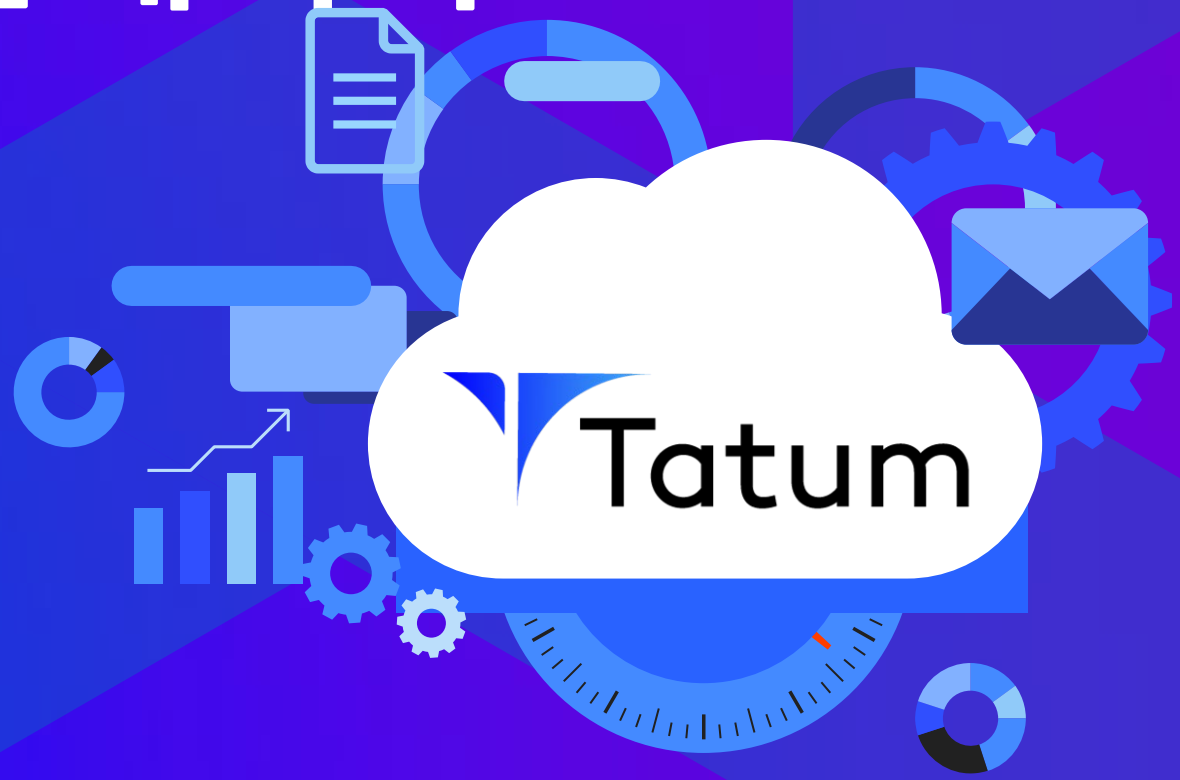
CISO를 위한
클라우드 보안 플레이북

클라우드 보안? 중요한
'권한 관리'부터 시작하라~



테이텀시큐리티
양혁재 대표

TATUM SECURITY

Table of Contents

TATUM SECURITY

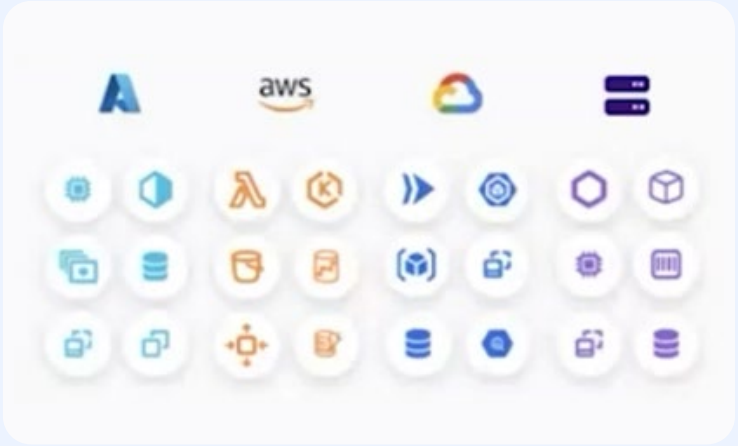
클라우드 보안의 현 주소

시작부터 지금까지

클라우드 보안에 아직 명확한 답은 없다

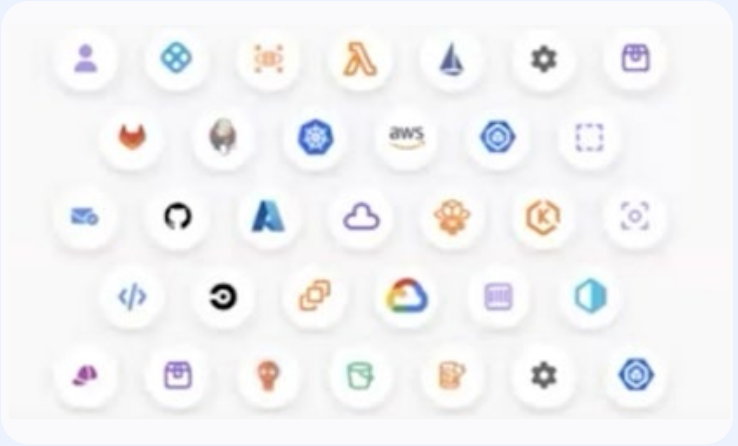
The new cloud operating model requires a new approach to security

