신뢰할 수 있는 의료기관 네트워크를 위한 새로운 보안 전략

최정수 부장 / AhnLab

AhnLab
30 Years of
Cybersecurity Excellence

주요 사이버 보안 이슈 – 취약점 증가

AhnLab
30 Years of
Cybersecurity Excellence

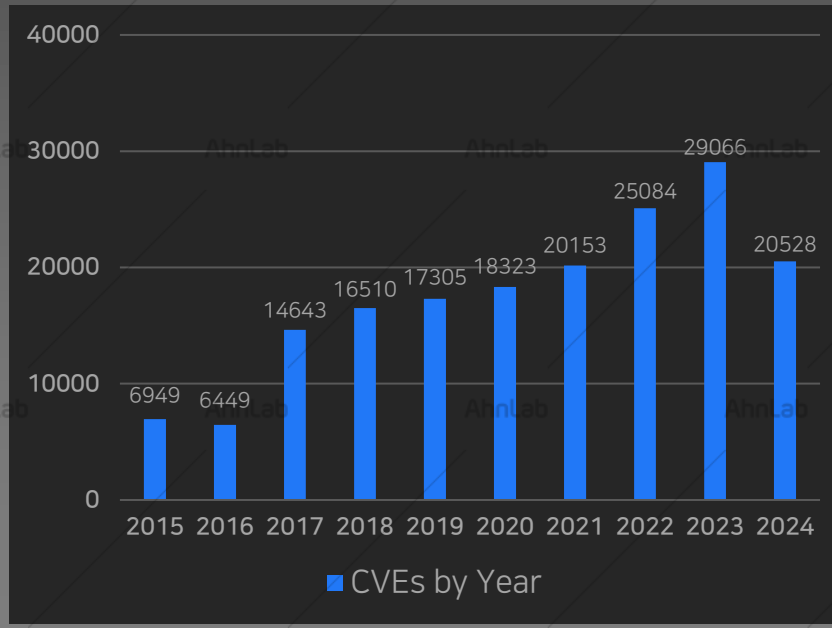
2025

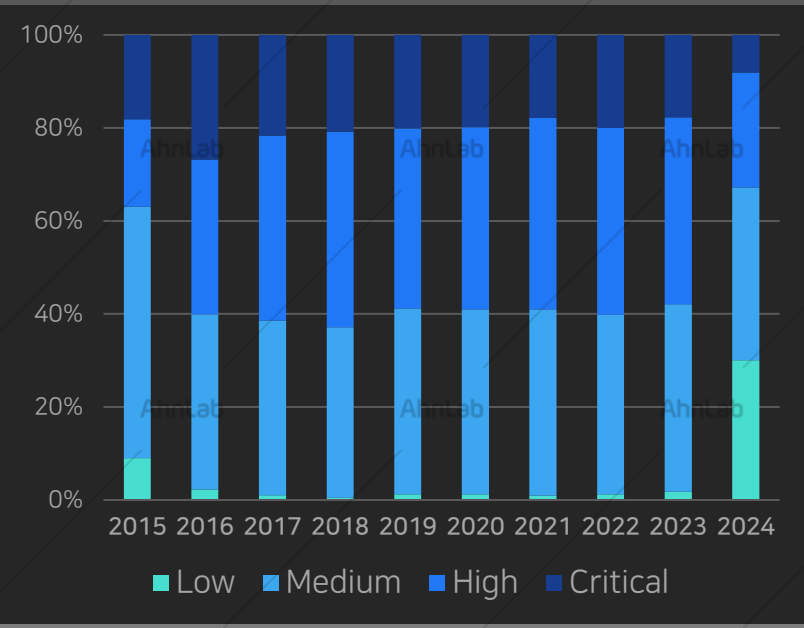
Day
100

Year
30,000

Critical,High
60%

2023년 기준





출처: CVEdetails.com

AhnLab
30 Years of
Cybersecurity Excellence

2025

단순한 시스템 감염에서

사회공학기법, 복합적 공격 루트로 변화


Virus


Worm


Trojan


Spyware


Phishing


Smishing


APT


DDoS


Malvertising


Mining

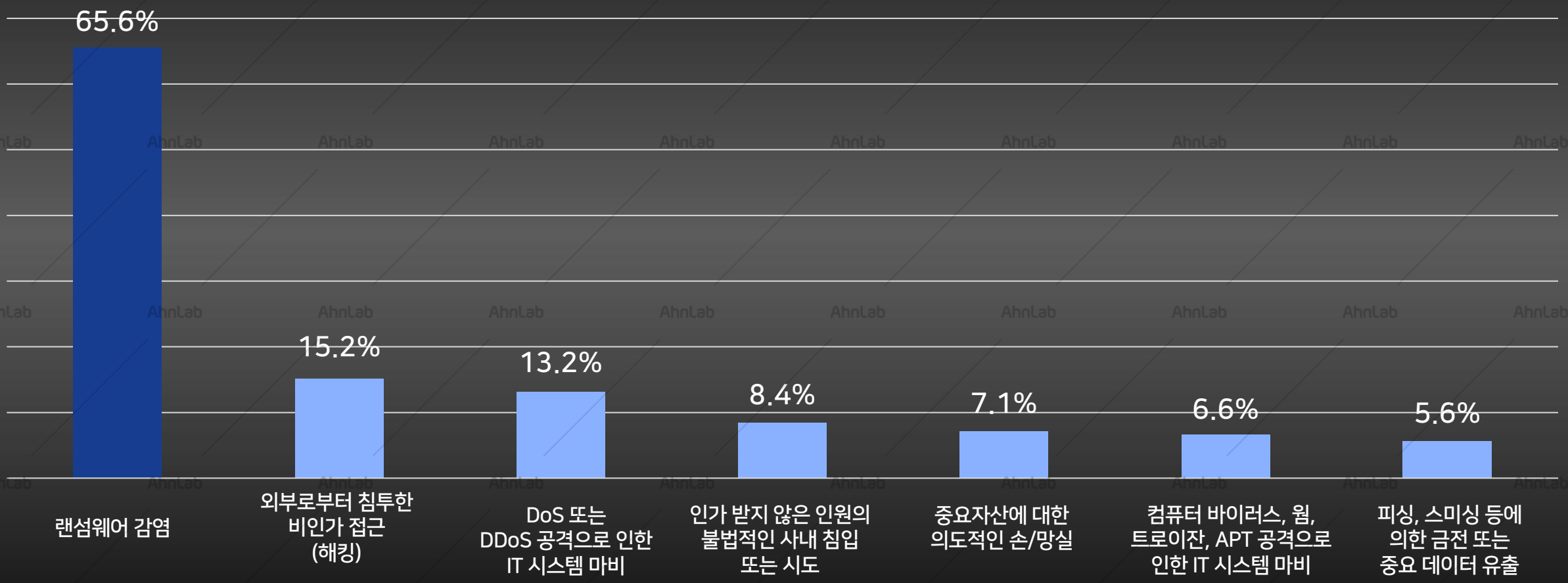

