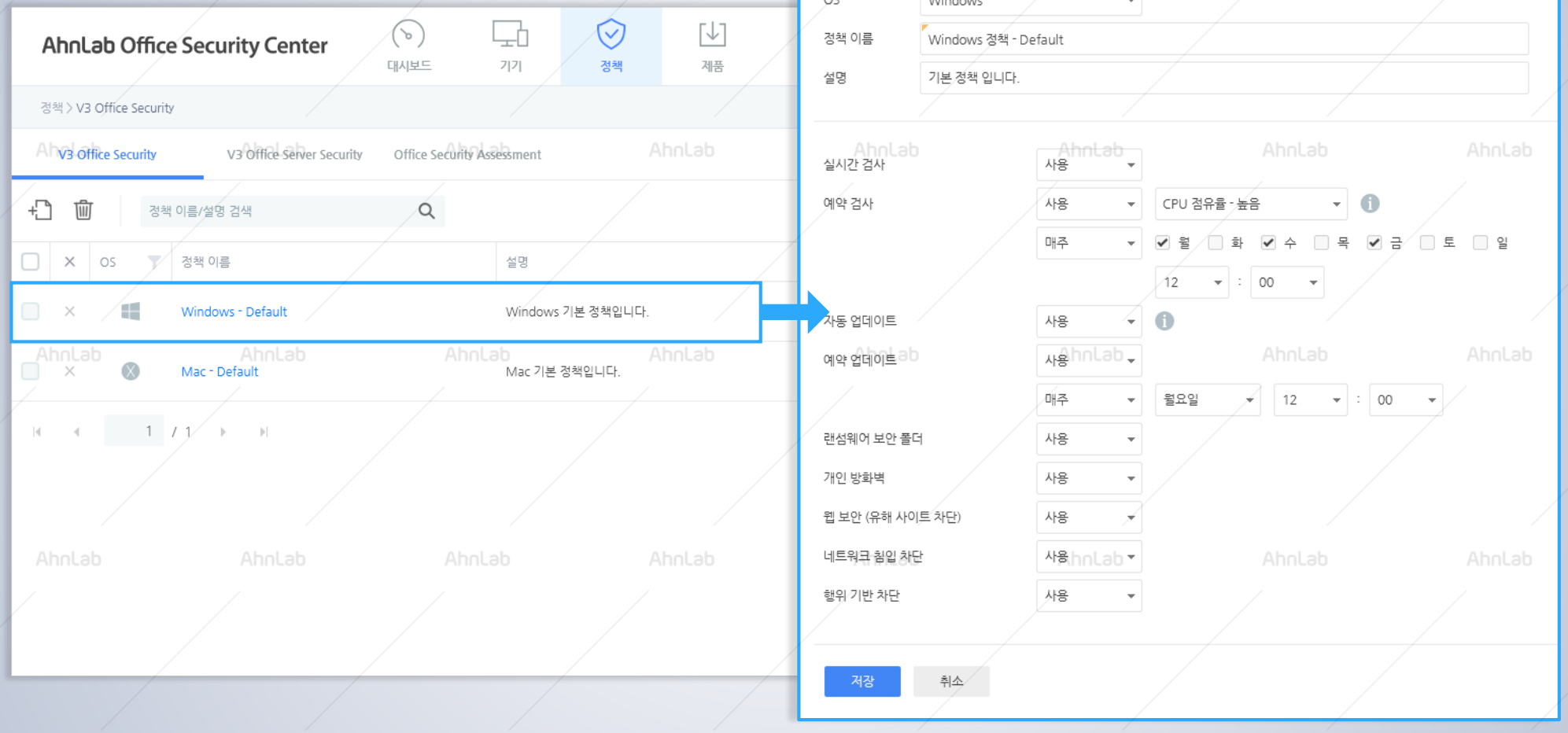
Office Security Center 주요 화면 (6/10)

기기 관리 : 그룹 및 직원 별 PC·Server 상태 확인 및 원격 검사/업데이트, 기기 등록 해제, 메일 보내기 등 관리 기능을 제공 합니다.



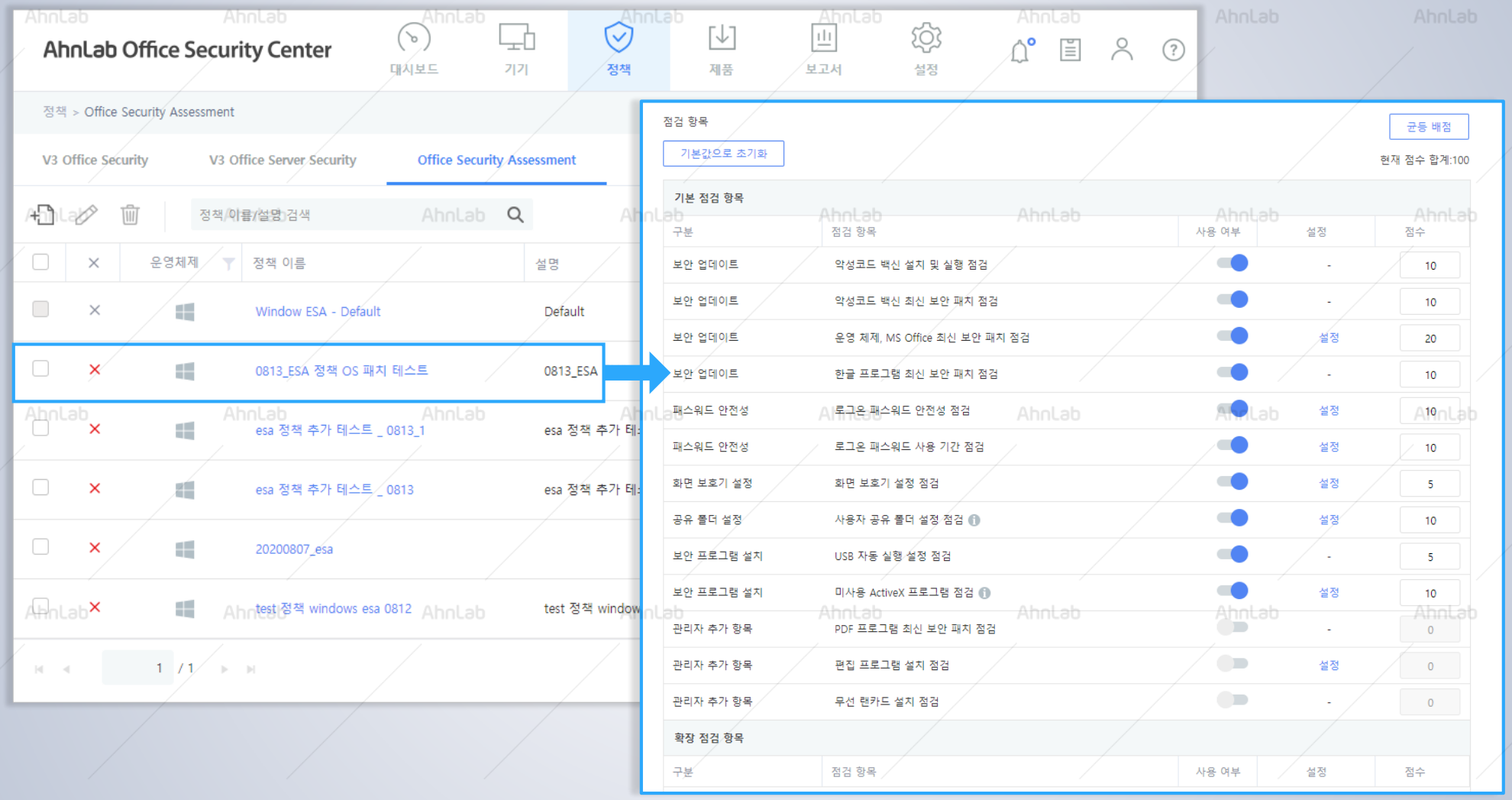
Office Security Center 주요 화면 (7/10)

보안 정책 관리 : V3 설치 대상 기기에 대한 그룹 또는 직원 별 보안 정책 적용 및 관리가 가능 합니다.



