More security,
More freedom

클라우드 환경에서의 효과적인 보안 전략

안랩

AhnLab

목차

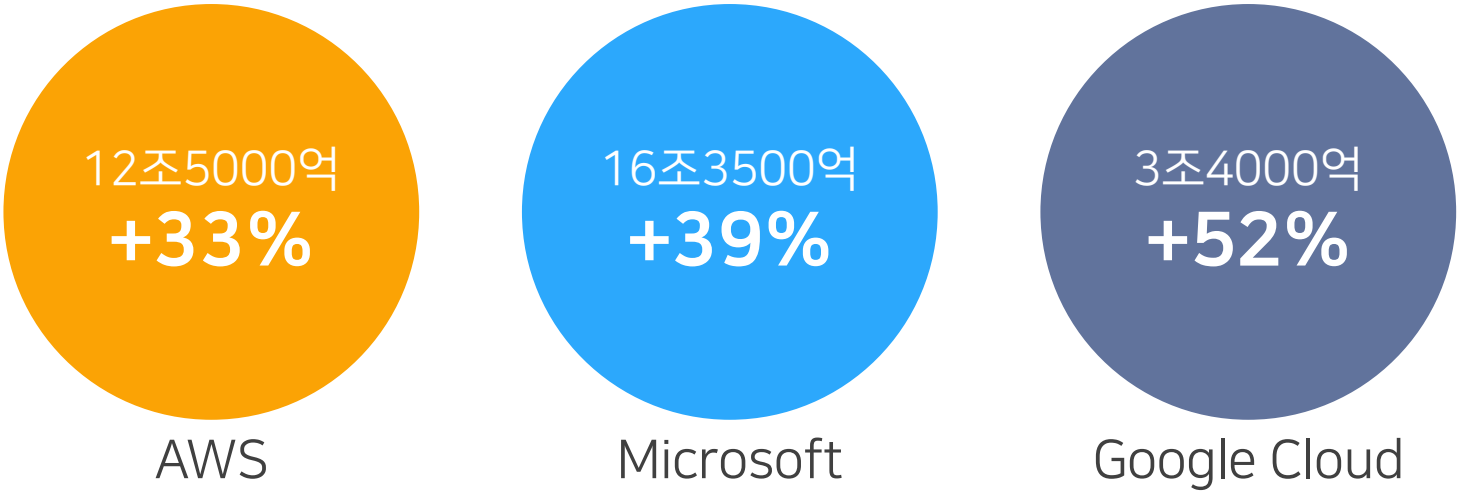
AhnLab

코로나 19 팬데믹

재택근무, 원격근무 등의 온라인 기반 다양한 비대면 활동이 빠르게 확산
