



클라우드 통합 보안 솔루션 (CNAPP)

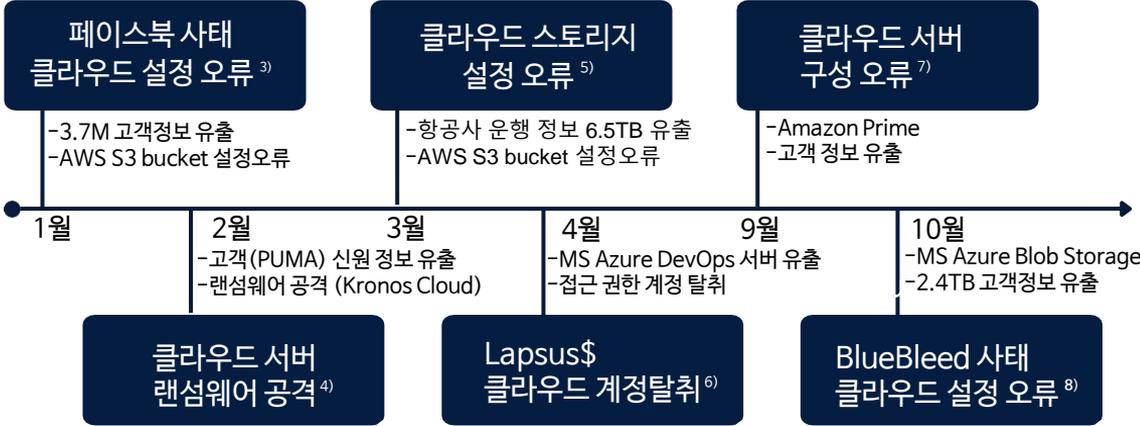


- I. 2023 클라우드 보안 동향
- II. Tenable 소개
- III. Tenable Cloud Security 클라우드 보안 올인원 솔루션
- IV. Tenable Cloud Security 차별점
- V. Tenable Cloud Security 기대효과

2022년 클라우드 보안 사고율 80%

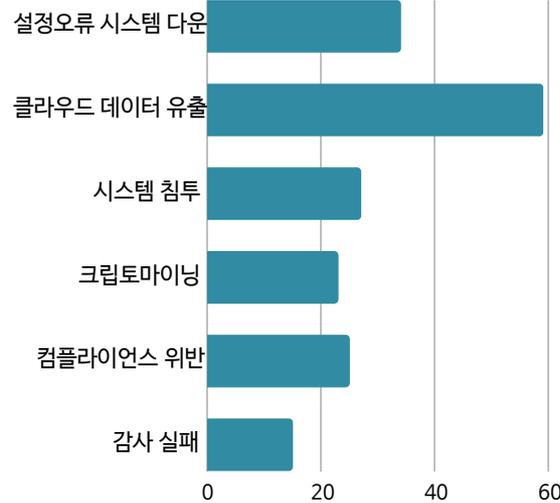
국내 클라우드 전환 75.1% ¹⁾ 클라우드 전환에 따른 위협 증가가 사이버 보안 위협의 주요 이슈로 떠오름
 2022년 클라우드 사용자 80% 보안 사고 경험, 클라우드 취약점 공격 2배 증가 ²⁾

2022 주요 클라우드 보안 사고



클라우드 전환률 증가 + 클라우드 취약점 공격 급증

2022 클라우드 보안사고 분석

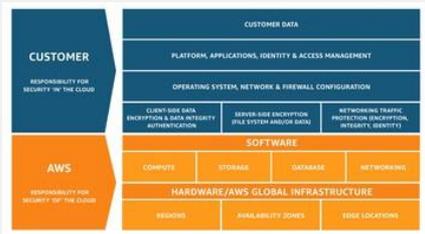


1) 2023년 국내클라우드컴퓨팅도입현황조사 및 전망, IDG 2) 2023 Global Threat Report, CrowdStrike 3) Flexbooker Suffers Massive Data Breach, Millions Of Users Compromised, Stealthlabs, 2022.01.22
 4) Maine Attorney General. Notification 2022.01.10 5) Turkish Based Airline's Sensitive FFB Data Leaked, Safety Detective, 2022.03 6) DEV-0537 criminal actor targeting organization for data exfiltration and destruction, Microsoft, 2022.4.22
 7) Amazon Accidentally Exposed an Internal Server packed with Prime Video viewing habits, 2022.10.28 TC 8) Sensitive Data of 65,000+ Entities in 111 countries leaked due to a single misconfigured data bucket, 2022.10.19

사용자 책임 클라우드 보안 범위

클라우드 서비스 공급자(CSP)는 “공동 책임 모델 (Shared Responsibility Model)”을 통해 서비스 제공
 사실상 “분할 책임 모델 (Split Responsibility Model)”로, **고객의 보안 책임 영역을 명시**
 클라우드 내부 관리 및 설정, 계정 관리, 정책 준수 책임 등 **클라우드 내부 보안 책임은 사용자의 영역**