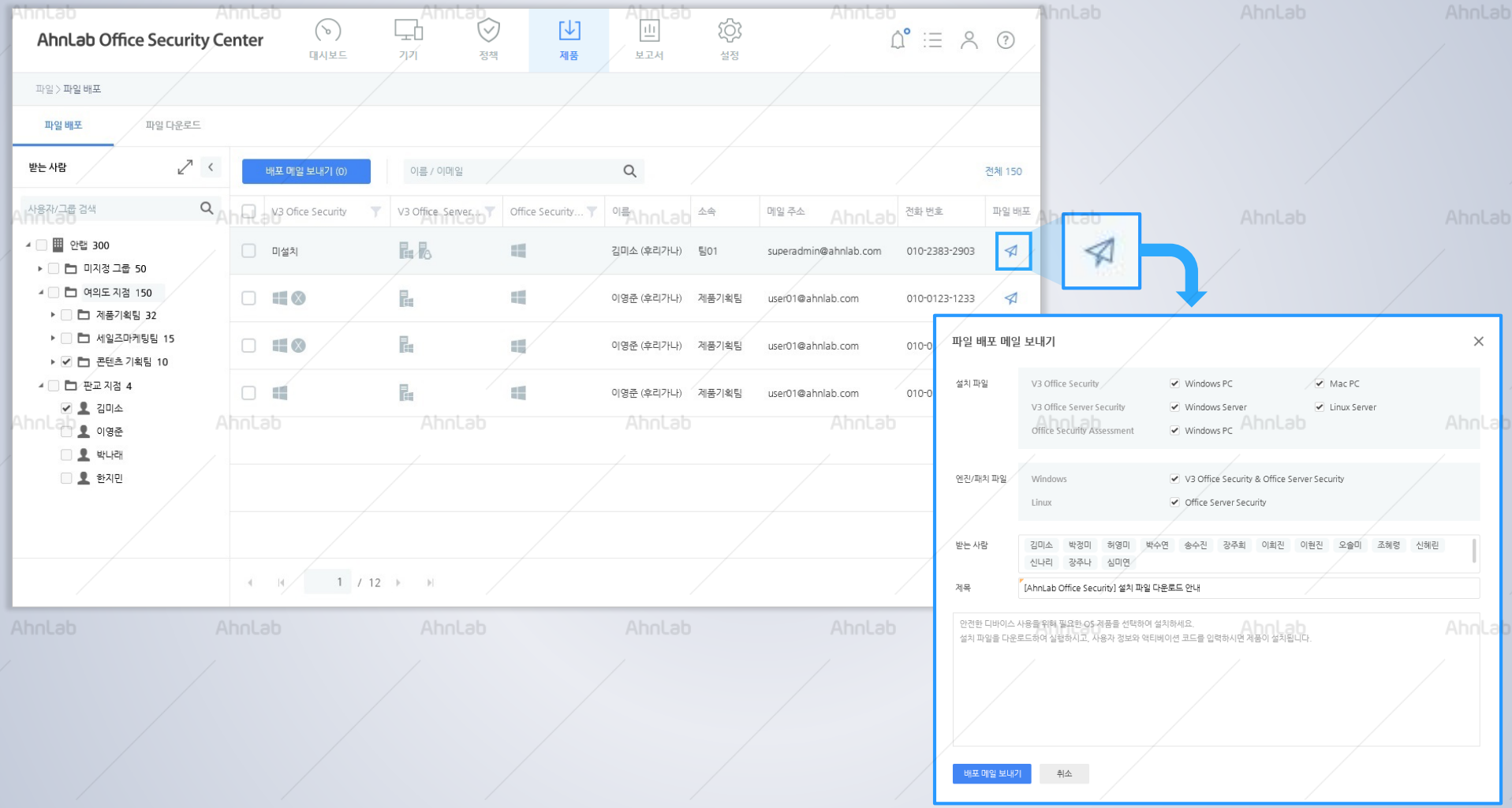
Office Security Center 주요 화면 (7/10)

보안 정책 관리 : Office Security Assessment 설치 대상 기기에 대한 그룹 또는 직원 별 보안 정책 적용 및 관리가 가능 합니다.



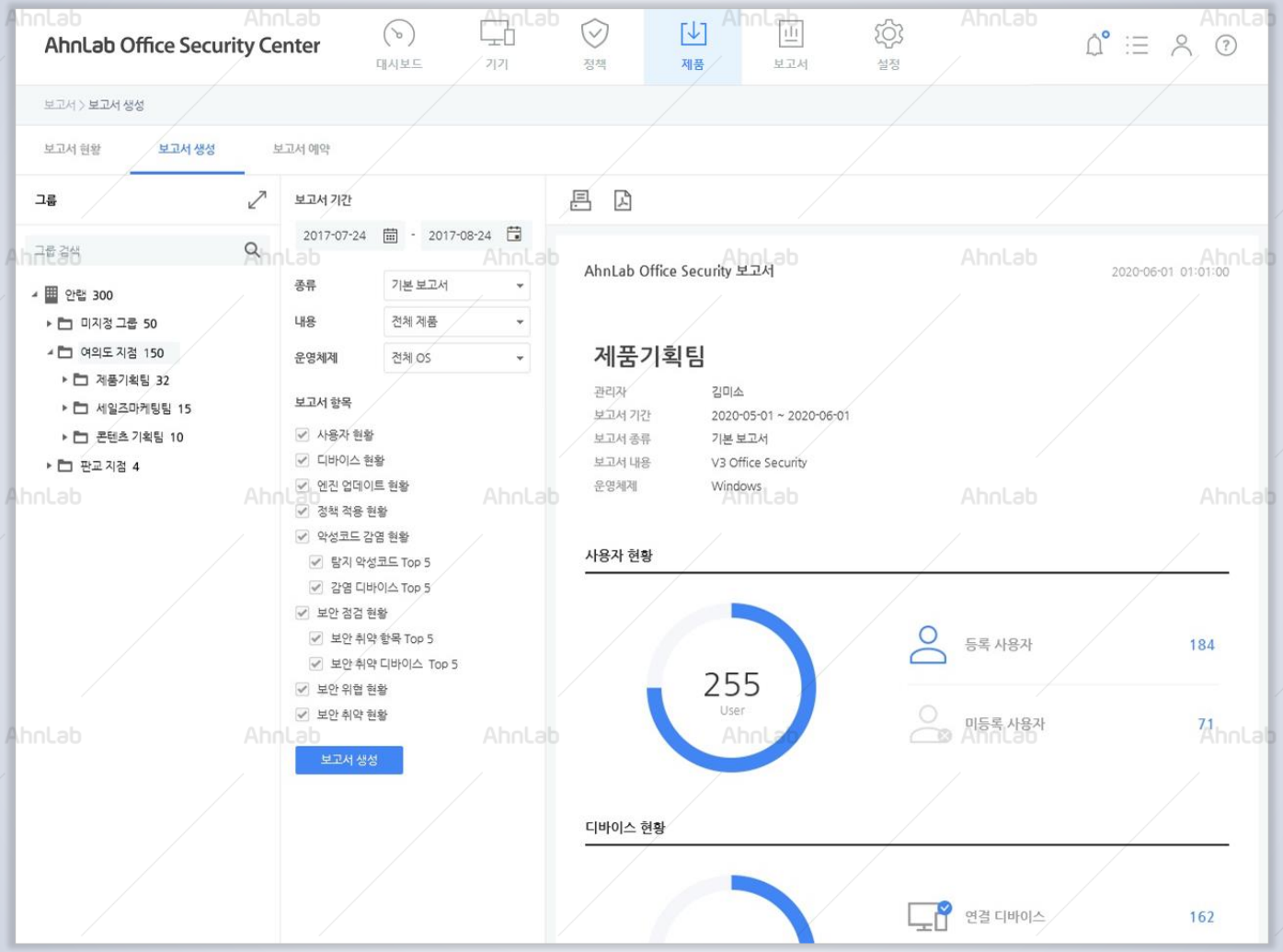
Office Security Center 주요 화면 (8/10)

제품 설치 관리 : 관리 대상 기기에 대한 보안 제품 설치 현황 파악 및 설치 요청 처리가 용이 합니다.



Office Security Center 주요 화면 (9/10)

보고서 생성 및 리포팅 : 보고서 발급 항목/주기 설정을 통해 자동으로 현황 리포팅(E-mail)을 받아볼 수 있습니다.



Office Security Center 주요 화면 (10/10)

보고서 이메일 수신 내용 : 보고서 발급 항목/주기 설정에 따라 자동으로 현황 리포팅(E-mail)을 받아볼 수 있습니다.

Management 기능 비교 (1/2)

AhnLab V3 MSS Security Center vs AhnLab Office Security Center

AhnLab Office Security는 기존 Windows Desktop 환경 외 Mac, Server 등의 멀티 OS, 멀티 디바이스를 지원하며 대응 및 관리자 보안 정책 관리를 쉽고 편하게 관리 · 운용 가능합니다.

AhnLab V3 MSS

Web 기반 관리 (운용 서버 구축 불필요)

- 웹 기반 매니지먼트로 언제 어디서든 접속/관리 가능
- V3 현황 모니터링을 위한 대시보드

AhnLab Office Security

Web 기반 관리 (운용 서버 구축 불필요)

- 웹 기반 매니지먼트 제공으로 언제 어디서든 접속/관리 가능
- 관리 대상 보안 현황 모니터링을 위한 간결한 대시보드 제공

Mobile Web 지원 예정 (2021. 1Q)

Management 기능 비교 (1/2)

AhnLab V3 MSS Security Center vs AhnLab Office Security Center

	AhnLab V3 MSS Security Center	AhnLab Office Security Center
Type	SaaS 타입 - 물리/가상화 별도 운용 서버 구축 불필요	SaaS 타입 - 물리/가상화 별도 운용 서버 구축 불필요
관리 콘솔	Web 로그인만으로 매니지먼트 접속 - 웹 기반 매니지먼트로 언제 어디서든 접속/관리 가능 - V3 현황 모니터링을 위한 대시보드	Web 로그인만으로 매니지먼트 접속 - 웹 기반 매니지먼트 제공으로 언제 어디서든 접속/관리 가능 - 관리 대상 보안 현황 모니터링을 위한 간결한 대시보드 제공
관리 제품	V3 MSS (Windows) 제품의 제한적 관리	V3 Office Security : Windows, Mac 백신 V3 Office Server Security : Windows Server, Linux Server 백신 Office Security Assessment : Windows 취약점 점검 솔루션 향후 추가 솔루션 연동 가능
정책 설정	V3 백신 제품 정책만 설정	그룹/직원 기기 별 '관리 제품' 정책 설정 가능 - 안전/감염/취약/휴면 기기 별 원격 검사, 업데이트 및 관리자 메일 발송 가능
대상 운영	그룹/직원 Windows 기기 대상 운용	그룹/직원 Windows, Mac 및 서버 대상 직관적 운용
관리 제품 패치	대상 기기 자동으로 제품 최신 패치 업데이트	대상 기기 자동으로 제품 최신 패치 업데이트
매니지먼트 패치	항상 최신 상태 유지	항상 최신 상태 유지
보고서	최근 2개월 내 그룹/PC별 백신 설정 상태 및 악성코드 현황 확인 보고서 자동 생성 및 이메일링 미제공	1년 내 캘린더 형태의 스냅샷 보고서 생성으로 시점 별 데이터 추이 분석 가능 그룹/제품/운영체제 설정에 따른 보고서 생성 가능 일별, 주별, 월별 설정에 따른 보고서 자동 생성 및 이메일링 제공

Management 기능 비교 (1/2)

