언택트 시대
보안 이슈 및 대응 방안

More security,
More freedom

솔루션컨설팅팀 백민경 부장 / CISSP

AhnLab

목차

AhnLab

최근 유행하는 악성코드는?

코로나19 이전, 원격/재택 근무 유형 및 이슈 사례

원격/재택 근무 유형

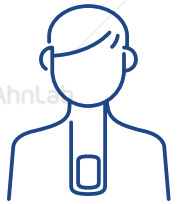
- 기업 임직원 국내(지방) 및 해외 출장
- 건설사 현장 사무소 원격 근무
- 스마트 워크 및 기타 재택근무

원격/재택 근무 이슈

- 외부 반출 후 반입 시, 단말에 대한 보안 검증
- 악성코드(랜섬웨어) 감염, 본사 업무 시스템 원격 접속 Risk
- 원격 접속 단말에 대한 보안 유지

패치 관리, 단말 취약점 점검 및 조치, 신/변종 악성코드 탐지 및 대응

언택트 시대, 재택근무 시 정보보호 6대 실천 수칙



사용자 실천 수칙

- 개인 PC 최신 보안 업데이트
- 백신 프로그램 업데이트 및 검사
- 가정용 공유기 보안설정 및 사설 와이파이·공용PC 사용 자제
- 회사 메일 권장, 개인 메일 사용 주의
- 불필요한 웹사이트 이용 자제
- 파일 다운로드 주의 (랜섬웨어 감염 주의)

관리자 실천 수칙

- 원격근무시스템(VPN) 사용 권장
- 재택근무 대상 보안지침 마련 및 보안인식 제고
- 재택근무자의 사용자 계정 및 접근 권한 관리
- 일정 시간 부재 시 네트워크 차단
- 원격 접속 모니터링 강화
- 개인정보, 기업정보 등 데이터 보안 (랜섬웨어 감염 주의)

※ 재택근무 시 지켜야 할 정보보호 6대 실천 수칙[자료=과학기술정보통신부]

재택근무 정보보호 6대 실천 수칙, 대응 방안

대응 요건

사용자 실천 수칙	보안 패치, 백신 최신 업데이트
사용자 실천 수칙	보안 인식 제고 교육
관리자 실천 수칙	사용자 인증, N/W 접근제어
관리자 실천 수칙	보안 지침 수립, 보안 교육
관리자 실천 수칙	보안 패치 관리, 악성코드 대응

대응 방안

- 보안 인식제고 교육
- 백신, APT
  단말 보안 패치/설정 점검
- VPN (+ MFA*)
  N/W 접근 제어
- 암호화, 화면 캡처 방지

※ MFA : Multi-Factor Authentication

재택근무 정보보호 6대 실천 수칙, 추가 고민?