CSP의 공동 책임 모델

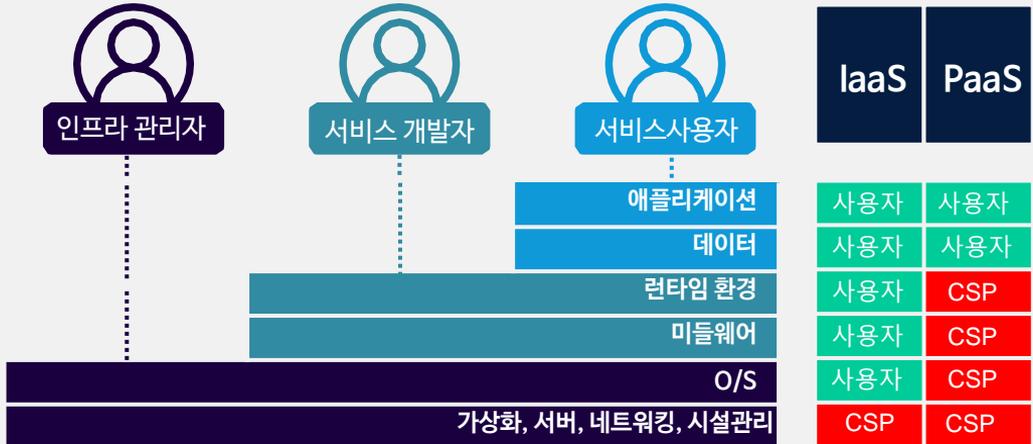


AWS: Shared Responsibility Model



Microsoft: Shared Responsibility Model GCP: Shared Responsibility Model

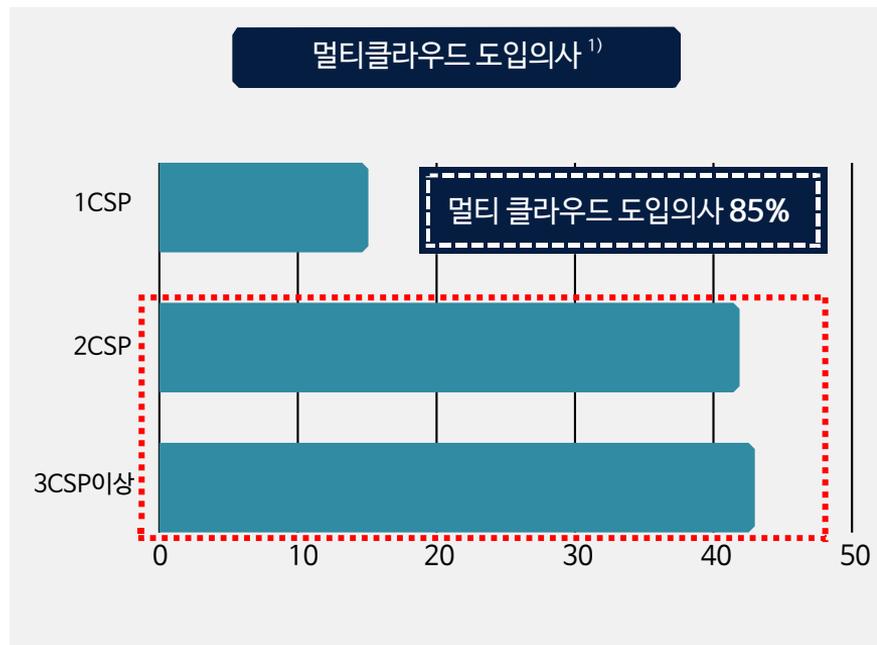
클라우드 보안 영역



클라우드 환경 복잡도 증가

클라우드의 사용이 보편적 인프라로 자리 잡으며 도입 목적에 따른 멀티클라우드 도입, 활용 높아짐

멀티 클라우드 환경 통합 보안 구축 및 전문 인력 확보 가장 큰 과제임
클라우드 보안 전문가의 수는 IT 개발자 수에 비해 부족해 구인이 어려움



SERVICES	aws	Azure	Google Cloud Platform
Virtual Servers	Elastic Cloud Compute	Virtual Machines	Google Compute Engine
Serverless Computing	Lambda	Azure Functions	Cloud Functions
Kubernetes Management	Elastic Kubernetes Service	Kubernetes Service	Kubernetes Engine
Object Storage	Simple Storage Service	Azure Blob Storage	Cloud Storage
File Storage	Elastic File Storage	Azure Files	Filestore
Block Storage	Elastic Block Storage	Azure Disk	Persistent Disk
Relational Database	Relational Database Service	SQL Database	Cloud SQL
NoSQL Database	DynamoDB	Cosmos DB	Firestore
Virtual Network	Virtual Private Cloud	Azure VNet	Virtual Private Network
Content Delivery Network	CloudFront	Azure CDN	Cloud CDN
DNS Service	Route 53	Traffic Manager	Cloud DNS
Authentication and Authorization	IAM	Azure Active Directory	Cloud IAM
Key Management	KMS	Azure Key Vault	KMS
Network Security	AWS WAF	Application Gateway	Cloud Armor

IT Private Cloud

1) 2023년 국내클라우드컴퓨팅도입현황조사 및 전망, IDG

새로운 공격 표면 급증

클라우드 기술 발전, 구성 환경 복잡도 증가로 인한 새로운 공격 표면 생성 인증, 쿠버네티스, IaC 등 새로운 공격 표면을 노리는 사례 급증

3rd파티 (자회사, 협력사 등) 접속 등 인증 관련 데이터 유출 사고 경험 83% ¹⁾



Security Intelligence

“Authorized” to break in: Adversaries use valid credentials to compromise cloud environments

크레덴셜 유출 : 클라우드 보안사고 36%

Application Security | 3 MIN READ | NEWS

Majority of Kubernetes API Servers Exposed to the Public Internet

Shadowserver Foundation researchers find 380,000 open Kubernetes API servers.