AhnLab V3 MSS Security Center vs AhnLab Office Security Center

메인 메뉴	세부 메뉴	V3 MSS Security Center	Office Security Center	설명
동작 환경	웹 매니지먼트	IE 10 이상	●	Internet Explorer 10 이상 / Microsoft Edge (Chromium) 83 이상 / Chrome 83 이상 / Safari 5.x 이상
	지원 언어	한글	●	한글, 영어
대시 보드	사용자/기기 현황	●	●	구성된 조직 구성에 따라 보안 제품이 설치된 사용자와 설치하지 않은 사용자 수 표시
	기기 연결 상태	●	●	등록된 기기의 정상 연결 상태 및, 휴면 기기 상태 수 표시
	취약 현황	●	●	감염 기기 수, 오래된 엔진 버전 사용 수, 실시간 검사가 해제된 기기에 따른 안전/취약 여부 표시
	보안 상태 알림		●	안전/취약 여부 상태 표기
	보안 위협 추이	●	●	사용 제품 대상, 보안 위협 추이 그래프
	예약 작업 현황		●	서버 관리자가 에이전트에게 내린 예약 작업의 종류와 기간별 진행 상태, 각 작업 별 상태 정보를 확인
	라이선스 사용 현황	●	●	라이선스 만료 및 사용 상태 표시
기기	기기 관리	●	●	기기 연결 상태, OS 정보, 취약점 정보(감염 기기 수, 오래된 엔진 실시간 검사 사용 안 함) 요약과 기기 목록 표시
	악성코드 감염 상황	●	●	기기의 OS 별 악성 코드 감염 여부, 탐지 악성 코드 표시
	기기 취약점 점검		●	OSA 제품 사용 시, 기기 취약점 점검 여부, 취약 상태 표시
	엔진 업데이트 현황	●	●	기기의 OS 별 엔진 업데이트 현황 표시
	원격 명령 실행		●	엔진 업데이트 및 원격 검사(점검) 명령 실행 가능
	검사/이벤트 로그		●	원격 명령 실행에 따른 검사/이벤트 로그
정책	정책 설정	●	●	설정된 정책 목록이 표시됩니다. 새 정책을 만들거나 편집 가능 (* 기본 정책 설정은 변경 불가)
제품	설치 파일 배포	●	●	조직도에 등록된 사용자 지정 후 설치 파일 배포 메일링 가능
	설치 파일 다운로드	●	●	활성화 코드의 복사와 OS 유형별 설치 파일을 다운로드 가능
보고서	보고서 현황		●	메일로 전송된 보고서 확인 가능 (보고서는 최대 1 년간 저장)
	보고서 생성	●	●	조직도에서 대상을 선택하고 제출 보고서의 표시 항목을 설정하여 생성 가능 (* 기본 보고서 항목 설정은 변경 불가)
	보고서 항목 설정		●	사용자, 기기, 엔진 업데이트, 정책 적용, 악성코드 감염, 보안 점검, 위협, 취약 현황 항목 설정 가능
	보고서 예약		●	작성한 보고서의 제출 시간 예약 가능 (* 기본 보고서 항목 설정은 변경 불가)
설정	시스템 설정		●	로그인 설정, 설치 파일 배포 기본 설정, 휴면 기기, 최근 검사 관리 설정 가능
	엔진 업데이트		●	최신 또는 Stable 엔진 업데이트 적용 여부를 설정 가능
	라이선스 관리	●	●	사용중인 기기 상태 및 라이선스에 대한 자세한 정보 확인.
		●	●	사용 가능한 라이선스를 초과하거나 만료 된 경우, 라이선스 갱신을 위한 구매 정보 확인 가능
	관리자 계정	●	●	최고 관리자는 정책 관리자 / 모니터링 관리자 지정 가능 (* 최고 관리자 변경은 안랩닷컴 계정 연동 됨. 변경 시 별도 문의 필요)
	그룹 / 사용자 관리	●	●	그룹 사용자 관리를 위해 목록 가져오기 기능 (xlsx) 조직도 등록/관리 (* 조직도는 최대 5단계까지 구성 가능 (* 그룹 정보가 없는 사용자는 자동으로 Default 그룹으로 지정.)
	알림 설정		●	다양한 상황의 알림 통지 대상 설정 가능 (*알림 통지 대상은 관리자만 가능)

Management 기능 비교 (2/2)

APC 4.6 for Windows vs AhnLab Office Security Center

기업 보안 환경 마련 시 어렵고 복잡했던 정책 관리를 쉽고 편하게 관리 · 운용이 가능합니다.

AhnLab Policy Center 4.6 for Windows

C/S 기반 (별도 콘솔 프로그램 구매 설치)

- 보안 관리 운용을 위한 서버 세팅 필요
- 서버 용량 초과 시 하위 도메인 서버 추가 증설 필요
- Windows 콘솔 프로그램 설치 환경에서만 운용 가능

AhnLab Office Security

Web 기반 관리 (운용 서버 구축 불필요 / 제품 통합 라이선스)

- 언제 어디서든 접속/관리 가능한 웹 매니지먼트 제공
- 관리 대상 보안 현황 모니터링을 위한 간결한 대시보드 및 운용

Mobile Web
지원 예정
(2021. 1Q)

Management 기능 비교 (2/2)

APC 4.6 for Windows vs AhnLab Office Security Center

	AhnLab Policy Center 4.6 for Windows	AhnLab Office Security Center
Type	S/W 타입 - Windows O/S, MSSQL 사용 - 2021.06 재계약 종료, 2022.06 서비스 종료 S/W 기반 상위-하위 도메인 구성 (Top-Down 방식)	SaaS 타입 - 물리/가상화 별도 운용 서버 구축 불필요
관리 콘솔	Windows C/S 기반 (콘솔 프로그램 설치/ 특정 포트 방화벽 오픈)	Web 로그인만으로 매니지먼트 접속 - 웹 기반 매니지먼트 제공으로 언제 어디서든 접속/관리 가능 - 관리 대상 보안 현황 모니터링을 위한 간결한 대시보드 제공
관리 제품	V3 백신 제품군 설치/관리	V3 Office Security : Windows, Mac V3 Office Server Security : Windows Server, Linux Server Office Security Assessment : Windows 취약점 점검 솔루션 향후 추가 솔루션 연동 가능
정책 설정	V3 백신 제품 정책만 설정 - 안전/감염/취약 기기 별 원격 검사, 업데이트 제어 가능	'관리 제품' 별 정책 설정 가능 - 안전/감염/취약/휴면 기기 별 원격 검사, 업데이트 및 관리자 메일 발송 가능
대상 운영	IP 기반 관리 대상 기기 운용	그룹/직원 Windows, Mac 및 서버 대상 직관적 운용
관리 제품 패치	관리 서버 → 에이전트 보안패치 배포	대상 기기 자동으로 제품 최신 패치 업데이트
매니지먼트 패치	신규 업데이트 시 콘솔 프로그램 업데이트 필요	항상 최신 상태 유지
보고서	Raw-data 현황 보고서 출력	1년 내 캘린더 형태의 스냅샷 보고서 생성으로 시점 별 데이터 추이 분석 가능 그룹/제품/운영체제 설정에 따른 보고서 생성 가능 일별, 주별, 월별 설정에 따른 보고서 자동 생성 및 이메일링 제공

Management 기능 비교 (2/2)

APC 4.6 for Windows vs AhnLab Office Security Center

메인 메뉴	세부 메뉴	APC 4.6 for Win	Office Security Center	설명
동작 환경	웹 매니지먼트		●	Internet Explorer 10 이상 / Microsoft Edge (Chromium) 83 이상 / Chrome 83 이상 / Safari 5.x 이상
	C/S 운용 서버	●		Windows Server 2008 / 2012 (공통 사항: R2 포함) Windows Server 2016 / 2019 Windows Vista / 7 / 8(8.1) / 10
	Agent 연동	●	미제공	에이전트를 통한 기기 상태 현황, 검사/업데이트 제어, 예약 동작 및 공지 기능 보조 업데이트 서버 설정: 패치 및 배포를 위한 보조 업데이트 서버 설정 기능 공유 폴더 관리: 자산 내 연결된 공유 폴더 관리 자산 관리 (HW/SW): Agent 설치된 자산의 HW/SW 정보 확인 시스템 최적화 관리: PC 내 시스템 최적화 기능(브라우저 캐쉬 삭제, 레지스트리 청소 등) 네트워크 완전 차단: V3의 방화벽 설정이 되어 있는 경우에 지원 가상 그룹: 특정 그룹에 대해 가상 그룹을 설정하여, 제품 배포/정책 설정 가능
	지원 언어	●	●	한글, 영어
대시 보드 (메인 화면)	에이전트 현황	●	●	에이전트의 설치 정보, 사용자 정보, 정책 적용 현황, 공유 폴더 정보 등을 확인
	보안 제품 현황	●	●	에이전트에 설치된 관리 대상 보안 제품의 현황을 확인
	엔진 업데이트 현황	●	●	에이전트의 업데이트를 현황을 확인
	감염 바이러스/스파이웨어 현황	●	●	감염된 바이러스와 스파이웨어 현황의 순위 정보를 확인
	바이러스별 감염 순위 현황	●	●	감염된 바이러스의 순위 정보를 일간, 주간, 월간 별로 구분하여 확인
	에이전트 악성코드 감염 현황	●		악성코드에 감염된 에이전트의 현황을 일간, 주간, 월간 별로 구분하여 확인
	에이전트별 바이러스 감염 현황	●		바이러스에 감염된 에이전트의 현황을 바이러스 진단 방법에 따라 구분하여 확인
	예약 작업 현황	●	●	서버 관리자가 에이전트에게 내린 예약 작업의 종류와 기간별 진행 상태, 각 작업 별 상태 정보를 확인
	정책 적용 현황	●	정책 설정에 포함	에이전트에 적용된 정책에 대한 현황 정보를 확인
	라이선스 사용 현황	●	●	라이선스 만료 및 사용 상태 표시

Management 기능 비교 (2/2)