클라우드 시장 성장의 촉매제로 적용

2020. 1분기 전세계 클라우드 시장

전년대비 37% 증가



국내 퍼블릭 클라우드 시장

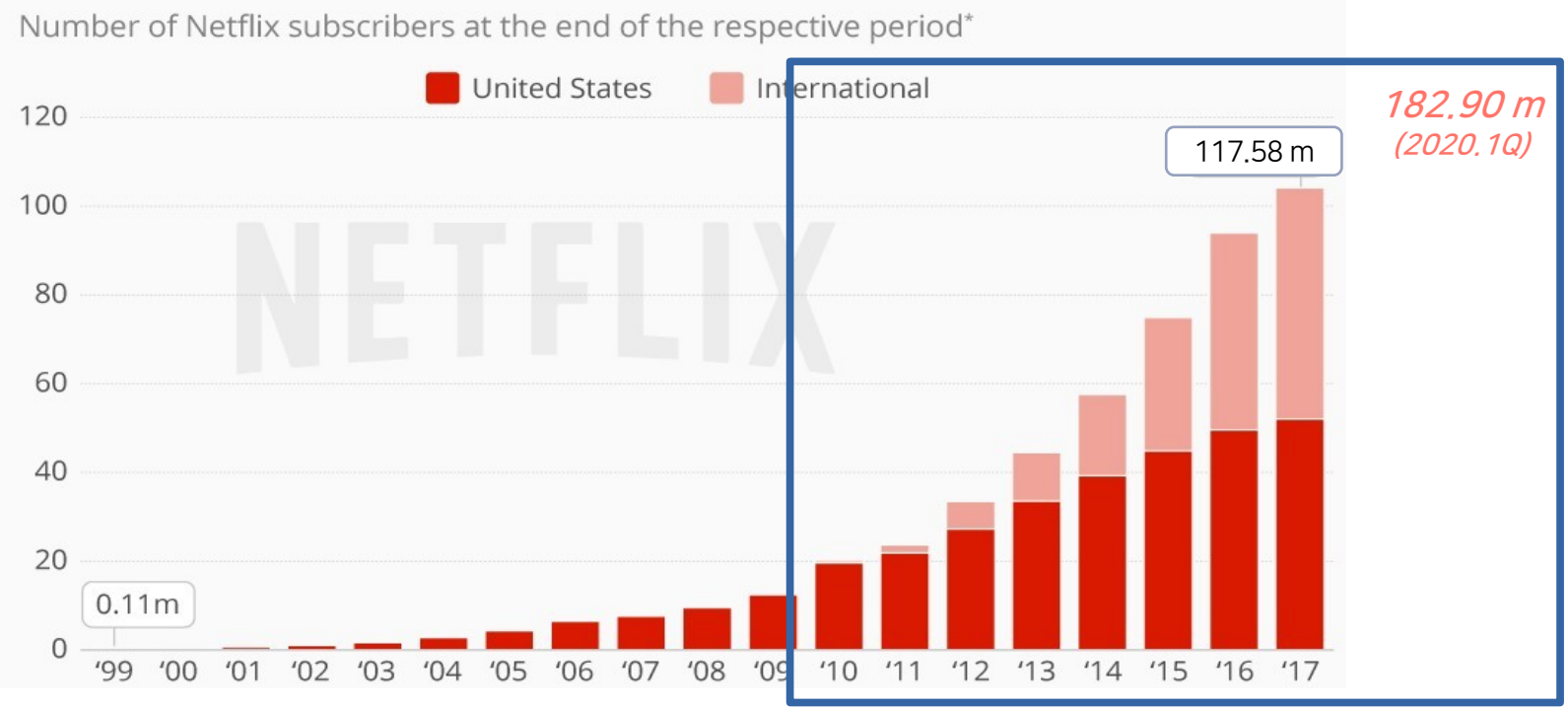
15.9%

2조 9천억(2020)

