Cyber Security Conference 2021

SAMSUNG SDS

클라우드 보안 FAQ

10년 동안 클라우드 보안에 대해 가장 많이 받은 질문들

천준호 프로 삼성SDS 보안플랫폼팀

10년 동안 클라우드 보안에 대해 가장 많이 받은 질문들

1위 클라우드 보안은 CSP가 해주는 것 아니었나요.

2위 삼성SDS 클라우드 보안 기준은 왜 그렇게 어려운가요.

3위 보안 5종 세트는 대체 무엇인가요.

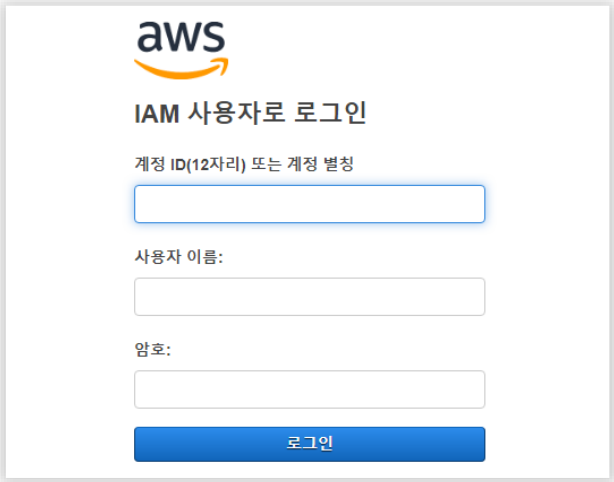
4위 Cloud가 On-premise 만큼 안전해지려면 어떻게 해야 하나요.

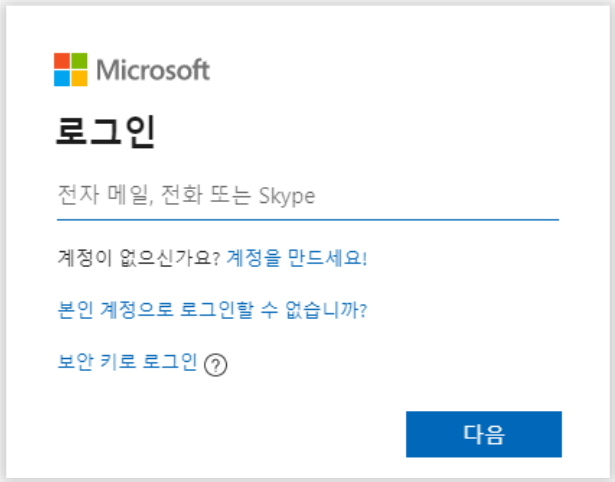
5위 클라우드 보안은 어떻게 공부해야 하나요.

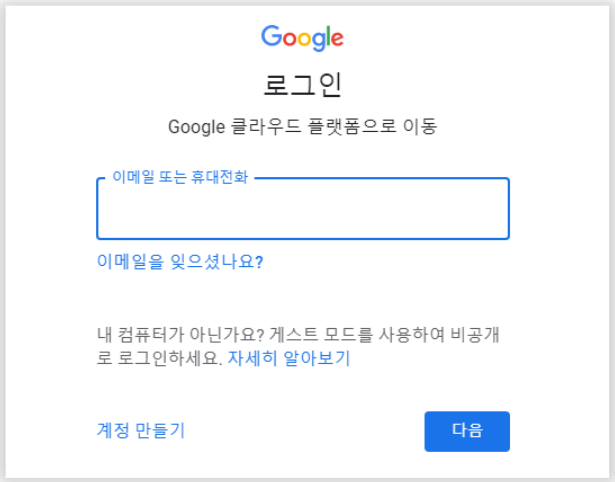
5위 클라우드 보안은 어떻게 공부해야 하나요.

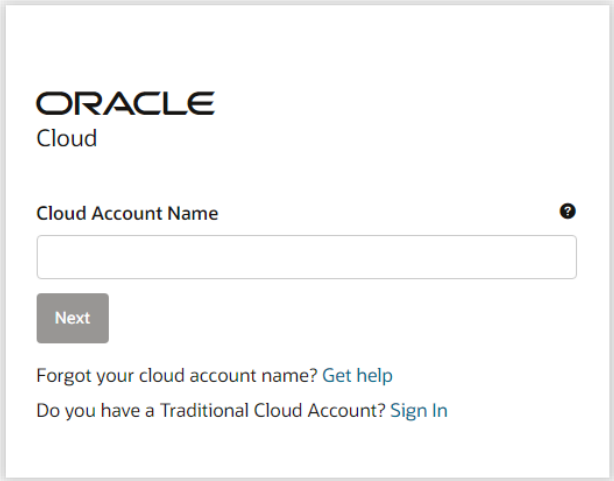
Q 마땅한 책도, 교육 과정도 없어서 입문하는 과정이 너무 어렵습니다.

