OSC ASIA GROUP LIMITED

TIGERA

Calico 창시자가 만든 K8s Security & Observability 솔루션 전문회사

Powered by OSC Korea

OSC Korea Co.,ltd info@osckorea.com 070-7757-3980

TIGERA

Tigera – K8s 보안 및 관측가능성(Observability) 분야 리더

- 오픈소스 Calico 프로젝트의 창시자에 의해 설립되어 K8s에서 가장 많이 사용되는 네트워크 및 보안 솔루션 제공
- 모든 클라우드 및 K8s 배포판에서 지원되며 Bare Metal, VM 수준까지 지원
- 166개국 백만 노드 이상에서 사용 중
- Kubernetes Network Policy 초기 Reference 구현체

오픈소스 Calico 창시자에 의해 설립

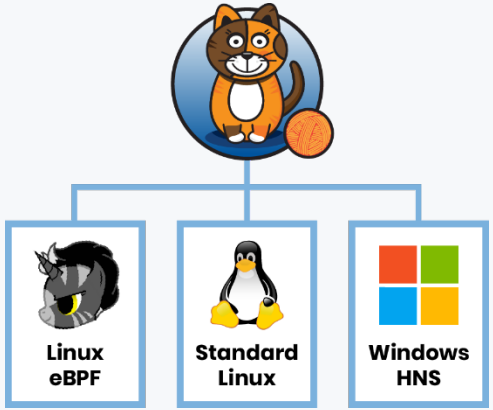
Kubernetes에서 가장 많이 사용되는 네트워크 및 보안 솔루션

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

주요 고객사 및 도입분야

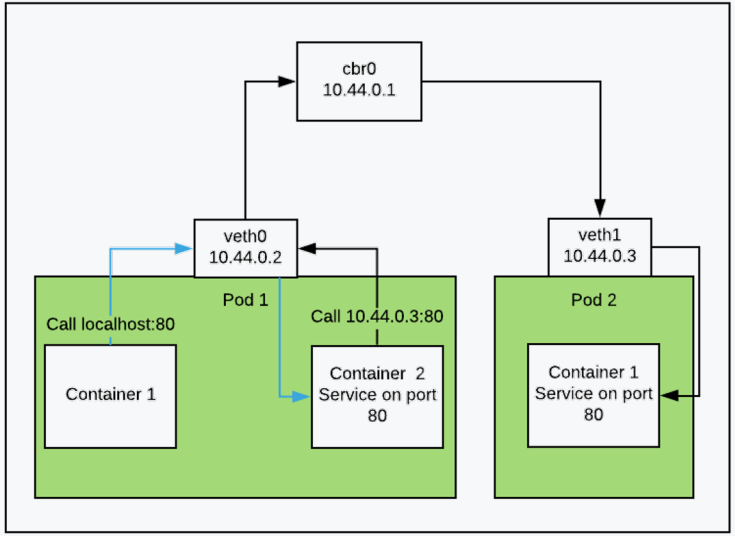
- 고객사
  - Fortune 500, 금융권, Cloud-native 회사, Telcos 및 대형 eCommerce