APC 4.6 for Windows vs AhnLab Office Security Center

메인 메뉴	세부 메뉴	APC 4.6 for Win	Office Security Center	설명
기기	기기 관리	●	●	기기 연결 상태, OS 정보, 취약점 정보(감염 기기 수, 오래된 엔진 실시간 검사 사용 안 함) 요약과 기기 목록 표시
	V3 환경설정 관리	●	▲	V3 환경설정 (PC보안/네트워크 보안/Active Defense/사용환경 설정) 제어 관리
	악성코드 감염 상황	●	●	기기의 OS 별 악성 코드 감염 여부, 탐지 악성 코드 표시
	기기 취약점 점검		●	Office Security Assessment 제품 사용 시: 기기 취약점 점검 여부, 취약 상태 표시
	엔진 업데이트 현황	●	●	기기의 OS 별 엔진 업데이트 현황 표시
	원격 명령 실행	●	●	엔진 업데이트 및 원격 검사(점검: OSA 제품) 명령 실행 가능
	검사/이벤트 로그	●	●	원격 명령 실행에 따른 검사/이벤트 로그
	장치제어 이벤트	●		기기에 연결되는 주변 장치를 통한 악성코드 감염 예방을 위해 장치 별 사용 여부 허용/차단 기능
	자산 변경 이력	●		S/W와 H/W의 변경 이력 확인 기능
	사전 방역	●		사내에 악성코드가 전파되는 것을 방지하기 위해 네트워크 차단을 통한 사전 방역 기능
	관리 IP 주소 범위 설정	●		서버의 IP 관리 범위를 지정하는 기능
	데이터베이스 백업	●		서버의 데이터베이스 백업 하는 기능
	기기 무결성 검사	●		기기 설치 디렉터리에 대한 파일 무결성 검사 기능
	도메인 설정/동기화	●		하위 도메인 설정 및 정책 동기화를 위한 기능
	로그 출력 기능	●		특정 기간을 설정하여 서비스, 에이전트 이벤트, 감염 경고 등 로그를 엑셀파일 형태로 출력 가능
정책	정책 설정	●	●	설정된 정책 목록이 표시됩니다. 새 정책을 만들거나 편집 가능 (* 기본 정책 설정은 변경 불가)
제품	설치 파일 배포	●	●	조직도에 등록된 사용자 지정 후 설치 파일 배포 메일링 가능
	설치 파일 다운로드	●	●	활성화 코드의 복사와 OS 유형별 설치 파일을 다운로드 가능
보고서	보고서 현황	●	●	배포 정보, 제품 정보, 감염 정보, 사용자 정의 보고서 생성 및 보고서 검색 기능 제공
	보고서 생성	●	●	조직도에서 대상을 선택하고 제출 보고서의 표시 항목을 설정하여 생성 가능 (* 기본 보고서 항목 설정은 변경 불가)
	보고서 항목 설정	●	●	사용자, 기기, 엔진 업데이트, 정책 적용, 악성코드 감염, 보안 점검, 위협, 취약 현황 항목 설정 가능
	보고서 예약	●	●	작성한 보고서의 제출 시간 예약 가능 (* 기본 보고서 항목 설정은 변경 불가)
설정	시스템 설정	●	●	로그인 설정, 설치 파일 배포 기본 설정, 휴면 기기, 최근 검사 관리 설정 가능
	엔진 업데이트	●	●	최신 또는 Stable 엔진 자동/수동 업데이트 여부를 설정 가능 서버와 Agent(제품)간 통신이 원활하지 않을 경우를 대비한 보조 업데이트 서버 설정 가능
	라이선스 관리	●	●	사용중인 기기 상태 및 라이선스에 대한 자세한 정보 확인.
		●	●	사용 가능한 라이선스를 초과하거나 만료 된 경우, 라이선스 갱신을 위한 구매 정보 확인 가능
	관리자 계정	●	●	관리자 권한 구분 (서버 관리자, 정책 관리자, 일반 관리자, 사용자 정의 관리자, 라이선스 별 관리자)
	그룹 / 사용자 관리	●	●	그룹 사용자 관리를 위해 목록 가져오기 기능 조직도 등록/관리 (* 조직도는 최대 15단계까지 구성 가능 (* 그룹 정보가 없는 사용자는 자동으로 Default 그룹으로 지정.)
	알림 설정	●	●	다양한 상황의 알림 통지 대상 설정 가능 (*알림 통지 대상은 관리자만 가능)

03.
구성 제품

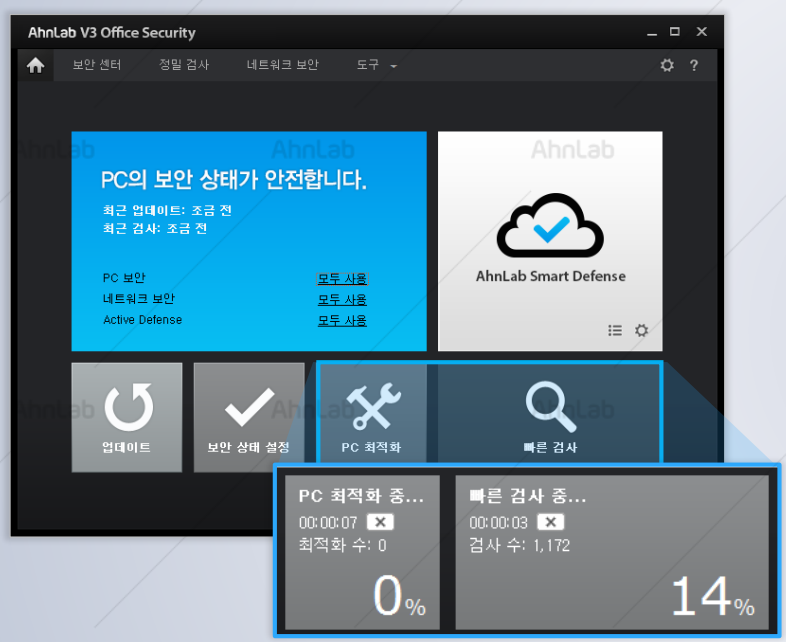
1. V3 Office Security (Windows/macOS)
2. V3 Office Server Security (Windows/Linux Server)
3. Office Security Assessment (Windows)
4. 구성 제품 운영 환경

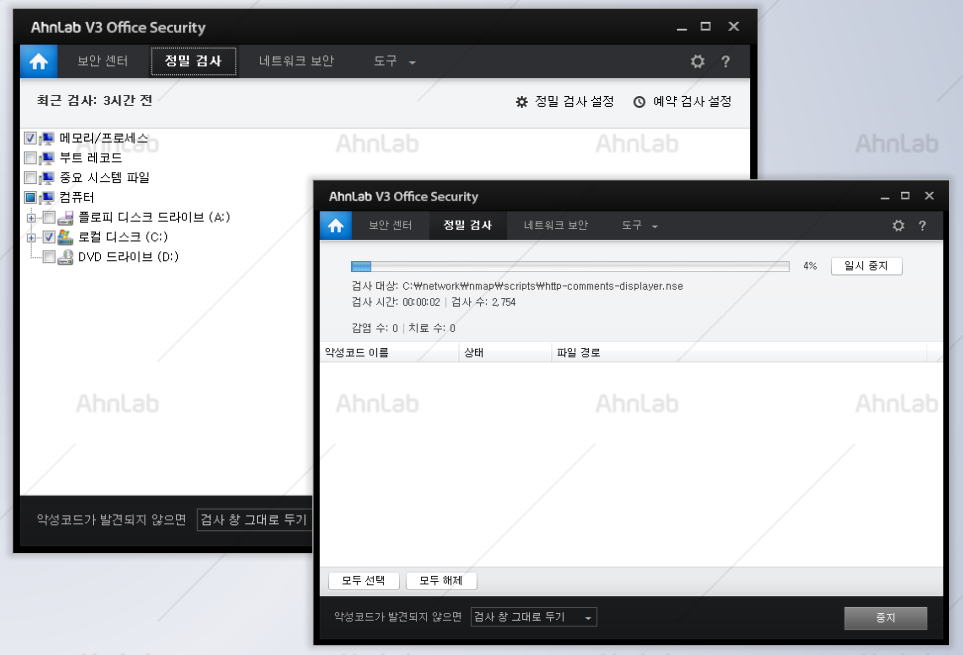
[Desktop] V3 Office Security (Windows) 주요 기능

악성코드 검사 및 치료, 진단 영역 확대 및 사전 방어

바이러스, 웜, 해킹은 물론 스파이웨어까지 인터넷을 통해 전파되는 각종 악성코드에 대해 완벽한 통합 검사, 치료, 실시간 검사를 진행함으로써 보안 위협으로부터 회사의 PC를 안전하게 보호합니다.

- 바이러스에서 스파이웨어까지 각종 악성코드에 대한 통합 보안
- 빠른 검사, 정밀 검사, 스마트 스캔, 사용자 정의 검사 등 사용자 편의를 고려한 다양한 검사 제공
- 행위/평판 기반 진단, 클라우드 진단을 통한 보안 위협 사전 방어
- PUP(불필요한 프로그램) 진단, 평판이 낮은 프로그램 진단 등을 통한 중요 시스템 보호
- 메인 화면에서 최적화, 빠른 검사 등 프로세스 진행