Self-service infrastructure



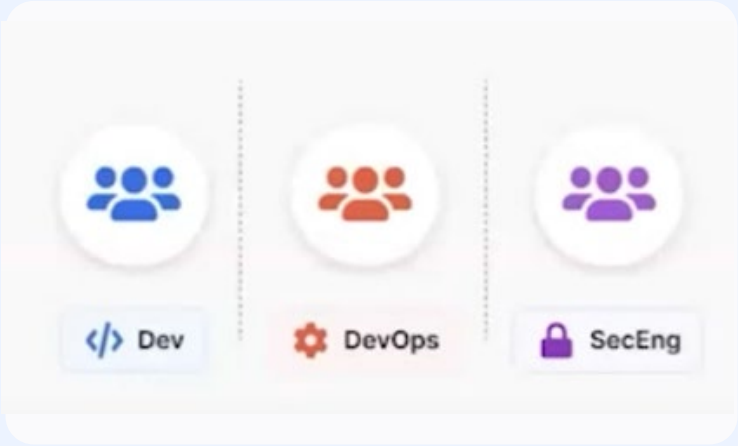
모든 팀은 리소스를 가동하고
특정 요구 사항에 따라
다양한 기술을 요구

Heterogeneous Environments



애플리케이션과 서비스는 클래식 서버부터
컨테이너, 서버리스, 엣지 컴퓨팅, 관리형
PaaS에 이르기까지 다양한 플랫폼에 배포

Security spans across multiple teams



팀은 사일로화되어 있으며서로
다른 우선 순위를 가짐

클라우드 보안은 어디에서 시작되었는가?

Biden cyber executive or[illegible] reignites push to cloud, zero trust

The Biden administration issued a long-awaited cybersecurity executive order Wednesday that, among other things, requires federal agencies to develop an implementation plan for a zero-trust architecture for security.

BY BILLY MITCHELL • MAY 12, 2021

2015 년 시작된 클라우드 보안

2021년 바이든 행정명령으로 본격화

제로트러스트, 클라우드 규제와

가이드 강제

클라우드 보안은 어디에서 시작되었는가?

바이든 행정명령
미국사이버보안국(CISA)
클라우드 보안에 대한
표준문서를 제정

Cloud Security Technical Reference Architecture

Coauthored by:

Cybersecurity and Infrastructure Security Agency,
United States Digital Service, and
Federal Risk and Authorization Management Program

June 2022
Version 2.0

Table of Contents

CSPM(Cloud Security Posture Management) 클라우드 서비스에 대한 정의부터 어떻게 이전해야되는가에 대한 표준을 제시

클라우드 보안은 어디에서 시작되었는가?

정부 기준 용어는 CSPM 시장에서는
CSPM에 CNAPP 영역을 포함

In this document, CSPM capabilities seek to support the following activity outcomes:

- Governance and Compliance,
- Standards and Policies,
- Privilege and Identity Access Management,
- Data Protections,
- Infrastructure and Application Protections,
- System Health and Resource Monitoring, and
- Incident Response and Recovery.

These capabilities include:

- Security and Risk Assessments,
- Continuous Monitoring and Alerting,
- Identity, Credential, and Access Management (ICAM),
- DevSecOps Integration, and
- Artificial Intelligence (AI)- and Machine Learning (ML)-Based Security Capabilities.

CSPM(Cloud Security Posture Management) 클라우드 서비스에 대한 정의부터 어떻게 이전해야되는가에 대한 표준을 제시

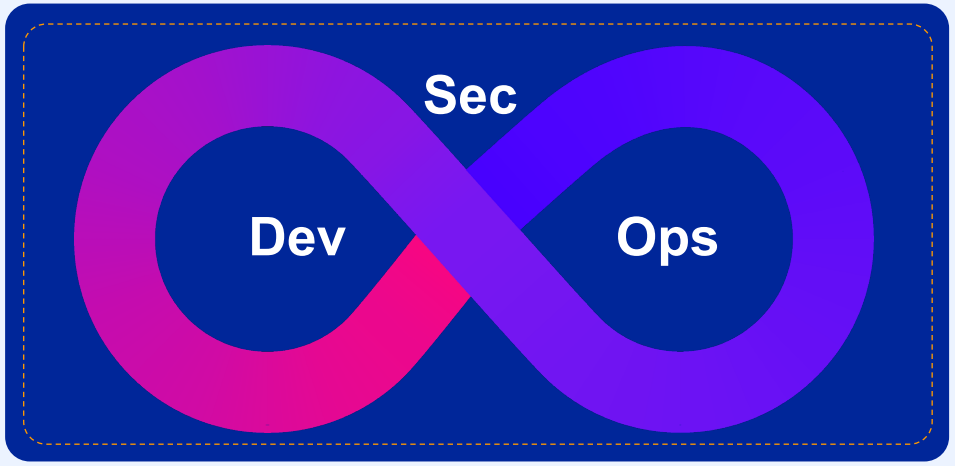
CNAPP(Cloud Native Application Protection Platform)

