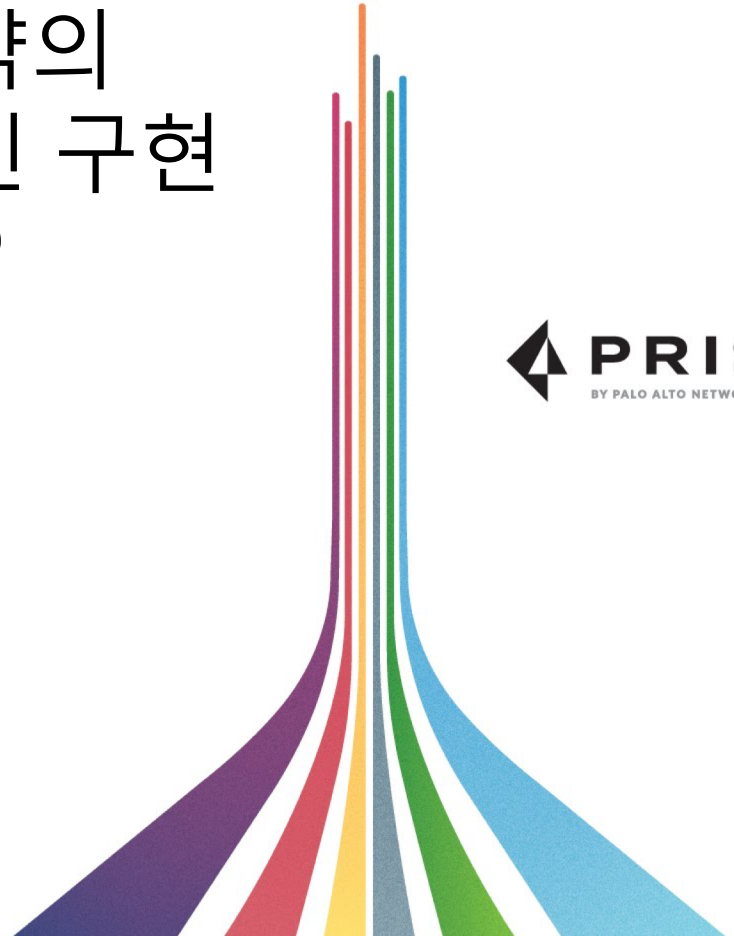
금융권 클라우드 전략의 성공적인 구현

(컨테이너, 서버리스, CI/CD 보안)



PRISMA™
BY PALO ALTO NETWORKS

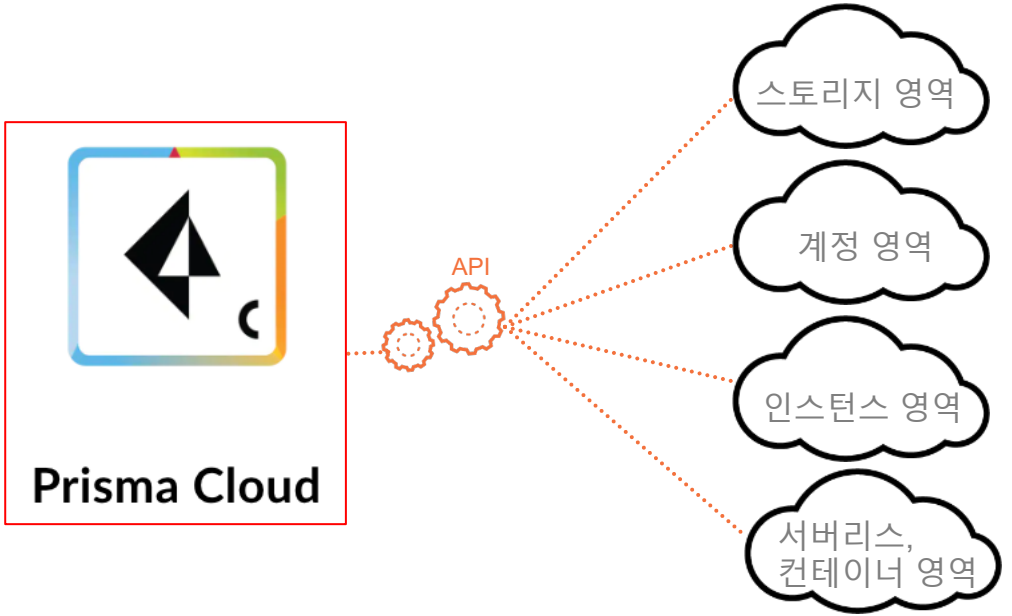
김 민석 이사 (Steve Kim)

stkim@paloaltonetworks.com
Cloud Specialist Systems Engineer
Palo Alto Networks, APAC CE Team

금융권 클라우드
: Container, Serverless, CI/CD. 보안

paloalto NETWORKS

지속적인 보안 모니터링 및 컴플라이언스 체크 및 차단



- MFA를 활성화할 수 있습니까?
- 민감한 데이터가 노출됩니까?
- 어떤 서비스가 구동되고 있습니까?
- 누가 이 리소스에 접근합니까?

리소스를 찾아내고 모니터링	안전한 스토리지 서비스	컴플라이언스 리포팅

클라우드 네이티브 애플리케이션을 위한 사이버 보안

호스트, 컨테이너, 서버리스

DevSecOps 라이프 사이클 전체적인 보안

왜 Prisma Cloud 인가?

자동화

가시성

방어

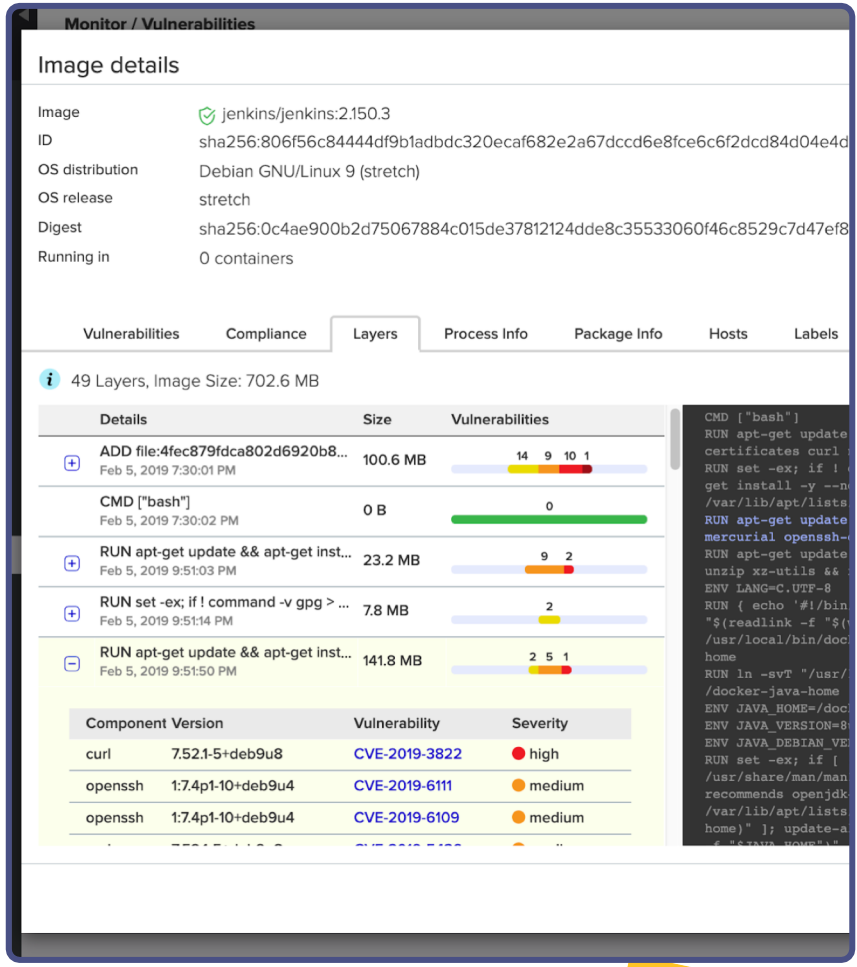
- 취약성 관리
- 런타임 방어
- 컴플라이언스
- 액세스 제어
- 클라우드 네이티브 방화벽 (CNNF, CNAP)
- CI/CD 통합

