쿠버네티스에 대한 보안 위협, 어떻게 대응할 것인가?
Calico Honeypods 로 블루팀 구성하기

OSC Korea | 인재홍 이사
OSC Korea | 명건우 매니저

Contents

- OSC KOREA / TIGERA 회사소개
- OPENMSA 소개
- CNAPP/CSPM/CWPP란?(가트너)
- Calico 아키텍처 및 Features
- 데모 (허니팟/Flow Visualization/Dynamic 패킷캡쳐)

OSC KOREA SUMMARY

OSC Korea는 디지털 트랜스포메이션 전문 기업입니다.
고객보다 한발 앞서 미래를 준비하고, 고객에게 가장 필요한 서비스를 제공합니다.
최고의 솔루션 및 컨설팅, 구축 및 운영에 이르기까지 다양한 서비스를 고객사에 제공하고 있으며
고객의 디지털 전환과 아키텍처 현대화에 있어 가장 신뢰할 수 있는 파트너입니다.

한국 리눅스 재단 운영

리눅스재단(Linux Foundation)은 글로벌 최대 비영리 오픈소스 프로젝트 재단으로, 산하 Project* 의 국내 활성화와 생태계 조성을 위해 다양한 활동을 수행

* CNCF, Hyperledge, LF Edge 등

THE LINUX FOUNDATION

MSA 전문 기업

Kubernetes, Rancher, Kafka 등 주요 오픈소스 기술에 기반한 아키텍처 컨설팅 및 구축을 지원하고 다양한 MSA 방법론 (DDD, Event-Driven, Event Sourcing/CQRS)에 입각한 Modern Architecture 설계를 지원

RANCHER kubernetes kafka

글로벌 솔루션 공급

디지털 트랜스포메이션 과정에 필요한 글로벌 솔루션을 발굴하고 국내 전략적 파트너로 원천사와 협력하며, 고객 요구사항 및 시장 환경에 부합하는 최적의 솔루션을 통합 제공

INSTANA imply sonatype
Gremlin Auth0 kubecost

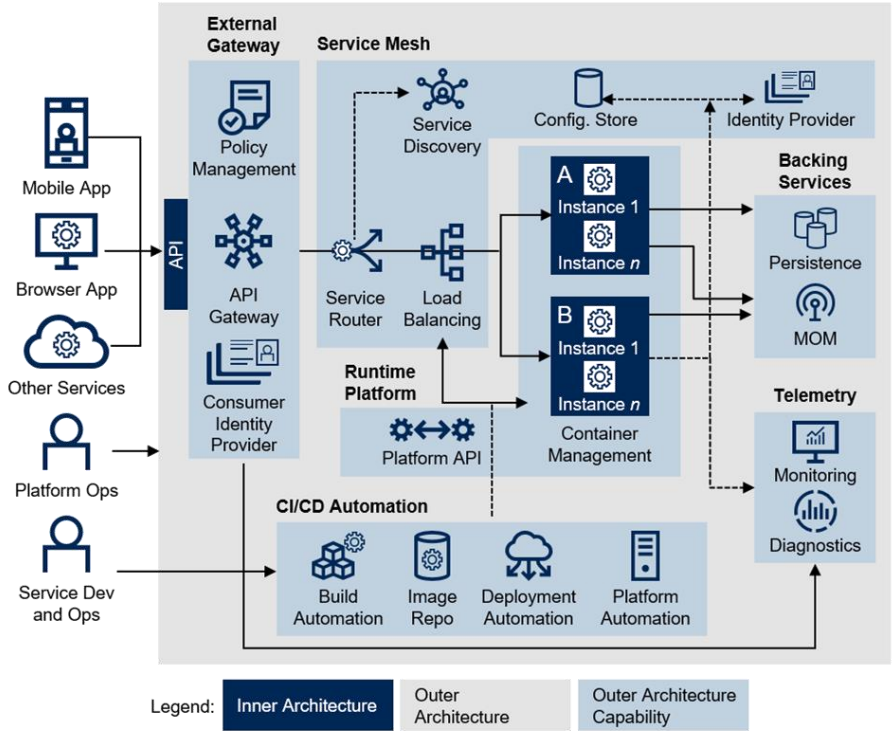
100% Opensource기반의 OpenMSA

- OpenMSA™ 소개

MSA (Micro Service Architecture)

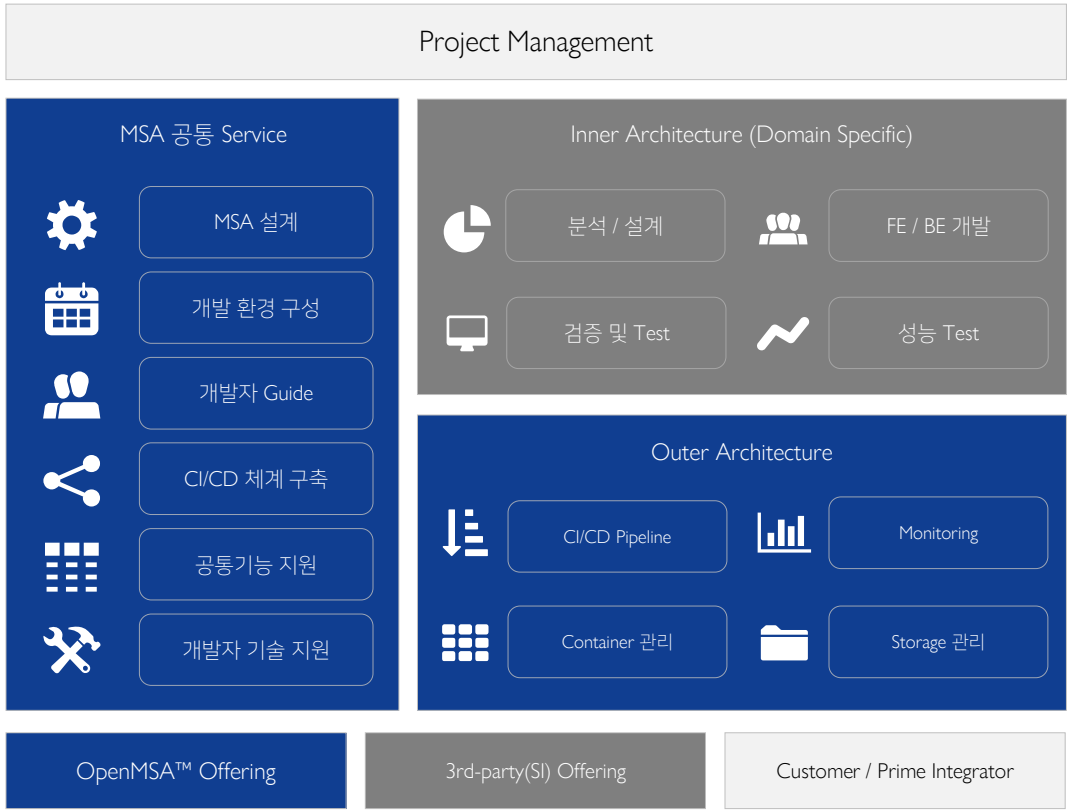
OSC에서 제공하는 OpenMSA™는 MSA 공통 Service와 Outer Architecture(DevOps, GitOps, DataOps, FinOps※, etc)에 대해
100% Opensource를 기반으로 자산화한 표준 MSA Framework으로, 산업별/Domain별 최적의 MSA 환경 제공