퍼블릭 액세스 국내 쿠버네티스 7.2만개

CYBERSECURITY | SECURITY NEWSWIRE | CYBERSECURITY NEWS

82% of companies give third parties access to all cloud data

3rd 파티 클라우드 통합권한 부여율 82%

1) 2021 State of Cloud - Tenable (Ermetic)

클라우드 보안의 문제점

클라우드 환경 복잡성이 증가로 클라우드 보안 성숙도 향상을 위한 전문성 확충이 어려움 (클라우드 보안 성숙도 낮음- 80%)¹⁾
포인트 솔루션 개별 도입으로 인한 클라우드 보안 통합 운영률 30% 미만²⁾
새로운 공격표면에 빠르게 대응할 수 있는 역량을 가진 통합 보안 솔루션 니즈 증가

분류	기존 클라우드 보안	클라우드 보안 문제점	해결책
전문성	IaaS 클라우드 설정오류	새로운 공격표면 대응, 전문 인적 자원 확보 어려움	쉽게 새로운 공격표면 대응
환경	단일 퍼블릭 클라우드 환경	멀티클라우드 환경 가시성 확보 어려움	다양하고 복잡한 IT 환경 대응 및 편이성
통합운영	포인트 솔루션 (CSPM, KSPM, CWP, CDR)	보안 도구 종류 증가, 효율 저해	단일화된 통합 솔루션
사용성	Dev, DevSecOps, IAM, CloudSec 개별 운영	협업 제한	개발 및 운영 워크플로우 전사 지원

1) Osterman Report: State of Cloud Security Maturity 2022 - Survey Findings

2) Cloud Security Alliance:: Cloud Native Application Protection Platform (CNAPP) Survey Report, August 2023

위험 노출 관리 점유율 1위 Tenable

Tenable은 2002년 설립된 취약점 관리 전문 기업, **전세계 점유율 1위를 차지하고 있는 마켓리더¹⁾**
 네서스 기술을 기반으로 위험 노출 관리를 통한 사이버 위험 감소를 위한 플랫폼 개발
전세계 최고 수준의 테너블 리서치 운영 (2020, 2021년 제로데이 취약점 141개, 167개 테너블 발견)



취약점 관리 시장 점유율 세계 1위
 27.5% 점유율 1위, 국내 100개 이상 기업 사용

44000+ 전세계고객사
 4.4만개 이상



취약점 진단 범위 세계 1위
 경쟁사 대비 20% 많은 CVE 진단 기준 적용

60% FORTUNE 500
 기업 사용률



제로 데이 연구분야 테너블 리서치 운영
 141/167 제로데이 취약점 발견 (2020/2021)
 24시간내 신규 취약점 업데이트

40% GLOBAL 2000
 기업 사용률



CyberSecAsia
 Best VM 2022



GartnerPeerInsights
 Choice for VA
 2019~2022



Frost & Sullivan
 VM leader
 2021



IDC
 Worldwide VM market
 점유율 1위 (2020~22)



2023 Forrester Wave
 Vulnerability Risk
 Management leader²⁾

1) 점유율 1위: Worldwide Device Vulnerability Management Market Shares, 2021: "The Stakes Are High"

