SAMSUNG SDS

REAL 2019

REALIZE YOUR VISION
THROUGH DIGITAL TRANSFORMATION

2019 . 5 . 8 . WED . The Shilla Seoul

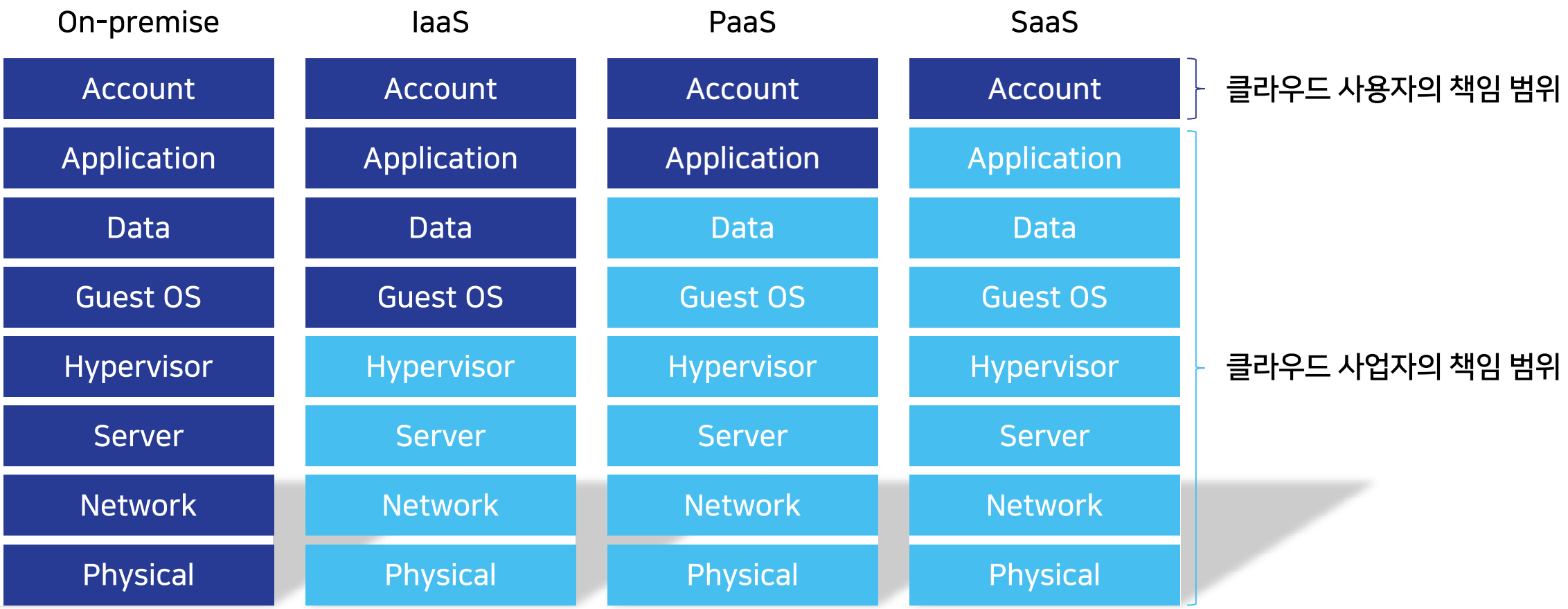
Native API

Security for Shared Infra

조병선 그룹장

Shared Responsibility Model

클라우드 사업자/사용자가 보안 책임을 분담, 사업자가 제공한 보안기능을 사용자가 설정하는 구조

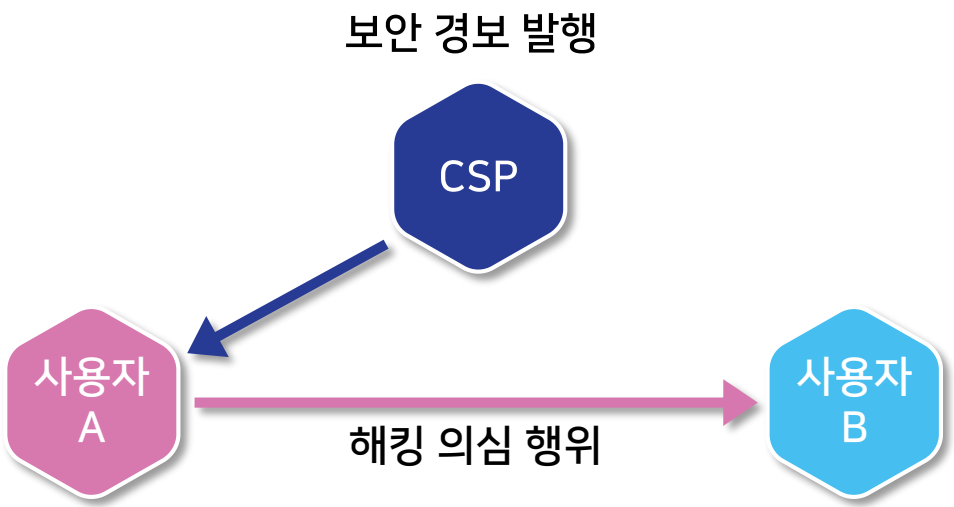


Customer Agreement

클라우드 이용약관 상 보안설정 미흡에 의한 책임은 사용자에게 귀책

구분	세부 내용
고객의 의무	고객은 서비스 오퍼링을 적절히 구성(Configuration) 및 사용하고 적절한 보안 및 보호를 제공하는 방식으로 고객의 계정 및 고객 콘텐츠를 안전하게할 책임을 가진다.
일시 정지	다음과 같은 경우 AWS는 통지를 하고 고객 권리를 즉시 정지할 수 있다: (a) 고객 또는 최종 사용자에 의한 서비스 오퍼링의 이용이 (i) 서비스 오퍼링 또는 여하한 제 3 자에게 보안상의 위험을 가하거나 .. (후략)

CSP 보안 경보