취약점 관리

호스트, 이미지, 컨테이너 및 서버리스 기능에서 업계 최고의 정밀도

고유한 환경에 기반한 취약점의 자동 우선 순위 지정

환경 전체에서 취약한 소프트웨어 실행 방지



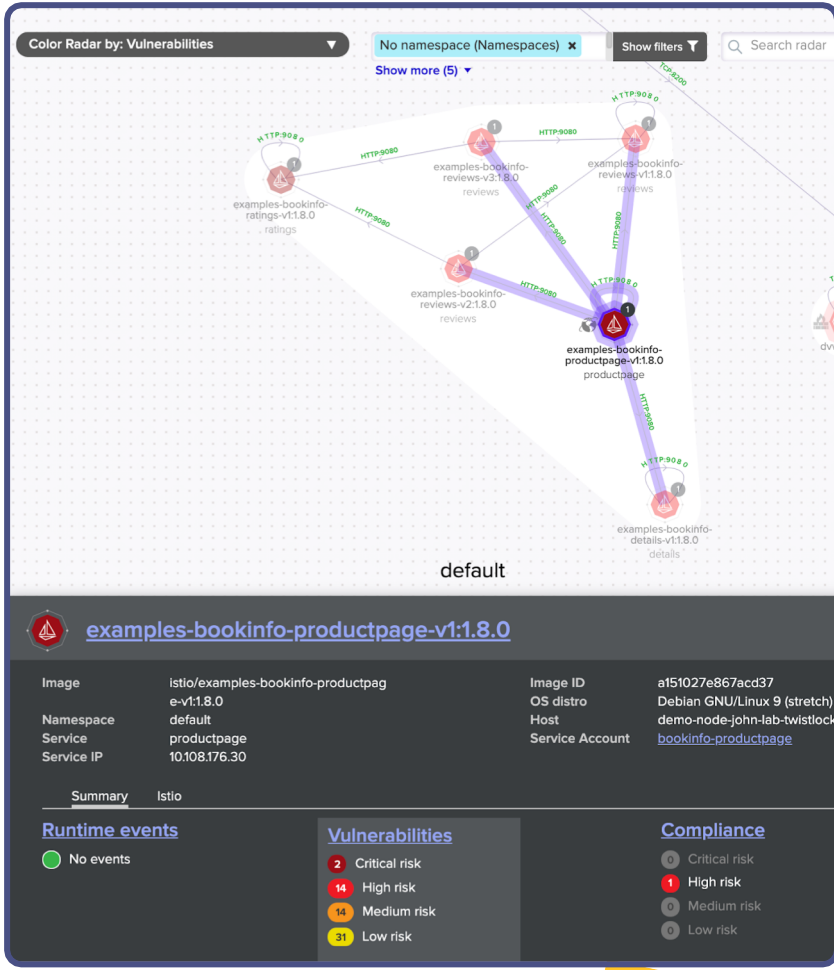
자동화 가시성 방어

클라우드 네이티브 방화벽

클라우드 네이티브 환경에 맞게 조정된 레이어 4 및 레이어 7 방화벽(CNNF, CNAF)

