

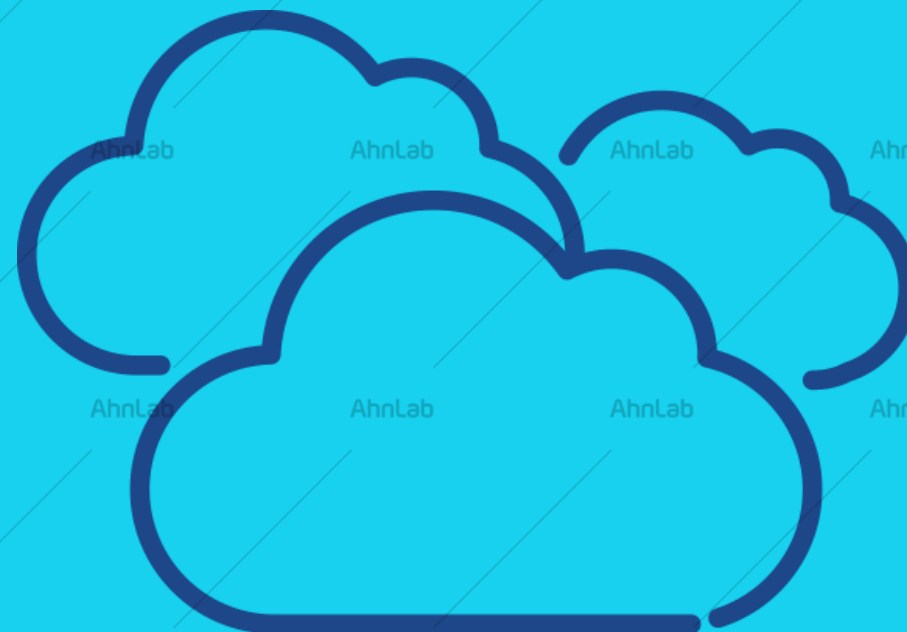
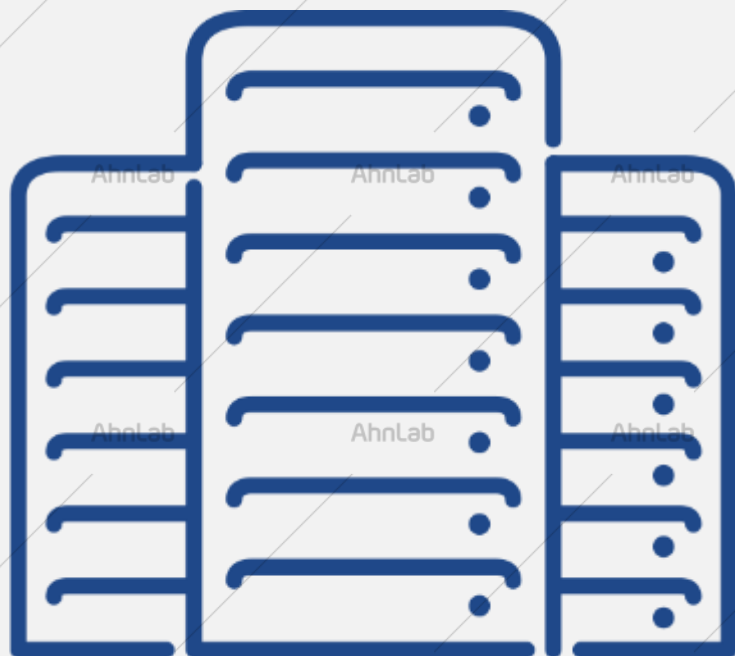
# 클라우드 서비스 수준별 개인정보보호 적용 방안