Microservice Architecture 구성 Guide by Gartner



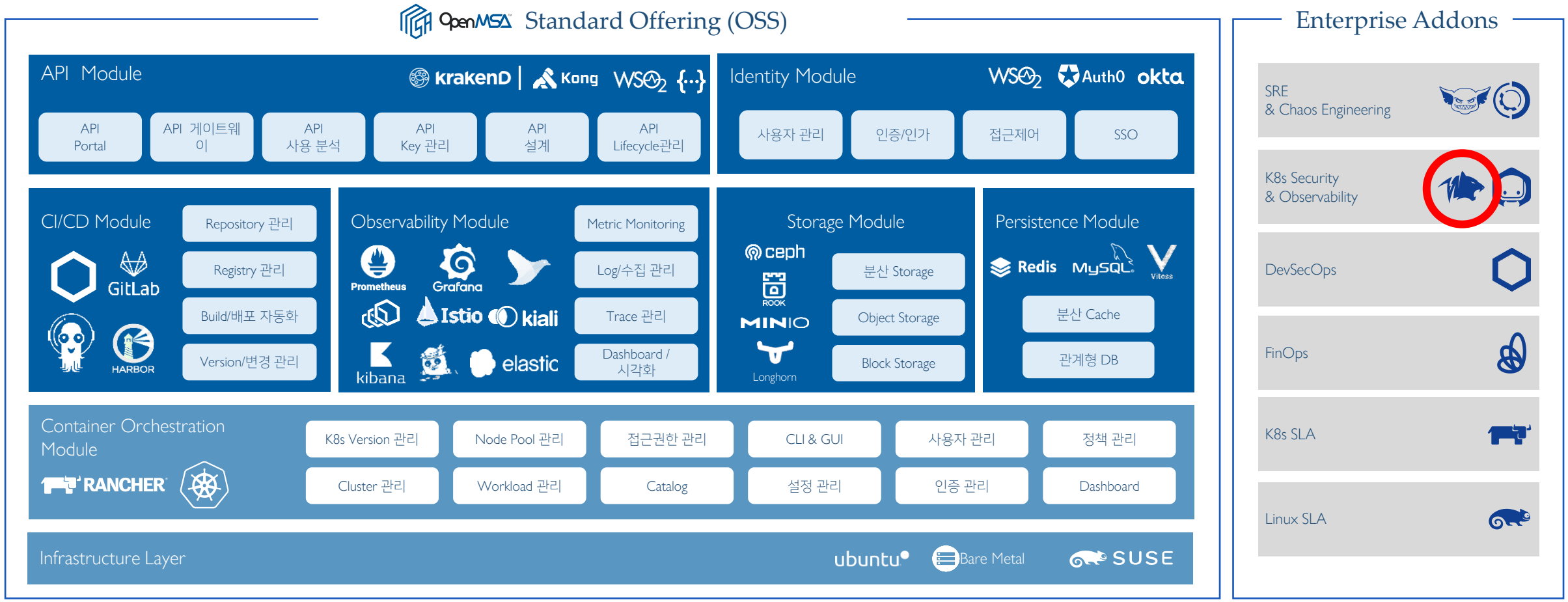
100% Opensource 기반으로 구체화한 Service Framework

Agile한 MSA 환경 구성(OpenMSA™)



100% Opensource기반의 OpenMSA (계속)

- OpenMSA™ 에서 제안하는 안정적인 MSA Outer Architecture 구성



TIGERA, K8S 보안 및 Observability 분야 리더

Kubernetes에서 가장 많이 사용되는 네트워크 및 보안 솔루션

오픈소스 Calico 창시자에 의해 2016년 설립

미국 샌프란시스코에 본사를 가지고 있으며 120명 이상의 직원들이 K8S 보안에 힘쓰고 있습니다.

전세계 고객사보유

글로벌 엔터프라이즈에서 SMB, 스타트업까지 다양한 고객사가 Calico를 사랑합니다

- 금융, Telco 사, 공공기관을 비롯한 다양한 산업군

K8S 네트워크 보안&Observability 업계표준

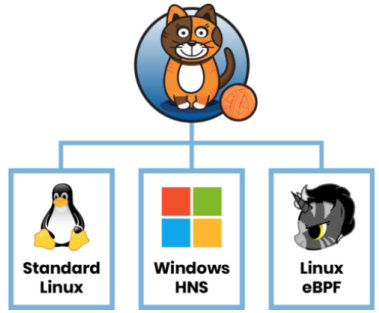
오늘도 Calico를 통해 다양한 어플리케이션에 안전하고 편리하게 접속합니다

By the inventors of Open Source Calico

Most Adopted Kubernetes Networking and Security Solution

10,000,000,000+	1,000,000+	250,000+	50,000+	166
Hours	Nodes	Clusters	Enterprises	Countries

Calico - Clear Winner Among All Tested CNIs



Kubernetes에서 가장 많이 사용되는 네트워크 및 보안 솔루션

CNI Benchmark August 2020 infraBuilder	Config	Performances (bandwidth)				Resources consumption (cpu/ram)					Security features			
	MTU	Pod to Pod		Pod to Service		Idle	Pod to Pod		Pod to Service		Network Policies		Encryption	
	setting	TCP	UDP	TCP	UDP	none	TCP	UDP	TCP	UDP	in	out	activation	Performance
Antrea	auto	Very fast	Very fast	Very fast	Slow	Low	Low	Low	Low	Low	yes	yes	at deploy time	Slow
Calico	manual	Very fast	Very fast	Very fast	Fast	Low	Very low	Very low	Very low	Very low	yes	yes	anytime	Very fast
Canal	manual	Very fast	Very fast	Very fast	Very fast	Low	Very low	Very low	Very low	Very low	yes	yes	no	n/a
Cilium	auto	Fast	Very fast	Very fast	Very fast	High	High	High	High	High	yes	yes	at deploy time	Slow
Flannel	auto	Very fast	Very fast	Very fast	Very fast	Very low	Very low	Very low	Very low	Very low	no	no	no	n/a
Kube-OVN	auto	Fast	Very slow	Fast	Very slow	High	High	High	High	High	yes	yes	no	n/a
Kube-router	none	Slow	Very slow	Slow	Very slow	Low	Very low	Low	Very low	Low	yes	yes	no	n/a
Weave Net	manual	Very fast	Very fast	Very fast	Fast	Very low	Low	Low	Low	Low	yes	yes	at deploy time	Slow

The exceptional performance of Calico encryption was described as having the “real wow effect” among all of the CNI comparisons. Strong network security should not come with a performance penalty. In the benchmark test with encryption enabled, Calico performed 6x faster than any other solution in the market!

