Multi Cloud Networking

2020. 10.

(2021년 3월까지 사용 권장)

안 종 석

james@jslab.kr

JS Lab

james@jslab.kr

I. 개요

II. 아키텍처

III. 기술

IV. 운영 모델

V. 네트워킹

VI. 관리

james@jslab.kr

I. 개요

II. 아키텍처

III. 기술

IV. 운영 모델

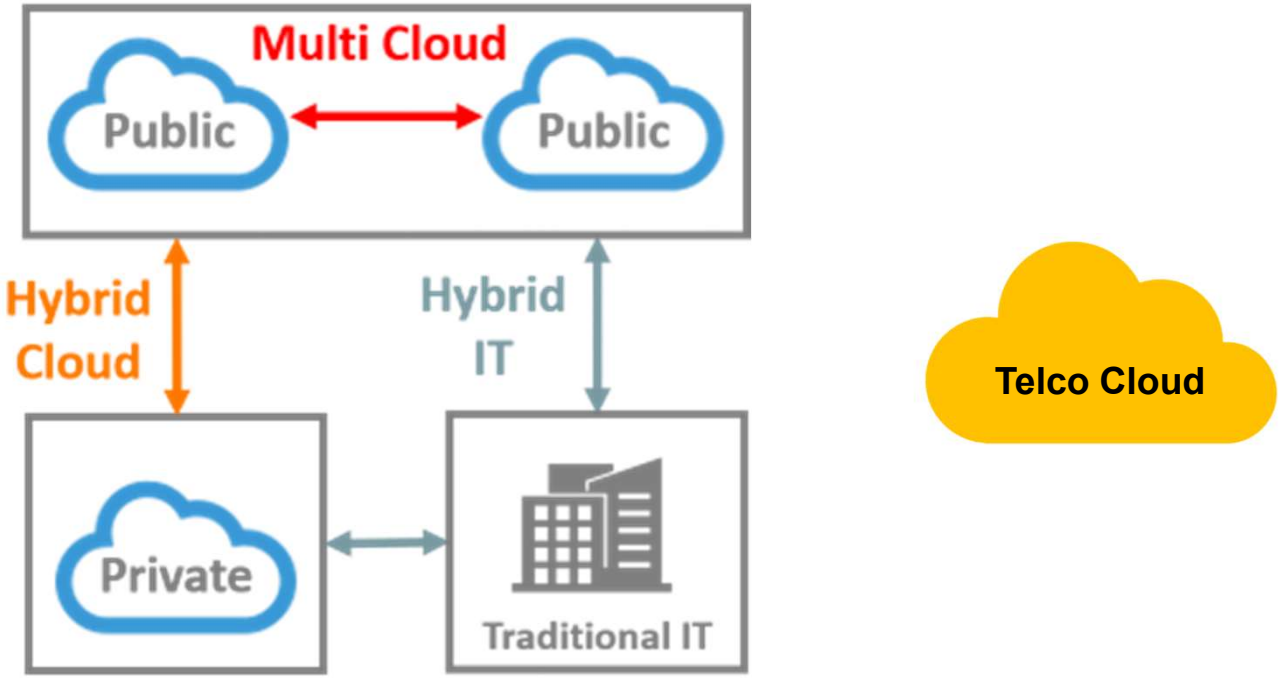
V. 네트워킹

VI. 관리

I. 개요

❖ Multi-Cloud는 Hybrid-Cloud와 Traditional IT를 연결하는 환경

- Multi Cloud: Public 클라우드간 연결
- Hybrid Cloud: Public 클라우드와 Private 클라우드의 연결
- Hybrid IT: 온프레미스(On-premise)와 Public 클라우드의 연결
- Telco Cloud: 멀티 클라우드 기술 기반 통신사 인프라



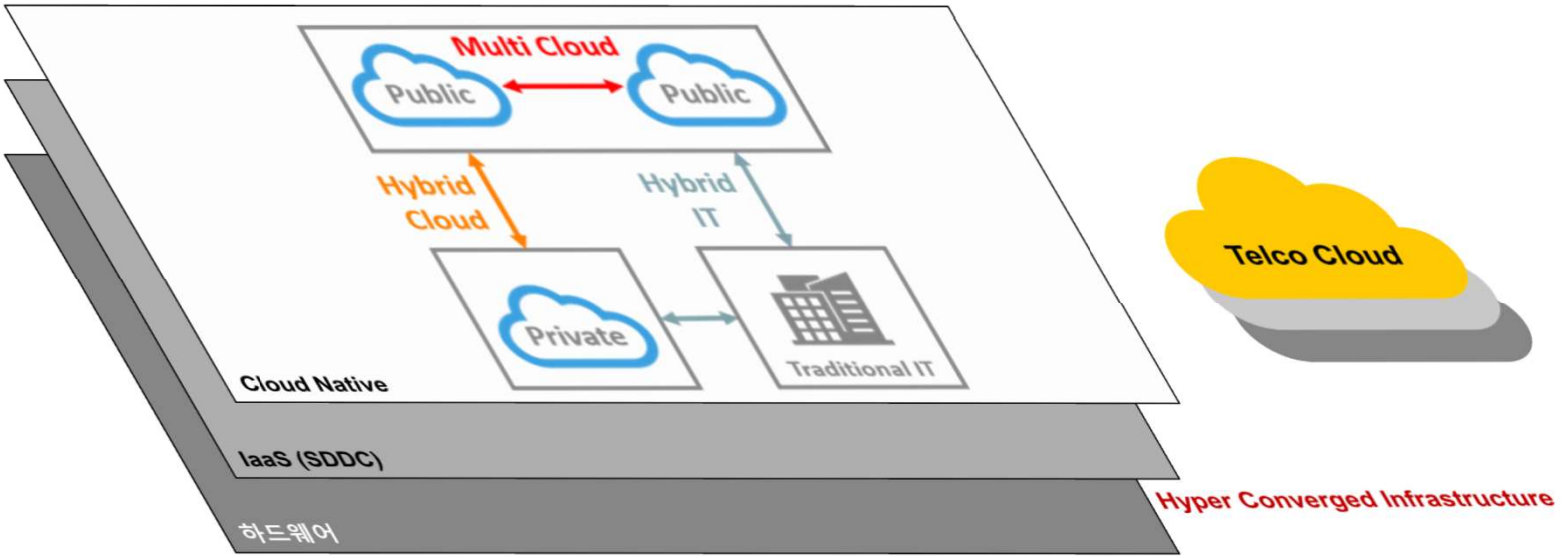
온프레미스: 기업이 자체 시설에서 보유하고 직접 유지 관리하는 프라이빗 데이터 센터

I. 개요

❖ 계층화 인프라

- 인프라의 계층별 추상화 (서비스에 집중)
- 계층간 격리와 정책 기반 서비스 노출
- 성능 개선 (계층 Offload 필요)
- 계층간 연결 호환성

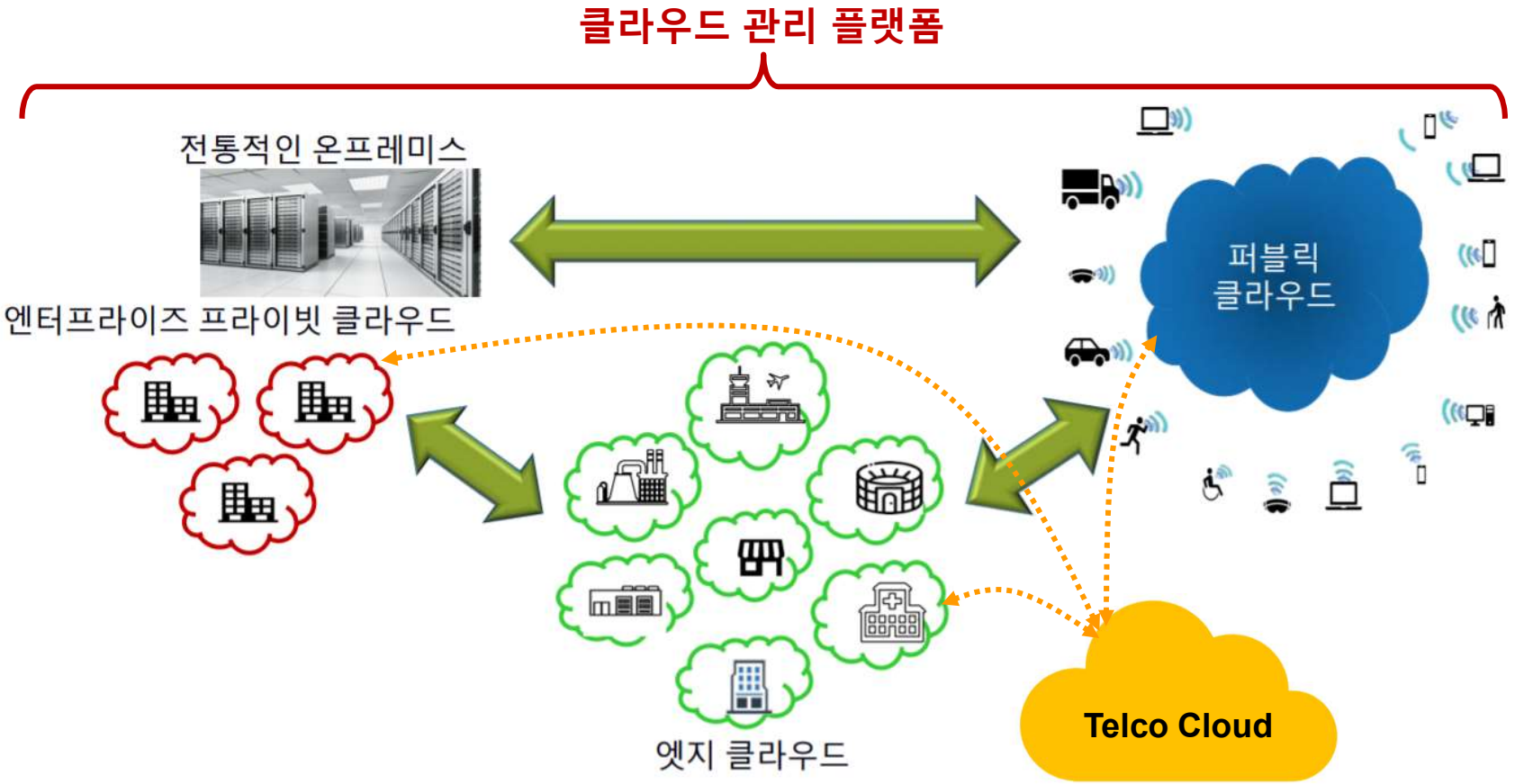
- 제품화를 위한 영역과 계층 고려
- (Managed) Service 제품화 vs. Product 제품화



I. 개요

❖ 멀티클라우드 관리 플랫폼

- **Multi Cloud Managed Service Platform** (MCMSP)
- **하이브리드/멀티 클라우드 관리** (Hybrid/Multi Cloud Management)
- **Telco Cloud**



james@jslab.kr

I. 개요

❖ Multi-Cloud 환경 이동 이유

벤더 락인 우려 최고 솔루션 선택

"Most organizations adopt a multicloud strategy out of a desire to avoid vendor lock-in or to take advantage of best-of-breed solutions" - Gartner analyst

유연한 커스터마이징

Flexible Customization
Each Cloud Service Provider has special Features

위험 완화

Risk Mitigation
Deploying critical systems across multiple Cloud services provides additional fault tolerance

데이터 유실과 다운타임 최소화

Minimize the threat of extensive data loss or downtime due to component failure in cloud.

I. 개요

❖ 클라우드 서비스 가격과 멀티 클라우드 구성

Instance type	AWS Instances	AWS RAM (GiB)	Azure VMs	Azure RAM (GiB)	Google VMs	Google RAM (GiB)
General purpose	m5.xlarge	16	B4MS	16	n1-standard- 4	15
Compute optimized	c5.xlarge	8	F4s v2	8	n1-highcpu-4	3.6
Memory optimized	r5.xlarge	32	E4 v3	32	n1-highmem-4	26
GPU instances	g3s.4xlarge	30.5	NC 6	56	NVIDIA@Tesla@ P4	64

Instance type	AWS	Azure	Google	AWS Pricing (per hour)	Azure Pricing (per hour)	Google Pricing (per hour)
General purpose	m5.xlarge	B4MS	n1-standard- 4	$0.192	$0.166	$0.214
Compute optimized	c5.xlarge	F4s v2	n1-highcpu-4	$0.170	$0.169~$0.17	$0.1626
Memory optimized	r5.xlarge	E4 v3	n1-highmem-4	$0.252	$0.252	$0.2696
GPU instances	g3s.4xlarge	NC 6	NVIDIA@Tesla@ P4	$0.75	$0.899	$2.4

https://www.simform.com/compute-pricing-comparison-aws-azure-googlecloud/

I. 개요

- ❖ 클라우드 서비스 가격의 유동성과 이를 고려한 아키텍처
- ❖ 빌링(Billing) 예
  - Customer
  - Managed Service
  - Public Cloud

james@jslab.kr

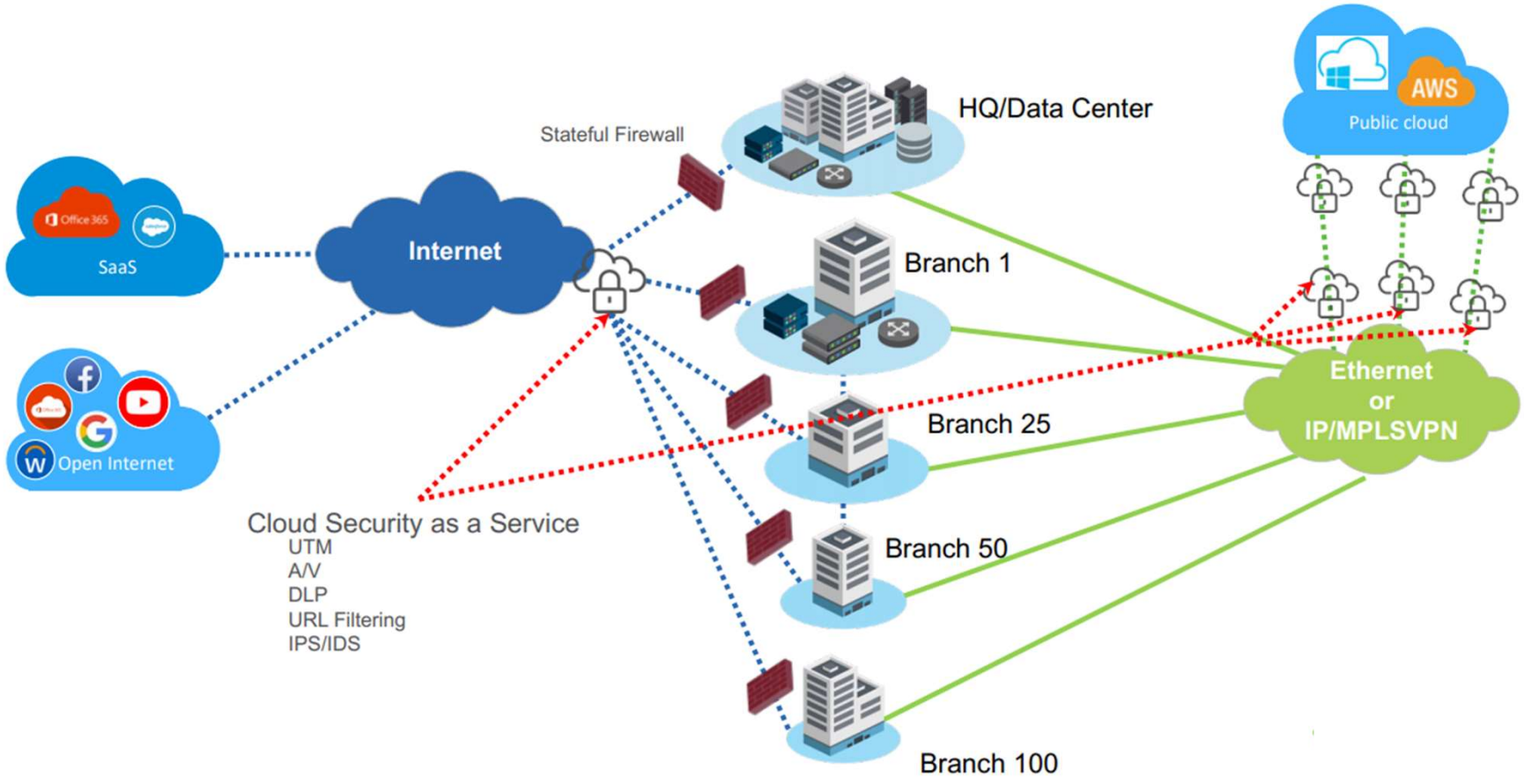
Discounted Pricing for 1-year Commitment with on upfront cost

Instance type	AWS	Azure	Google	AWS Pricing (per hour)	Azure Pricing (per hour)	Google Pricing (per hour)
General purpose	m5.xlarge	B4MS	n1-standard- 4	$0.123	$0.097	$0.128
Compute optimized	c5.xlarge	F4s v2	n1-highcpu-4	$0.107	$0.099	$0.095
Memory optimized	r5.xlarge	E4 v3	n1-highmem-4	$0.159	$0.156	$0.159
GPU instances	g3s.4xlarge	NC 6	NVIDIA@Tesla@ P4	$0.551	$0.572	$0.864

https://www.simform.com/compute-pricing-comparison-aws-azure-googlecloud/

I. 개요

- **SD-WAN의 발전**
- **Multi-Cloud 를 위한 엔터프라이즈 인터넷 접속** (or Cloud Security as-a-Service)

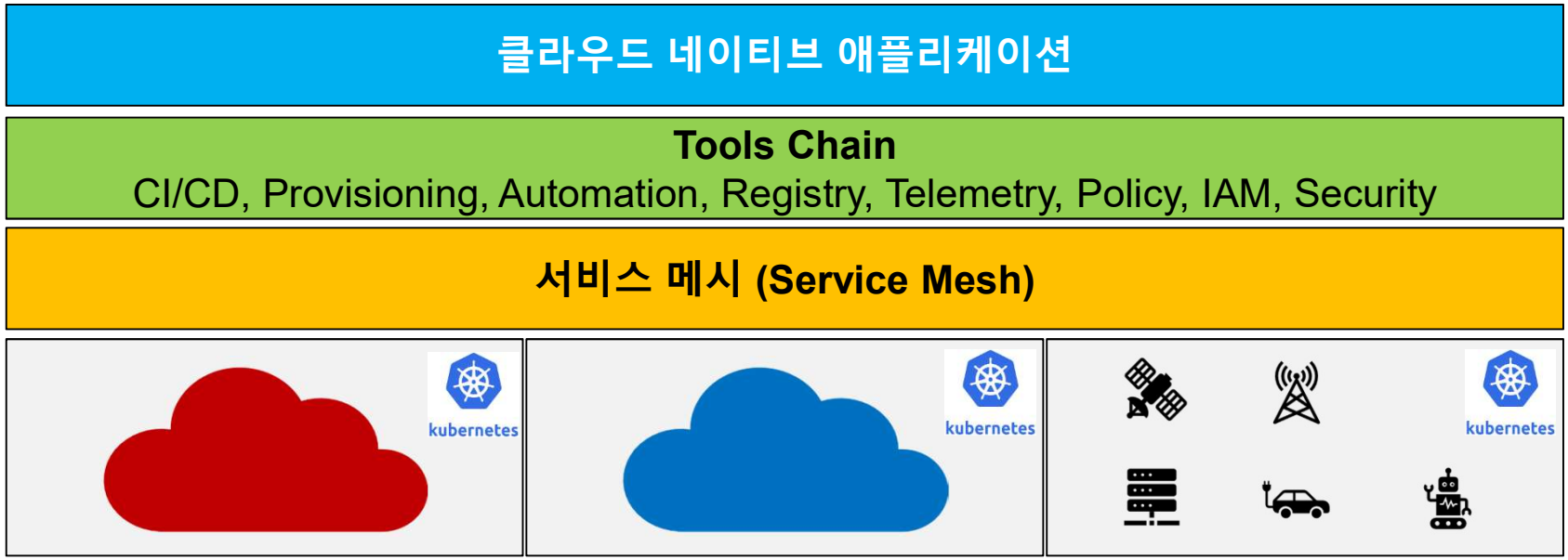


Versa Networks, SDxCentral.