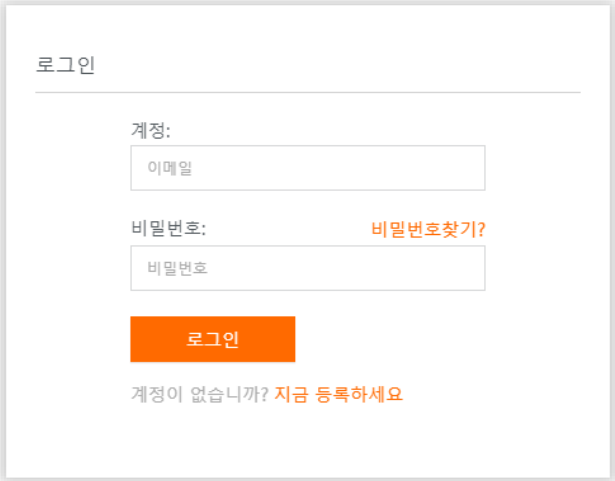
클라우드를 직접 사용해보기

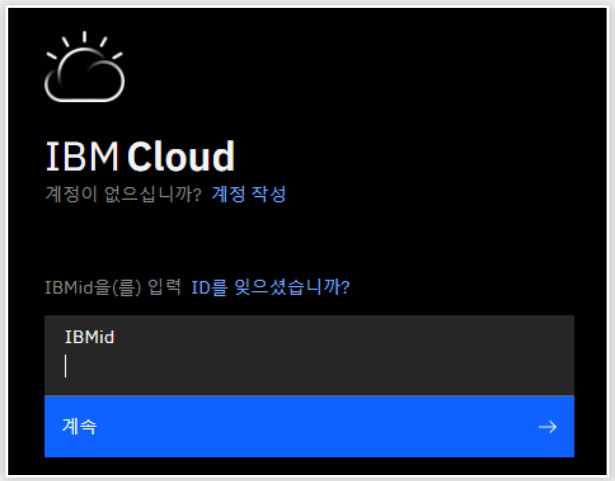












시작은 클라우드 보안 점검부터

2. 상세 진단 항목

2.1. Identity and Access Management

2.1.1. AWS Console 'root user' 사용 제한

각 IAM User에게 최소 권한을 부여하여 AWS Console에 접속하는 것을 원칙으로 하되 'root User' 권한이 필요한 경우, 사전 승인을 통해 인가된 범위 안에서 사용해야 합니다.

(1) 위험 수준 : Critical

(2) 적용 난이도 : Mid

(3) 점검 방식 : 정성 점검

(4) 진단 주기 : 실시간 권장, 최소 월별 점검

(5) 진단 항목 설명

a. "root user"가 비활성화, 즉 AWS Account 생성 이후 PW, MFA, Access Key 등이 설정되지 않은 상태로 한번도 사용된 적이 없는 경우에 한하여 '양호'로 간주함

b. AWS 기능 중 "root user"를 반드시 이용해야 하는 경우는 예외로 인정하나 "root user"를 활성화한 이후 관리 방안이 부재한 경우 '취약'으로 간주함

['root user' 필수 사용의 예시]

- 'root User' Password 변경
- AWS 지원 계획 변경
- 결제 방식 변경 또는 삭제
- 계정의 결제 정보 보기
- AWS 계정 닫기
- Amazon EC2 요청에 대한 역방향 DNS를 제출
- CloudFront 키 페어 생성
- AWS에서 만든 X.509 서명 인증서 생성
- Amazon Route 53 도메인을 다른 AWS 계정으로 이전
- 더 긴 리소스 ID에 대한 Amazon EC2 설정 변경
- AWS 인프라에 대한 침투 테스트 수행 요청 제출
- Regarding: Account and Billing Support를 지원하는 AWS 지원 사례를 열기
- EC2 인스턴스에 대한 포트 25 이메일 제한 제거 요청
- AWS 계정 표준 사용자 ID를 찾기

(6) 진단 방법

a. "root user" 비활성화 여부 확인

b. "root user" 사용 내역 확인

[AWS Console]

- CloudTrail > 사용자 이름 "root"로 필터링 > 사용 내역 확인 (인터뷰)

(7) 판단 기준

a. "root user" 비활성화 상태일 경우 '양호'

b. AWS CloudTrail Event 확인 결과, "root user" 사용 이력이 없을 경우 '양호'

c. 담당자 인터뷰 및 증적을 통해 "root user" 사용 필요성이 소명된 경우 '양호'

(8) Remediation

a. "root user" 사용 시 사전/사후 전결 규정의 수립

b. 그 외 "2.1. Identity and Access Management"의 "root user" 관련 조치 방안 준용

(9) Logging & Monitoring

a. "root user" 관련 Event 탐지 및 실시간 Alert을 복수의 담당자에게 발송

[실시간 Alert 발송 조건]

- "root user"의 로그인
- "root user"의 Password 또는 MFA 변경
- "root user"의 Access Key 생성/변경

(10) Reference

a. AWS

- AWS account root user [LINK]
- Tasks that require root user credentials [LINK]
- Lock away your AWS account root user access keys [LINK]

b. CIS

- 1.4. Ensure no root user account access key exists
- 1.5. Ensure MFA is enabled for the "root user" account
- 1.7. Eliminate use of the root user for administrative and daily tasks

c. SSI

- 1.1. AWS 관리 콘솔 Root 계정 관리

진단방법

조치 가이드와 재발 방지로 마무리

위험수준
적용 난이도
점검 방식
진단 주기
근본 취지

2. 상세 진단 항목

2.1. Identity and Access Management

2.1.1. AWS Console 'root user' 사용 제한

각 IAM User에게 최소 권한을 부여하여 AWS Console에 접속하는 것을 원칙으로 하되 'root User' 권한이 필요한 경우, 사전 승인을 통해 인가된 범위 안에서 사용해야 합니다.

(1) 위험 수준 : Critical

(2) 적용 난이도 : Mid

(3) 점검 방식 : 정성 점검

(4) 진단 주기 : 실시간 권장, 최소 월별 점검

(5) 진단 항목 설명

a. "root user"가 비활성화, 즉 AWS Account 생성 이후 PW, MFA, Access Key 등이 설정되지 않은 상태로 한번도 사용된 적이 없는 경우에 한하여 '양호'로 간주함

b. AWS 기능 중 "root user"를 반드시 이용해야 하는 경우는 예외로 인정하나 "root user"를 활성화한 이후 관리 방안이 부재한 경우 '취약'으로 간주함

['root user' 필수 사용의 예시]

- 'root User' Password 변경
- AWS 지원 계획 변경
- 결제 방식 변경 또는 삭제
- 계정의 결제 정보 보기
- AWS 계정 닫기
- Amazon EC2 요청에 대한 역방향 DNS를 제출
- CloudFront 키 페어 생성
- AWS에서 만든 X.509 서명 인증서 생성
- Amazon Route 53 도메인을 다른 AWS 계정으로 이전
- 더 긴 리소스 ID에 대한 Amazon EC2 설정 변경
- AWS 인프라에 대한 침투 테스트 수행 요청 제출
- Regarding: Account and Billing Support를 지원하는 AWS 지원 사례를 열기
- EC2 인스턴스에 대한 포트 25 이메일 제한 제거 요청
- AWS 계정 표준 사용자 ID를 찾기