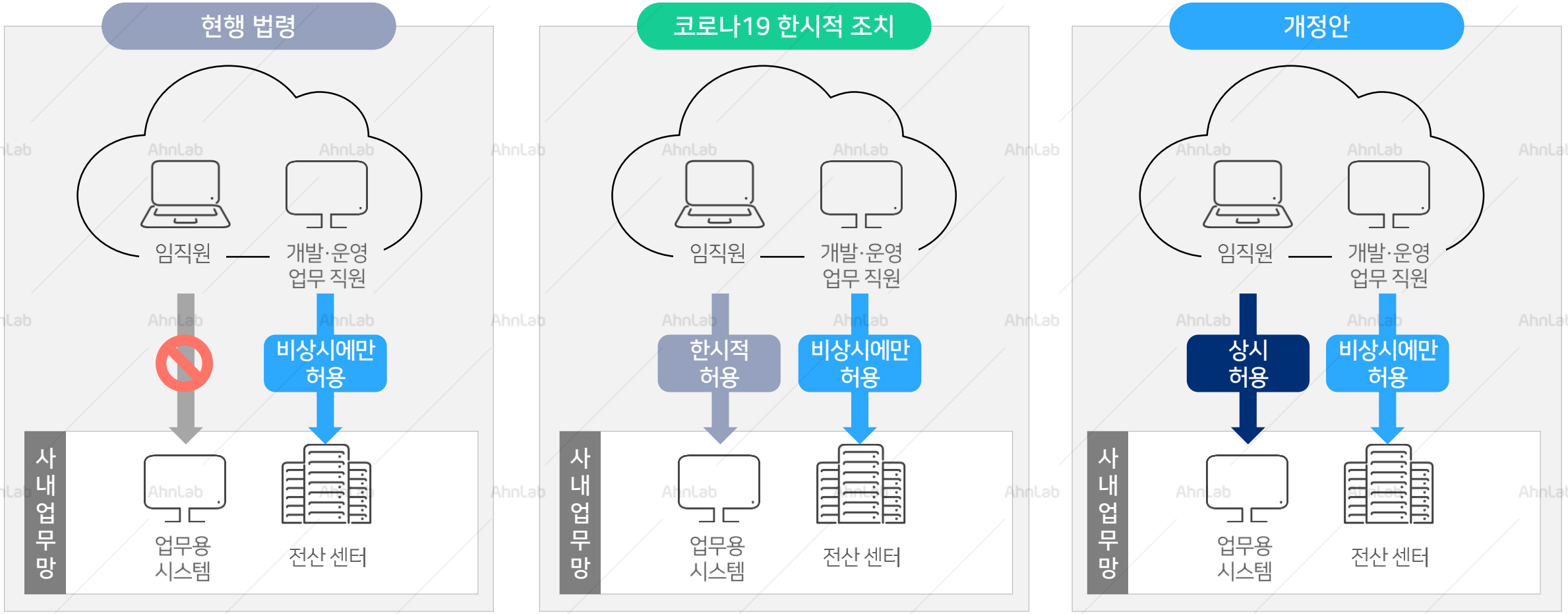
개인 사용 단말 or 회사 지급 단말 사용 여부 / 단말 인증

사외 단말의 보안 (패치, 보안 설정, 백신) **최신 업데이트 유지**

사외 단말의 Unknown 악성 코드/악성 행위 노출에 대한 극복 방안

금융권 재택근무, " 원격 접속 허용 "