클라우드 전환 - 이유

클라우드 전환 - 사례

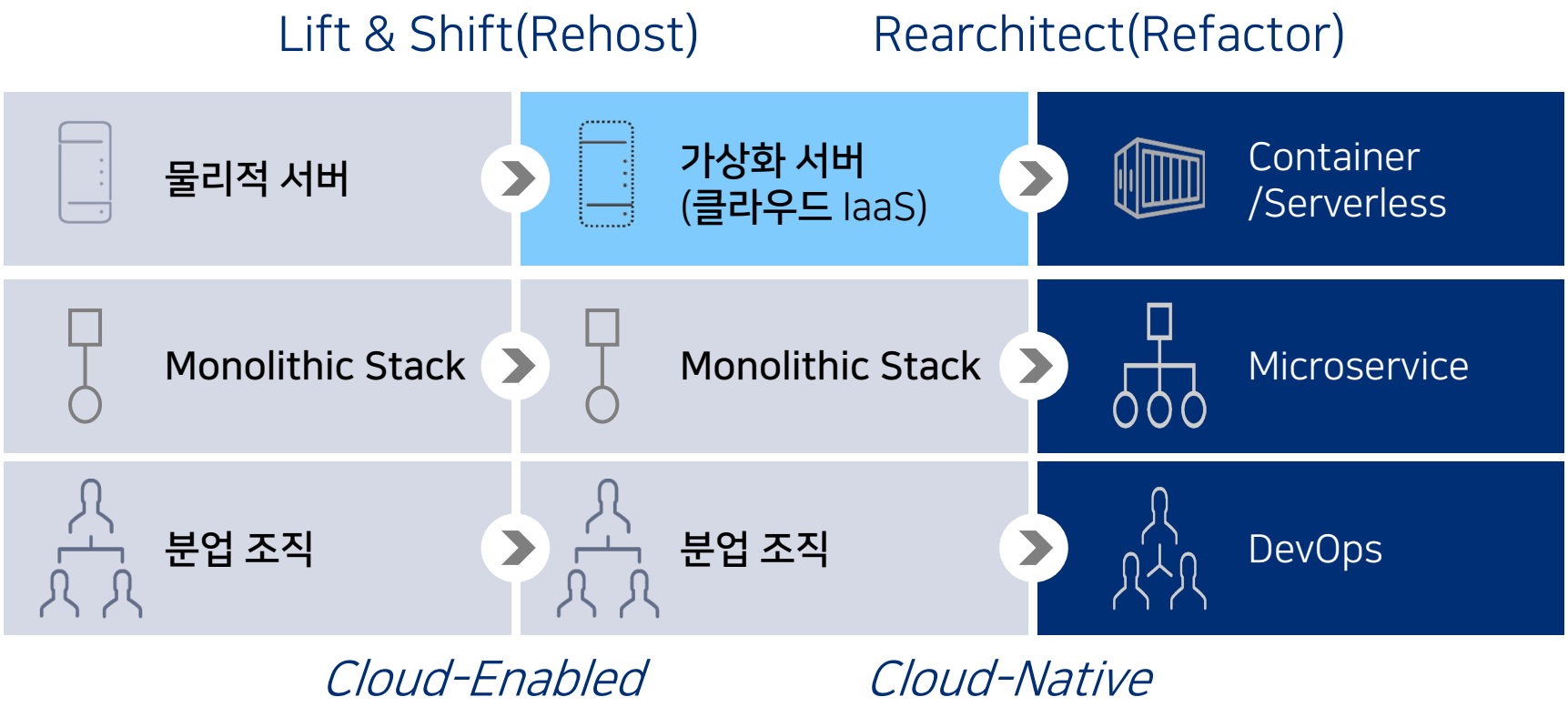
Netflix everywhere



클라우드 전환 – 방법

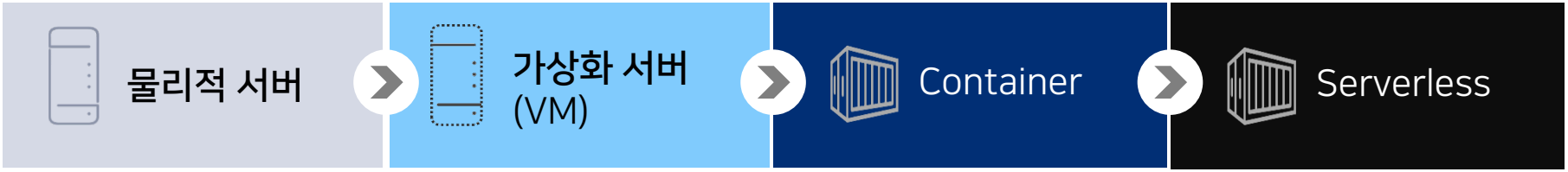
데이터, 애플리케이션 또는 기타 비즈니스 요소를 클라우드 컴퓨팅 환경 으로 이동하는 프로세스

