REAL

SUMMIT 2022

SAMSUNG SDS

클라우드의 시작과 끝,
클라우드 보안

삼성SDS 클라우드보안서비스그룹 **천준호 그룹장**

AGENDA

Ⅰ. 개요

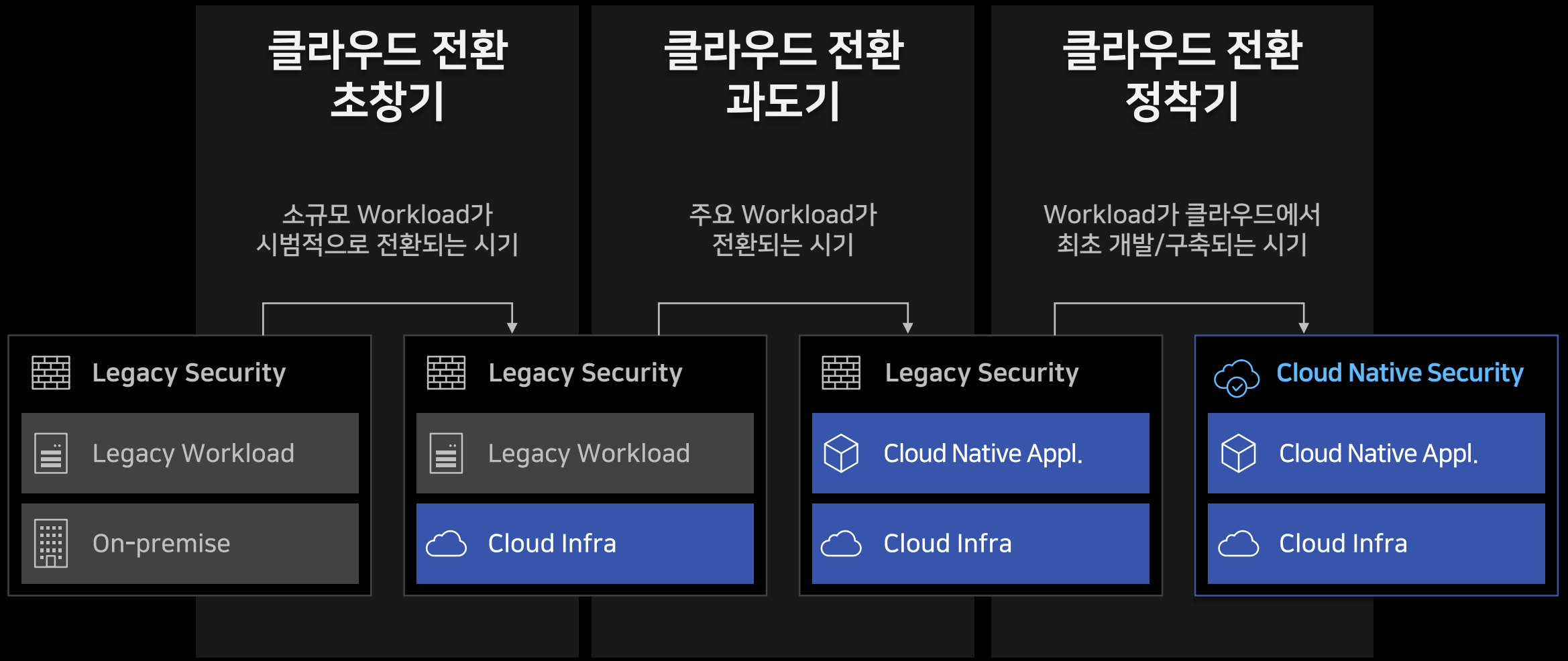
Ⅱ. 클라우드 전환 초창기

Ⅲ. 클라우드 전환 과도기

Ⅳ. 클라우드 전환 완성기

Ⅴ. 결론

개요



Shared Responsibility Model

클라우드 사업자와 사용자가 보안 역할을 분담하는 클라우드 고유의 보안 체계

On-premise	IaaS	PaaS	SaaS
Account	Account	Account	Account
Application	Application	Application	Application
Data	Data	Data	Data
Guest OS	Guest OS	Guest OS	Guest OS
Hypervisor	Hypervisor	Hypervisor	Hypervisor
Server	Server	Server	Server
Network	Network	Network	Network
Physical	Physical	Physical	Physical