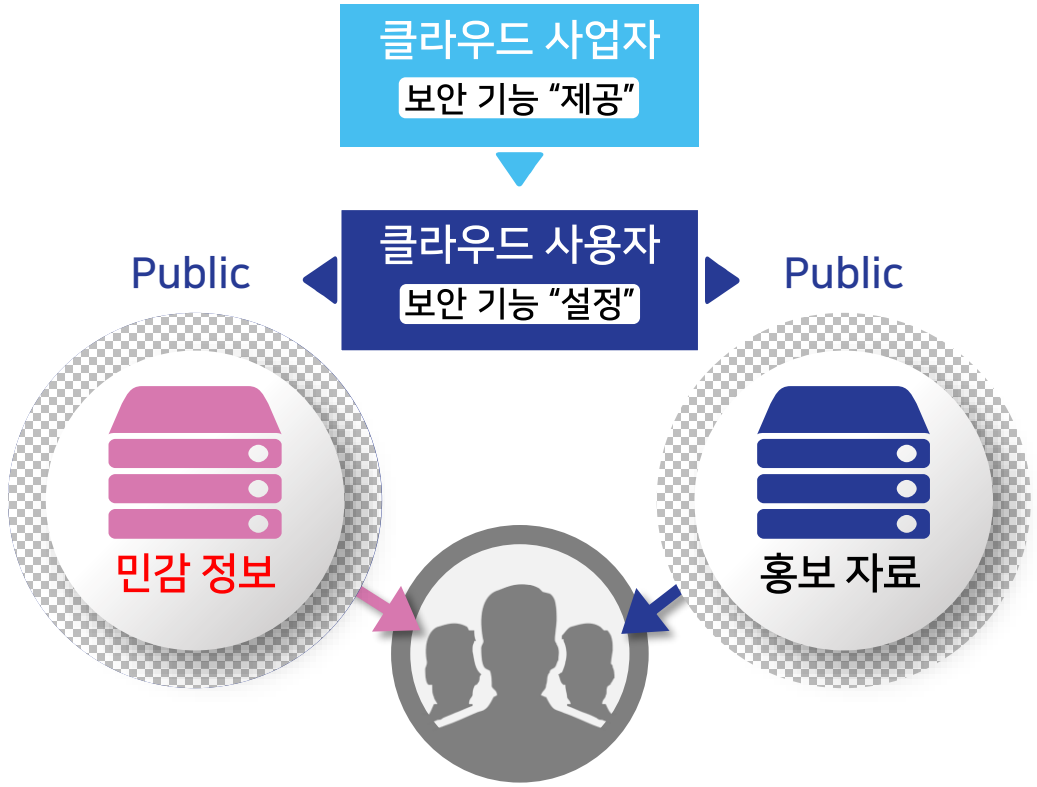
Hello. ID #123456789
타 사용자에게 해킹으로 의심되는 행위를 탐지하였습니다.
본 메일을 수신하시는 즉시 자세한 사유 회신 바랍니다.
Please take action to stop the reported activity and reply directly to this email with details of the corrective actions you have taken ···

Cloud Security Incidents

클라우드 보안 설정 미흡에 의한 보안사고 다수 발생, 운영자의 Human Error가 공통 원인

시점	피해 기관/기업	피해 성격 및 규모
`19. 1월	Blur	인증 정보 240만명
`18. 6월	Honda	무인 차량 이용자 정보 5만명
`18. 6월	Universal Group	FTP/SQL 및 AWS 접속 정보
`18. 2월	FedEx	개인 정보 12만명
`17.12월	Alteryx	부동산 정보 1.26억 가구
`17.11월	美국방부	개인 정보 3,100만명
`17.10월	Accenture	개인 정보 137GB
`17. 7월	Verizon	통신 정보 600만명
`17. 6월	美공화당	유권자 정보 2억명
`17. 5월	DowJones	금융 정보 2,200만명

