안전한 클라우드 환경 구성을 위한 보안 전략

위수복 / NHN Cloud 클라우드보안실

목차

01 들어가기 전

02 보안 백서 발간 배경

03 보안 백서의 구성과 주요 내용

04 보안을 고려한 환경 구성 전략

들어가기 전

NHN Cloud

NHN Cloud On

2015 2023

121

210

NHN Cloud

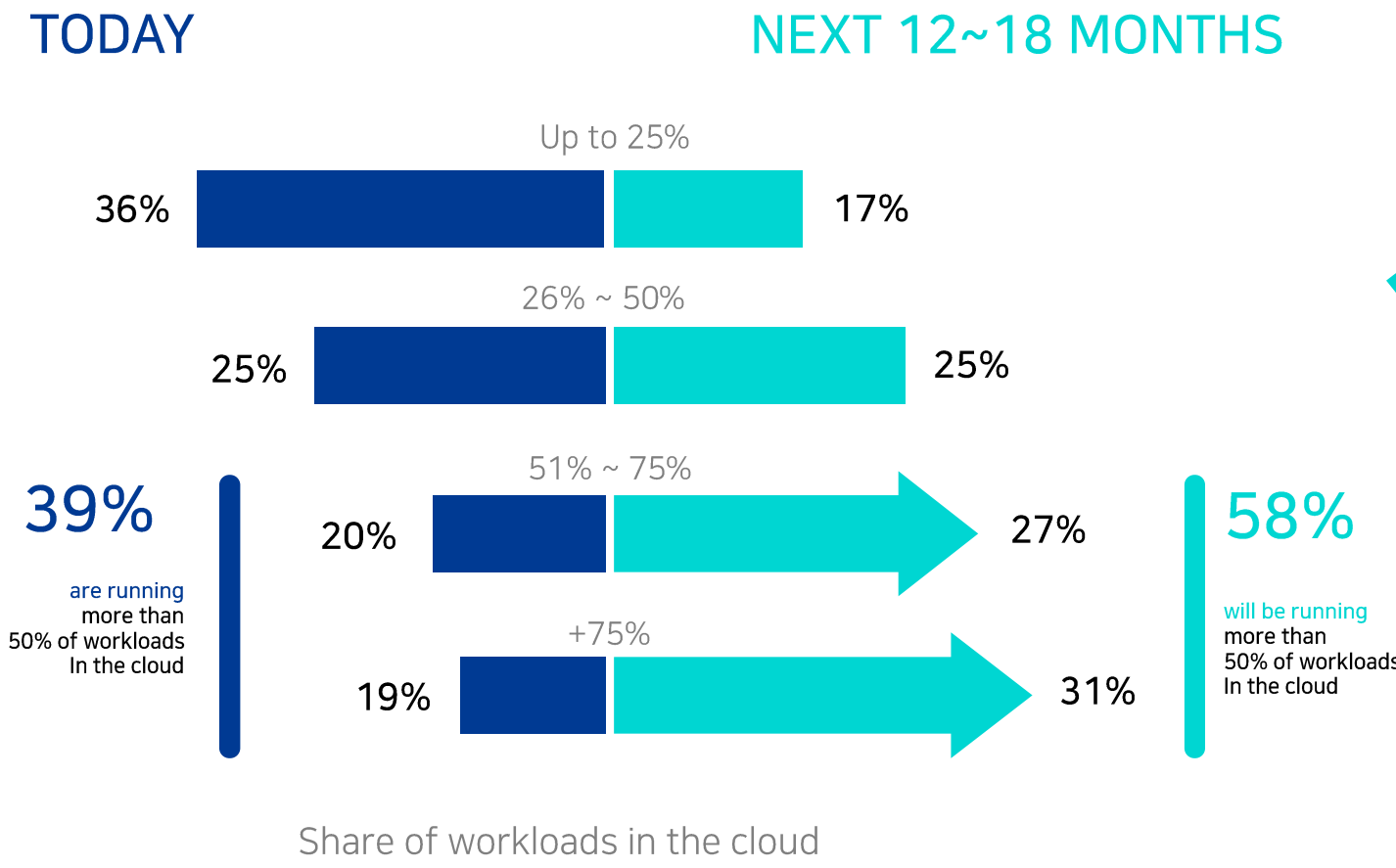
NHN Cloud On

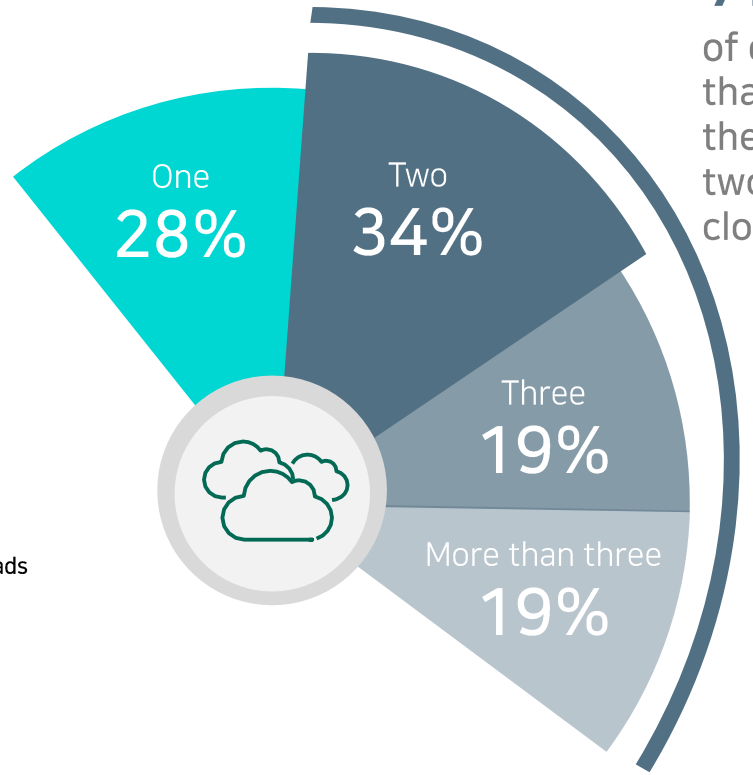
400

4800

클라우드 보안 백서 발간 배경

클라우드 전환은 자연스러운 변화





72%
of organizations that are in the cloud use two or more cloud providers

2023 Cloud Security Report(ISC)² ,Cybersecurity INSIDERS

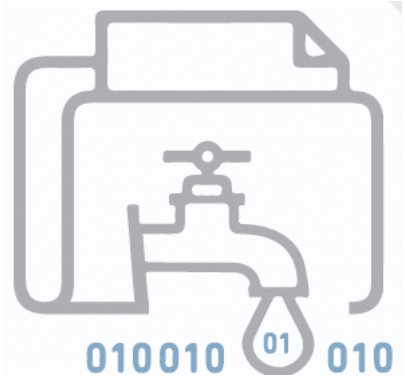
그러나 클라우드 도입의 장벽은 아직도…

37%

Lack of staff resource
of expertise

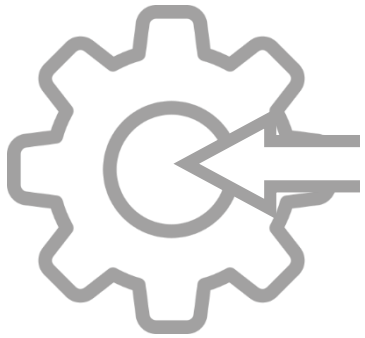
30%

Legal & regulatory
compliance



29%

Data security,
Loss & leakage risks



27%

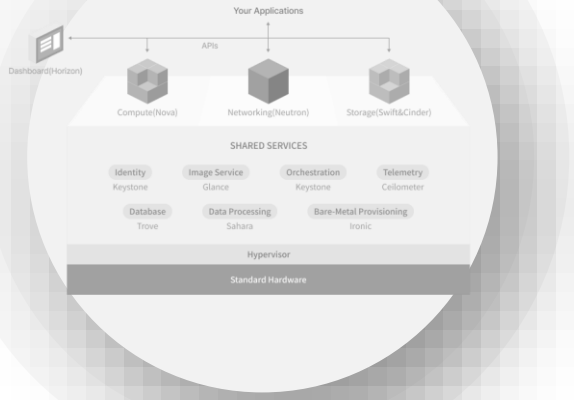
Integration with
Existing IT environment

Cost/lack of ROI 21% | Internal resistance and inertia 20% | Loss of control 19% | Complexity managing cloud deployment 18% | Lack of transparency and visibility 15% | Billing & tracking issues 14% | Lack of maturity of cloud service models 13% | Lack of management buy-in 13% | Dissatisfaction with cloud service offerings/performance/pricing 12% | Lack of customizability 10% | Lack of support by cloud provider 8% | Performance of apps in the cloud 8% | Availability 8% | Other 5%

2023 Cloud Security Report(ISC)[2] ,Cybersecurity INSIDERS

고민 해결을 위해 무엇을 해야 할까?