클라우드 사용자의 보안 범위

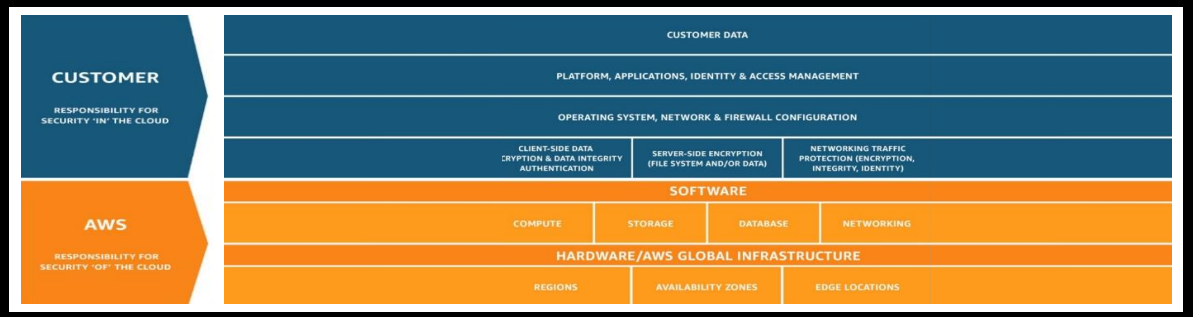
클라우드 사업자의 보안 범위

Shared Responsibility Model

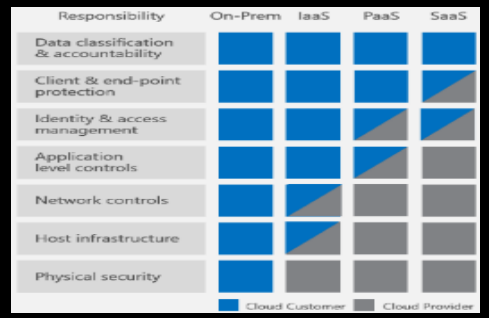
주요 CSP의 Shared Responsibility Model

☑ 각 CSP 마다 '공동책임모델'의 표현은 다르지만 같은 원리로 사업자와 사용자의 영역을 표현

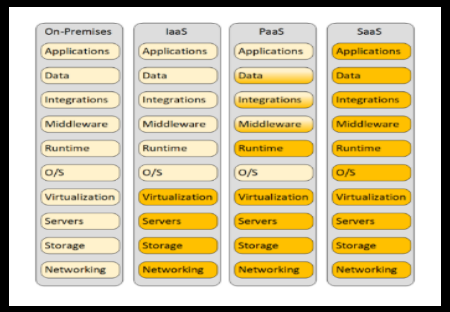
amazon



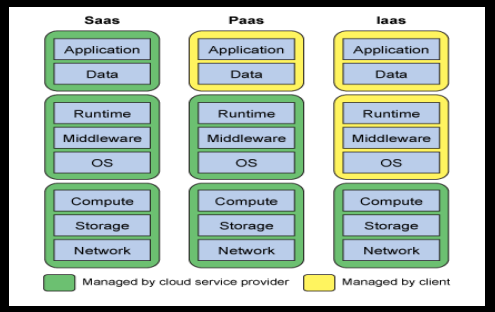
Microsoft



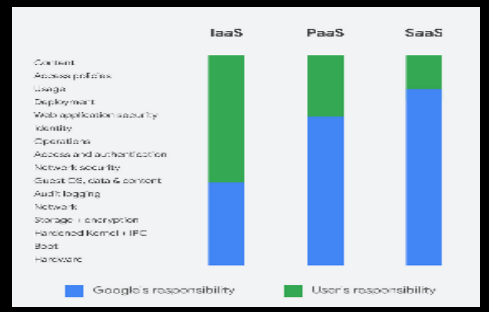
ORACLE



IBM



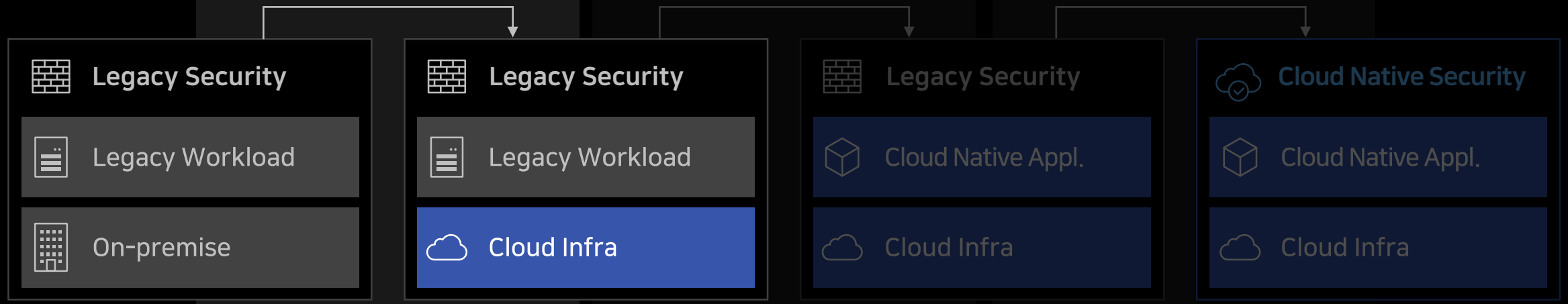
Google



클라우드 전환 초창기

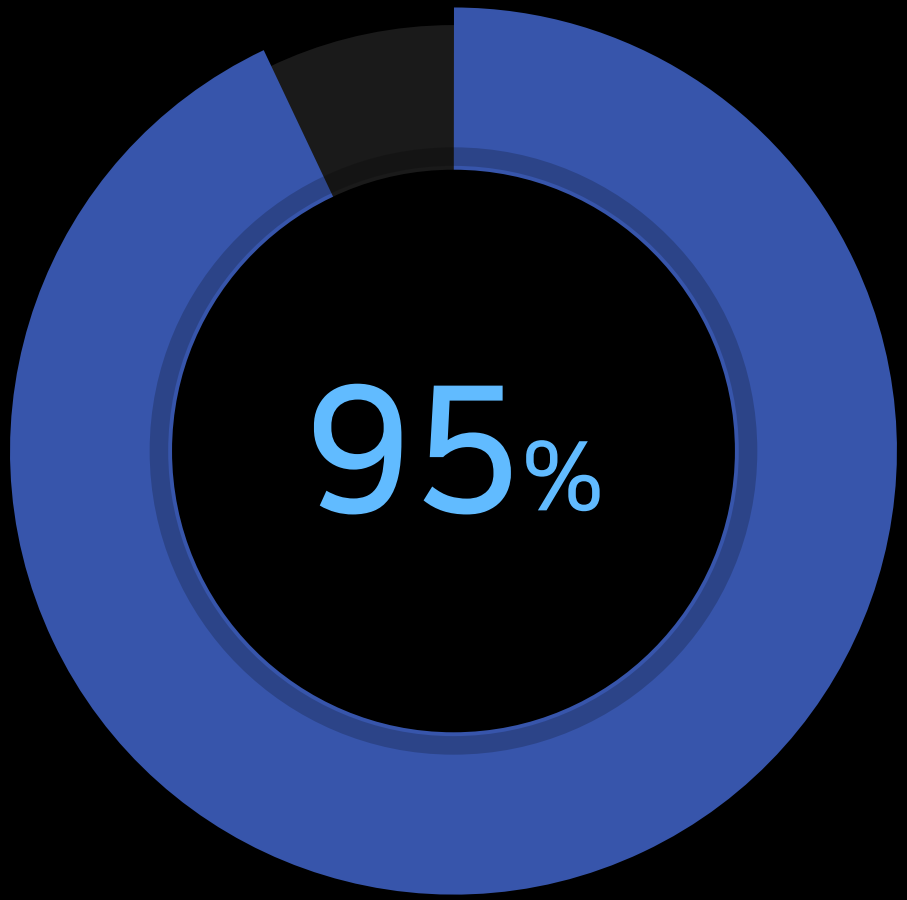
클라우드 전환 초창기

❶ 클라우드 보안 정책
❷ 클라우드 보안 진단



클라우드 전환 과도기

클라우드 전환 정착기



클라우드 보안 사고의 95%는

사용자의 실수에 의해 발생할 것이다.

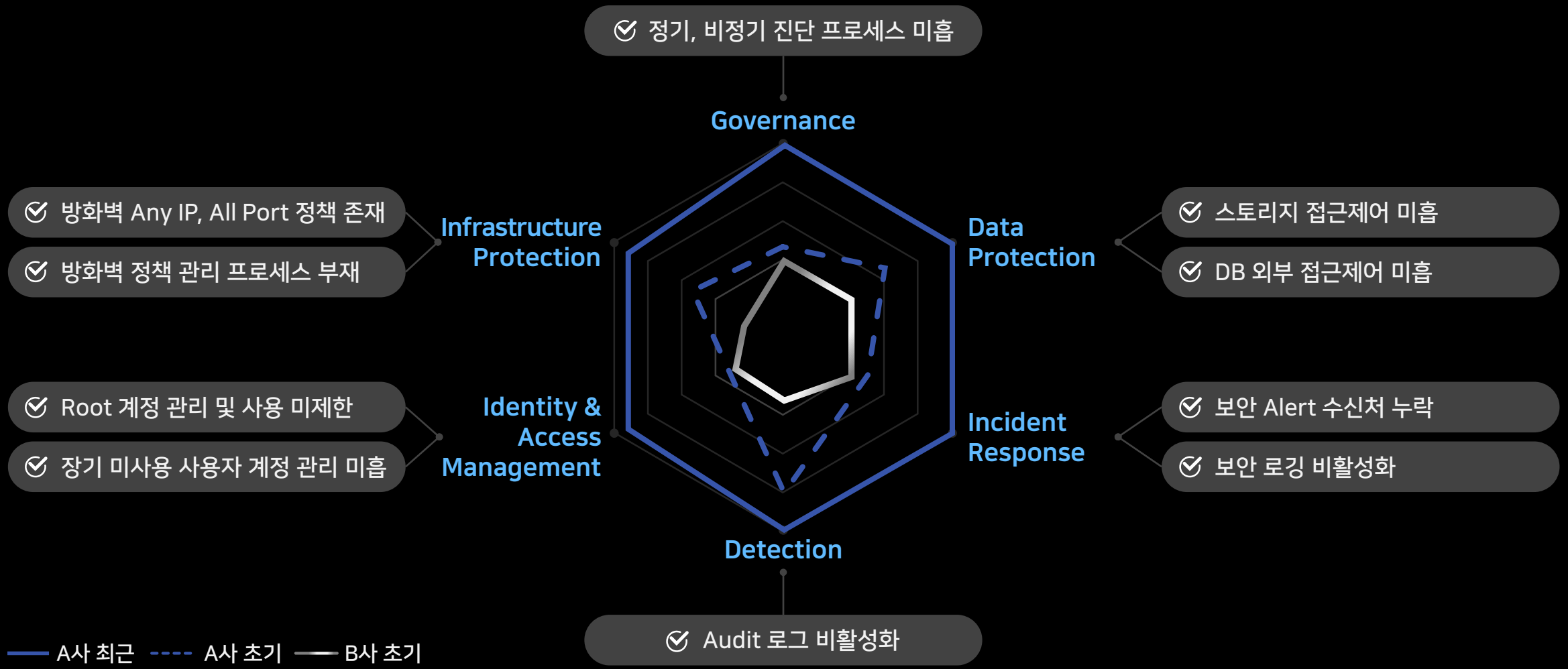
Misconfiguration

- Gartner -

1. 클라우드 보안 정책

❶ 적합성 검토	심사	승인	**통보**	클라우드 활용 현황의 전사적 공유 체계
❷ 업체 선정	CSP		**MSP** **MSSP**	CSP / MSP / MSSP 모두에게 보안 요구사항 제시
❸ 책임 식별	CSP		**사용자**	Shared Responsibility Model에 입각한 책임 식별
❹ 폐기 절차	완전 폐기		**부분 폐기**	CSP 상품 일부의 활용 중지 또는 인적 변동 고려
❺ 침해 대응	준비 단계 재발 방지	외부 공격 사고 인지	**내부 시도** **인지 수단**	해커의 주요 목표가 CSP Console로 전환
❻ 취약점 진단	정량 진단 정성 진단	정기 진단 비정기 진단	**진단 기준** **진단 자동화**	진단 기준의 단순화를 통한 자동화, 상시화 지향