보안사고 원인

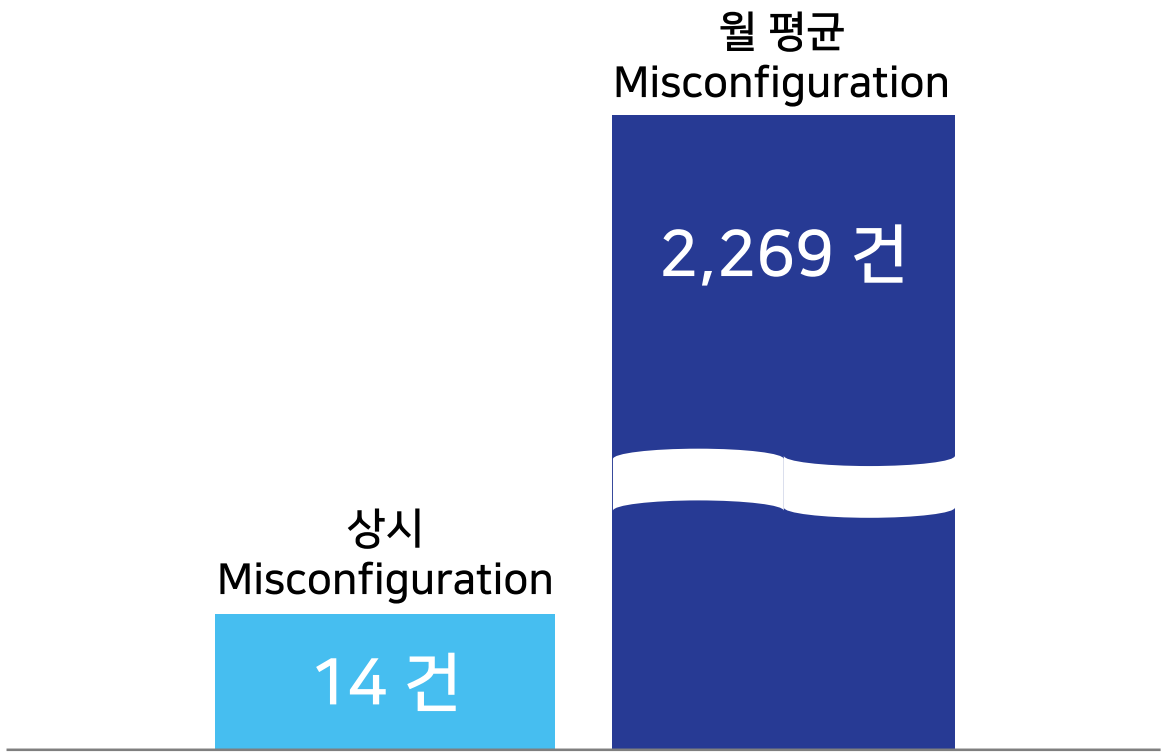


Misconfiguration

클라우드 사업자가 제공한 보안기능을 미적용, 비활성화 및 안전하지 못한 상태로 방치

	TOP 10 Misconfiguration
1	디스크 암호화 기능 (EBS Data Encryption) 비활성화
2	Outbound 통신 허용
3	운영자 권한 설정 시 Role 미적용
4	Security Group의 Port 설정 오류
5	Security Group의 Inbound 접속 설정 오류
6	암호화하지 않은 VM 원본 이미지 (AMI) 방치
7	사용하지 않는 Security Groups 방치
8	네트워크 로깅 기능 비활성화 (VPC Flow Logs)
9	운영자 계정에 (IAM User) MFA 미적용
10	스토리지 암호화 기능 비활성화 (S3 Bucket Encryption)