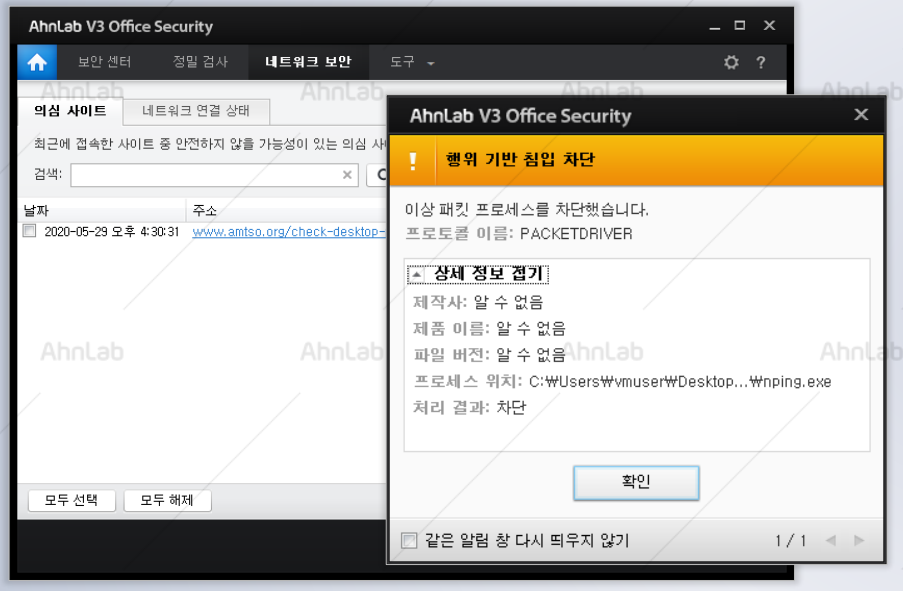


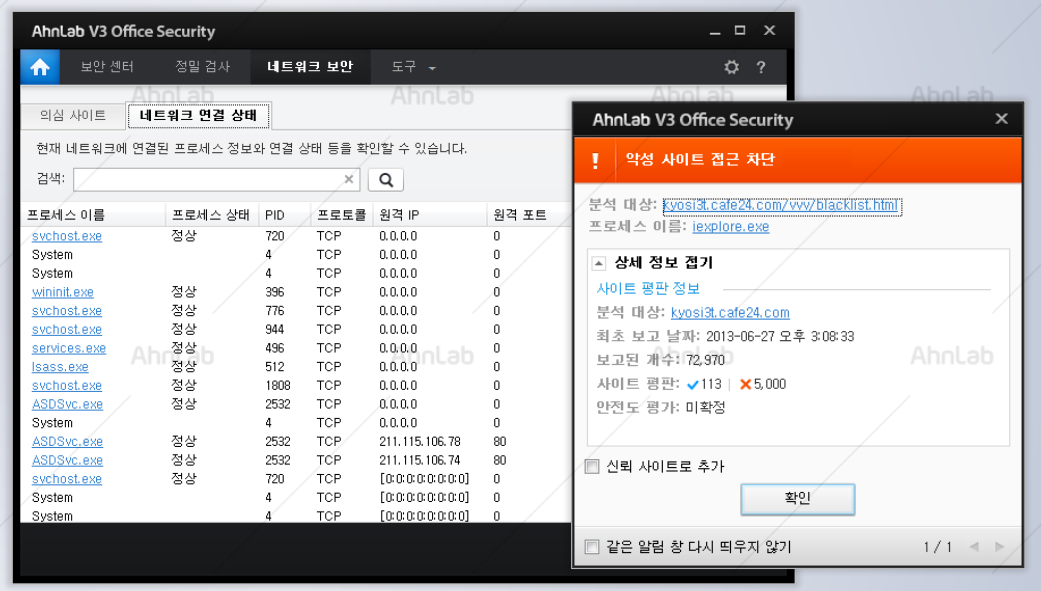
[Desktop] V3 Office Security (Windows) 주요 기능

개인 방화벽과 네트워크 침입 차단 설정을 통한 해킹 차단, 강력한 웹 보안

알려진 포트나 패킷을 통한 네트워크 침입을 차단하는 기능과 달리, 네트워크의 위협 방어를 위한 기능으로 알려지지 않은 프로토콜 드라이버 차단, 이상 트래픽 차단, IP 스푸핑, MAC 스푸핑, ARP 스푸핑 탐지 등이 가능합니다.

- 개인 방화벽(네트워크 완전 차단, 신뢰 프로그램 판단 기준 설정, 방화벽 정책 목록, 포트 숨김)
- 유해 웹 사이트, 피싱 사이트, PUS(불필요한 사이트) 차단
- 서명 기반 네트워크 침입 차단(허용/차단 IP 사용, 공격자 IP 임시 차단)
- 행위 기반 네트워크 침입 차단(Unknown Protocol Driver 방어, 이상 트래픽 방어, IP/MAC/ARP 스푸핑 방어)
- 포트 차단(포트 차단 방식, 예외 포트 사용, 포트 차단 규칙 관리)
- 신뢰할 수 있는 IP와 차단해야 할 IP 등록



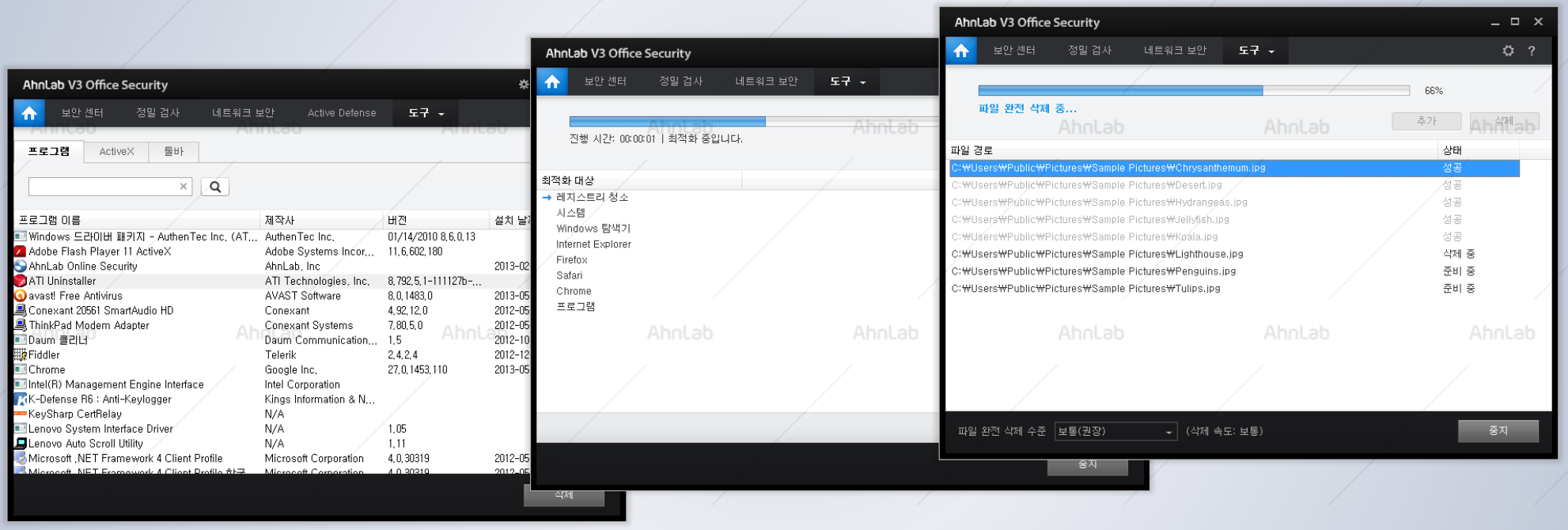


[Desktop] V3 Office Security (Windows) 주요 기능

PC 최적화 및 프로그램/ActiveX/툴바 관리, 파일 완전 삭제를 통한 개인정보 유출 방지

PC 최적화를 통해 메모리 사용과 인터넷 연결 속도를 향상 시킬 수 있으며 PC 관리 메뉴를 통해 불필요하게 설치된 프로그램과 ActiveX, 툴바를 손쉽게 확인 및 처리할 수 있습니다.
보안상 중요한 파일이나 자신의 개인적 문서를 삭제하고자 할 때에는 파일 완전 삭제를 통해 보안 강화를 꾀할 수 있습니다.

- PC 최적화(Internet Explorer, Firefox, Opera, Safari, Chrome 지원)
- 프로그램 관리 / Active X 관리 / 툴바 관리
- 파일 완전 삭제

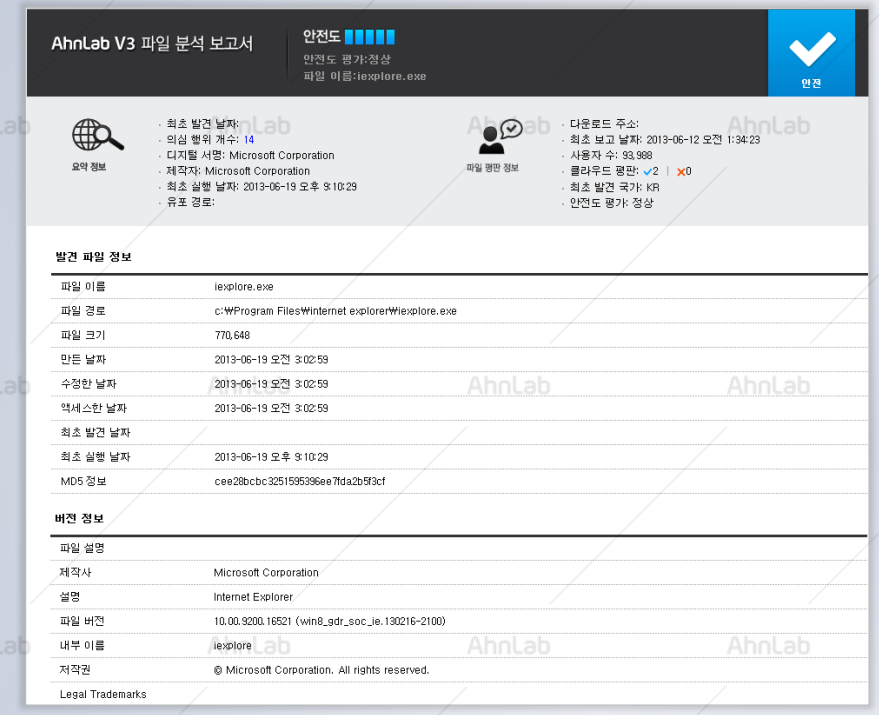


[Desktop] V3 Office Security (Windows) 주요 기능

고급 사용자를 위한 Active Defense 파일/URL 보고서

생성 파일 및 프로세스에 대한 분석 보고서를 통해, 사용자 자신이 보안 상태를 확인 이용 가능 합니다.