2. 클라우드 보안 진단



2. 클라우드 보안 진단

클라우드 보안 진단의 예시

모든 사용자 계정은 다중 인증(MFA)을 실시하는가

IAM 사용자 계정의 MFA 설정

AWS

AWS 콘솔 접속
- IAM
- Users
- 사용자 선택
- Security Credentials

▶ Assigned MFA Device 설정 값 "Yes" 확인

RAM 사용자 계정의 MFA 설정

AliCloud

Alibaba Cloud 콘솔 접속
- RAM
- Identities
- Users
- 사용자 선택
- Console Logon Management

▶ Console Access :"Enabled" 확인
▶ Required to Enable MFA 설정 값 "Yes" 확인

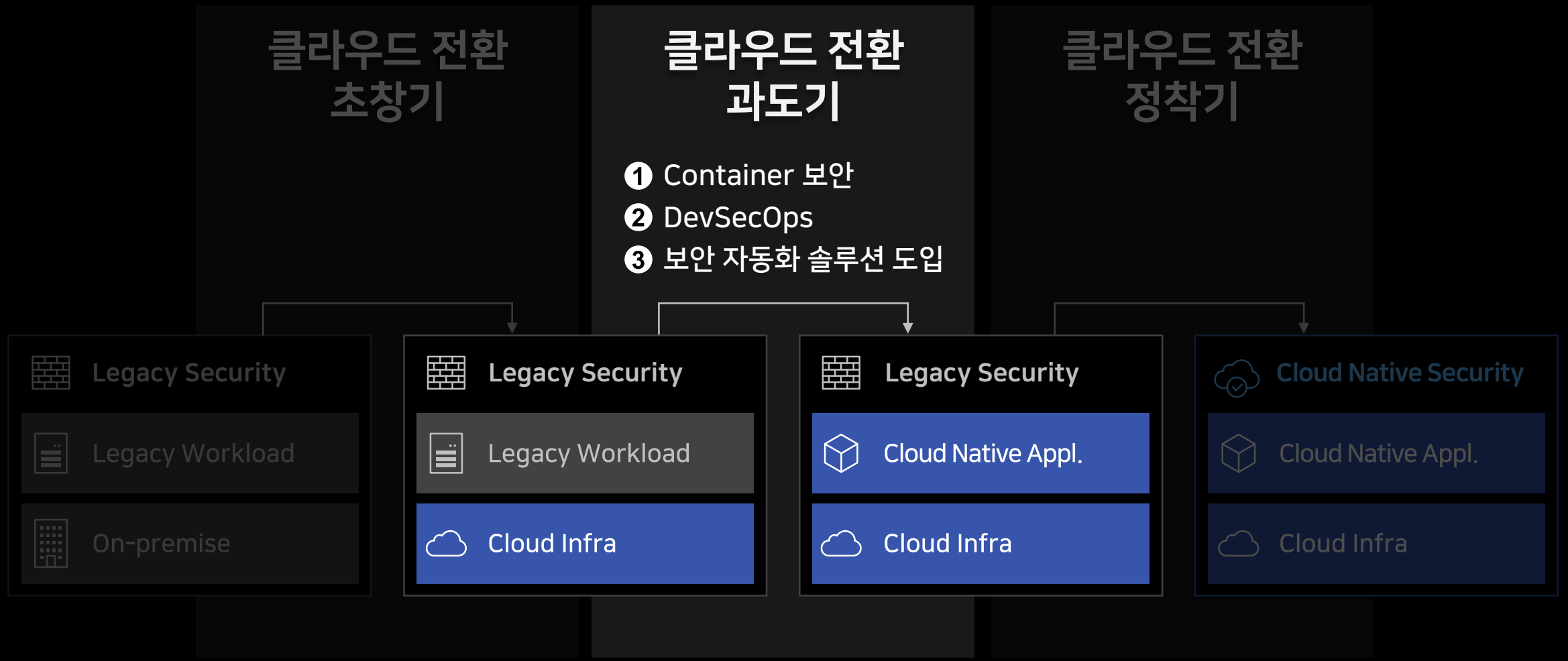
Sub Account의 MFA 설정

NCP

NCP 콘솔 접속
- Products & Services
- Sub Account
- 리소스 中 서브 계정 선택

▶ 2차 인증 설정 값 "필수" 확인

클라우드 전환 과도기



Dev		Sec		Ops
100	:	1	:	10

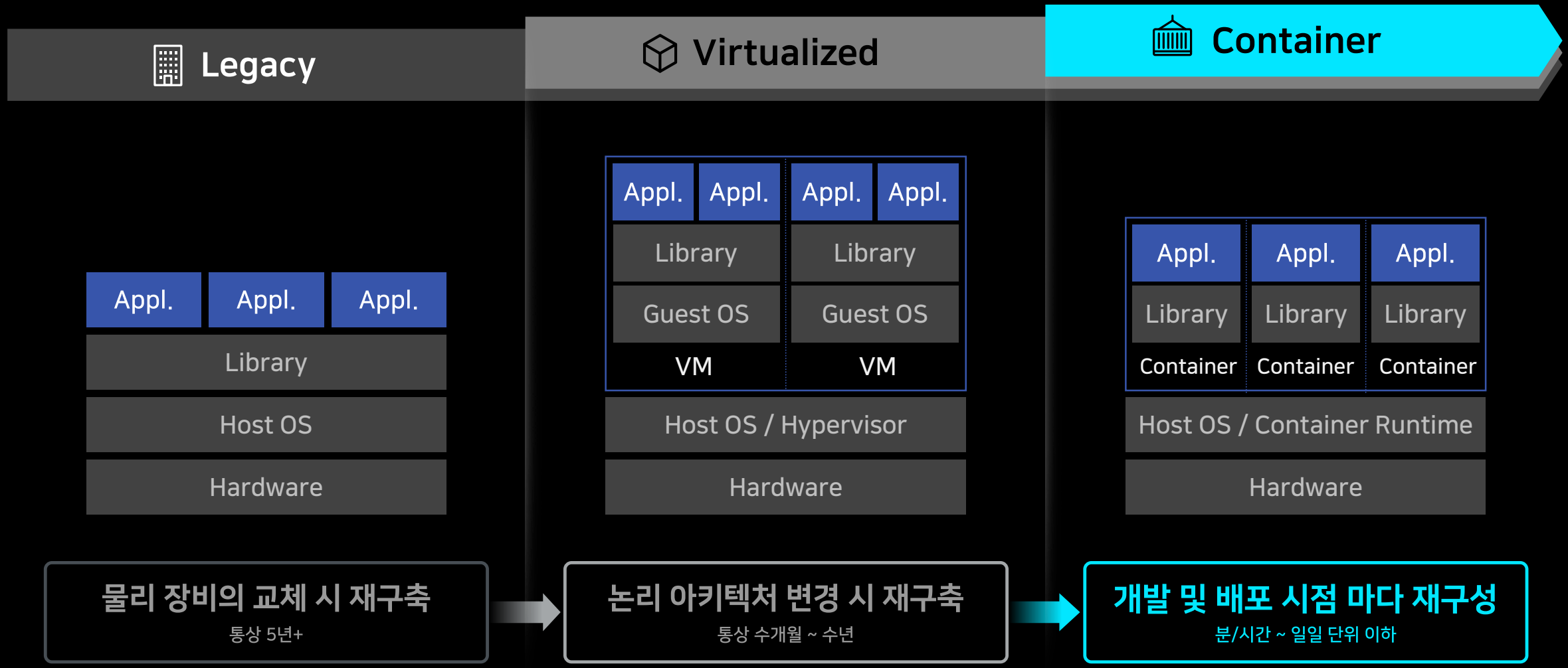
DevSecOps를 위한 **인력 구성**의 최적 비율은 **100:1:10** 이며

보안은 모든 구성원의 책임이 되어야 한다.