Calico supports native Linux (based on iptables), eBPF for modern Linux kernels, and Windows HNS, No matter which dataplane you choose, Calico delivers blazing fast performance and exceptional scalability, as the latest benchmark tests confirm.

TIGERA: Leader in Kubernetes Security & Observability

TIGERA

- Inventor and maintainer of Project Calico
  - Most adopted opensource Kubernetes networking & security solution
  - 1.5+ Million nodes in 166 countries
- Customers include
  - Fortune 500
  - 금융회사
  - Cloud-native 회사
  - Telcos 및 대형 e-Commerce

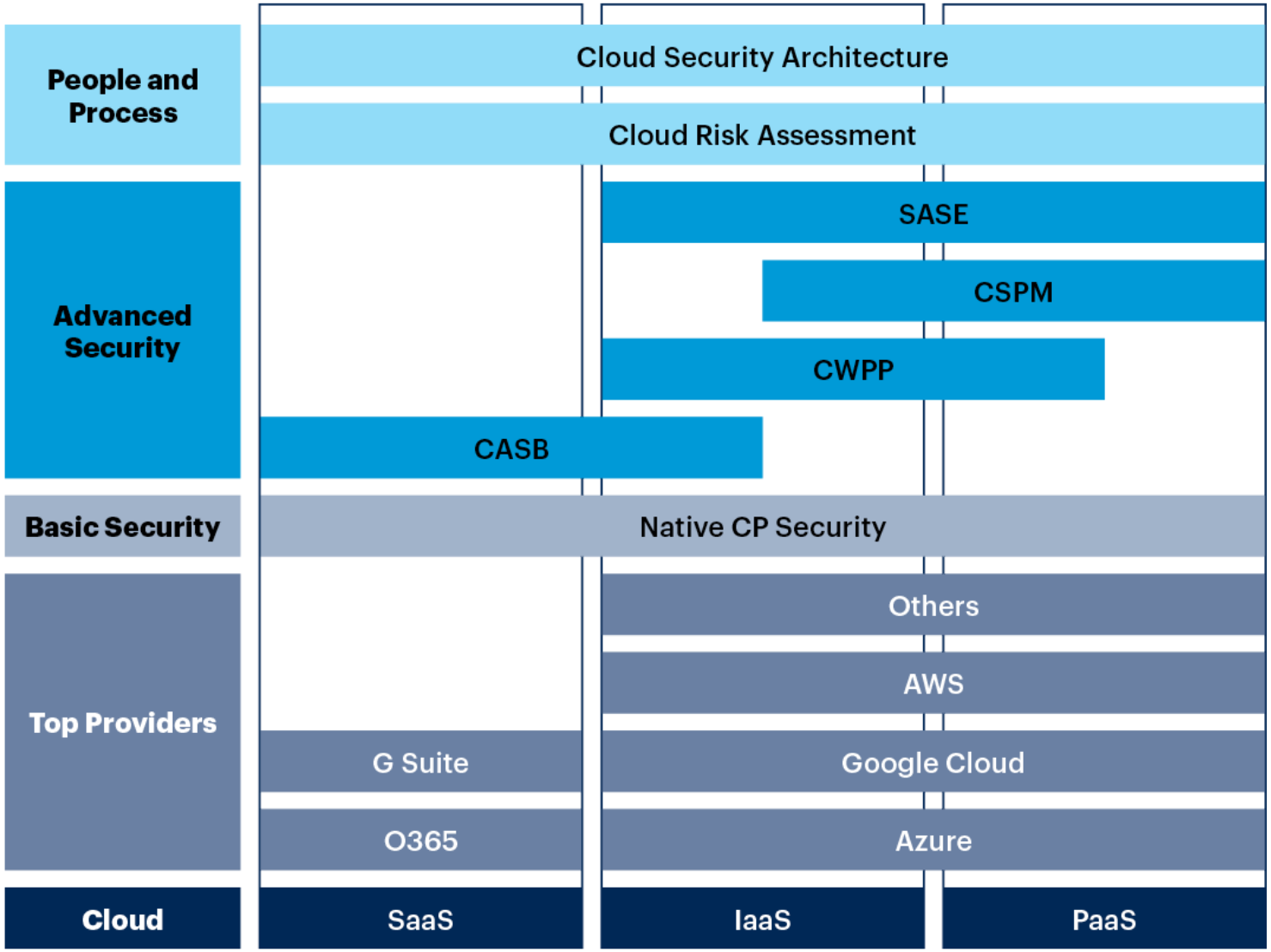
Customers

Bloomberg, AT&T, Morgan Stanley, VISA, DISCOVER, Bell, JPMorganChase, fiserv., mastercard, RBC, Allstate, Ford, box, MARSH & McLENNAN COMPANIES, MERCK, amadeus

Tech. Partners

aws, Azure, Google Cloud, IBM Cloud, RANCHER, OPENSHIFT, MIRANTIS, D2IQ, FORTINET

GTP Cloud Security Core Topic Coverage



Source: Gartner
720923_C

CSPM

Cloud Security Posture Management

Compliance 또는 기업 보안 정책에 따라 클라우드 인프라의 위험요소를 예방, 탐지 대응 및 예측하여 클라우드 위험을 지속적으로 관리하는 솔루션

CSPM is external, looking for cloud misconfigurations and compliance violations.

CWPP

Cloud Workload Protection Platform

Private 및 하이브리드 클라우드 내의 모든 워크로드(Workload) 에 대해 워크로드 전 수명주기 걸쳐 실시간 대응 보호 위한 플랫폼

CWPP is internal, looking for threats inside the software that runs in the cloud.