(6) 진단 방법

a. "root user" 비활성화 여부 확인

b. "root user" 사용 내역 확인

[AWS Console]

- CloudTrail > 사용자 이름 "root"로 필터링 > 사용 내역 확인 (인터뷰)

(7) 판단 기준

a. "root user" 비활성화 상태일 경우 '양호'

b. AWS CloudTrail Event 확인 결과, "root user" 사용 이력이 없을 경우 '양호'

c. 담당자 인터뷰 및 증적을 통해 "root user" 사용 필요성이 소명된 경우 '양호'

(8) Remediation

a. "root user" 사용 시 사전/사후 전결 규정의 수립

b. 그 외 "2.1. Identity and Access Management"의 "root user" 관련 조치 방안 준용

(9) Logging & Monitoring

a. "root user" 관련 Event 탐지 및 실시간 Alert을 복수의 담당자에게 발송

[실시간 Alert 발송 조건]

- "root user"의 로그인
- "root user"의 Password 또는 MFA 변경
- "root user"의 Access Key 생성/변경

(10) Reference

a. AWS

- AWS account root user [LINK]
- Tasks that require root user credentials [LINK]
- Lock away your AWS account root user access keys [LINK]

b. CIS

- 1.4. Ensure no root user account access key exists
- 1.5. Ensure MFA is enabled for the "root user" account
- 1.7. Eliminate use of the root user for administrative and daily tasks

c. SSI

- 1.1. AWS 관리 콘솔 Root 계정 관리

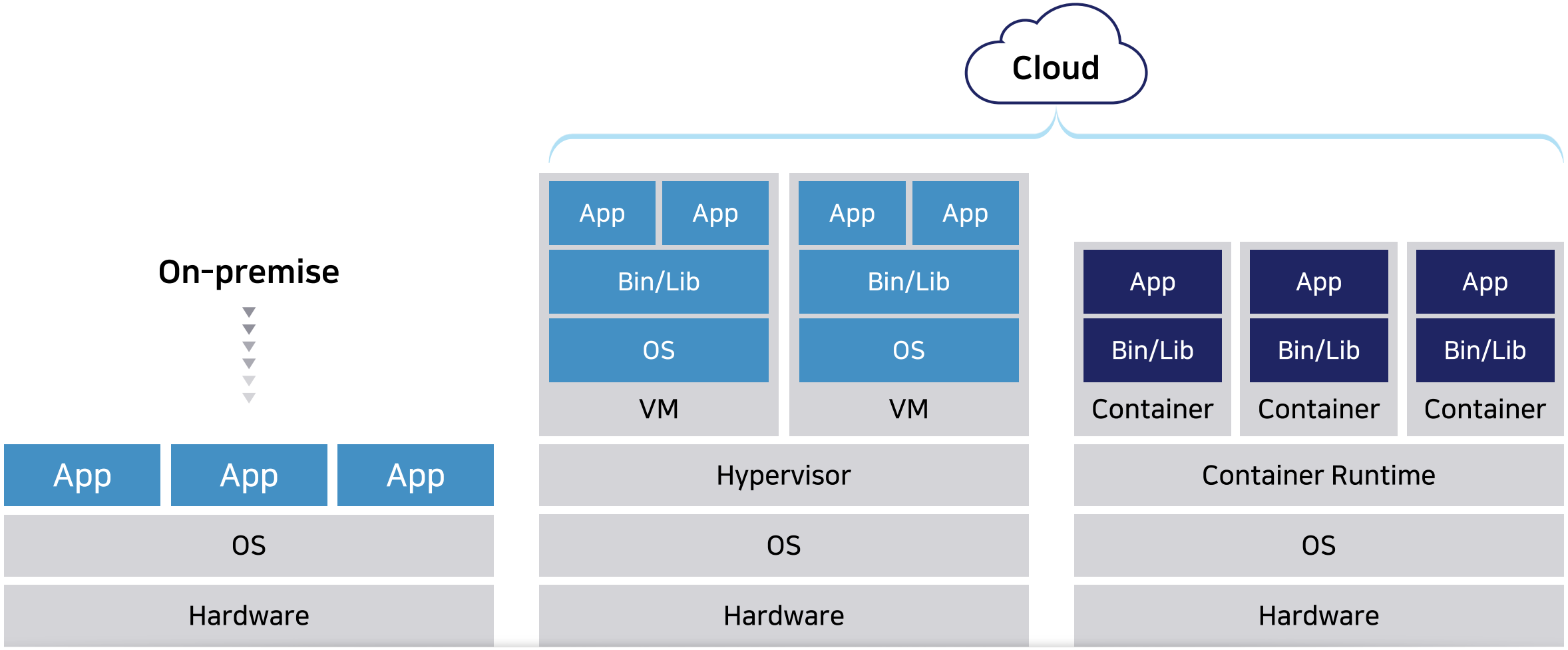
판단 기준
조치 방법
모니터링
참고 자료

클라우드가 On-premise 만큼 안전해지려면 어떻게 해야 하나요?