NHN Cloud



NHN Cloud는 OpenStack을
기반으로 다양한 서비스를
유연하고 안전하게 제공

컴플라이언스

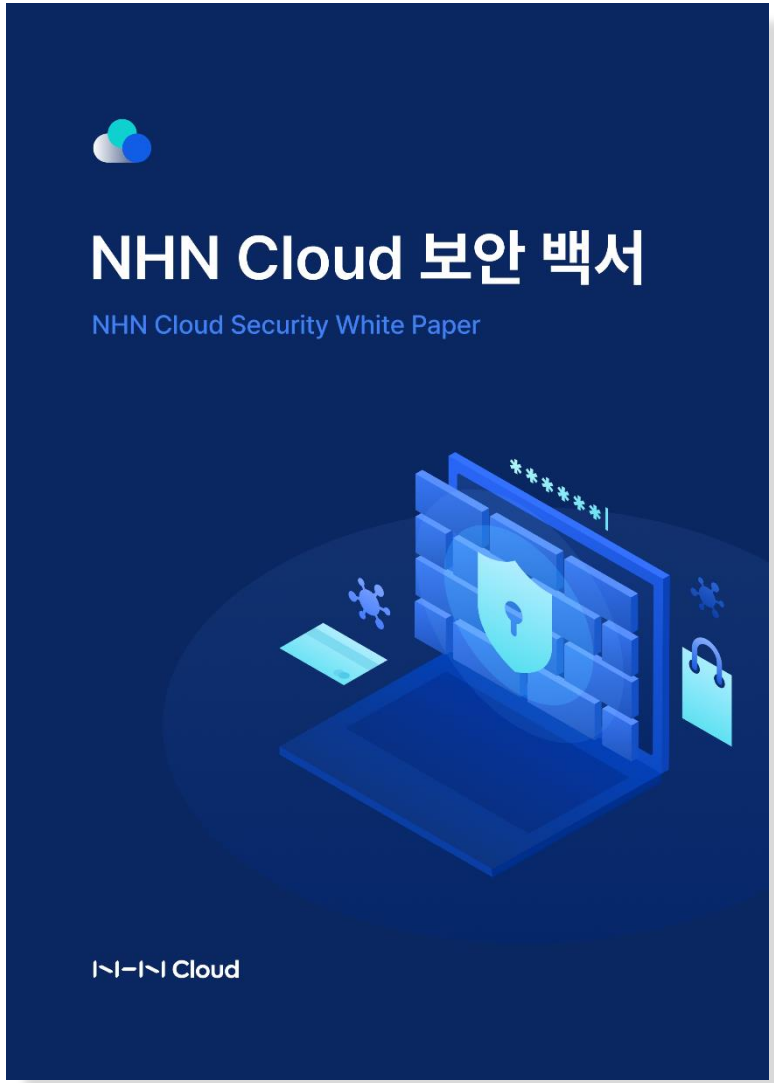
클라우드 인증 및 안정성
확보를 위해 NHN Cloud는
물리적 · 관리적 · 기술적 보안 제공

보안 아키텍처

이전 On-premise 수준의 보안을
담보하기 위한 주요 서비스 구간의
보안 아키텍처 구성

보안 백서의 구성과 주요 내용

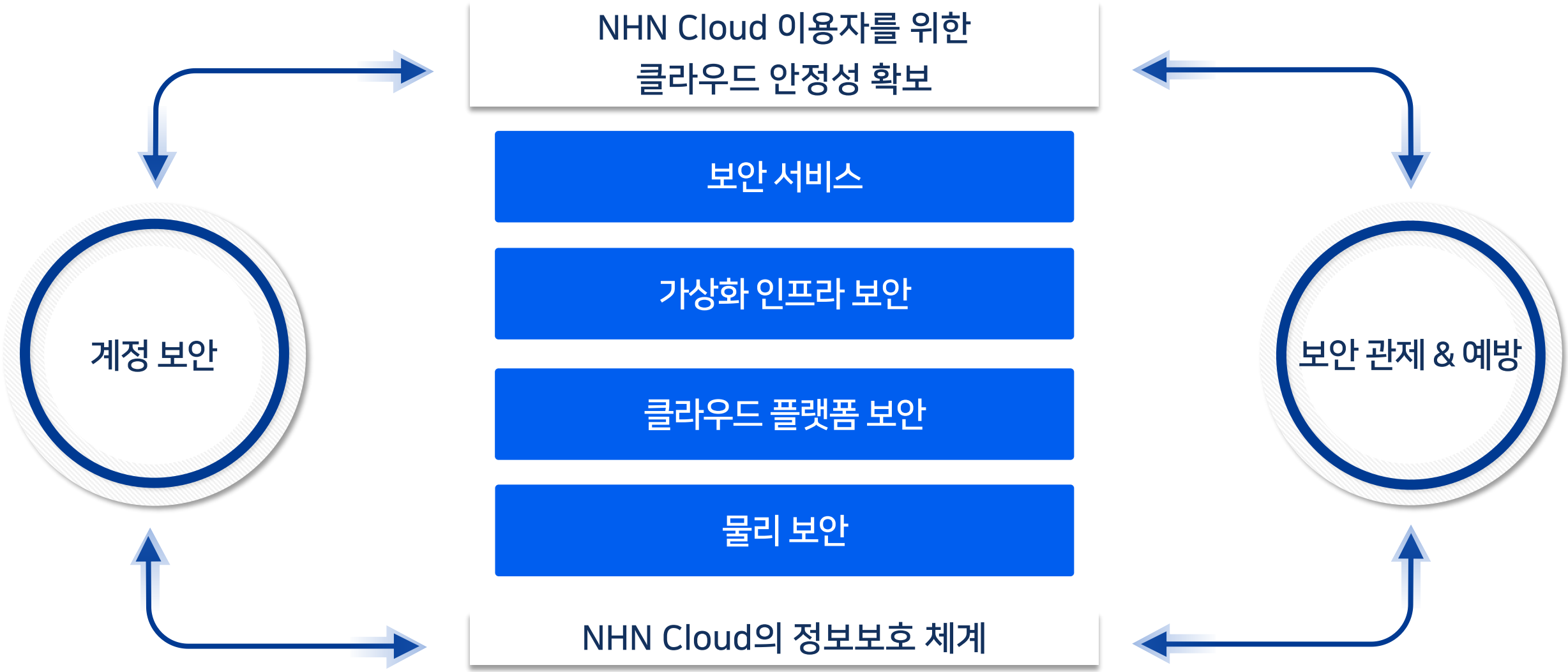
NHN Cloud Security White Paper



NHN Cloud의 보안은?

- 목적
  - NHN Cloud의 클라우드 환경, 보안 체계, 서비스의 보안 요소를 이해하고 활용하기 위해
- 대상
  - NHN Cloud의 서비스를 이용하시는 분
  - NHN Cloud에 관심 있는 모든 분
- 구성
  - 2장 8절
  - 1장. 클라우드의 이해와 개념(#1)
  - 2장. NHN Cloud의 보안(#2~#8)

보안 백서의 프레임워크


NHN Cloud 이용자를 위한
클라우드 안정성 확보
보안 서비스
가상화 인프라 보안
클라우드 플랫폼 보안
물리 보안
NHN Cloud의 정보보호 체계
계정 보안
보안 관제 & 예방

보안 백서의 구성 및 주요 내용

#1 클라우드 컴퓨팅 개념

클라우드 개념
클라우드 서비스의
장점 · 제공 · 형태 · 유형

클라우드 보안 위협
관리적 / 기술적 보안 위협

보안 책임 공유 모델
제공자 / 이용자의 책임과 역할

#2 정보보호 체계

정보보호 관리 체계
정책 · 조직 · 프로세스

규정 준수와 인증
법령 · 규정 · 정보보호 인증

비즈니스 연속성 관리
서비스 연속성 확보

#3 물리보안

환경 및 설비 보안 관리
화재 · 항온 · 항습 · 전력

출입 통제
기준 · 구역 · 보안 등급 · CCTV

자료 및 설비 관리
자료 관리 및 설비 점검

#4 클라우드 플랫폼 보안

호스트 보안
침입 탐지 · 취약점 점검· 하드닝

데이터 보안
저장 장치 · 암호화
데이터 보호 · 데이터 폐기

네트워크 보안
가용성 영역 · 영역 분리
망 분리 · 접근 통제 · DDoS 대응

가상화 보안
하이퍼바이저 보안
격리(컴퓨트, 스토리지, 네트워크)