Ransomware


OT Attack

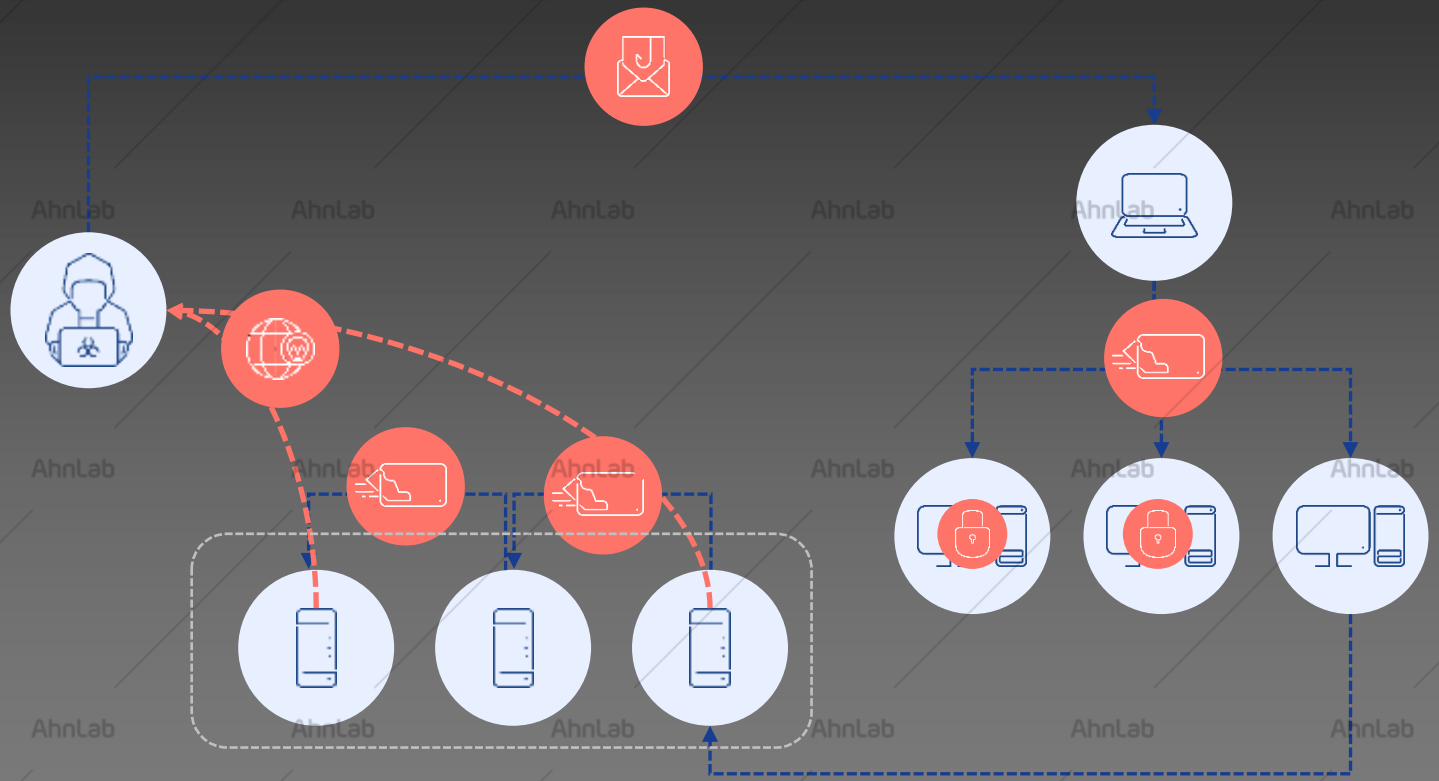
2024년 주요 사이버 보안 이슈 – 침해 사고 유형

AhnLab
30 Years of
Cybersecurity Excellence

침해사고 경험 유형 Top7



피싱 공격 침투 과정



스피어 피싱 메일 이용한 공격

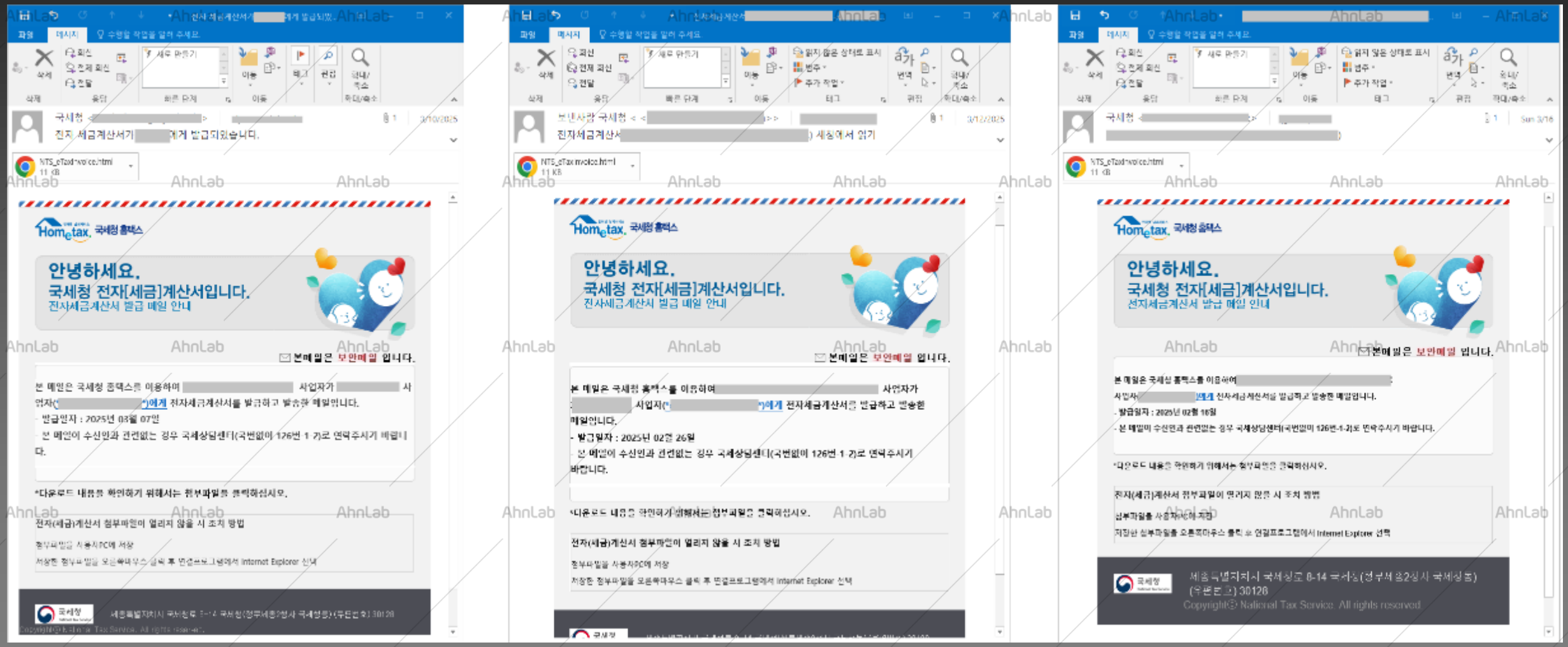
내부 스캔을 통해 관리자 접속 권한 획득

일부 관리자 접속 가능 PC 랜섬웨어 감염

서버 접속 후 정보 수집

정보 유출 의심 정황

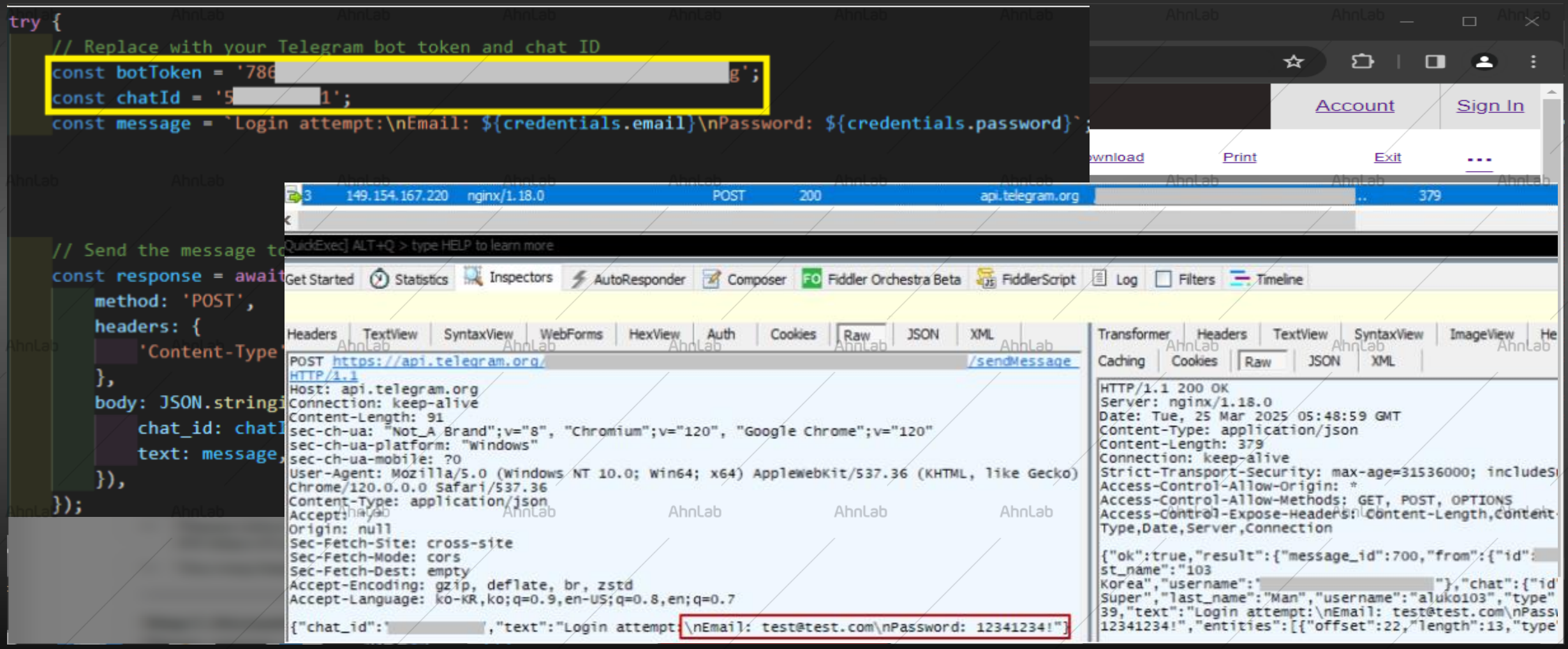
클릭 하고 싶다.. 클릭 하고 싶다..



출처: AhnLab TIP

클릭 하고 싶다.. 클릭 하고 싶다..

국세청(홈텍스) 사칭 피싱 메일 유포



출처: AhnLab TIP

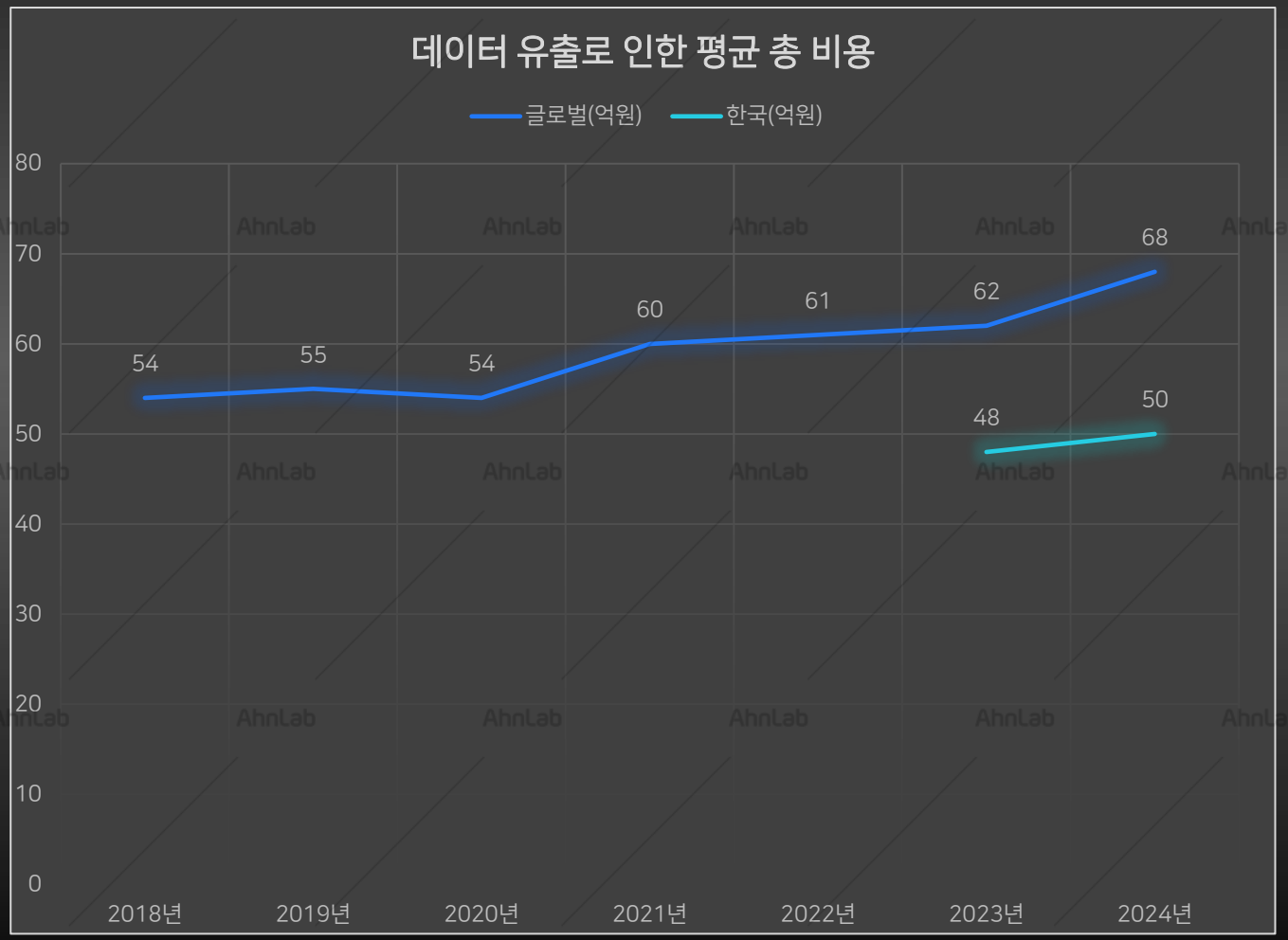
침해사고 발생으로 인한 손실 비용

2024년 피해 조직별 손실 비용은 글로벌 평균 **68억원**, 한국 평균 **50억원** 소요

- 연구기관 : Ponemon Institute (IBM 후원)
- 조사 기간 : 2023/03 ~ 2024/02
- 대상: 데이터 유출로 피해입은 604개 조직
- 범위 : 16개 국가, 17개 업종
- 방법 : 피해 조직의 CEO / CISO 3,556명 인터뷰
- 보고서 : https://www.ibm.com/reports/data-breach

유출로 인한 평균 총 비용

데이터 유출 비용의 평균치가 2023년의 445만 달러에서 488만 달러로 10% 급증했습니다. 이는 팬데믹 발발 이후 가장 높은 증가율입니다. 이러한 비용 증가를 견인한 요인은 바로 영업 손실 비용(예: 운영 중단 시간, 고객 상실 등) 및 데이터 유출 후 대응 비용(예: 고객 서비스 헬프 데스크 인력 충원, 고액의 규제 과징금 납부 등)의 상승이었습니다. 상기 비용들을 합산하면 총 280만 달러인데, 이는 지난 6년간의 영업 손실 및 데이터 유출 후 활동 관련 비용 합계 중에서도 최고 수준의 금액입니다.