I. 개요

❖ 멀티 클라우드 애플리케이션 제공

- 혼합된 워크로드 구성
- 고성능 컴퓨팅
- 멀티 데이터 워크로드 오케스트레이션



james@jslab.kr

I. 개요

II. 아키텍처

III. 기술

IV. 운영 모델

V. 네트워킹

VI. 관리

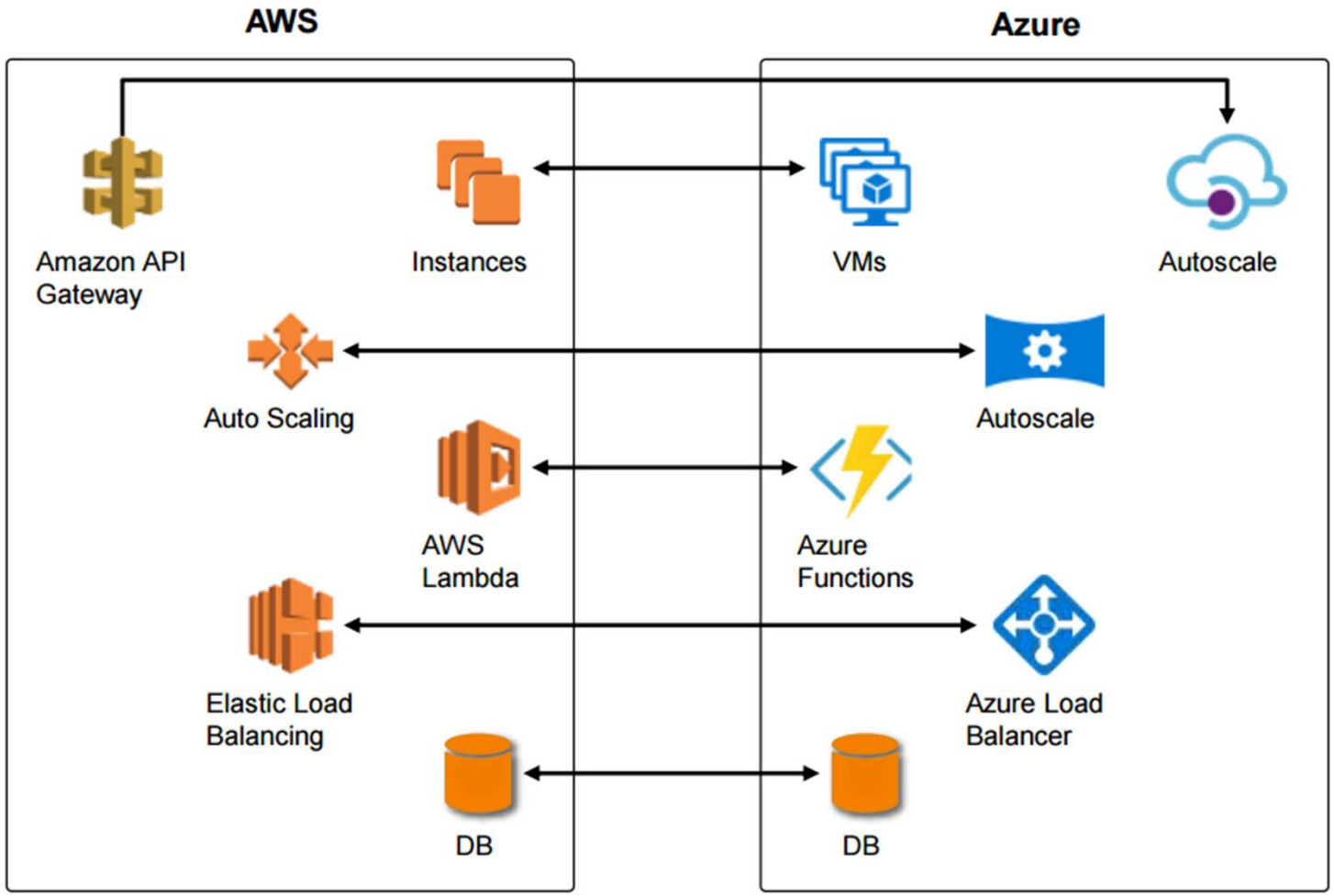
II. 아키텍처

❖ **Key Takeaways** (요소)

- **비용 고려:** More financial institutions are turning to hybrid and multicloud setups
- **장점:** Multi-cloud offers a myriad of benefits in today's financial landscape
- **중앙 관리:** Multi-cloud requires a centralized, unified approach
- **보안/제어:** Multi-cloud can be secure, compliant, and allow for more fine-tuned control

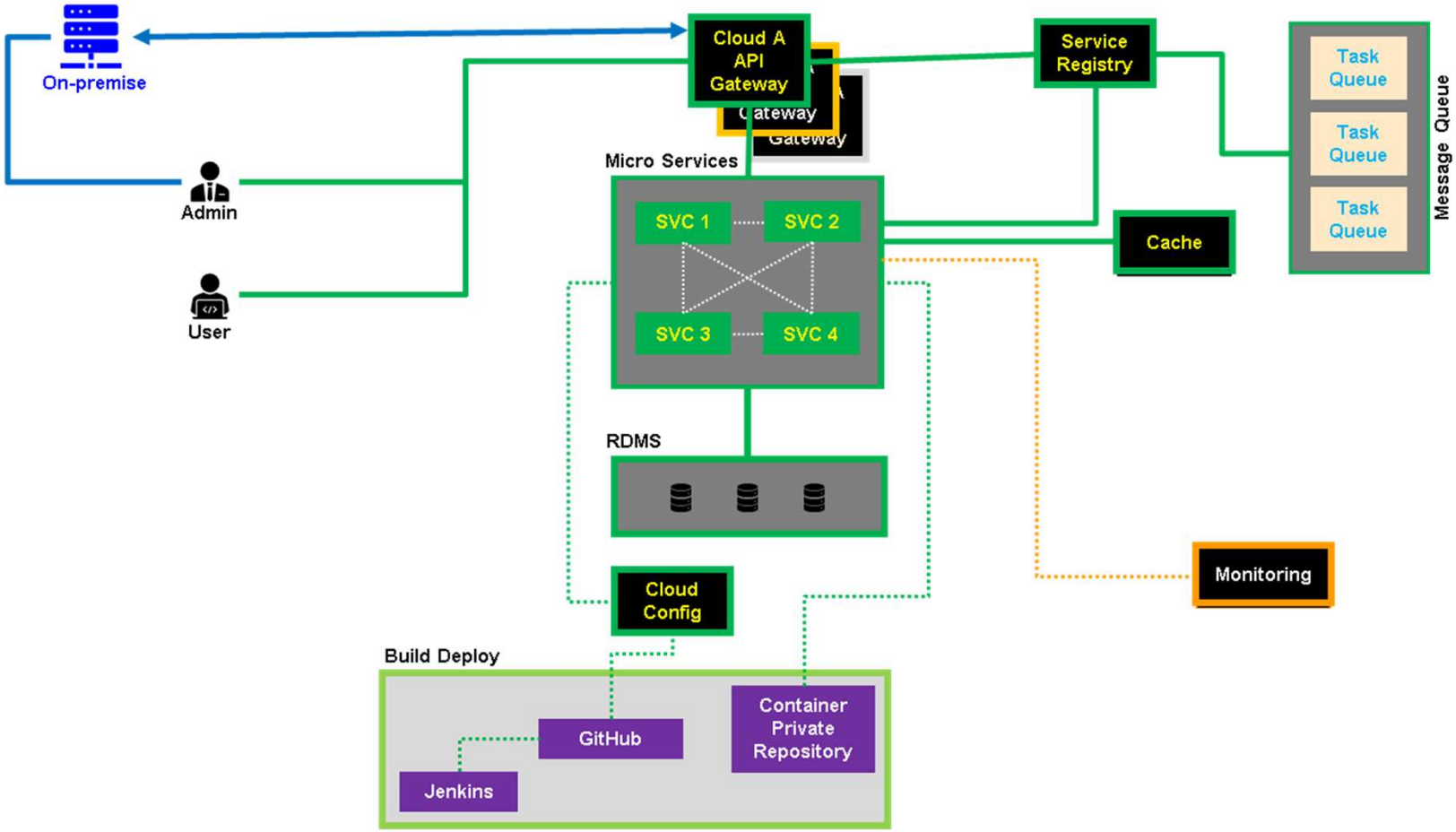
II. 아키텍처

❖ 동일 서비스 고려하는 Multi-Cloud Architecture



II. 아키텍처

❖ 온프레미스 연동 고려 Hybrid/Multi-Cloud Architecture (예)



II. 아키텍처

❖ Basic Cloud Architecture

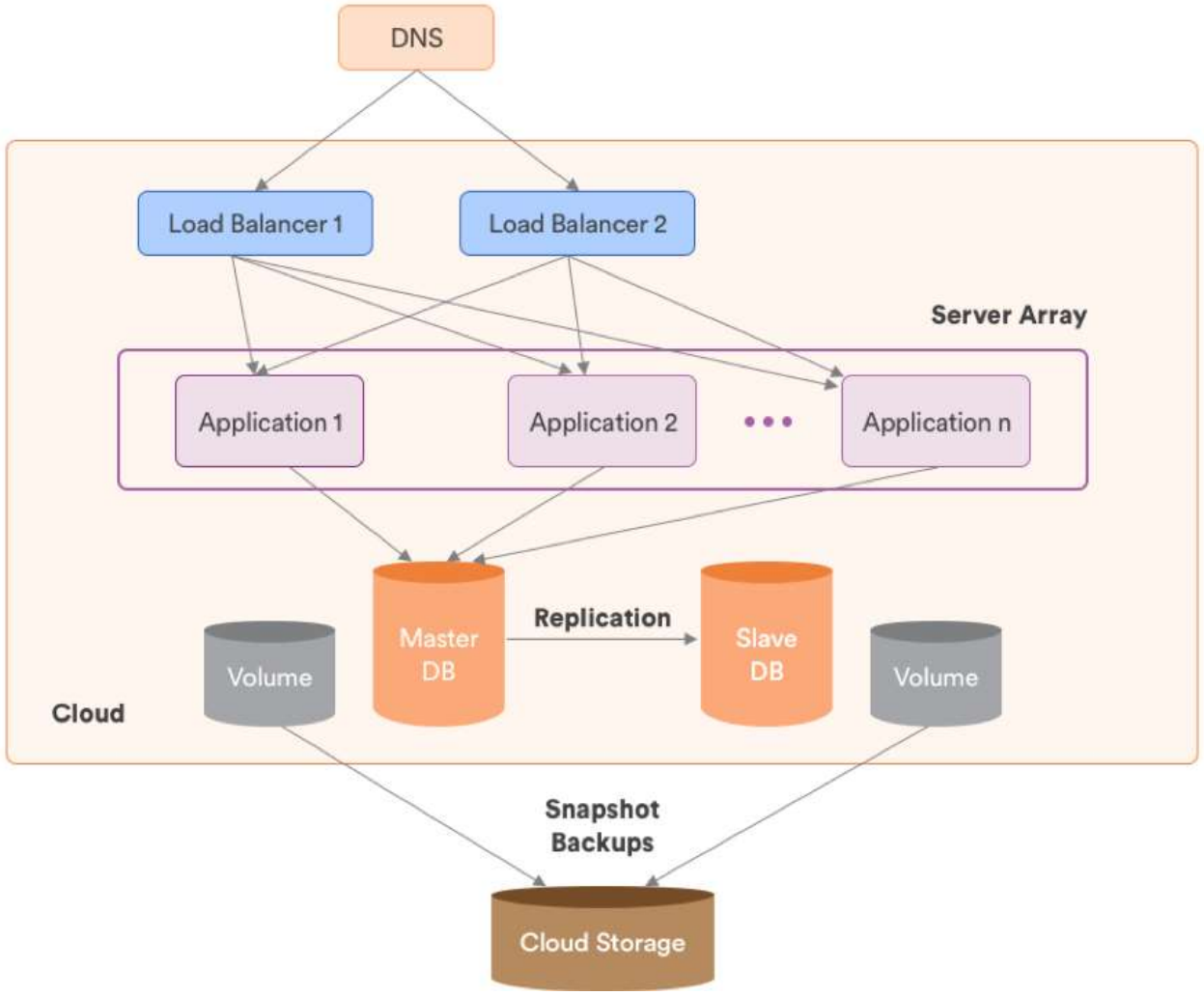


Image: Rightscale

II. 아키텍처

❖ Basic Cloud Architecture (2 Datacenters)

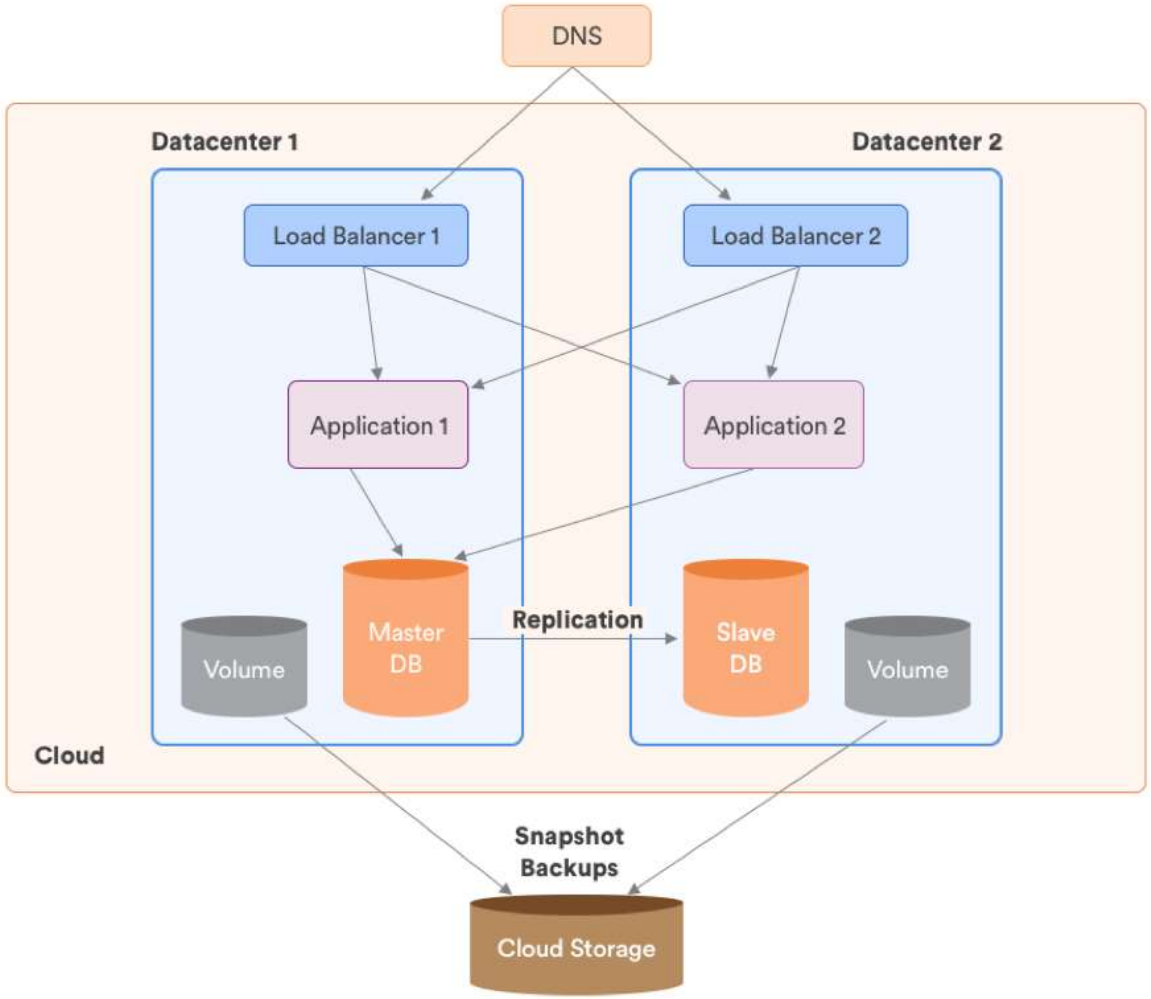
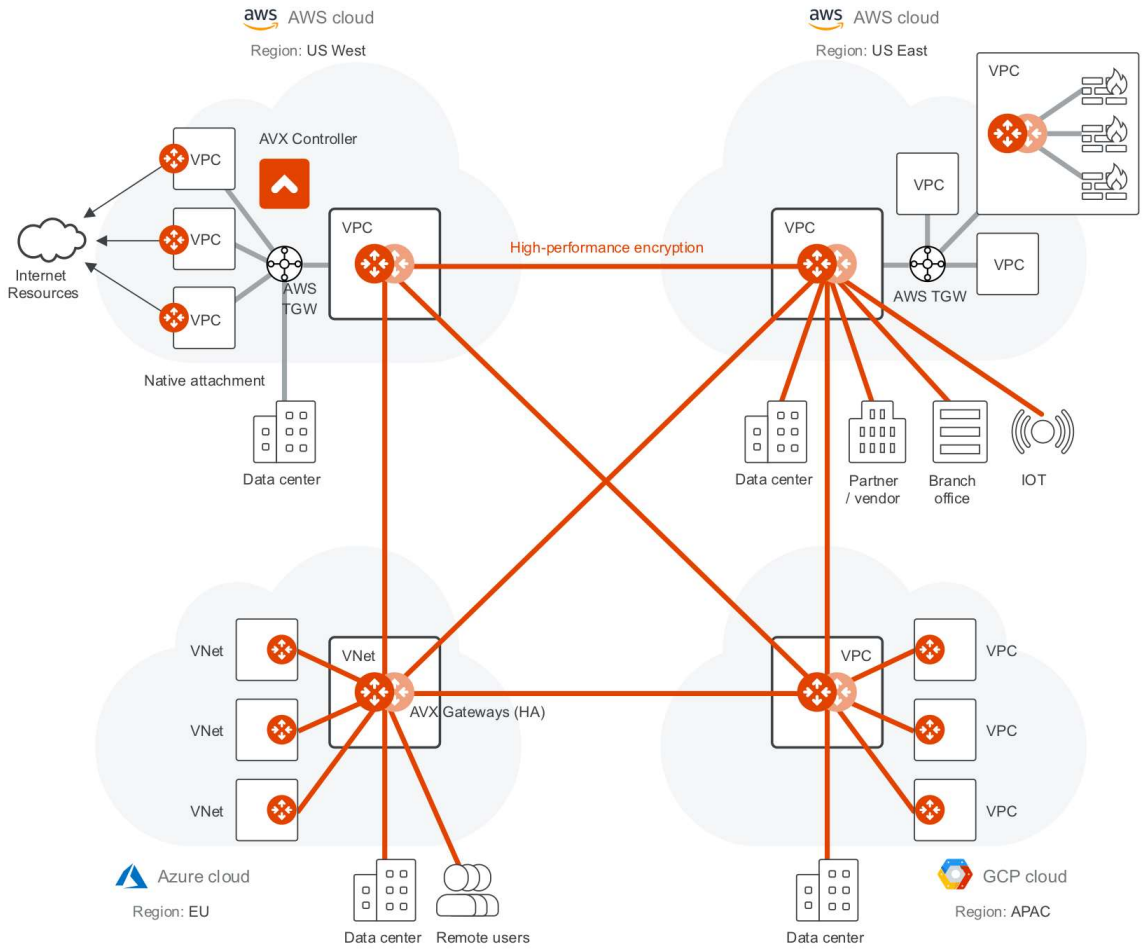