Q

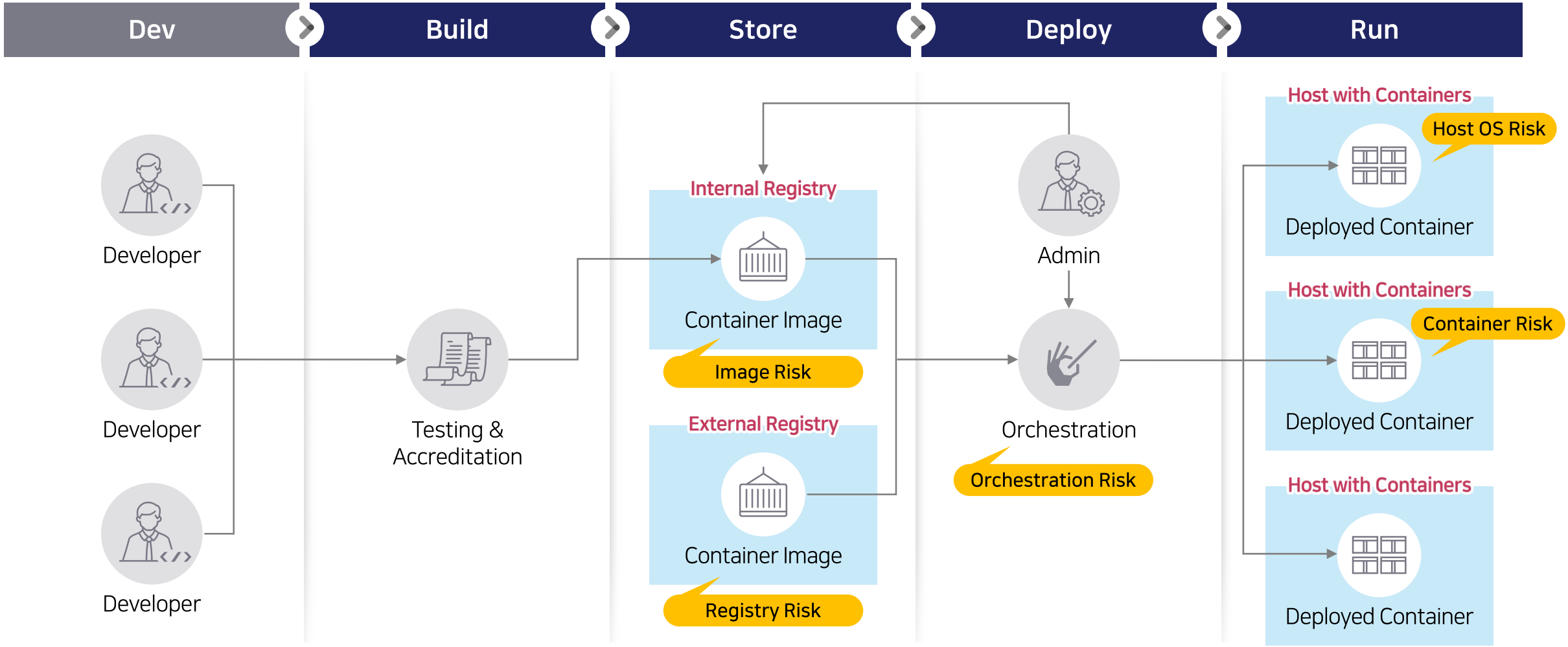
On-premise에서 사용하던 보안 솔루션을 그대로 클라우드에 대등하게 옮길 수 있나요?

On-premise와 클라우드의 차이



Container 보안

On-premise와 클라우드 보안이 동일하지 않은 첫번째 Challenge – 짧은 Lifecycle을 갖는 환경



※ NIST.SP.800-190 - Application Container Security Guide

DevSecOps Pipeline과 Tool-chain을 통한 보안

On-premise와 클라우드 보안이 동일하지 않은 두번째 Challenge – 개발, 운영, 보안의 경계가 없는 환경

Collaborate

Communication
- Slack
- Mattermost

Knowledge Sharing
- Confluence
- Reddit

Appl. Lifecycle Mgmt.
- JIRA
- Launchpad
- Trello
- Basecamp

Build

SCM / VCS
- Gitlab
- GitHub

Cont. Integration
- Circle CI
- Jenkins

Build
- Docker
- Helm

Database
- TiKV
- Vitess

Test

OSS License Mgmt.
- Blackduck
- Fossid
- White Source

Static Appl. Security Testing
- SonarQube
- Fortify
- Checkmark

Vulnerability Analysis
- Kube-bench
- Kube-hunter
- Clair

Key Management
- Spiffe
- Spire
- Vault

Deploy

Artifact Mgmt.
- Nexus Repository
- Artifact Hub

Deployment
- Spinnaker
- Octopus Deploy

Config / Provisioning
- Terraform
- Ansible
- Chef
- Puppet

Run

Orchestration
- K8s
- Mesos

IaaS / PaaS
- AWS
- Azure

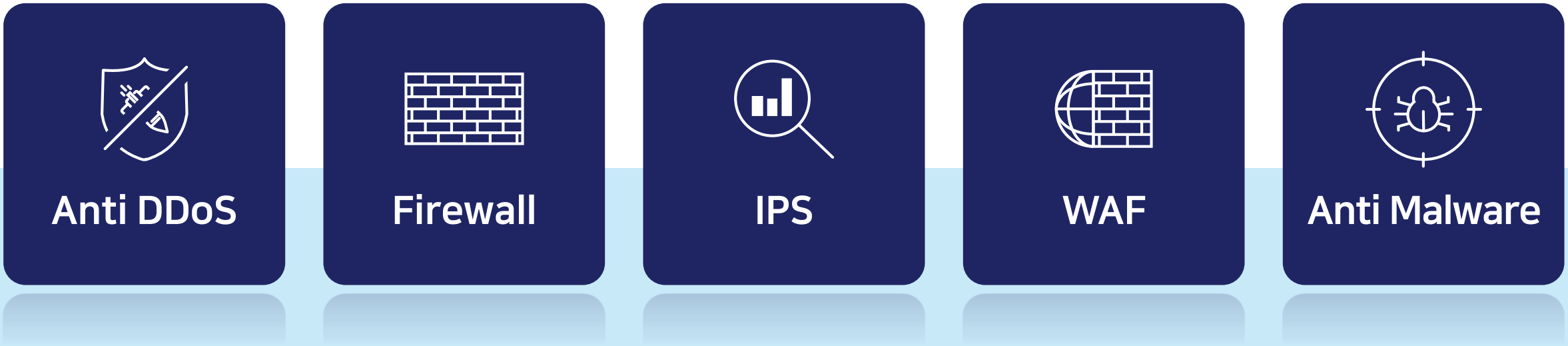
Monitoring
- Prome-theus
- Grafana

Logging
- Elastic Search
- Datadog

3위 보안 5종 세트는 대체 무엇인가요?