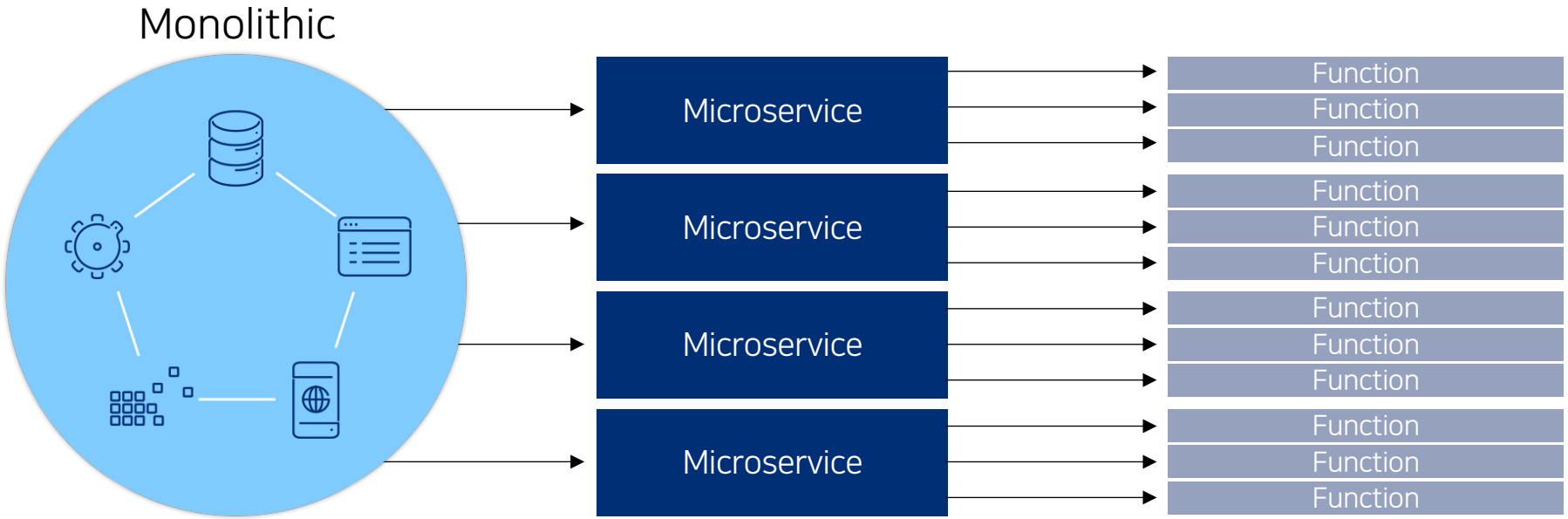
클라우드 마이그레이션 모델



클라우드 환경 – 워크로드 변화

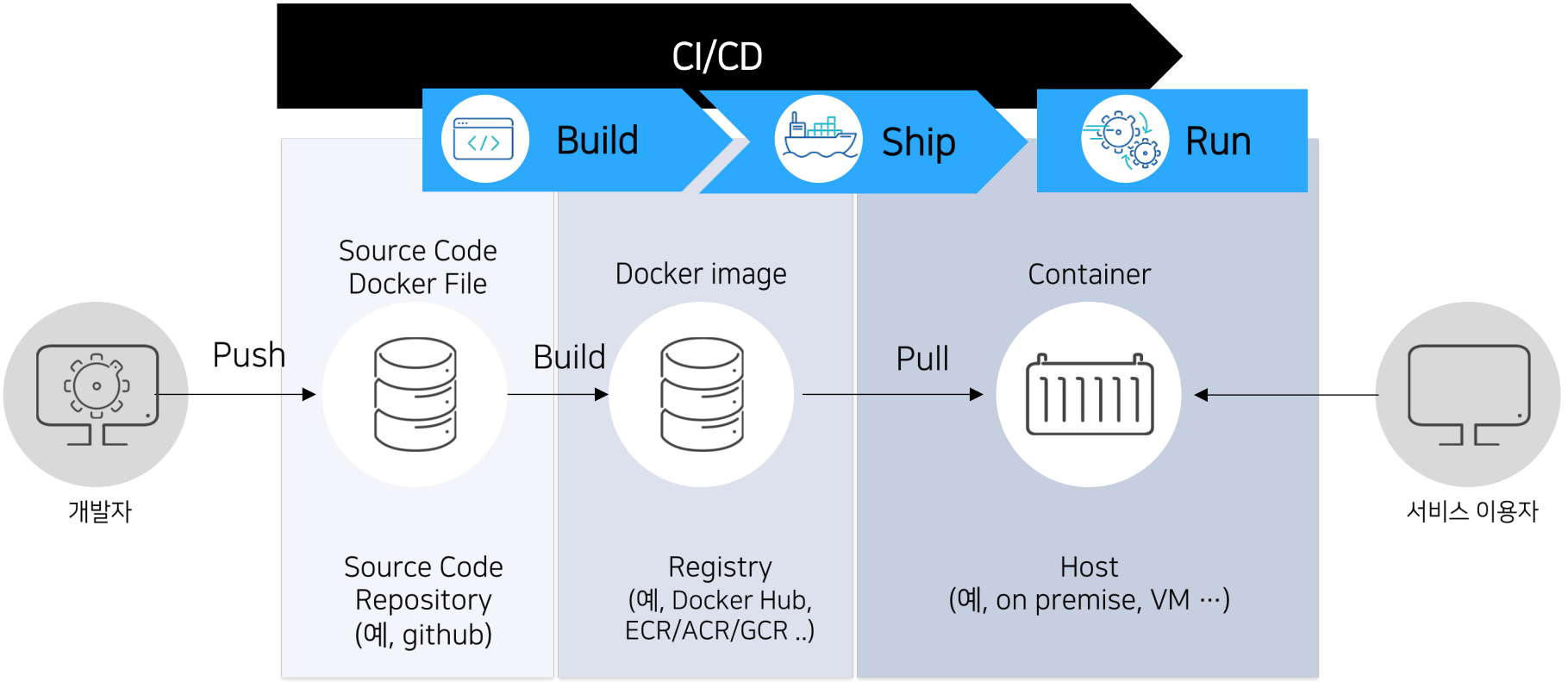
워크로드 유형 변화





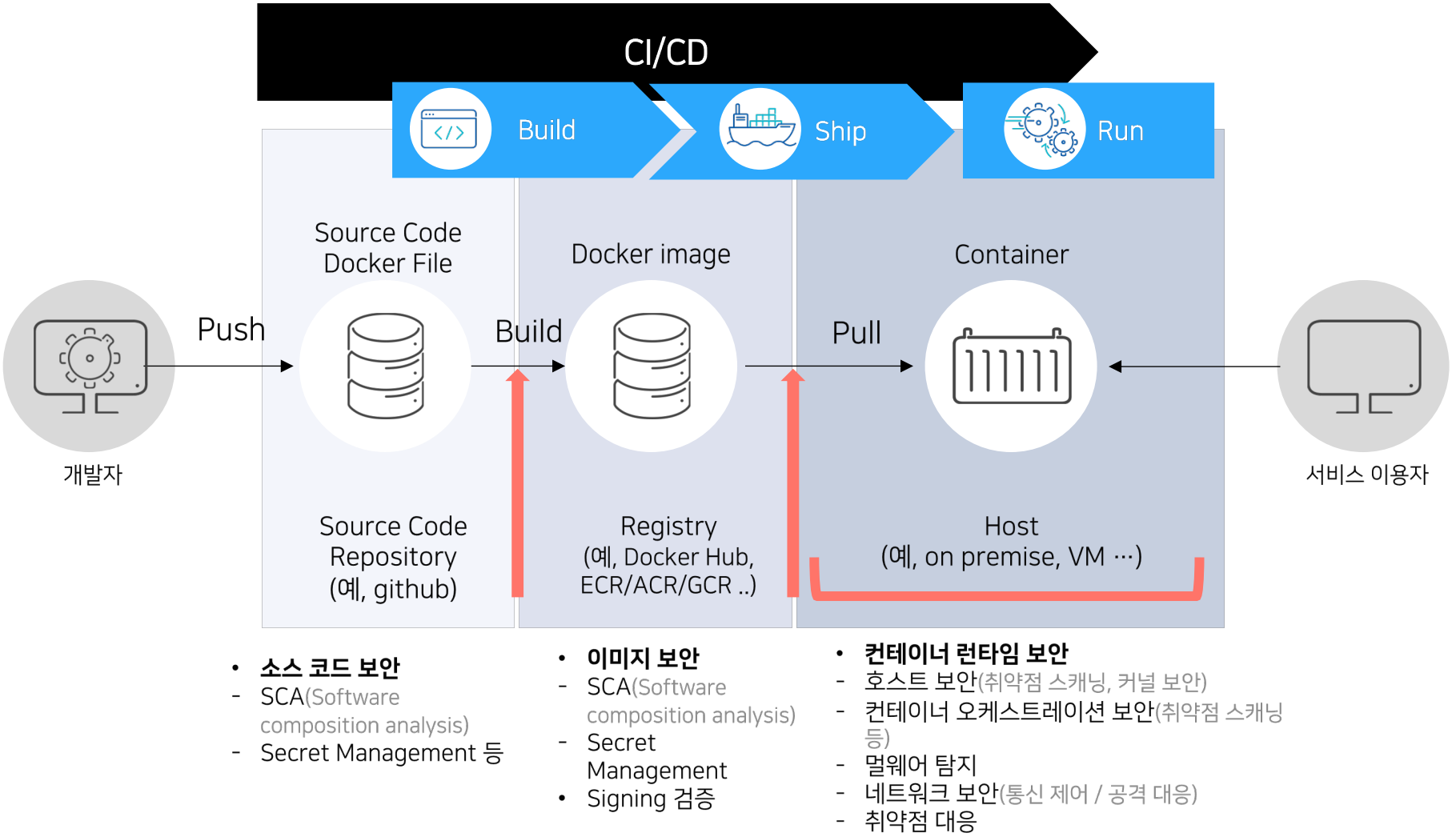
클라우드 환경 – 컨테이너 운영

Container