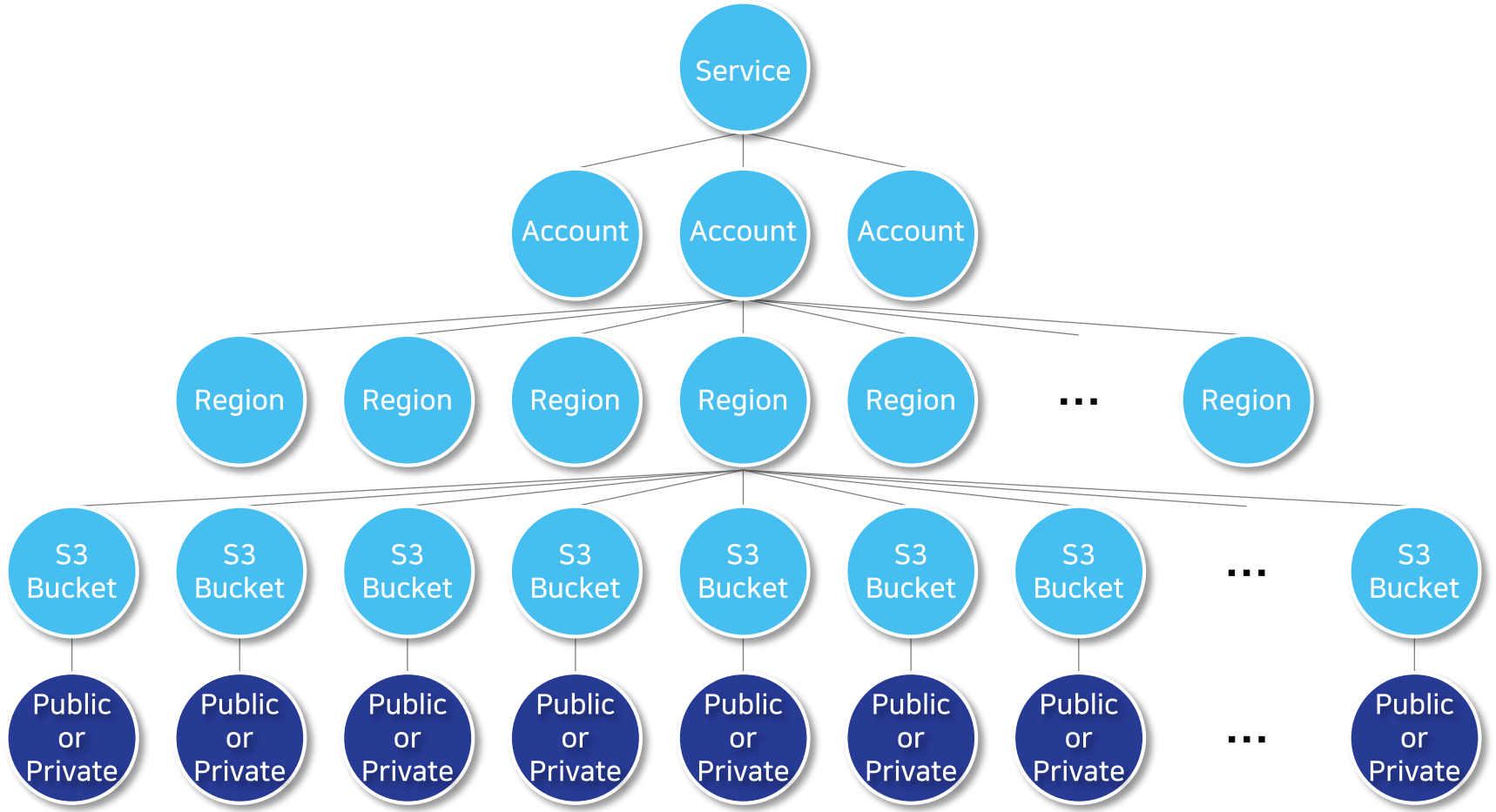
Misconfiguration 발생 빈도



※ Source: Cloud Adoption Risk Report 2019, McAfee

Root Cause

자동화된 점검 부재, 상시 변동되는 클라우드 보안 설정을 수작업으로 점검 불가



서비스 당 평균
× 3개 Account

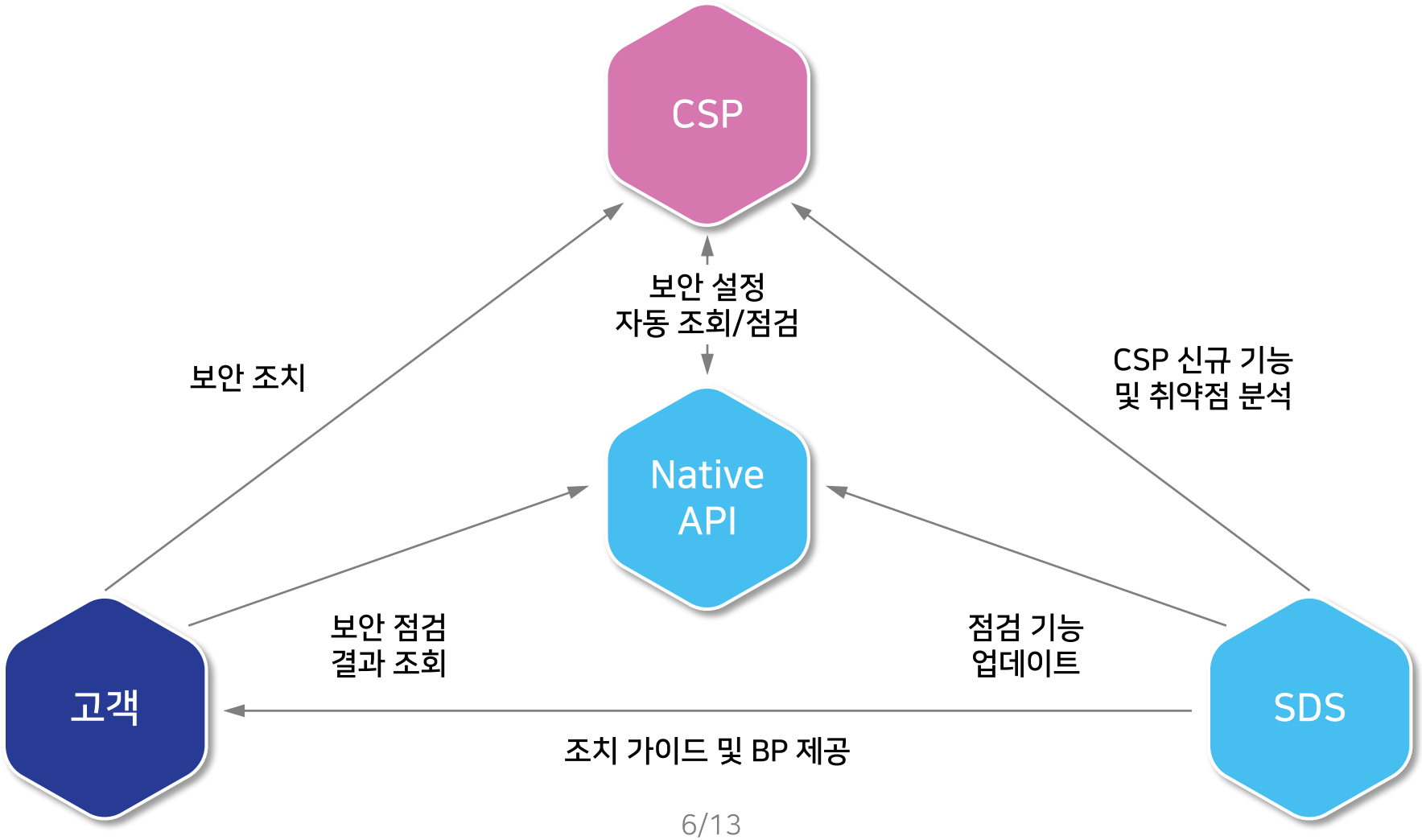
Account 당 평균
× 19개 권역

권역 당
× Bucket 수량 ∞

보안 점검 대상

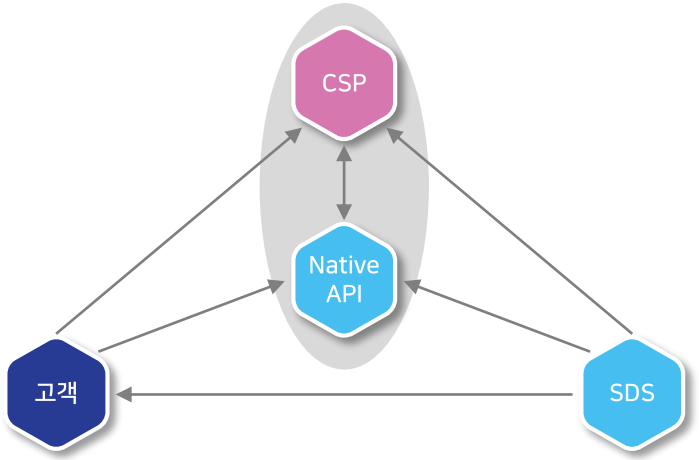
SDS's Solution - Native API

클라우드 자동 점검 및 조치를 위한 삼성SDS의 Echo System



SDS's Solution - Native API

보안 설정 자동 조회/점검



- CSP의 API를 통한 상시 현황 조회
- 삼성의 보안 노하우 및 CSP의 BP를 기준으로 취약한 보안 설정을 점검