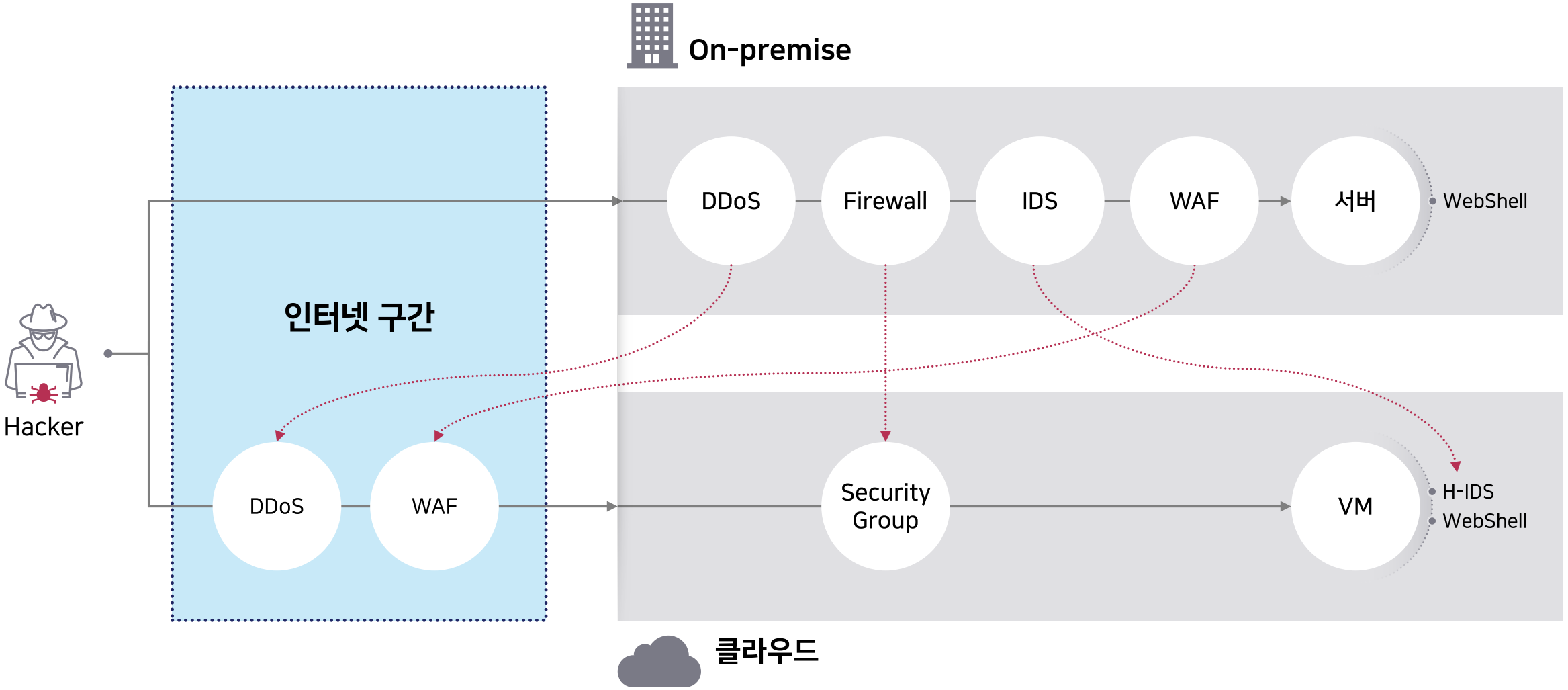
Q 클라우드 보안은 이것만 하면 된다고 들었습니다.

보안 5종 세트의 구성



보안 5종 세트는 On-premise에서 시작

보안 5종 세트도 클라우드 환경에 맞게



2위

삼성SDS 클라우드 보안 기준은 왜 그렇게 어려운가요?

Q

보안 때문에 일을 못하겠어요!

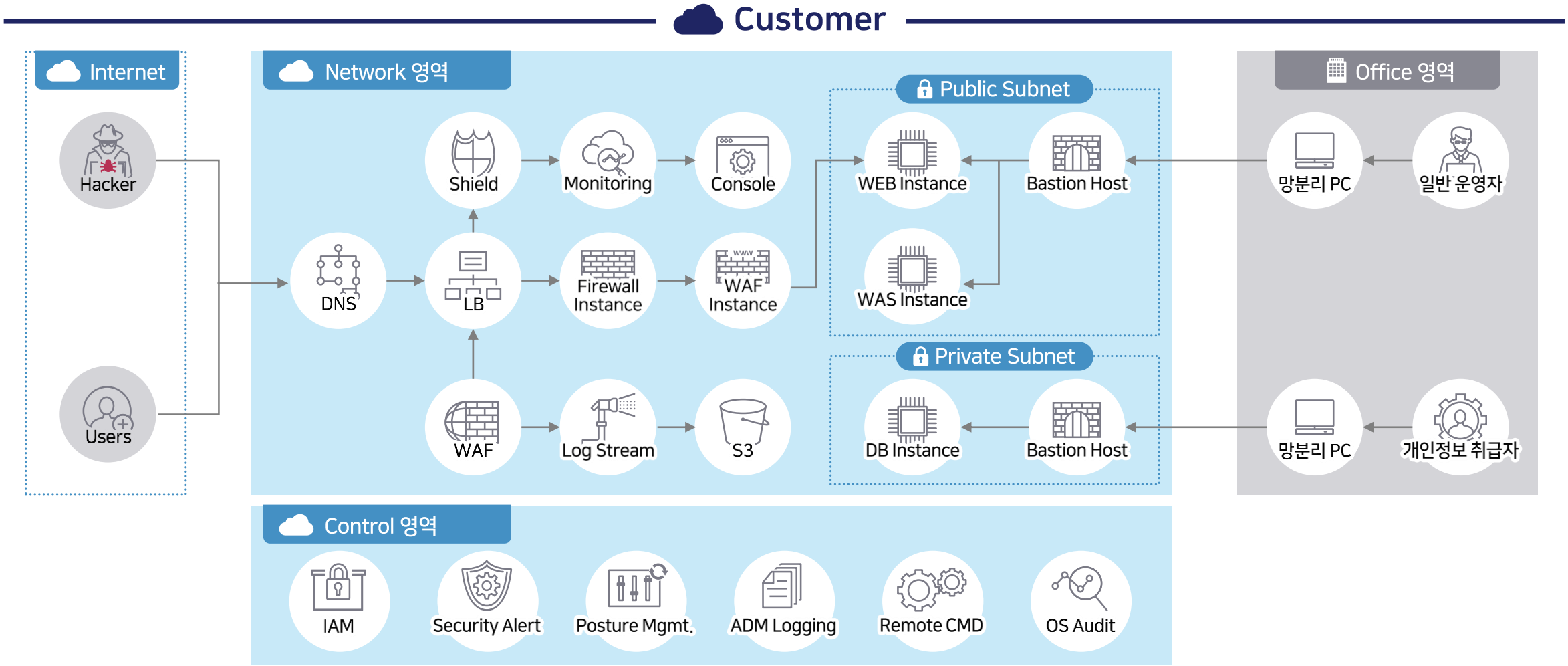
정량적 보안 규정은 글로벌 기준이 좀 더 엄격합니다.