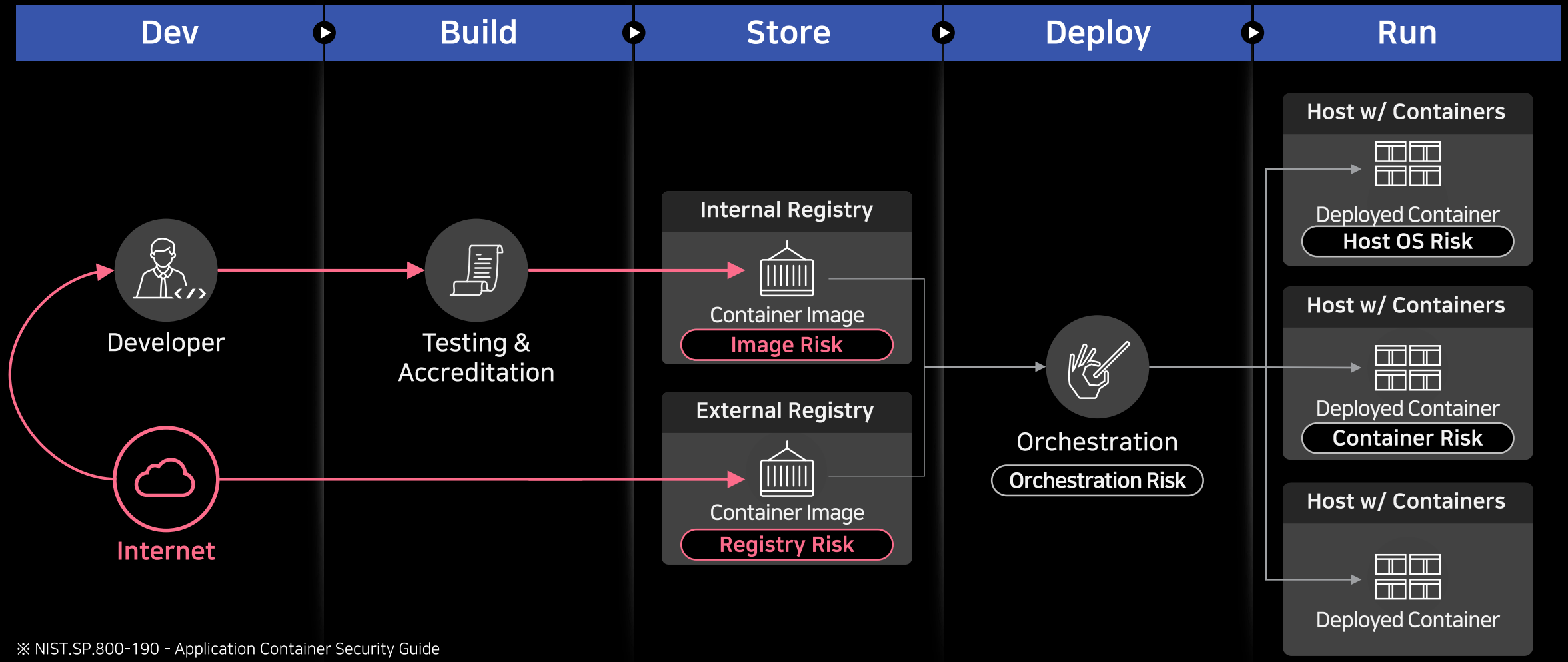
Security is Everyone's Responsibility

- Shannon Liets -

1. Container 보안



1. Container 보안

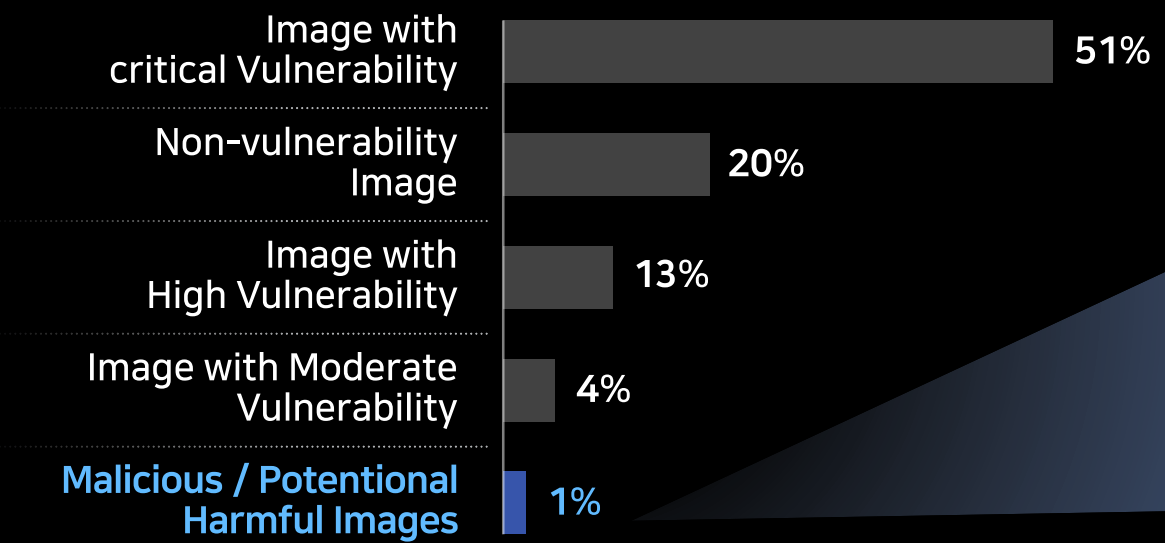


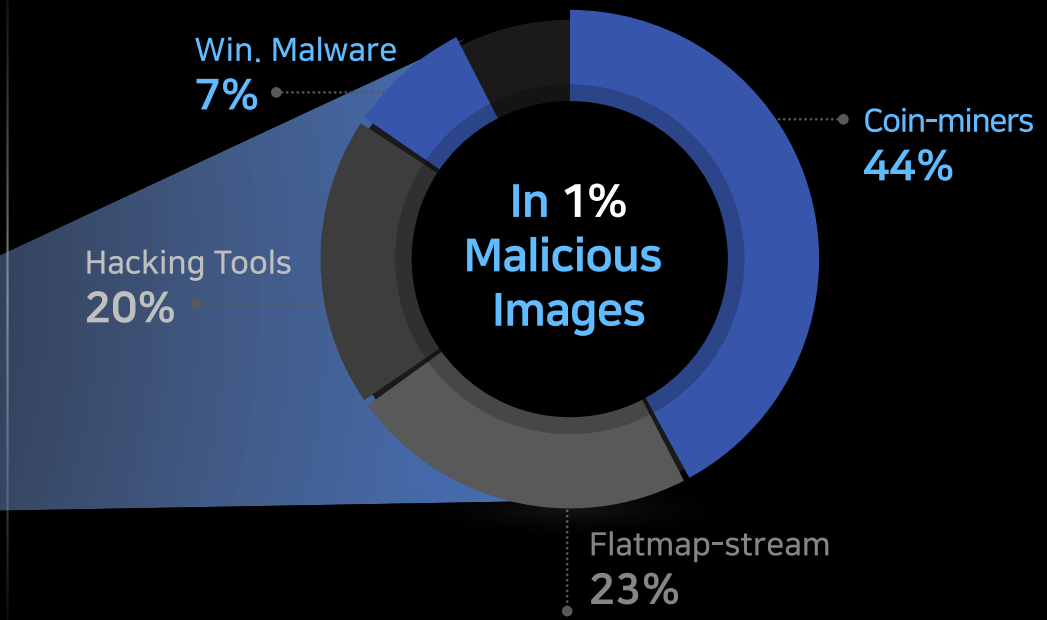
※ NIST.SP.800-190 - Application Container Security Guide