클라우드 환경에서의 보안

Container



- **소스 코드 보안**
  - SCA(Software composition analysis)
  - Secret Management 등

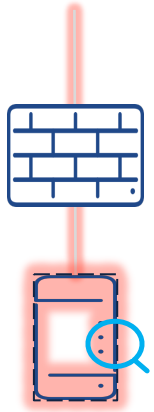
- **이미지 보안**
  - SCA(Software composition analysis)
  - Secret Management
- Signing 검증

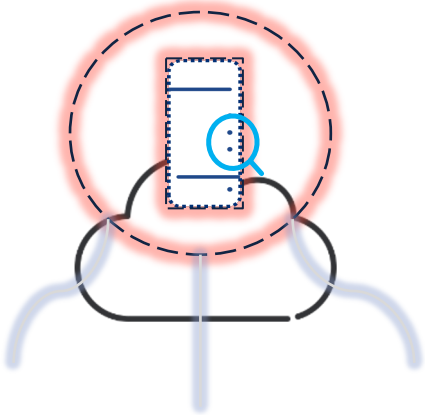
- **컨테이너 런타임 보안**
  - 호스트 보안(취약점 스캐닝, 커널 보안)
  - 컨테이너 오케스트레이션 보안(취약점 스캐닝 등)
  - 멀웨어 탐지
  - 네트워크 보안(통신 제어 / 공격 대응)
  - 취약점 대응