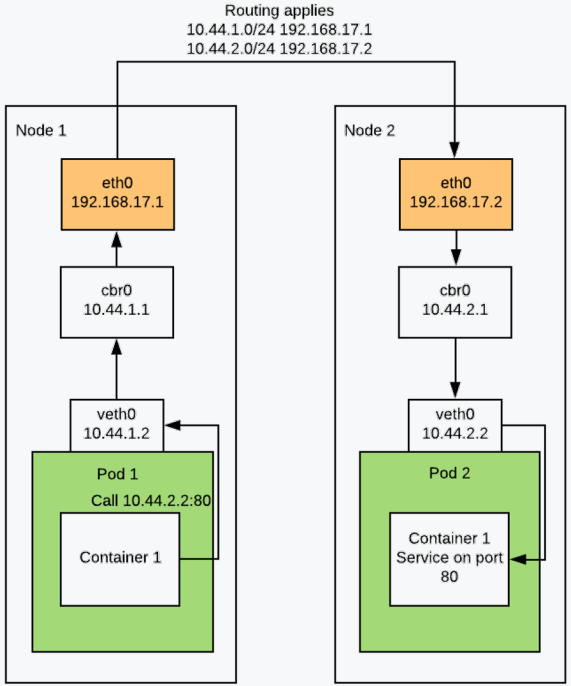
- Pluggable data plane



Customers	Partners
Bloomberg, AT&T, Morgan Stanley, VISA, DISCOVER, robinhood, JPMorganChase, servicenow, HanseMerkur, Ford, box, MARSH & McLENNAN COMPANIES, MERCK	aws, Azure, Google Cloud, IBM Cloud, RANCHER, OPENSHIFT, MIRANTIS, D2IQ, FORTINET, World Wide Technology