TATUM SECURITY

TATUM CNAPP Detailed View

Artifact Scanning

- Traditional SAST/DAST
- API Scanning
- Software Composition Analysis
- Development Pipeline Security Posture
- Exposure Scanning
  - CVEs
  - Secrets
  - Sensitive Data
    - Malware
    - Unknown Vulnerabilities
    - Attack Path Analysis



Cloud Configuration

- Infrastructure as Code Scanning
- Network Configuration and Security Policy
- Cloud Infrastructure Entitlements Management
- Cloud Security Posture Management
- Kubernetes Security Posture Management
- Data Security Posture Management

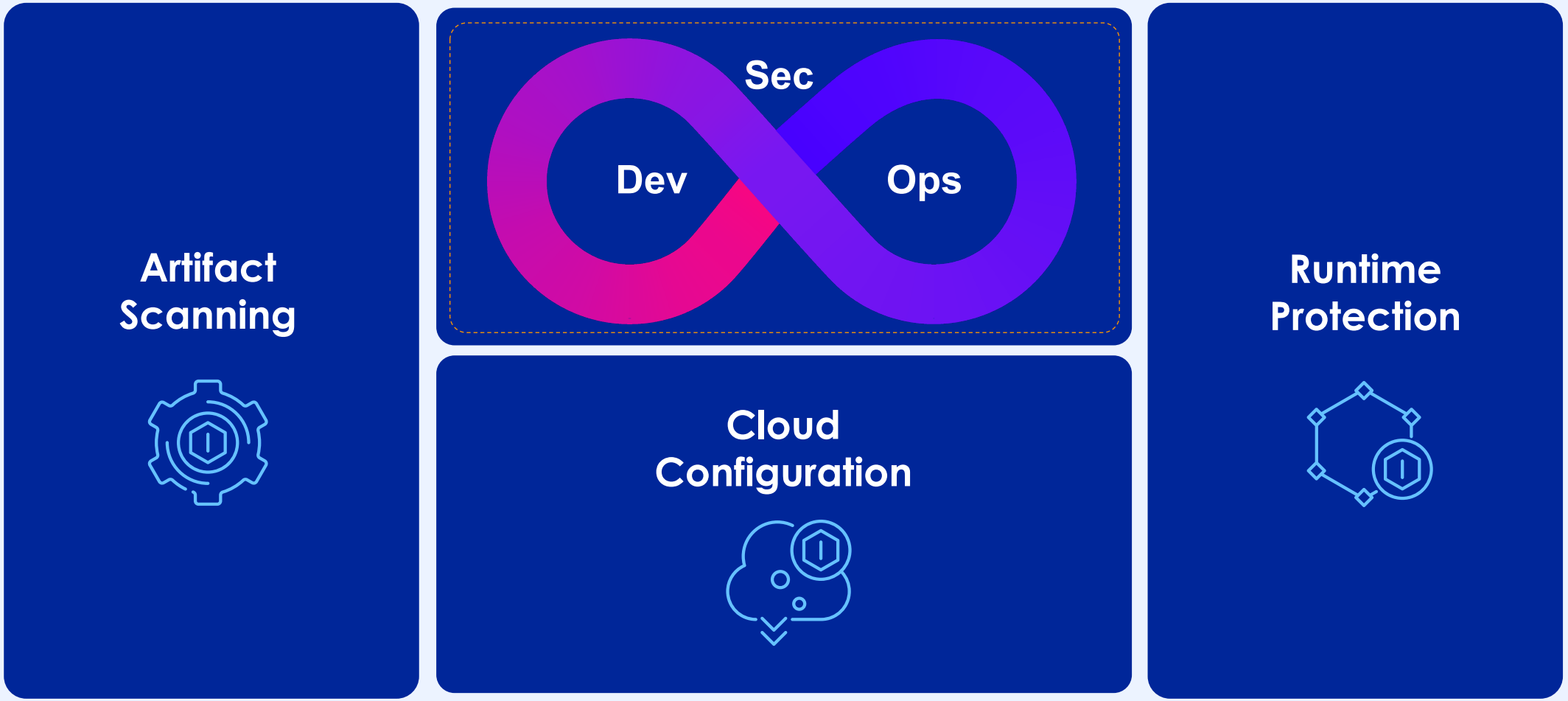
Runtime Protection

- Web Application and API Protection
- Application Monitoring Observability
- Cloud Workload Visibility Protection Platform
- Network Observability Exposure Scanning
  - CVEs
  - Secrets
  - Sensitive Data
  - Malware
  - Unknown Vulnerabilities
  - Attack Path Analysis