보안 백서의 구성 및 주요 내용

#5

계정 보안

멤버

조직 · 프로젝트 · 회원 · IAM

인증

MFA · 접근 통제
키 페어 · API 보안

권한 부여

회원 · IAM
조직 / 프로젝트 역할

감사(Audit)

CloudTrail

#6

보안 관제 및 예방

위협 탐지 및 대응

보안 위협 관제 / 분석 센터
침해 사고 대응

취약점 점검 및 모의 훈련

모의 해킹 · 소스 코드 진단
취약점 점검 · 침해 모의 훈련

#7

가상화 인프라 보안

Compute

Instance · 보안 그룹 · 키 페어
IP/MAC Spoofing 방어

컨테이너

NKS · NCS · NCR

스토리지

Block Storage · NAS
Object Storage · Backup

네트워크

VPC · Load Balancer
X Gateway

데이터베이스

태넌트 분리 · 고가용성
접근 제어 · 백업 및 복구

#8

보안 서비스

취약점 점검

Server · APP Security Check

네트워크 보안

Basic · Security Monitoring
DDoS Guard · Web Firewall

시스템 보안

Vaccine · App Guard
WebShell Threat Detector

보안 관리

SIEM · Security Compliance

암호 및 인증

Secure Key Manager

1. 클라우드 컴퓨팅 개념

보안 책임 공유 모델

클라우드 제공자와 이용자의 역할과 책임을 확인하고 보안 확립

Shared Security Responsibility Model (SSRM)

- 클라우드 서비스 제공자와 클라우드 서비스 이용자의 책임과 역할 분류 및 명시
- 서로 협력해 각자의 통제 요소를 보호하여 클라우드 전반의 안전한 보안을 확립

분류	온프레미스	IaaS	PaaS	SaaS
클라우드 포털 고객 영역	●	●	●	●
데이터	●	●	●	●
애플리케이션	●	●	●	◐
가상 네트워크	●	●	●	◐
운영체제	●	●	●◐	◐
하이퍼바이저, 클라우드 소프트웨어	●	◐	◐	◐
물리 시스템 (시스템, 스토리지, DB, 네트워크)	●	◐	◐	◐
물리 시설	●	◐	◐	◐

● CSC(cloud service customer) ◐ CSP(cloud service provider)

2. NHN Cloud 정보보호 체계

비즈니스 연속성 관리

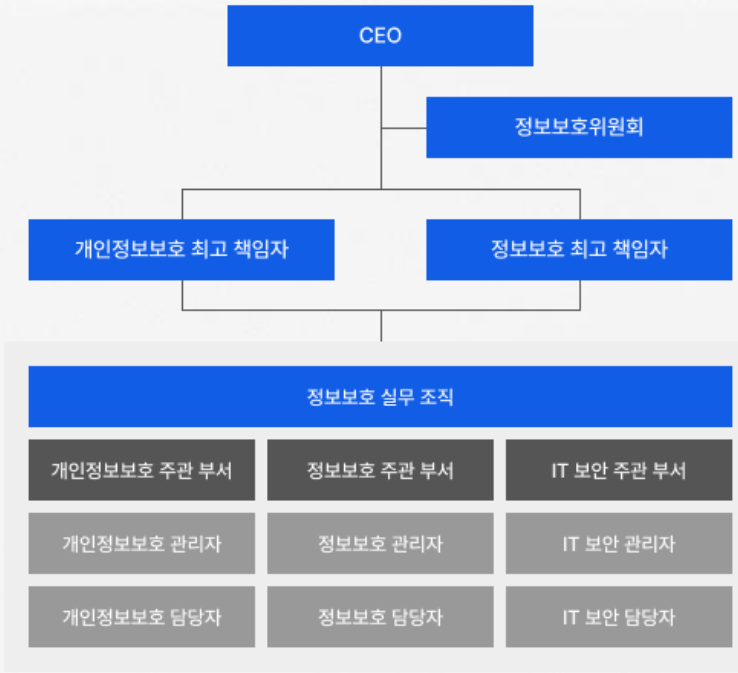
재해 · 재난을 대비하여 서비스 핵심 기능 복구 및 대응 체계 유지

정보보호 정책 · 조직

- CEO 및 CISO, CPO를 지정하고 하위 실무 부서로 구성
- 정책과 지침을 통해 세부 절차·방법을 주기적으로 검토 및 최신화

Business Continuity Plan(BCP)

- KR1, KR2 이중화 구성을 통해 비즈니스 연속성 제공
- BCP 대응 조직은 각 분야별 책임자과 구성으로 인력 배치



3. NHN Cloud 물리보안

데이터 센터 보안 관리

자체 기술력으로 설계 · 구축한 도심형 고집적 데이터 센터

Dynamic UPS

- 전력 공급원의 이중화 구성과 무중단 전원 공급 장치를 도입해 자가발전 설비로 전원 공급

출입 통제

- 출입 구역 및 보안 등급으로 최소 출입 권한 관리
- 사각지대 없는 CCTV 와 녹화

4. NHN Cloud 클라우드 플랫폼 보안

안전한 서비스 구성

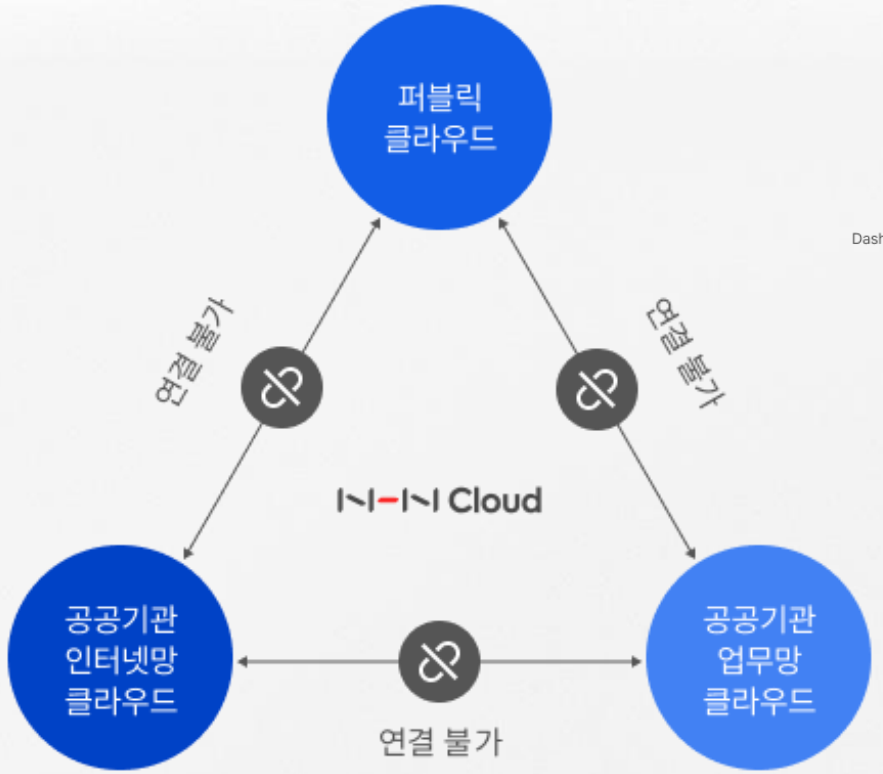
클라우드 영역 분리

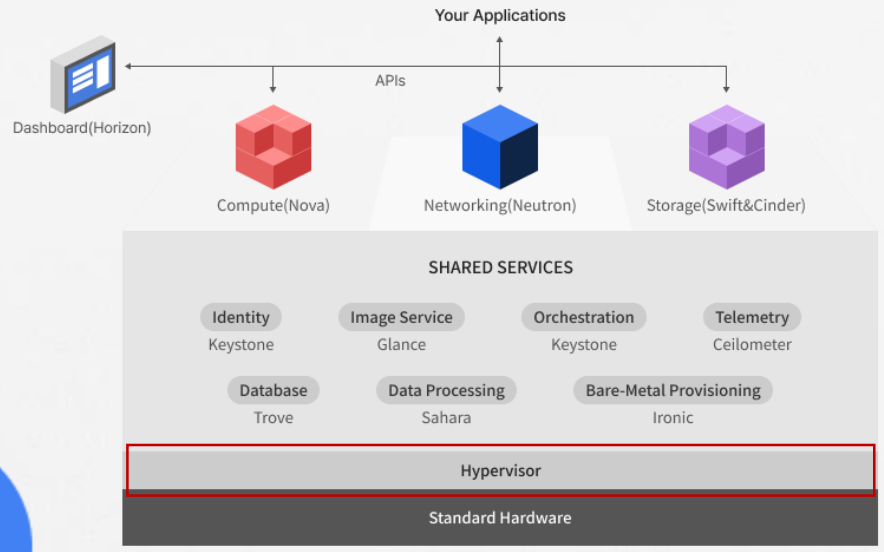
- 클라우드 구성 하드웨어의 물리적 분리되어 있으며, 상호 연결이 불가한 독립적 구성