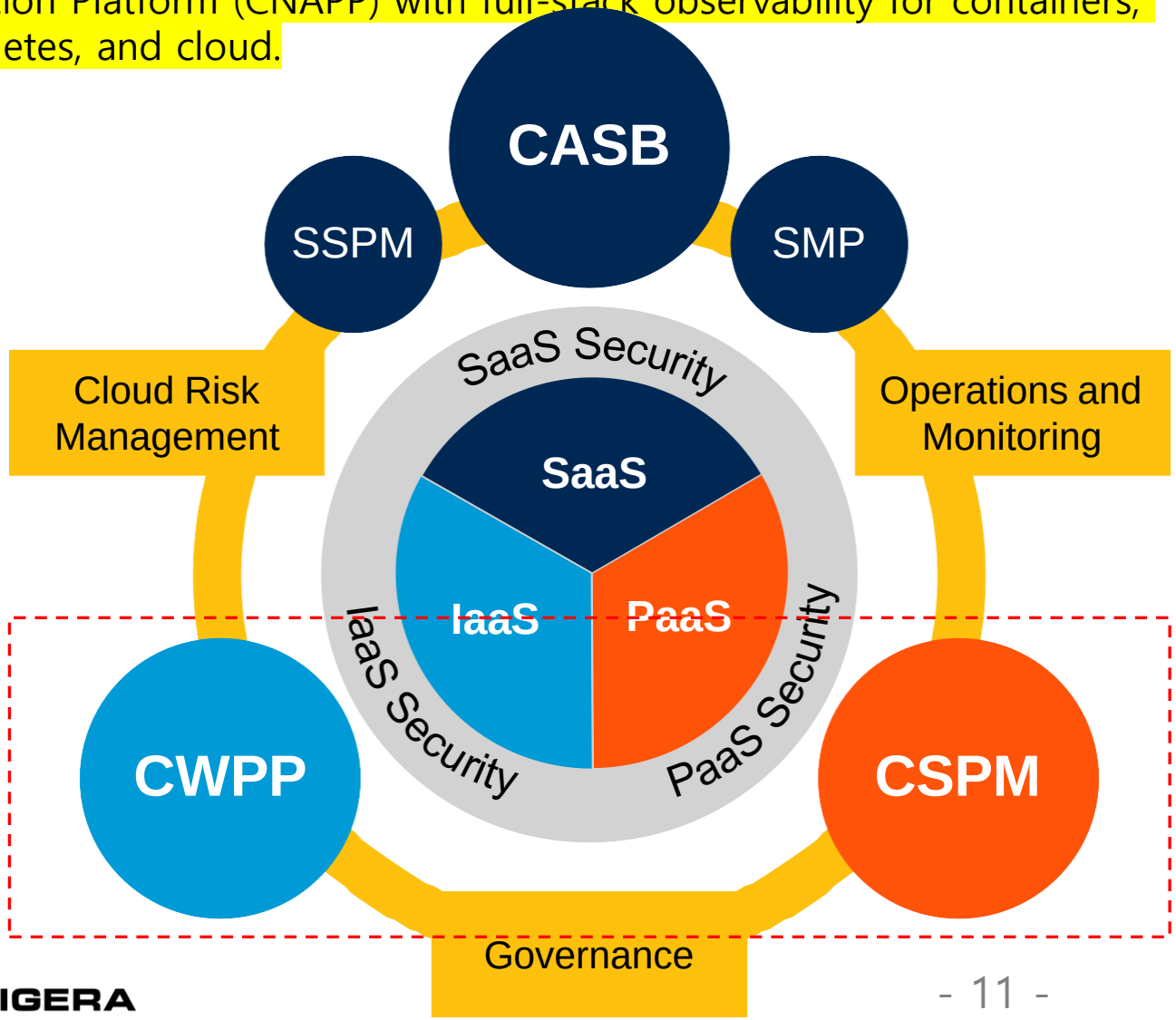
CNAPP

Cloud Native Application Protection Platform

Cloud Native Application 의 최적의 보안을 위해서는 개발 단계에서 시작하여 런타임 보호로 확장되는 통합적인 보안 접근 방식이 필요합니다.

새로운 범주의 보안 플랫폼인 CNAPP형태로 변모중

Calico Cloud - The industry's only active Cloud-Native Application Protection Platform (CNAPP) with full-stack observability for containers, Kubernetes, and cloud.



What's Next — Third-Party Tools

- **CASB** — Cloud Access Security Broker
- **CWPP** — Cloud Workload Protection Platform
- **CSPM** — Cloud Security Posture Management
- **SSPM —** SaaS Security Posture Management
- **SMP** — SaaS Management Platform
- **CNAPP** — Cloud-Native Application Protection Platform

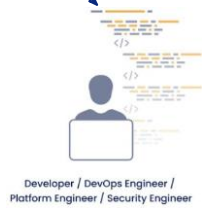
Cloud-Native Application Attack Vectors

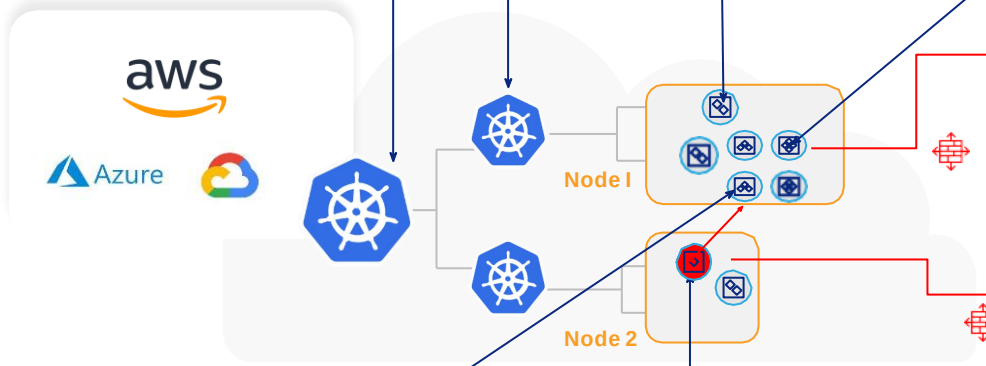
Deploy time threats in environment
3. Misconfigurations in environment

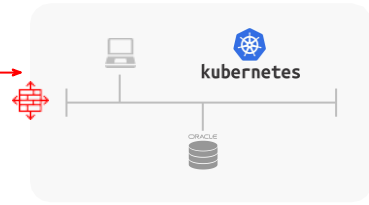
Runtime threats in workloads
4. Vulnerabilities, Malware