* source : https://www.ibm.com/reports/data-breach 의 데이터로 재작성/ AhnLab ASEC

의료기관은 안전할까?

AhnLab
30 Years of
Cybersecurity Excellence

RansomeWare - BlackCat

UnitedHealth Group자회사 Change Healthcare 랜섬웨어 공격

- MFA(로그인시 다중 요소 인증) 미사용 을 대상으로 공격 진행
- 미국 보건복지부를 통해 시민권국이 발표한 침해 보고서에 따르면, 이 공격으로 인해 1억 명이 넘는 개인 건강 데이터 손상
- 2200만 달러 탈취, 또 탈취 해커는 이직 ..

ALPHV BlackCat - Scam 20M

Posted in Ramp Forum
Posts in thread 13
First posting Mar 3, 2024, 20:43
Most recent posting Mar 4, 2024, 11:31
Previous 10 Next 10

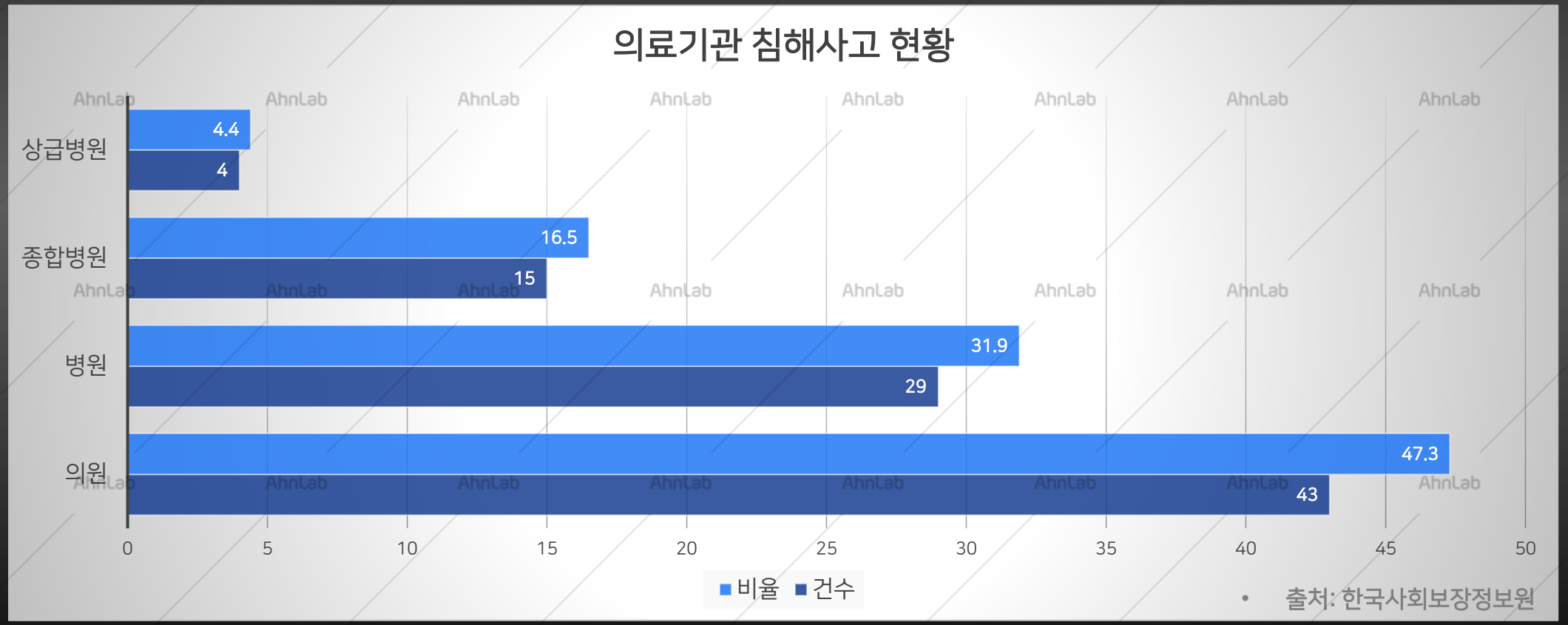
we are affiliate plus who has been work with **ALPHV** for long time and on 1st of march 2024 the victim **change healthcare** - OPTUM paid **ALPHV** 22M as ransom to prevent data leakage and decryption key.
But after receiving the payment **ALPHV** team decide to suspend our account and keep lying and delaying when we contacted **ALPHV** admin on TOX.
he kept saying they are waiting ro chief admin and the coder until today they emptied the wallet and took all the money.
sadly for the target **Change Healthcare** - OPTUM their data still with us with 4TB of the critical data the same data they were worry if it got leaked
production data that will affect all **change healthcare** & OPTUM clients.
The list of affected Change Health partners that we have sensitive data for is actually huge with names such as:
- Medicare
- Tricare
- CVS-CareMark
- **Loomis**
- **Davis Vision**
- **Health Net**
- MetLife
- **Teachers Health Trust**
- Tens of insurance companies and others

AND more!
PROOF of **ALPHV** scam:
link to the payment address :
<https://mempool.space/address/14Q5xgBHAkWxDVrnHautcm4PPGmy5cfw6b>
be careful everyone and stop deal with **ALPHV**

Post 1 of 13 by notchy on Mar 3, 2024, 20:43

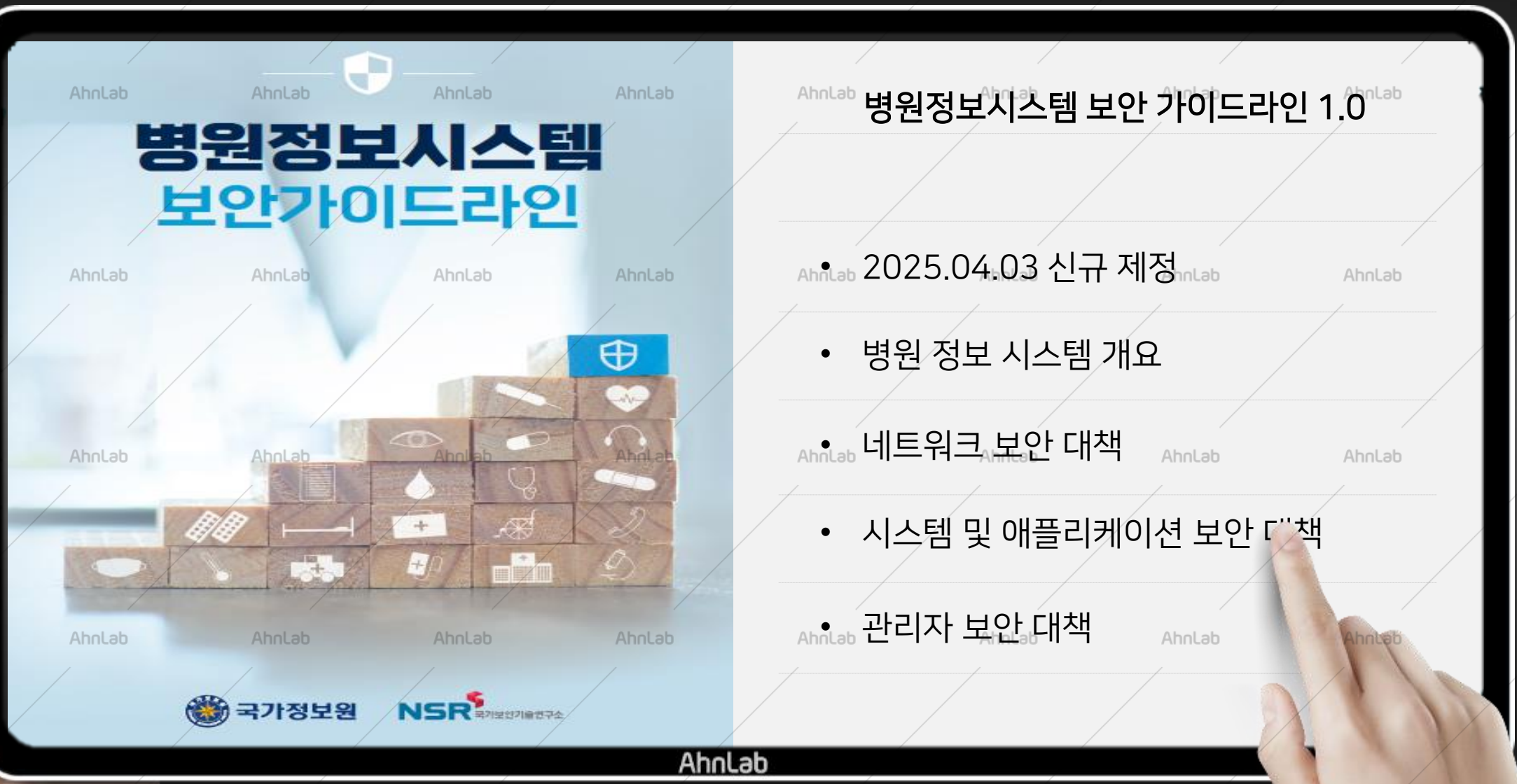
의료기관은 안전할까?