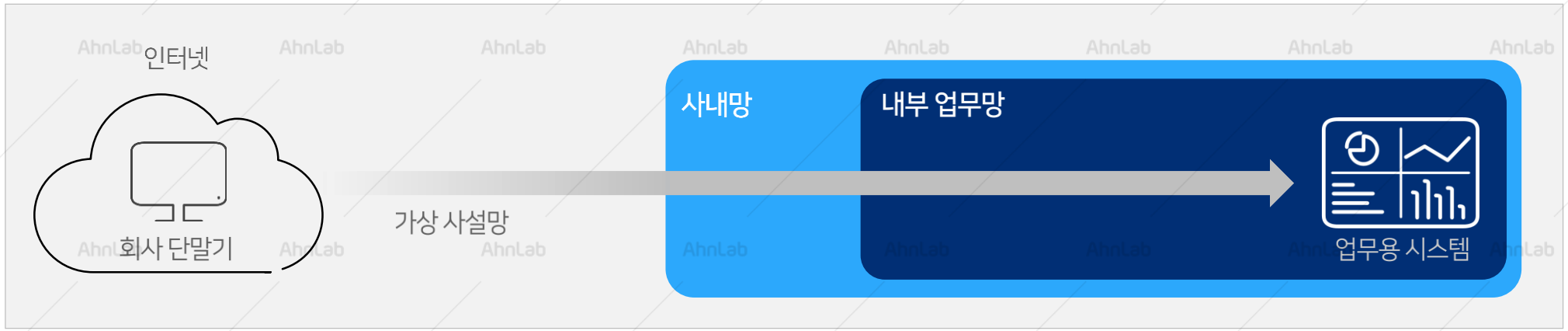
재택근무 관련 망분리 제도 개선사항



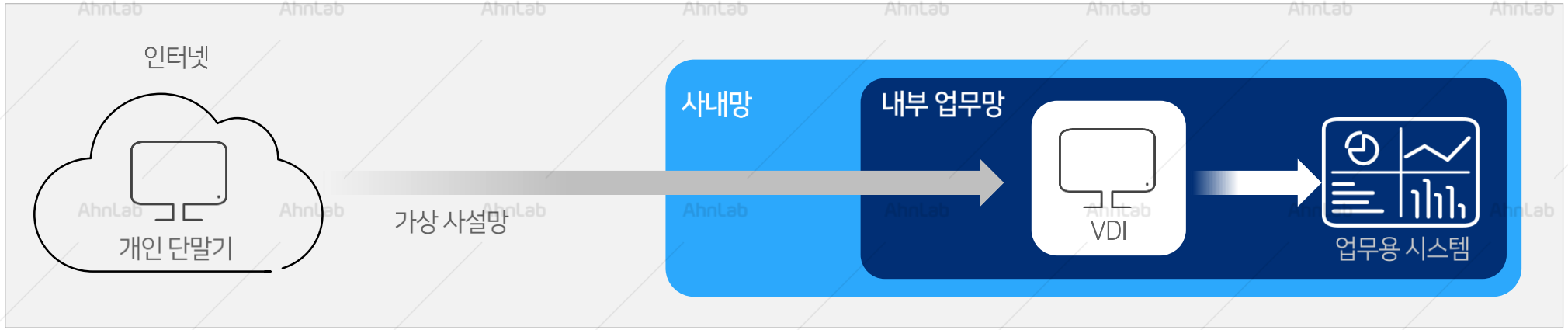
※ 금융감독원 재택근무 관련 망분리 제도 개선사항 참조

금융권 재택근무, " 원격 접속 허용 "

직접 연결 방식 예시



간접 연결 방식 예시



※ 금융감독원 재택근무 관련 망분리 제도 개선사항 참조

금융권 임직원의 재택근무를 위한 보안 가이드

금융권 보안중점 사항

외부 단말기 보안관리
재택근무자가 사용하는 외부 단말기는 백신 프로그램 설치

개인 PC
백신 프로그램 설치 및 검사, 운영체제 버전, 로그인 비밀번호, 화면 보호기 설정 등의 보호대책

통신회선
외부 단말기의 내부망 접속 시에는 전용회선과 동등한 보안수준을 갖춘 가상사설망(VPN)을 사용

내부망 접근통제 및 인증
금융회사 내부망에 접속 가능한 IP 주소 등은 최소한으로 제한하고 비인가자의 접속을 방지하기위해 이중인증(Multi-Factor Authentication)을 적용

보안준수
재택근무자에 대한 보안 서약서 징구, 공공장소에서의 원격접속 금지를 의무 적용

접속보안 권고 사항

금융 접속보안 권고 사항

보안 정책	직접 연결	간접 연결
허용되는 단말기의 종류	회사 지급 단말기만 가능	개인 단말기도 가능
인터넷 차단	항상 차단	업무망 연결시 차단
백신 설치, 최신 운영체제 유지, 비밀번호 설정	사내 근무시와 동일	사내 근무시와 동일
파일 송수신	허용	차단
단말기 설정 변경, 외부저장장치 사용	차단	허용
내부 전산자료 출력, 화면 캡쳐	차단	차단
내부 전산자료 저장	암호화 저장	차단

[직접 연결] 외부 단말기에서 내부망에 직접 접속
[간접 연결] 외부 단말기에서 회사 내부의 업무용 단말기(이하 `업무용 단말기')를 경유하여 내부망에 접속

재택근무(원격접속) 보안강화

보안 통제 적정성 운영
- 보안패치 적용
- 시간 동기화
- 신규 보안정책
- 공격 탐지
- 관리적 보안지침 준수
- 접속로그 분석
- 취약점 대응

01 사내 정보의 외부 유출 방지
- 원격접속 모니터링 구성 필수
- 업무 단말기 인터넷 접속통제
- EDR, DLP,SIEM

02 외부 악성코드의 내부 유입 방지
- 원격접속 모니터링 구성 필수
- 접속 포인트에서 AV검사
- SSL검사, EDR, DLP

03 엔드포인트/ 네트워크 보안
- 원격접속 모니터링 구성 필수
- 업무용 단말기 지급
- Anti-Virus / VPN / MFA

※「전자금융감독규정시행세칙」[시행 2021. 1. 1.] [금융감독원세칙 , 2020. 11. 6., 일부개정] "[별표7] 망분리 대체 정보보호통제" 기준

금융권 재택근무, 추가 고민?