1. Container 보안

Container 보안 취약점 동향

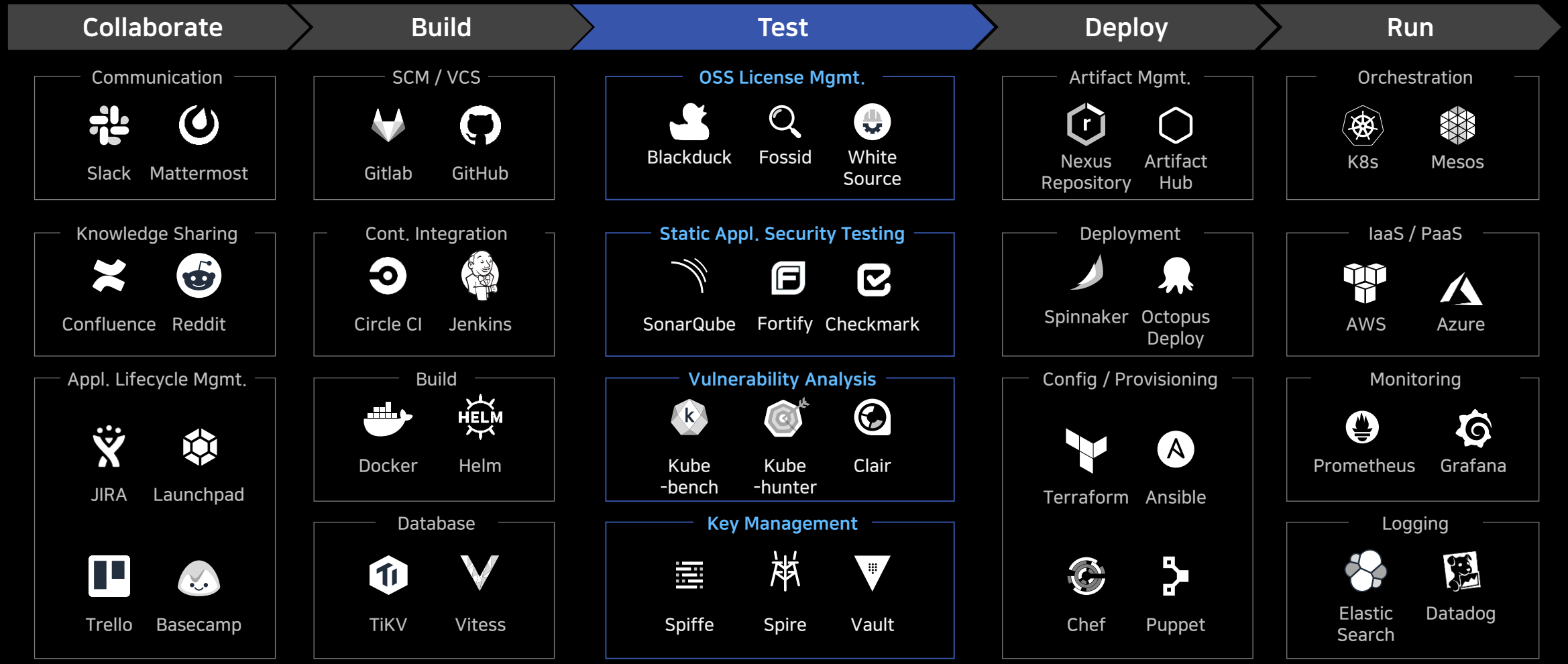
Public Docker Container Images in Docker Hub