- Global : 의료 부문 84%의 조직이 IT인프라에서 사이버 공격 발견, 69%는 금전적 피해 경험
- Korea : 최근 4년간 의료 기관 진료 정보 침해사고 91건 포함 총 220건 침해 사고 발생



- 출처: 한국사회보장정보원

HIS 보안 가이드라인 1.0



IT 환경 변화에 따른 보안 전략 변화

AhnLab
30 Years of
Cybersecurity Excellence

신뢰할 수 있는 내부와 신뢰할 수 없는 외부로 경계를 나누어
바라보던 보안을 클라우드 전환과 D·T확산에 따라
경계가 무너지거나 확장되는 현상 발생

무엇이든 막을 수 있다는 **위협탐지**(Detection & Prevention) 중심에서
복원을 위해 중요자산을 보호하는
대응(Response) 중심으로 변화

지금까지 보안은 …

Who are U ?

AhnLab
30 Years of
Cybersecurity Excellence

ZERO TRUST

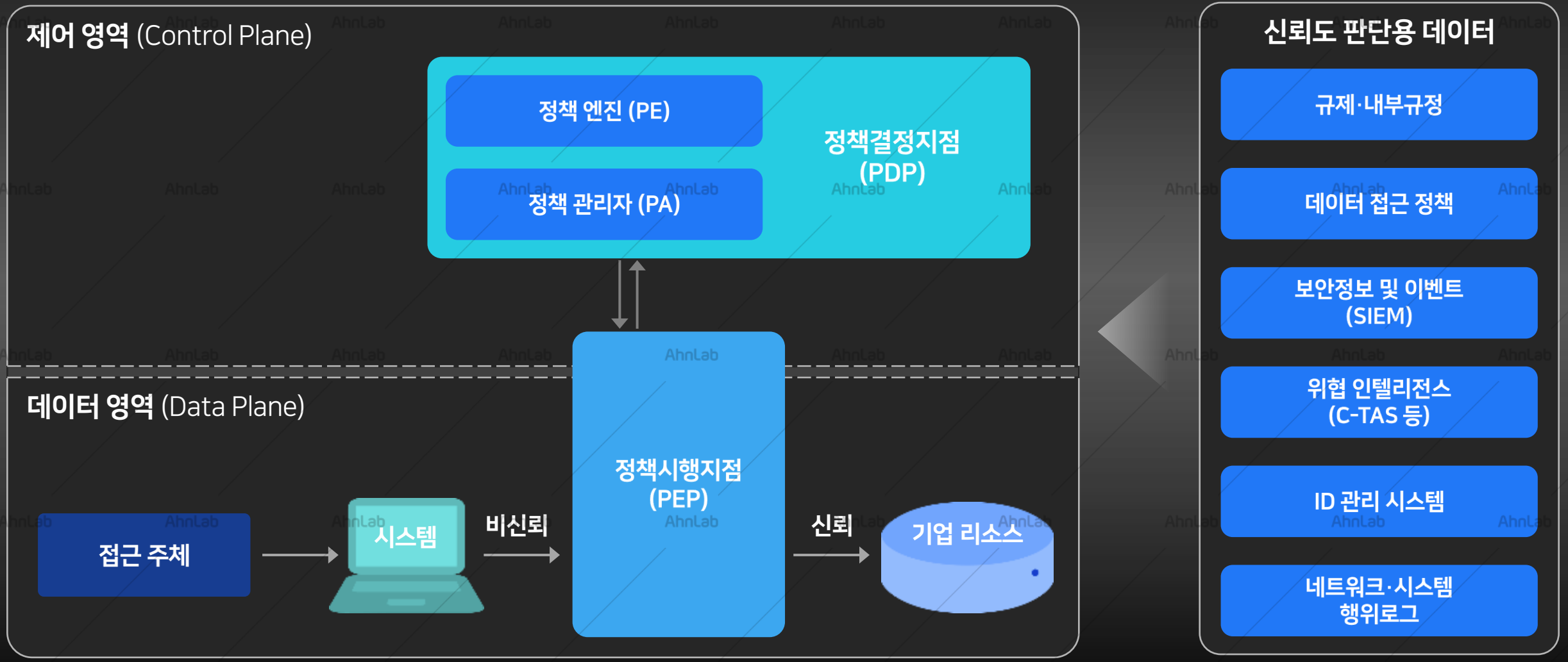
제로트러스트 기본 원리

AhnLab
30 Years of
Cybersecurity Excellence

1. 모든 종류의 접근에 대해 신뢰하지 않을 것
2. 일관되고 중앙 집중적인 정책 관리 및 접근제어 결정, 실행 필요
3. 사용자, 기기에 대한 관리 및 강력한 인증
4. 리소스 분류 및 관리를 통한 세밀한 접근제어
5. 논리 경계 생성 및 세션 단위 접근 허용, 통신 보호 기술 적용
6. 모든 상태에 대한 모니터링, 로그 및 이를 통한 신뢰성 지속적 검증, 제어

제로트러스트 아키텍처 보안모델

AhnLab
30 Years of
Cybersecurity Excellence



제로트러스트 성숙도

천리길도 한걸음부터

- 제로트러스트 가이드라인2.0 발췌

제로트러스트에 대해 정확히 이해하기 위해서는, 본 가이드라인 외에도 제로트러스트를 정의하는 대다수 문서들이 가지고 있는 공통적인 개념을 다시 한 번 생각해 볼 필요가 있다. 이 공통 개념은 다음과 같은 3가지 내용을 포함한다. 첫째, 기업망 내부 네트워크는 이미 침투당한 상태일 가능성을 포함하고 있으며, 둘째, 정확한 (신뢰도 평가에 기반하고 지속적이며 동적인) 접근 제어를 하고자 한다는 것이고, 마지막으로 제로트러스트는 **특정 기술이 아니라 보안 개념, 패러다임, 아이디어의 집합이라는 것이다.**

가. 레거시 보안 기술과 제로트러스트에 대한 이해

제로트러스트 기수로가 레거시 보안 기술은 명확히 다르거나 구분되는 기술이 아니다. 제로트러스트 아키텍처 구축을 위해서는 **레거시 보안 기술 솔루션을 모두 걷어내기 보다, 적절히 유지하면서 새로운 보안 기술을 도입·연동하면서 제로트러스트 성숙도 수준을 끌어 올릴 수 있다.**

다. '최적화 수준' 제로트러스트 아키텍처 구현의 완성

제로트러스트 아키텍처 구현은 단기간에 '최적화 수준'으로 완성하기 어려우며 **장기적인 목표와 단계적 전략 수립이 필요**하다.