2) Forrester Wave™: Vulnerability Risk Management, Q3 2023

Tenable 위험 노출 관리 솔루션



EXPOSURE VIEW
사이버 위험 분석

ATTACK PATH ANALYSIS
유출 및 공격경로 분석

CYBER ASSET MANAGEMENT
자산 통합 모니터링

취약점 관리



웹앱 보안



클라우드 보안



인증보안



외부공격표면



OT보안



THIRD
PARTY
DATA

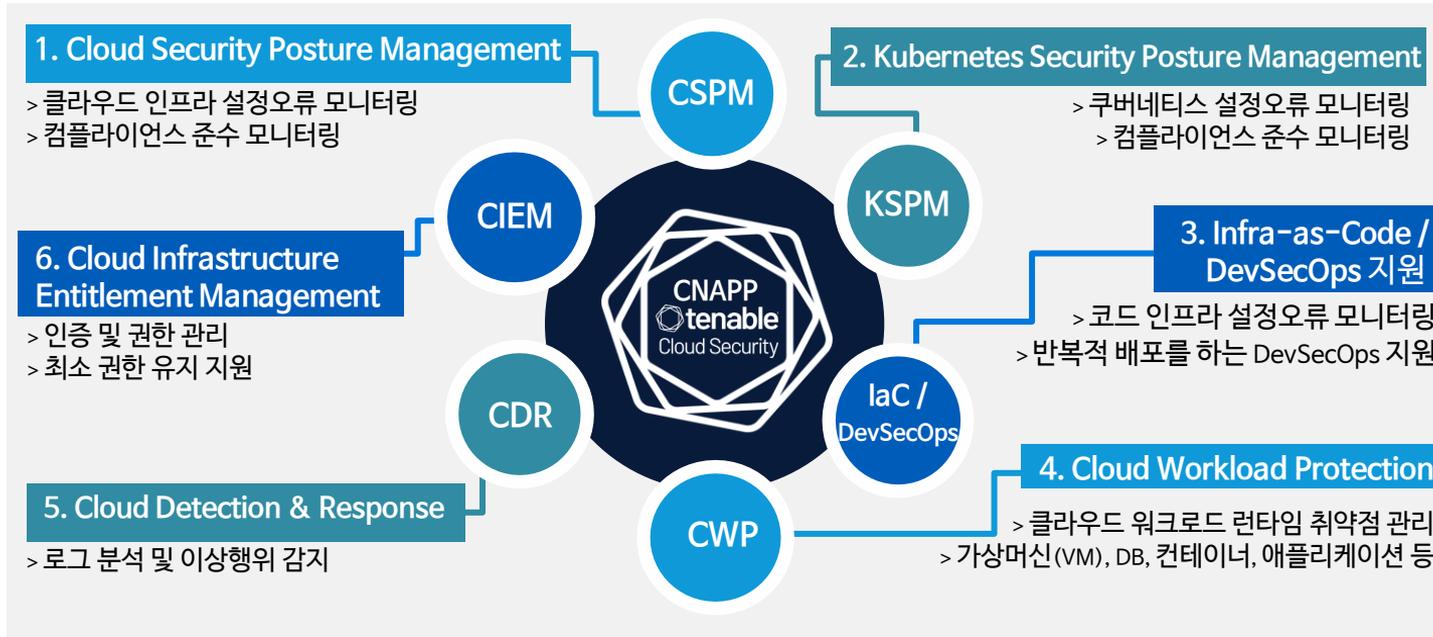
ExposureAI

THIRD
PARTY
DATA

EXPOSURE GRAPH

Solution : 클라우드 보안 올인원 솔루션

Tenable Cloud Security는 AWS, Azure, GCP를 지원하는 클라우드 네이티브 애플리케이션 보호 플랫폼 인증, IaC, 쿠버네티스, PaaS 등 새로운 공격 표면에 대응하는 통합 클라우드 보안 솔루션 멀티 클라우드 및 하이브리드 등 복잡해진 클라우드 환경에서 쉽게 확장 가능한 에이전트리스 보안 솔루션



“
 CNAPP는
 클라우드 네이티브앱의
 전체 수명주기를
 보호하는
 핵심 보안 기술 1)
 Gartner®
 ”

1) 4 Must-Have Technologies That Made the Gartner Hype Cycle for Cloud Security -Gartner, 2021

CSPM : 클라우드 설정 오류 탐지, 컴플라이언스 모니터링

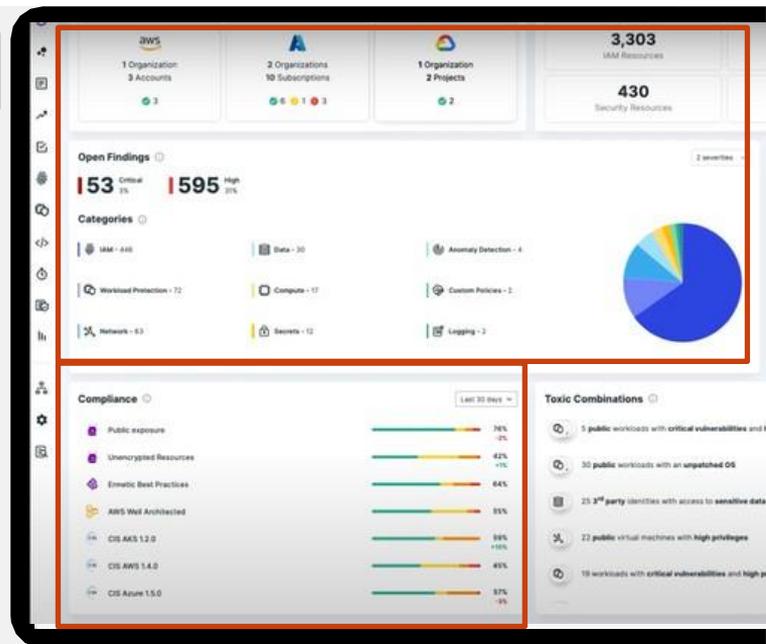
클라우드 인프라의 인증, 네트워크, 워크로드, 데이터 등 모든 클라우드 설정 오류 탐지 로그 및 이상행동 분석을 기반으로 클라우드 자산에 악영향을 미치는 조치 우선순위 생성 컴플라이언스 준수 내역 지속적 모니터링 및 리포트 자동화



클라우드 인프라의 모든 잘못된 설정 내역을 확인할 수 있습니다. 또한 로그 및 이상행동 분석을 기반으로 조치 우선 순위를 제공합니다. 컴플라이언스 준수 모니터링 및 자동 리포트 생성합니다.

주요기능

- 클라우드 인프라 전체 설정오류 탐지 : 인증, 네트워크, 워크로드, 데이터 등
- 조치 우선순위 지정 : 로그, 이상행동 분석과 결합하여 위험상황 파악
- 외부 노출 클라우드 자산, 네트워크 접속 탐지
- 컴플라이언스 준수 모니터링 : SOC2, CIS, NIST, GDPR, HIPAA, ISO, PCI, ISMS-P 등
- 사용자 정의 정책 템플릿 제공 : 수동 작업 최소화
- 자동 컴플라이언스 리포트 생성 : 자산목록, 네트워크 설정, 접속인증 감사



KSPM : 쿠버네티스 설정오류 탐지, 컴플라이언스 모니터링

클라우드 보안 형상 관리시 쿠버네티스 컨테이너 설정 오류 탐지는 필수
지속적 스캔 및 모니터링을 통해 설정오류, 위험 권한, 위험 시나리오를 상세 조치 방법과
함께 제공 쿠버네티스 관련 컴플라이언스 준수 내역 지속적 모니터링



쿠버네티스 컨테이너 설정 오류, 위험 권한, 위험 시나리오를 탐지하여
관련 사용자가 빠르게 수정할 수 있도록 알려줍니다. 지속적으로 스캔
하며 상세한 조치 방법을 제공하고 쿠버네티스 관련 컴플라이언스 준수를
모니터링 합니다.

주요기능

- 쿠버네티스 컨테이너 설정오류 탐지
- 쿠버네티스 컨테이너 위험 권한 부여 탐지
- 위험 시나리오 탐지
- 상세 조치 제공
- 컴플라이언스 준수 모니터링 : CIS Benchmark (쿠버네티스용), NSA 등

EKS workload is running privileged containers

EKS cluster John-cluster has Deployment hello-world-deployment-2 with
Container hello-app-2 set as privileged

Created on: 10:34 am Feb 21, 2019 | Account: AcmeProd (123252999261)

Description

Running a container in a privileged mode enables the container to access the host's resources and kernel ca...
Since an attacker may gain access to privileged containers, it is not recommended to run privileged contain...
Ermetic evaluates all Kubernetes workload types (such as Deployments and DaemonSet) and alerts on ever...
spec that has the securityContext.privileged flag set to true.