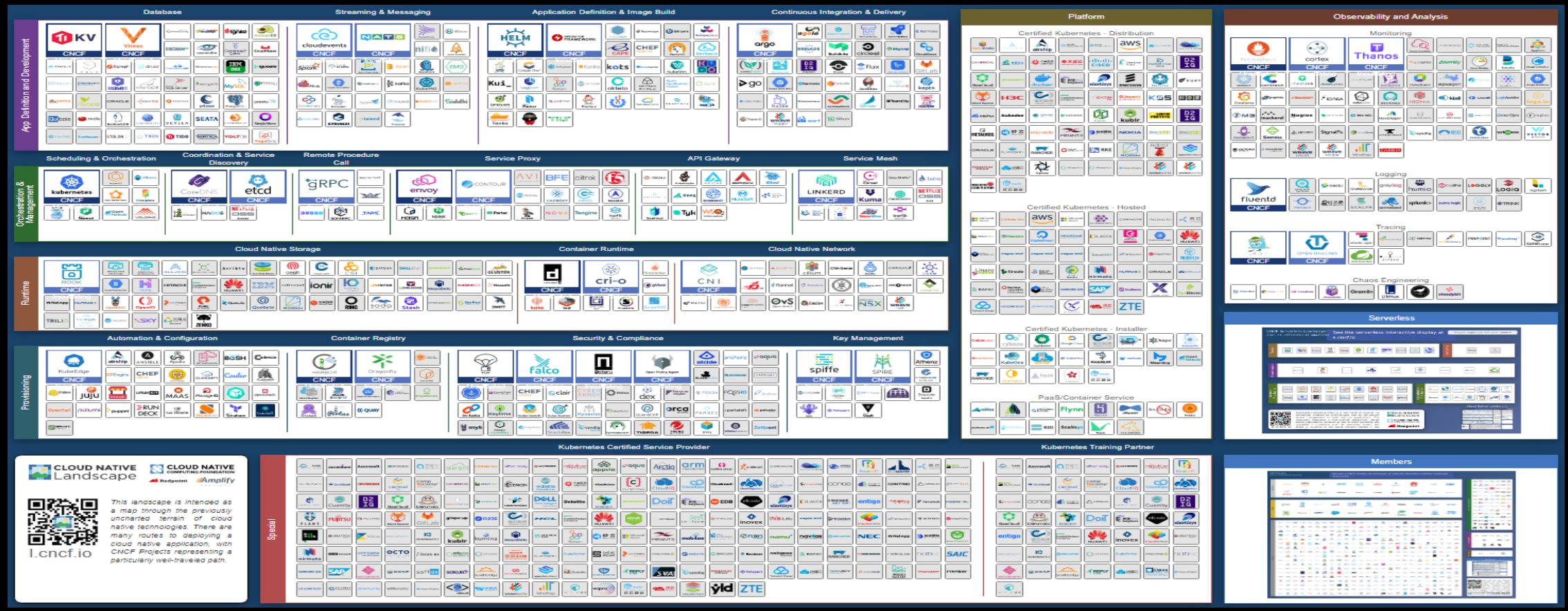


※ Prevasio, 2020

2. DevSecOps

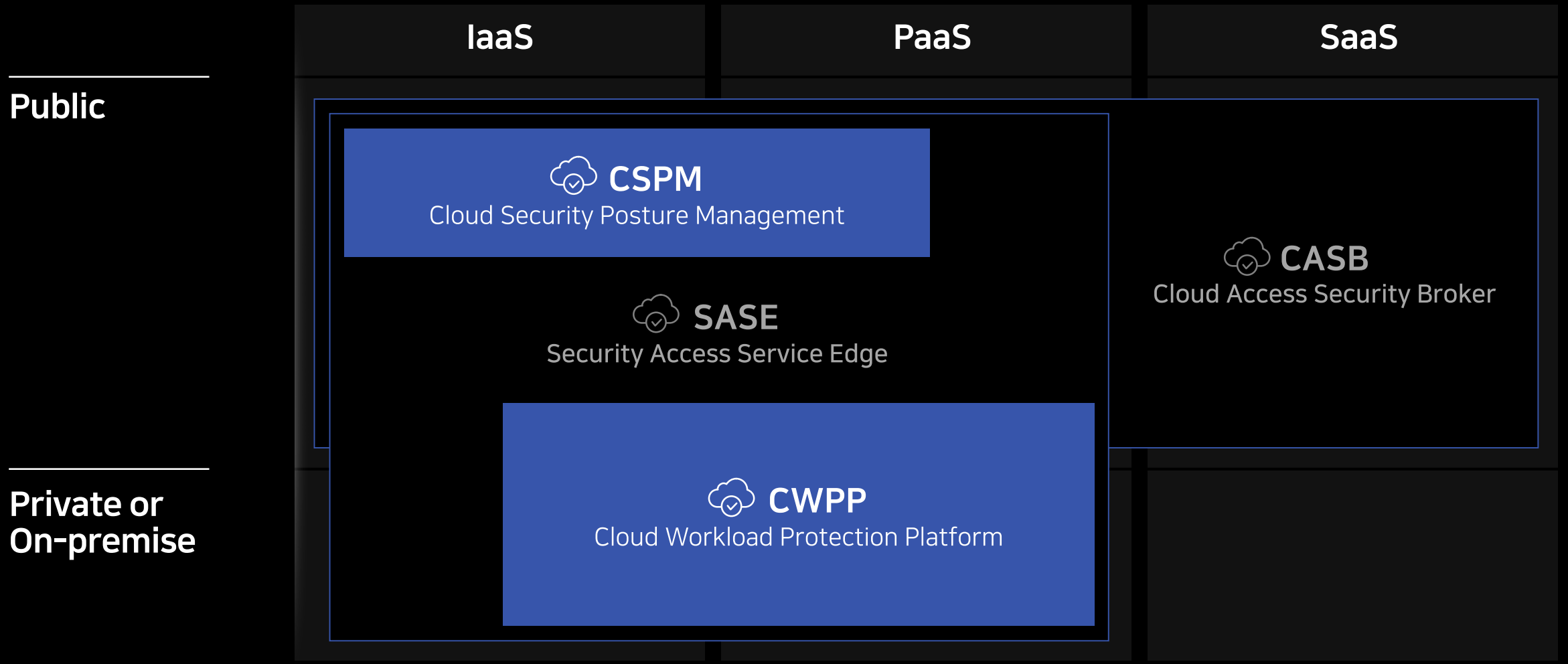


2. DevSecOps



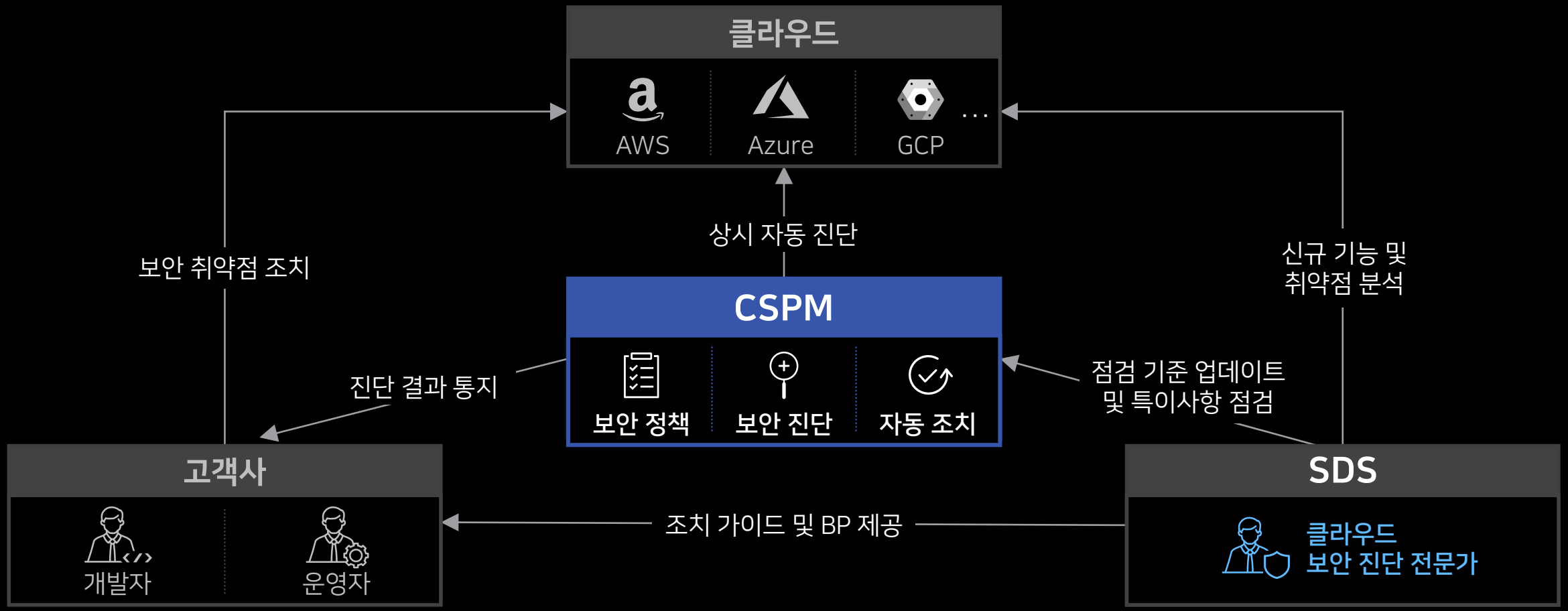
※ Cloud Native Computing Foundation, 2022