AhnLab XTG

AhnLab
30 Years of
Cybersecurity Excellence

ZTNA
(Zero Trust Network Access)

SD-WAN

Lightweight VPN

Firewall

IPS

Application Control

C&C Server Detection and Block

SSL VPN
PC
PC

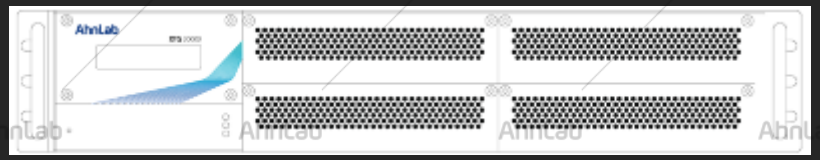
DLP
(Data Loss Prevention)

Anti-Spam

Geolocation-based Block

8 – Tuple Filtering

AhnLab XTG



Anti-Malware (AV)
File-based
Packet-based

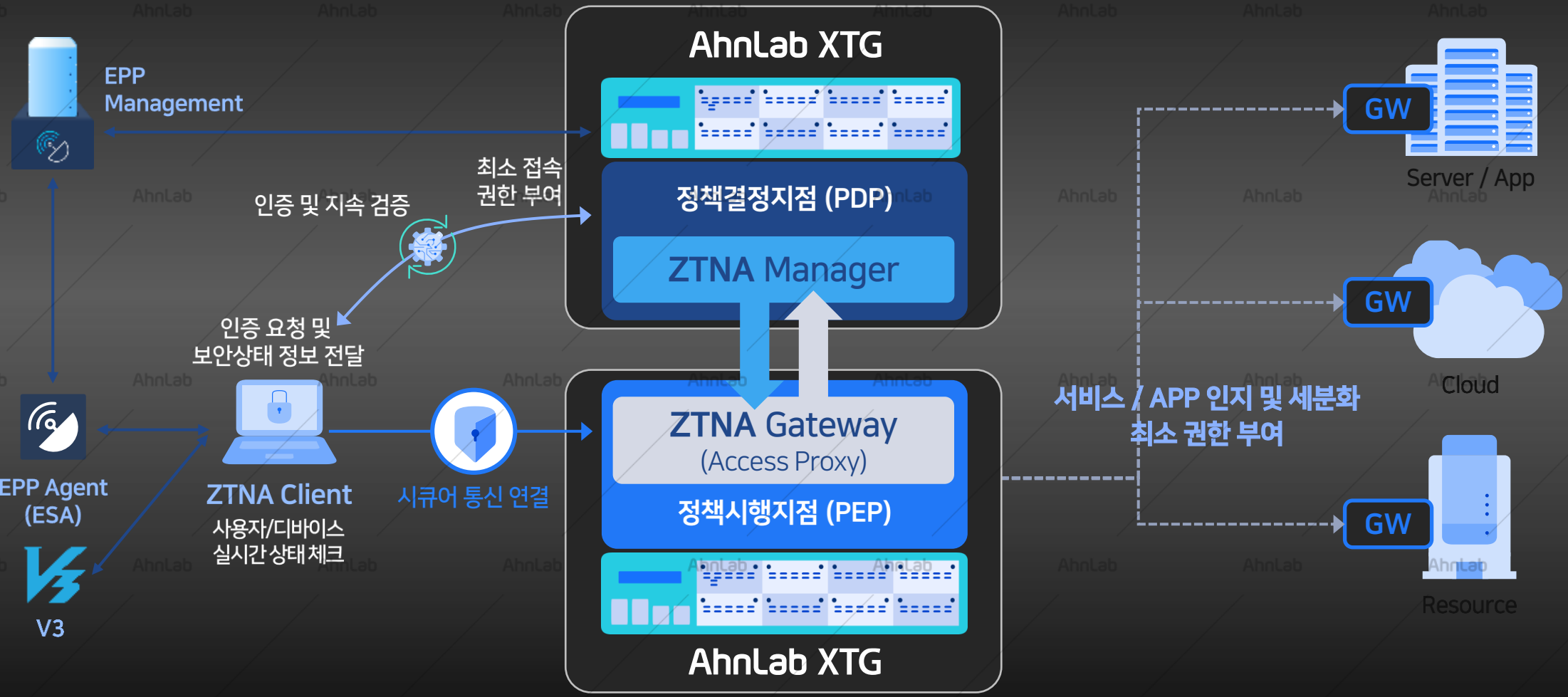
SSL Inspection
(Detects Encrypted Traffic)