인터넷 차단 환경 기준, 업무 연속성 보장

사외 단말의 보안 (패치, 보안 설정, 백신) **최신 업데이트 유지**

사외 단말의 Unknown 악성 코드/악성 행위 노출에 대한 극복 방안

AhnLab ESA

AhnLab ESA(Endpoint Security Assessment)는 업무용 PC의 보안 상태를 점검하고 자동조치를 통해 엔드포인트의 전반적인 보안 수준을 강화(hardening)하는 취약 시스템 점검 및 조치 솔루션입니다. 업무용 PC의 보안 상태 점검 및 자동 조치를 통해 관리자와 사용자의 업무 부담은 최소화하고 기업의 엔드포인트 보안 수준을 극대화합니다.

- 쉽고 간편한 기능 및 다양한 정책으로 관리자와 사용자의 보안 부담 해소 및 업무 생산성 향상
- 플랫폼 기반의 백신, 패치, 개인정보 통합 관리를 통한 엔드포인트 하드닝(Endpoint Hardening) 효과

AhnLab ESA

원클릭으로
쉽고 간편하게

효율적인 엔드포인트
취약점 관리

관리자와 PC사용자의
업무 효율성 극대화

PC 보안 점검으로 인한 업무 부담 및 리소스 소모 최소화

- 기술적인 지식이 없는 일반 사용자도 손쉽게 PC 보안 상태 확인 및 조치 가능

중앙에서 개별 PC의 보안 상태를 한 눈에 파악

- 사내 모든 PC에 최신 패치 자동 적용
- 통합 매니지먼트로 간편하게 관리 및 보고서 작성 가능

다양한 취약점에 대한 사전 대응 조치 가능

- 타사 대비 최다 점검 항목 지원
- 더욱 안전한 PC 환경 구현

정보보안 관련 규제 대응 및 준수

- 공공기관 '사이버 보안 진단의 날' 의무 규정 준수
- 금융기관 '정보보안 점검의 날' 대응

재택근무 접속 환경 보안 점검 항목

← ESA 기본 정책

ESA 기본 정책입니다.