Build time threats in containers
2. Misconfigurations in images

Data-exfiltration threat
5. Lack of granular egress access control







Build time threats in containers
1. Vulnerabilities and threats in images

Threats from unauthorized access
6. Lack of integration with firewall

Threats from Malware and Ransomware
8. Lateral movements of APTs

Zero-day threats
7. Compromises and Zero-Day threats go undetected

주요 Use Cases & Features

Egress Access Control

클러스터 외부(DB, SaaS, Data Center등) 와 POD 수준의 안전한 연결 지원

Visibility and Troubleshooting

K8s 환경의 Connection 이슈를 시각화하고 Flow를 추적하여 쉽게 문제 분석

Enterprise Security Controls

K8s 환경에 엔터프라이즈 보안 정책을 적용하고 Compliance 모니터링

Extend Firewalls to Kubernetes

기존 방화벽 정책을 K8s 와 연계하여 단일 정책을 통해 보안정책 통합 운영

Zero Trust Security

워크로드 인증, 인가 및 최소권한 부여 등 심층 보안 구현

Intrusion Detection (IDS)

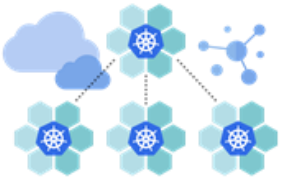
K8s 환경의 IDS 지원으로 비정상행위를 모니터링 하고 Alert, 격리 지원

Cloud Micro-segmentation

호스트 및 컨테이너가 정적/동적으로 복합된 환경에서 일원화된 Segmentation 정책 적용

Self-Service Security

팀원이 각자 자동으로 보안정책을 코드로 생성하여 안전하게 서비스 활용



Unified Control

Multi-Cluster, Multi-Cloud 및 Hybrid Cloud에 걸쳐 통합된 네트워크 보안 제공

주요 Use Cases & Features

Application Layer Observability

어플리케이션 수준(Layer 7)의 관측가능성을 Service Mesh 없이 제공

DNS Policy & Dashboard

안전한 외부 리소스 접근 방식을 제공하며 세부 DNS 관련 정보를 제공

Policy Tiers

계층별 정책 설정 및 적용으로 일관된 정책을 쉽게 수립

Dynamic Service Graph

서비스간 의존성을 쉽게 확인할 수 있는 시각화 도구를 통해 각종 메타 데이터 확인

AWS Security Groups Integration

인스턴스 수준의 보안그룹을 POD 수준의 정책으로 확장 적용

Dynamic Packet Capture

POD 수준에서 필요한 트래픽을 쉽게 캡처

Host, Container/VM & Application protection

컨테이너는 물론 VM 및 호스트 수준의 어플리케이션 보호기능 제공

Data-in-Transit Encryption

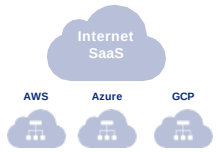
낮은 CPU 점유율로 향상된 성능을 제공하는 WireGuard 암호화엔진 사용

Flow Visualizer

플로우 로그를 시각화 하여 성능관리 및 문제분석에 활용

Why Tigera? Calico Enterprise/Cloud

Reduce Attack Surface with Zero-Trust



- Zero-trust workload access
- Identity-aware micro-segmentation for workloads
- Universal Firewall integration
- Envoy-based Application Level Security
- Network encryption (Wireguard)

Detect known and unknown threats

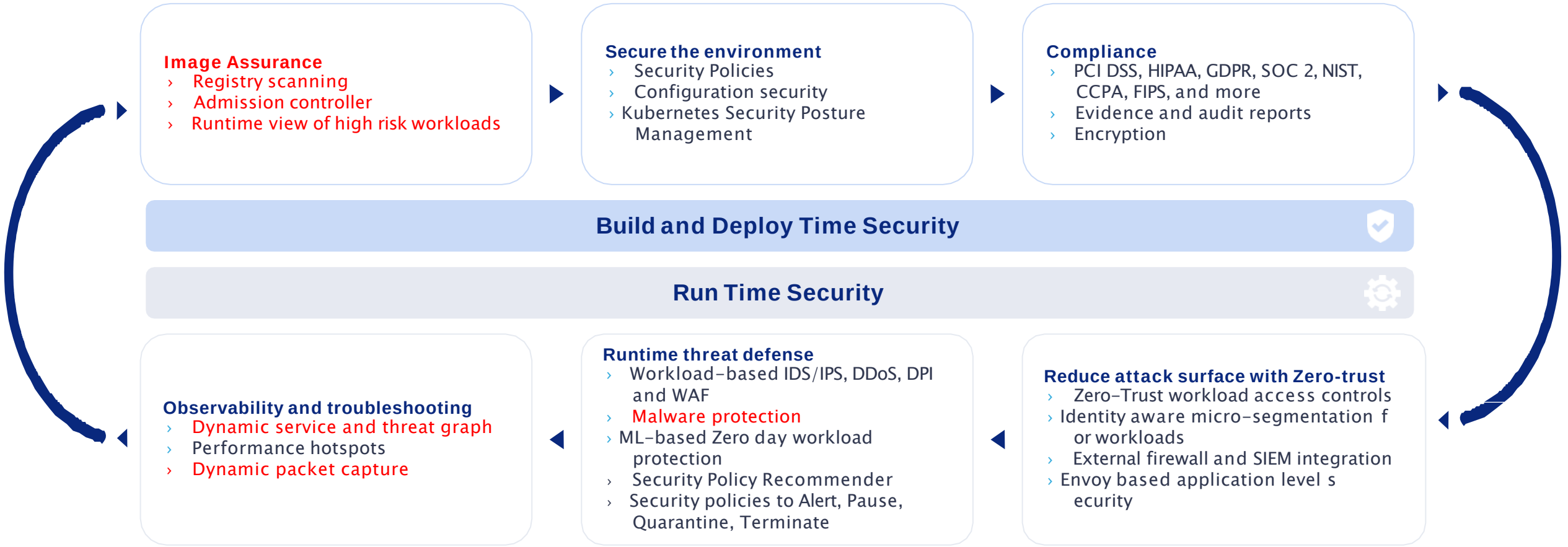
- Protect workloads from container and network based threats
- Workload based WAF, IDS/IPS with Deep packet inspection
- ML-based Zero-day workload threat identification
- Vulnerabilities and Malware protection
- Honeypods

Automatic risk mitigation

- Dynamic Service and Threat Graph
- Security policy recommender
- Admission Controller
- Alert, Pause, Quarantine, Terminate

ACTIVE BUILD AND RUNTIME SECURITY

Calico Cloud - Features at a Glance



Unified Controls **Multi-Cluster** **Multi-Cloud** **Hybrid Cloud**

TIGERA

OSC

Choose Calico for a cloud-native networking and security solution that is easy to deploy, operate and support compared to traditional offerings.