Cloud Detection And Response

Development Pipeline Detection and Response

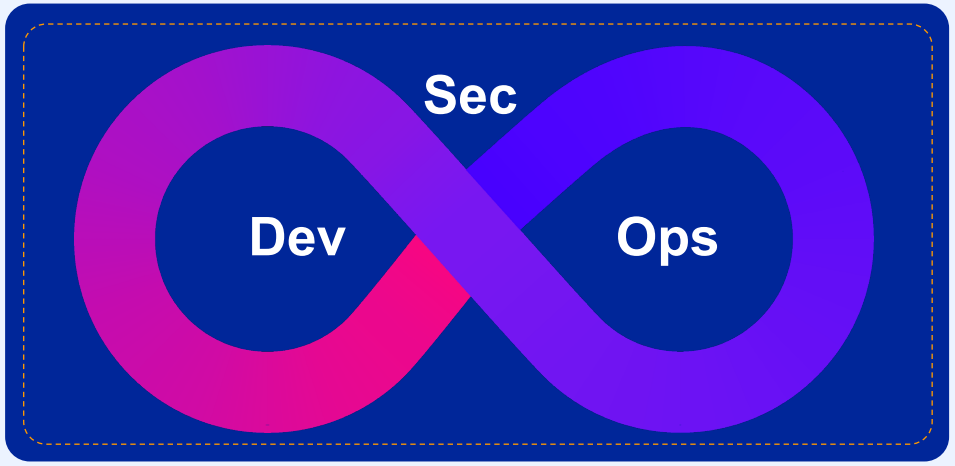
TATUM CNAPP Detailed View



Artifact Scanning

Artifact Scanning

- Traditional SAST/DAST
- API Scanning
- Software Composition Analysis
- Development Pipeline Security Posture
- Exposure Scanning
  - CVEs
  - Secrets
  - Sensitive Data
    - Malware
    - Unknown Vulnerabilities
    - Attack Path Analysis



Cloud Configuration

Runtime Protection

Cloud Detection And Response

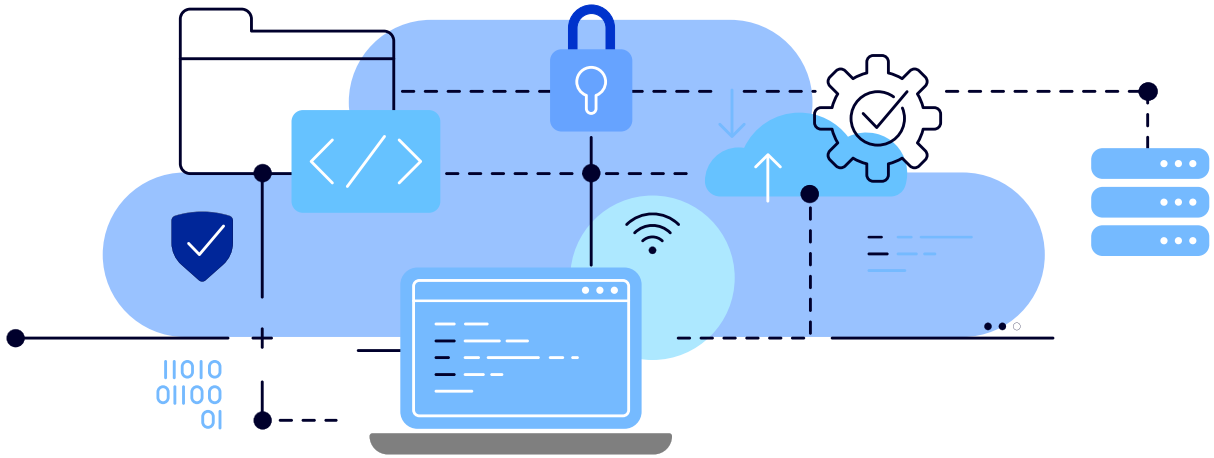
Development Pipeline Detection and Response

Artifact Scanning

Artifact Scanning

- Traditional SAST/DAST
- API Scanning
- Software Composition Analysis
- Development Pipeline Security Posture
- Exposure Scanning
  - CVEs
  - Secrets
  - Sensitive Data
    - Malware
    - Unknown Vulnerabilities
    - Attack Path Analysis

사실은, 우리가 이미 대부분 하고 있는 영역



소프트웨어 구성 분석
-SBOM
-SCA

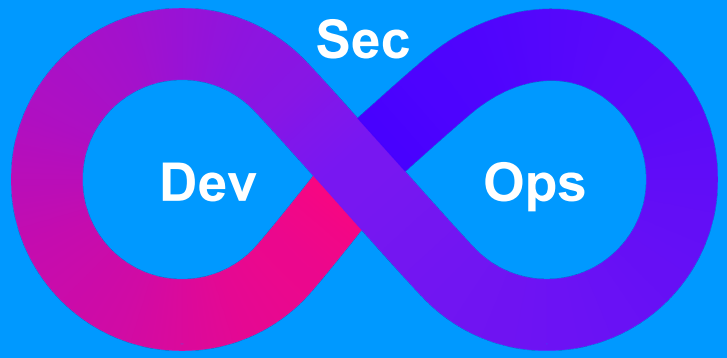
애플리케이션 보안 테스트
-SAST
-DAST

CNAPP(Cloud Native Application Protection Platform)