Image: Rightscale

II. 아키텍처

❖ 기업용 **Multi-Cloud Backbone** (Aviatrix 예)

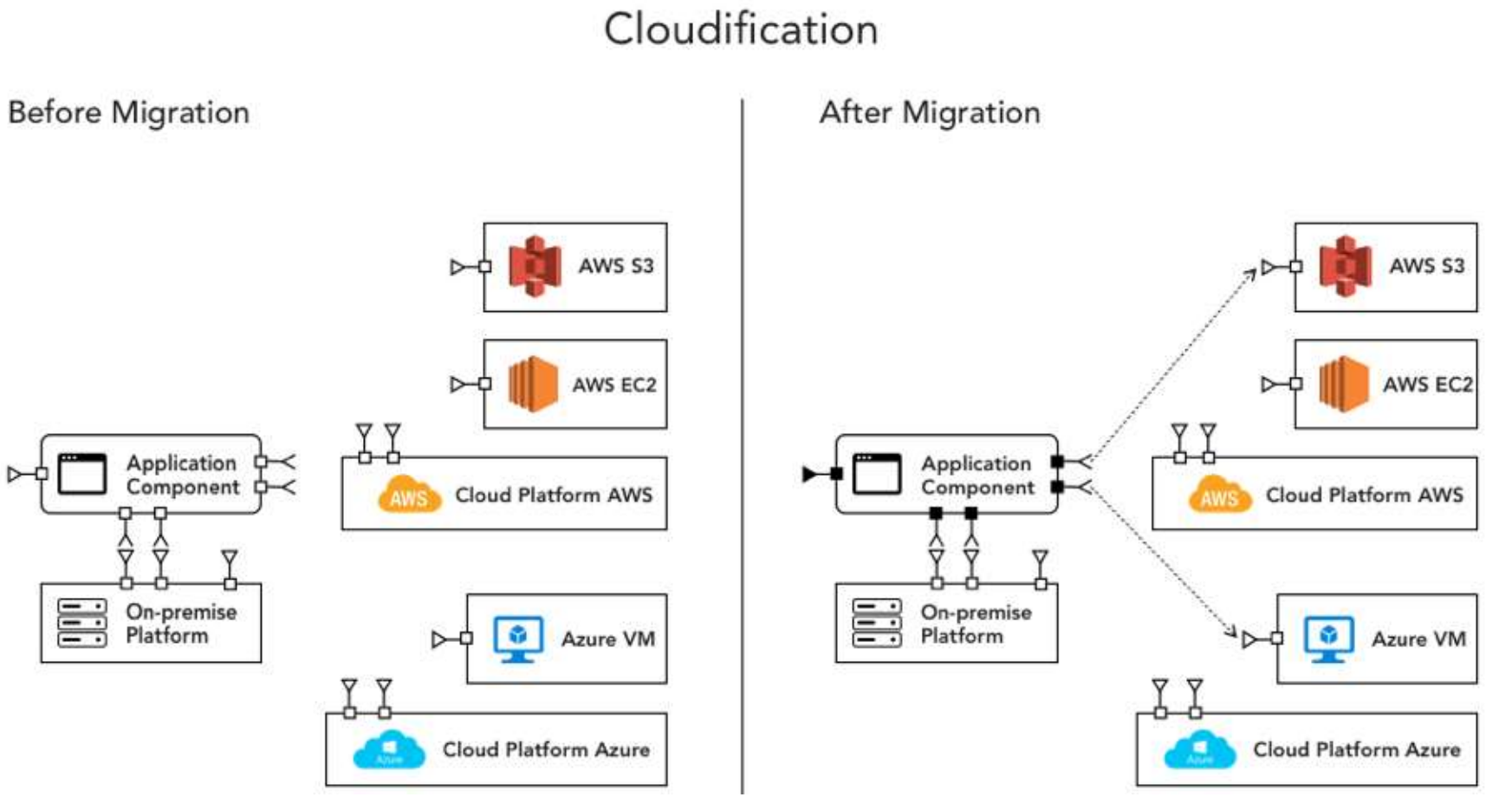


https://www.simform.com/compute-pricing-comparison-aws-azure-googlecloud/

II. 아키텍처

❖ 애플리케이션을 위한 Multi-Cloud Architecture

- 애플리케이션의 클라우드화 (Cloudification)

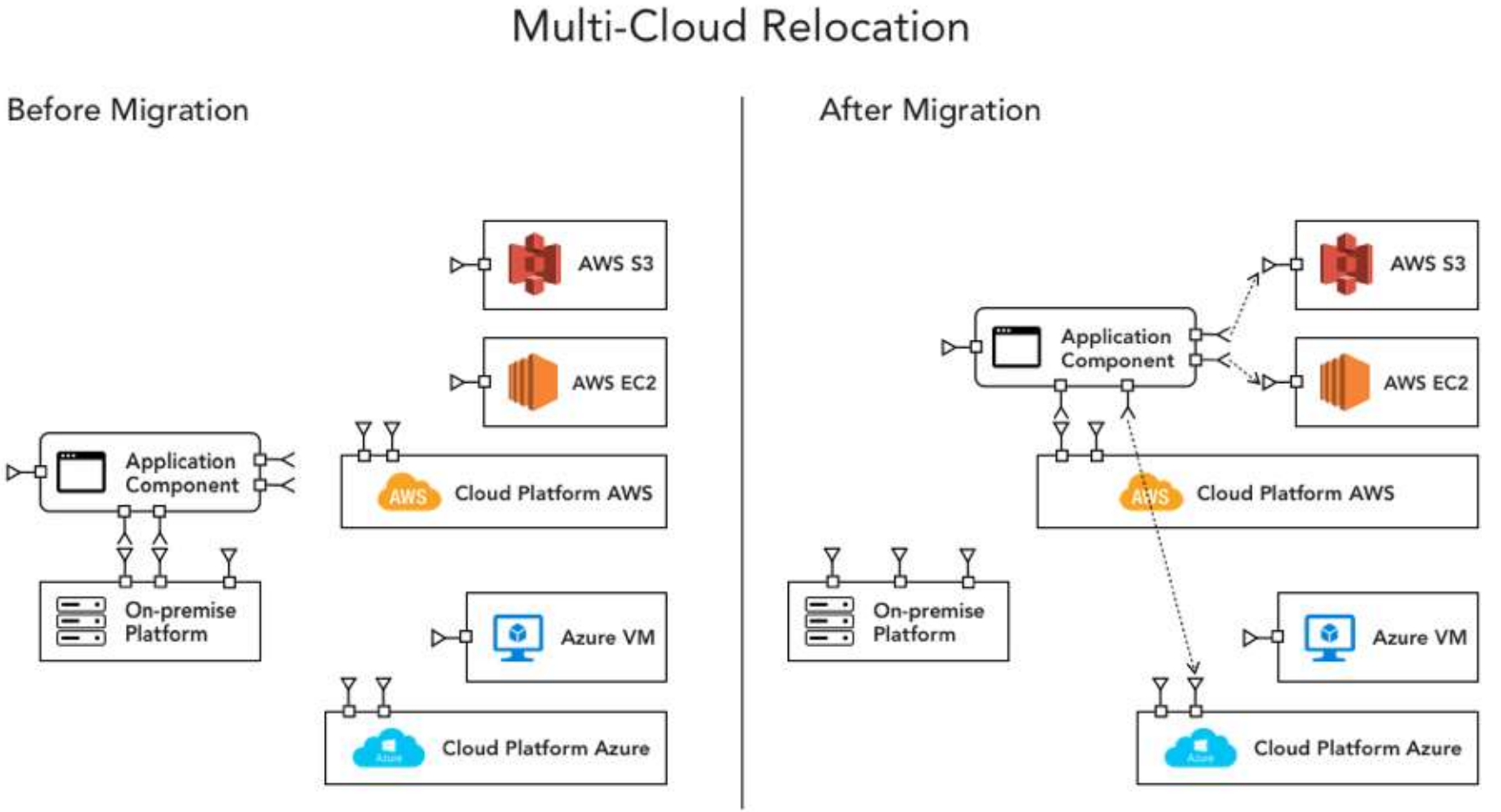


Jignesh Solanki, leads Simform's Product Engineering team

II. 아키텍처

❖ 애플리케이션을 위한 Multi-Cloud Architecture

- 클라우드 이전 (Multi-Cloud Relocation)

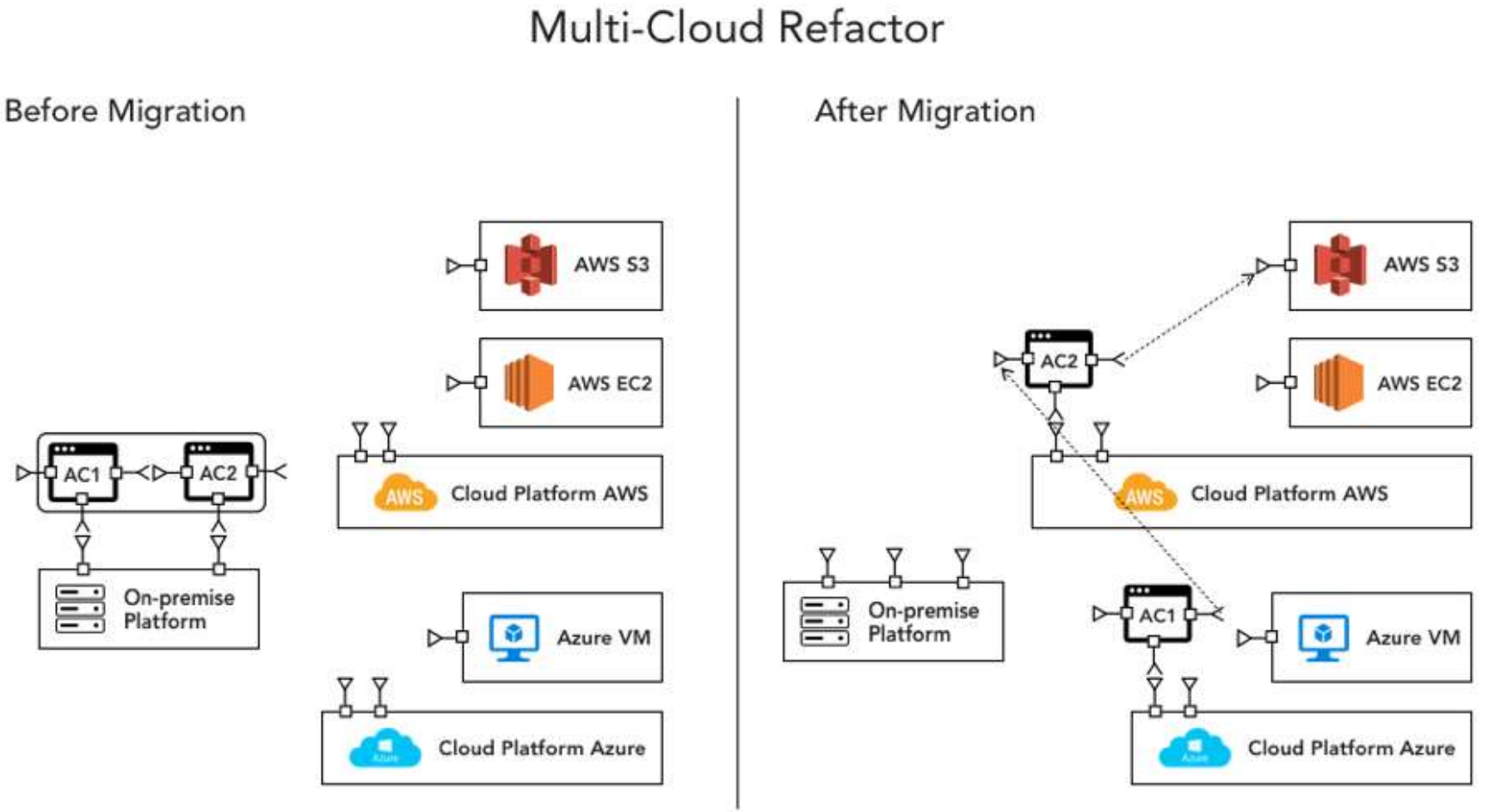


Jignesh Solanki, leads Simform's Product Engineering team

II. 아키텍처

❖ 애플리케이션을 위한 Multi-Cloud Architecture

- 클라우드 이전 변환 (Multi-Cloud Refactor)