진정한 침입 탐지 및 침입 방지

완전 자동화된 메시 발견 및 마이크로 세그먼트

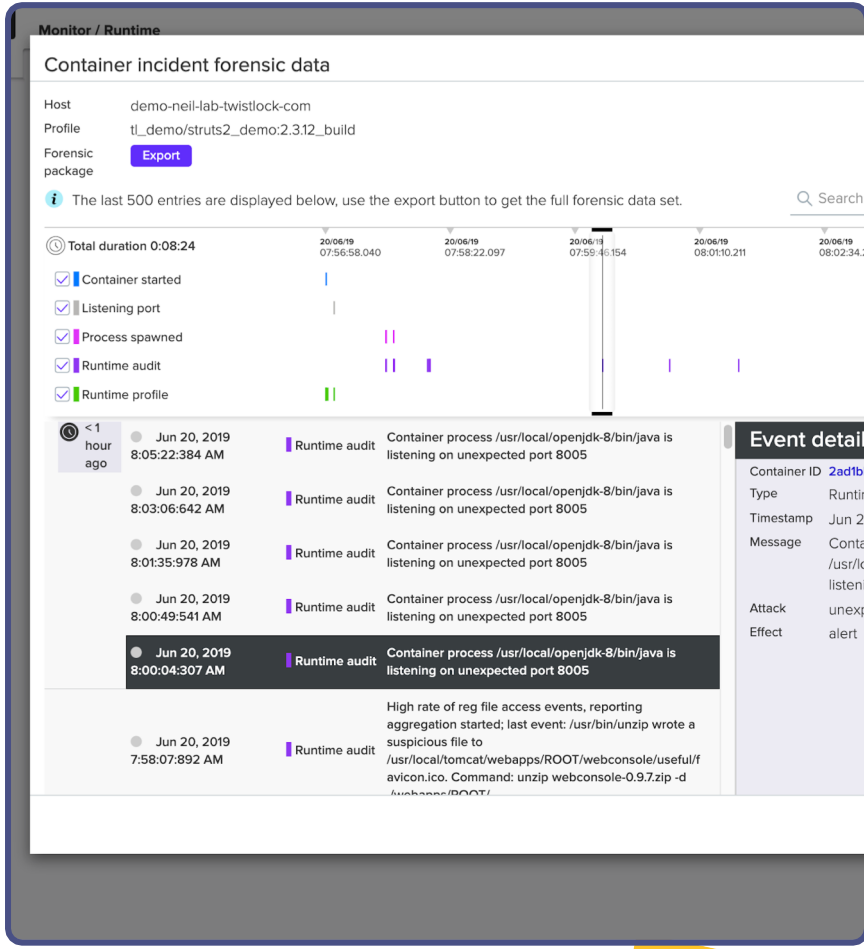


런타임 방어

모든 앱에서 명시적인 '허용 목록' 자동 모델링

모델 및 위협 지표를 기반으로 한 자동 사고 탐지 및 예방

환경의 모든 컨테이너 및 호스트에 대한 지속적인 포렌식



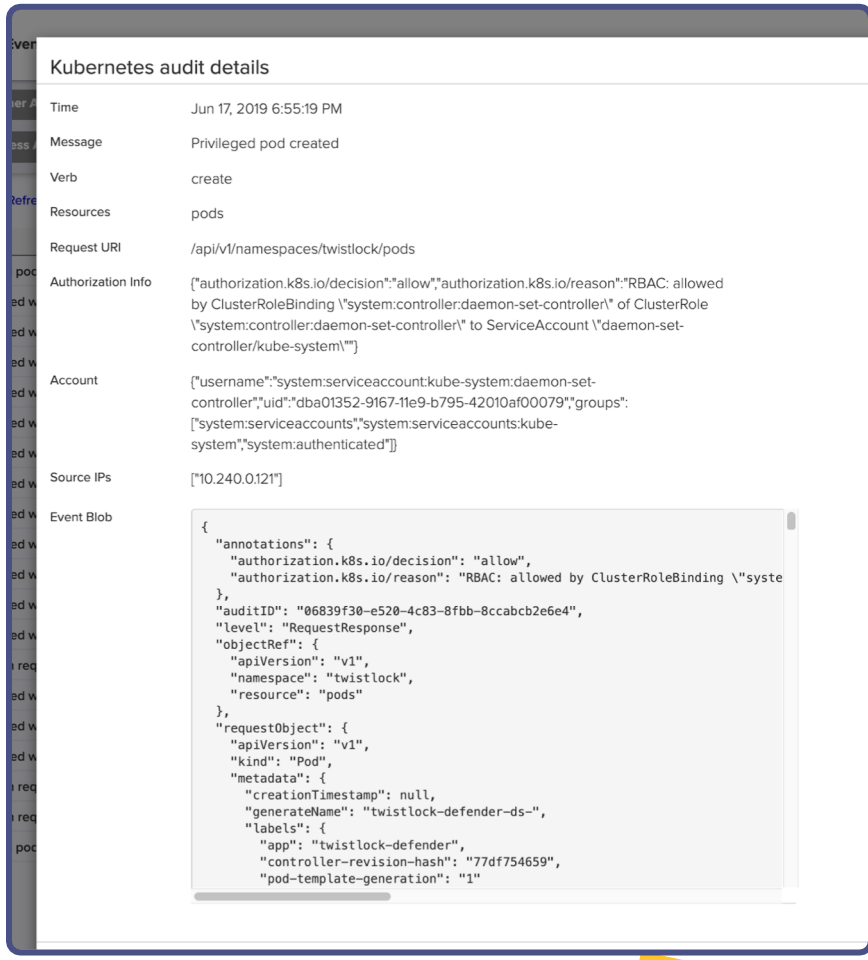
액세서 제어

엔터프라이즈급 파일 무결성 모니터링, 호스트 감사 및 로그 파일 검사

모든 인기있는 공급자와 통합된 비밀 관리

도커, sshd 및 sudo 이벤트의 중앙 모니터링

Kubernetes AuditSink의 실시간 스트림 처리

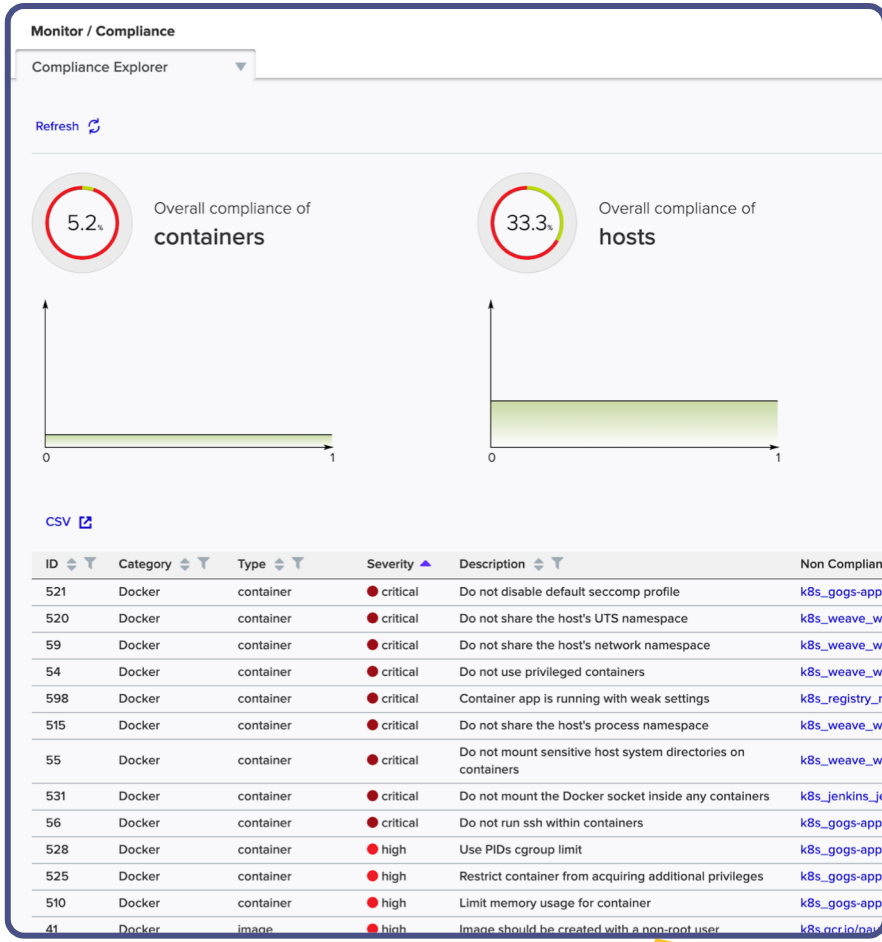


컴플라이언스

CIS, PCI-DSS, HIPAA, GDPR, NIST SP 800-190 및 FISMA에 대한 원 클릭 시행

모든 제공 업체, 계정 및 지역에서 클라우드 네이티브 서비스를 중앙에서 검색하고 모니터링

OpenSCAP, PowerShell 및 Bash 스크립트를 사용한 사용자 정의 검사

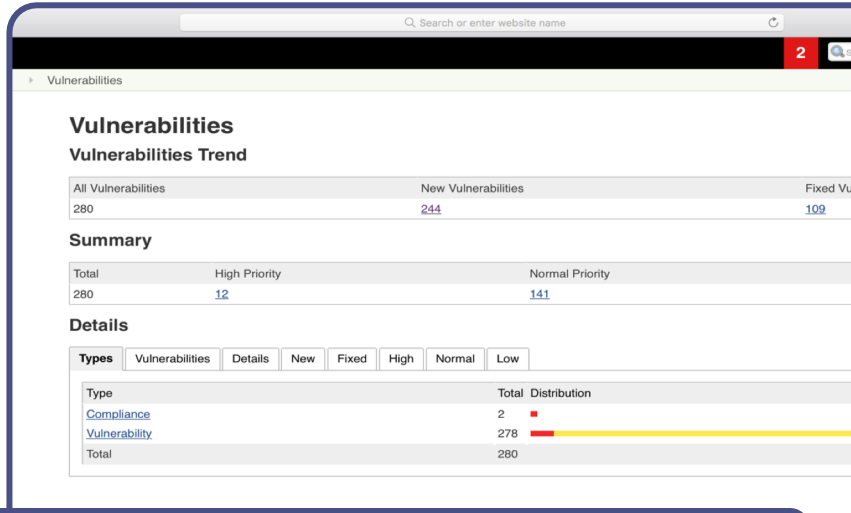


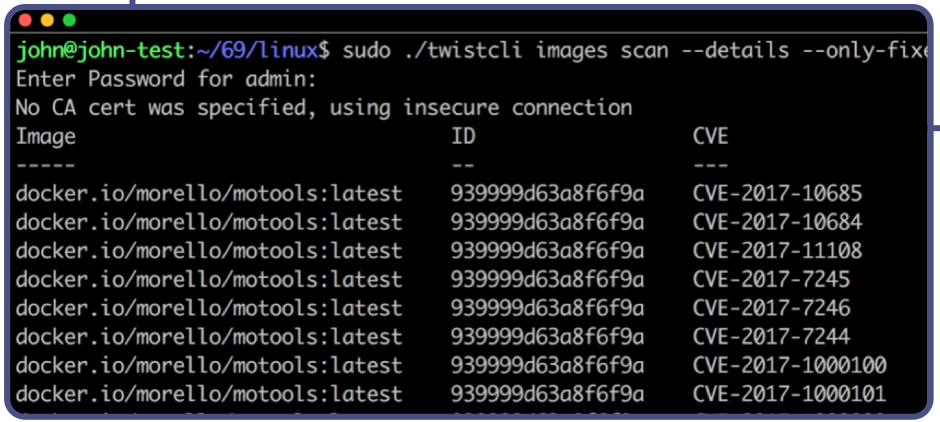
CI/CD 통합

모든 CI / CD 워크 플로우 또는 도구에 통합 할 수 있는 기본 플러그인 및 독립형 스캐너

모든 빌드에서 규정 준수 및 취약성 임계 값이 있는 ”Shift left” 품질 보증

스캔 호스트, 컨테이너 이미지, 서버리스 기능 및 PCF BLOB 저장소 스캔

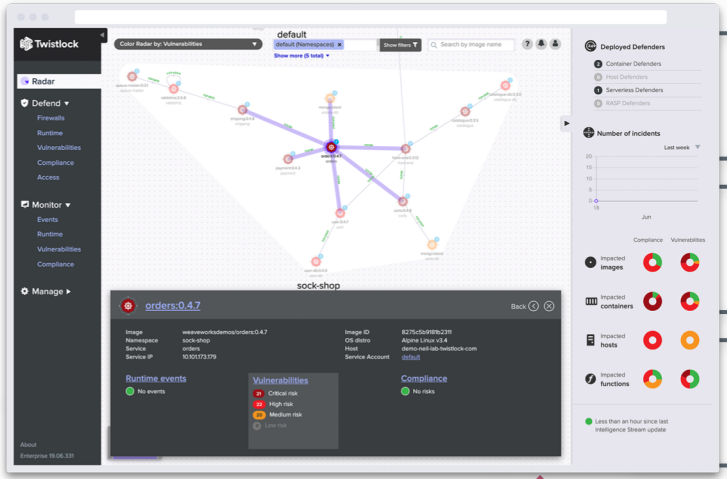




Prisma Cloud 아키텍쳐

Console

UI를 통해 정책을 정의하고 Twistlock 배포를 구성 및 제어하고 환경의 전반적인 상태를 확인할 수 있음



API

UI의 모든 클릭은 API를 통해 정보 제공

IAM

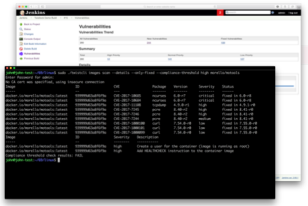
광범위한 엔터프라이즈 사용자 식별 지원

Alerting

티켓팅, SIEM 또는 각종 분석 틀링과 데이터 통합

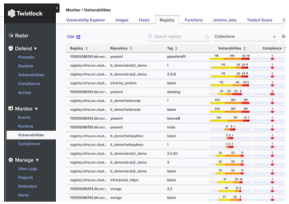
Intelligence Stream

30개 이상의 업스트림 소스에서 제공하는 최신 위협 인텔리전스



CI/CD

독립형 Jenkins 플러그인 지원 및 twistcli를 통한 통합