사례	SAMSUNG SDS	글로벌 (CIS Benchmark)
MFA 적용 (Multi-Factor Auth.)	• 모든 AWS 관리콘솔 계정에 MFA 필수 적용	• (좌동) • root 계정은 Hardware 방식의 MFA 적용
운영자 활동 로그	• 모든 Region에 활성화	• (좌동) • 이상 동작 감지 시 Alert 발생하도록 설정
패스워드 복잡도	• 8글자 이상, 영문자+기호+숫자 조합	• 14글자 이상, 대문자+소문자+숫자+기호
패스워드 재사용	• 최근 패스워드 2개 기록	• 최근 패스워드 24개 기록

하지만 정성적 점검은 삼성SDS가 좀 더 면밀하게 살피고 있습니다.

사례	SAMSUNG SDS	글로벌 (CIS Benchmark)
권한 설정	• (좌동) • 직무 및 사용 목적에 따라 IAM 사용자 권한 최소화	• 모든 권한을 의미하는 "*:*" 설정 금지
접근 제어	• (좌동) • N/W 접근 정책은 최소 허용 원칙에 따라 설정	• 모든 IP에 22, 3389 포트 오픈 금지
Key 관리	• (좌동) • 1인 1개의 Access Key 발급만 허용	• root의 Access Key 발급 금지
N/W 연동	• (좌동) • N/W 연동 시 최소 범위로 오픈	• 모든 IP, Port 해제 금지

삼성SDS가 수고한 만큼 고객은 더 안전한 클라우드를 사용할 수 있습니다.



클라우드 보안은 CSP가 해주는 것 아니었나요?

Q 왜 CSP의 고객인 우리가 대신 해주어야 하나요?

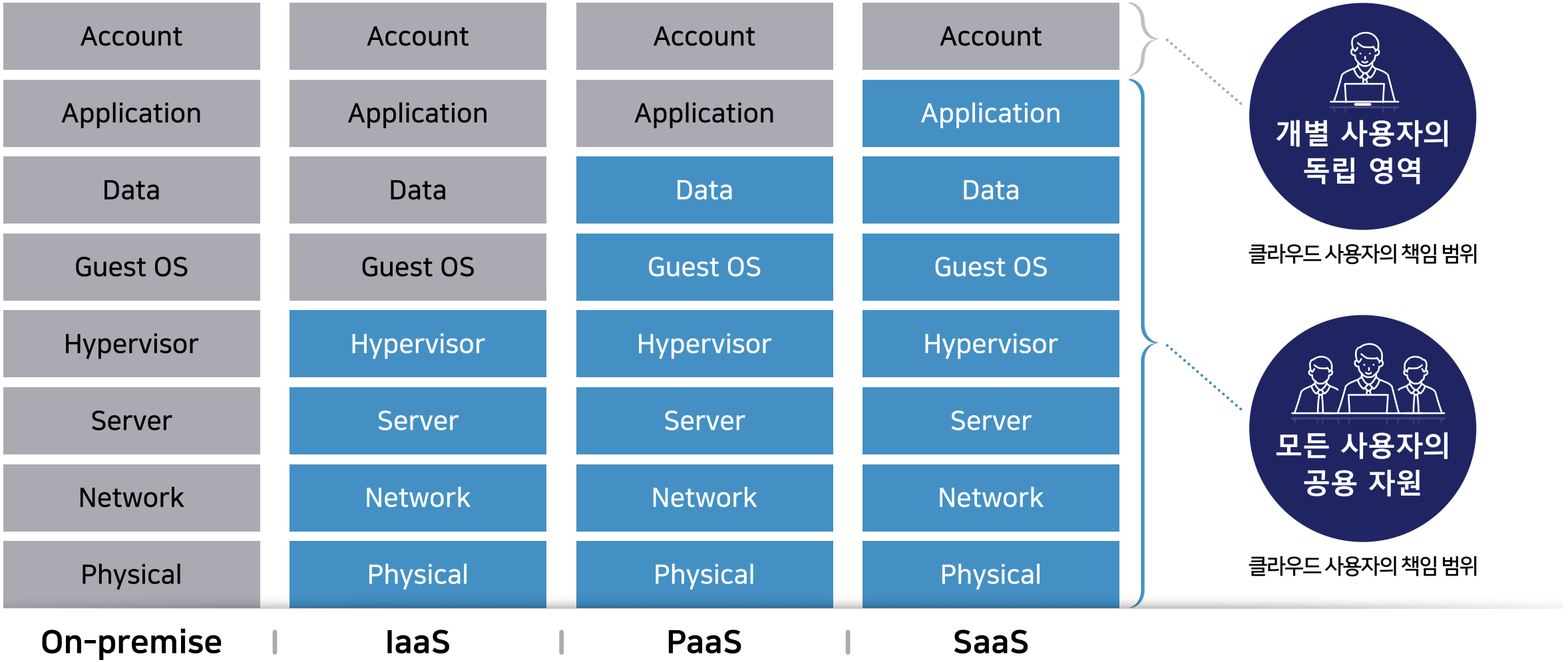
클라우드 보안 사고의 책임은 대부분 고객에게 돌아옵니다.