하이퍼바이저 보안

- 접근 통제를 통한 시스템 관리와 버그 및 보안 패치로 시스템 보안성 강화

하드웨어 및 가상화 보안 기술 사용으로 리소스 격리





5. NHN Cloud 계정 보안

이용자 계정 보안

계정 · 인증 · 권한 부여 · 감사 관리 중요

조직 · 프로젝트

- 조직은 효율적 관리 그룹
- 프로젝트는 서비스 이용 그룹

NHN Cloud 회원 IAM 멤버

- 조직 및 프로젝트를 관리 하고 서비스를 이용할 수 있으며, 각 계정에 따라 콘솔 접근이 상이함

구분	NHN Cloud 회원	IAM 멤버
정의	• 조직 관리를 위한 멤버 • NHN Cloud 이용 약관에 동의한 NHN Cloud 회원으로 서비스 이용에 대한 책임과 의무를 가지는 멤버 • NHN Cloud 서비스 전체에서 유효한 멤버로 소속된 조직이 삭제되어도 NHN Cloud 회원으로 존재	• 서비스 이용을 위한 멤버 • NHN Cloud 이용 약관에 동의하지 않은 멤버 • 조직 내에서만 유효한 멤버로 소속된 조직이 삭제되면 더이상 사용할 수 없고 삭제되는 멤버
멤버 등록 방법	• 조직의 OWNER나 ADMIN이 NHN Cloud 회원 ID (E-mail)를 입력하여 등록	• 조직의 OWNER나 ADMIN이 조직 내 유일한 ID를 입력하여 등록
멤버 역할	• 조직 관리(조직 생성 · 수정 · 조직 멤버 관리 · 조직 서비스 관리 · 결제 관리) • 프로젝트 생성 · 삭제	• 조직 서비스 이용
콘솔 접근	• NHN Cloud 콘솔(https://console.nhncloud.com)접근 • 회원 ID/비밀번호로 로그인 • 회원 정보에서 설정한 로그인 보안 [2차 인증(이메일, SMS) 사용]	• IAM 콘솔(https://조직 도메인.console.nhncloud.com)접근 • 조직의 OWNEER 또는 ADMIN이 설정한 ID/비밀번호로 로그인 • 조직에서 설정한 로그인 보안 [2차 인증(이메일, Google OTP)] 인증

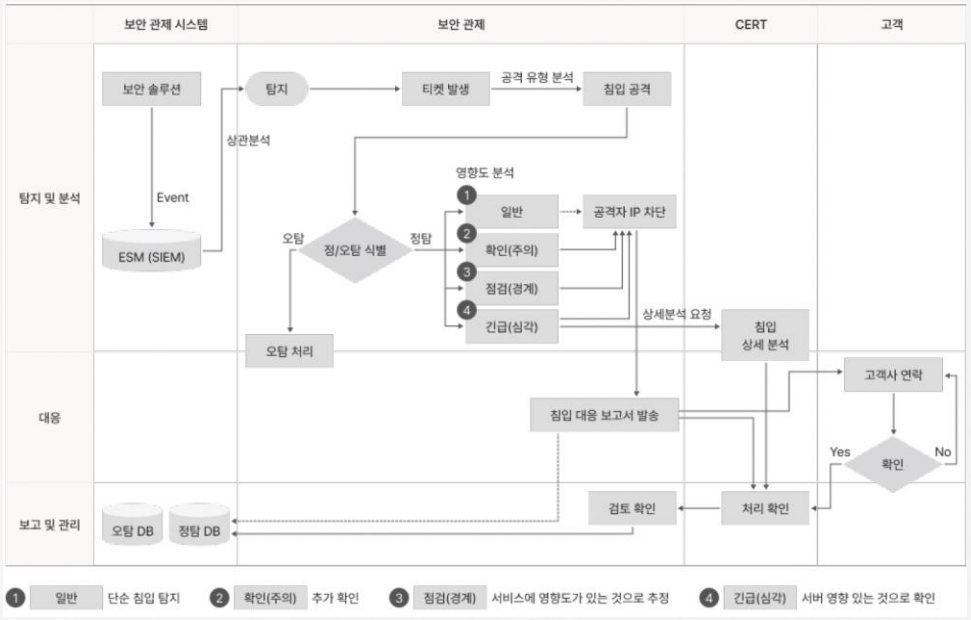
6. NHN Cloud 보안 관제 및 예방

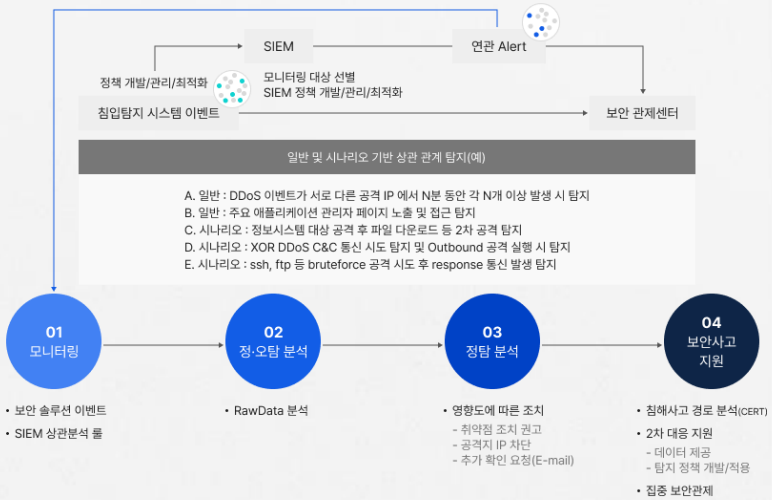
위협 탐지 · 대응

클라우드 플랫폼 및 이용자의 서비스 보호를 위한 위협 대응

보안 위협 탐지 · 분석 센터

- 이벤트 수집, 위협 탐지 및 분석, 대응 및 보고의 프로세스 수행
- 식별: 보안 장비 및 환경 분석
- 탐지 · 분석: 이벤트 수집, 실시간 모니터링, 이벤트 분석, 정책 설정, 상황 전파, 보안 정보 수집
- 대응: 위협 정보 상세 분석. 침해 사고 대응, 차단
- 보고 · 관리: 침입 대응 보고, 정기 보고 등