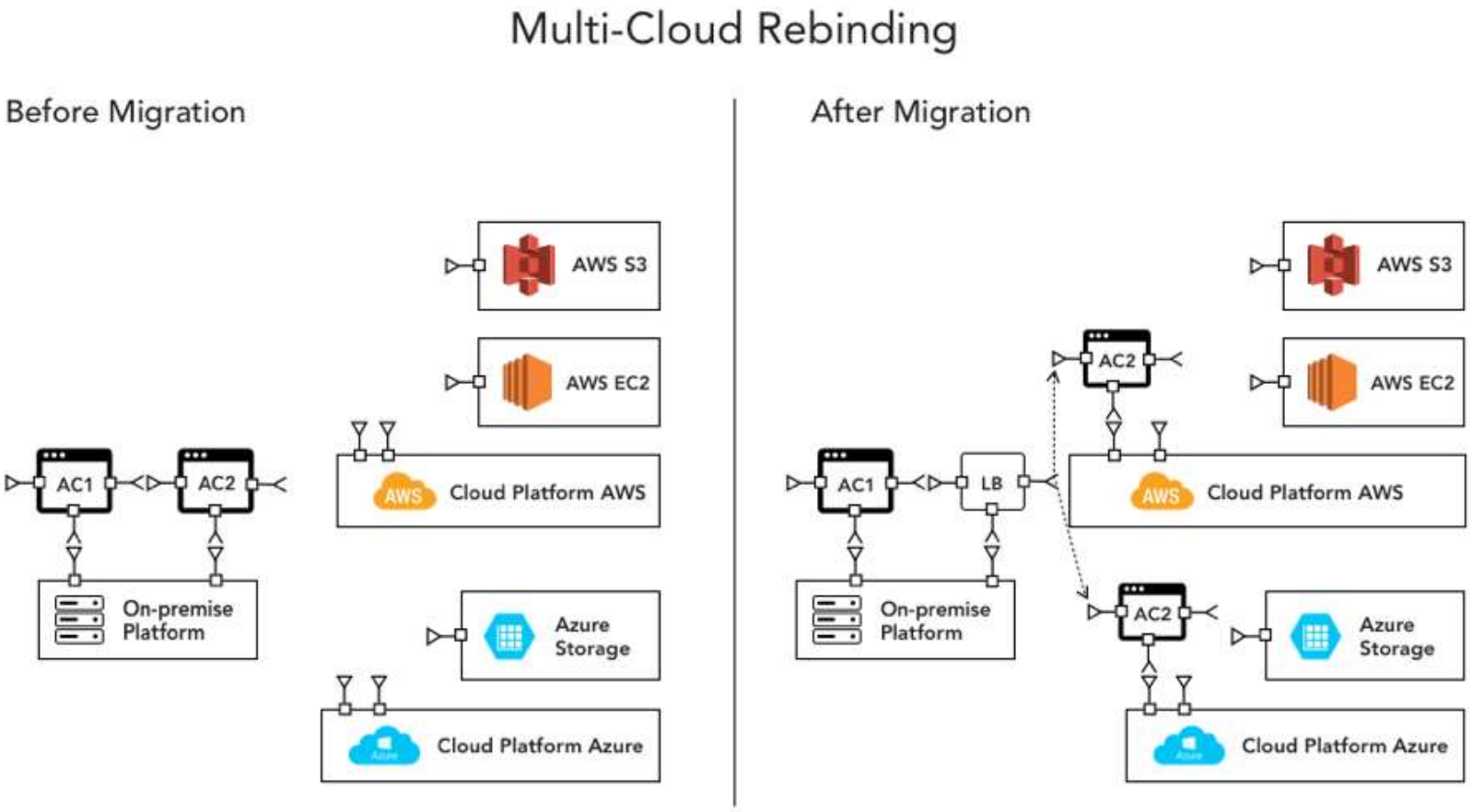


Jignesh Solanki, leads Simform's Product Engineering team

II. 아키텍처

❖ 애플리케이션을 위한 Multi-Cloud Architecture

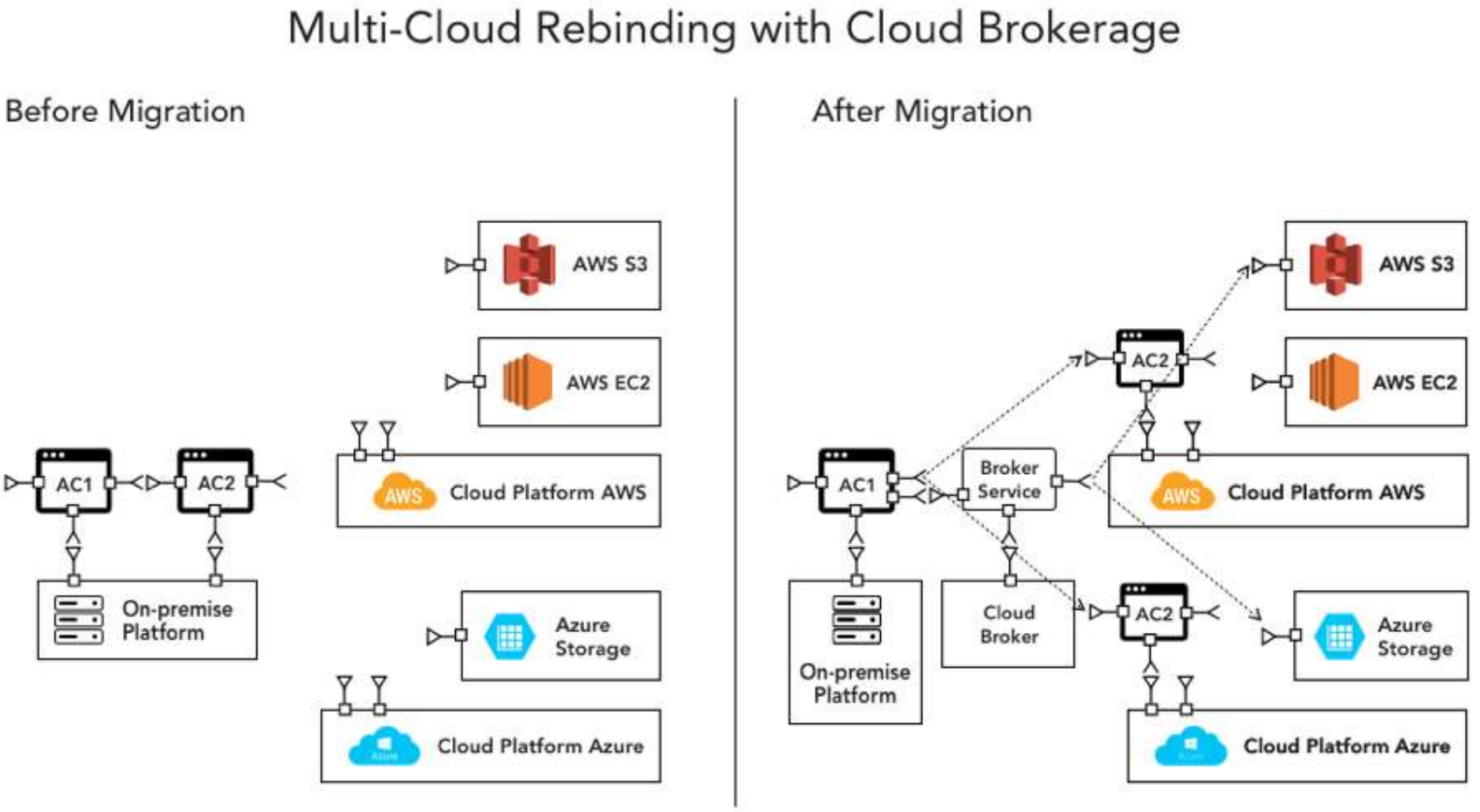
- **결합 (Multi-Cloud Rebinding)**



II. 아키텍처

❖ 애플리케이션을 위한 Multi-Cloud Architecture

- **Multi-Cloud Rebinding with Cloud Brokerage**

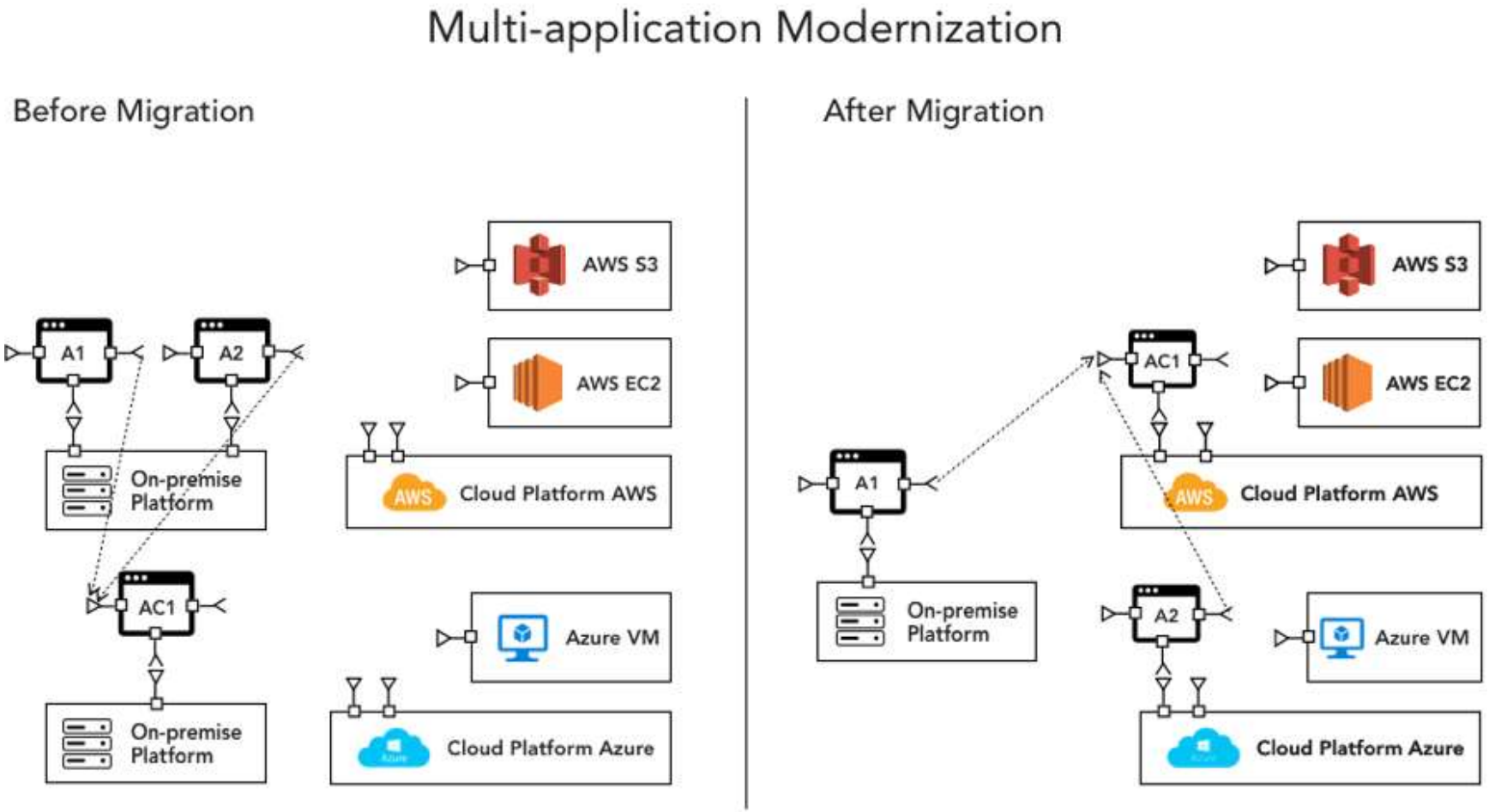


Jignesh Solanki, leads Simform's Product Engineering team

II. 아키텍처

❖ Multi-Cloud Architecture

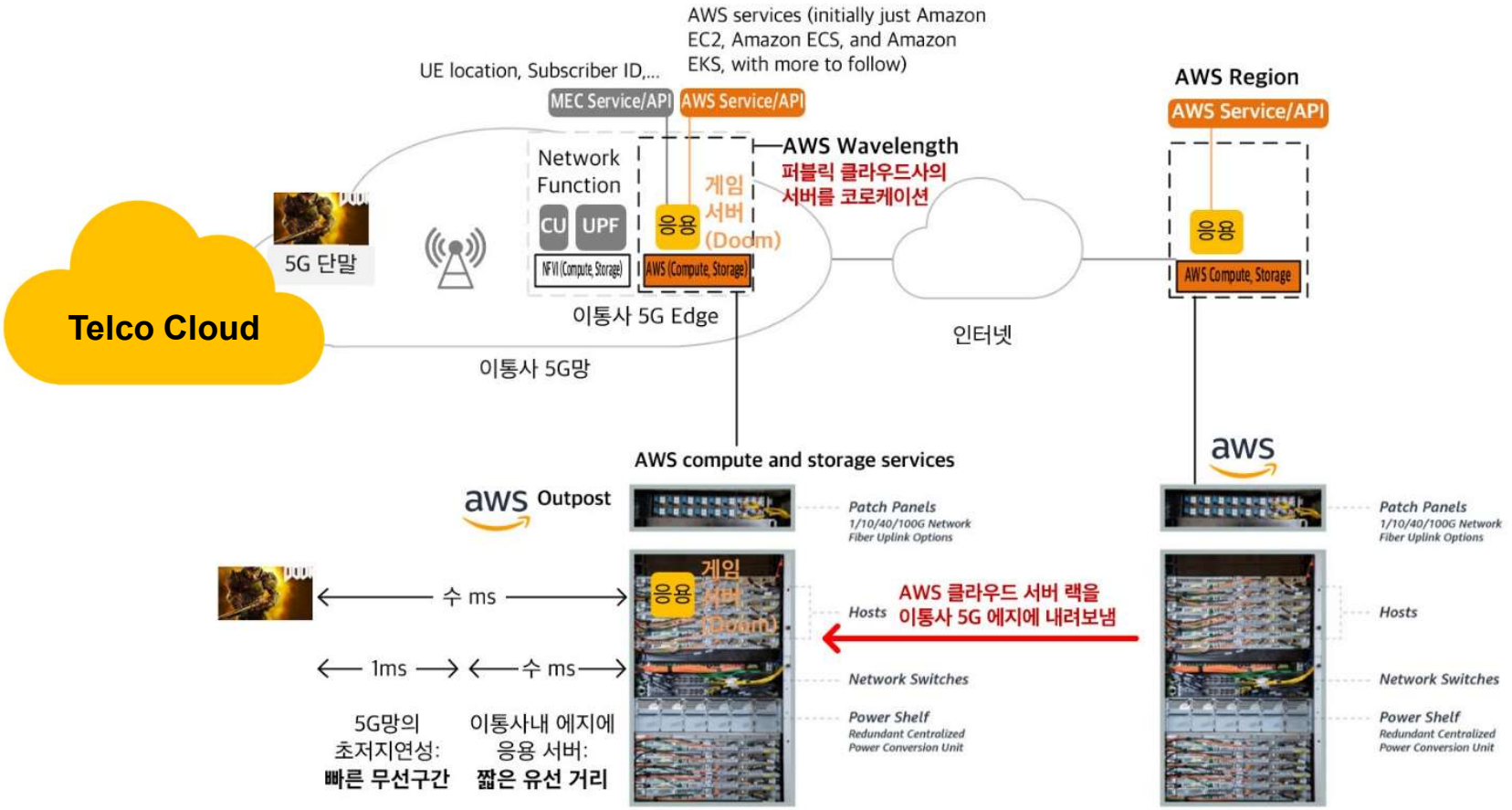
- 현대화 (Multi-Application Modernization)



II. 아키텍처

❖ Telco의 Multi-Cloud Architecture

▪ Telco Cloud 설치



james@jslab.kr

I. 개요

II. 아키텍처

III. 기술

IV. 운영 모델

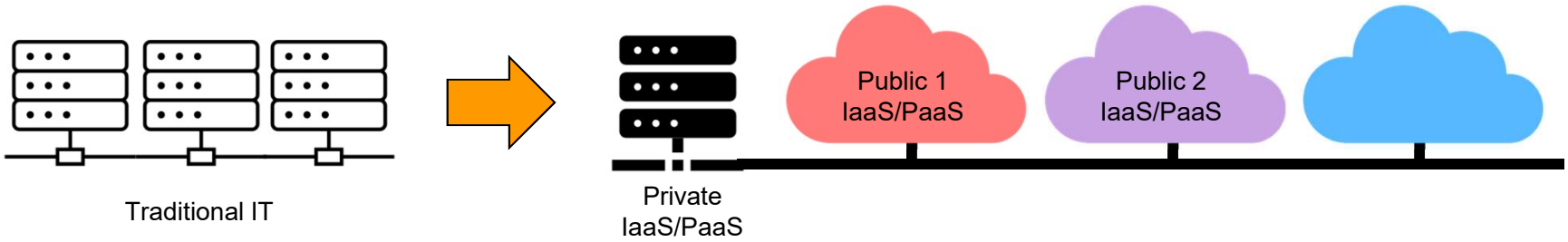
V. 네트워킹

VI. 관리

III. 기술

❖ 클라우드 운영 모델의 변화

- **Run:** 전용 인프라 → 클라우드 상의 스케듈링
- **Connect:** 고정 IP 주소 → 서비스 기반 유동 IP
- **Secure:** IP 주소 기반 보안 정책 → Identity 기반
- **Provisioning:** 전용 서버 → 요청 기반 용량



james@jslab.kr

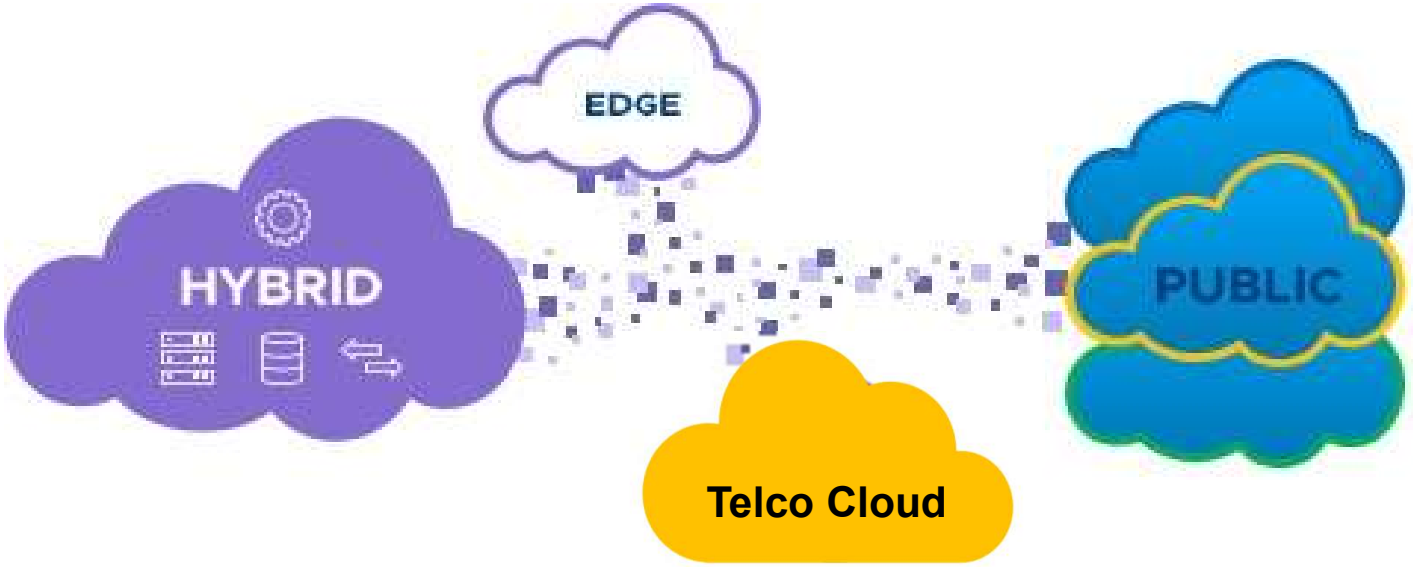
III. 기술

❖ Public Cloud 구성

- Infrastructure Provisioning
- Security
- Service Networking
- Application Delivery

❖ Telco Cloud 구성 추가 고려 사항

- 하드웨어 계층 고려
- 가상화 계층 고려(SDDC)



https://blogs.vmware.com/telco/delivering-applications-and-services-for-a-multi-cloud-and-5g-network-with-vmware-vcloud-nfv-3-0/

III. 기술

❖ Transitioning to a Multi-Cloud Environment – Challenges

- **Networking:** 네트워크 계층의 전환 - 물리적 위치와 역동적으로 변화하는 서비스와 애플리케이션의 IP 주소 (Dynamic registry of services for discovery, segmentation, and composition)

Network Services / Function	AWS	Azure	Google
Network Administration	Account	Subscription	Project
Virtual Network	VPC & Subnets	VNET & Subnet	VPC and Sub-Network
DNS	Route 53	Traffic Manager	Cloud DNS
VPN	VGW	VPN Gateway	VPN Gateway
Peering	AWS Peering or DirectConnect	Azure Peering or ExpressRoute	Google Cloud Interconnect
Load Balancer	ELB	NLB	Cloud Load Balancer
Security	Sec Groups	Network Security Groups	Network ACLs
Storage	S3	Blob Storage	Cloud Storage
Notifications	SNS	Notification hubs	Cloud Messaging
Messaging	SQS	Batch	Pub/Stub
Logging	CloudTrail	Operational Insights	Cloud Logging
Monitoring	CloudWatch	Application Insights	Cloud Monitoring

https://aviatrix.com/learn-center/answered-multi-cloud/how-to-do-multicloud-networking-abstraction-and-orchestration-across-aws-azure-and-google/

III. 기술

❖ 복잡성 단순화 (Simplifying Complexity)

- **단순화 필요:** While a multi-cloud strategy will help to avoid vendor lock-in, increase reliability and protect mission-critical data, it has inherent complexity. Before leaping into multi-cloud, consider these few potential methods to simplify the complexity.
- **단순화 방안** (Potential Methods)
  - ✓ **SD-WAN or Software-defined networking**
  - ✓ **Cloud On Ramp Service Providers**
  - ✓ **Carrier-Neutral Colocation Services**
  - ✓ **AWS Direct Connect**
  - ✓ **Azure Express Route**
  - ✓ **Products and Services from Local Vendors**

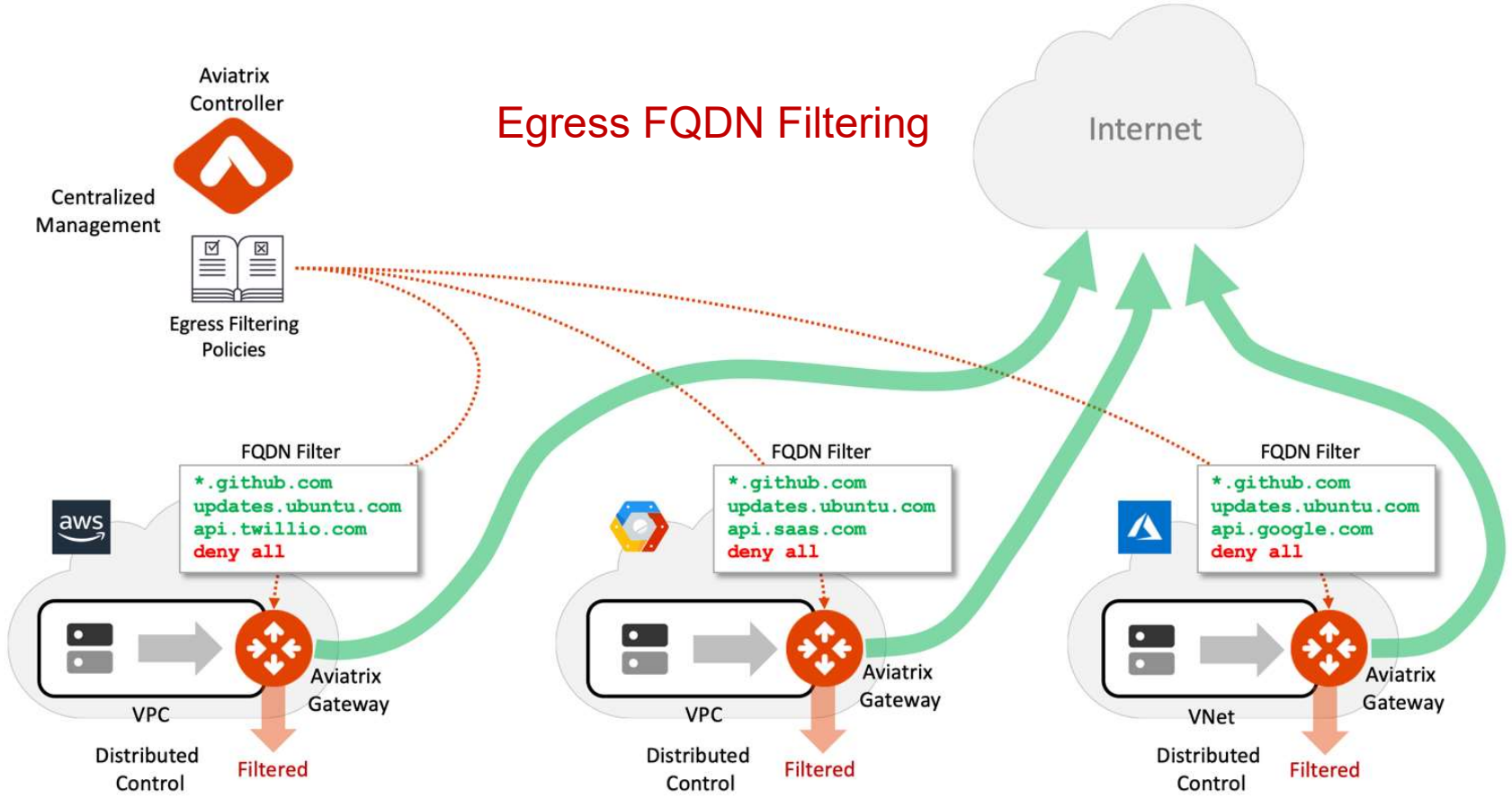
james@jslab.kr

III. 기술

❖ Multi-Cloud 운영 이슈

III. 기술

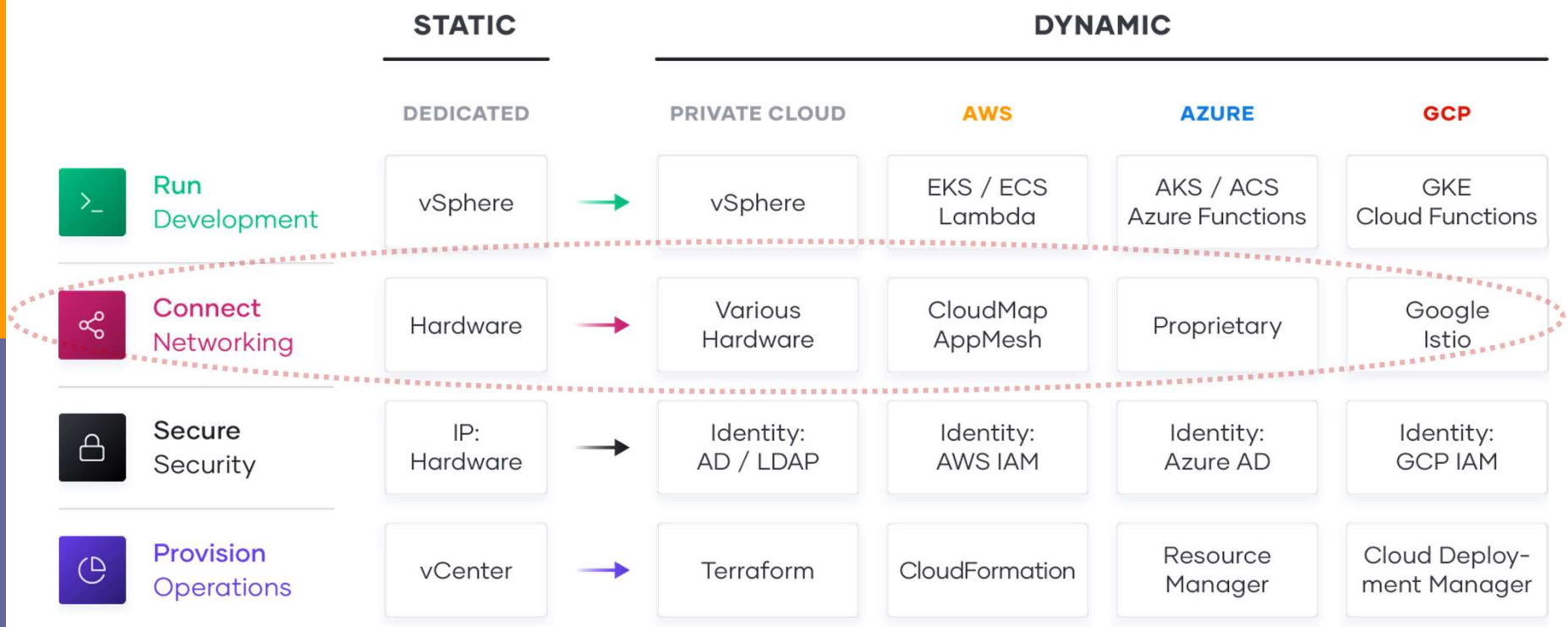
❖ 제조사 (예) - Aviatrix



III. 기술

❖ 멀티 클라우드 사용 기술 확대 (예)