Capital One

amazon

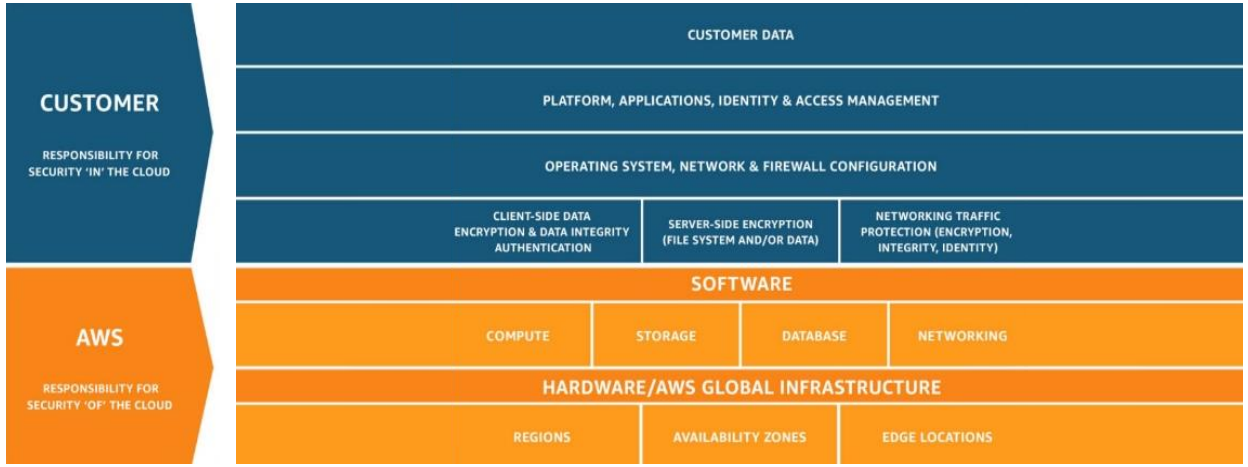
※RSAC 2020, CSV-T10, Cloud Threat Hunting (p6)

‘공동책임모델’에 따라 보안 책임과 역할이 정해집니다.

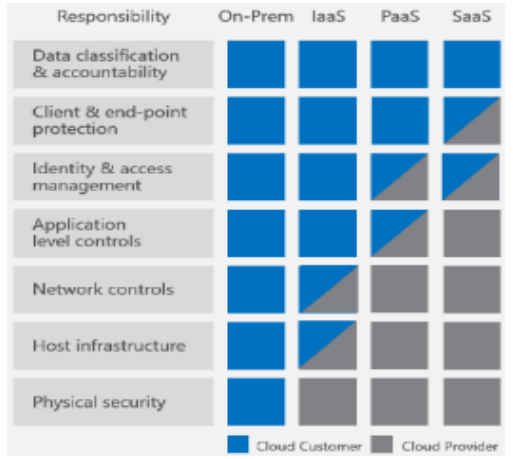


CSP 마다 '공동책임모델'의 표현은 다르지만 같은 원리를 다룹니다.