보안점검 대상

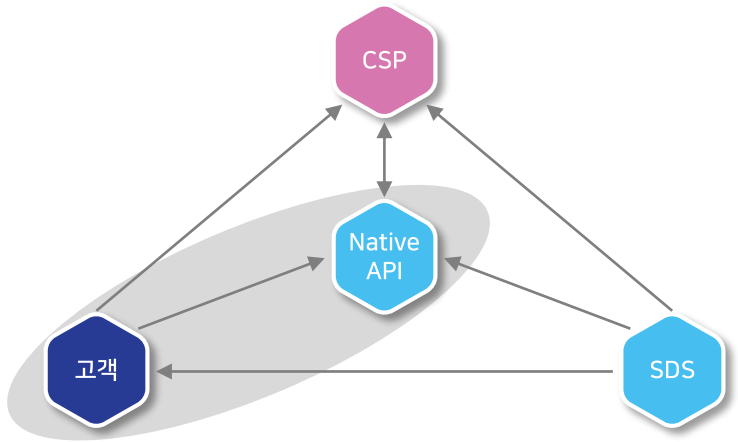
- Amazon AWS
- Microsoft Azure (TBD)
- Google Cloud Platform (TBD)

보안점검 기준

삼성 보안 규정 (전 삼성 관계사 공통) + CSP 보안 BP (Whitepaper, Tech Blog) + 주요 보안 기관 (CIS Benchmark, CSA 등)

SDS's Solution - Native API

보안 결과 조회

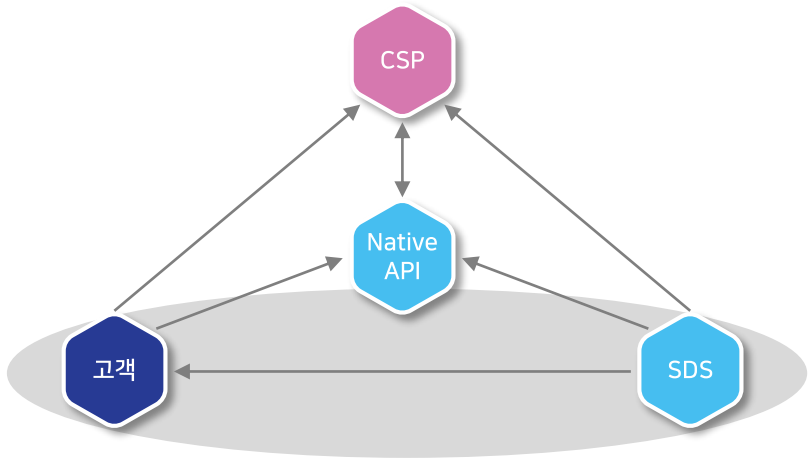


- WEB UI를 통한 Misconfig. 상시 조회
- 개발/운영/보안 담당자 및 조직별 조회 권한 차등 적용

보안점검 결과

SDS's Solution - Native API

조치 가이드 및 BP 제공



- 클라우드 특성에 부합하는 조치 가이드
- 상시 CSP 신규 기능을 분석하여 점검 기능 업데이트 실시

CSP 기능 업데이트 (4월)