- **Enterprise IT 고려**
- **제공 기술 별 도구**
- **Telco Cloud 전용 도구 필요**



https://www.hashicorp.com/cloud-operating-model

james@jslab.kr

I. 개요

II. 아키텍처

III. 기술

IV. 운영 모델

V. 네트워킹

VI. 관리

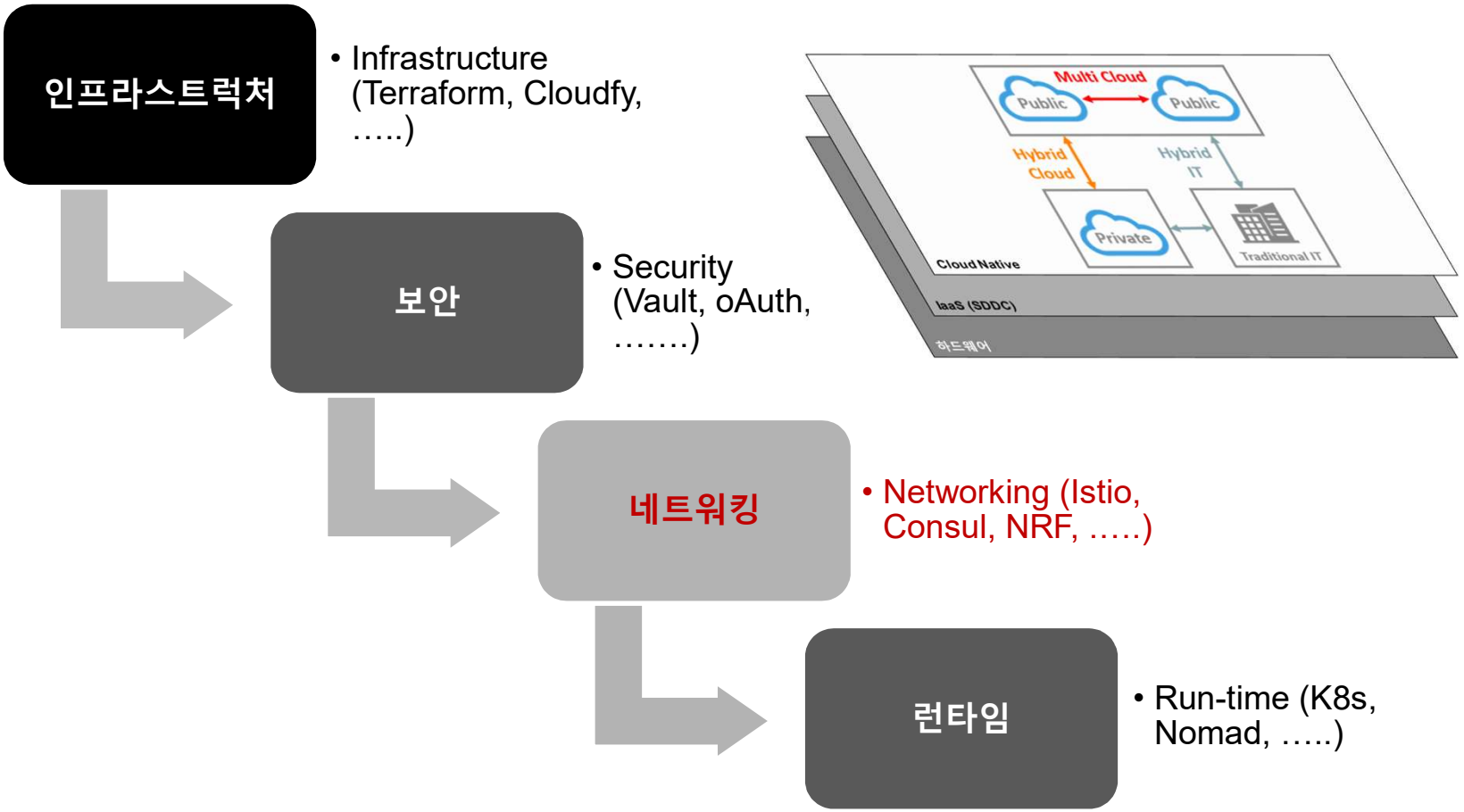
IV. 운영 모델

- 담당자: multi-cloud 기술 보유
  - 멀티클라우드 환경 재사용 기술 보유
  - 분산 환경 DevSecOps 등 continuously deliver를 위한 애자일(Agile) 도구
- 프로세스: 셀프 서비스 IT
  - 위험을 최소화하며 서비스 적용을 위한 Central IT 기반 애플리케이션 제공
  - 클라우드 각 계층간 셀프 서비스 제공
- 도구: 동적 환경 지원
  - 분산 처리 환경에서 특정 기술에 의존하지 않는 도구 사용
  - 셀프 서비스 환경의 빠른 준수 (compliance)로 위험을 관리하는 도구 사용

james@jslab.kr

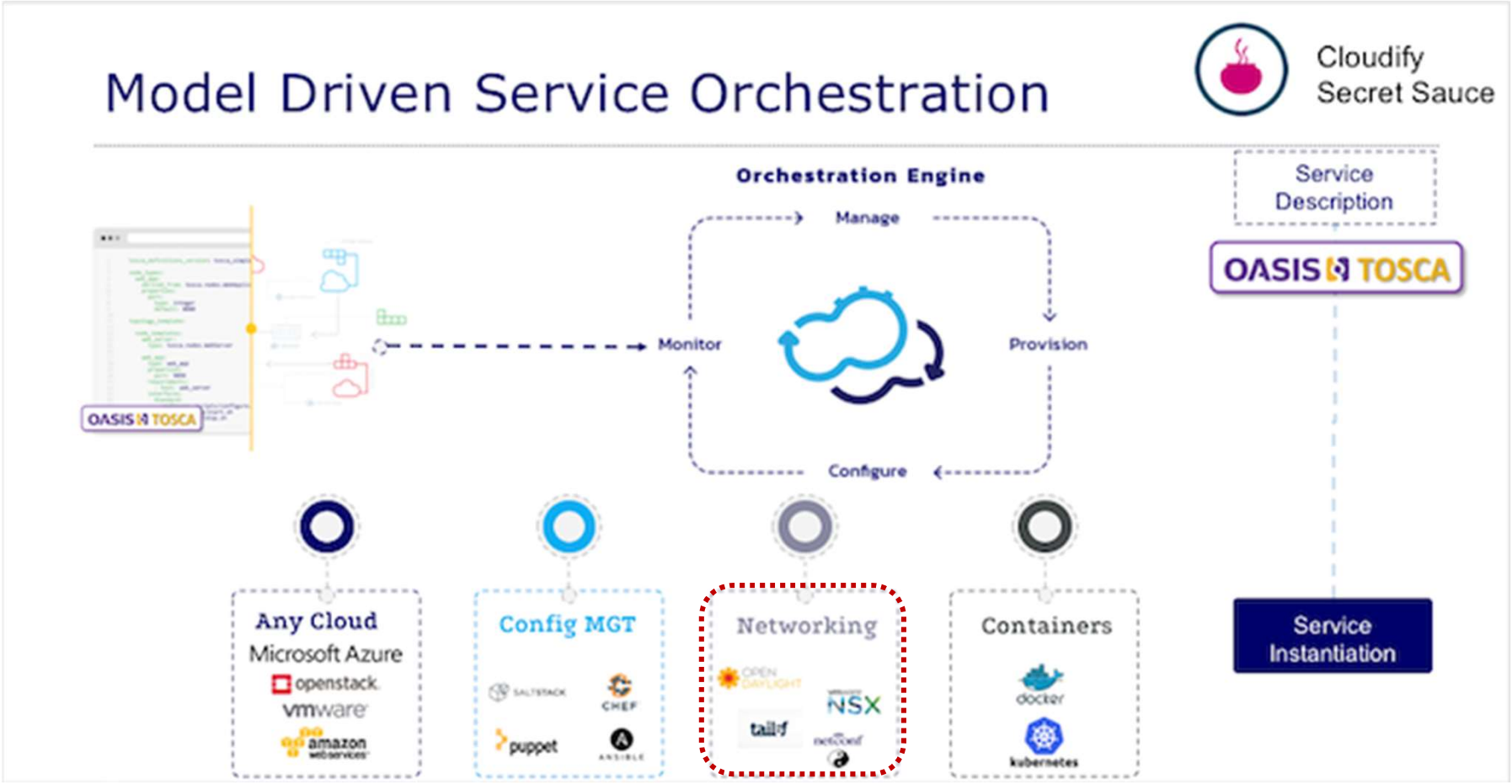
IV. 운영 모델

❖ 클라우드 구성



IV. 운영 모델

❖ Multi-Cloud Service Networking

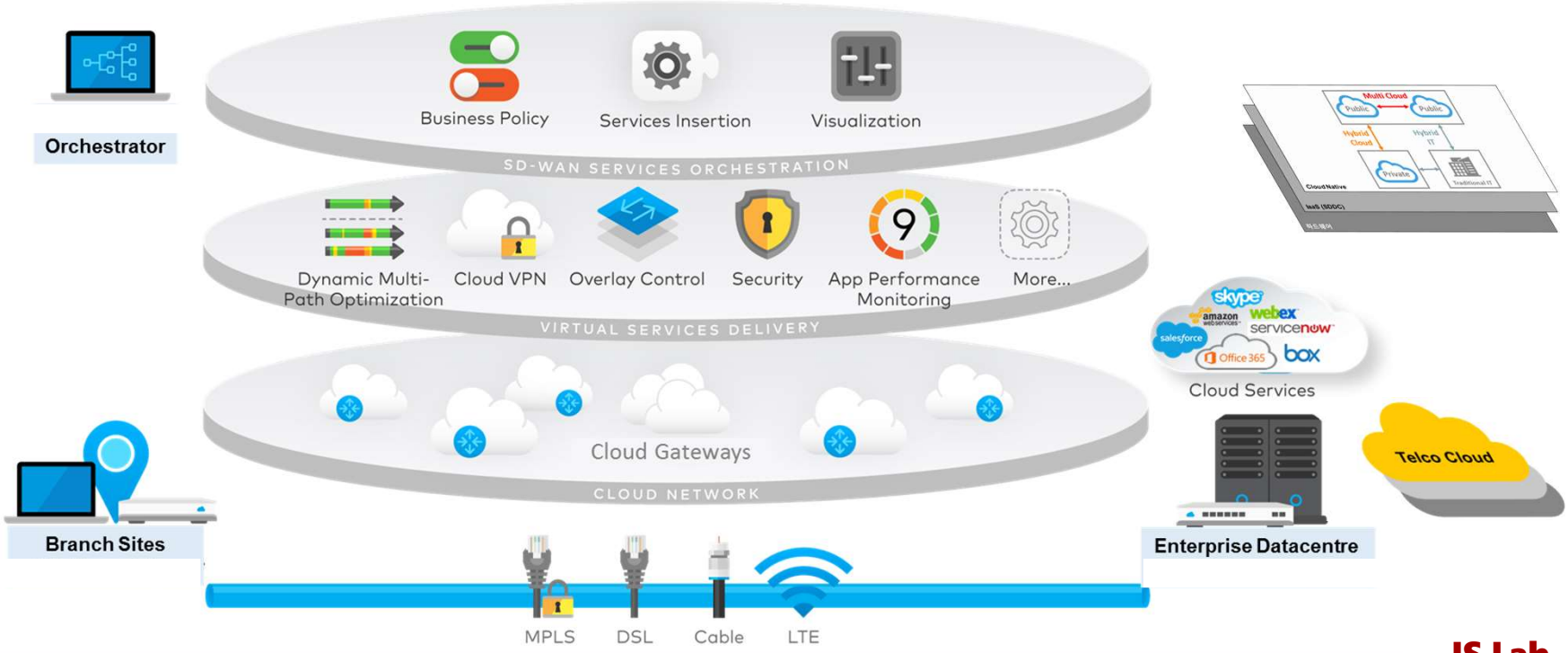


https://cloudify.co/blog/edge-cloud-service-orchestration-with-azure-and-azure-stack-hybrid-multi-cloud-cloudify/

IV. 운영 모델

❖ 클라우드 계층별 네트워크 요소

- **물리적 연결:** MPLS, DSL, Cable, 4G/5G
- **클라우드 게이트웨이:** 멀티 클라우드 게이트웨이
- **운영:** 다중 경로 최적화, 클라우드 VPN, 오버레이 제어, 보안, 성능 모니터 등
- **서비스:** 비즈니스 정책, 서비스 추가, 가시화



Contributor: Aravindhan

james@jslab.kr

I. 개요

II. 아키텍처

III. 기술

IV. 운영 모델

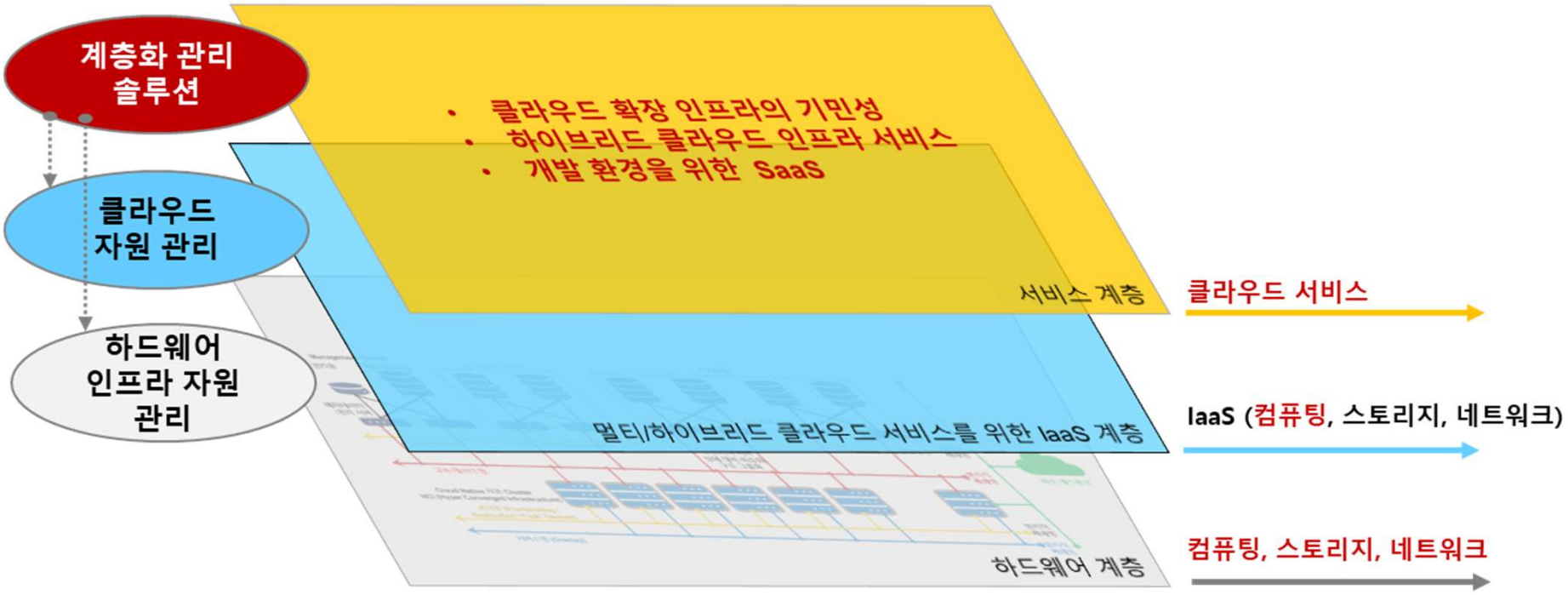
V. 네트워킹

VI. 관리

V. 네트워킹

❖ 멀티 클라우드 네트워킹의 계층 구조

- **클라우드 네트워킹:** 가상과 물리 네트워크와 독립적 추상화
- **가상 네트워크 환경 (Overlay SDN):** OpenStack Neutron, VMware NSX 등
- **물리 네트워크 환경 (Underlay SDN):** OCP Network, Cisco의 ACI 등