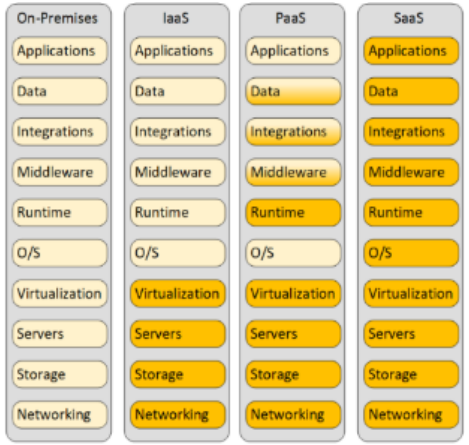
amazon



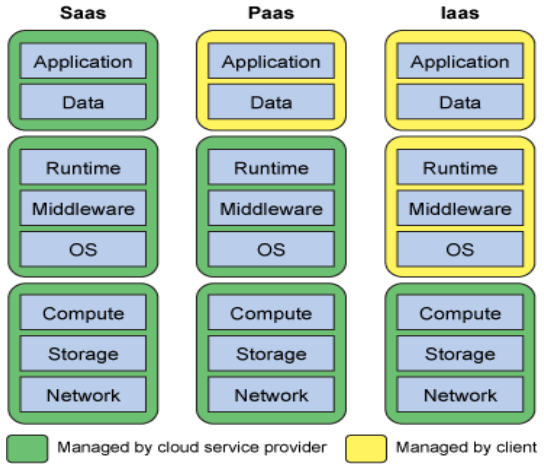
Microsoft



ORACLE



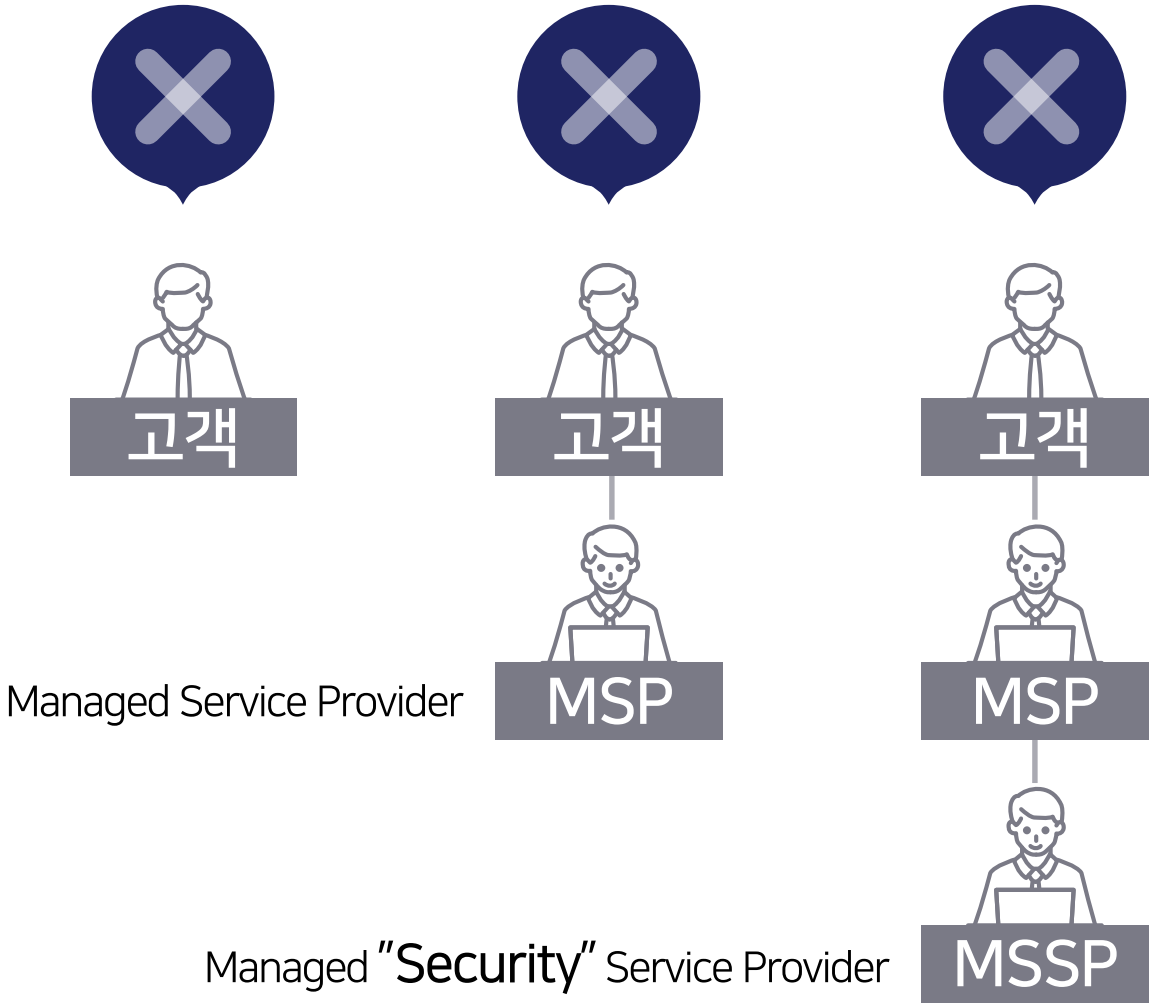
IBM

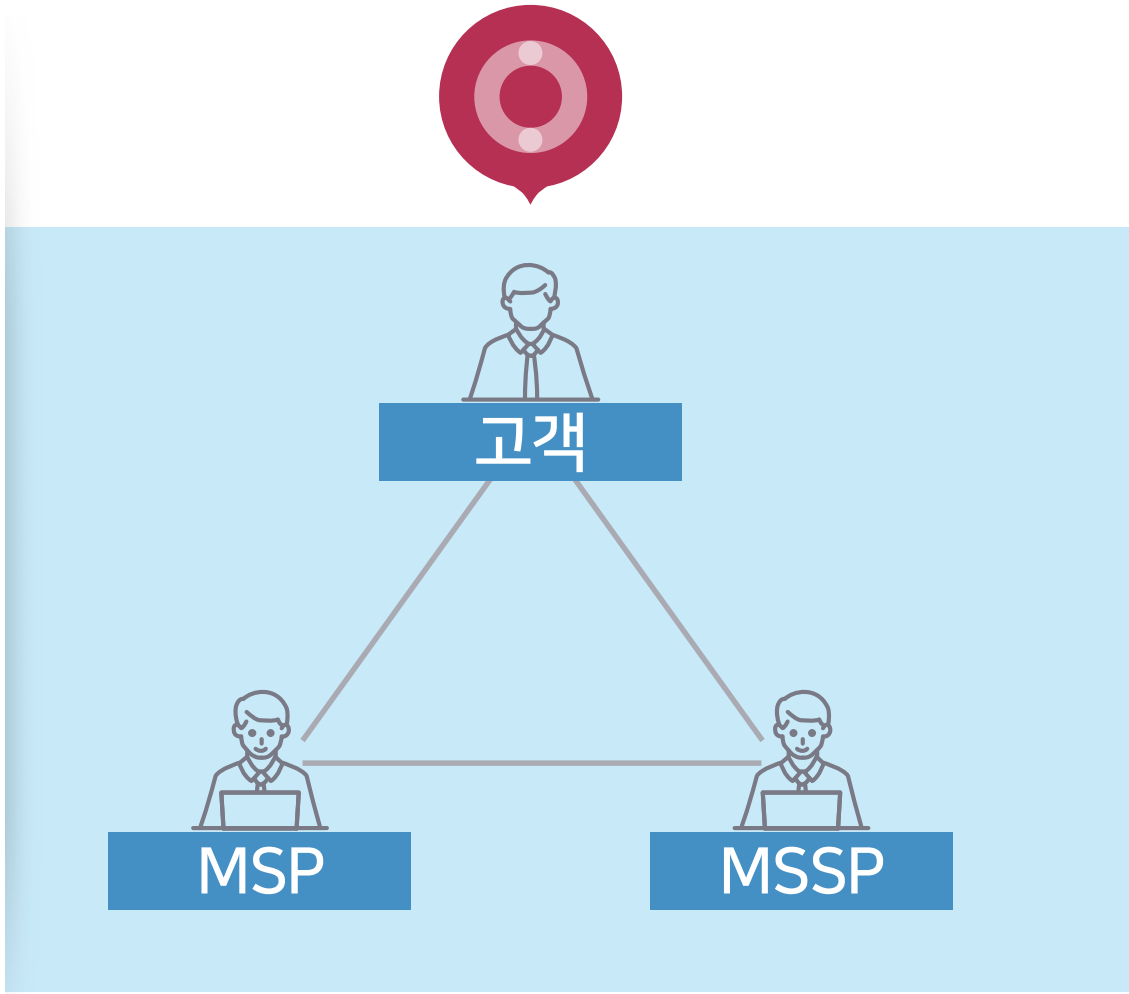


Google

사용자도 사용자의 보안 책임과 역할을 다해야 합니다.

역량 있는 MSSP를 활용하시는 것도 좋은 선택이십니다.





결언

“ 클라우드에서 **보안**은 걸림돌로 생각되기 쉽지만 ”
보안이 해결된다면 **클라우드를 선도하는 지렛대**가 될 수도 있습니다.

Thank you

SAMSUNG SDS