일반 설정

점검 항목 설정

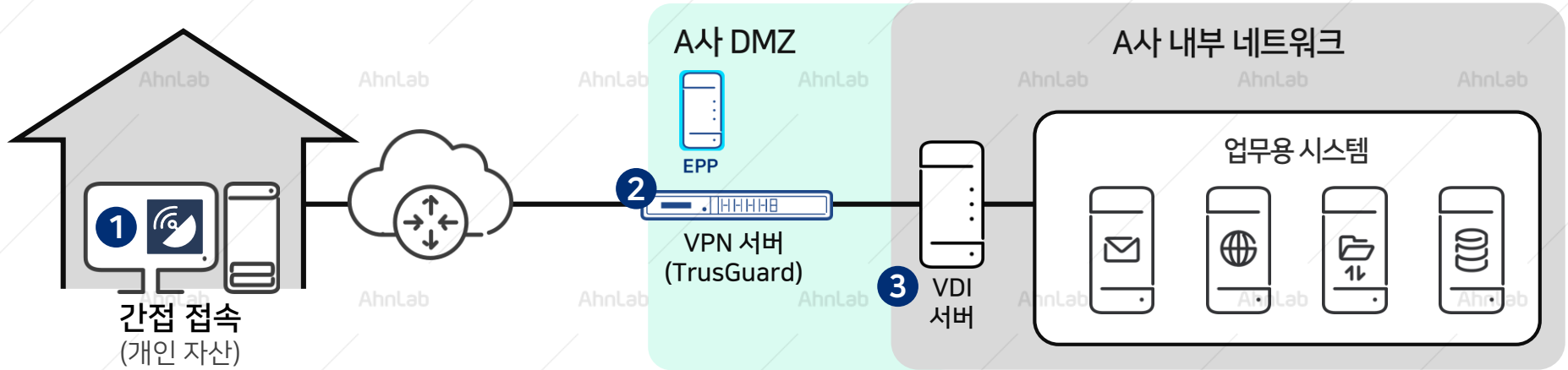
프로그램 검증 설정

점검 예외 설정

구분	점검 항목	점검 예외	긴급 조치	설정	강제 조치	네트워크 차단	점수
▲ 기본 점검 항목							
보안 업데이트	악성코드 백신 설치 및 실행 점검	☐	-	-	-	☐	15
보안 업데이트	악성코드 백신 최신 보안 패치 점검	☐	-	-	☐	☐	15
보안 업데이트	운영체제, MS Office 최신 보안 패치 점검	☐	-	설정	☐	☐	14
보안 업데이트	한글 프로그램 최신 보안 패치 점검	☐	-	설정	☐	☐	14
패스워드 안전성	로그온 패스워드 안전성 점검	☐	-	설정	☐	☐	14
화면 보호기 설정	화면 보호기 설정 점검	☐	-	설정	☐	☐	14
▲ 확장 점검 항목							
기타 항목	취약 OS 점검	☐	-	설정	☐	☐	6
기타 항목	필수 소프트웨어 설치 (VDI)	☐	-	설정	☐	☐	4
기타 항목	필수 소프트웨어 설치 (VPN)	☐	-	설정	☐	☐	4

AhnLab 대응 방안 적용 사례 > VPN Client 연동

VPN Client 연동



VPN Client 연동 : 재택 근무 사용자 업무 환경 접속 Flow

1

1) TG VPN Client 구동
2) TG VPN Client에서 ESA 점검결과 확인
3.1) 조건 만족 시 VPN 연결
3.2) 조건 불만족 시 VPN 연결 실패 및 조치방안 안내

2

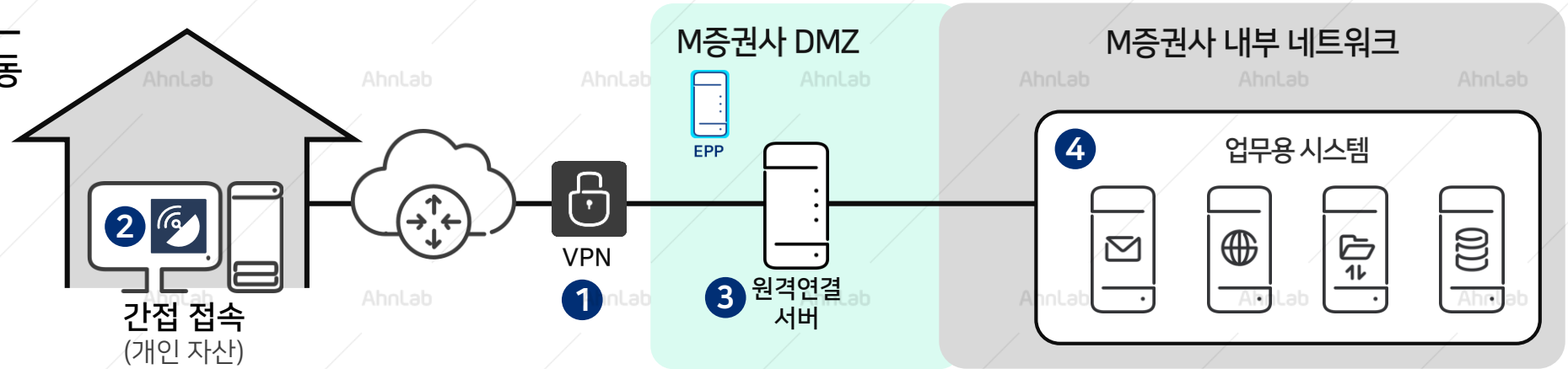
1) 조건 만족 된 PC는VPN 연결
2) VPN 연결 시 <개인 자산> PC의 인터넷 차단
3) 유휴시간 경과 후 VPN 연결 종료

3

재택 업무 수행을 위한 VDI 접속
재택 업무 수행

AhnLab 대응 방안 적용 사례 > 원격접속 프로그램 연동

원격접속 Agent 연동



원격접속 Agent 연동 : 재택 근무 사용자 업무 환경 접속 Flow

1

1) VPN Client 설치

2) VPN 구동 및 연결

2

1) 원격 연결 홈페이지 접속

2) 필수 SW 설치
(원격접속 Agent, ESA)