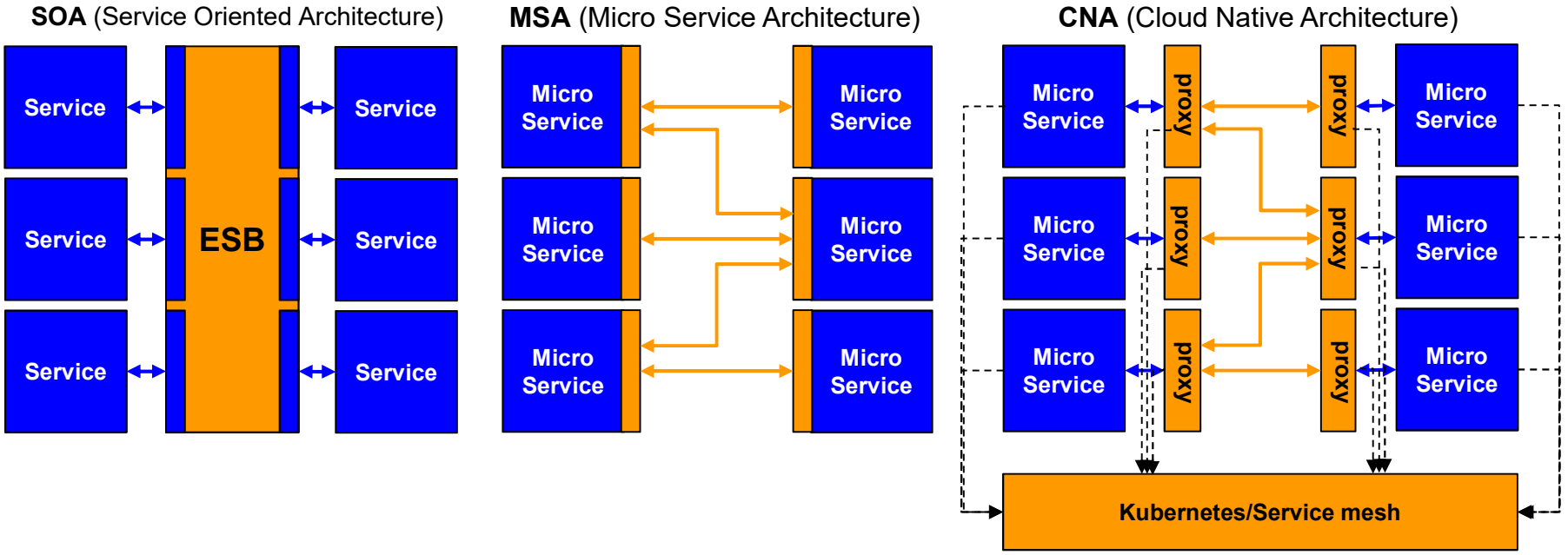


V. 네트워킹

❖ **User Plane – Control Plane 분리 : SDN Architecture**

❖ **컨테이너 기반 아키텍처**

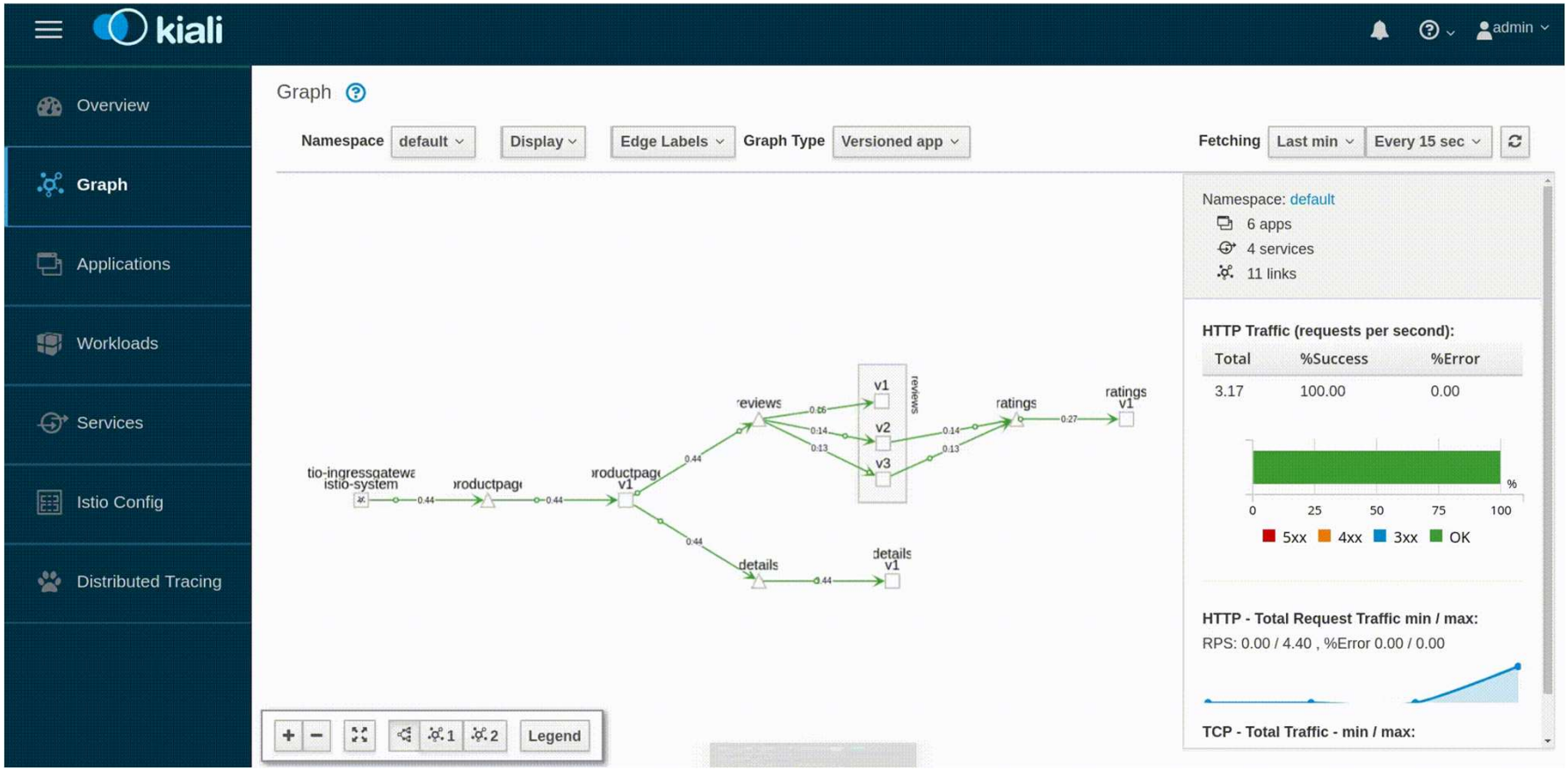
- **SOA** (Service Oriented Architecture): Smart pipes, dump endpoints
- **MSA** (Micro Service Architecture): Smart endpoints, dump pipes
- **CNA** (Cloud Native Architecture): Infrastructure focused smart platform, business logic focused smart services



V. 네트워킹

❖ Multi-Cloud Service Networking

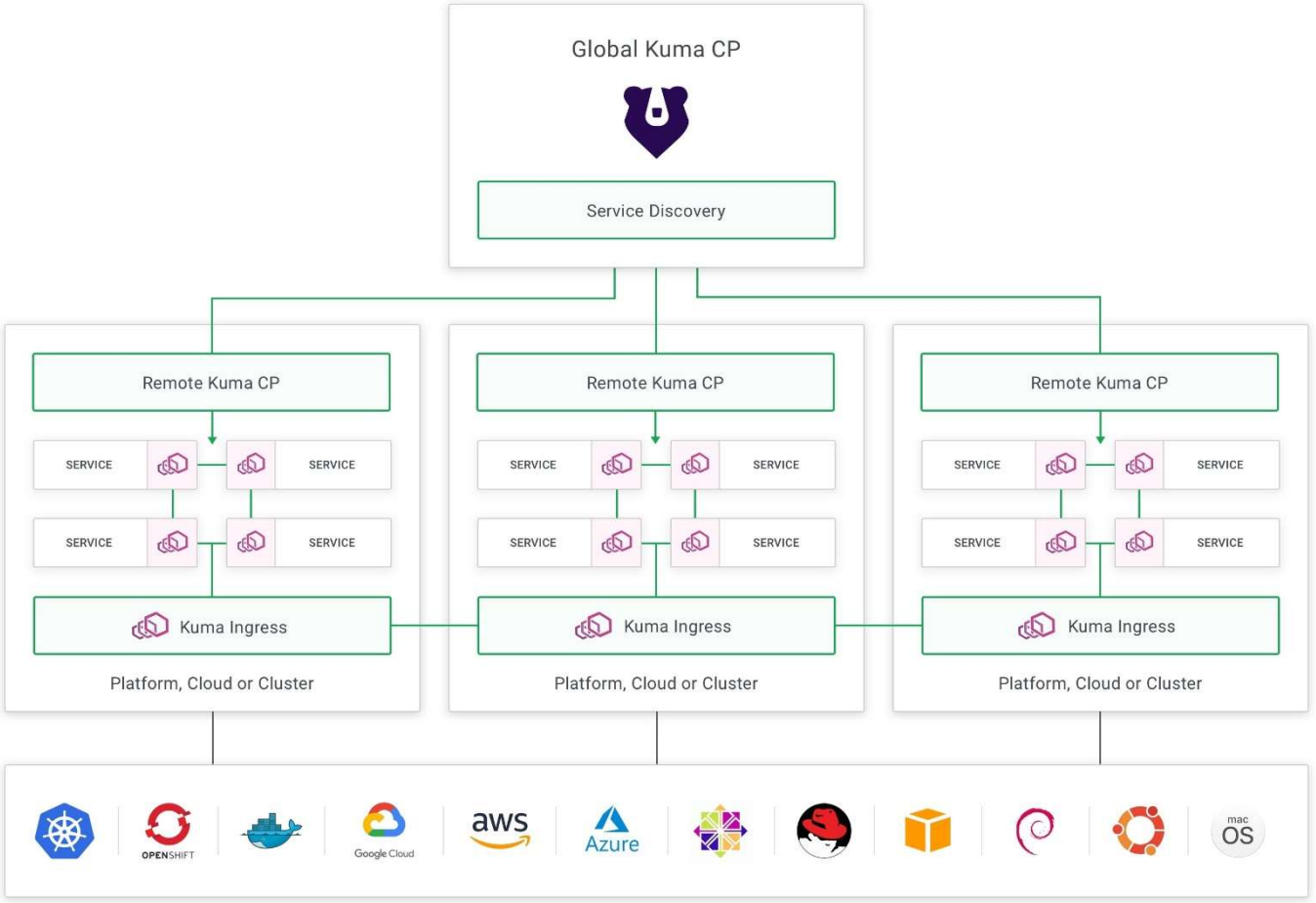
- **Istio (Service Mesh)**



V. 네트워킹

❖ Multi-Cloud Service Networking

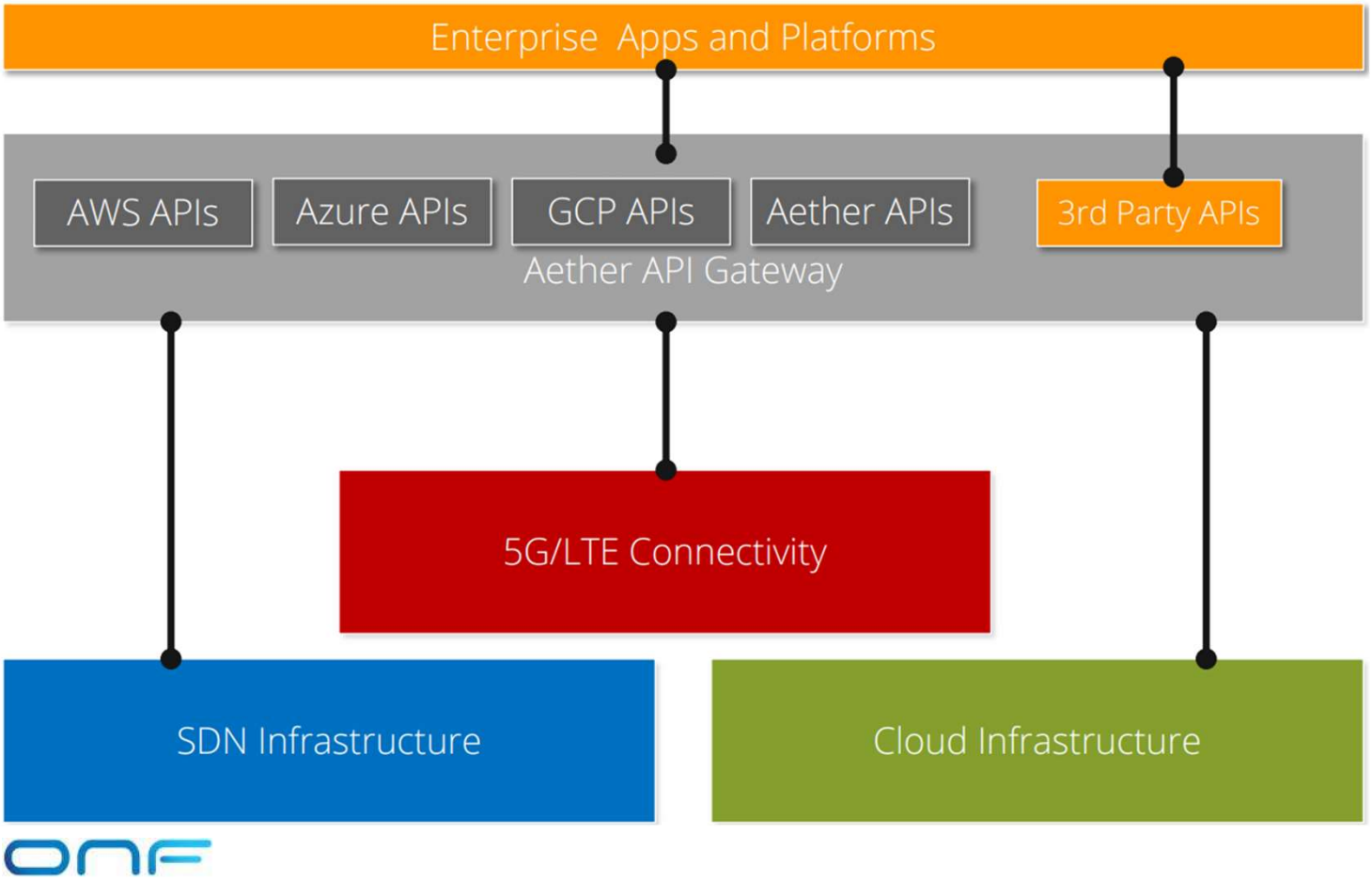
▪ Multi-Cluster & Multi-Cloud Service Mesh with Kuma and Envoy



https://kuma.io/docs/0.6.0/overview/what-is-kuma/#flat-and-distributed-deployments

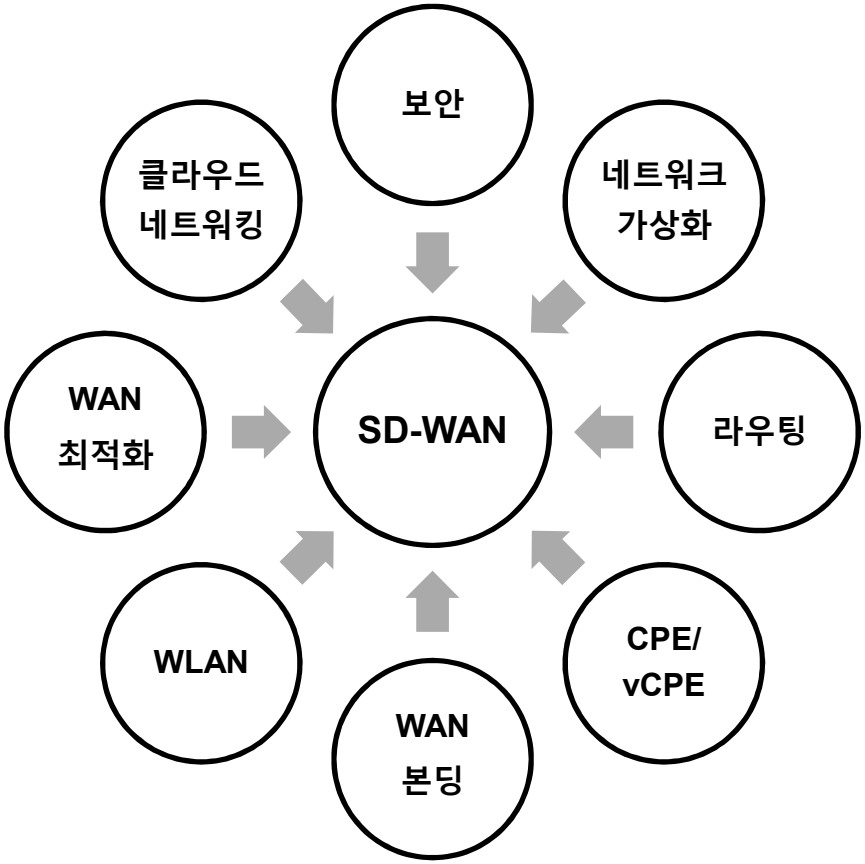
V. 네트워킹

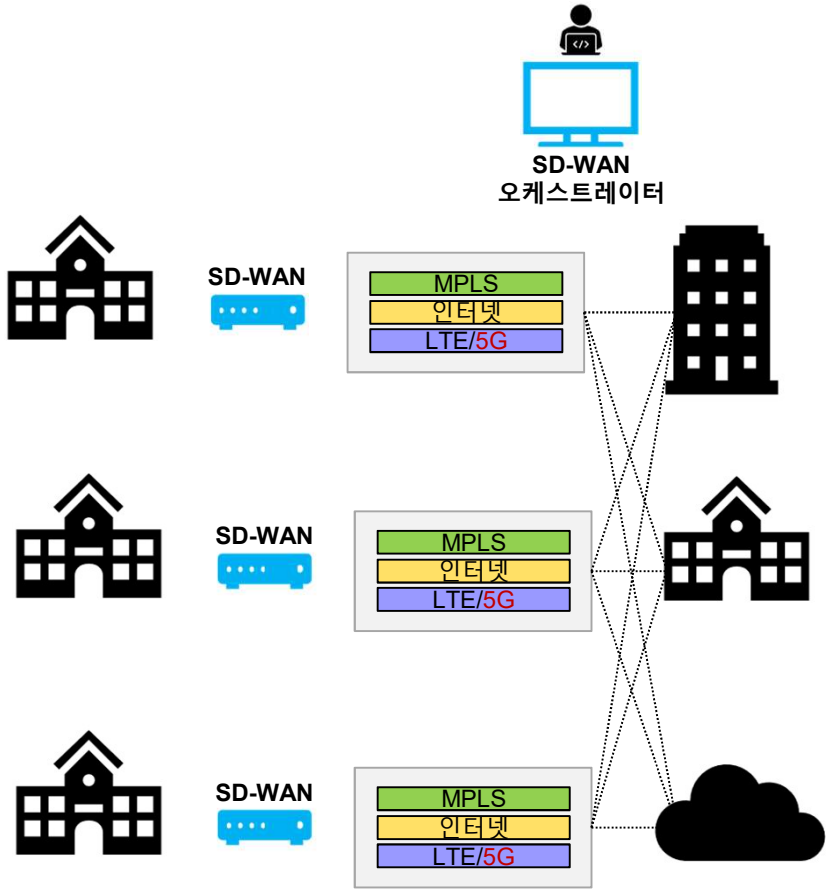
❖ **기업용 Telco Cloud 에지 오픈소스 프로젝트'Aether':** APIs for third-party edge applications and platforms



V. 네트워킹

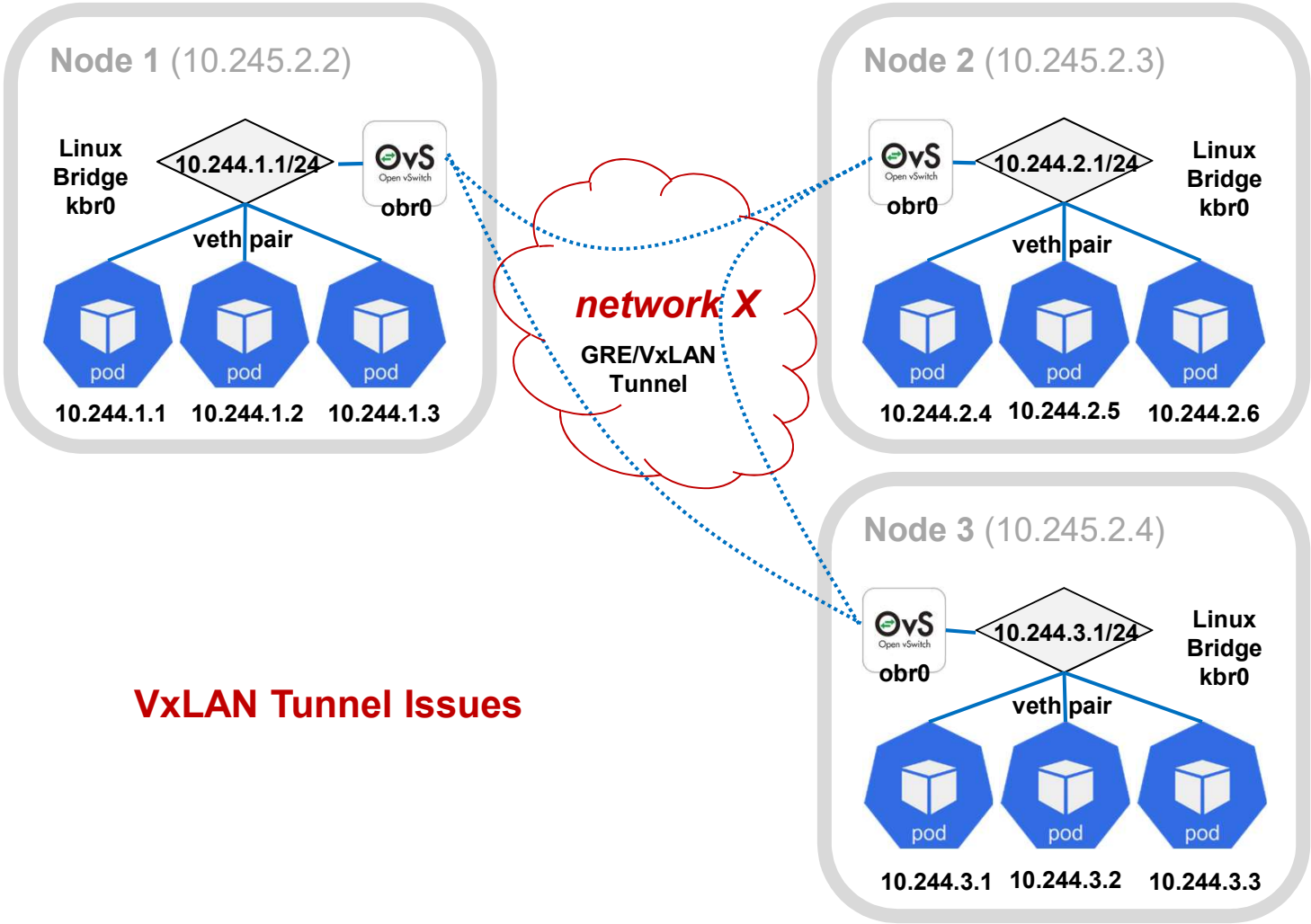
❖ **SD-WAN 확장:** SD-WAN is sometimes viewed as a catch-all marketing term for next-gen enterprise edge solutions (www.sdxcentral.com SDxCentral, 2019)