3. 보안 자동화 솔루션 도입



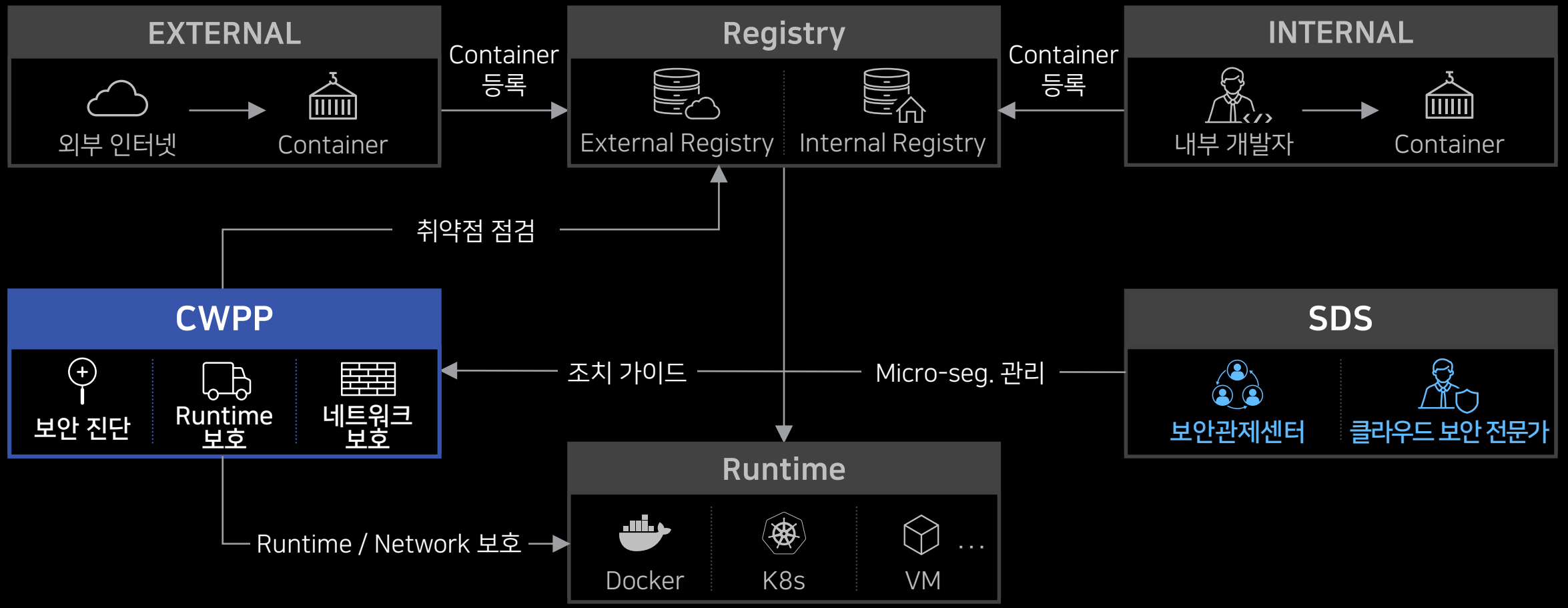
3. 보안 자동화 솔루션 도입

Cloud Security Posture Management : Posture 상의 보안 취약점을 상시 자동 진단하는 솔루션



3. 보안 자동화 솔루션 도입

Cloud Workload Protection Platform : Container 환경의 취약점 진단과 네트워크 제어하는 솔루션



클라우드 전환 완성기

클라우드 전환 초창기

- Legacy Security
- Legacy Workload
- On-premise

클라우드 전환 과도기

- Legacy Security
- Legacy Workload
- Cloud Infra

클라우드 전환 정착기

1. CSP Native vs 3rd Party
2. 보안의 클라우드 전환

- Legacy Security
- Cloud Native Appl.
- Cloud Infra

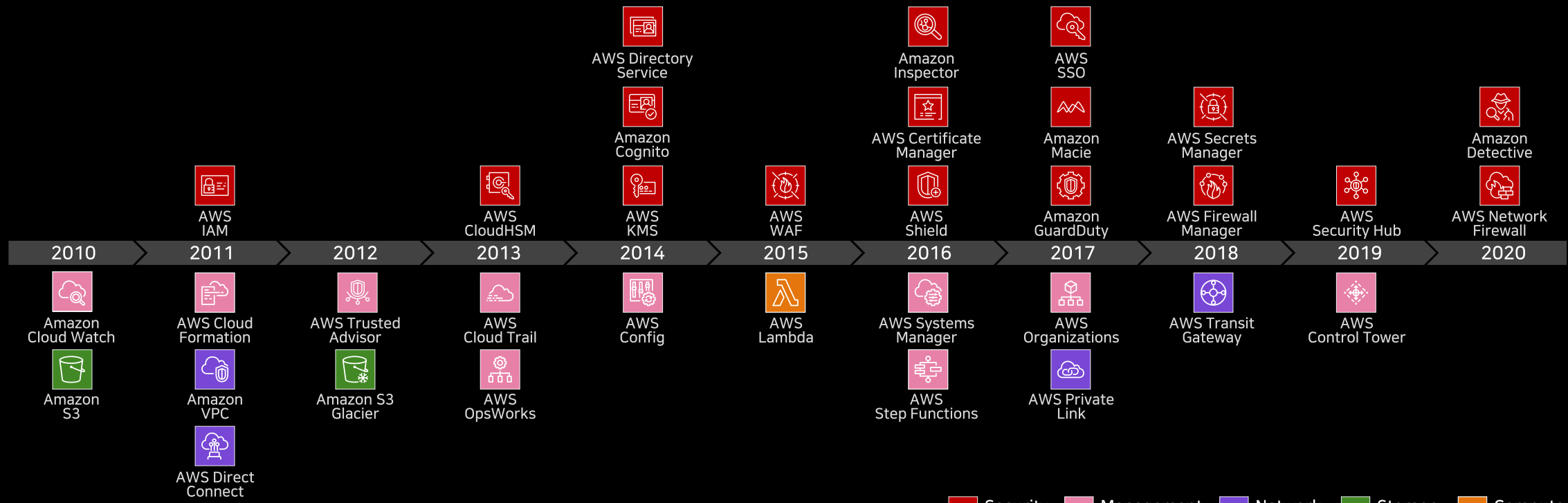
- Cloud Native Security
- Cloud Native Appl.
- Cloud Infra

1. CSP Native vs 3rd Party 보안 솔루션

		비교 우위
비용 효율성	CSP Native는 초기 투자 비용이 없으며 사용한 만큼 지불 할 수 있음	CSP Native / 3rd Party ISV
가용성	CSP Native는 CSP가 SLA를 보장하며, 고객의 운영 부담이 낮음	CSP Native / 3rd Party ISV
탄력성	CSP Native는 사용량 증감에 따라 CSP가 자동으로 Resource를 조절함	CSP Native / 3rd Party ISV
도입 및 전환 속도	CSP Native 보안 기능은 구매 / 설치 등의 절차가 불필요함	CSP Native / 3rd Party ISV
Multi 클라우드	3rd Party ISV는 모든 CSP에 동일 솔루션 적용 및 관리 가능함	CSP Native / 3rd Party ISV
Hybrid 클라우드	3rd Party ISV는 On-premise 까지 동일 솔루션 적용 및 관리 가능함	CSP Native / 3rd Party ISV
난이도 및 기술지원	3rd Party ISV는 각 솔루션 제조사의 기술지원을 받기 용이함	CSP Native / 3rd Party ISV