K8s Networking & CNI

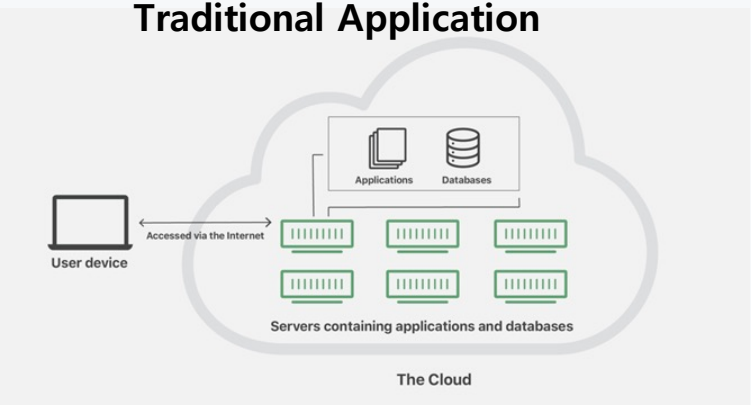




TIGERA flannel PROJECT CALICO canal weave net OSC

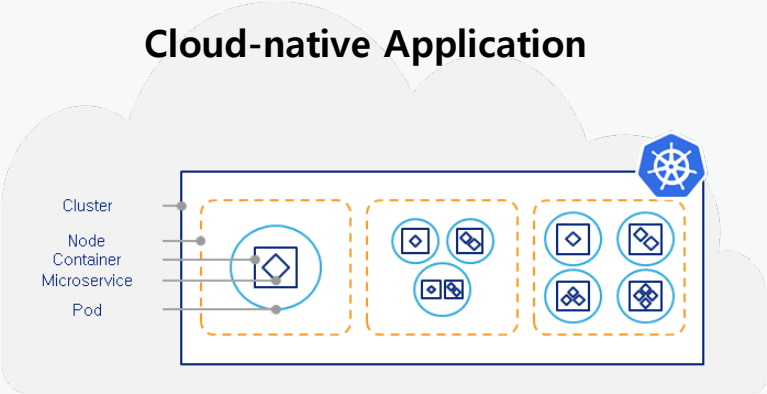
Cloud-Native Architecture 환경 Review

Traditional Application



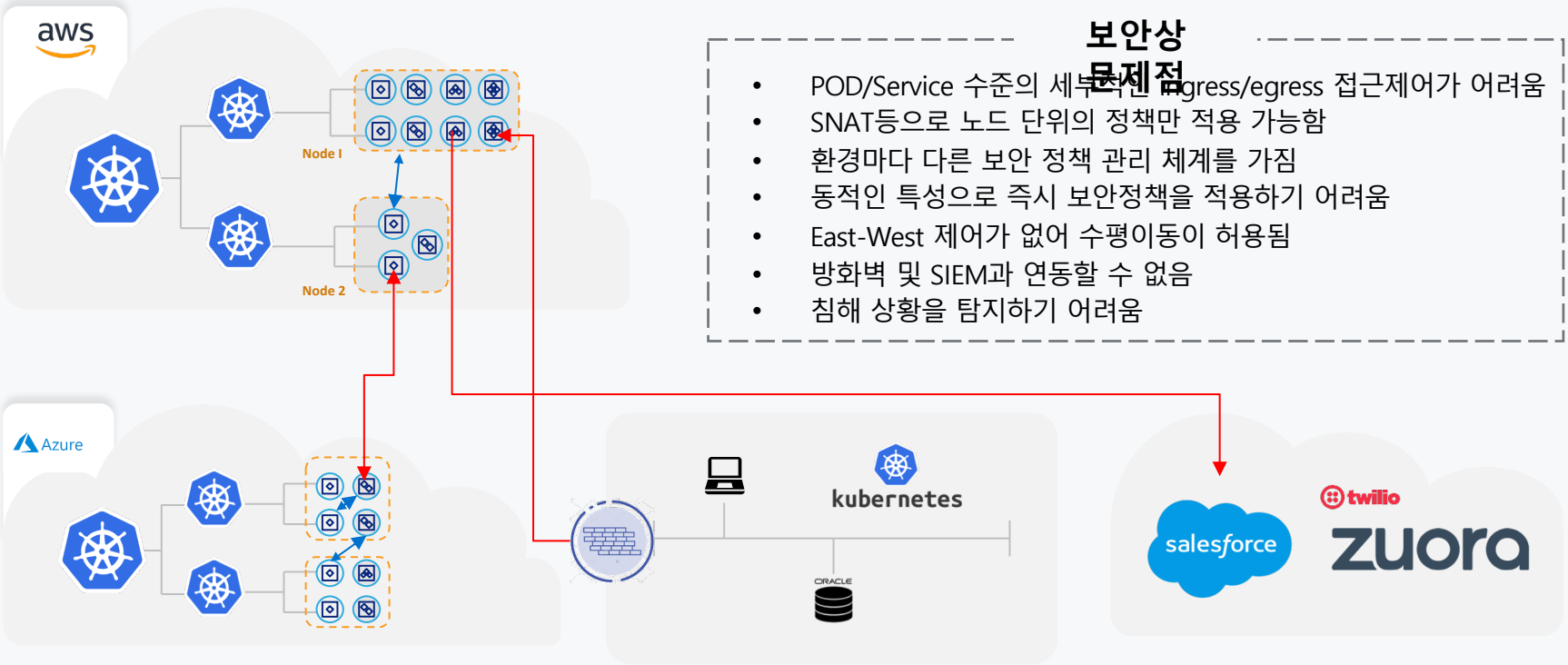
- 호스트 또는 VM 단위 구성요소
- 정적인 워크로드가 긴 생명주기를 가짐
- Perimeter 기반의 보안에 의존
- 전통적인 모니터링 방식

Cloud-native Application



- 컨테이너 단위 구성요소
- 동적이며 생명주기가 짧은 마이크로서비스
- Perimeter 기반 보안으로 충분하지 않음
- 분산형 어플리케이션, HW, OS

Cloud-Native Architecture 환경 Review – Cont.