클라우드사업본부 SaaS솔루션팀 김경민 수석

More security,  
More freedom

AhnLab

# 클라우드 전환



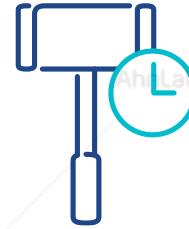
# 클라우드 전환의 어려움



복잡성, 다양성



클라우드 보안



규정 준수



책임 공유 모델

# 클라우드 전환의 어려움



책임 공유 모델



데이터 액세스와 권한 관리에 대한 책임



암호화 적용 및 약한 암호화 알고리즘



네트워크 및 채널 보안

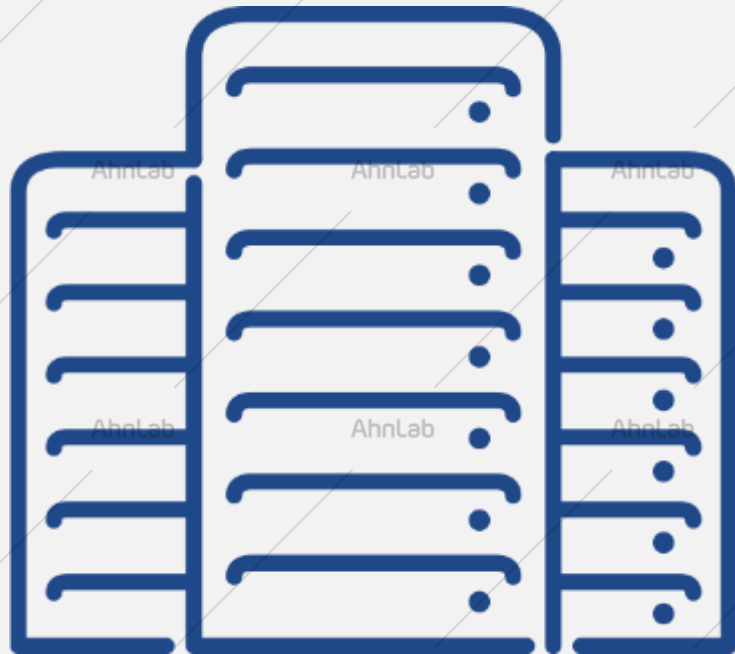


감사, 로깅 및 모니터링

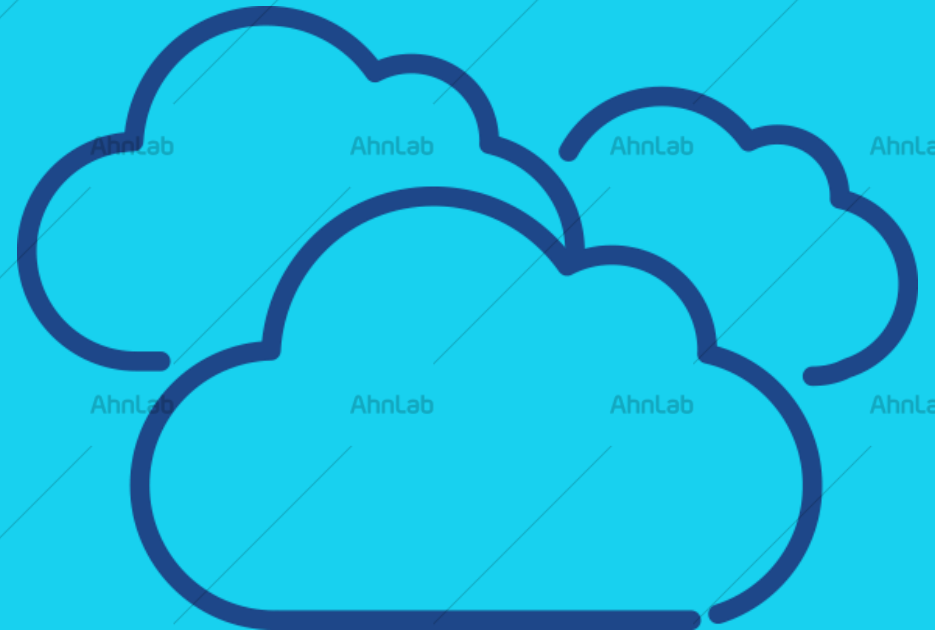


서비스 업데이트

# 클라우드 송환



Cloud  
Repatriation



# 데이터 보호

## Access Management

AD Integration

RBAC

MFA

Granular Permission

## Network Control

Security Group

Jump Servers

NACLs

## Perimeter Network Control

Firewall

IDS/IPS

Detonation

Proxy

White/Black List

DoS Protection

## VM Management

Patch Management

Image Management

System Hardening

Base S/W Management

Tag Asset Management

## Data Protection

Encryption

Data Residency

PII Evaluation

## Governance & Incident Management

Cloud API

Logging

Monitoring

APT

Forensics

## Scalability Reliability

CDN

Self-healing

Redundancy

DR Plan

# 데이터 암호화

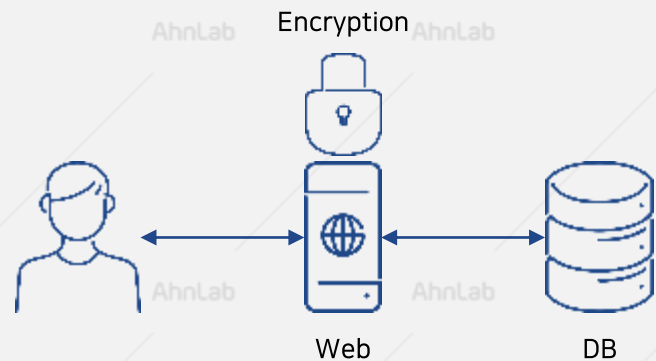
## 제24조 (고유식별정보의 처리 제한)