1. CSP Native vs 3rd Party 보안 솔루션

CSP Native 보안의 예시 - AWS

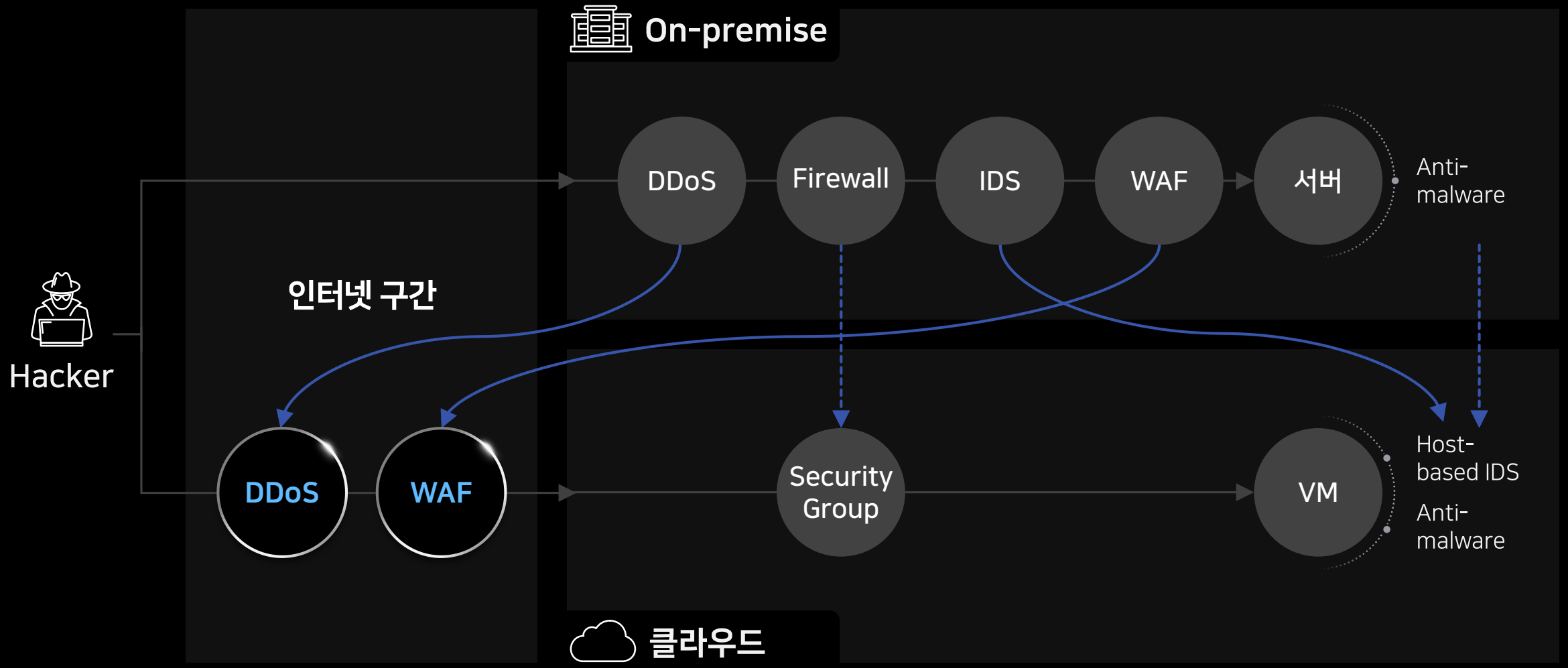


1. CSP Native vs 3rd Party 보안 솔루션

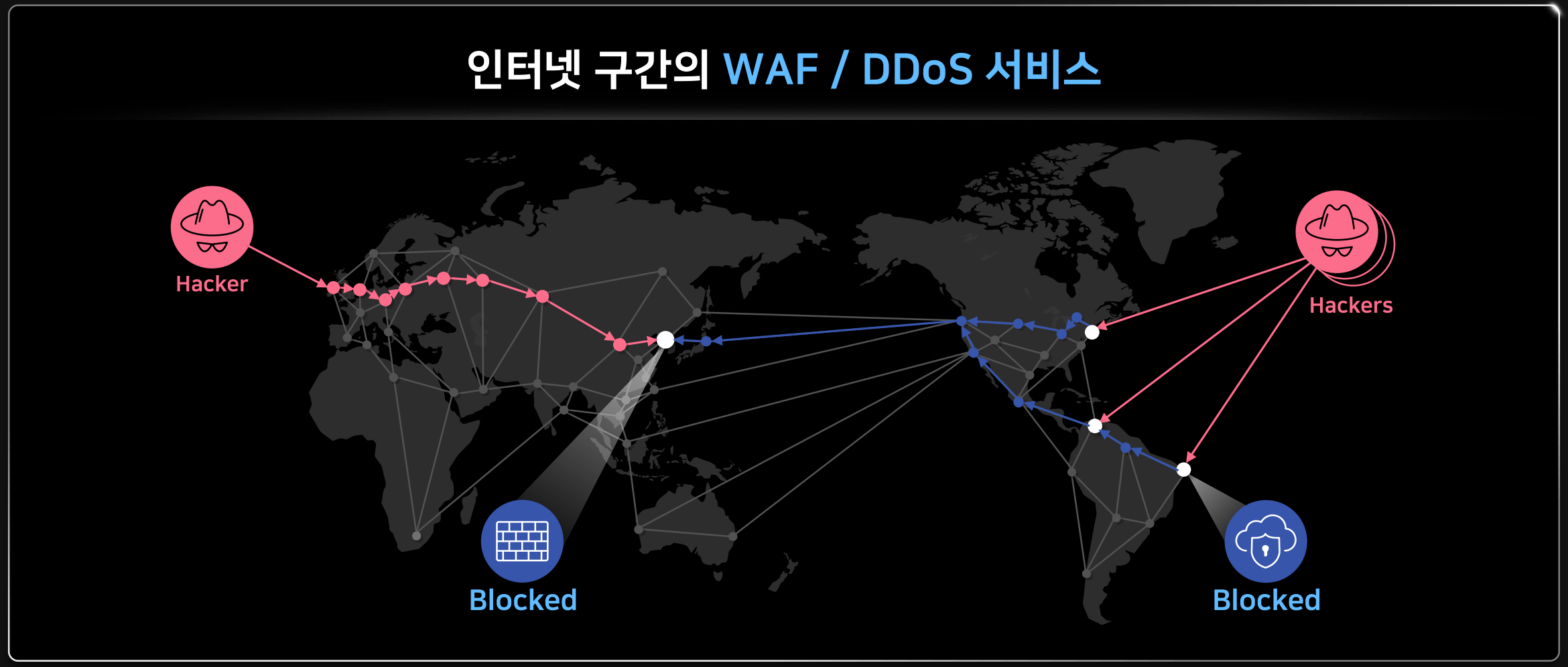
CSP Native vs 3rd Party 기능 비교의 예시 - NW 보안

		범위		기능					비용	Scaling
3rd Party	Marketplace	L7	L3/4	Allow	Deny	Alert	Count	Block	유료 (고정비)	수동 (사용자 정의)
CSP Native	AWS WAF	L7	L3/4	Allow	Deny	Alert	Count	Block	유료 (종량제)	자동
	AWS Network Firewall	L7	L3/4	Allow	Deny	Alert	Count	Block	유료 (종량제)	자동
	Security Group	L7	L3/4	Allow	Deny	Alert	Count	Block	무료	자동
	Network ACL	L7	L3/4	Allow	Deny	Alert	Count	Block	무료	자동

2. 보안의 클라우드 전환

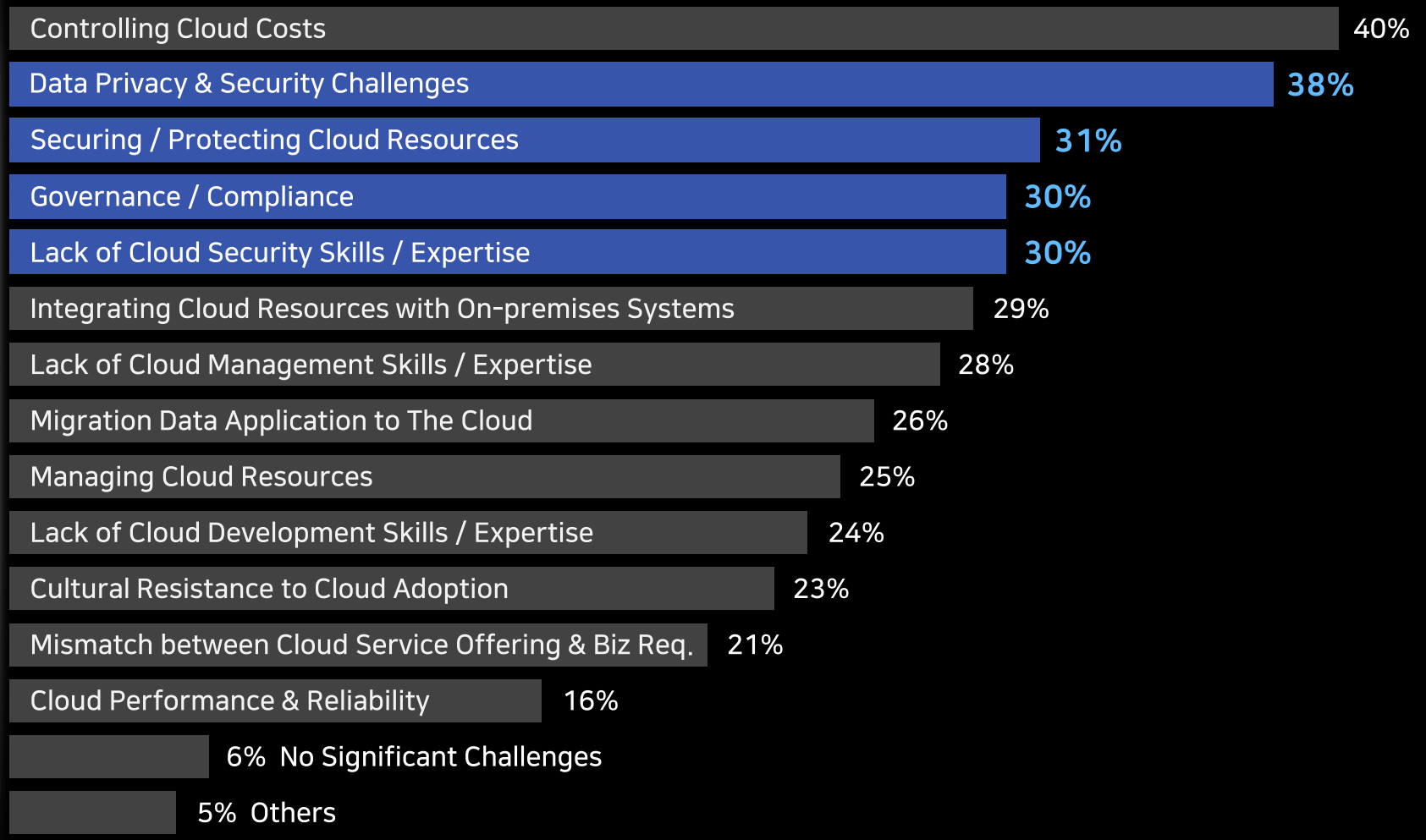


2. 보안의 클라우드 전환



클라우드 보안 위협

사용자 데이터 보호
클라우드 자원에 대한 보호
보안 거버넌스 및 컴플라이언스
클라우드 보안 역량 및 전문성 부재



※ Statista, 2020

삼성SDS의 클라우드 보안

삼성SDS는 국내 최초로 클라우드 보안 서비스를 개시한 이후
AWS Security Competency 획득, IDC Marketscape 등재를 통해 클라우드 보안 역량을 입증하고 있습니다.

2015

국내 최초
클라우드 보안 서비스 상용화

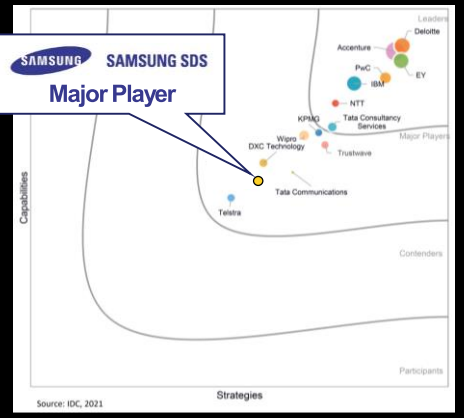
Amazon AWS
Microsoft Azure
Google Cloud Platform
Alibaba Cloud
ORACLE CLOUD
IBM Cloud

2018

국내 최초
AWS Security Competency 획득
- 전 분야 종합 최초 -

2021

국내 최초
IDC Marketscape, APAC 등재
- Cloud Security Services 분야 -



2022

국내 최초
IDC Marketscape, Worldwide 등재
- Managed Cloud Security Services 분야 -

IDC
Analyze the Future

클라우드의 시작과 끝,
클라우드 보안

Thank you

SAMSUNG SDS