일	월	화	수	목	금	토
	1 NEW	2 NEW	3 NEW	4 NEW	5 NEW	6
7	8 NEW	9 NEW	10 NEW	11	12 NEW	13
14	15	16 NEW	17 NEW	18 NEW	19 NEW	20 NEW
21	22	23	24 NEW	25 NEW	26 NEW	27
28	29 NEW	30 NEW				

삼성SDS 조치 가이드

보안 경험
국내 최초 AWS Competency

+

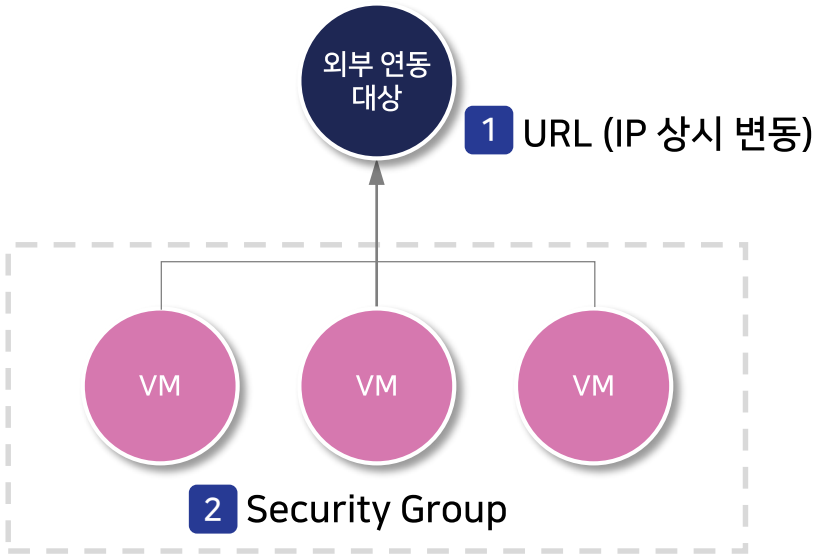
운영 경험
국내 최대 규모 MSP 사업자

+

개발 경험
DevOps 및 CI/CD 활용 등

Use Case #1

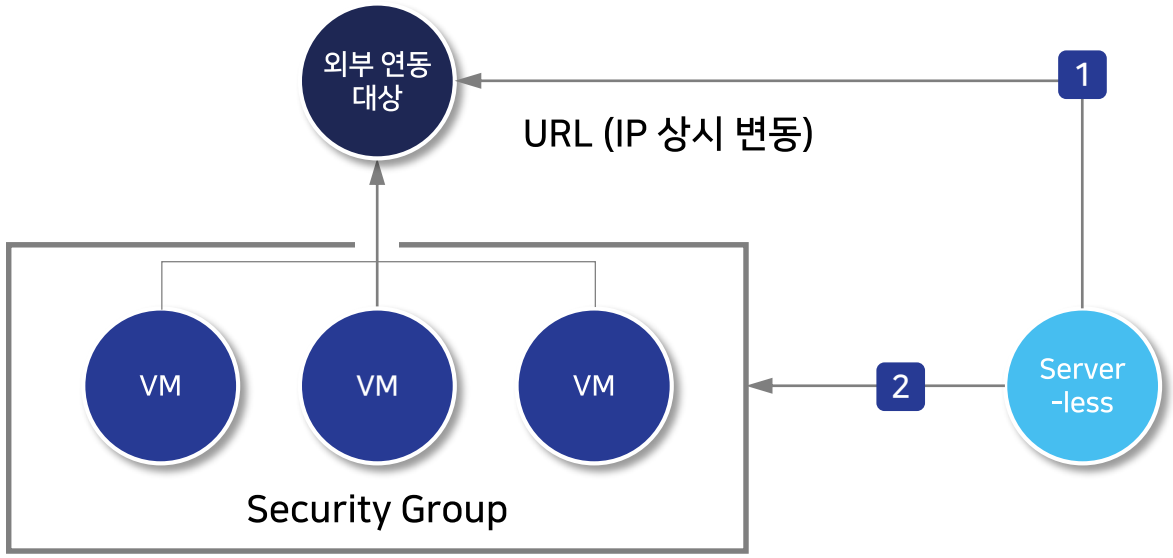
Outbound 통신 허용