IPSec VPN

Web Filtering

PQC

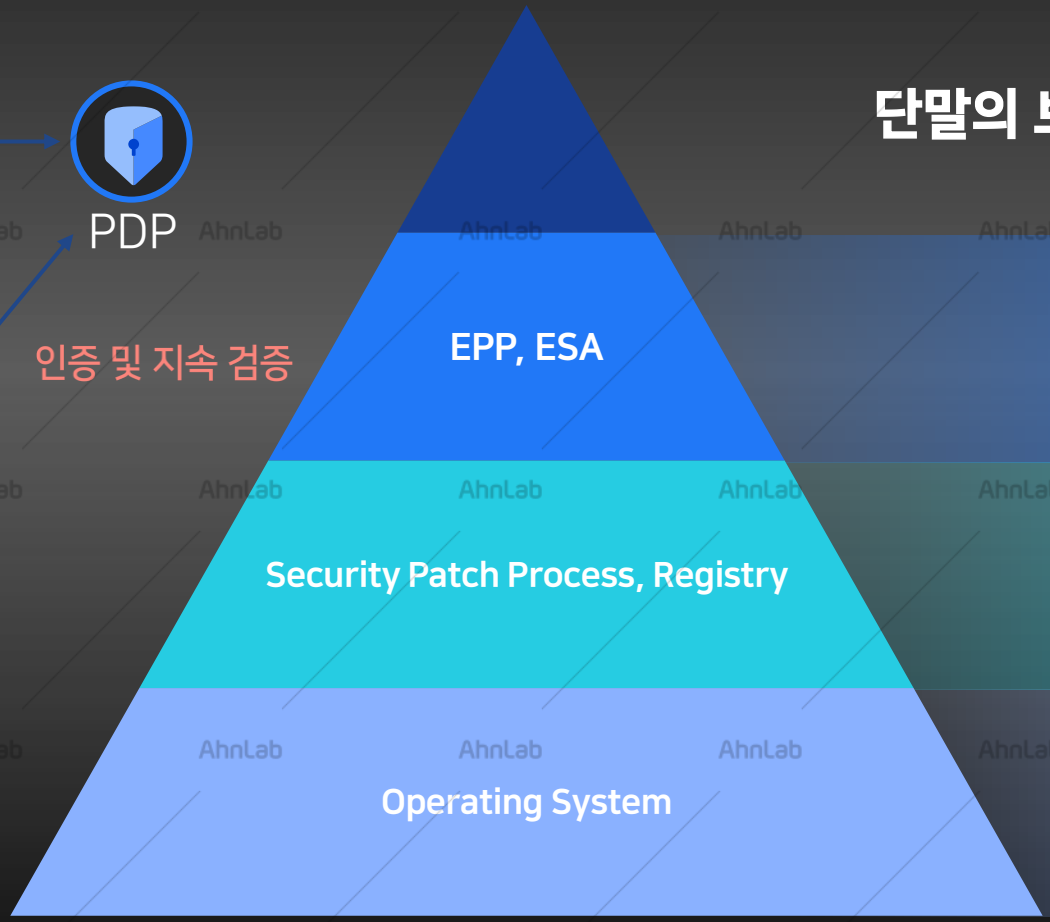
제로트러스트 아키텍처 – AhnLab XTG



모든 사용자와 디바이스의 신원을 철저히 검증하고, 최소 권한만 부여하여 접근 허용하는 ZTNA 기능 제공

제로트러스트 아키텍처 – AhnLab XTG

AhnLab
30 Years of
Cybersecurity Excellence



단말의 보안상태 변화 즉시 접속 권한 변경

백신 상태 및 AhnLab EPP/ESA 연동을 통한 단말의 보안상태 변경 추적, 보안정책 이행에 대한 점수 연동을 통한 인증

Agent가 실행되는 단말의 패치 정보, 프로세스 상태 레지스트리 조건에 따른 인증

Windows, MAC, Linux 등 단말 운영체제 별 세부 상태 체크를 통한 검증

AhnLab XTG - 제로트러스트 세부역량

AhnLab
30 Years of
Cybersecurity Excellence

ZTNA 성숙도 평가 핵심 요소

식별자·신원 Identity & User

- **식별자 관리**
  - 사용자 인벤토리
  - ID연계 및 사용자 자격증명
- **인증**
  - 다중인증(MFA)
  - 지속인증
- **위험도 평가**
  - 통합 ICAM 플랫폼
  - 행동, 컨텍스트기반 ID 및 생체인식
- **접근관리**
  - 조건부 사용자 접근
  - 최소 권한 접근

기기 및 엔드포인트 Device & Endpoint

- **정책 준수 모니터링**
  - 기기감지 및 규정 준수
- **데이터 접근제어**
  - 사용자 인벤토리
- **자산관리**
  - 사용자 인벤토리
  - ID연계 및 사용자 자격증명
- **기기 위협 보호**
  - 사용자 인벤토리
  - ID연계 및 사용자 자격증명

네트워크 Network

- **네트워크 세분화**
  - 매크로 세그멘테이션
  - 마이크로 세그멘테이션
  - 소프트웨어정의 네트워킹
- **위협 대응**
  - 위협 대응
- **트래픽 암호화**
  - 트래픽 암호화
- **트래픽 관리**
  - 데이터 흐름 매핑
- **네트워크 회복성**
  - 네트워크 회복성

시스템 System

- **접근 통제**
  - 접근 통제
- **사용자 계정 관리**
  - PAM
  - 자격 증명 관리
- **네트워크 분리 정책**
  - 네트워크 세분화 및 그룹간 이동
- **시스템보안 및 정책관리**
  - 시스템 환경에 따른 정책 관리

응용 및 워크로드 Application & Worklaod

- **애플리케이션 접근**
  - 리소스 권한 부여 및 통합
- **애플리케이션 위협보호**
  - 지속적인 모니터링 및 진행중인 승인
- **접근가능한 애플리케이션**
  - 원격 접속
- **안전한 애플리케이션 배포**
  - 안전한 애플리케이션 배포
  - 애플리케이션 인벤토리
- **S/W, 애플리케이션 보안**
  - 안전한 소프트웨어 개발 및 통합
  - 소프트웨어 위험 관리

데이터 Data

- **데이터 목록 관리**
  - 데이터 카탈로그 위험 정렬
  - 기업데이터 거버넌스
- **접근 결정방법**
  - 데이터 접근제어
- **데이터 암호화**
  - 데이터암호화 및 권한관리
- **데이터 분류**
  - 데이터 라벨링 및 태그지정
- **데이터 손실 방지**
  - 데이터 손실방지(DLP)
  - 데이터 모니터링 및 감지

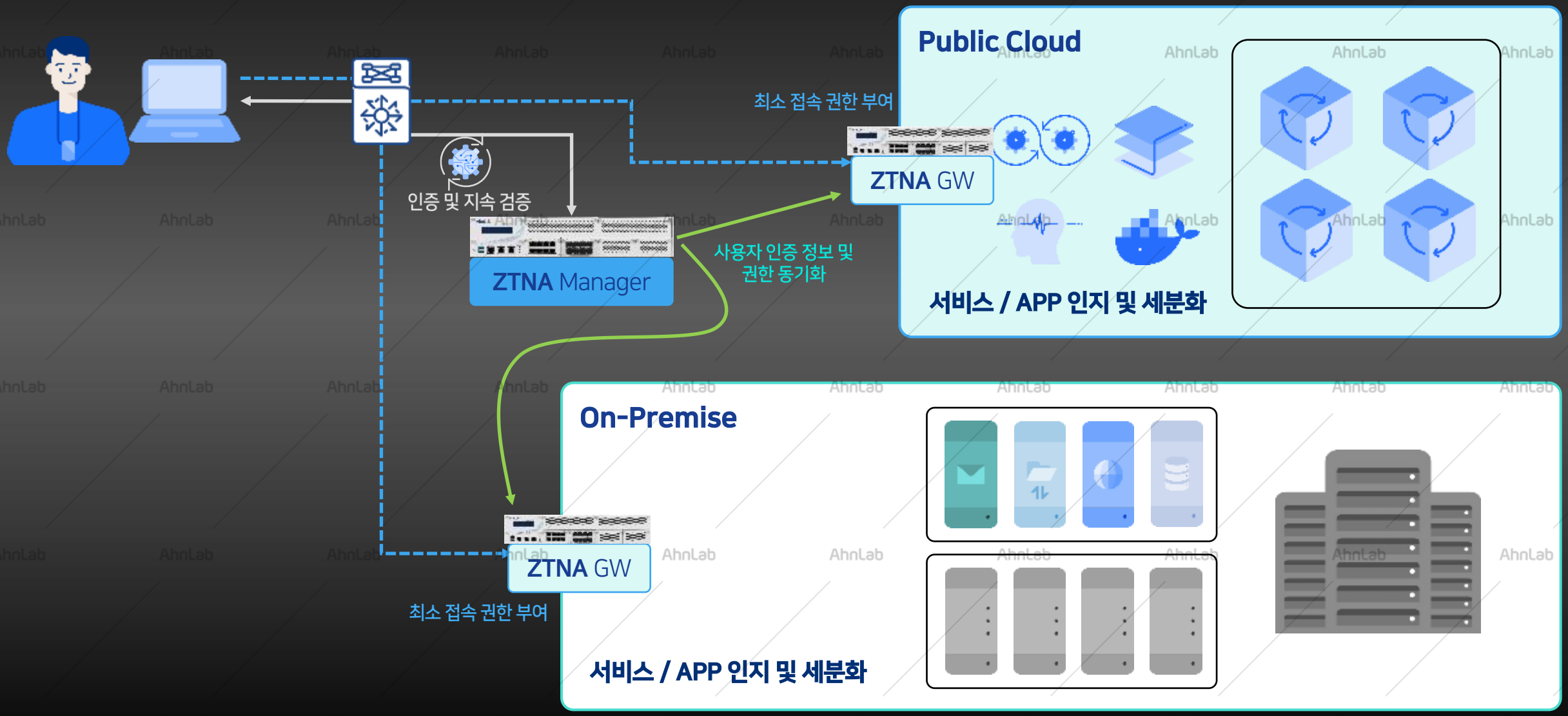
가시성 및 분석

- 모든 관련 활동 기록
- 중앙집중적 보안정보 및 이벤트 관리
- 보안 위협 분석
- 사용자 및 기기동작분석
- 위협 인텔리전스 통합
- 자동화된 동적 정책