TATUM SECURITY

Cloud Configuration

Artifact Scanning



Cloud Configuration

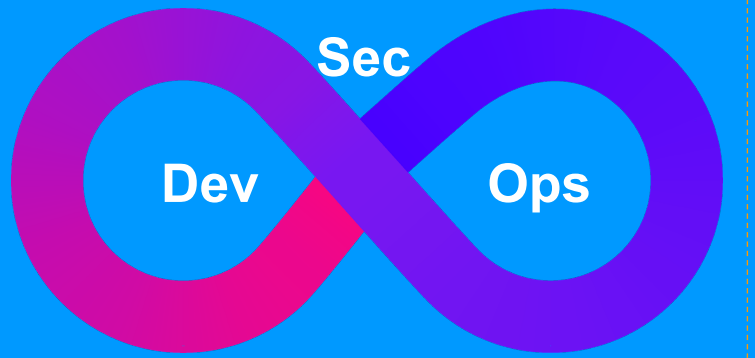
- Infrastructure as Code Scanning
- Network Configuration and Security Policy
- Cloud Infrastructure Entitlements Management
- Cloud Security Posture Management
- Kubernetes Security Posture Management
- Data Security Posture Management

Runtime Protection

Cloud Detection And Response

Development Pipeline Detection and Response

Cloud Configuration



Cloud Configuration

- Infrastructure as Code Scanning
- Network Configuration and Security Policy
- Cloud Infrastructure Entitlements Management
- Cloud Security Posture Management
- Kubernetes Security Posture Management
- Data Security Posture Management

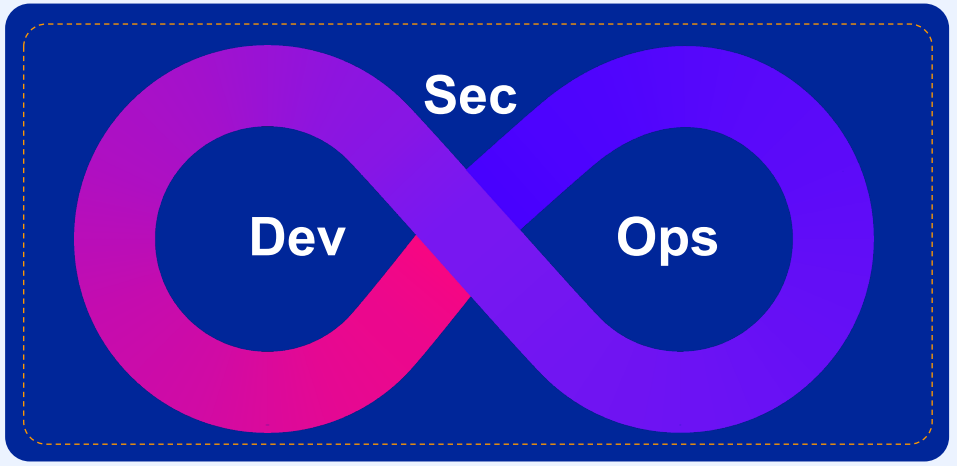
완전한 Cloud Native 영역

CNAPP(Cloud Native Application Protection Platform)

TATUM SECURITY

Runtime Protection

Artifact Scanning



Cloud Configuration

Runtime Protection

- Web Application and API Protection
- Application Monitoring Observability
- Cloud Workload Visibility Protection Platform
- Network Observability Exposure Scanning
  - CVEs
  - Secrets
  - Sensitive Data
  - Malware
  - Unknown Vulnerabilities
  - Attack Path Analysis

Cloud Detection And Response

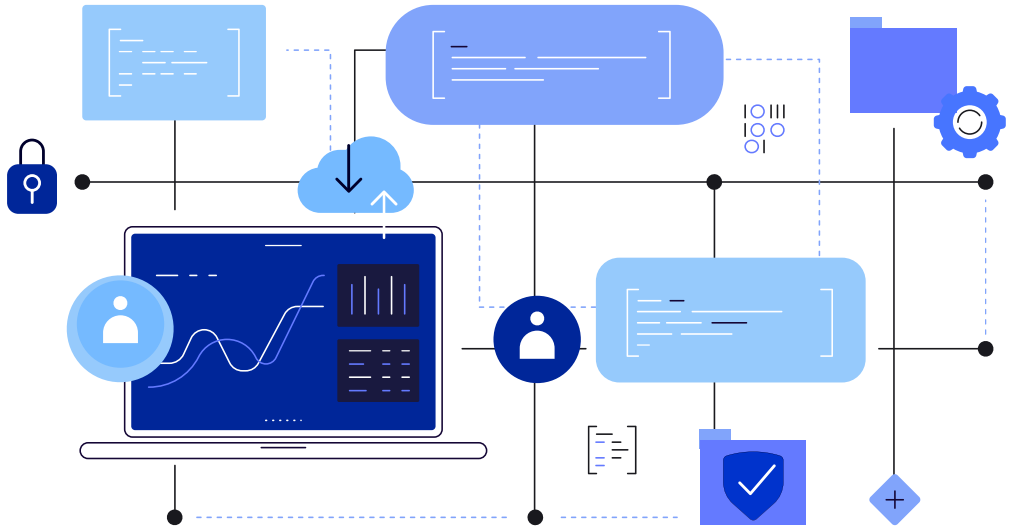
Development Pipeline Detection and Response