- ☑ 개인정보처리자가 제1항 각 호에 따라 고유식별정보를 처리하는 경우에는 그 고유식별정보가 **분식·도난·유출·위조·변조 또는 훼손되지 아니하도록** 대통령령으로 정하는 바에 따라 **암호화** 등 안전성 확보에 필요한 조치를 하여야 한다.

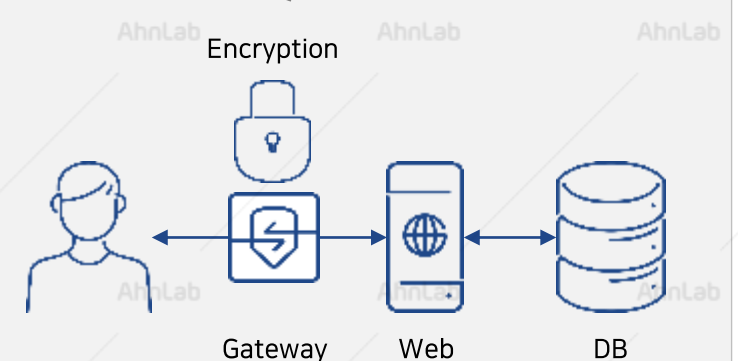
### Plug-in



### API



### Secure Gateway

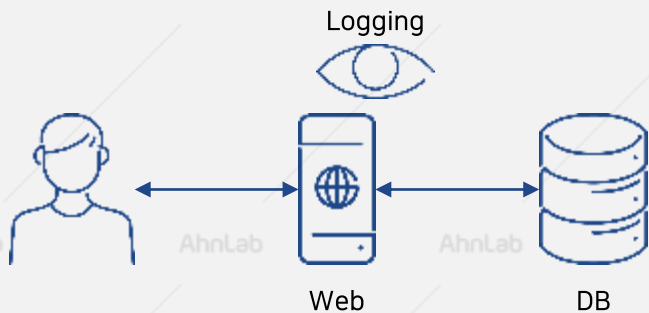


# 개인정보 접속기록 관리

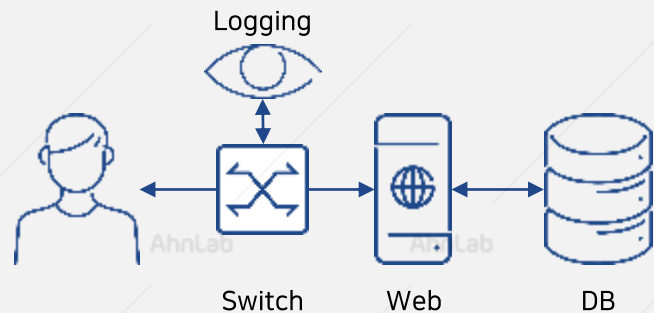
## 제29조 (안전조치의무)

- ☑ 개인정보처리자는 개인정보가 분식·도난·유출·위조·변조 또는 훼손되지 아니하도록 내부 관리계획 수립, 접속기록 보관 등 대통령령으로 정하는 바에 따라 안전성 확보에 필요한 기술적·관리적 및 물리적 조치를 하여야 한다.