자동화 및 통합

- 정책 통합
- 중요 프로세스 자동화
- 인공지능
- 보안통합, 자동화 및 대응
- 데이터 교환 표준화
- 보안운영 조정 및 사고 대응

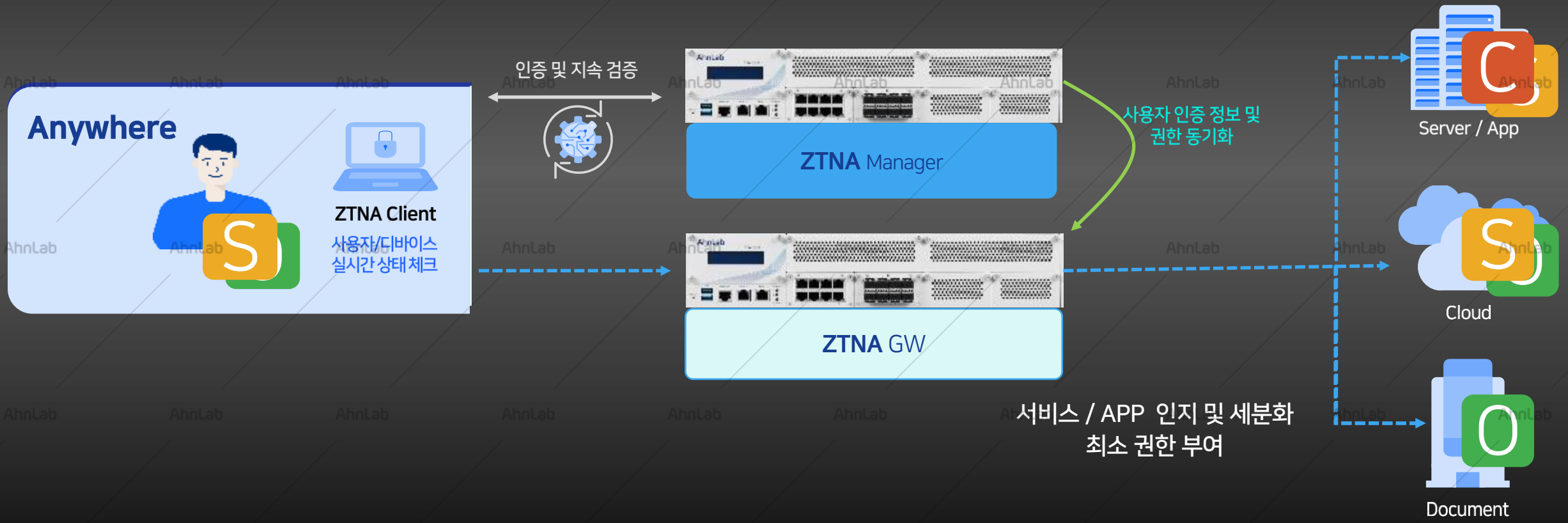
AhnLab XTG 운영



AhnLab XTG 운영

AhnLab
30 Years of
Cybersecurity Excellence

동일 단말/사용자의 업무 위치에 의한 접속 권한 제어



AhnLab XTG(ZTNA) + EDR + XDR

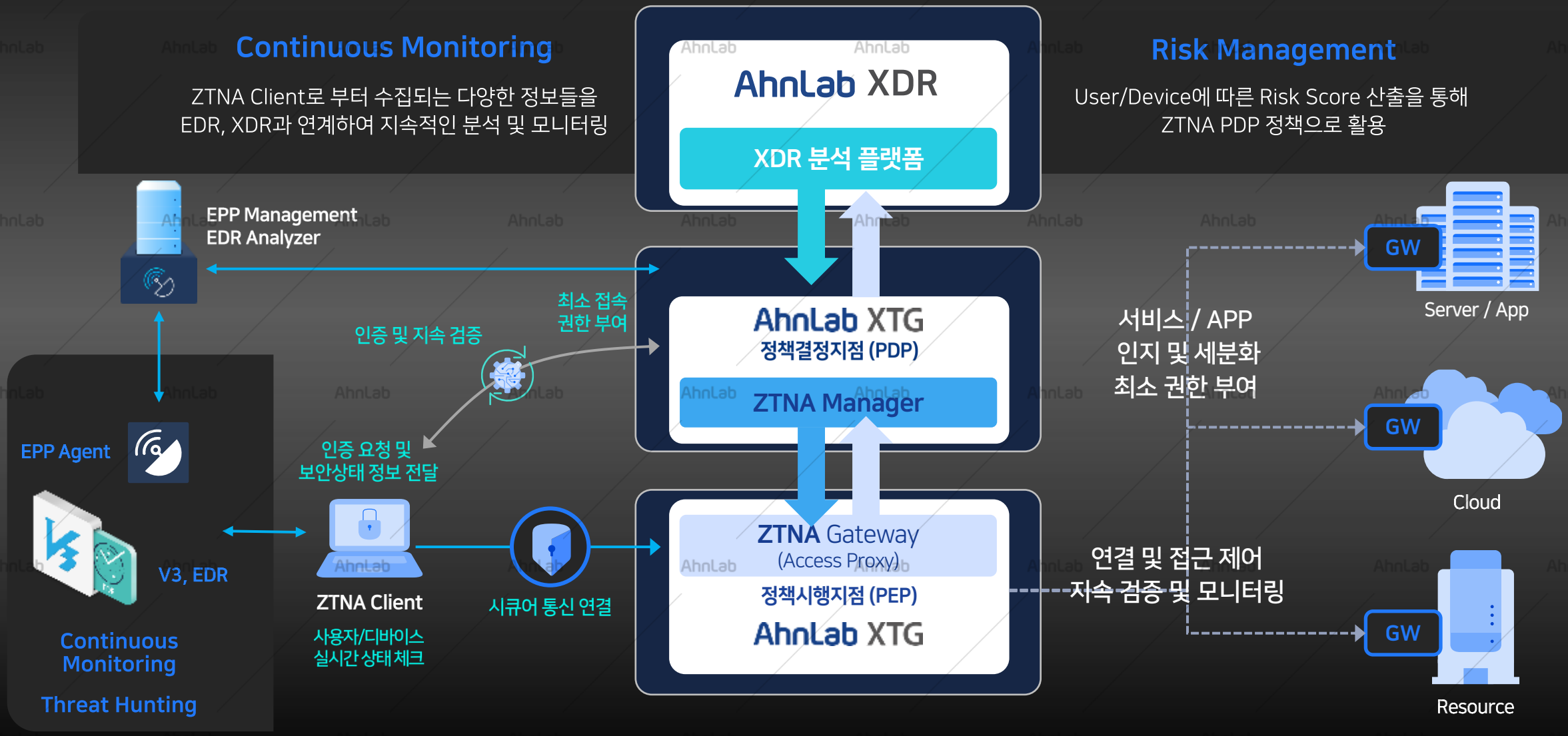
AhnLab
30 Years of
Cybersecurity Excellence

Continuous Monitoring

ZTNA Client로 부터 수집되는 다양한 정보들을
EDR, XDR과 연계하여 지속적인 분석 및 모니터링

Risk Management

User/Device에 따른 Risk Score 산출을 통해
ZTNA PDP 정책으로 활용



AhnLab
30th Anniversary

감사합니다.

AhnLab
30 Years of
Cybersecurity Excellence