Note: Workloads part of kube-system namespace will not be evaluated

YAML

```
1 apiVersion: apps/v1
2 kind: Deployment
3 metadata:
4   annotations:
5     deployment.kubernetes.io/revision: "2"
6     kubecti.kubernetes.io/last-applied-configuration: |
7       {"apiVersion":"apps/v1","kind":"Deployment","metadata":{"annotations":{},"name":"hello-world-
8 creationTimestamp: 2023-01-16T18:40:46.000000Z
9 generation: 2
```

IaC, DevSecOps : IaC를 통한 CI/CD 프로세스 보안

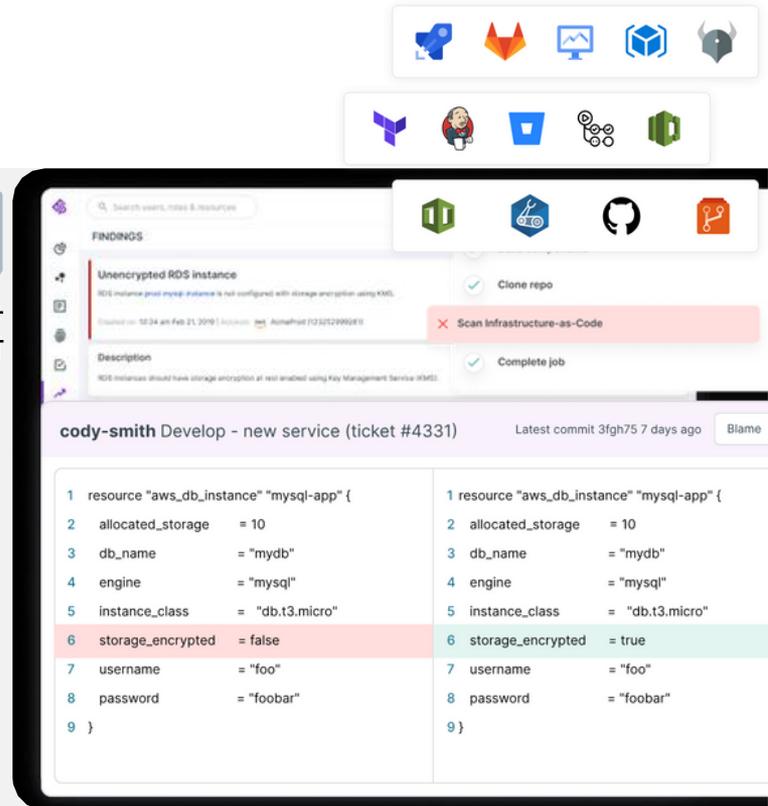
IaC (Infra As Code, 코드형 인프라)의 설정 오류와 위험을 탐지
CI/CD 파이프라인의 일부로서 클라우드 인프라 보안을 강화
IaC 환경에서 탐지된 보안 취약점 조치 자동화 프로세스 지원



코드형 인프라의 잘못된 권한 및 설정 오류를 탐지하고 조치 마법사를 통해 신속하게 수정할 수 있습니다. CI/CD 파이프라인에 티켓 자동 생성, 알림 할당 등 조치 자동화 프로세스를 지원합니다.

주요기능

- ◆ IaC 설정오류 및 위험 탐지 : Terraform, CloudFormation
- ◆ CI/CD 파이프라인 보안 적용 : 개발, 스테이징 환경 보안 평가 및 보안 프로그램 배포 관리 등 프로세스 임베디드 (Jenkins, BitBucket, CircleCI, Gitlab 등)
- ◆ 조치 자동화 프로세스 지원 : 코드를 통한 조치, 티켓 시스템, 자동알림 (Jira, Service now 등) 등을 통해 기존 워크플로우 자동화 프로세스 적용



CWP : 워크로드 취약점 관리

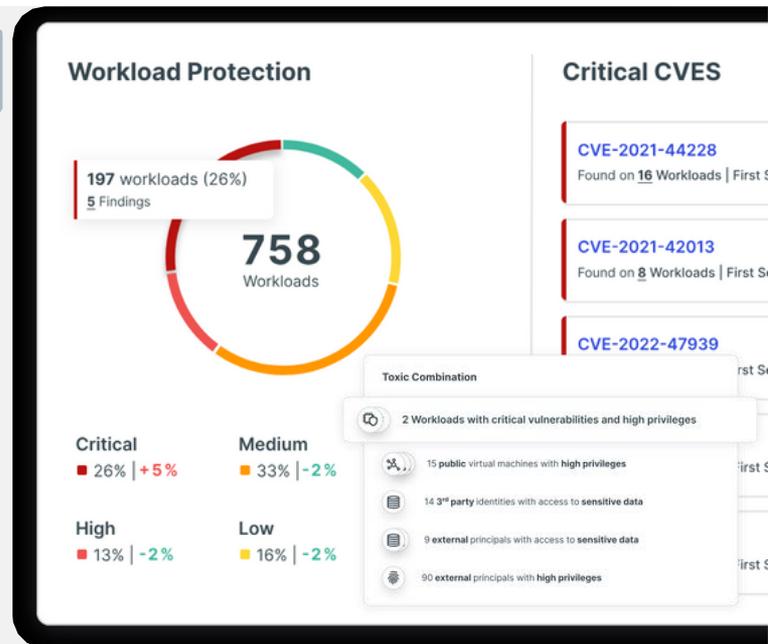
가상머신, 서버리스 기능, 컨테이너 이미지, 쿠버네티스 클러스터 전역에 걸친 취약점 진단
CVE, 구성오류, 노출데이터, 맬웨어 등 광범위한 진단 능력
OS 패키지, 애플리케이션, 라이브러리의 취약점 상관관계를 통한 취약점 동적 조치 우선순위 제공



빠른 개발 주기 동안 쉽게 발생하는 취약점 및 위험으로부터 워크로드를 보호합니다.