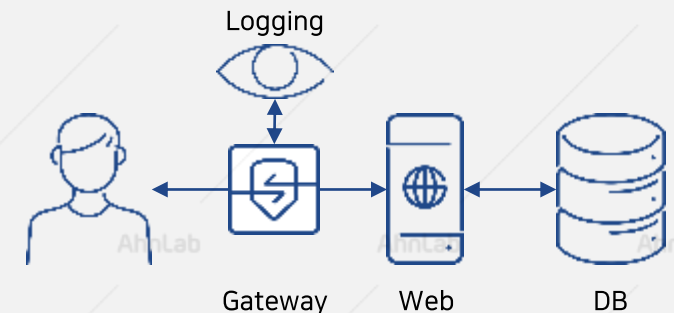
### Byte Code Instrumentation



### Network Mirroring



### Secure Gateway





# 개인정보 탐지 및 노출 차단

### 제34조의2 (노출된 개인정보의 삭제·차단)

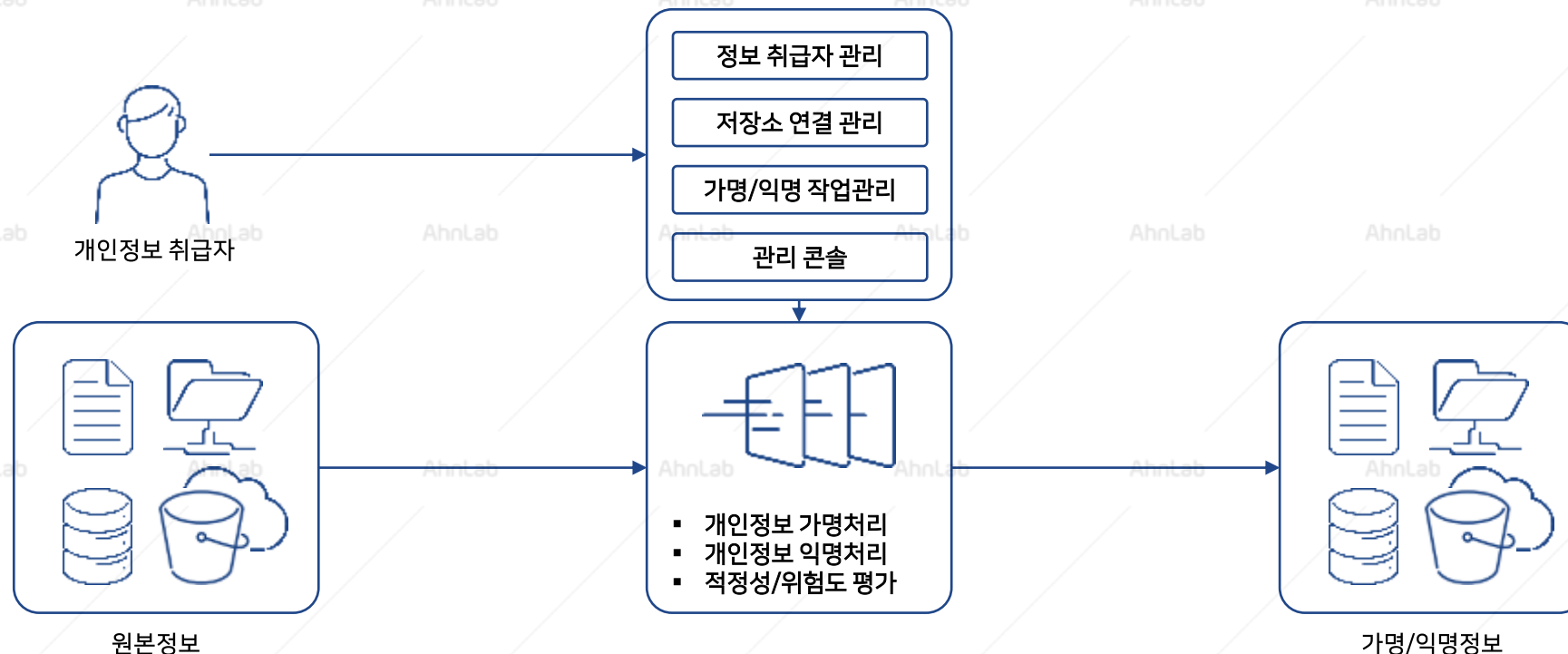
☒ 개인정보처리자는 **학교유식별정보, 계좌정보, 신용카드정보 등 개인정보**가 정보통신망을 통하여 **공중(公衆)에 노출되지 아니하도록** 하여야 한다