Runtime Protection

Runtime Protection

- Web Application and API Protection
- Application Monitoring Observability
- Cloud Workload Visibility Protection Platform
- Network Observability Exposure Scanning
  - CVEs
  - Secrets
  - Sensitive Data
  - Malware
  - Unknown Vulnerabilities
  - Attack Path Analysis

Endpoint 영역과 겹침



런타임 프로텍션

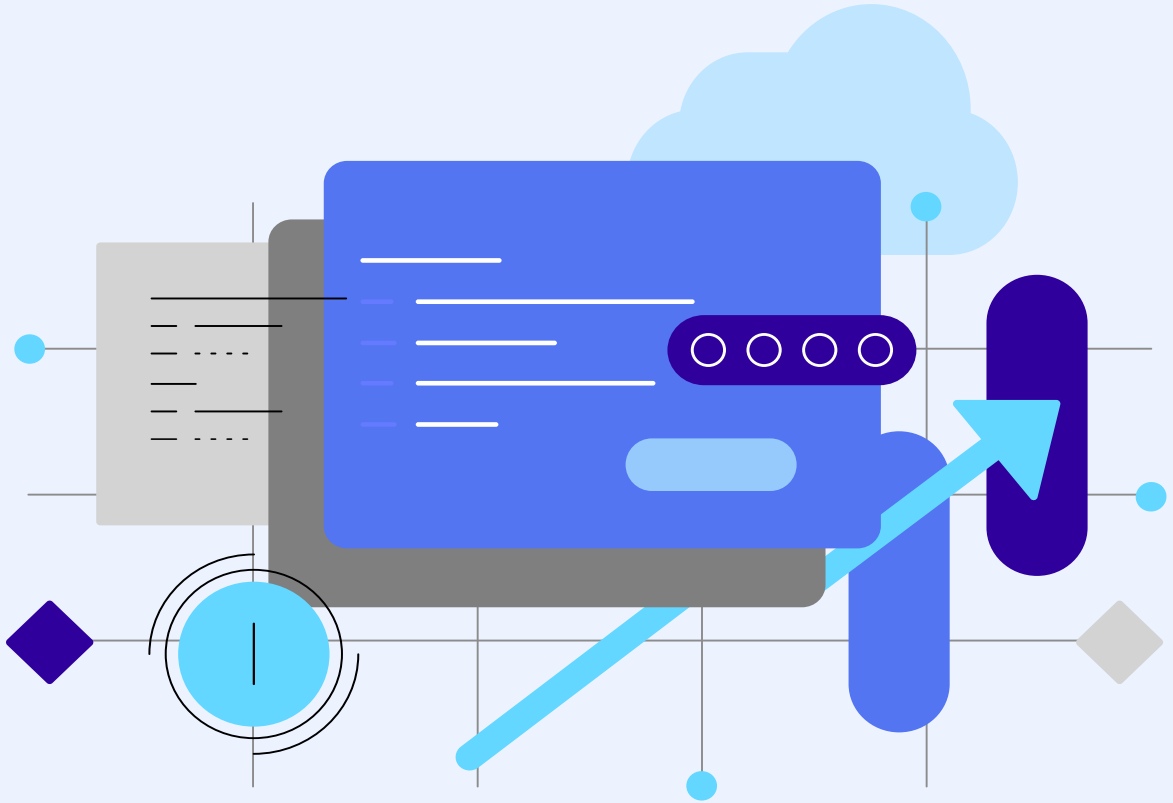
- 권한 상승
- 의심스러운 명령
- 트로이목마

TATUM SECURITY

그러면 정말로 클라우드 보안이 끝날까?

우리 상황에 맞게 가야 한다

선택적으로 도입하세요. 부채로 돌아올 수 있습니다.