V. 네트워킹

❖ Clustering for Multi-Cloud

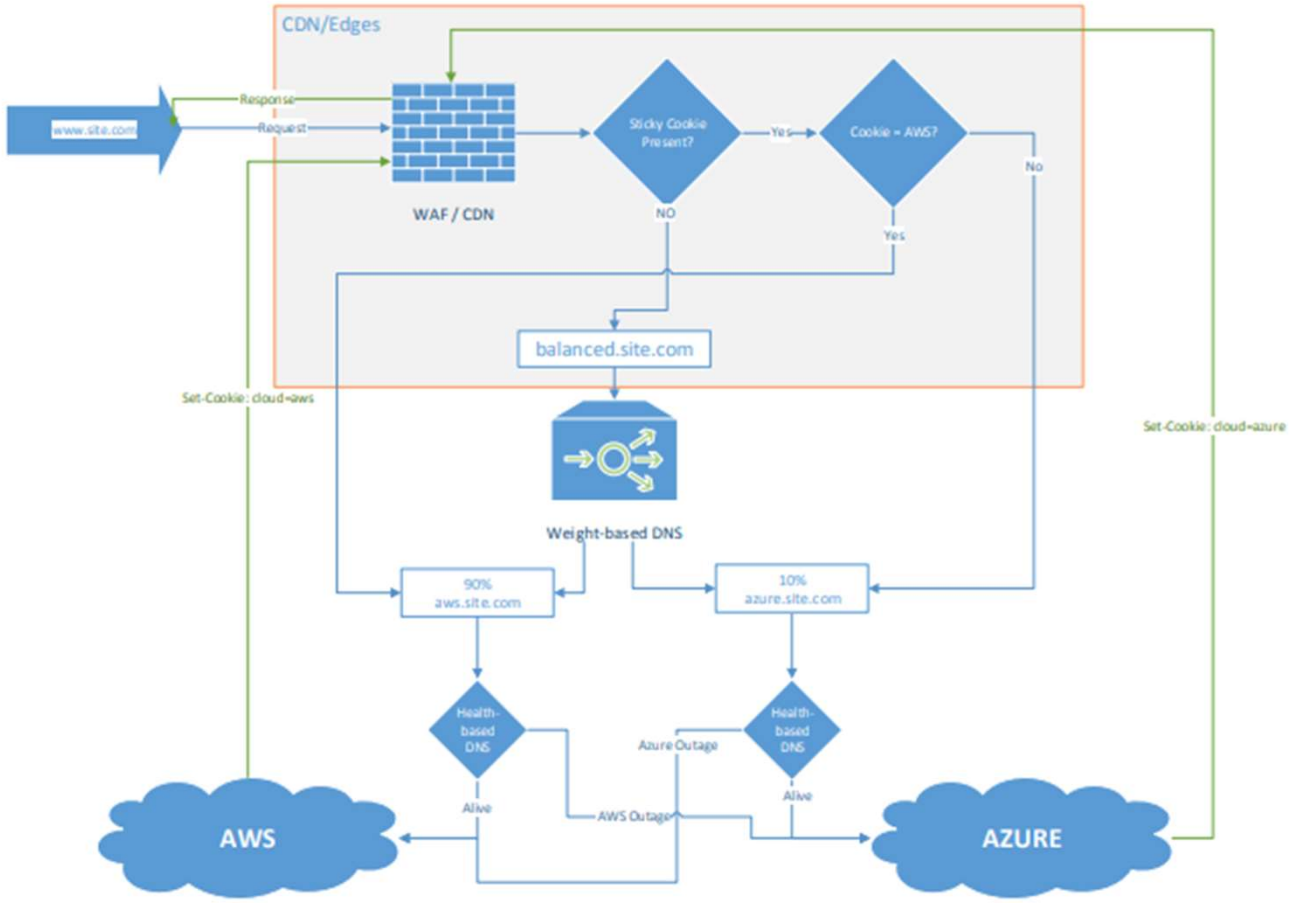


VxLAN Tunnel Issues

V. 네트워킹

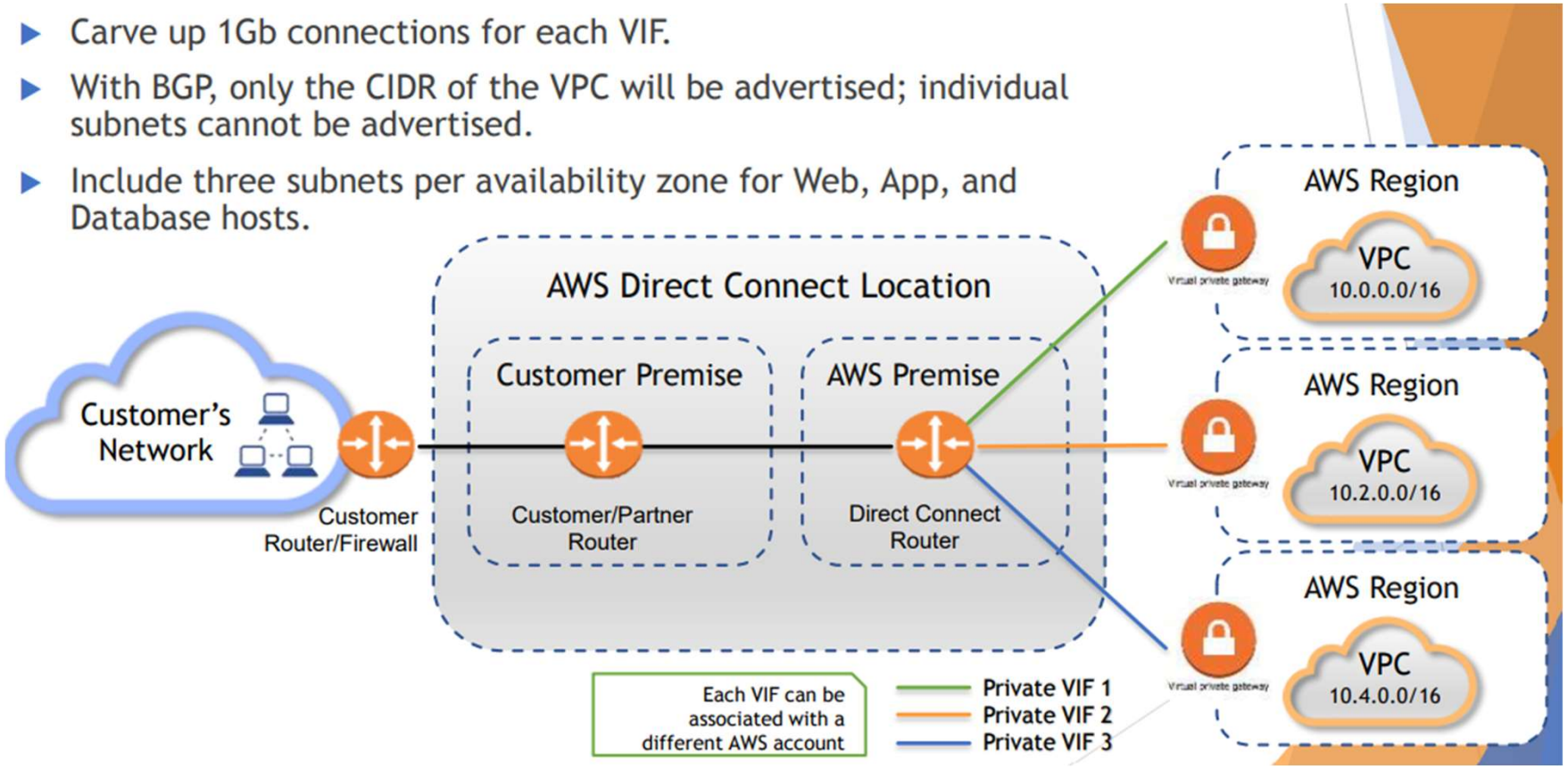
❖ Routing with cloud stickiness

- DNS – weight-based with health checks
- WAF/CDN + Rules Engine (on CDN Edges)
- Location stickiness



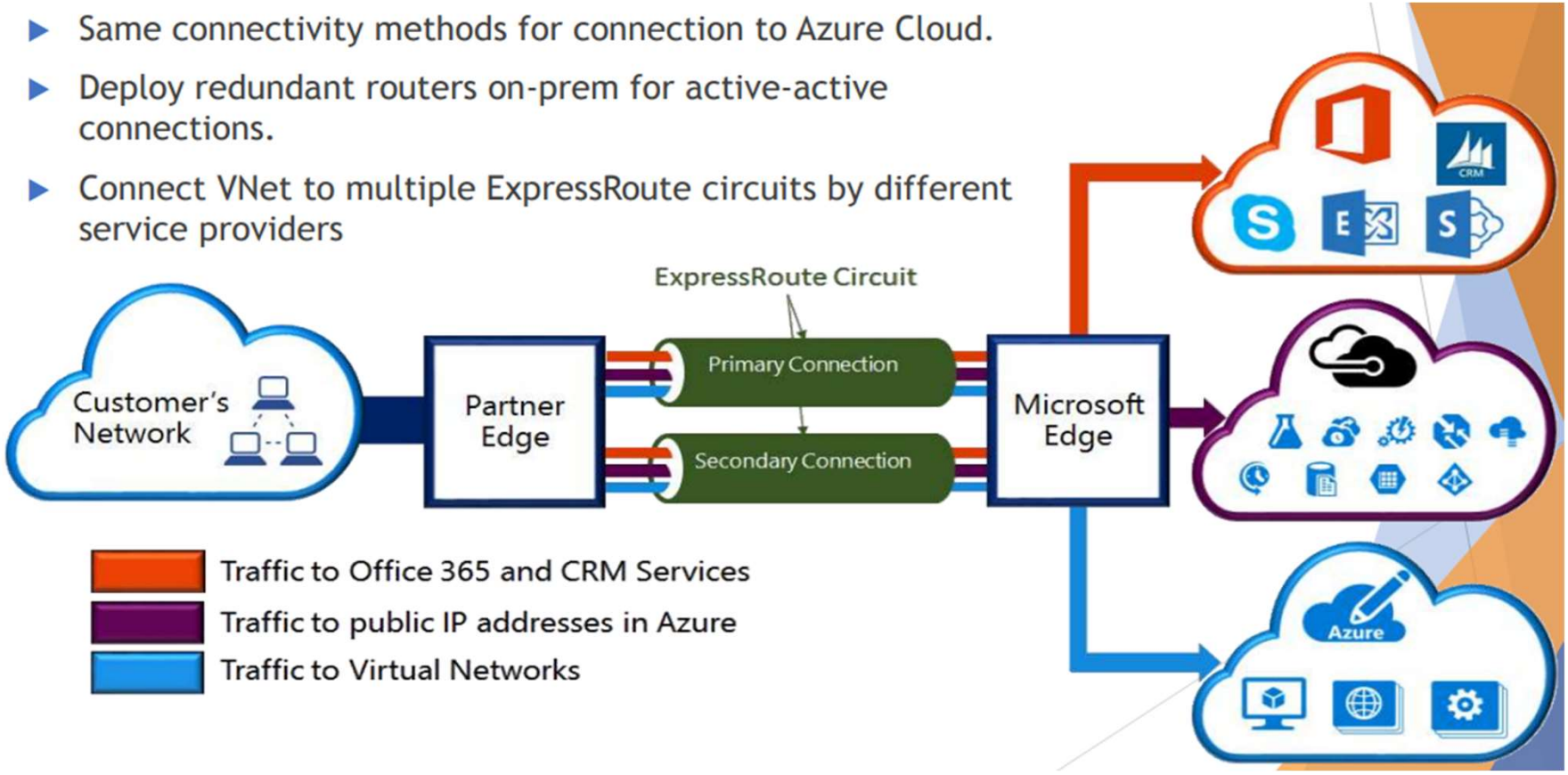
V. 네트워킹

- ❖ **Direct Connect Architecture (AWS)**
- ❖ **Outpost for Hybrid Cloud**



V. 네트워킹

- ❖ **ExpressRoute Architecture (Azure)**
- ❖ **Azure Stack (Edge) for Hybrid Cloud**



V. 네트워킹

- **Security Capability Software Stack**
- **제조사(예): SD-Brance, SD-WAN, SD-Security** (VERSA Networks)

VERSA NETWORKS

Market Leading Security Functions					
Stateful Firewall	CGNAT	URL Feeds and Filtering	Lateral Movement Protection	Malware Protection	File Filtering
DOS Protection	NG-Firewall (NGFW)	IP Feeds and Filtering	Captive Portal	Network DLP (*)	NG-IPS
IPSec	User & Group Authentication	Device Fingerprinting	HTTP / SSL Proxy	DNS Feeds and Security (*)	Anti-Virus

- **Visibility & access control**
  - Application, domain & URL
  - User, device & location
- **Layer 7 & content security**
  - SSL decryption
  - App / URL / IP Feeds and filtering
  - File filtering
  - Anti-virus
  - IPS
  - DNS Security (*)

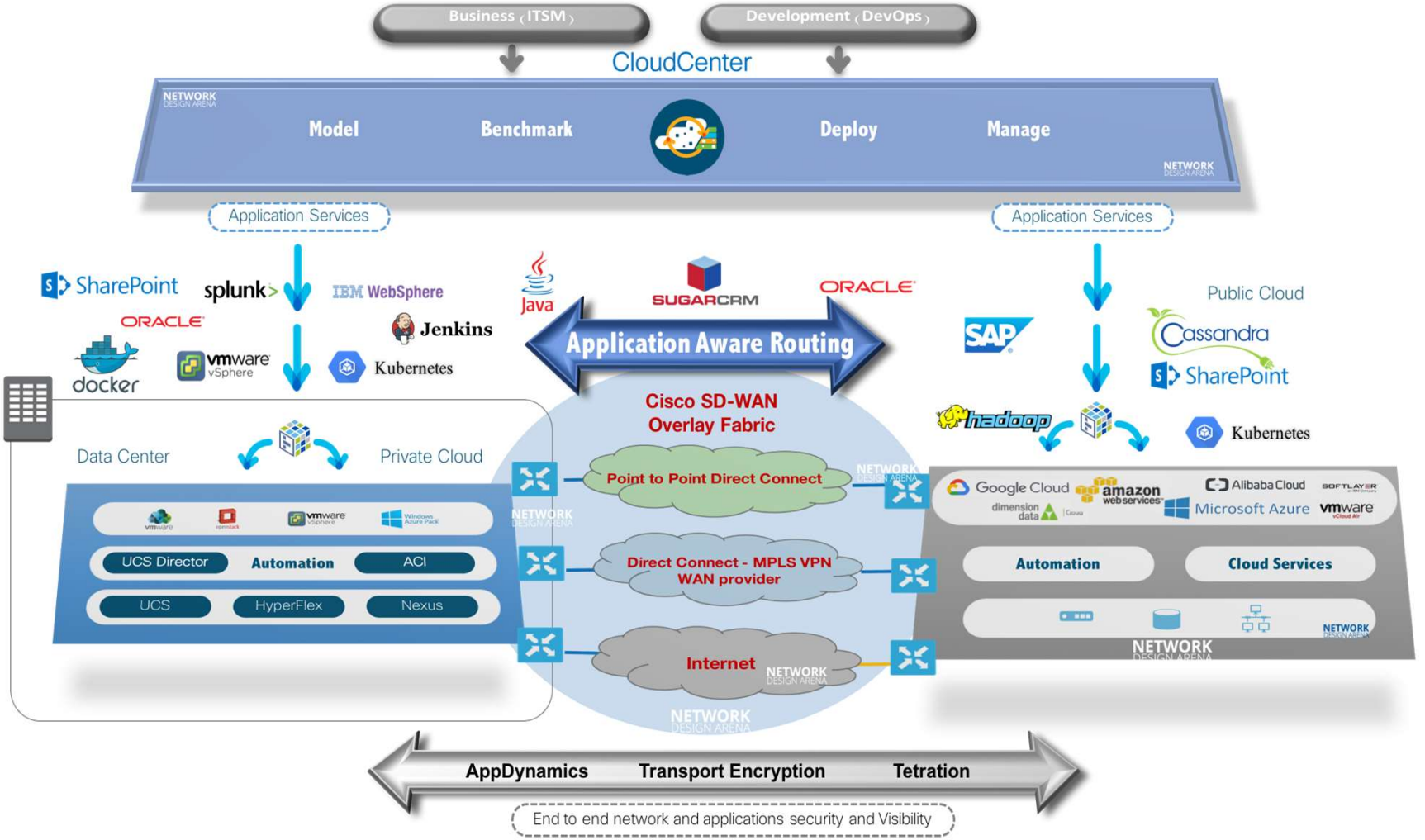
- **Layer 4**
  - Reconnaissance
  - DoS protection (ICMP, UDP, TCP flood)
    - Rate limiting
- **Layer 3**
  - ARP, IP ICMP protocol defence
  - IP spoofing
  - Strict source routing checks
  - Fragment overlaps



Versa Networks, SDxCentral.