- 파일 / URL에 대한 상세 리포트 제공



AhnLab V3 파일 분석 보고서

안전도

안전도 평가:정상

파일 이름:iexplore.exe

안전

요약 정보

- 최초 발견 날짜:
- 의심 행위 개수: 14
- 디지털 서명: Microsoft Corporation
- 제작자: Microsoft Corporation
- 최초 실행 날짜: 2013-06-19 오후 9:10:29
- 유포 경로:

파일 평판 정보

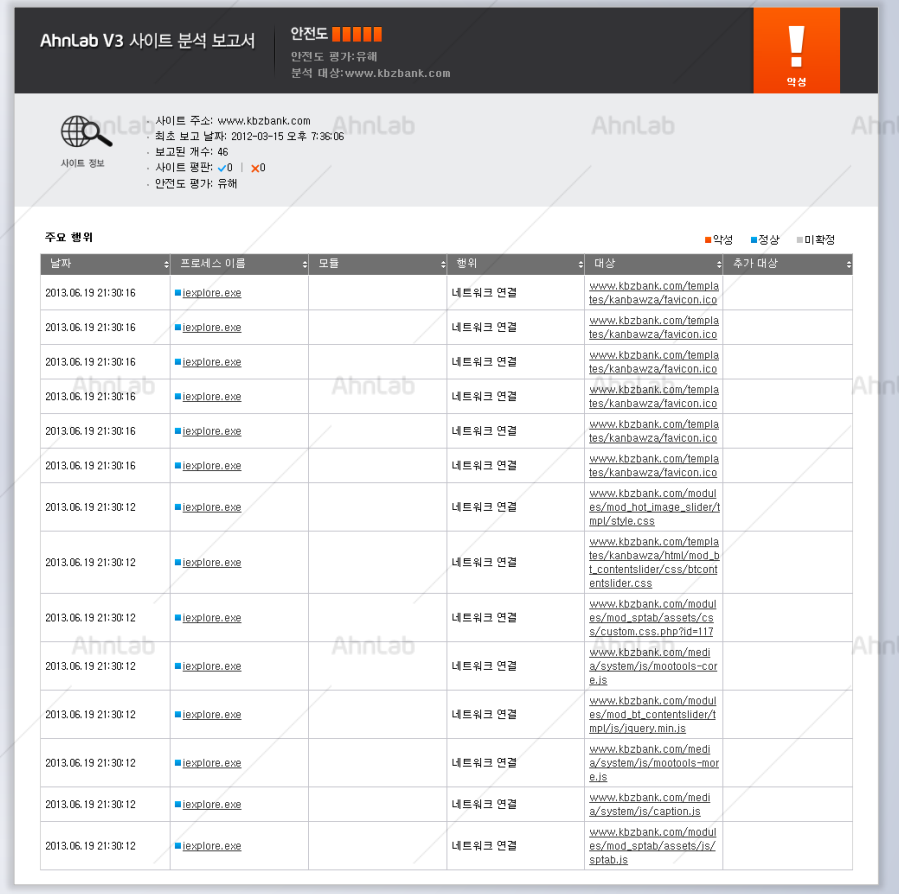
- 다운로드 주소:
- 최초 보고 날짜: 2013-06-12 오전 1:34:23
- 사용자 수: 93,988
- 클라우드 평판: ✓2 | ✗0
- 최초 발견 국가: KR
- 안전도 평가: 정상

발견 파일 정보

파일 이름	iexplore.exe
파일 경로	c:₩Program Files₩Internet explorer₩iexplore.exe
파일 크기	770,648
만든 날짜	2013-06-19 오전 3:02:59
수정한 날짜	2013-06-19 오전 3:02:59
액세스한 날짜	2013-06-19 오전 3:02:59
최초 발견 날짜	
최초 실행 날짜	2013-06-19 오후 9:10:29
MD5 정보	cee28bcbc3251595396ee7fda2b5f3cf

버전 정보

파일 설명	
제작사	Microsoft Corporation
설명	Internet Explorer
파일 버전	10.00.9200.16521 (win8_gdr_soc_ie.130216-2100)
내부 이름	iexplore
저작권	© Microsoft Corporation. All rights reserved.
Legal Trademarks	



AhnLab V3 사이트 분석 보고서

안전도

안전도 평가:유해

분석 대상:www.kbzbank.com

악성

사이트 정보

- 사이트 주소: www.kbzbank.com
- 최초 보고 날짜: 2012-03-15 오후 7:36:06
- 보고된 개수: 46
- 사이트 평판: ✓0 | ✗0
- 안전도 평가: 유해

주요 행위

■악성 ■정상 ■미확정

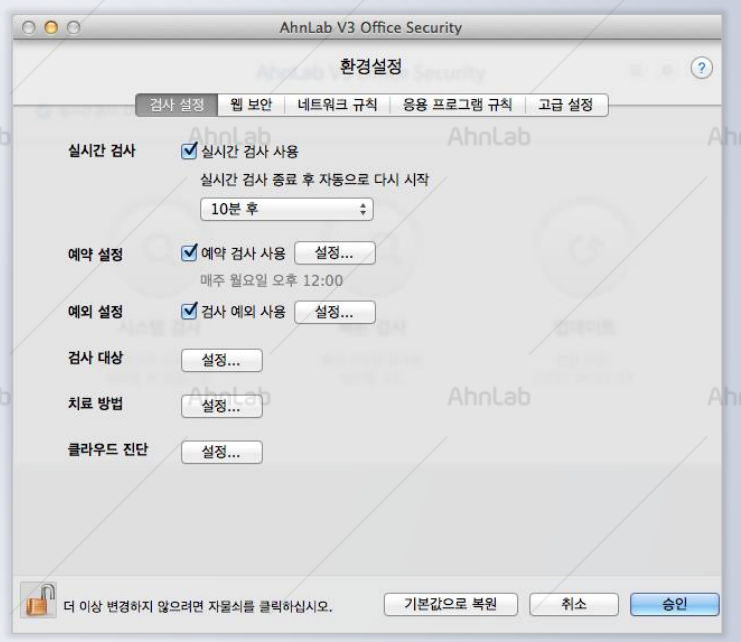
날짜	프로세스 이름	모듈	행위	대상	추가 대상
2013.06.19 21:30:16	iexplore.exe		네트워크 연결	www.kbzbank.com/templates/kanbawza/favicon.ico	
2013.06.19 21:30:16	iexplore.exe		네트워크 연결	www.kbzbank.com/templates/kanbawza/favicon.ico	
2013.06.19 21:30:16	iexplore.exe		네트워크 연결	www.kbzbank.com/templates/kanbawza/favicon.ico	
2013.06.19 21:30:16	iexplore.exe		네트워크 연결	www.kbzbank.com/templates/kanbawza/favicon.ico	
2013.06.19 21:30:16	iexplore.exe		네트워크 연결	www.kbzbank.com/templates/kanbawza/favicon.ico	
2013.06.19 21:30:16	iexplore.exe		네트워크 연결	www.kbzbank.com/templates/kanbawza/favicon.ico	
2013.06.19 21:30:12	iexplore.exe		네트워크 연결	www.kbzbank.com/modules/mod_hot_image_slider/tmpl/style.css	
2013.06.19 21:30:12	iexplore.exe		네트워크 연결	www.kbzbank.com/templates/kanbawza/html/mod_bt_contentslider/css/btcontentslider.css	
2013.06.19 21:30:12	iexplore.exe		네트워크 연결	www.kbzbank.com/modules/mod_sptab/assets/css/custom.css.php?id=117	
2013.06.19 21:30:12	iexplore.exe		네트워크 연결	www.kbzbank.com/media/system/js/mootools-core.js	
2013.06.19 21:30:12	iexplore.exe		네트워크 연결	www.kbzbank.com/modules/mod_bt_contentslider/tmpl/js/jquery.min.js	
2013.06.19 21:30:12	iexplore.exe		네트워크 연결	www.kbzbank.com/media/system/js/mootools-more.js	
2013.06.19 21:30:12	iexplore.exe		네트워크 연결	www.kbzbank.com/media/system/js/caption.js	
2013.06.19 21:30:12	iexplore.exe		네트워크 연결	www.kbzbank.com/modules/mod_sptab/assets/js/sptab.js	

[Desktop] V3 Office Security (macOS) 주요 기능

V3 Office Security(macOS)는 기업용 맥 OS(macOS) 전용 Anti-Malware 솔루션

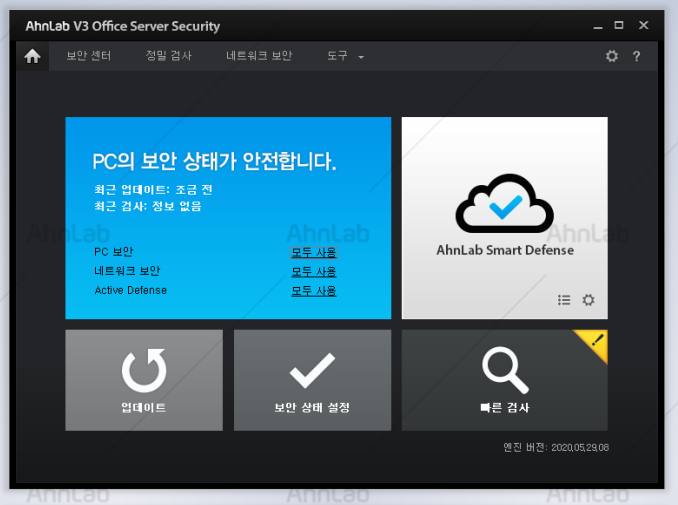
macOS에 최적화된 V3 Office Security는 macOS를 노리는 다양한 악성코드 대응이 가능합니다.
또한 Office Security Center를 통해 쉽고 간편하게 관리할 수 있습니다.