K8S 시스템(Kubeadm, EKS) 를 통한 네트워크 Segmentation, Access Control 등
기존 시스템에서는 지원하지 않는 부분은 Calico Cloud 를 통해서,
유럽 보안 표준 지침을 준수하고, 손쉬운 문제분석 가능

BACKGROUND

런던증시에 상장된 Gambling 소프트웨어 개발 회사 - Playtech

유로존에 B2B, B2C 서비스 제공

VMWARE 기반 K8S (KubeADM) 과 AWS EKS (~100노드) 운영중

기존 Check Point 방화벽이 K8S Segmentation 및 Access Control 제어 불가

SOLUTIONS

정책기반 라이프사이클 관리(추천/프리뷰/감사/스테이지)

UI를 통한 네트워크 Access Control정책적용

Flows 로그, 서비스 그래프를 통한 K8S 내의 서비스 트래픽 패턴 이해, 분석, 네트워크 가시성 확보

Dynamic 패킷 캡쳐를 통한 손쉬운 문제 분석

OUTCOMES

GDPR, PCI 및 유럽내에 보안 표준 규정 준수

Segmentation 과 Access Control, 트래픽 모니터링

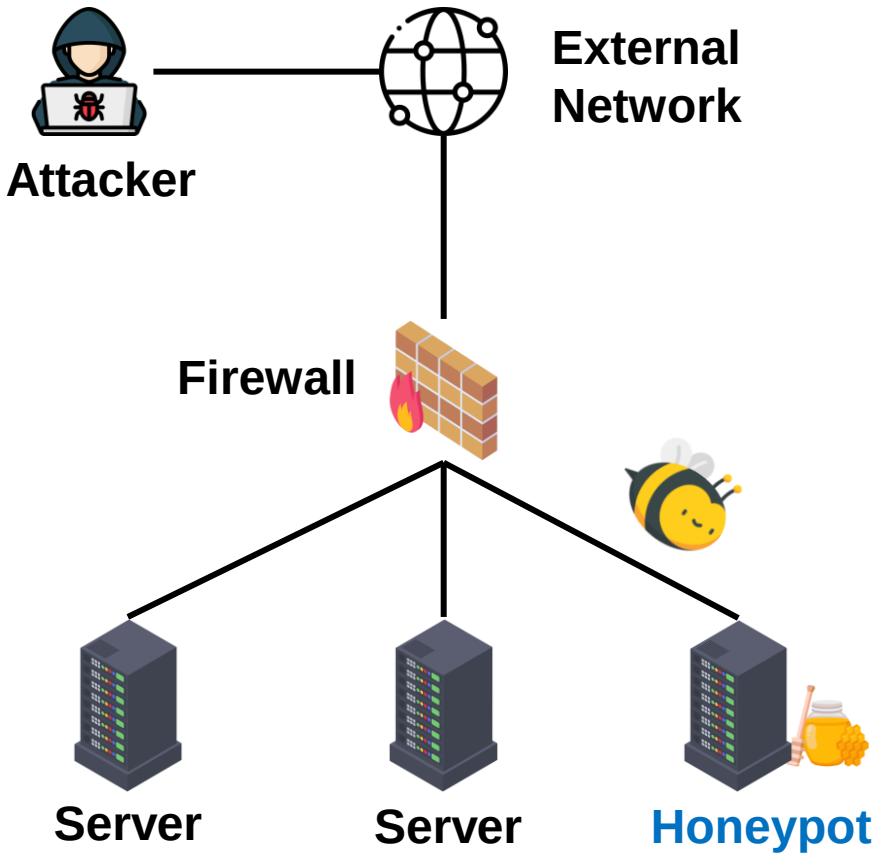
클라우드 워크로드 보호

Honeypod /Flow Visualization /Dynamic Packet Capture Demo

Intrusion Detection and Prevention

Honeypot

- 1990년대 중반 MIT 교수 David Clock의 제안으로 등장
- 비정상적인 접근을 탐지, 대응하기 위해 의도적으로 취약한 시스템을 운영
- Honeypot에 접근 발생시 알림을 통해 보안팀이 공격자의 침입 사실을 초기에 인식 및 대응할 수 있도록 함
- 공격자가 Honeypot을 공략하도록 하여 실제 서비스를 보호하고, 공격에 대응할 시간을 확보



Honeypod 데모

- Honeypod는 Honeypot의 concept을 채용하여 비정상적인 접근을 탐지, 대응하기 위해 의도적으로 배포된 취약한 pod
- Tigera calico에서 제공하는 template을 통해 하나의 서비스처럼 구성 된 Honeypod 세트를 손쉽게 클러스터에 배포 및 Alert 설정 가능
- 미리 설정된 alert 규칙에 의해 Honeypod에 대한 접근 발생시 Calico Cloud 대시보드의 Alert을 통해 탐지 가능

[Honeypod] Pod subnet port scan by default/victim-759698dbc4-*

Severity	100
Origin	honeypod.port.scan
Source IP	N/A
Source port	N/A
Source namespace	default
Source name	N/A
Source name aggregation	victim-759698dbc4-*
Destination IP	N/A
Destination port	N/A
Destination namespace	tigera-internal
Destination name	N/A
Destination name aggregation	tigera-internal-app-*
Host	N/A