Registries & Repos

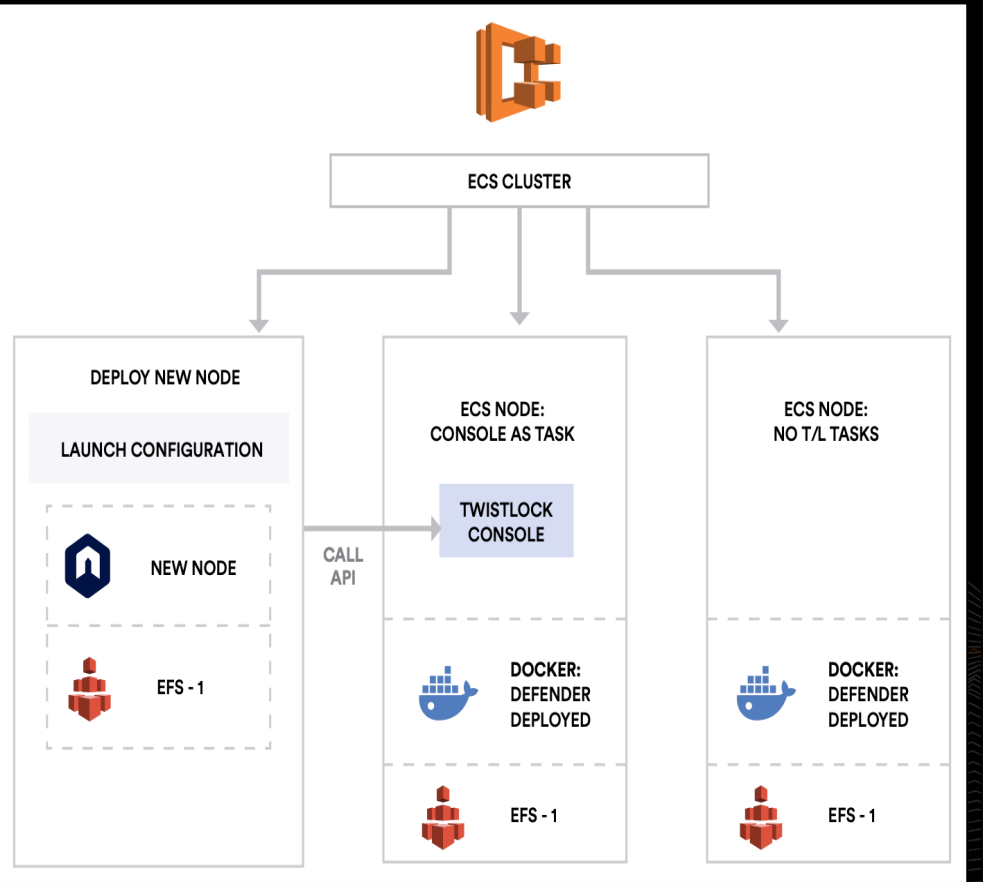
모든 Docker v2 레지스트리 또는 서버리스 저장소를 지원

Defenders

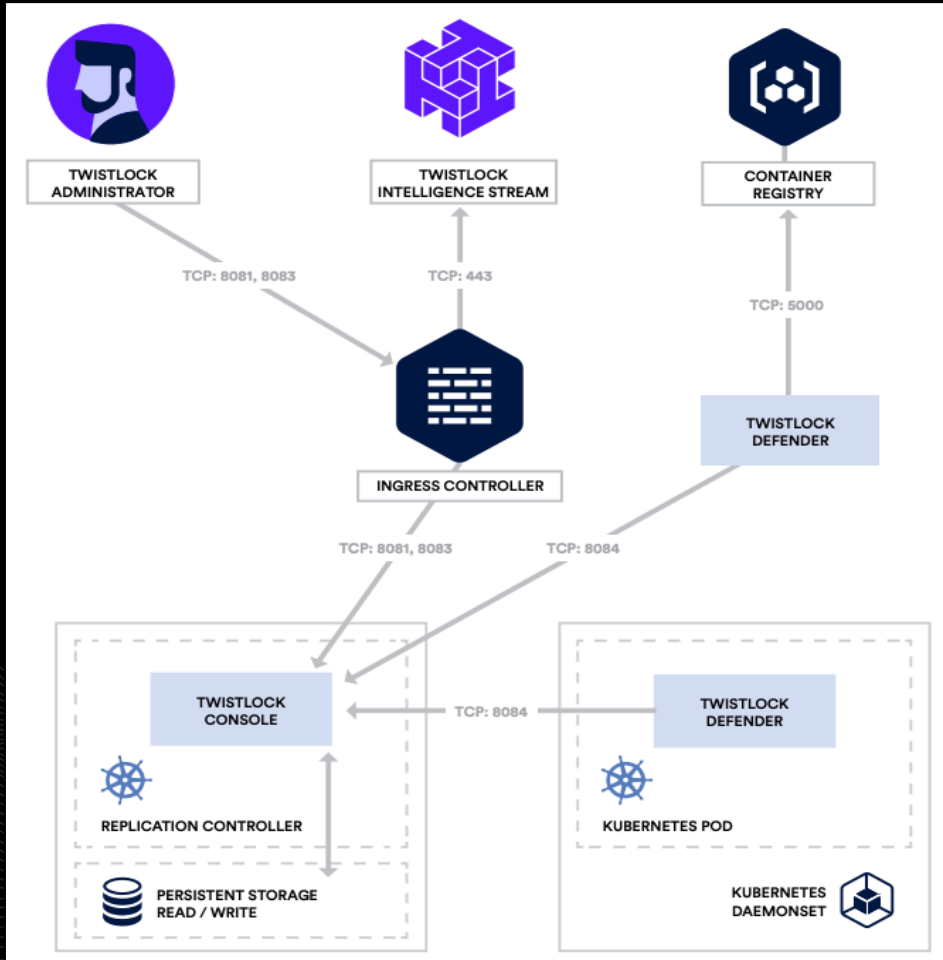
container runtime		
host OS	host OS	serverless / PaaS
metal / VM / IaaS	metal / VM / IaaS	cloud provider

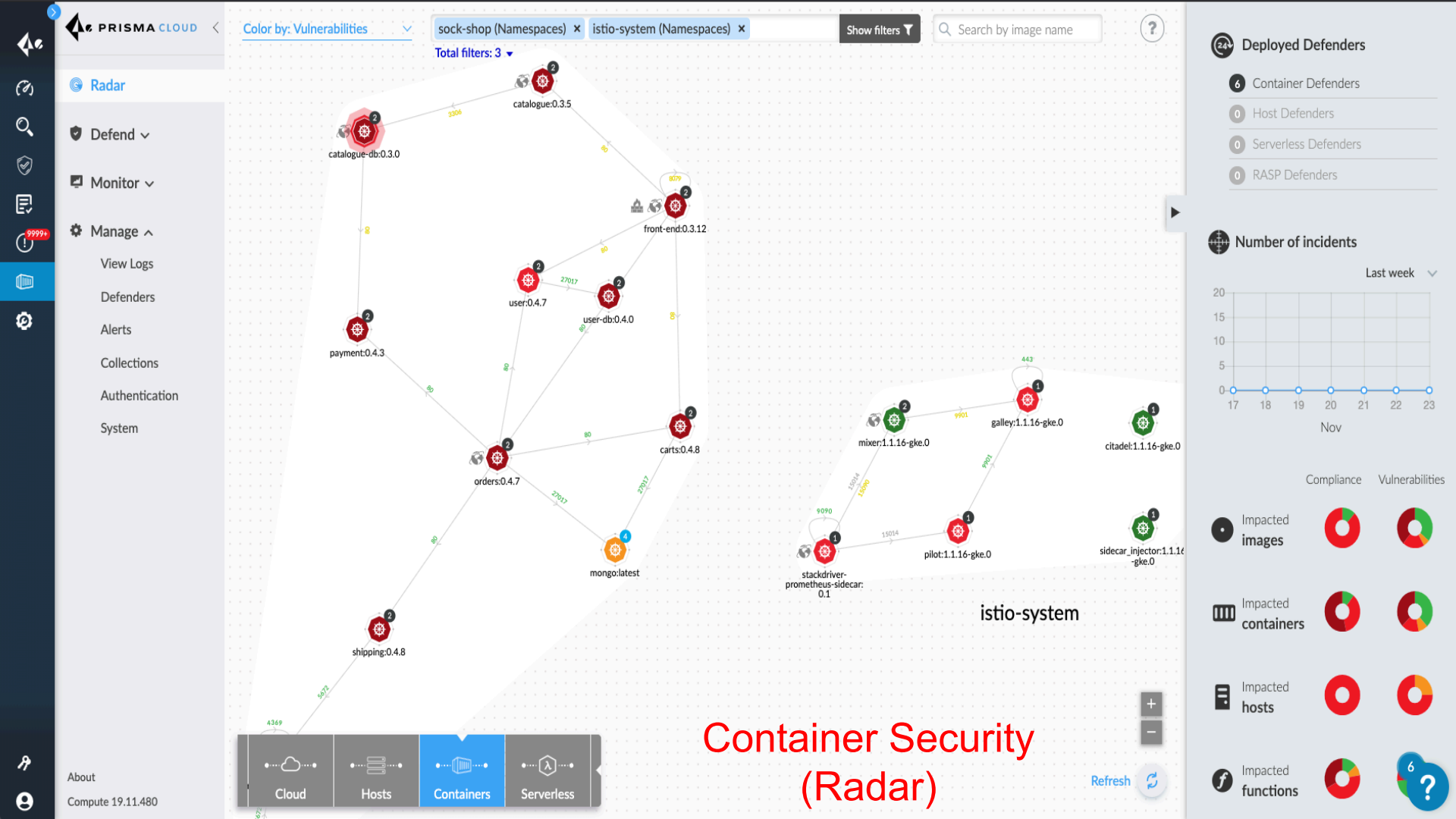
Prisma Cloud
: Container, Serverless Security
데모 화면

ECS Cluster



Kubernetes




PRISMA CLOUD
Color by: Vulnerabilities
sock-shop (Namespaces)
istio-system (Namespaces)
Show filters
Search by image name
Total filters: 3
Radar
Defend
Monitor
Manage
View Logs
Defenders
Alerts
Collections
Authentication
System
About
Compute 19.11.480
catalogue:0.3.5
catalogue-db:0.3.0
front-end:0.3.12
user:0.4.7
user-db:0.4.0
payment:0.4.3
carts:0.4.8
orders:0.4.7
mongo:latest
shipping:0.4.8
mixer:1.1.16-gke.0
galley:1.1.16-gke.0
citadel:1.1.16-gke.0
pilot:1.1.16-gke.0
sidecar_injector:1.1.16-gke.0
stackdriver-prometheus-sidecar:0.1
istio-system
Cloud
Hosts
Containers
Serverless
Refresh
Deployed Defenders
6 Container Defenders
0 Host Defenders
0 Serverless Defenders
0 RASP Defenders
Number of incidents
Last week
20
15
10
5
0
17
18
19
20
21
22
23
Nov
Compliance
Vulnerabilities
Impacted images
Impacted containers
Impacted hosts
Impacted functions
Container Security
(Radar)