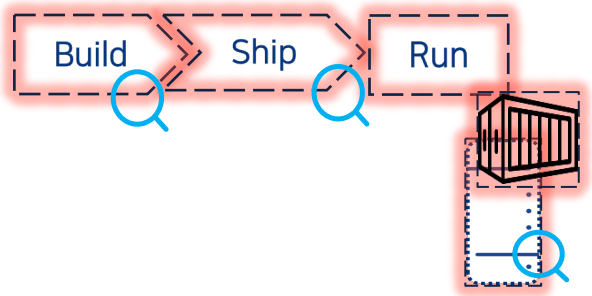
클라우드 환경에서의 보안

워크로드 유형별 보안

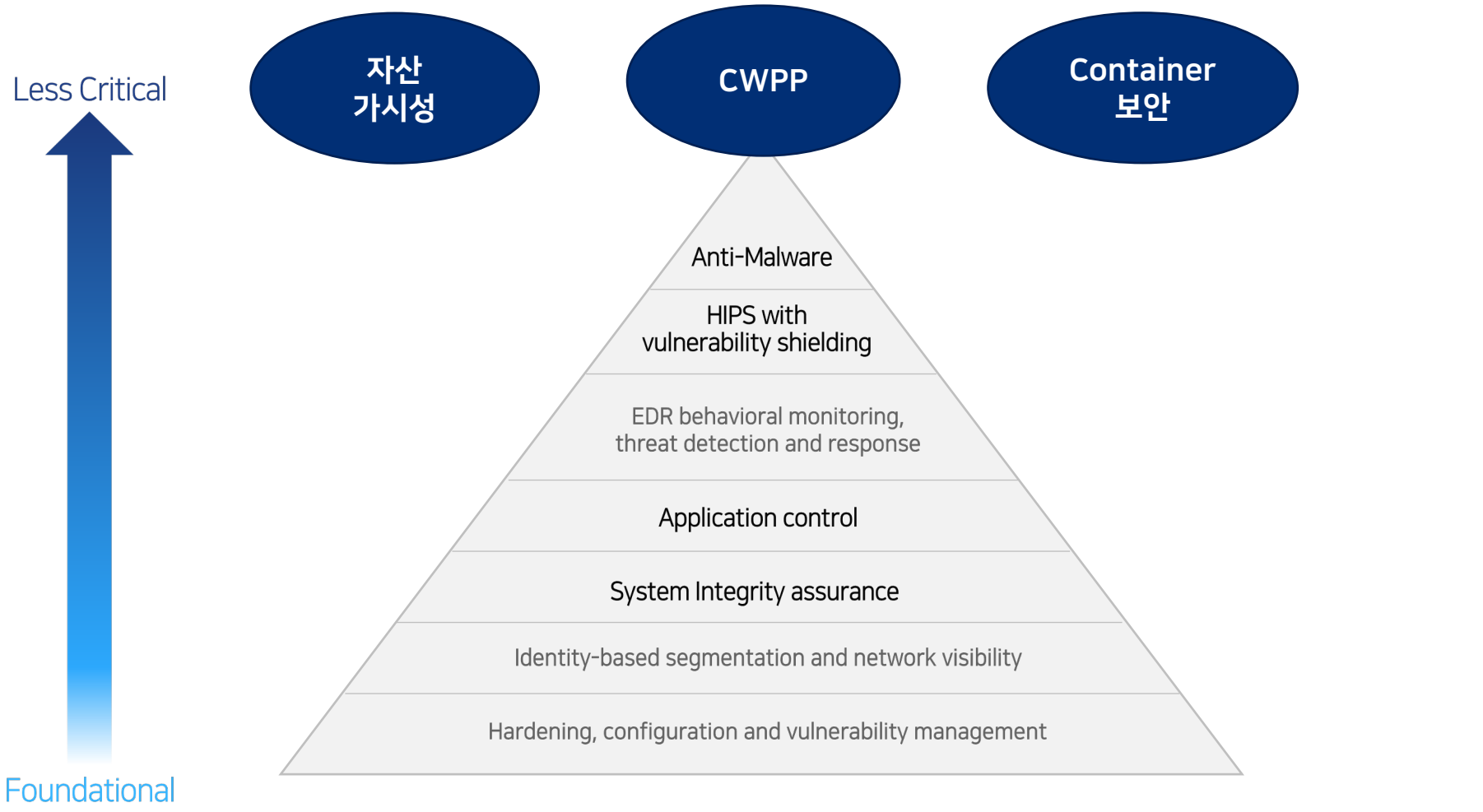
물리적 서버	가상화 서버 (VM)	Container
경계 보안 단말 보안 데이터 보안	CSPM / CASB CWPP 데이터 보안	CI/CD 보안 CWPP







클라우드 환경에서의 보안



Gartner 'Market Guide for Cloud Workload Protection Platforms 2019

AhnLab CPP

Application Control

화이트리스트 기반 어플리케이션 실 제어

- 워크로드 용도에 맞는 어플리케이션만 실행 허용
- 중요 파일로의 접근 제어로, 서비스 안정성 보장

Host IPS & Firewall

네트워크 공격 탐지/방지

- 시그니처 기반 네트워크 침입 공격 탐지 및 차단
- 시그니처 추천 지원
- IP, Port , 프로토콜 기반 통신 제어
- 국가 차단(IP 기반) 지원