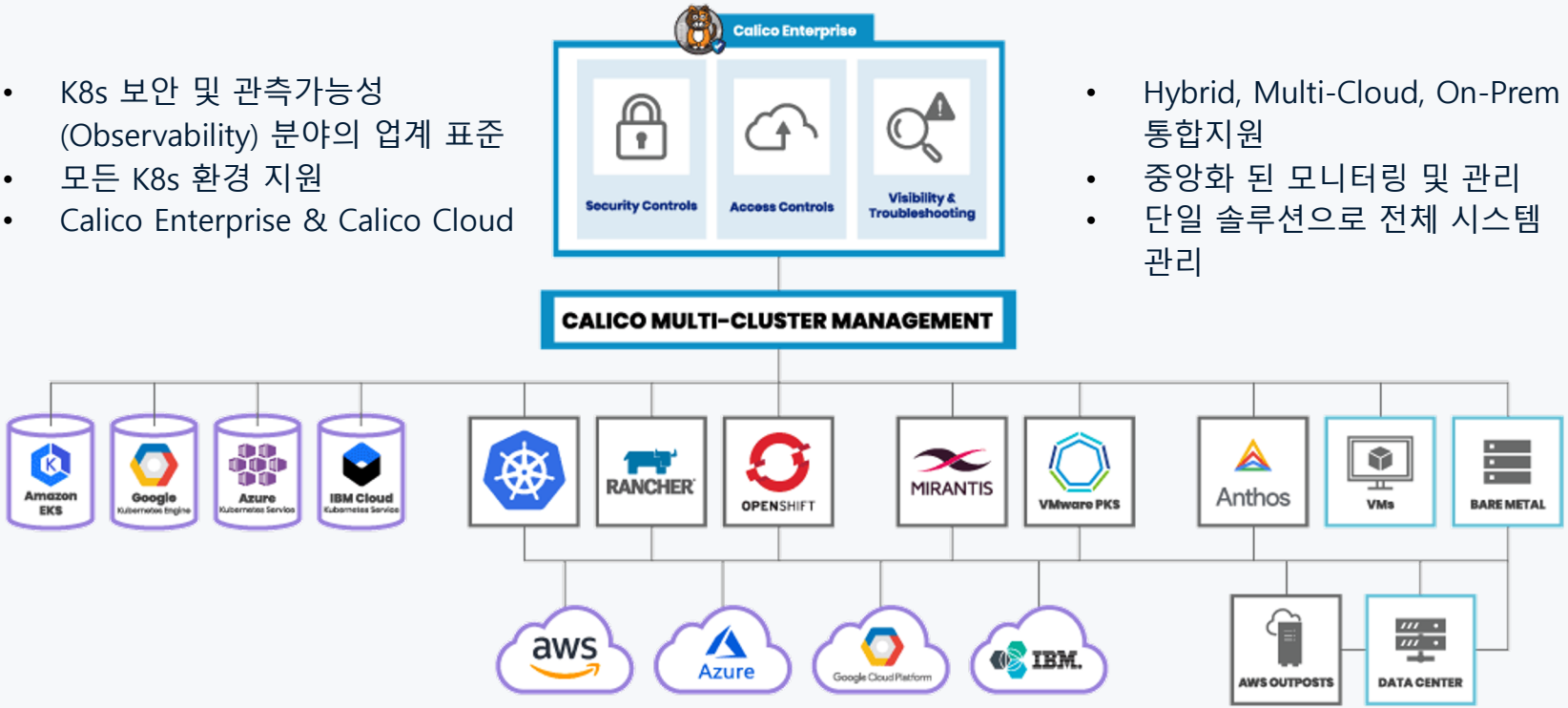


보안상 문제점

- POD/Service 수준의 세부적인 ingress/egress 접근제어가 어려움
- SNAT등으로 노드 단위의 정책만 적용 가능함
- 환경마다 다른 보안 정책 관리 체계를 가짐
- 동적인 특성으로 즉시 보안정책을 적용하기 어려움
- East-West 제어가 없어 수평이동이 허용됨
- 방화벽 및 SIEM과 연동할 수 없음
- 침해 상황을 탐지하기 어려움

K8s Network Security & Observability 업계 표준

- K8s 보안 및 관측가능성 (Observability) 분야의 업계 표준
- 모든 K8s 환경 지원
- Calico Enterprise & Calico Cloud



- Hybrid, Multi-Cloud, On-Prem 통합지원
- 중앙화 된 모니터링 및 관리
- 단일 솔루션으로 전체 시스템 관리

Calico– 아키텍처

SELF-SERVICE | CI/CD INTEGRATION

UNIFIED CONTROLS

Multi-Cluster	Multi-Cloud	Hybrid Cloud

NORTH-SOUTH CONTROLS	EAST-WEST CONTROLS	SECURITY COMPLIANCE	OBSERVABILITY
Universal Firewall & SIEM Integration	Application-level Service Controls	PCI, HIPAA, SOC 2, & GDPR	Dynamic Packet Capture
DNS Policy	Microsegmentation for Containers & VMs	Intrusion Detection & Prevention	Performance Hotspots
Ingress / Egress Access Controls	Host Protection	Encryption	Dynamic Service Graph