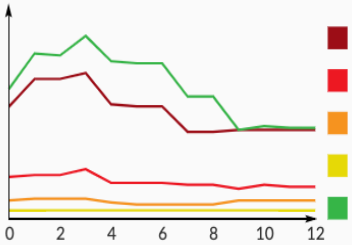
Vulnerabilities Explorer

Radar
Defend
Monitor
Events
Runtime
Vulnerabilities
Compliance
Manage

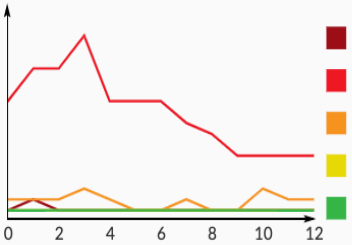
Refresh

Collections

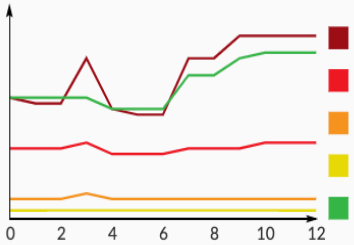
Impacted **containers** over time (30 days)



Impacted **hosts** over time (30 days)



Impacted **images** over time (30 days)



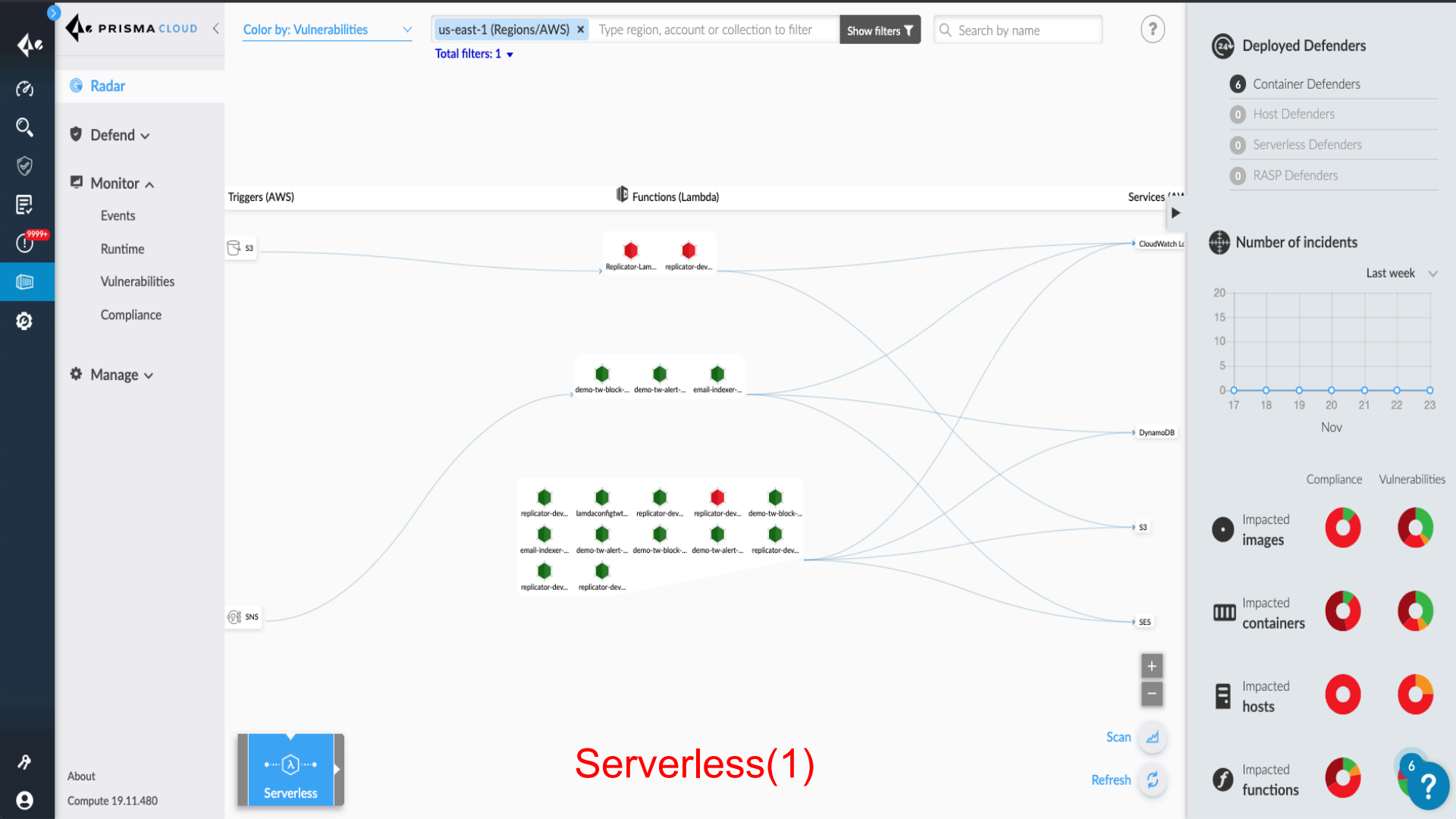
Top 10 most critical vulnerabilities (CVEs)