주요기능

- ◆ 멀티 클라우드 워크로드 포괄적 가시성
- ◆ 넓은 진단 범위 : 가상머신, 컨테이너 (컨테이너화 서비스), 서버리스 기능 진단 능력 :
- ◆ CVE, 구성오류, 노출 데이터, 맬웨어
- ◆ Toxic Combination : OS 패키지, 애플리케이션, 라이브러리 전반의 취약점 상관관계 파악을 통한 동적 조치 우선순위 제공



CDR: 비정상 행위 탐지

비정상 행위 지속적 감지 및 알림 제공

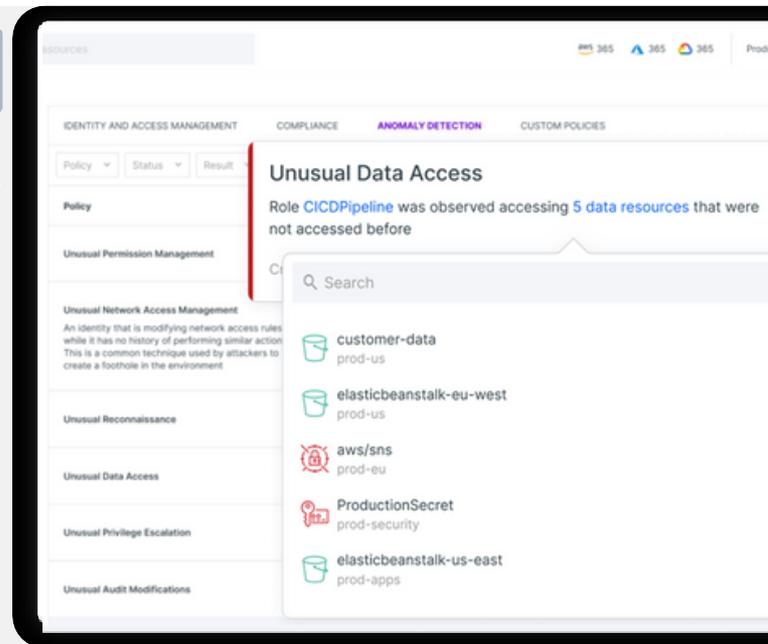
데이터 액세스, 갑작스런 권한 변경, 비정상적 정찰행위, 액세스 키 무단 사용 등 **사이버 위협 감지**
로그인, 감사설정, 네트워크 구성 등 변경 식별



행동 기준 ID 기반 위협 식별을 통해 지속적으로 위협을 감지하고, 강화된 로그 쿼리를 통해 인시던트 대응 이해, 보고, 조사를 간소화합니다.

주요기능

- 위협 감지: 비정상적 데이터 접근, 갑작스런 권한 변경, 로그인 세팅 변경, 비정상적 정찰 시도, 허가되지 않은 인프라의 설정, 액세스 크레덴셜 탈취 또는 비정상 사용 등
- 인시던트 대응 간소화 : 액세스, 권한, 인프라 구성 전반의 위협을 지속적으로 모니터링 하여 자동화 알림 및 대응 제공
- SIEM 솔루션 통합 : SIEM (Splunk, IBM Qradar), 티켓팅/알림 (Service now, Jira)



CIEM : 권한 최소화 관리

클라우드 사용자 및 서비스 권한 관리 솔루션

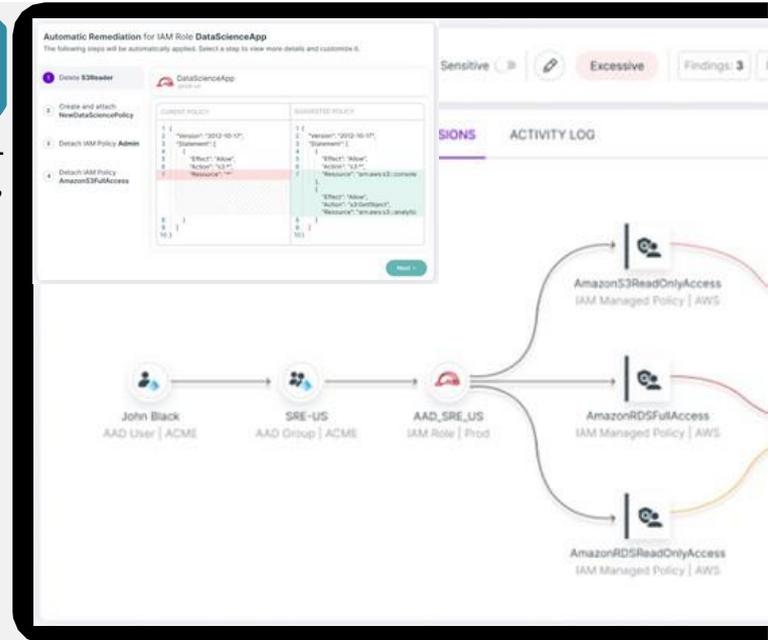
멀티 클라우드 환경 내 모든 인증, 자격, 리소스 및 구성을 지속적으로 분석하여 위험 가시성 확인
교정도구, 최소권한 코드 조각을 통한 권한관리 Shift-Left



클라우드 환경의 모든 클라우드 ID, 자격, 리소스 및 구성 전체의 인벤토리를 지속적으로 검색하여 시각화합니다. 과도한 권한, 네트워크 노출, 숨겨진 위험을 통합한 ID 관련 위험을 확인할 수 있습니다.