Record

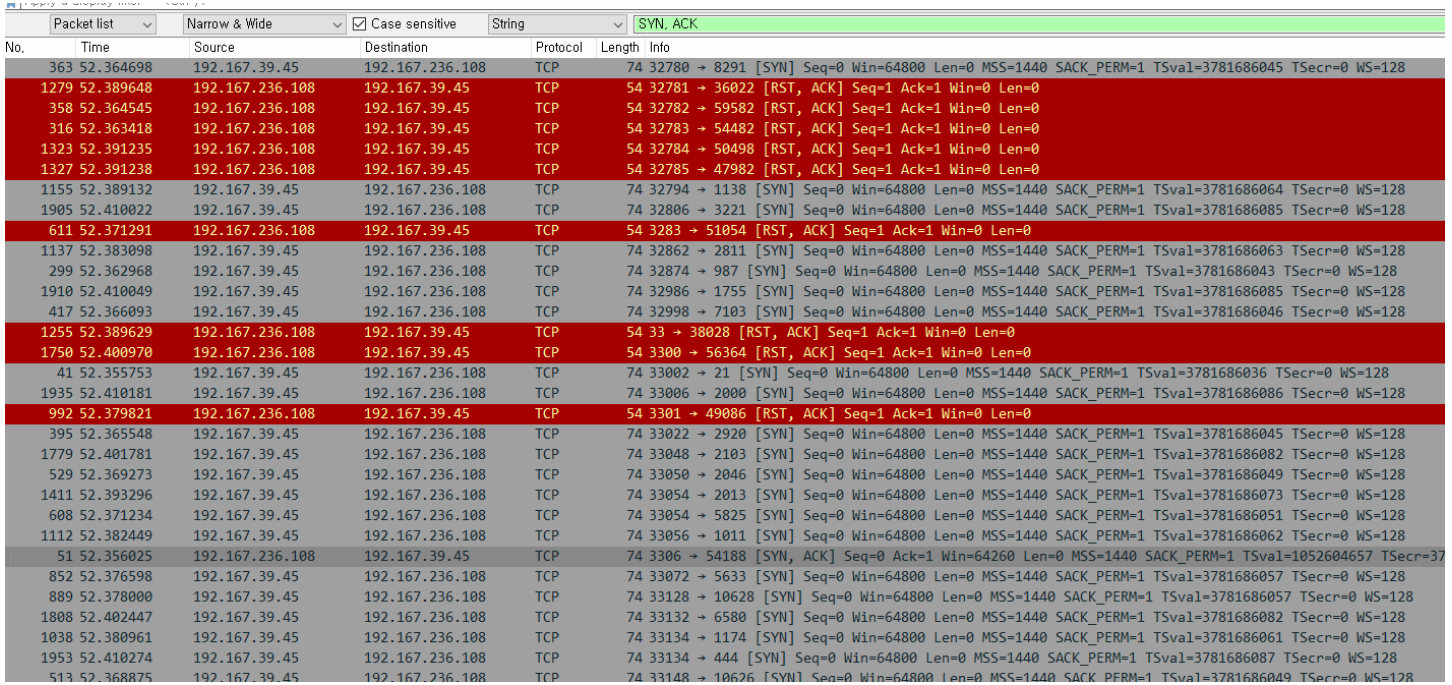

```
{
    "count": 1002,
    "dest_name_aggr": "tigera-internal-app-*",
    "dest_namespace": "tigera-internal",
    "host.keyword": "master-1",
    "source_name_aggr": "victim-759698dbc4-*",
    "source_namespace": "default"
}
```


결과 :가짜 POD로 오는 트래픽은 분석을 통해 알려진 Malware 인지 탐지 하며,

좀 더 안정적인 시스템운영을 가능

Honeypod with Dynamic Packet Capture

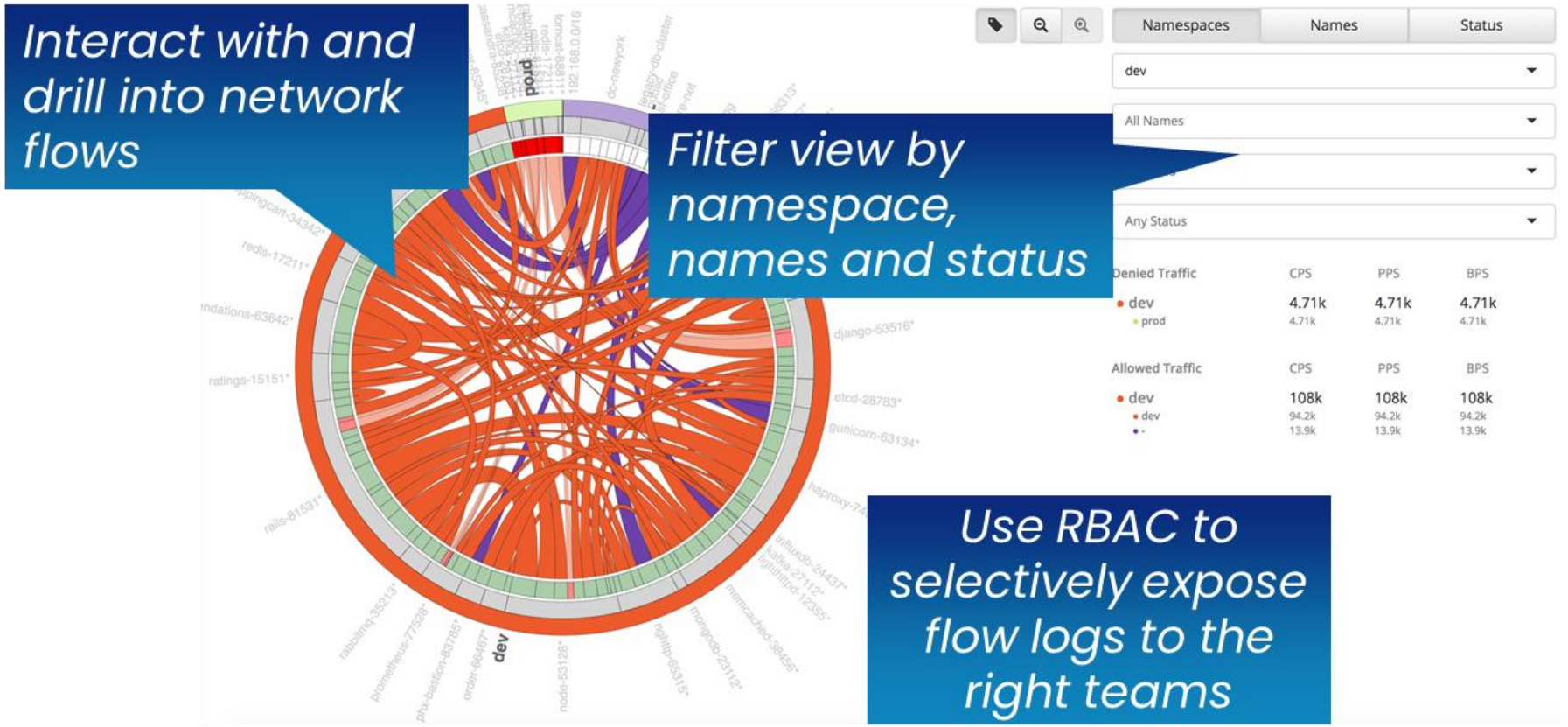
- 자동화된 Kubernetes 네이티브 접근 방식 적용 - 지루하고 시간 소모적인 수동 프로세스를 제거
- 운영자가 필요한 네트워크 진단을 하는데 필요한 시간과 노력을 크게 단축
- 네트워크 문제에 대한 빠르고 효과적인 해결
- Calico의 Dynamic Packet Capture 기능을 통해 Honeypod 접근 발생 시점에 대한 Network Traffic을 자동으로 캡처하여 더욱 빠르고 효과적으로 침해사고 분석 가능