Images | Hosts

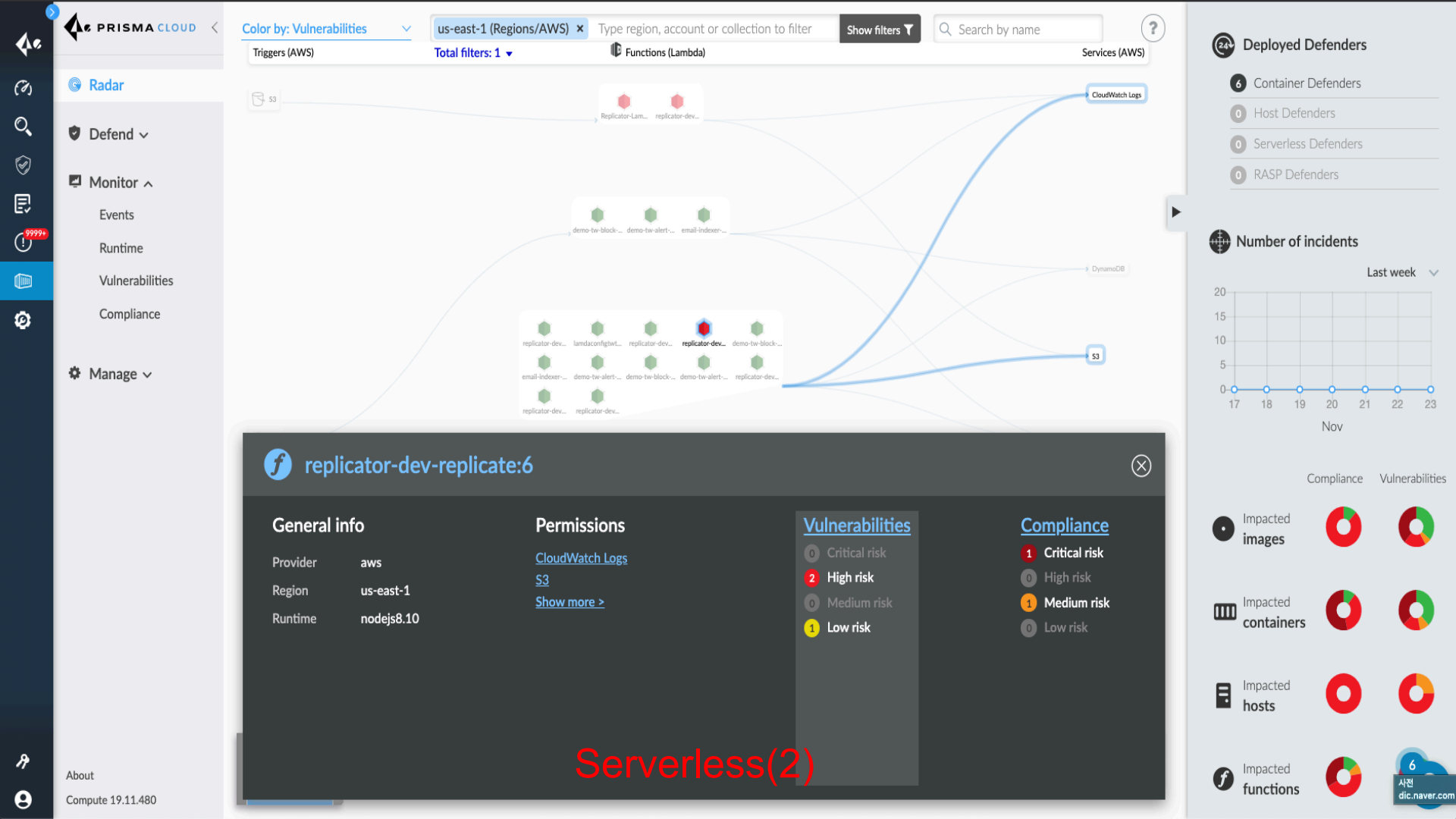
CSV

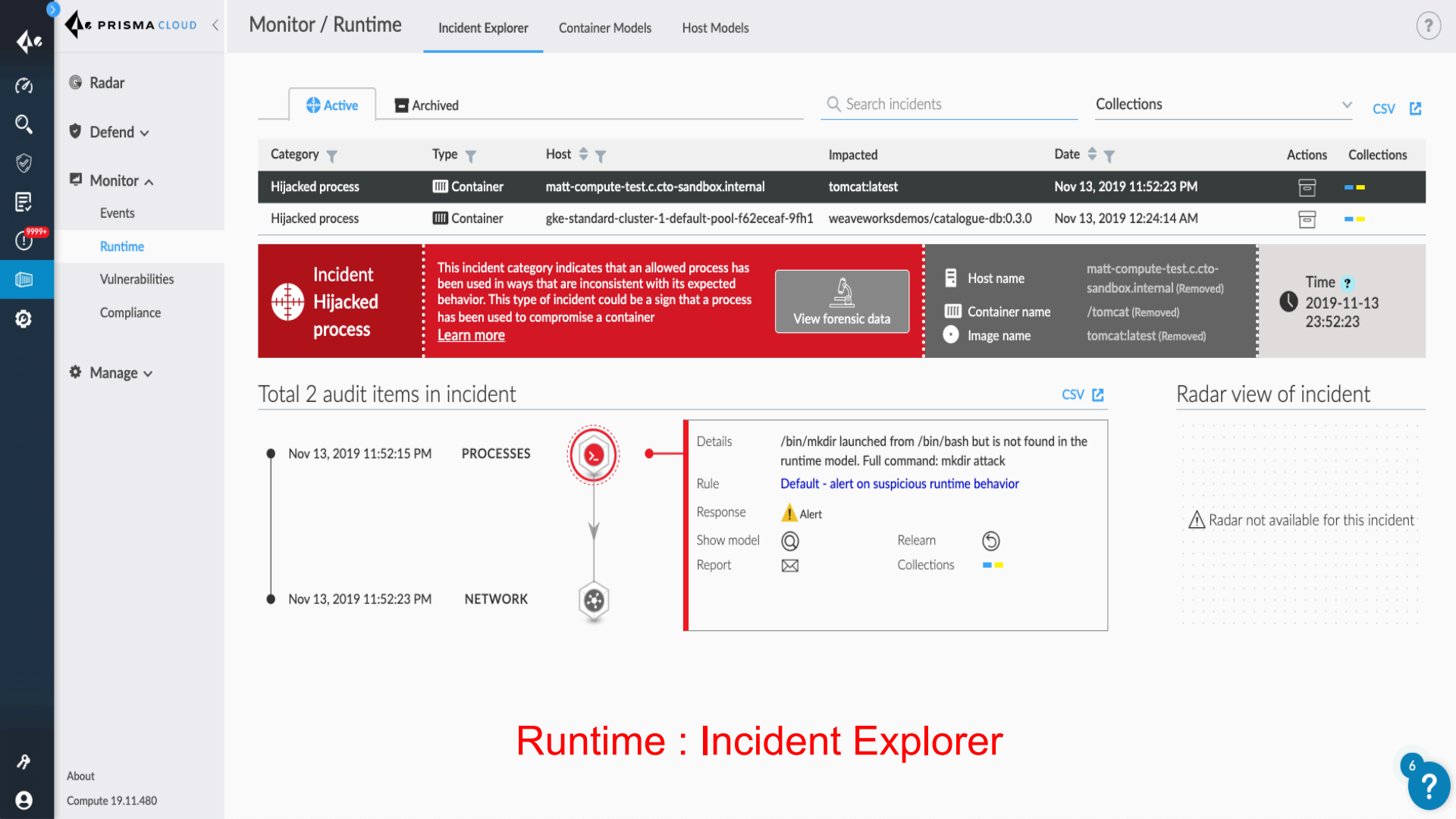
Search for specific CVEs

ID	Risk Score (0-100)	Risk Factors	Impacted Packages	Impacted Images
CVE-2018-14719	92	6	com.fasterxml.jackson.core_jackson-databind:2.8.6, com.fasterxml.jackson.core_jackson-databind:2.8.1	5.5%
CVE-2018-7489	92	6	com.fasterxml.jackson.core_jackson-databind:2.8.6, com.fasterxml.jackson.core_jackson-databind:2.8.1	5.5%
CVE-2019-14379	92	6	com.fasterxml.jackson.core_jackson-databind:2.8.6, com.fasterxml.jackson.core_jackson-databind:2.8.1	5.5%
CVE-2018-14718	92	6	com.fasterxml.jackson.core_jackson-databind:2.8.6, com.fasterxml.jackson.core_jackson-databind:2.8.1	5.5%
CVE-2017-17485	91	5	com.fasterxml.jackson.core_jackson-databind:2.8.1, com.fasterxml.jackson.core_jackson-databind:2.8.6	5.5%