3) ESA 보안 사전점검 수행 및 결과 생성
-> 로컬에 결과파일

3

1) 원격접속 Agent 실행

2) 원격접속 Agent에서 점검결과 확인
-> 4시간 이내 점검 실행, 점수 100점)

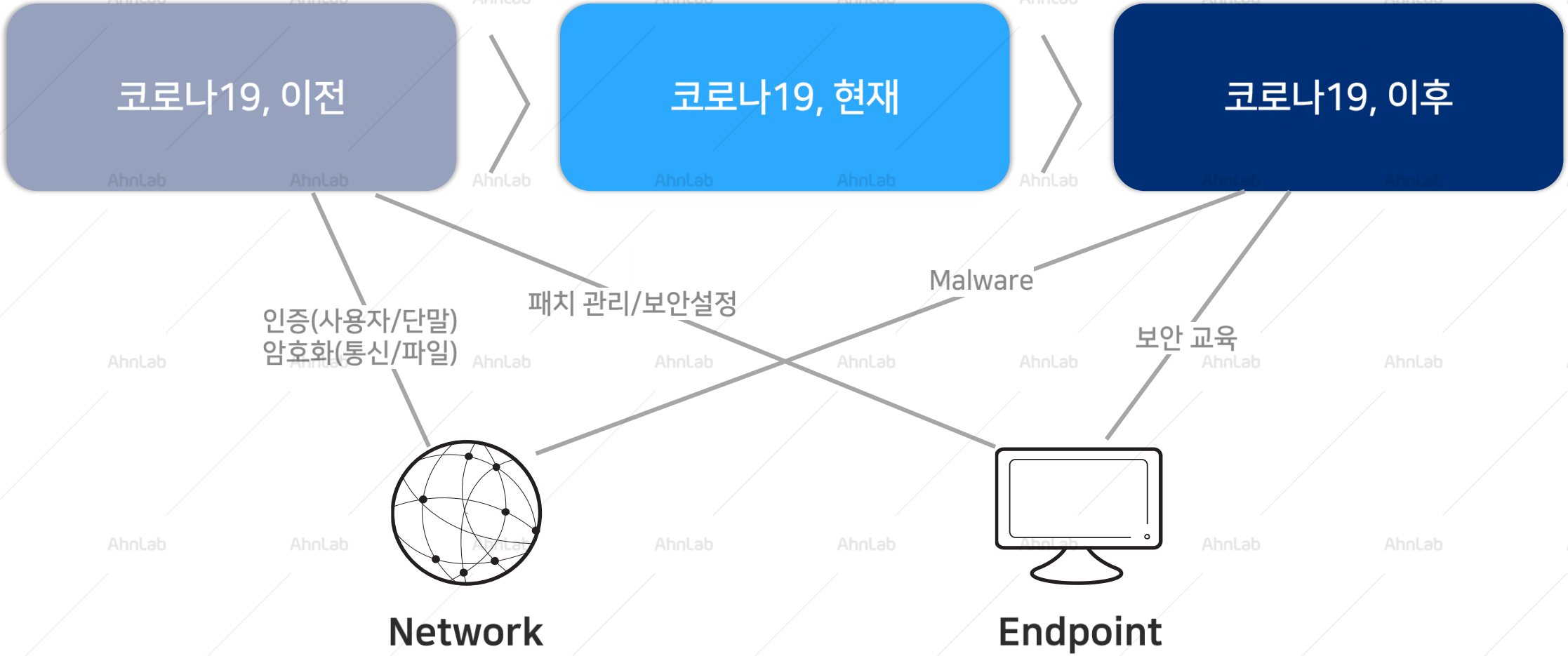
3) 조건 만족 시 원격 연결
불만족 시 점검 점수 개선 가이드

- 원격 Agent에서 ESA의 점검결과를 조회하고, 그 결과에 따라 조치하는 기능 연동 및 개발 적용

4

1) 재택 업무 수행

언택트 환경 보안 . . .



More security, More freedom

AhnLab