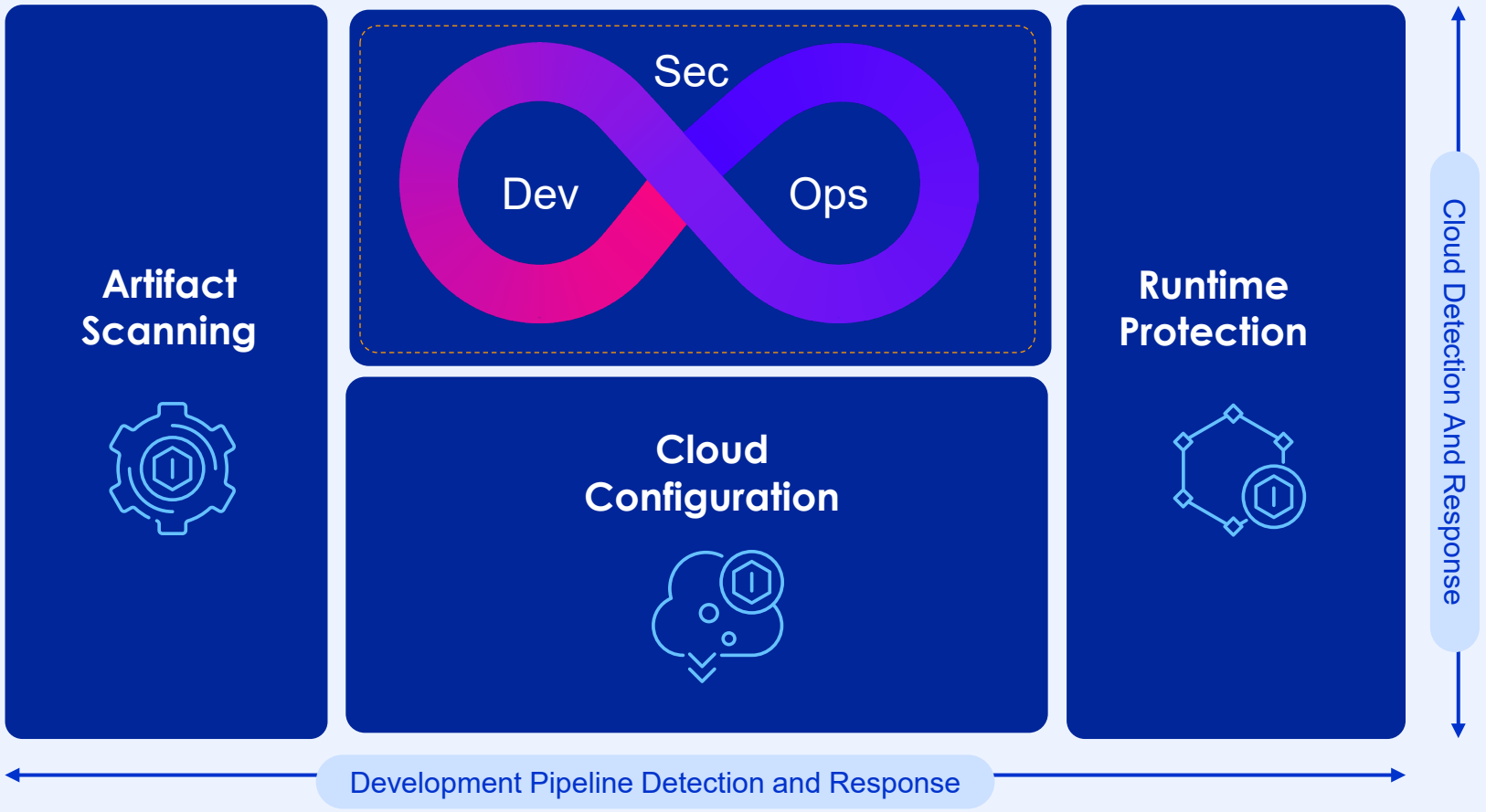


국내 컴플라이언스에 맞출 수 있는가?

하이브리드 클라우드 환경에 맞출 수 있는가?

팀의 KPI로는 어떻게 적용시키는가?

TATUM CNAPP Detailed View



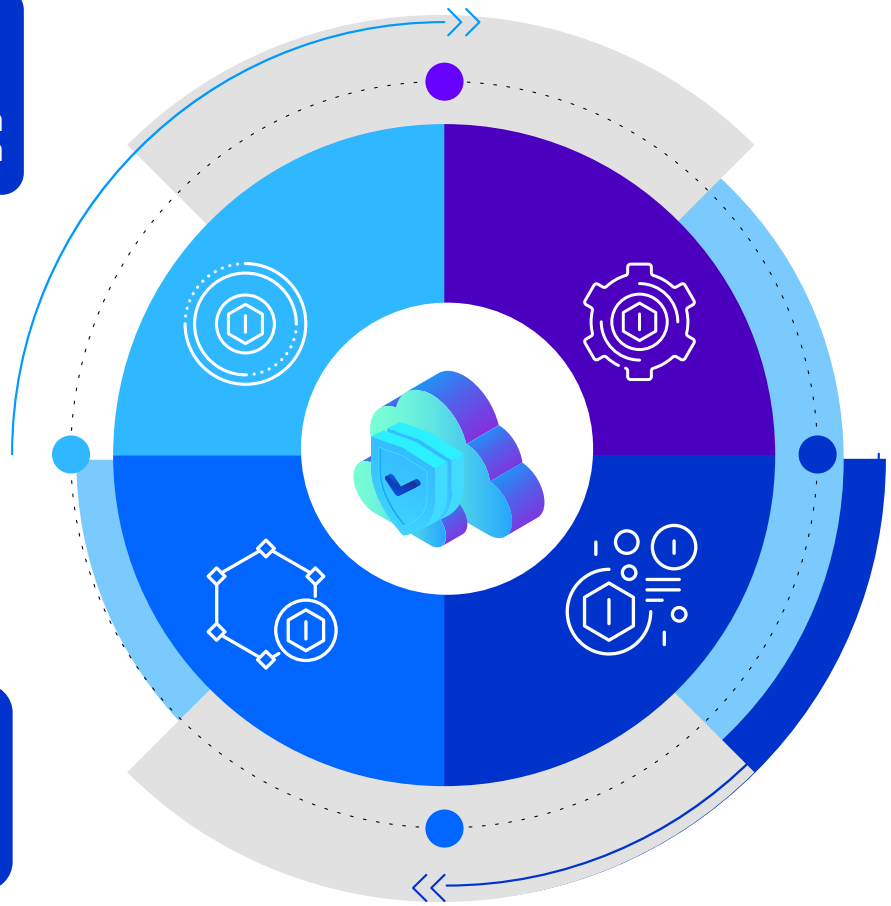
- CSPM은 필수
- 클라우드 권한 관리의 중요성(CIEM)
- CWPP 도입 어려움
- ASPM과 SBOM 같이 고려