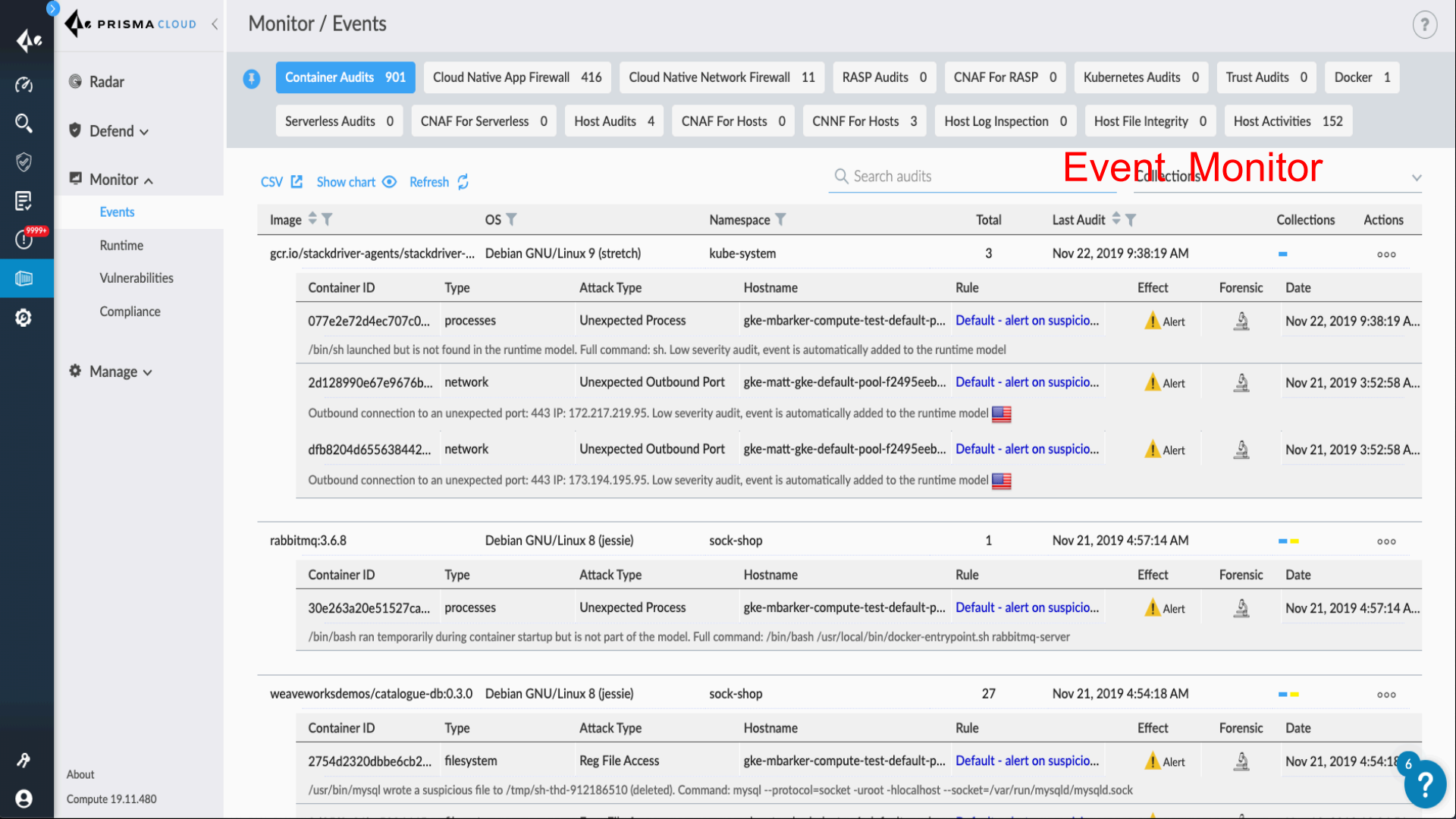


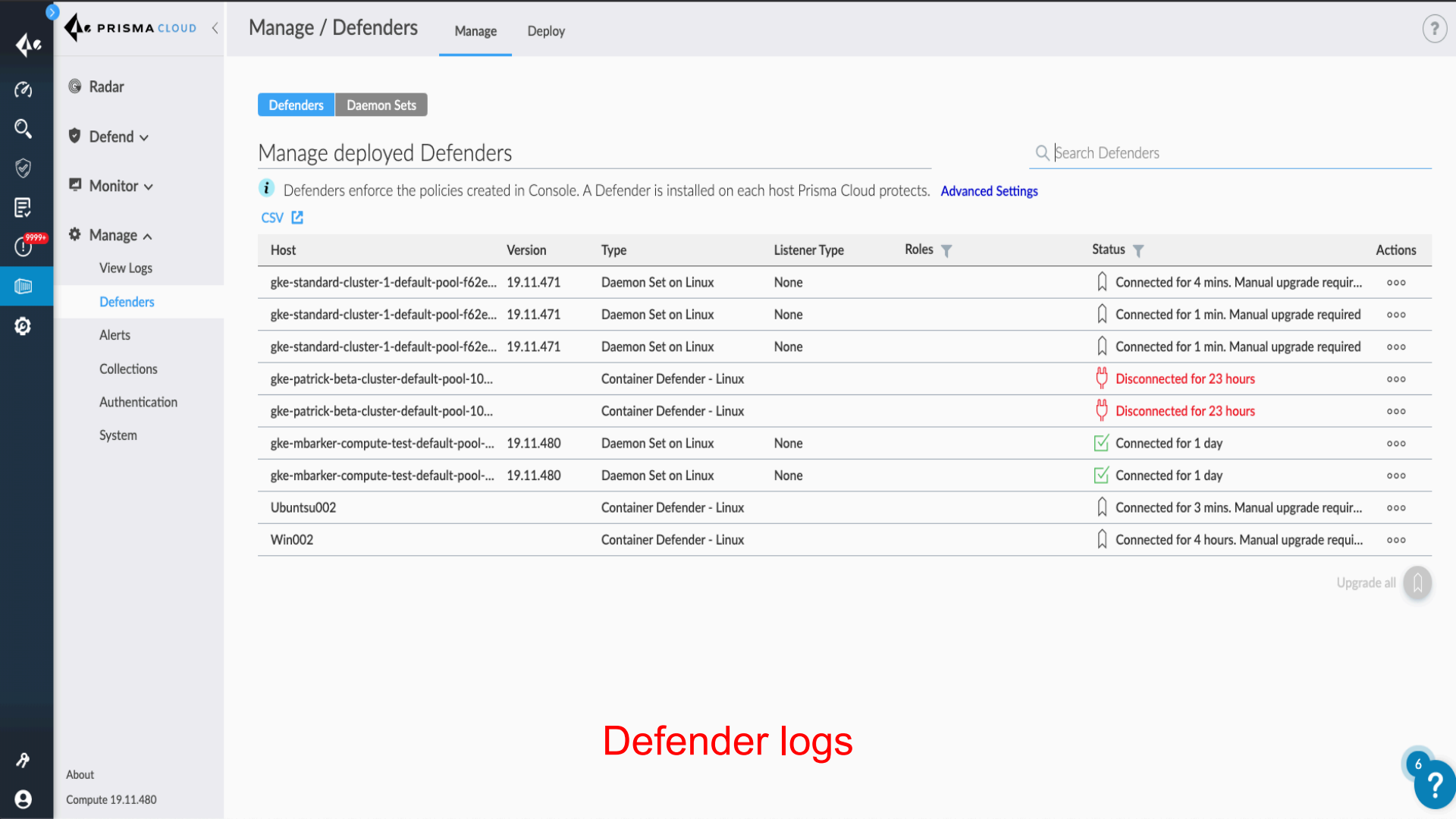
Serverless(1)


PRISMA CLOUD
Color by: Vulnerabilities
us-east-1 (Regions/AWS)
Type region, account or collection to filter
Show filters
Search by name
Triggers (AWS)
Total filters: 1
Functions (Lambda)
Services (AWS)
Radar
Defend
Monitor
Events
Runtime
Vulnerabilities
Compliance
Manage
About
Compute 19.11.480
CloudWatch Logs
DynamoDB
S3
replicator-dev-replicate:6
General info
Provider aws
Region us-east-1
Runtime nodejs8.10
Permissions
CloudWatch Logs
S3
Show more >
Vulnerabilities
0 Critical risk
2 High risk
0 Medium risk
1 Low risk
Compliance
1 Critical risk
0 High risk
1 Medium risk
0 Low risk
Serverless(2)
Deployed Defenders
6 Container Defenders
0 Host Defenders
0 Serverless Defenders
0 RASP Defenders
Number of incidents
Last week
20
15
10
5
0
17 18 19 20 21 22 23
Nov
Compliance
Vulnerabilities
Impacted images
Impacted containers
Impacted hosts
Impacted functions



Runtime : Incident Explorer


PRISMA CLOUD
Monitor / Events
Radar
Defend
Monitor
Events
Runtime
Vulnerabilities
Compliance
Manage
About
Compute 19.11.480
Container Audits 901
Cloud Native App Firewall 416
Cloud Native Network Firewall 11
RASP Audits 0
CNAF For RASP 0
Kubernetes Audits 0
Trust Audits 0
Docker 1
Serverless Audits 0
CNAF For Serverless 0
Host Audits 4
CNAF For Hosts 0
CNNF For Hosts 3
Host Log Inspection 0
Host File Integrity 0
Host Activities 152
CSV
Show chart
Refresh
Search audits
Collections
Event_Monitor
Image
OS
Namespace
Total
Last Audit
Collections
Actions
gcr.io/stackdriver-agents/stackdriver-...
Debian GNU/Linux 9 (stretch)
kube-system
3
Nov 22, 2019 9:38:19 AM
Container ID
Type
Attack Type
Hostname
Rule
Effect
Forensic
Date
077e2e72d4ec707c0...
processes
Unexpected Process
gke-mbarker-compute-test-default-p...
Default - alert on suspicio...
Alert
Nov 22, 2019 9:38:19 A...
/bin/sh launched but is not found in the runtime model. Full command: sh. Low severity audit, event is automatically added to the runtime model
2d128990e67e9676b...
network
Unexpected Outbound Port
gke-matt-gke-default-pool-f2495eeb...
Default - alert on suspicio...
Alert
Nov 21, 2019 3:52:58 A...
Outbound connection to an unexpected port: 443 IP: 172.217.219.95. Low severity audit, event is automatically added to the runtime model
dfb8204d655638442...
network
Unexpected Outbound Port
gke-matt-gke-default-pool-f2495eeb...
Default - alert on suspicio...
Alert
Nov 21, 2019 3:52:58 A...
Outbound connection to an unexpected port: 443 IP: 173.194.195.95. Low severity audit, event is automatically added to the runtime model
rabbitmq:3.6.8
Debian GNU/Linux 8 (jessie)
sock-shop
1
Nov 21, 2019 4:57:14 AM
Container ID
Type
Attack Type
Hostname
Rule
Effect
Forensic
Date
30e263a20e51527ca...
processes
Unexpected Process
gke-mbarker-compute-test-default-p...
Default - alert on suspicio...
Alert
Nov 21, 2019 4:57:14 A...
/bin/bash ran temporarily during container startup but is not part of the model. Full command: /bin/bash /usr/local/bin/docker-entrypoint.sh rabbitmq-server
weaveworksdemos/catalogue-db:0.3.0
Debian GNU/Linux 8 (jessie)
sock-shop
27
Nov 21, 2019 4:54:18 AM
Container ID
Type
Attack Type
Hostname
Rule
Effect
Forensic
Date
2754d2320dbbe6cb2...
filesystem
Reg File Access
gke-mbarker-compute-test-default-p...
Default - alert on suspicio...
Alert
Nov 21, 2019 4:54:18
/usr/bin/mysql wrote a suspicious file to /tmp/sh-thd-912186510 (deleted). Command: mysql --protocol=socket -uroot -hlocalhost --socket=/var/run/mysqld/mysqld.sock
6


PRISMA CLOUD
Manage / Defenders
Manage
Deploy
Radar
Defend
Monitor
Manage
View Logs
Defenders
Alerts
Collections
Authentication
System
About
Compute 19.11.480
Defenders
Daemon Sets
Manage deployed Defenders
Search Defenders
Defenders enforce the policies created in Console. A Defender is installed on each host Prisma Cloud protects.
Advanced Settings
CSV
Host
Version
Type
Listener Type
Roles
Status
Actions
gke-standard-cluster-1-default-pool-f62e... 19.11.471 Daemon Set on Linux None Connected for 4 mins. Manual upgrade requir...
gke-standard-cluster-1-default-pool-f62e... 19.11.471 Daemon Set on Linux None Connected for 1 min. Manual upgrade required
gke-standard-cluster-1-default-pool-f62e... 19.11.471 Daemon Set on Linux None Connected for 1 min. Manual upgrade required
gke-patrick-beta-cluster-default-pool-10... Container Defender - Linux Disconnected for 23 hours
gke-patrick-beta-cluster-default-pool-10... Container Defender - Linux Disconnected for 23 hours
gke-mbarker-compute-test-default-pool-... 19.11.480 Daemon Set on Linux None Connected for 1 day
gke-mbarker-compute-test-default-pool-... 19.11.480 Daemon Set on Linux None Connected for 1 day
Ubuntsu002 Container Defender - Linux Connected for 3 mins. Manual upgrade requir...
Win002 Container Defender - Linux Connected for 4 hours. Manual upgrade requi...
Upgrade all
Defender logs

Prisma Cloud : Compute License

PRISMA CLOUD

- Dashboard
- Investigate
- Policies
- Compliance
- Alerts 9999+
- Compute
- Settings
  - Cloud Accounts
  - Account Groups
  - Roles
  - Users
  - Access Keys
  - SSO
  - Integrations
  - IP Whitelisting
  - Licensing
  - Audit Logs
- Subscription
- Steve Kim