7. NHN Cloud 가상화 인프라 보안

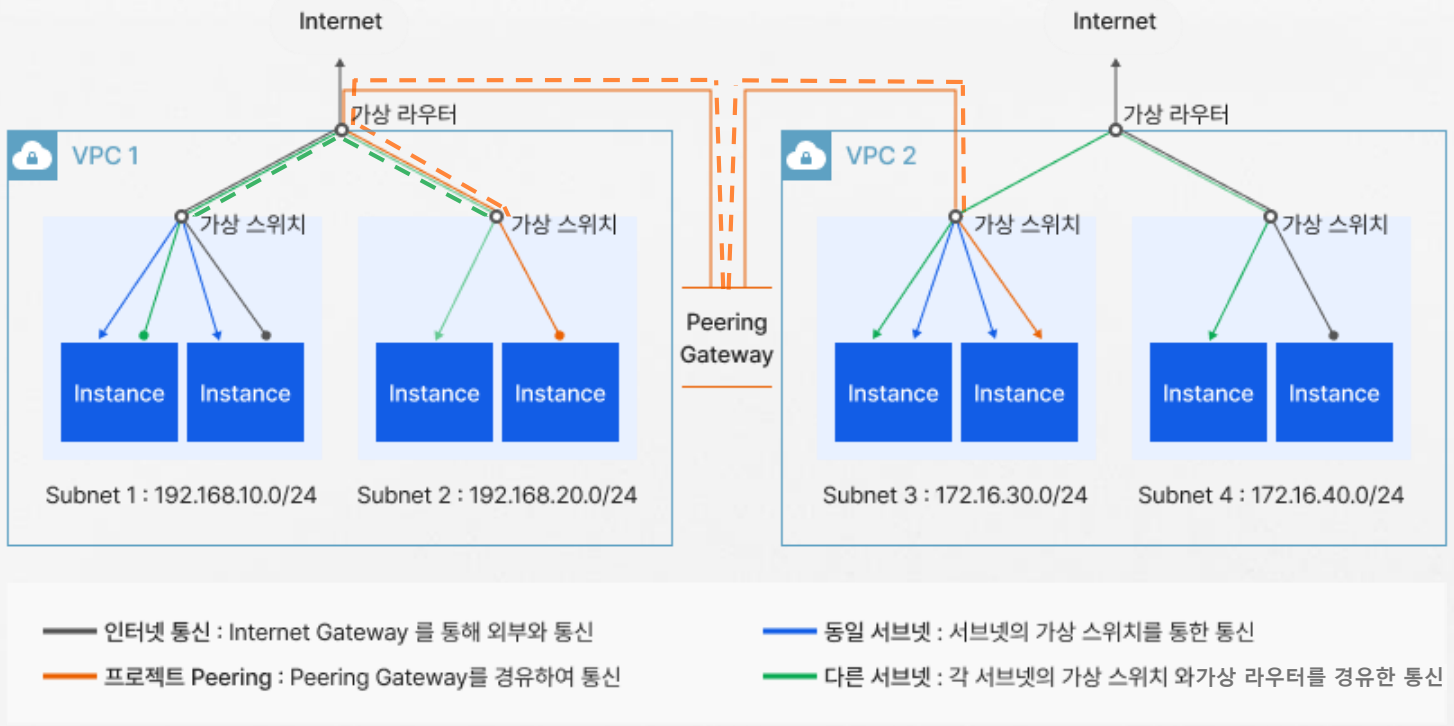
가상화 기술

가상화 자원을 보호하기 위한 접근 제어 · 데이터 보호 · 암호화

네트워크

- VPC(virtual private cloud)는 터널링 기술을 기반으로 이용자의 논리적으로 격리된 가상 네트워크를 구축하고 완전히 독립된 네트워크를 구성

- Security Groups 과 Network ACL 을 이용해 인스턴스 및 VPC 로 유입되는 트래픽을 제어(허용/차단)



8. NHN Cloud 보안 서비스

보안 서비스

컴플라이언스 및 서비스 보호를 위한 보안 서비스 제공

시스템 보안

- 수년간 축적된 위협 패턴 및 대응 체계를 바탕으로 보안 전문 인력이 24시간 365일 침입 시도에 대한 보안 관제 서비스 제공
- 자체 보유한 IDS/SIEM 과 관제 플랫폼을 통한 침입 탐지 · 분석 · 대응 · 보고 · 예방 활동을 지속적으로 수행

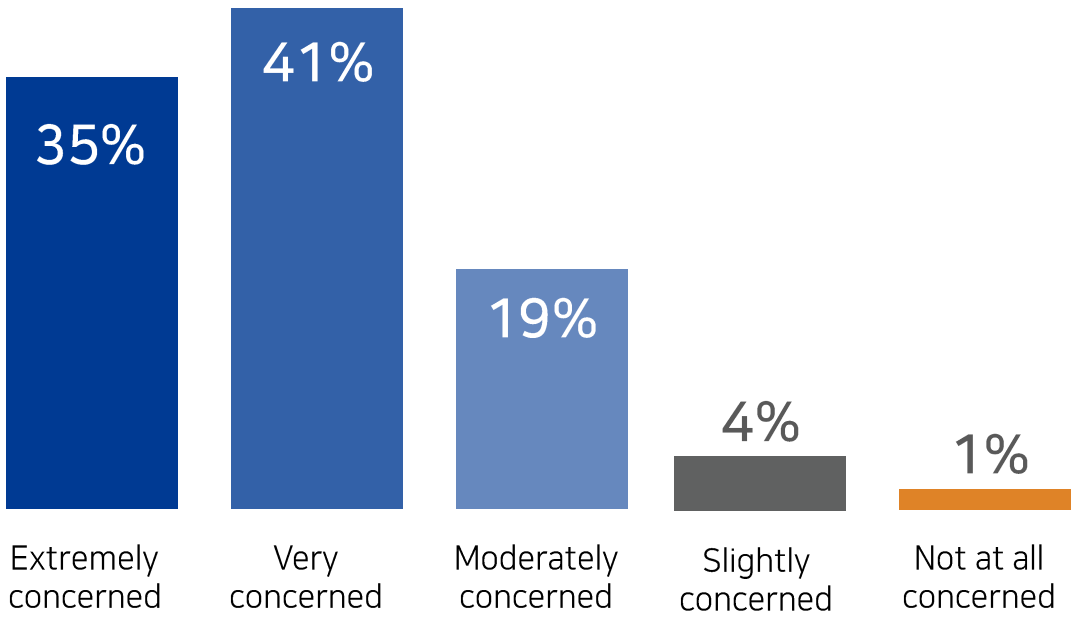
보안을 고려한 환경 구성 전략

백서의 활용

퍼블릭 클라우드의 보안에 대한 우려는 아직도…

95%

of organizations are moderately to extremely concerned about cloud security



클라우드 채택은 증가

클라우드 보안에 대한 우려 증가

2023 Cloud Security Report(Fortinet) ,Cybersecurity INSIDERS

퍼블릭 클라우드의 보안 위협은?

59%

Misconfiguration
of the cloud
platform/wrong setup

51%

Exfiltration of
sensitive data

51%

Insecure
interfaces/APIs

49%

Unauthorized
access

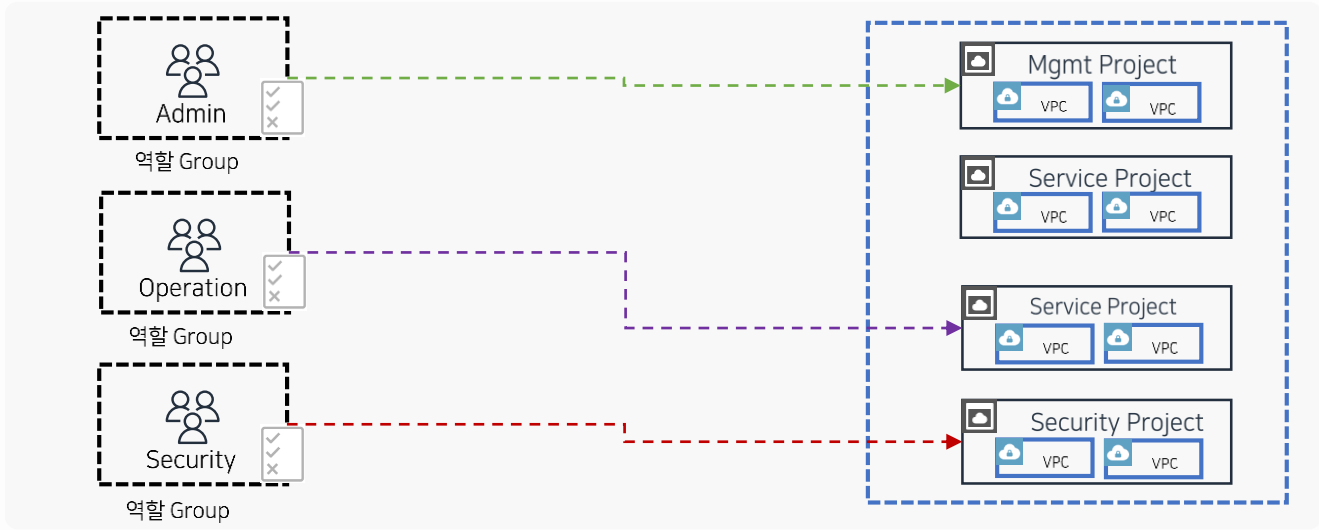
Hijacking of accounts, services, or traffic 45% | External sharing of data 39% | Malicious insiders 38% | Malware/ransomware 37% | Foreign state-sponsored cyberattacks 37% | Denial of service attacks 31% | Cloud cryptojacking 21% | Theft of service 20% | Lost mobile devices 13% | Don't know/other 7%

2023 Cloud Security Report(Fortinet) ,Cybersecurity INSIDERS

클라우드 보안의 시작은 권한 관리부터!!