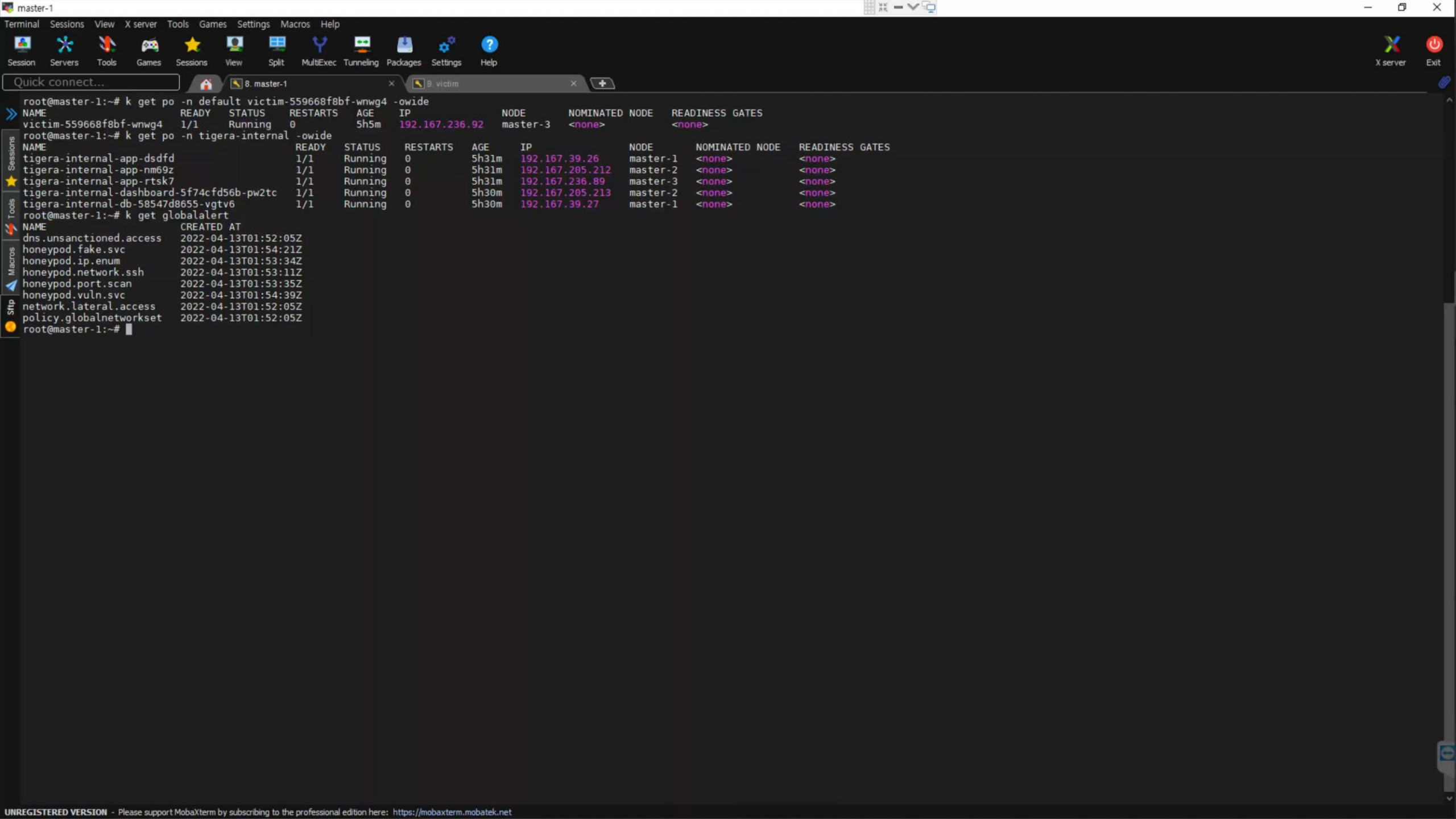


Flow Visualizer

- Calico 에서 제공하는 Flow Visualizer 를 통해서 360도 Viewing 가시성 확보

Creates flow logs that are graphically displayed on a Flow Log Visualizer with the context required to debug connectivity problems and security issues




master-1
Terminal Sessions View X server Tools Games Settings Macros Help
Session Servers Tools Games Sessions View Split MultiExec Tunneling Packages Settings Help
X server Exit
Quick connect...
8. master-1
9. victim
Sessions Tools Macros Sftp
root@master-1:~# k get po -n default victim-559668f8bf-wnwg4 -owide
NAME READY STATUS RESTARTS AGE IP NODE NOMINATED NODE READINESS GATES
victim-559668f8bf-wnwg4 1/1 Running 0 5h5m 192.167.236.92 master-3 <none> <none>
root@master-1:~# k get po -n tigera-internal -owide
NAME READY STATUS RESTARTS AGE IP NODE NOMINATED NODE READINESS GATES
tigera-internal-app-dsdfd 1/1 Running 0 5h31m 192.167.39.26 master-1 <none> <none>
tigera-internal-app-nm69z 1/1 Running 0 5h31m 192.167.205.212 master-2 <none> <none>
tigera-internal-app-rtsk7 1/1 Running 0 5h31m 192.167.236.89 master-3 <none> <none>
tigera-internal-dashboard-5f74cfd56b-pw2tc 1/1 Running 0 5h30m 192.167.205.213 master-2 <none> <none>
tigera-internal-db-58547d8655-vgtv6 1/1 Running 0 5h30m 192.167.39.27 master-1 <none> <none>
root@master-1:~# k get globalalert
NAME CREATED AT
dns.unsanctioned.access 2022-04-13T01:52:05Z
honeypod.fake.svc 2022-04-13T01:54:21Z
honeypod.ip.enum 2022-04-13T01:53:34Z
honeypod.network.ssh 2022-04-13T01:53:11Z
honeypod.port.scan 2022-04-13T01:53:35Z
honeypod.vuln.svc 2022-04-13T01:54:39Z
network.lateral.access 2022-04-13T01:52:05Z
policy.globalnetworkset 2022-04-13T01:52:05Z
root@master-1:~#
UNREGISTERED VERSION - Please support MobaXterm by subscribing to the professional edition here: https://mobaxterm.mobatek.net

More Information

Calico Demo Request

아래 링크를 통해 Calico Cloud 데모를 신청하세요. 담당자가 필요한 정보를 가지고 곧 연락 드리겠습니다.

www.osckorea.com/contact

TIGERA

OSC Korea 문의

tigera@osckorea.com