1 Security Group은 IP/Port만 접속 허용/차단 정책에 입력 가능

2 URL 연동이 요구되는 경우 IP 변동을 감안하여 Outbound Any Open 설정

Server-less를 활용한 Security Group 설정

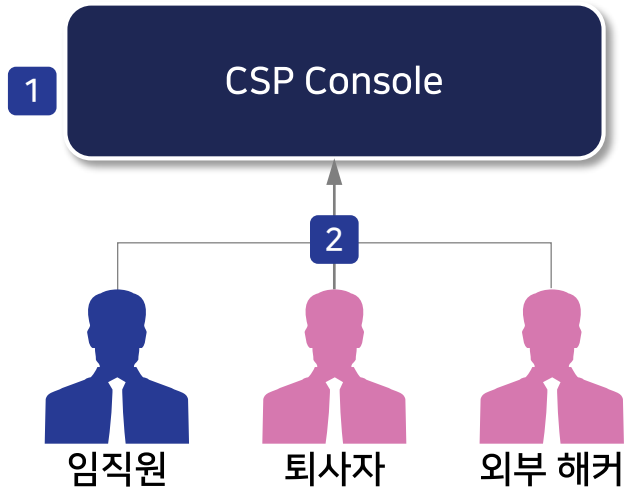


1 Server-less 기술을 통해 매시간 URL/IP 조회
- 조회 건 당 과금, 평균 백만건 단위 $1 이하

2 IP 변동 시 Security Group에 변경된 IP 자동 입력

Use Case #2

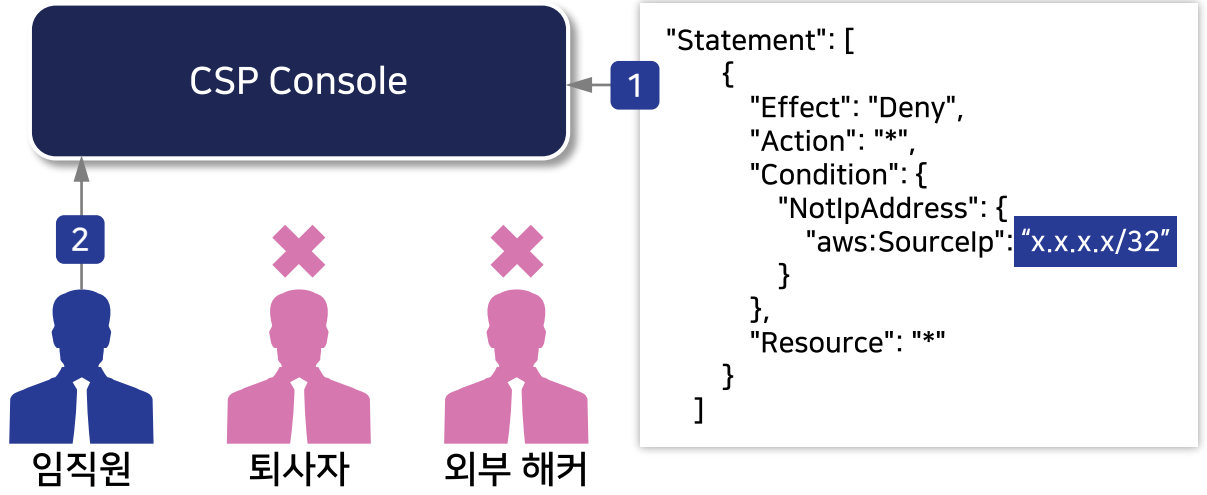
Console 접근 제어



1 클라우드는 WEB UI로 구성된 Console을 통해 모든 VM 생성/삭제 등의 작업 수행