# 데이터 활용을 위한 비식별화

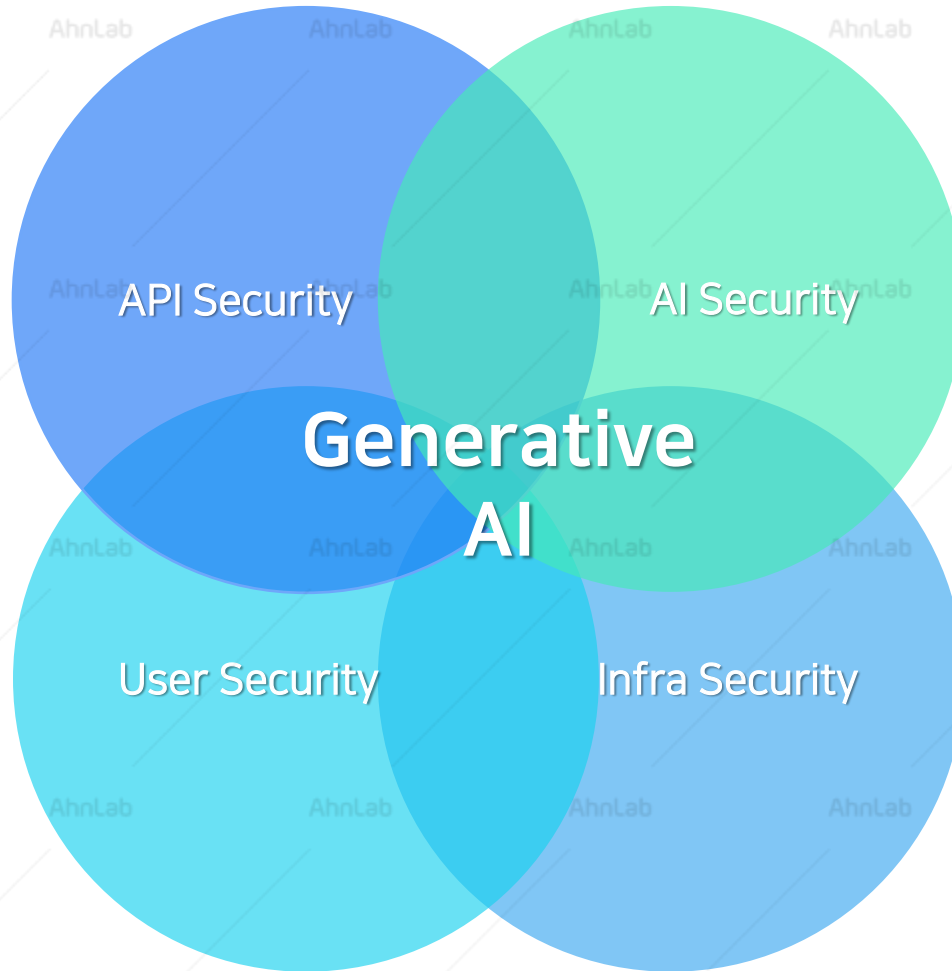
## 가명정보 처리 가이드라인

- ☑ 데이터3법\*이 시행('20.8.5.)되어 개인정보처리자가 통계작성, 과학적 연구, 공익적 기록보존 등을 위한 목적으로 개인정보를 **가명처리하여 활용**할 수 있는 기반이 새롭게 마련됨



# 생성형 AI를 위한 보안

- Prompt Injection
- Insecure Output Handling
- Sensitive Information Disclosure
- Model Denial of Service
- Overreliance



- Training Data Poisoning
- Model Theft
- Model Denial of Service
- Sensitive Information Disclosure
- Excessive Agency
- Supply Chain Vulnerabilities
- Insecure Plugin Design

\* Ref: OWASP Top 10 for LLM v1.0 (2023.08)

# 생성형 AI를 위한 보안 솔루션 아키텍처

## API

### Prompt Injection

- Prompt Injection Detector

### Insecure I/O Handling

- Access Control
- Source Code/Script Filter
- Blacklisting

### Sensitive Information Disclosure

- De-identification
- Confidential Information Detector
- PII/SPI Detection Model

### Model Denial of Service

- Heavy Operation Detector

## Gen AI

### Training Data Poisoning

- Data Cleansing
- De-identification
- Confidential Information Detector

### Model Theft

- Access Control

### Supply Chain Vulnerabilities

- Security Consulting
- Whitelisting
- Incident Response Process

### Prediction of Response

- AI Engineering, Data Analysis
- Domain Expert
- MLOps

## Plugin/Tool

### Insecure Plugin Design

- Malware Detection
- Data Loss Prevention
- Access Control
- Security Consulting

### Supply Chain Vulnerabilities

- Security Consulting
- Whitelisting

## Knowledge Base







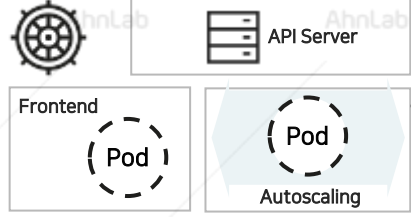
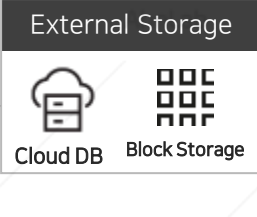
### Training Data Poisoning