주요기능

- 인증 위험 가시화 : 위험 발생 원인과 가능성 시각화, 비전문가도 쉽게 위험 분류 및 조치가 가능하도록 함
- 외부 권한, 계정, 서비스 계정, 연합 계정 등 모든 인증 관련 위험 확인
- 워크로드 전체 폴스택 분석을 통한 인증 위험 우선순위
- 세분화된 인증 정책 권장 사항 제공 (리소스 단계에 따른 최소 권한 정책)
- 권한 관리 Shift Left : 마법사기능, 클라우드 기본연계, API, 웹훅을 통한 자동 조치 지원



멀티 클라우드 자산 인벤토리 관리

Tenable Cloud Security는 멀티 클라우드 환경의 모든 자산 (인증, 인프라, 워크로드, 데이터)의 위험관리 지원 에이전트리스 (에이전트 없는 ID 우선 접근방식) 클라우드 보안으로 넓은 가시성 및 확장성 유지 클라우드 스냅샷 기술로 Real-Time 자산 관리 (소프트웨어 목록 포함)

멀티 클라우드환경 실시간 자산 확인



306
IAM Resources

723
Data Resources

123
Containers Resources

AWS	GCP	Azure
DynamoDB Tables: 49	BitQuery Datasets: 32	Cassandra Clusters: 36
Kinesis Data Streams: 52	BigTables Clusters: 78	CosmosDB Accounts: 98
RDS Clusters: 30	Firestore Instances: 26	MySQL Database Servers: 76
Redshift Clusters: 70	Pub/Sub Topics: 15	SQL Servers: 56
S3 Buckets: 36	Redis Instances: 98	Storage Accounts: 76

ACTIVITY LOG

Identity: prd-app-svc | Action: | Service: | Resource: | Severity: |

prd-app-svc (acme-prod-us-1) Sensitive Public Machine Findings: 2 Excessive permissions: 29%

INFO FINDINGS PERMISSIONS NETWORK ACTIVITY LOG **PACKAGES** VULNERABILITIES

Name Version Type Vulnerabilities First Seen

Host Packages 2

Name	Version	Type	Vulnerabilities	First Seen
Apache Log4j	2.12.1	Library	CVE-2021-44228 +5	Nov 6, 2022 10:34:01 AM
Linux Kernel	5.15.20	OS	CVE-2022-0847 +2	Dec 3, 2022 02:42:59 AM
Apache HTTP Server	2.4.49	Application	CVE-2021-42013 +56	Aug 12, 2021 08:12:31 PM

acme/core-app:2.46.1

acme/logging-svc:latest

Resource

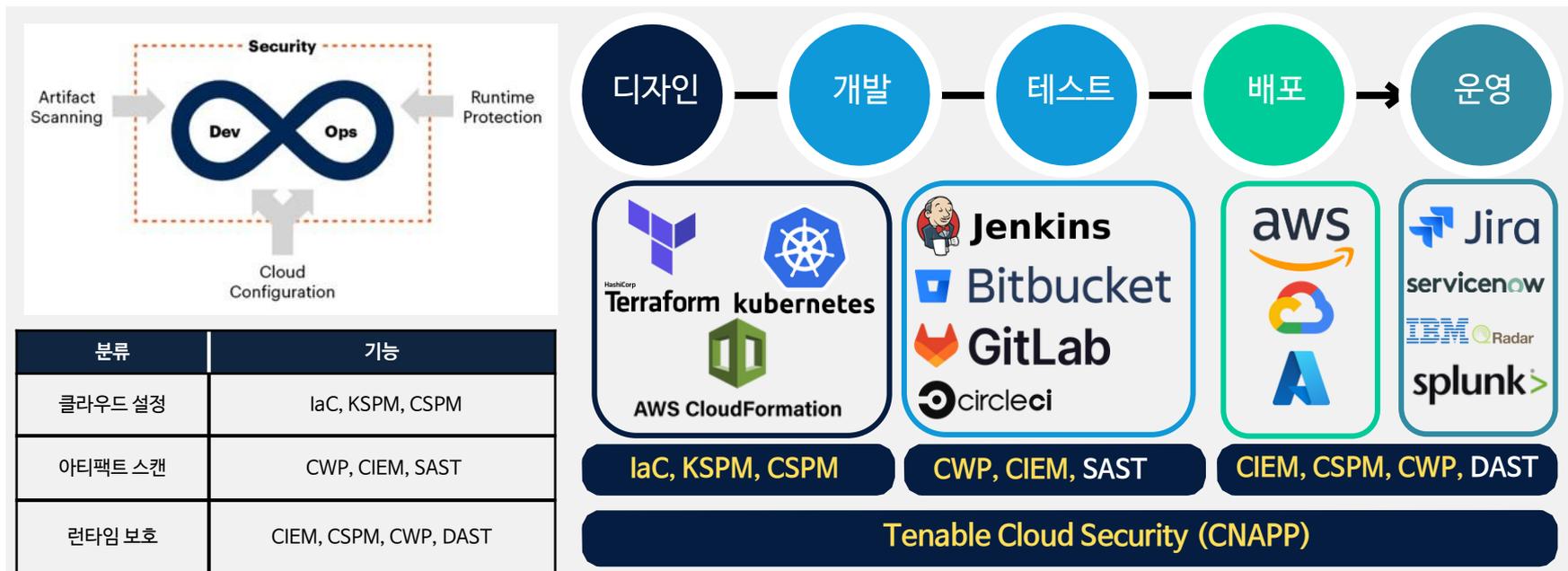
- elasticbeanstalk-us-... S3 Bucket | Org1Ac...
- ermatic-de-... S3 Bucket | Org1Ac... Unusual Data Access: Role Users was observed accessing 5 data resources that were not accessed before
- elasticbeanstalk-us-... S3 Bucket | Org1Ac...
- arn:aws:iam-... S3 Bucket | Org1Ac...
- arn:aws:iam-... AM Role | Org1Ac...
- aws-cloudtrail-logs-... S3 Bucket | Org1Ac...
- ermatic-demo-2-... S3 Bucket | Org1Ac...