2 Default Policy는 모든 사용자에게 Console 접속을 허용

Policy 적용을 통한 사내 IP 외 접속 차단

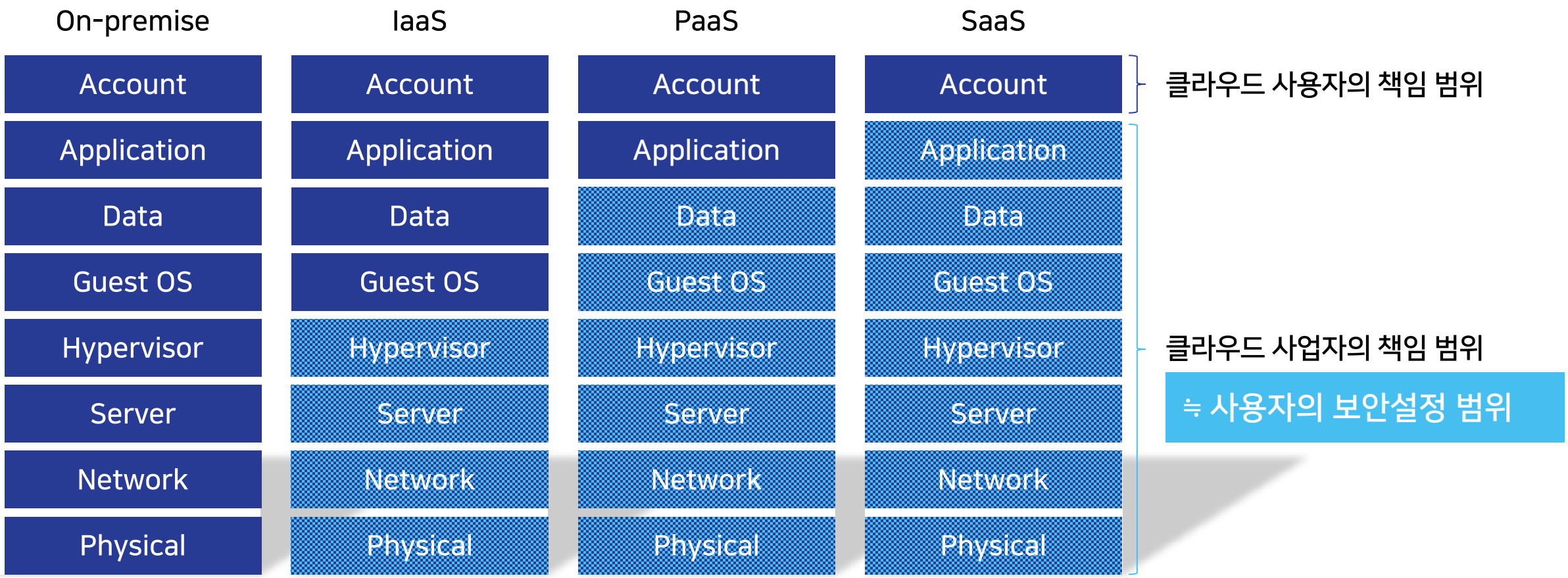


1 특정 IP만 접속 가능하도록 Policy 작성
- 임직원 ID를 Role, Policy로 상세 관리

2 임직원 이외 퇴사자, 외부 해커 등의 타 IP 사용자의 접속을 차단

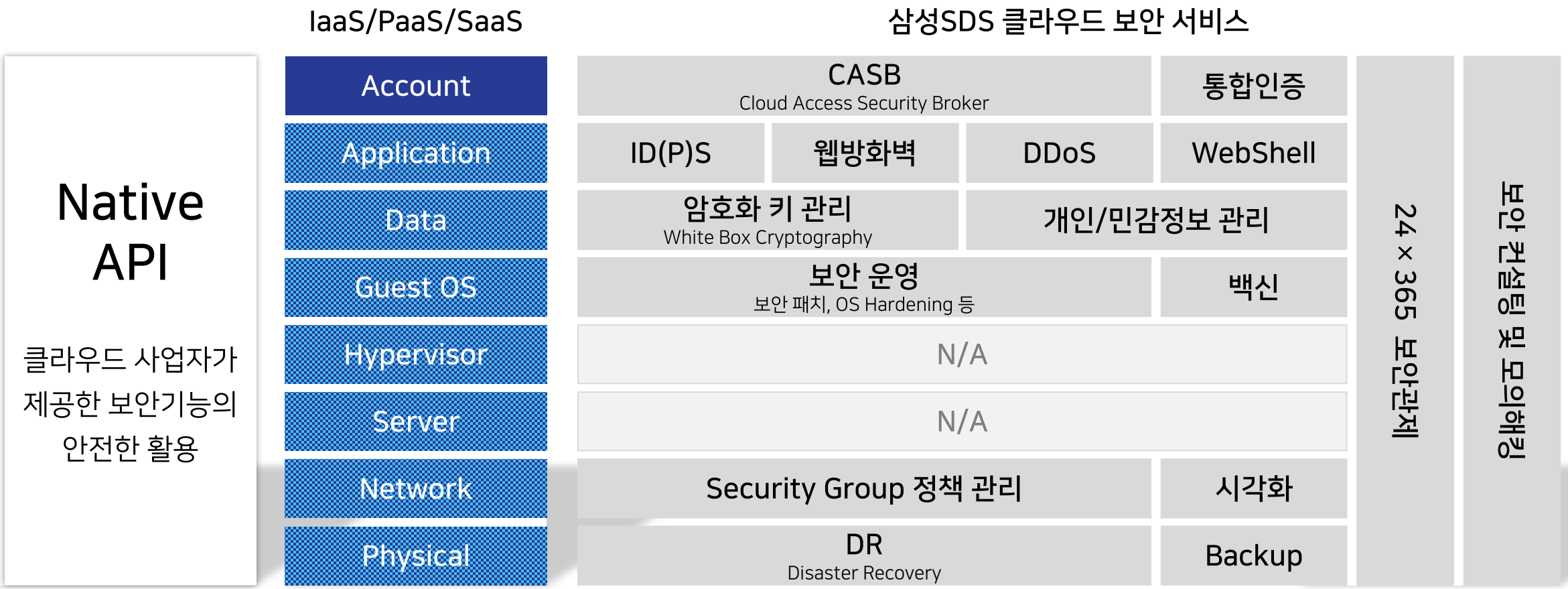
Conclusion

클라우드 보안은 사용자의 지속적인 관리에 의해서만 유지 가능



Recommendation

고객이 핵심 역량에 집중할 수 있도록 삼성SDS의 다양한 클라우드 보안 서비스를 제안



Thank you

Q&A