ECOSYSTEM

Amazon EKS · Azure Kubernetes Service · Google Kubernetes Engine · IBM Cloud Kubernetes Service · OPENSHIFT · RANCHER · MIRANTIS · VMware Tanzu · AWS OUTPOSTS · Anthos

Kubernetes Security and Observability

TIGERA

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)

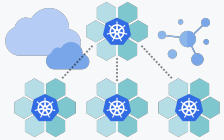
K8s 환경의 IDS 지원으로 비정상행위를 모니터링 하고 Alert, 격리 지원

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

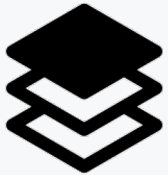
주요 Use Cases & Features – Cont.

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

Opensource vs. Enterprise

AREA	FEATURE	OPENSOURCE	ENTERPRISE
Networking	High-performance scalable pod networking	V	V
	Advanced IP address management	V	V
	Direct infrastructure peering without the overlay	V	V
Security	Security policy enforcement	V	V
	Data-in-transit encryption	V	V
	Hierarchical tiers		V
	FQDN / DNS based policy		V
	Micro-segmentation across Host/VMs/Containers		V
	Security policy preview, staging, and recommendation		V
	Compliance reporting & alerts		V
	Intrusion detection & prevention (IDS / IPS) for Kubernetes		V
	SIEM Integrations		V
Observability	Dynamic Service Graph		V
	Application Layer Observability		V
	Dynamic Packet Capture		V
	DNS Dashboards		V
	Flow visualizer		V
Management	Multi cluster, multi-cloud & hybrid Cloud networking		V

Common Roadblocks With Opensource

가시성
문제해결에 필요한 충분한 가시성이 확보되지 못함

외부 연동에 따른 이슈
대부분의 워크로드는 클러스터 외부 데이터베이스를 비롯해 다른 Endpoint와 연동이 필요하나 접근을 세부적으로 제어하지 못함

보안 정책
보안팀에서 전통적으로 요구하는 정책 및 규제 기준을 맞추기 어려움

TIGERA

- 새로운 서비스가 탑재될 때 마다 방화벽 정책을 변경해야 하는데 기존 변경절차는 시간이 너무 오래 걸려 프로젝트 일정에 차질 발생
- Multi-Tenancy를 요구하는 경우 클러스터내에 Isolation 이 반영되어야 하나 K8s 환경에서 이를 구현하는데 복잡하고 어려움이 있음
- 외부 인터넷과 연동이 필요한 어플리케이션은 방화벽을 거쳐야 하는데 보안팀에서는 필요한 보안정책을 검토하고 적용하는데 있어 가시성을 확보해야 함
- 어플리케이션이 늘어날 수록 다양한 보안/규제 요구사항이 발생하며 중앙화 된 관리로는 한계가 있어 이를 DevSecOps 환경에 발맞춰 보안정책을 빠르게 적용할 수 있는 분산 방안이 필요함
- 정책관리시스템은 클라우드 환경에 최적화되어 있지 않아 호스트에서 K8s 환경에 이르기까지 확장 적용할 수 있는 방안이 필요함

Why Calico Enterprise?

The Enterprise Kubernetes Journey

Open Source Calico	Calico Enterprise Solutions		
Open Source 기반으로 서비스 준비	**Egress 접근제어**	K8s로 방화벽 확장	Microsegmentation
	Observability & Troubleshooting	Self-Service 보안 적용	침입탐지
	Enterprise 보안정책 K8s 확대 적용	멀티 클러스터 보안 및 Observability	Zero Trust Security

THANK YOU