클라우드포탈
관리 접속
(HTTPS/API)

프로젝트 관리
및
서비스 이용 역할



CloudTrail

클라우드 콘솔 보안 강화는 선택이 아닌 필수!!

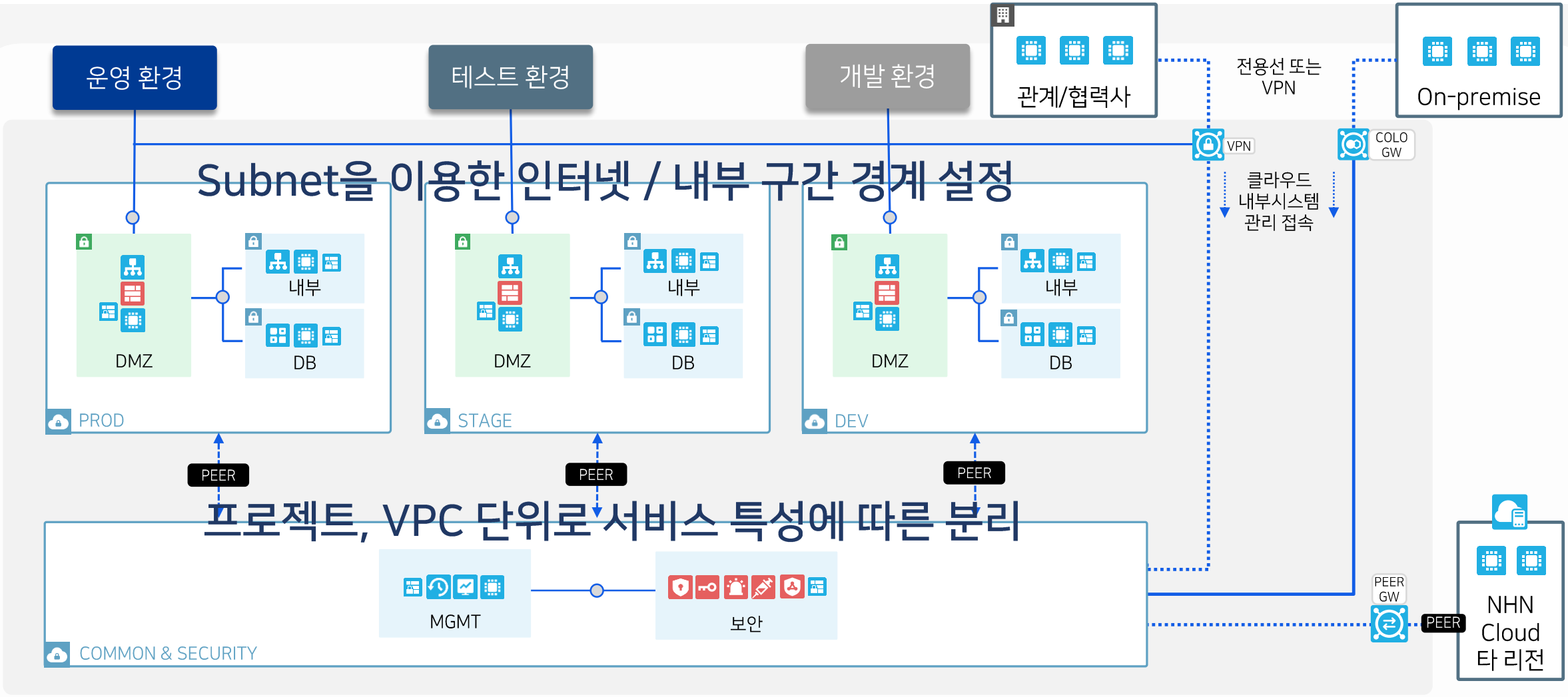
클라우드 콘솔 2차 인증(MFA)

로그인 보안 설정

IAM 회원의 콘솔 접속 보안(2차 인증, 로그인 실패 보안, 로그인 세션)을 설정할 수 있습니다.

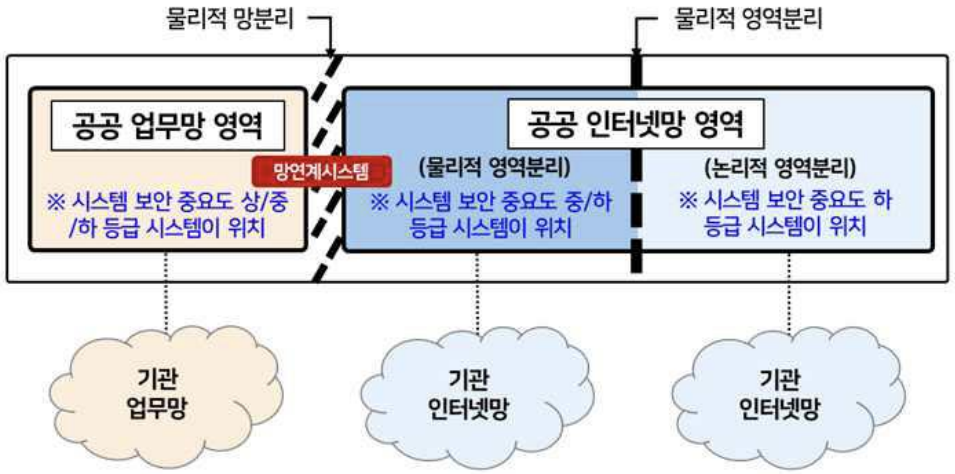
클라우드 콘솔 접근 제어

서비스 환경을 고려한 네트워크 분리



클라우드에서 망 분리는 어떻게 해야 하나?

공공 업무망 영역의 명확한 물리 망 분리



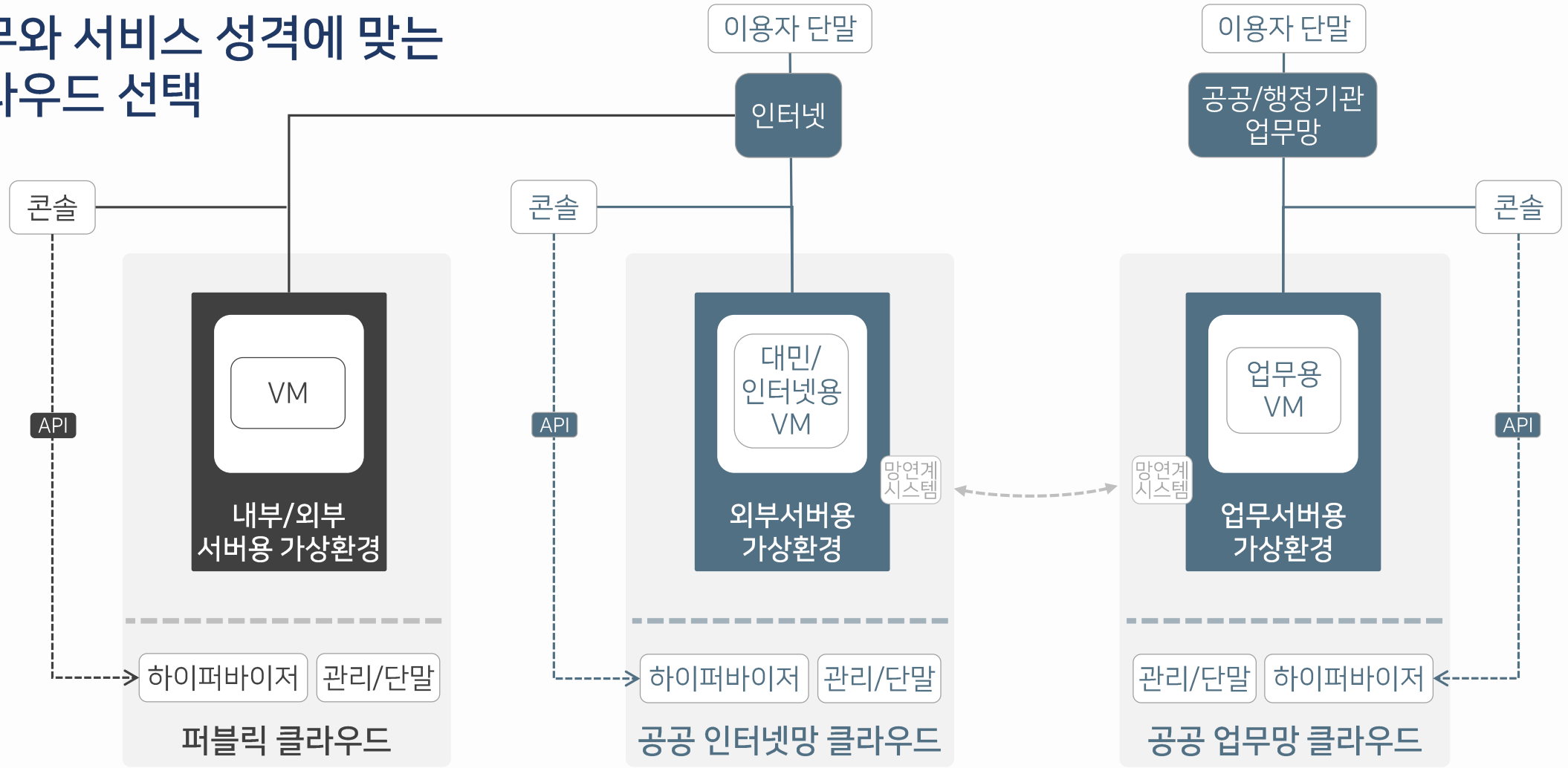
	공공 업무망 영역	공공 인터넷망 영역	
분리 방안	물리적 망분리	물리적 영역분리	논리적 영역분리
인터넷 연결	X	O	O
위치 가능한 시스템 보안 중요도 등급	上 / 中 / 下	中 / 下	下