- Data Cleansing
- De-identification
- Confidential Information Detector

## Infra Security

\* Ref: OWASP Top 10 for LLM v1.0 (2023.08)

# 클라우드 전환 수준 별 보안 고려 사항

	Data Center	Cloud	
Rehost	 <p>Database on VM</p>	 <p>Database on Cloud VM</p>	<p>주요 인프라 수준에서의 보안 고려 사항이 중요</p> <ul style="list-style-type: none"> <li>• 데이터 암호화</li> <li>• 기존 서비스 네트워크의 In/Out Bound 정책</li> <li>• IAM 활용과 접근 제어, 로깅 및 감사 기능의 활용</li> <li>• 소스코드 수정 없이 적용 할 수 있는 데이터 보안 서비스</li> <li>• 데이터 활용 및 개인정보의 대외 전송 여부를 위한 비식별화</li> <li>• 클라우드 이전이 불가능한 시스템 및 인프라 식별</li> </ul>
Replatform	 <p>Database on VM</p>	 <p>Cloud DB</p>	<p>주요 인프라 수준에서의 보안 고려와 클라우드 보안 도구의 활용</p> <ul style="list-style-type: none"> <li>• 클라우드 지원 인프라에 대한 보안 업데이트 및 패치 관리</li> <li>• 인프라의 보안 및 HA 구성 강화 (WAF, Load-balancer 등)</li> <li>• 기존 보안 솔루션의 동작 여부 및 라이선스 정책 확인</li> <li>• 소스코드 수정 및 취약점 보안을 위한 범위, 비용 및 시간 산정</li> </ul>
Refactor	 <p>Application on VM</p>	 <p>Kubernetes Service</p>	<p>클라우드의 다양한 보안 기능을 적극 활용</p> <ul style="list-style-type: none"> <li>• 보안 규정, 감사 및 모니터링</li> <li>• 클라우드 인프라의 유연성 확보 및 보안 서비스 활용 (Auto-scaling, Security Monitoring)</li> <li>• 서버리스 아키텍처를 위한 보안, 컨테이너 보안 검토</li> <li>• 보안 코딩 및 개발 프로세스 강화</li> <li>• CI/CD 파이프라인 구축을 통한 보안 테스트 및 코드 검토 자동화</li> </ul>
Rearchitect	 <p>Frontend API Server</p>	 <p>Pod Autoscaling External Storage Cloud DB Block Storage</p>	<p>클라우드의 다양한 보안 서비스를 활용하여, 새로운 보안 고려 사항에 대응</p> <ul style="list-style-type: none"> <li>• Native SaaS 보안 서비스를 활용하여, 네트워크, 데이터, 인프라 보안 강화</li> <li>• MSA를 위한 보안 아키텍처 검토</li> <li>• 서비스의 고가용성 및 재해 복구 전략 수립</li> <li>• DevSecOps 보안 코딩 원칙 수립 및 준수</li> </ul>

# AhnLab Data Security

## Next - Generation MSP

- '보안'에 기반한 클라우드 구축/운영



### AhnLab Privacy Scanner for Web

웹서비스에 노출되어 있는 개인정보/민감정보를 탐지



### AhnLab Privacy Filter for Web

웹서비스에 민감정보나 금치어의 무단 업로드를 방지



### AhnLab Access Log Manager

개인정보 접속기록을 관리하고 이상징후를 탐지



### AhnLab Data Encryption

어플리케이션 레벨의 데이터 및 데이터베이스 암호화



### AhnLab De-identification

개인정보 데이터 활용을 위한 개인정보 비식별화

# 믿을 수 있는 조력자

## 클라우드 컨설팅

클라우드 구축/운영/보안을  
고려한 전문적인 컨설팅



## 클라우드 구축

안랩의 보안프레임워크 기반  
가장 안전한 클라우드 설계



## 클라우드 운영

효율적이고 체계적인  
클라우드 운영 지원



## 클라우드 보안

클라우드 환경에 필요한  
보안요소들을 모두 해결



## 데이터/AI 보안

데이터 및 AI를 위한  
보안 아키텍처 및 솔루션



AhnLab 보안 프레임워크



A person in a brown suit is walking up a long, wide staircase that recedes into the distance. The staircase is made of light-colored stone or concrete. Above the person, the sky is a clear, bright blue with a few wispy white clouds. A large, white, stylized checkmark is superimposed on the sky, pointing downwards towards the person. The overall scene conveys a sense of achievement and progress.

# The MSP must ensure customer success

## AhnLab Cloud