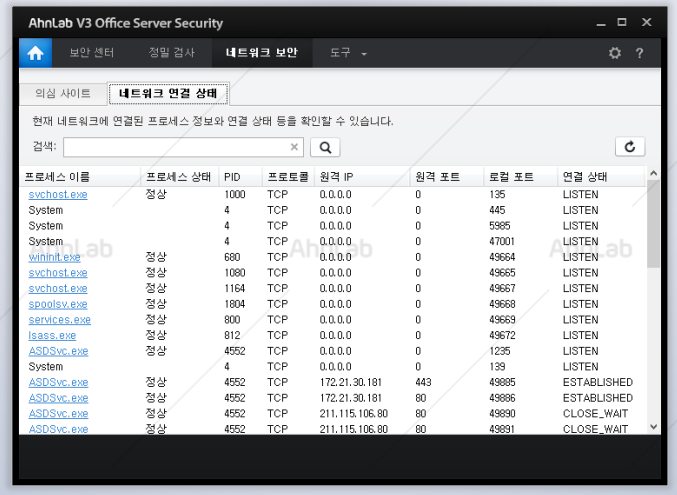
- 중앙관리 솔루션 연동을 통한 관리 편의성
- V3에 적용된 TS 엔진 적용
- Mac 최적화 UI로 탁월한 사용성 구현



[Server] V3 Office Server Security (Windows) 주요 기능

V3 Office Server Security는 서버 방역을 통해 기업의 정보 자산 보호가 가능하며 특히 다차원 분석 플랫폼이 적용돼 사전 방역과 서버 운영에 효과적입니다.





- 다차원 분석 플랫폼 기반의 차별적인 서버 방역
  - 다차원 분석 플랫폼 기반의 차별적인 방역(행위/평판, 악성 URL/IP 정보 활용)
  - 클라우드 기반의 ASD로 정확한 진단 및 실시간 치료
  - Active Defense 기능으로 위협에 대한 가시성 확보, 능동적인 대응 가능

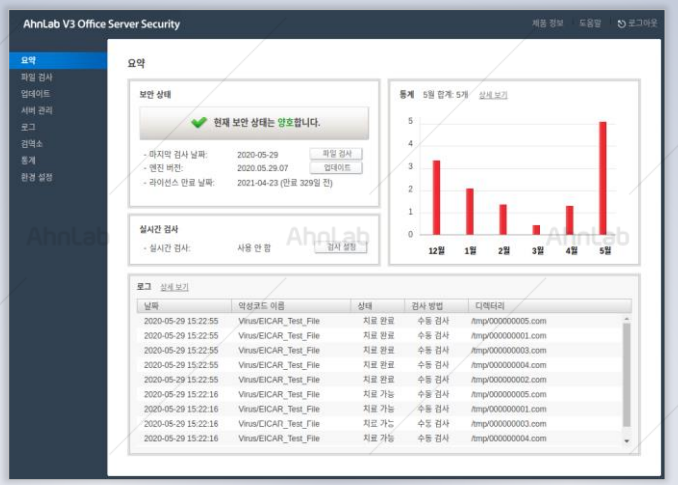
- 서버 활용성 극대화를 위한 다양한 기능 제공
  - 악성코드 등 위협 상태 정보를 Office Security Center에 전송
  - 다양한 기업 환경에 최적화

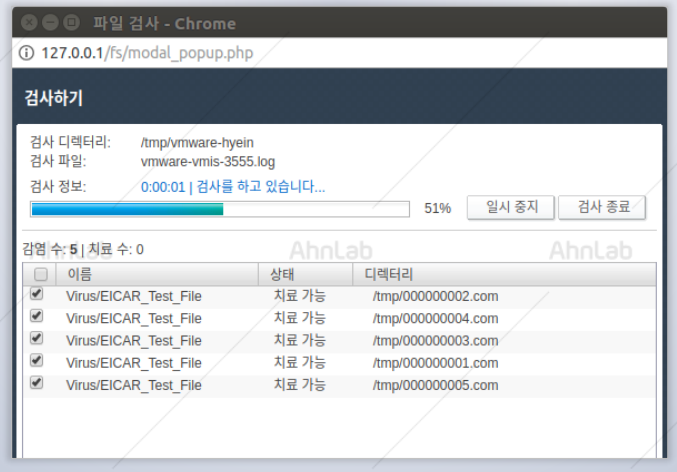
- 스마트 스캔 기술로 신속•정확한 검사
  - 최초 1회 검사로 안정성 확보한 파일을 제외하고 검사하는 스마트 스캔(Smart Scan) 기술 적용
  - 빠른 검사를 통한 사용자 편의성 극대화

- 쉬운 컬러, 메인 화면에서 문제 한번에 해결
  - 선명하고 이해하기 쉬운 컬러로 서버 보안 상태를 확인
  - 필요한 검사 기능을 메인 화면에서 간단히 이용 가능

[Server] V3 Office Server Security (Linux) 주요 기능

V3 Office Server Security는 갈수록 심각해지는 바이러스에 의한 피해를 서버 차원에서 원천적으로 차단하는 서버 방역 제품으로 Linux 서버 전용의 악성코드 방역을 위한 제품입니다.





- 정확하고 신속한 서버 방역

- 실시간 검사 기능을 통한 모니터링
- 독보적인 엔진으로 신속하고 정확한 바이러스 진단/치료
- 다양한 다중 압축 파일 검사/치료 지원

- 서버 활용성 극대화를 위한 다양한 기능 제공

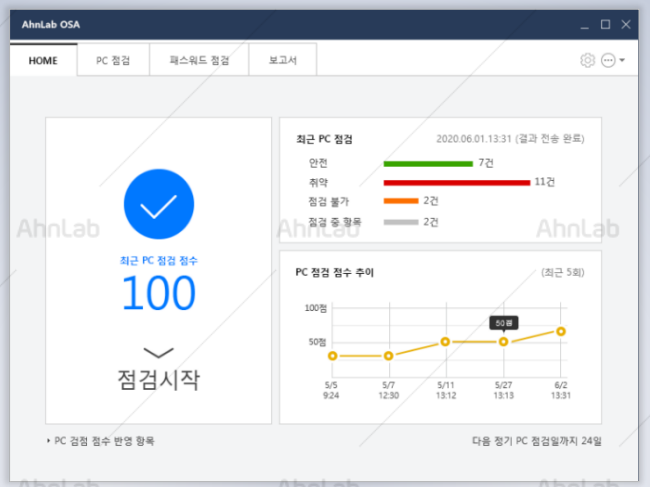
- 효율적인 수동 및 예약 검사 기능
- 지정된 시간에 자동 엔진 업데이트를 할 수 있는 예약 기능

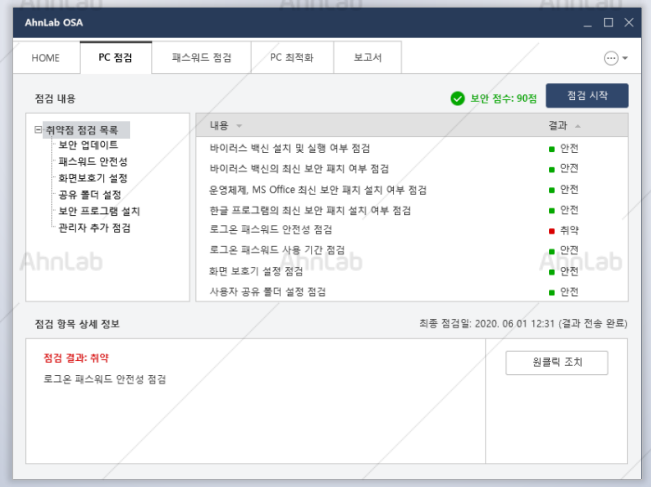
- 관리자 편의를 고려한 효율적인 관리 기능

- 검사 예외 설정 기능으로 효율적인 방역 정책 적용
- 바이러스 검사/치료에 대한 다양한 통계 리포트 제공
- 검사 예외 설정 기능으로 효율적인 방역 정책 적용
- 악성코드 방역 정책 수립, 적용 및 모니터링을 위한 Office Security Center 연계로 통합 관리 지원

[Desktop] Office Security Assessment (Windows) 주요 기능

AhnLab OSA는 기업 환경에 따라 모든 개별 PC의 필요 점검 항목을 선택 적용 할 수 있어 더욱 효율적인 운영 및 관리가 가능합니다.





- '44개 점검 항목'의 선택적 운영 및 평가 점수 배점
  - 기업 환경 및 내부 정책에 따라 '점검 항목' 전체 또는 선택 적용 가능
  - 13개 기본 취약점 점검 및 31개 확장 취약점 점검 항목 구성
  - 자동실행 서비스 목록 및 윈도우 시작 프로그램 목록 수집 기능

- 점검 주기 동작에 따른 운영 편의성
  - 관리자가 원하는 시점으로 '점검 주기' 설정 가능
  - 일정한 점수 미만 기기의 파악 및 조치 용이

- 적극적인 사용자 유도 기능
  - 기준 점수 이하인 경우, 위젯(Widget)을 통한 PC 취약점 점검 현황 상시 알림
  - 구체적인 조치 방법 안내 제공

- OS 보안 패치 점검

  OS(Windows), MS Office, 한글 프로그램의 최신 보안 패치 점검

[Desktop] Office Security Assessment 특장점

탁월한 사용자 편의성

AhnLab OSA는 전문 지식이 없는 일반 사용자/관리자도 손쉽게 이용할 수 있는 편리한 사용성과 직관적인 UI를 제공합니다.