Licensing

Cloud Services | Compute

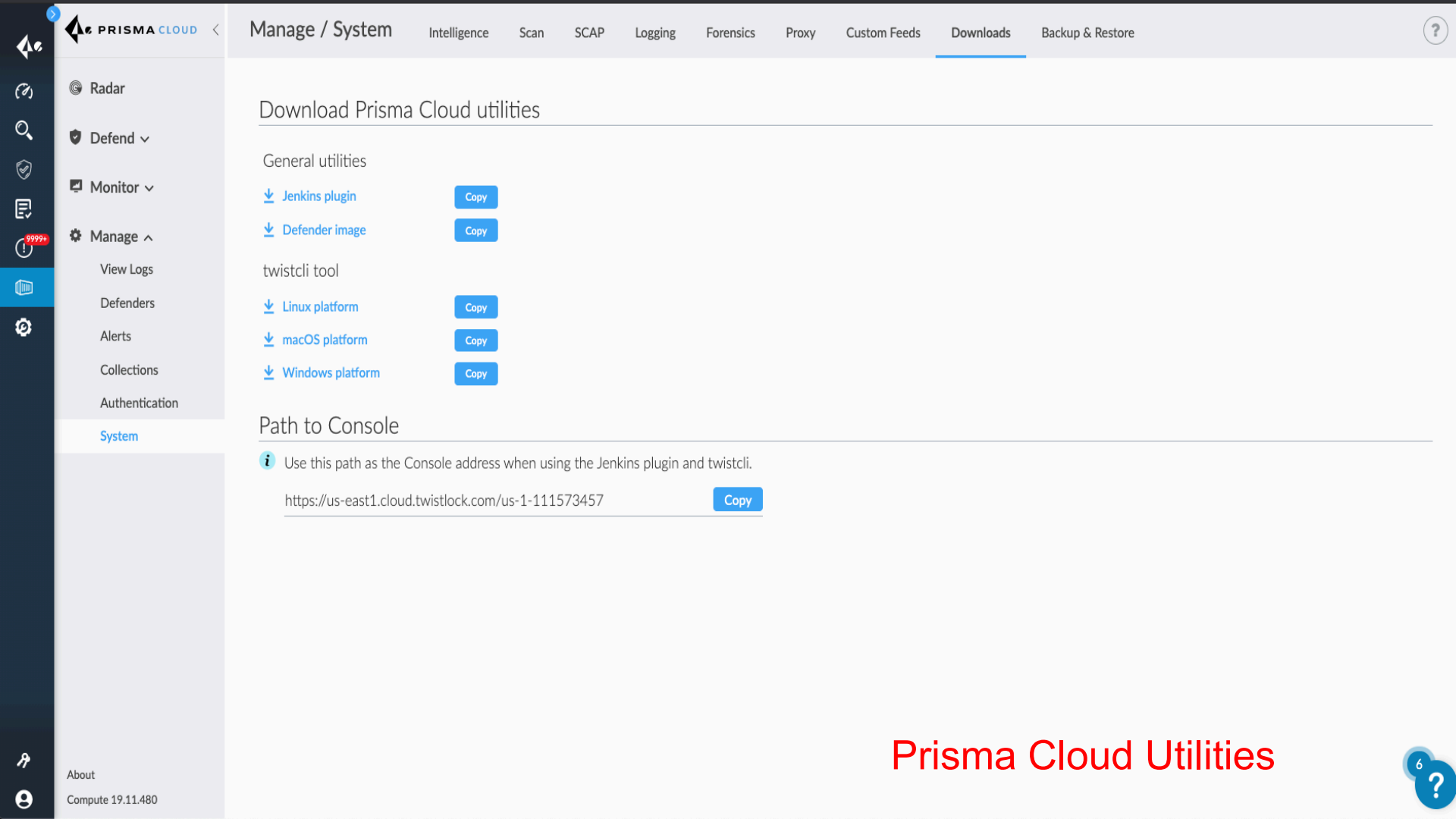
Time Range

Past 3 months

Resource Trend

Compute

TOTAL	CONTAINER WORKLOADS	SERVERLESS WORKLOADS
64	64	0


PRISMA CLOUD
Manage / System
Intelligence
Scan
SCAP
Logging
Forensics
Proxy
Custom Feeds
Downloads
Backup & Restore
Radar
Defend
Monitor
Manage
View Logs
Defenders
Alerts
Collections
Authentication
System
About
Compute 19.11.480
Download Prisma Cloud utilities
General utilities
Jenkins plugin
Copy
Defender image
Copy
twistcli tool
Linux platform
Copy
macOS platform
Copy
Windows platform
Copy
Path to Console
Use this path as the Console address when using the Jenkins plugin and twistcli.
https://us-east1.cloud.twistlock.com/us-1-111573457
Copy
Prisma Cloud Utilities

Prisma Cloud License 체계

“Workload” 정의

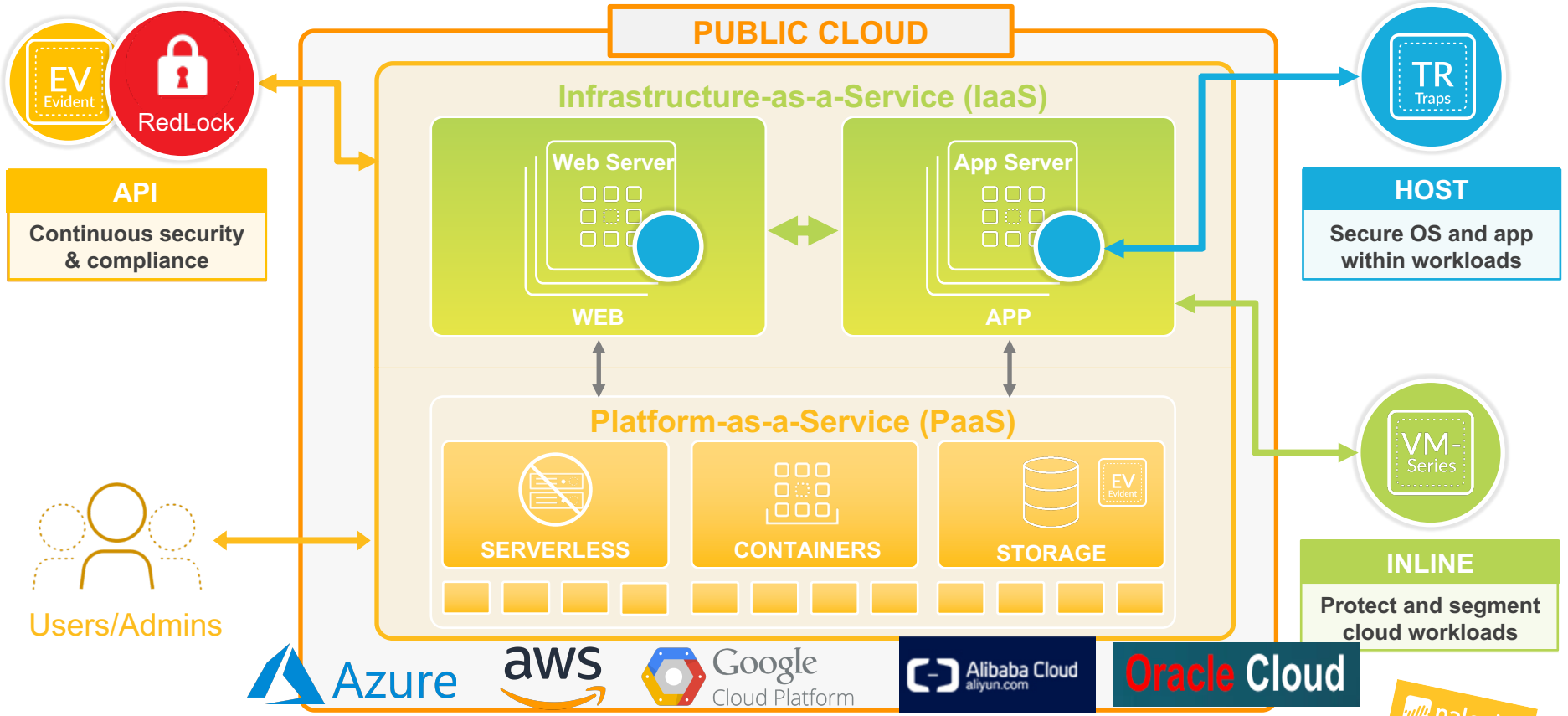
Table 1: Mapping Workloads to Common Public Cloud Resources	
1 Prisma Cloud workload	Every instance of these resources in an AWS account onboarded into Prisma Cloud: • EC2 • RDS • RedShift • DynamoDB • ALB & ELB (load balancers) • NAT gateways
	Every instance of these resources in an Azure subscription onboarded into Prisma Cloud: • Virtual machines • SQL databases • Load balancer • Application Gateway • Gateway

Table 1: Mapping Workloads to Common Public Cloud Resources (continued)	
1 Prisma Cloud workload	Every instance of these resources in a GCP project onboarded into Prisma Cloud: • Google Compute Engine (GCE) • Cloud SQL • Cloud Spanner • Load balancer • Cloud NAT
	Every host (not running containers) where a Prisma Cloud Defender is deployed
	Every Prisma Cloud Defender for container as a service (AWS Fargate, Azure Container Instance, Pivotal Cloud Factory, etc.)
	Every 12 million annual function executions (AWS Lambda, Azure Functions, Google Cloud Functions)
8 Prisma Cloud workloads	Every host (running containers) where a Prisma Cloud Defender is deployed

Prisma Cloud
보안 요약 정리

paloalto NETWORKS

결론 : 가장 완벽한 Public Cloud 보안을 위한 제안 1,2,3



 |

감사합니다.

stkim@paloaltonetworks.com