Anti-malware

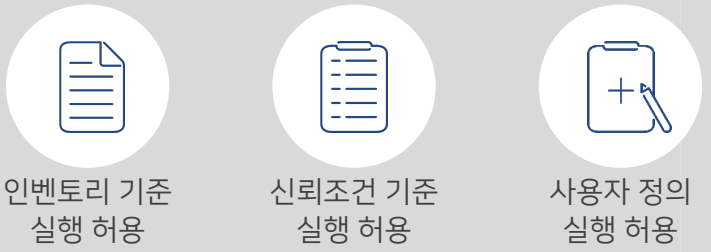
악성코드 탐지/대응

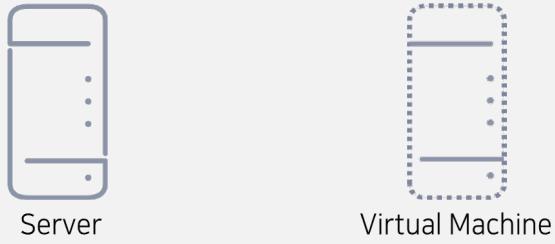
- 수동/예약 검사
- 실시간 검사
- 검사 성능/리소스 이슈 최소화

AhnLab CPP

Application 실행 제어

- 화이트리스트 기반 어플리케이션 실행 제어
- 신뢰 조건 기반 어플리케이션 실행 제어
- 사용자 정의 기반 어플리케이션 실행 제어
- 중요 파일 및 폴더의 접근 제어
- 다양한 운영 모드 지원(Lockdown/ simulation / Maintenance 모드)





AhnLab CPP

네트워크 침입 공격 방어

- 서버, VM, 컨테이너에 대한 네트워크 침입 공격을 탐지, 차단
- 기본 시그니처 지원 및 주기적 업데이트 지원
- 사용자 정의 시그니처 지원(Snort, PCRE 패턴 지원)
- 시그니처 추천 및 자동 적용 지원
- 서버 가용성을 고려하여 탐지 모드, 바이패스 모드 지원

AhnLab CPP

Firewall

- 호스트로 인/아웃되는 트래픽을 모니터링
- IP/Port/프로토콜 기반의 트래픽 허용/차단 지원
- 국가 IP 기반 인/아웃바운드 통신 차단/허용 지원
- 서버 가용성을 고려하여 탐지 모드, 바이패스 모드 지원

AhnLab CPP

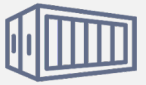
Anti-malware

- 서버, VM, 컨테이너 파일에 대한 악성코드 탐지 및 치료 지원
- 수동, 예약 검사 지원
- Windows server 와 다양한 Linux 서버에서의 실시간 검사 지원
- 검사 예외 설정 지원
- CPU 점유율 설정 지원으로, 과도한 리소스 사용 방지

악성코드 탐지 및 치료

Server

Virtual Machine



Container

AhnLab CPP

안전한 보안 환경 구축

- 온프레미스와 클라우드 서버에 대한 통합 관리 및 일원화된 보안 관리 지원
- 기업 내 서버에서 발생하는 보안 위협에 대한 통합된 가시성 확보
- 다양한 대시 보드 및 제품간 연계 규칙을 통해 보다 빠른 대응 지원
- SIEM, 통합 로그 분석 시스템 연동을 통한 보안 관제 효과 증대

업무 연속성 확보

- 시스템 안정적인 운영 지원으로 업무 연속성 및 생산성에 기여
- 불필요한 통신, 애플리케이션에 대한 차단으로 잠재적인 위협 요소 사전 제거
- 다양한 모드와 함께 예외처리 지원으로 시스템 운영에 최적화된 정책 설정 지원

관리비용 절감

- 플랫폼 기반에서 보안 솔루션 통합 운영으로 업무 부담 최소화 및 연계 규칙을 통한 도입 효과 극대화
- 서비스 특성에 맞춘 선별적 보안 적용으로 솔루션 도입 비용 절감 효과

More security, More freedom

AhnLab