편리한 사용성, **직관적인** UI

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

관리 기준 설정에 따른
주기적 점검

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

Office Security Center를 통한
현황 모니터링 · 관리 효율화

구성 제품 운영 환경 (권장 지원 환경)

AhnLab V3 Office Security (Windows) 지원 환경

구분	권장 사양
운영체제	Windows 7 SP1 (KB4490628, KB4474419 패치 환경)
	Windows 8(8.1), Windows 10
CPU	Intel Core i3 이상
Memory	4GB 이상
Storage	800MB 이상
지원 언어	한국어, 영어

AhnLab V3 Office Security (macOS) 지원 환경

구분	권장 사양
운영체제	10.12 (Sierra) ~ 11.0 (Big Sur)
CPU	Intel Core 2 Duo 2.53GHz 이상
Memory	4GB 이상
Storage	2GB 이상
지원 언어	한국어, 영어

AhnLab Office Security Assessment 지원 환경

구분	권장 사양
운영체제	Windows 7 SP1 (KB4490628, KB4474419 패치 환경)
	Windows 8(8.1), Windows 10
CPU	Intel Core i3 이상
Memory	4GB 이상
Storage	800MB 이상
지원 언어	한국어, 영어

AhnLab V3 Office Server Security (Windows Server) 지원 환경

구분	권장 사양
운영체제	Windows Server 2008 R2 SP1(KB4490628, KB4474419 패치 환경)
	Windows Server 2012 R2 이상
CPU	2GHz 이상
Memory	4GB 이상
Storage	800MB 이상
지원 언어	한국어, 영어

AhnLab V3 Office Server Security (Linux Server) 지원 환경

구분	권장 사양
운영체제	CentOS 5.0 ~ 8.0
	Debian 9.5 ~ 10.4
	Fedora 16 ~ 32
	openSUSE 12.1 ~ 15.2
	Oracle Linux 5.5 ~ 8.2
	RedHat Enterprise Linux 5.0 ~ 8.2
	SuSE Enterprise Linux 11.0 ~ 15.1
	Ubuntu 11.10 ~ 20
Memory	1GB 이상
Storage	2GB 이상
지원 언어	한국어, 영어

* OS 지원여부는 일반 사항이며, 모든 OS 버전의 지원을 보장하지는 않습니다.

AhnLab
Office Security

04.
제품 경쟁력·도입 기대 효과

1. 경쟁력
2. 도입 기대 효과

AhnLab

AhnLab Office Security 경쟁력

Multi-OS · Multi Device 통합관리

스마트한 기업의 선택

01 SaaS형 매니지먼트를 통해 **각 디바이스 보안 현황 관리 및 모니터링**

02 관리 서버 구축 및 별도 투자 없이 **저 비용으로 보안 환경 마련**

03 다차원 분석 플랫폼 기반 **탁월한 진단율, 사전 방역 효과까지**

04 클라우드 기반의 악성코드 분석 기술로 **신·변종 악성코드 대응**

05 독자 개발 엔진 및 스마트 스캔 기술을 통해 **차별화된 검사 속도**

06 관리자가 언제 **어디에서든 Multi-OS/Devices 점검 관리**

Office Security Center (Web) 인터페이스

연동 구성 제품

- V3 Office Security (Windows / macOS)
- V3 Office Server Security (Windows / Linux)
- Office Security Assessment (Windows)

AhnLab Office Security 도입 기대 효과

Smart Office 업무 환경 보안에 최적화된 Security Management 솔루션

AhnLab Office Security

보안 관리·대응을 위한 **중소기업형 보안 플랫폼**

보안 인프라 구축 비용 절감 효과

- 보안 부서, 전문가 채용 없이 라이선스 구매만으로 손쉽게 보안 환경 마련
- 구성 제품 계약 시 무료 제공되는 AhnLab Office Security Center로 보안 체계 구축·운영 관리 비용 고민 해결
- 단일 업체의 올인원(All-in-one) 서비스 도입으로, 다중 계약 관리 번거로움 최소화

쉽고 편한 위협 관리·대응 플랫폼

- 클라우드 환경 기반으로, 언제 어디서나 온라인 접속만으로 매니지먼트 액세스 가능
- 이해하기 쉽고 간결한 직관적 유저 인터페이스(User Interface)로 간편한 관리 가능
- 한 곳에서 위협 모니터링, 즉각적인 대응 및 보안 정책 수립 가능
- 설정에 따라 주기적으로 이메일링되는 보안 리포트를 통해 보안 상태 및 라이선스 현황 확인

효율적 기업 자산 보안 관리

- SaaS 기반 통합 매니지먼트(AhnLab Office Security Center)를 통한 일원화된 보안 운영 및 관리 환경 마련
- 멀티 OS, 멀티 디바이스의 보안 점검 및 다양한 관리 기능을 통한 운영 편의성 향상

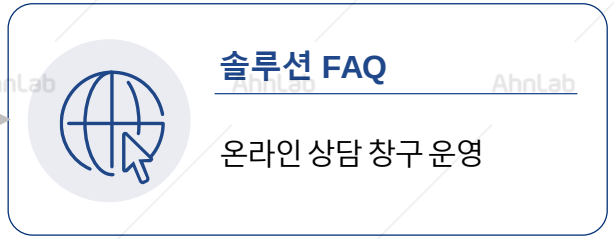
05.
별첨

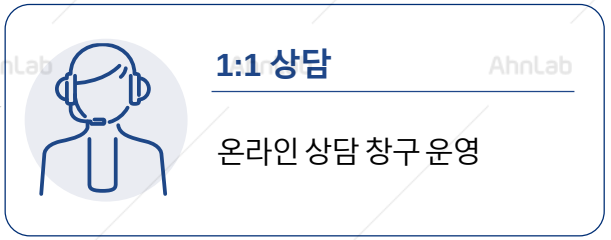
1. Management 기능 비교 (요약)
2. 구성 제품군 비교 (SMB 대상)
3. 고객 지원
4. 안랩의 입체적 대응 서비스
5. 악성코드 대응 프로세스
6. '2019 올해의 엔드포인트 보안 기업' 선정

Office Security 고객 지원

※전문 상담 인력 운영으로 문의 응대 및 기술지원. 1:1상담, 핫라인, FAQ 등 온라인 서비스로 제공 됩니다.

- 지원 대상 : Office Security 관련 솔루션 구매 고객
- 지원 방식 : 온라인 지원 대응 (오프라인 非대응)
- 고객 대응 : 고객서비스팀





AhnLab.com

- 안랩닷컴 FAQ (기업) 제공

2020.11. zendesk (https://atac.ahnlab.com) 이관 예정

AhnLab.com

- 안랩닷컴 로그인 필요

전문 상담 운영

- 제품 문의 및 이슈 대응
- 오전 9시 ~ 오후 6시 (토,공휴일 제외)

※솔루션 구매 문의(구입/계약/등록) / 1588-3096 / 오전 9시 ~ 오후 6시 (토,공휴일 제외)

안랩의 입체적 대응 서비스

안랩은 25여 년간 축적한 악성코드 분석 기술을 바탕으로 '분석(ASEC)+대응(CERT)+제품'으로 이어지는 입체적 대응 서비스를 제공합니다.
또한 국내 최고 수준의 보안 전문가로 고객사의 위협 대응 및 장애에 대해 즉각적이고 안정적인 지원을 제공하고 있습니다.

AhnLab

보안 전문 기업의
노하우 적용

클라이언트 환경에
대한 높은 이해

다양한 고객 환경에
대한 이해

통합 보안기업의
수준 높은 보안 서비스

Company

- 다년간 보안 영역에 관한 전문적인 노하우 축적
- 최신 위협에 대한 실시간 대응 체제 구축
- 엔드포인트 부터 어플라이언스까지 다양한 보안 제품 개발 경험 보유

Technology

- 클라우드(Cloud) 기반의 실시간 악성코드 진단 기술 ASD(AhnLab Smart Defense) 보유
- 분석(ASEC)+대응(CERT)+제품을 통한 입체적 대응 서비스 제공

Reputation

- 국내 최대 개발/지원/보안 인력 보유로 이슈 발생 시 빠른 대처 가능
- 공공/금융/기업 등 전 산업 분야에 걸쳐 다양한 고객을 보유

악성코드 대응 프로세스

안랩 시큐리티 대응 센터(ASEC)의 4단계 대응 프로세스를 기반으로 강력한 악성코드 및 해킹 억제력을 제공합니다.

ASEC

AhnLab Security Emergency response Center

1단계 : 접수 > **2단계 : 분석** > **3단계 : 1차 대응** > **4단계 : 2차 대응**

1단계 : 접수

신·변종 바이러스, 해킹 사고 접수

바이러스·해킹 툴 수집

2단계 : 분석

상황 분석

1. 국내·외 피해 조사 및 예측
2. 프로그램 용도
3. 바이러스·해킹 발생 시점 및 행동 분석

샘플 분석

1. 샘플 입수·분석
2. 분석 리포트 제출
3. 대응 방식 결정
4. 대응 일정 확정

3단계 : 1차 대응

엔진 대응

1. 바이러스·해킹 툴 대응 엔진 제작
2. 엔진 업데이트

추가 공격 대응 준비

1. 변종 바이러스·해킹 툴 모니터링
2. 고객 응대 확대

4단계 : 2차 대응

모듈 변경

1. 변종 바이러스 엔진 추가 등록
2. 해킹 툴 방지 모듈 개발
3. 제품 업데이트

※ **ASEC**(AhnLab Security Emergency response Center)은 안랩에서 운영하는 비상 대응 조직으로, 바이러스 및 보안 위협의 24시간 감시, 신속한 대응 및 지속적인 연구를 수행하여 고객사의 중요 정보 자산 및 비즈니스 연속성을 보호하여 고객사의 대외 신뢰도 강화에 기여합니다.

'2019 올해의 엔드포인트 보안 기업' 선정

안랩은 엔드포인트 보안 분야에서의 기술력, 시장 점유율 등을 인정받아 글로벌 리서치 기관인 프로스트 앤 설리번(Frost & Sullivan)이 주최한 2019 Frost & Sullivan Korea Best Practices Award에서 '올해의 엔드포인트 보안 기업'으로 선정되었습니다.

2019 프로스트 앤 설리번 베스트 프랙티스 어워드

2019 Frost & Sullivan Best Practices Award
South Korea Endpoint Security Vendor of the Year

2019년 11월 14일

"안랩은 멀티OS, 멀티 클라우드 등 기업 환경 변화와 요구에 최적화된 엔드포인트 보안 솔루션을 제공하고 있다. 복잡한 엔드포인트 환경을 안랩의 단일 에이전트와 단일 관리 콘솔을 통해 대한 효과적으로 보호할 수 있다."

Kenny Yeo
Associate Director and Head of Asia-Pacific Cyber Security
Frost & Sullivan

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 Office Security

AhnLab

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