클라우드 네이티브 앱 라이프 사이클 가시성

CI/CD 모델에서 보안을 초기부터 고려되어야 함

DevSecOps 는 인프라가 보안 상 배포하기에 안전한지 확인하는 작업부터 시작해야 함

기존 개발 프로세스 및 개발 도구에 클라우드 보안 검사를 추가할 수 있도록 지원



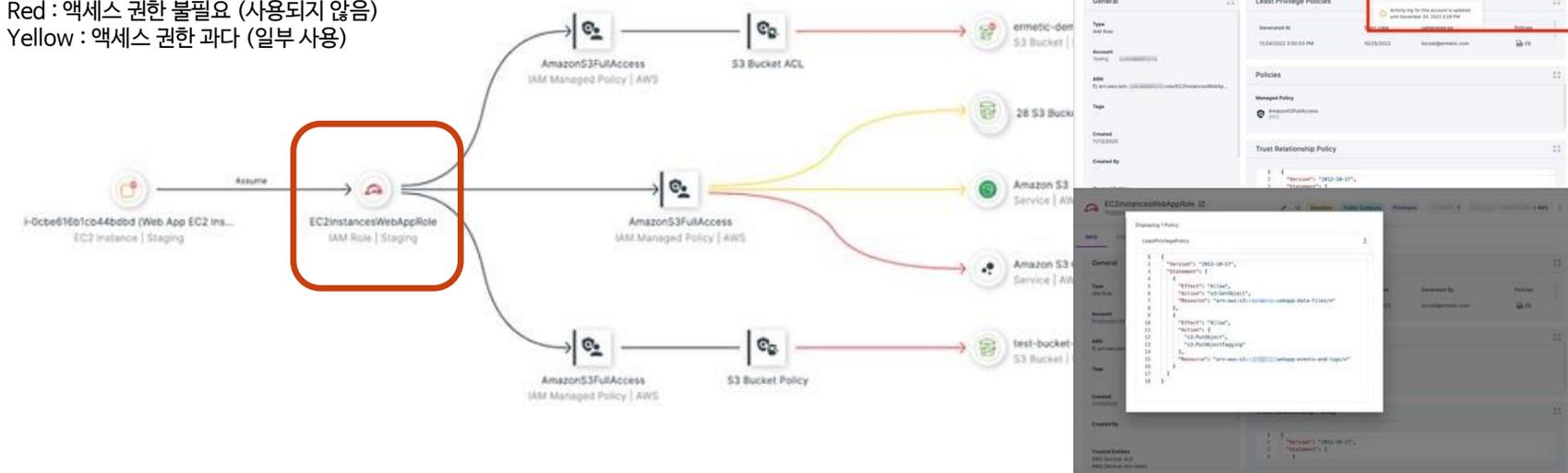
1) [Gartner: Cloud-Native Application Protection Platform \(CNAPP\) scope](#)

최소 권한 및 제로트러스트 달성

클라우드 보안 실패의 75% : ID 관리, ID 는 새로운 공격표면
여러 ID로부터 SSO (Single Sign On) 데이터를 수집하여 유해한 조합과 위험한 신원, 과도한 권한 식별
최소 권한 정책 자동 생성 지원

AmazonS3FullAccess 최소권한 적용

Red : 액세스 권한 불필요 (사용되지 않음)
Yellow : 액세스 권한 과다 (일부 사용)



다양한 확장 기능 - JIT (일회용 접속권한 관리)

필요 기간 동안 액세스 권한을 부여, ID 손상 노출 최소화
개발자가 빠른 요청, 승인, 임시 액세스 권한 획득
일시적 권한으로 공격표면을 최소화하여 제로트러스트 시행의 열쇠

주요기능

- 관리자 설정 기능 : 접속권한 사용자, 계정, 보유권한, 권한 사용시간, 승인자 설정
- 사용자 권한 요청 : 포털을 통해 기능 제공
- 사전 승인 및 수동 최소 승인 (2인이상) 프로세스 제공
- 이메일, 슬랙을 통한 권한 요청 공유
- 권한 요청 및 승인 검토에 대한 감사 제공

Access Requests + Request Permission

2

Cloud	Requestor	Group	Permission	Duration	
aws	Theo Wiggins	IT	Power user	3 Hours	<input type="button" value="Deny"/> <input type="button" value="Approve"/>
gcp	Mary Smith	IT			

Active

Johnathan Roberts
Department: R&D
Group membership: Alpha, Engineering, Employees
Johnathan has requested access to **aws Production** for **4 hours** to debug JIRA issue **SEC-2113 (Critical)**

Created	Requestor		
aws	Robert Garcia		10:34 am Nov 7, 2022
A	Ahmud Haddad	Contributor	1 Week <input type="button" value="Denied by admin 09:25 am Nov 21, 2022"/>

Tenable Cloud Security 기대효과



자산 인벤토리

멀티클라우드
자산 인벤토리 가시성



앱 라이프사이클
취약점 탐지

개발부터 배포까지
모든 클라우드 자산
설정오류, 취약점 탐지



통합 분석을 통한
조치 우선순위

클라우드
통합분석
조치 우선순위 제공



위협 탐지 및
조치

조치마법사,
협업 티켓팅을 통한
위협탐지 및 조치



제로트러스트
달성

권한 모니터링
최소 권한 액세스
지속적용

Tenable Cloud Security

위험 노출 관리, 지금 시작하세요

테너블 공식 총판 (주) 롤텍
E-mail : sales@roltech.co.kr
문의처 : 031-711-7108