TATUM CNAPP : Cloud Native Application Protection Platform

TATUM SECURITY

TATUM **CNAPP** PLATFORM

CNAPP
Cloud Native Application Protection Platform

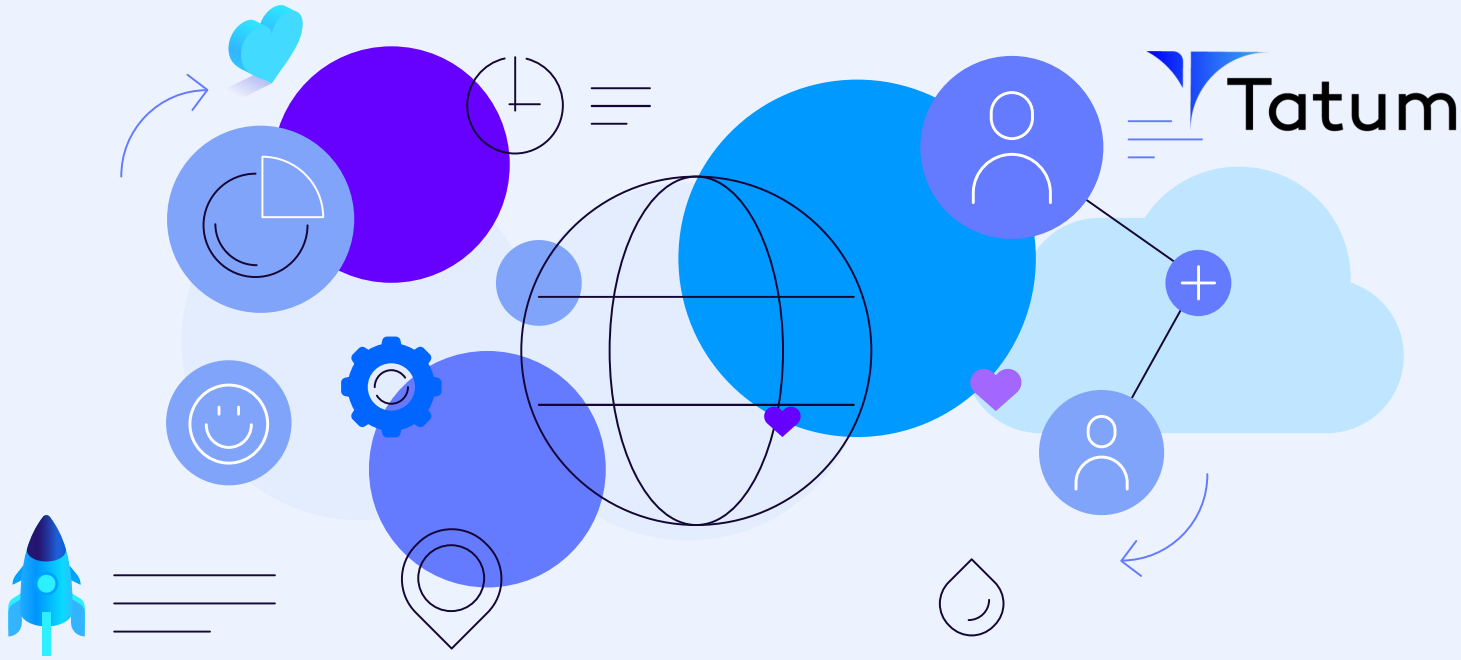


CWPP
Cloud Workload Protection platform

CSPM
Cloud Security Posture Management

CIEM
Cloud Infrastructure Entitlements Management

클라우드로의 여정, 테이텀이 함께하겠습니다.



TATUM SECURITY

클라우드 보안 시장 혁신의 기회,
테이텀 시큐리티와 함께 하시겠습니까

Contact Point

E-mail : ask@tatumsecurity.com
Web : www.tatumsecurity.com
Tel : 02-6949-2446

Protect Your Cloud
Clearly, Obviously