분류	특징
공공 업무망 영역	- 공공 업무망 영역은 다음과 같은 클라우드 센터에 위치 : 각급 기관이 자체 구축·운영하는 클라우드 센터 : 통합 관리기관이 운영하는 데이터 센터 : 공공 업무망 전용 민간사업자 클라우드 센터 **- 각급 기관의 업무망과 연결하여 클라우드 서비스 제공하며 인터넷과의 접점 없음** **- 민간 서비스 영역과 물리적 영역 분리가 되어 있으며 공공 인터넷망 영역과 물리적 망 분리된 영역** - 단, 공공 인터넷망 영역과 자료 전송 체계 구축 운영 가능 - 영역 내부에서 기관 및 서비스별 분리 - 시스템 중요도 상/중/하 등급 위치 가능 - 국내 관리·운영

국가 클라우드 컴퓨팅 보안 가이드라인(2023.01), 제3장 제2절 클라우드 영역 분류

클라우드에서 망 분리는 어떻게 해야 하나?

업무와 서비스 성격에 맞는 클라우드 선택



VPC 및 인스턴스의 트래픽을 제어하기 위해서…

적절한 통신 제어가 필수

구분	Security Groups	Network ACL
제어 대상	• 인스턴스	• 네트워크
설정 대상	• Protocol, IP, Port	• Protocol, IP, Port
제어 트래픽	• 유입/유출 트래픽 선택 가능	• Src, Dst 주소 선택 가능
접근 제어 타입	• 허용 정책만 설정	• 허용 또는 차단 정책 선택 가능

스토리지에 저장된 데이터를 보호하기 위해서는…

암호화 블록 스토리지 선택

블록 스토리지 생성

블록 스토리지 이름
255자 이내로 작성해주세요.

설명

블록 스토리지 타입 HDD SSD Encrypted HDD Encrypted SSD

암호화 대칭 키 ID 대칭 키 ID를 입력해 주세요.
40자 이내로 작성해 주세요. 영문과 숫자만 입력 가능합니다.

블록 스토리지 크기(GB) 10 GB
10 2000

가용성 영역 kr2-pub-a

- 블록 스토리지 생성 후에는 암호화 사용 여부 및 대칭 키 ID는 변경할 수 없습니다.
- 사용자의 부주의에 의해 Secure Key Manager 서비스에서 대칭 키를 삭제하는 경우 해당 대칭 키로 암호화한 객체에 대해 복호화 할 수 없습니다. 이 경우 NHN Cloud는 책임지지 않습니다. 실수 등에 의해 삭제되지 않도록 주의하여 대칭 키를 관리하시기 바랍니다.
- 대칭 키 변경 시 변경 전에 업로드 한 객체는 변경 전의 대칭 키로 암/복호화 됩니다. 변경 후에 업로드한 객체는 변경 후의 대칭 키로 암/복호화 됩니다.

☐ 사용자 부주의에 의한 Secure Key Manager 대칭 키 삭제 시의 주의사항에 대해 확인했습니다.

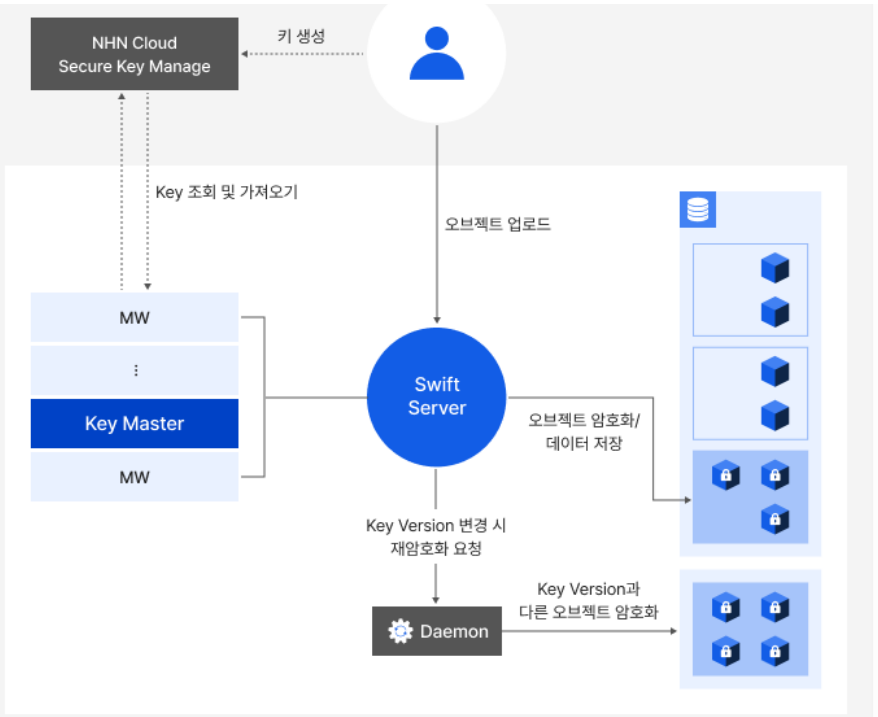
취소 확인

Object Storage 객체 암호화

암호화 설정

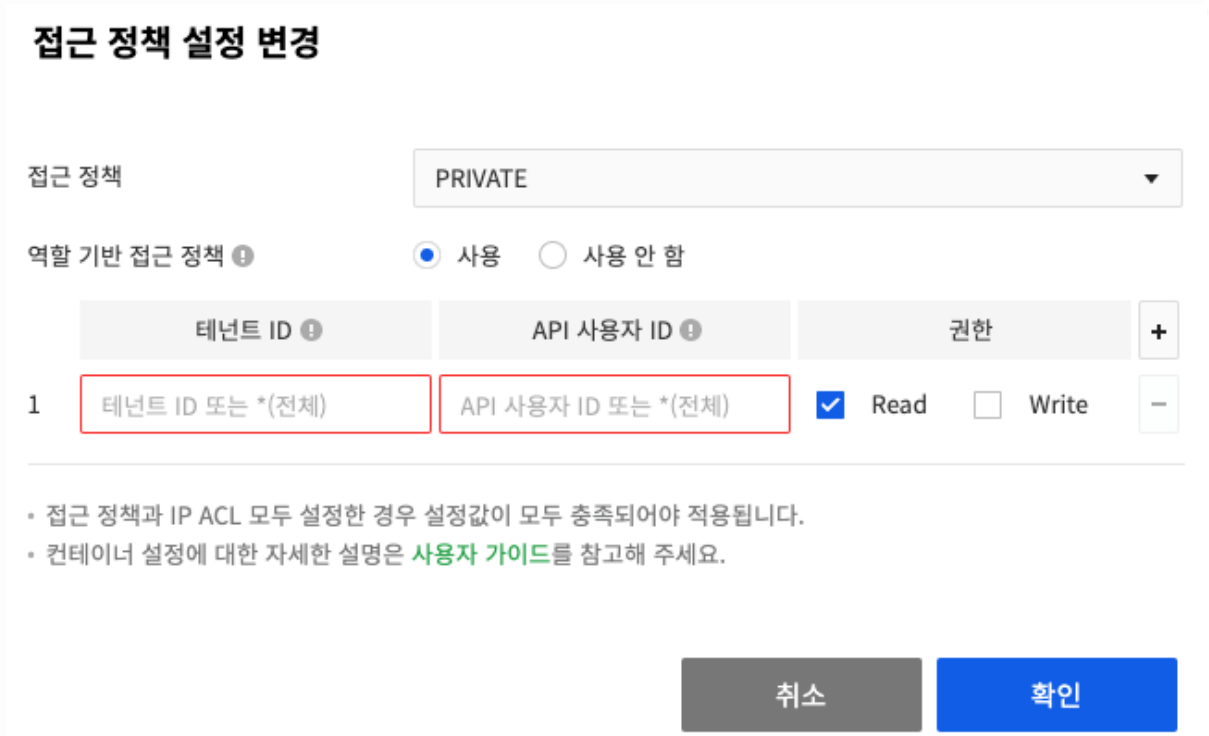
암호화 사용 사용 안 함

대칭 키 ID
40자 이내로 작성해 주세요. 영문과 숫자만 입력 가능합니다.



