

# 클라우드 네이티브 애플리케이션의 취약점과 대응 방안

## 1. CNAPP 개요

CNAPP(Cloud-Native Application Protection Platform)는 클라우드 환경에서 운영되는 애플리케이션의 보안 취약점 탐지, 대응, 규정 준수 관리를 통합적으로 수행하는 플랫폼이다. Gartner가 2021년 처음 제안한 개념으로, CSPM(Cloud Security Posture Management), CWPP(Cloud Workload Protection Platform), CIEM(Cloud Infrastructure Entitlement Management) 등 다양한 보안 기능을 하나의 플랫폼에서 제공한다.

CNAPP는 다음과 같은 특징을 가진다:

- DevSecOps 통합: 개발 초기 단계부터 보안을 적용하는 ‘시프트 레프트’ 전략
- 멀티클라우드 지원: 다양한 클라우드 환경에서 일관된 보안 정책 적용
- 자동화된 위협 탐지 및 대응: 머신러닝 기반 이상행위 탐지
- 규정 준수 및 권한 관리: 최소 권한 원칙과 지속적인 컴플라이언스 모니터링

## 2. 클라우드 네이티브 애플리케이션의 주요 취약점

클라우드 네이티브 애플리케이션은 컨테이너, 쿠버네티스, 마이크로서비스 아키텍처 등으로 구성되어 있으며, 다음과 같은 보안 취약점을 내포하고 있다:

### 1. 쿠버네티스(Kubernetes) 취약점

- API 서버 접근 통제 미흡
- RBAC 설정 부재
- etcd 데이터스토어 노출
- CVE-2024-10220, CVE-2024-7646 등 최근 취약점 사례

### 2. 마이크로서비스 아키텍처 취약점

- 서비스 간 트래픽 암호화 미적용
- 디버그 포트 노출
- 잘못된 네트워크 접근 정책

### 3. CI/CD 및 공급망 취약점

- 악성 오픈소스 라이브러리 사용
- CI/CD 도구의 보안 패치 미적용
- 개발자의 인증 정보 노출

## 3. 클라우드 네이티브 애플리케이션 대응 방안

CNAPP는 위와 같은 취약점에 대응하기 위해 다음과 같은 전략을 제공한다:

### 1. 제로 트러스트 보안 모델

- 모든 사용자와 시스템을 기본적으로 신뢰하지 않음
  - MFA, 최소 권한 원칙, 마이크로세그멘테이션 적용
2. DevSecOps 및 자동화
    - 코드 정적 분석, 취약점 스캐닝, 이미지 검증을 CI/CD에 통합
    - 보안 점검을 배포 전에 자동화
  3. AI 기반 위협 탐지
    - 머신러닝을 활용한 이상행위 탐지 및 자동 대응
  4. 멀티클라우드 보안 강화
    - IAM 연동, 클라우드 간 모니터링 자동화
    - 통합된 보안 정책 수립

#### 4. CNAPP에 대한 종합적인 고찰

CNAPP는 단순한 보안 도구의 집합이 아니라 클라우드 보안의 패러다임 전환을 의미한다. 기존의 사후 대응 중심 보안 모델에서 벗어나, 개발 초기부터 보안을 내재화하는 DevSecOps 전략은 매우 현실적이고 효과적이다.

특히 클라우드 환경의 복잡성과 빠른 변화 속도는 보안팀과 개발팀 간의 협업을 필수로 만든다. CNAPP는 이 간극을 메우는 협업 플랫폼으로서의 역할도 수행한다는 점에서 매우 의미적이다.

다만 CNAPP의 도입은 단순히 기술적 구현만으로는 부족하다. 조직 내 보안 문화의 변화, 개발자와 보안 담당자의 지속적인 교육, 그리고 자동화된 도구에 대한 신뢰 구축이 병행되어야 한다.

즉, CNAPP는 클라우드 네이티브 환경에서의 보안 취약점을 효과적으로 대응할 수 있는 플랫폼이다. 기술적 도입뿐 아니라 조직 문화와 협업 구조의 변화까지 고려한 전략적 접근이 필요하다.