스토리지에 저장된 데이터를 보호하기 위해서는…

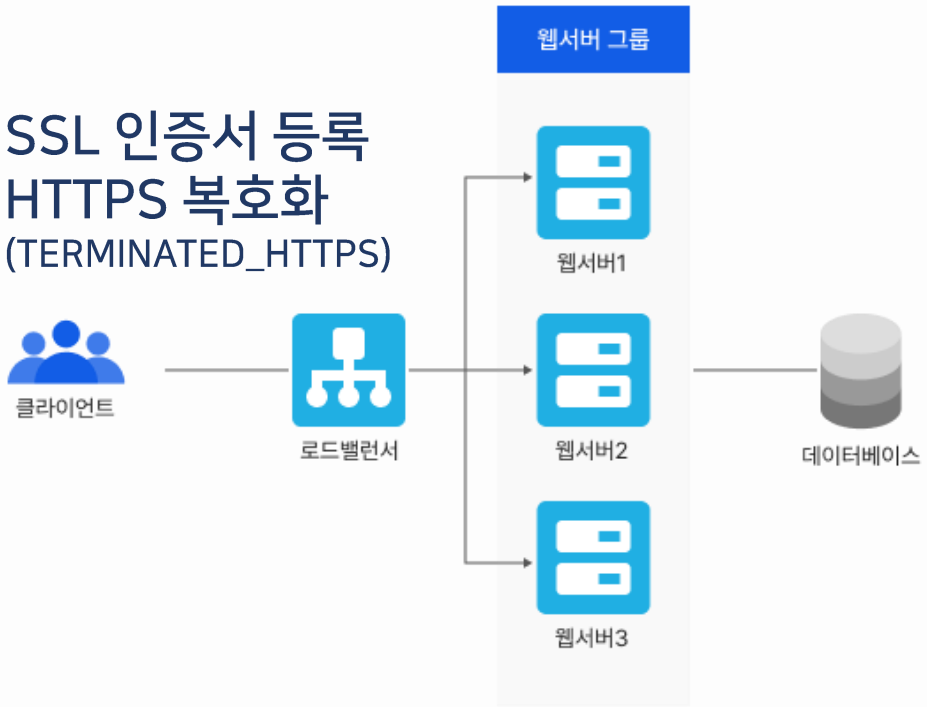
Object Storage 객체 접근 제어

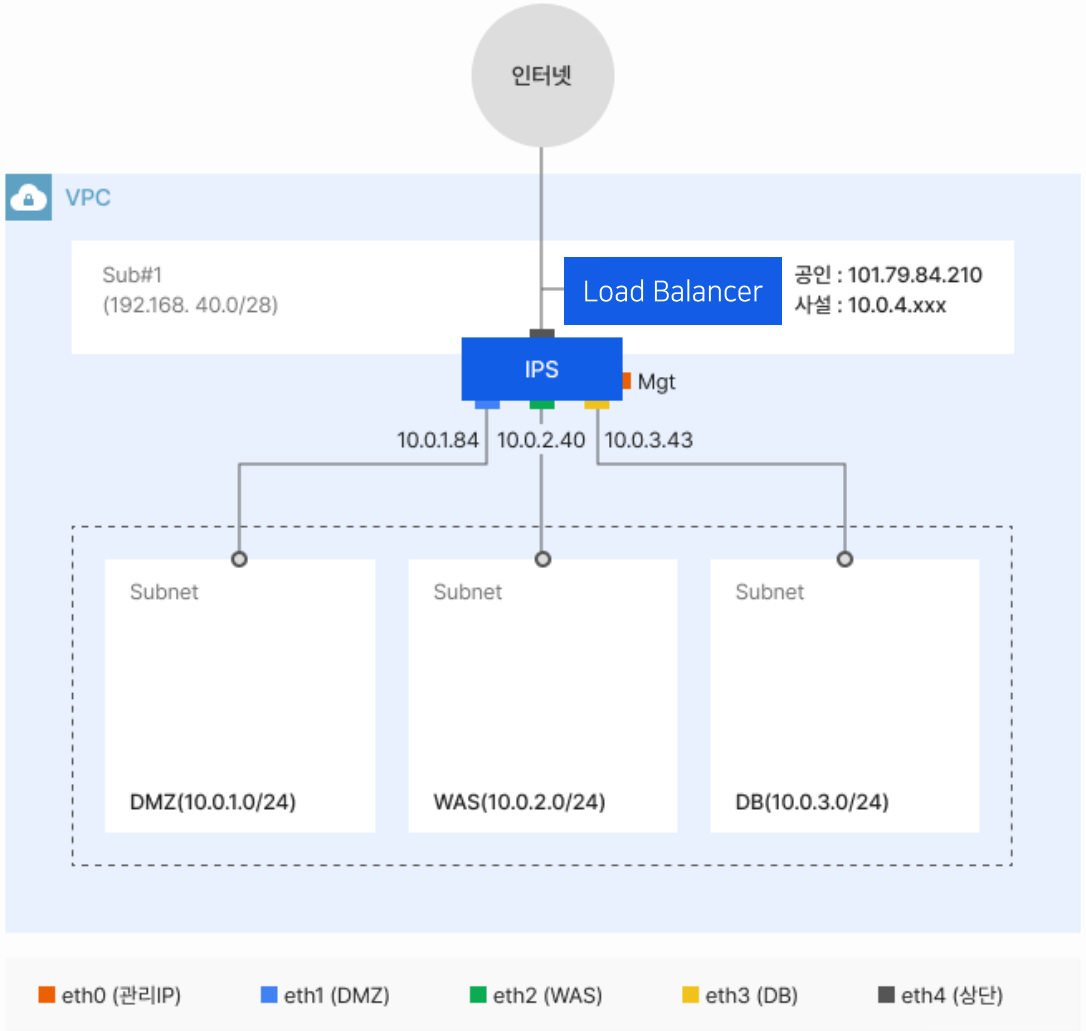


암호화 트래픽의 위협은 어떻게 탐지할 수 있을까?

SSL 가시성 확보를 위한 로드밸런서 활용

SSL 인증서 등록
HTTPS 복호화
(TERMINATED_HTTPS)





클라우드의 다양한 보안 서비스를 적극 활용

취약점 점검

서버 및 앱
잠재적 취약점 제거

Server Security Check

App Security Check

네트워크 보안

DDoS 및 웹 공격에 대한 방어
다년간 축적된 보안 관제로
침해 위협 탐지/대응

DDoS Guard

WEB Firewall

Security Monitoring

Basic Security

시스템 보안

바이러스 및 악의적인
웹 셸로부터 서버와 서비스
를 안전하게 보호

Vaccine

Webshell Threat Detector

NHN AppGuard

보안 관리

이벤트 수집 분석
컴플라이언스 대응

SIEM

Security Compliance

암호 및 인증

서버 및 앱
잠재적 취약점 제거

Secure Key Manager

NHN Cloud

클라우드로의 전환은 선택이 아닌 필수

지속적인 보안 강화를 위한 인식과 개선이 안전한 클라우드 서비스를 보장 합니다.

많은 기업과 기관들이 빠르게 변화하는 IT 환경에서
NHN Cloud를 안전하고 친숙하게 이용하는 계기가 되었으면 합니다.

NHN Cloud

유연하게, 안전하게
비즈니스에 힘이 되다.