V. 네트워킹

❖ Cisco Multi-Cloud – A Cloud Architect Perspective

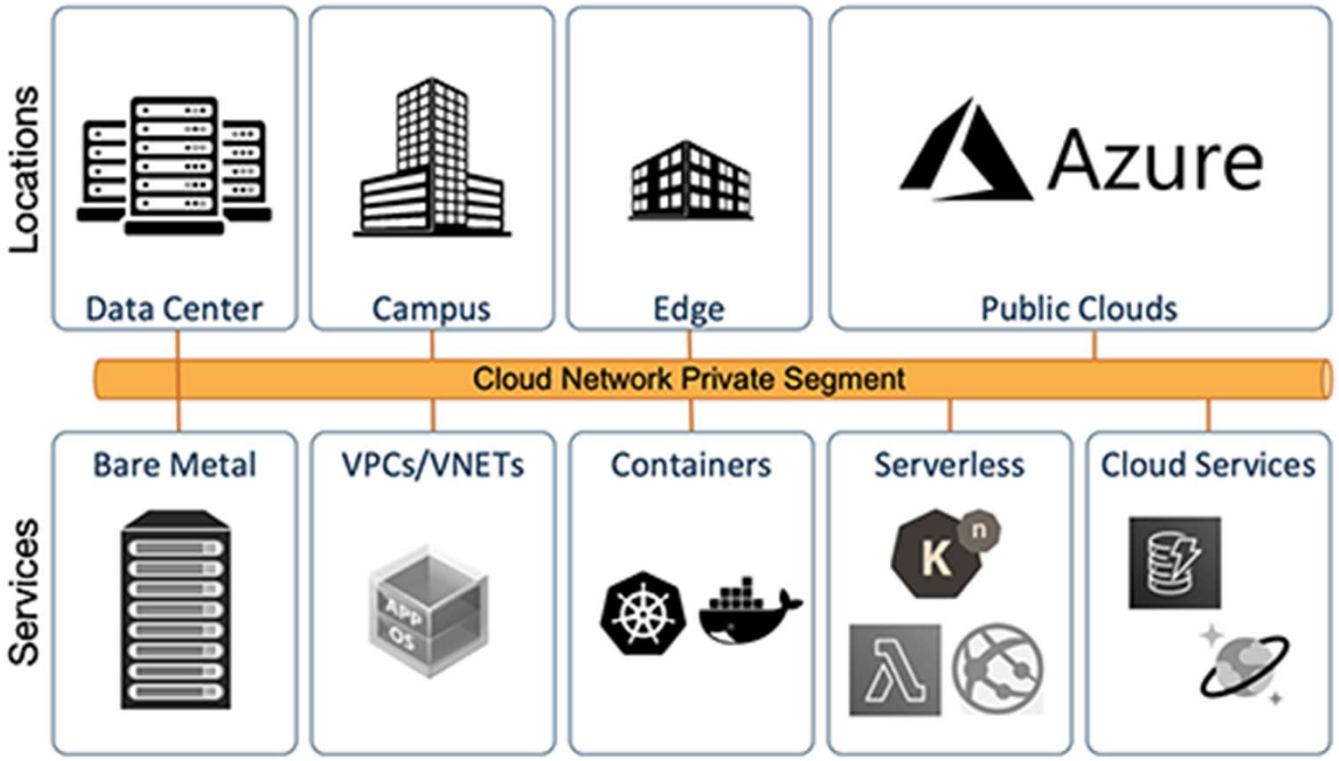


Cisco, https://www.netdesignarena.com/index.php/2018/05/30/why-cisco-multi-cloud-a-cloud-architect-perspective/

V. 네트워킹

❖ Arista

- **CloudEOS Router provides multi-cloud networking and security using proven EOS Software**



https://azuremarketplace.microsoft.com/en-us/marketplace/apps/arista-networks.cloudeos-router-payg?tab=Overview

V. 네트워킹

❖ 클라우드 네트워킹의 복잡성

- **라우팅:** Routing traffic rapidly and securely between disparate cloud platforms is complex; avoid complex Managed VPN solutions
- **자동화:** Automation needed for disparate CLI's, BGP ASN's, and routing tables
- **관리:** Managing multiple cloud, SaaS, network, and colocation providers is a juggling act!
- **중앙 관리:** Every provider will have their own proprietary method for management, monitoring, storage, and network solutions.
- **표준 보안 정책:** Establishing standard security capabilities and policies
- **보안 강화:** Ability to enforce security for users, data, and applications everywhere is essential

james@jslab.kr

I. 개요

II. 아키텍처

III. 기술

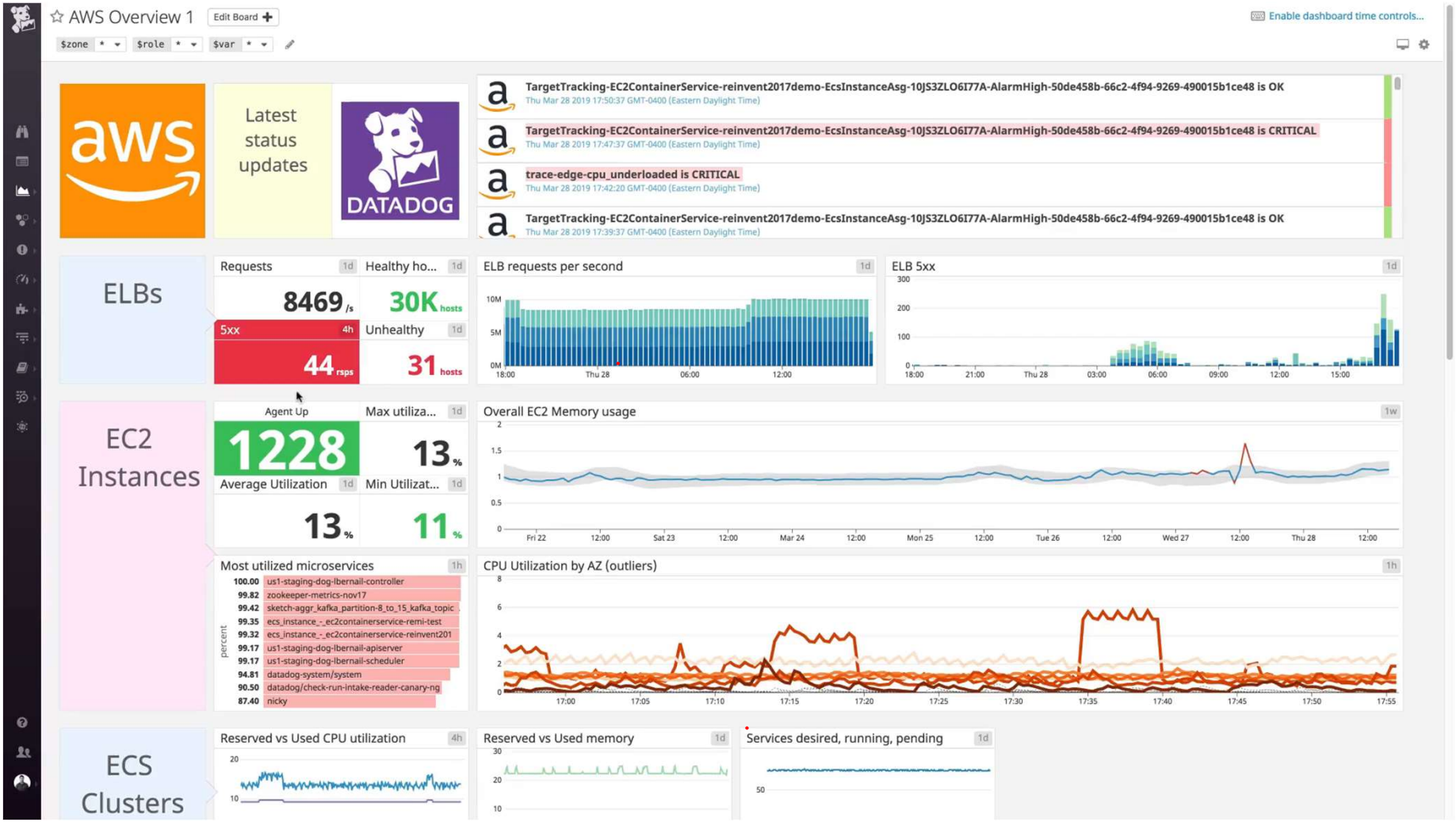
IV. 운영 모델

V. 네트워킹

VI. 관리

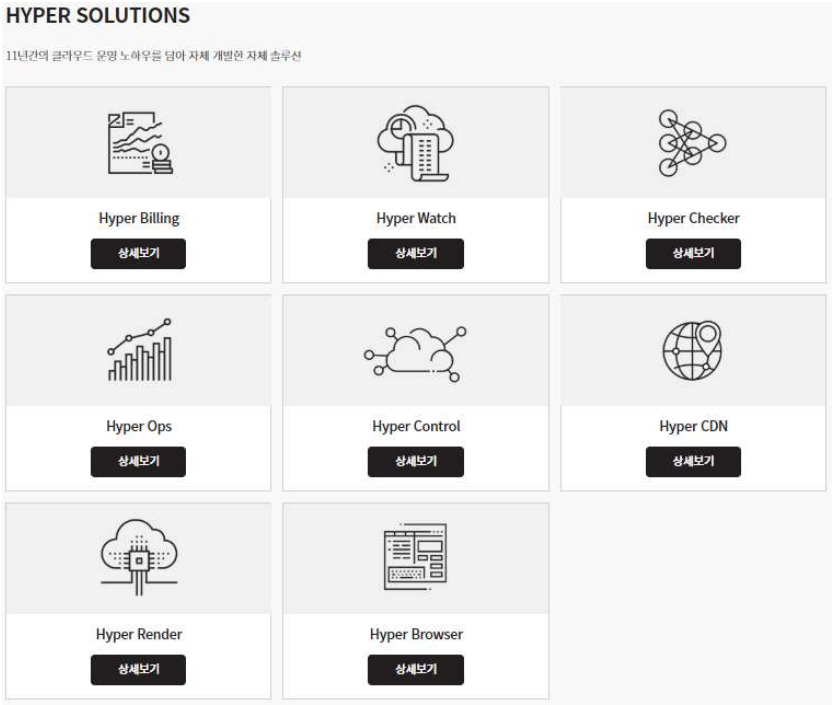
VI. 관리

❖ Datadog



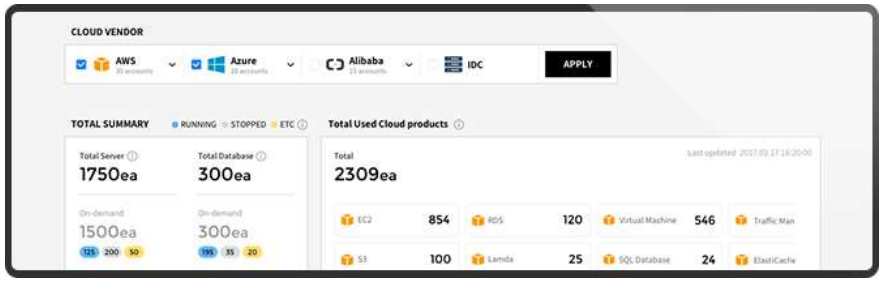
VI. 관리

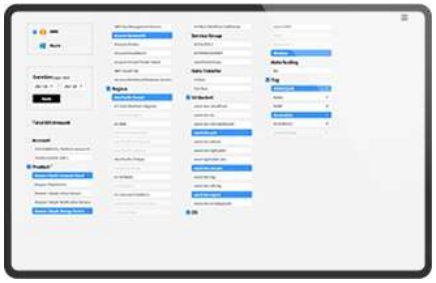
- ❖ 클라우드 관리
- ❖ 국내의 Public Cloud 기반 관리 서비스 제공 레퍼런스
  - OpsNow (베스핀글로벌)
  - Hyper Solutions (메가존)

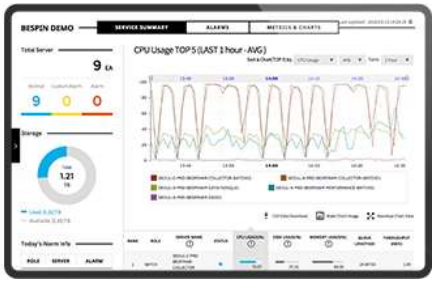


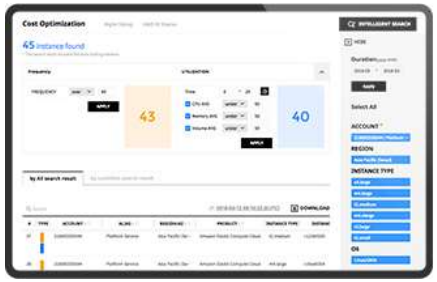
VI. 관리

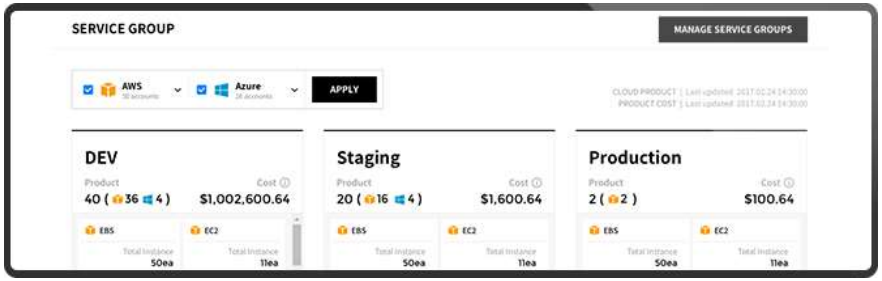
❖ OpsNow







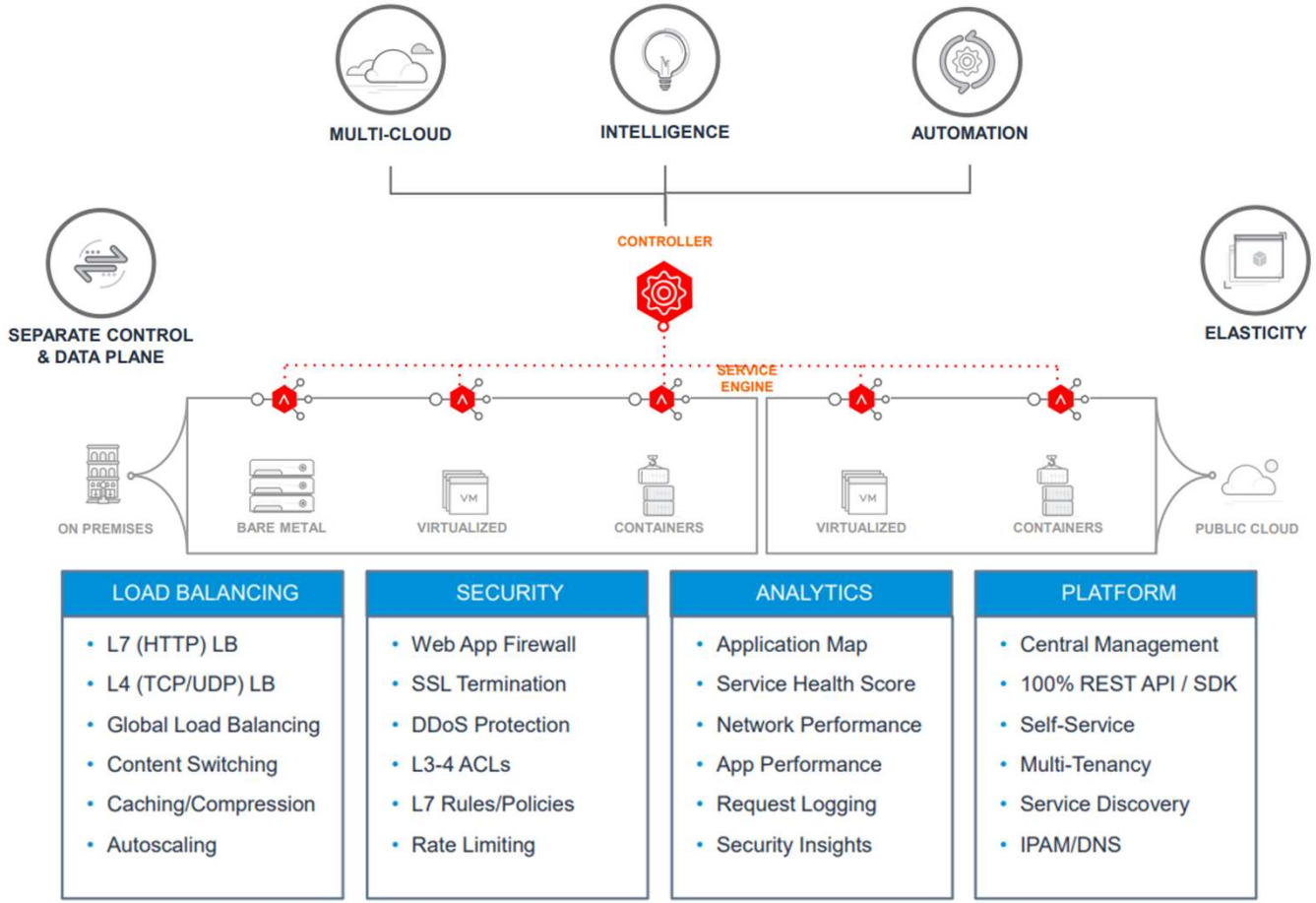




VI. 관리

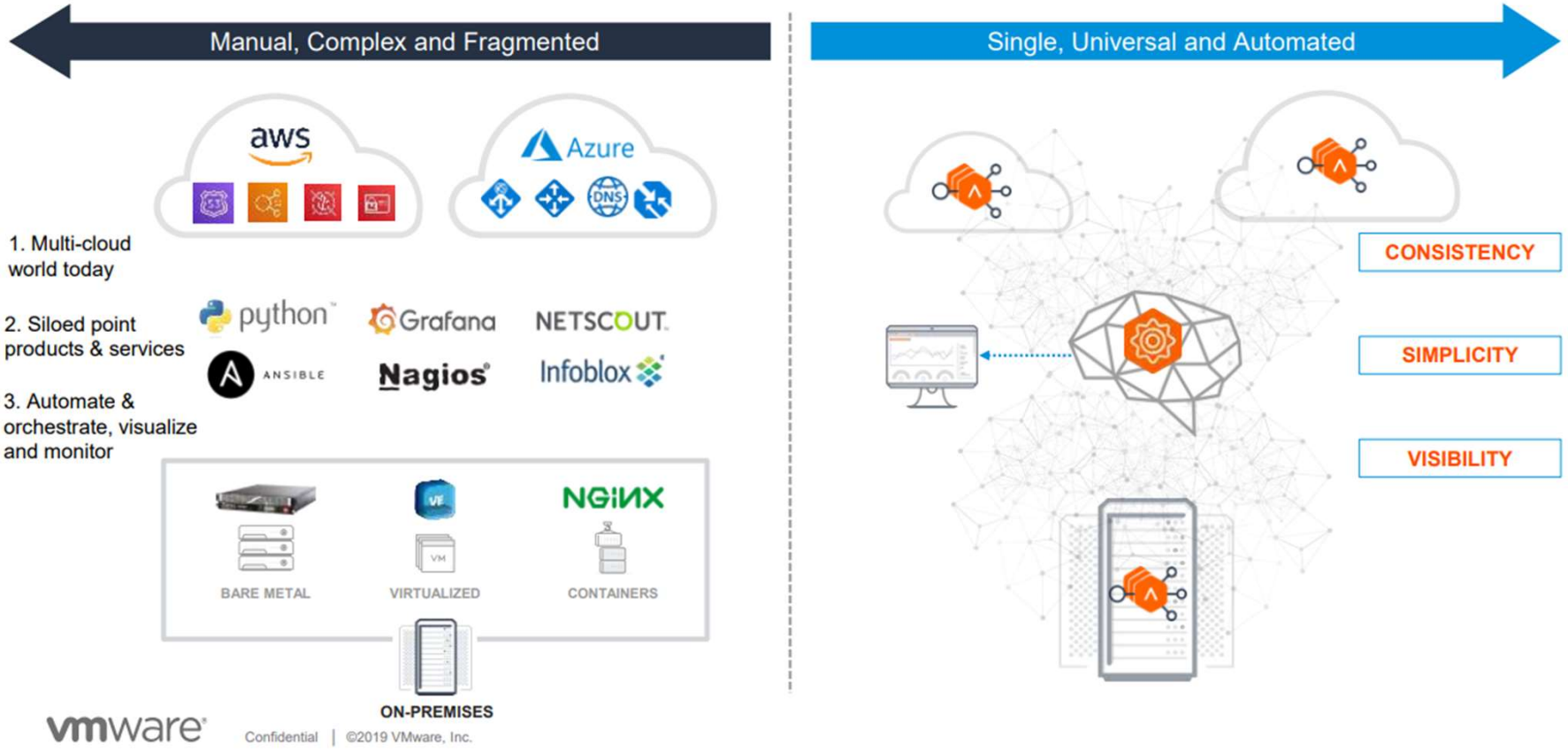
❖ Multi-Cloud Application Services Challenges (VMware/AVI)

■ **Multi-Cloud Architecture** (Virtual Cloud Networking with NSX)



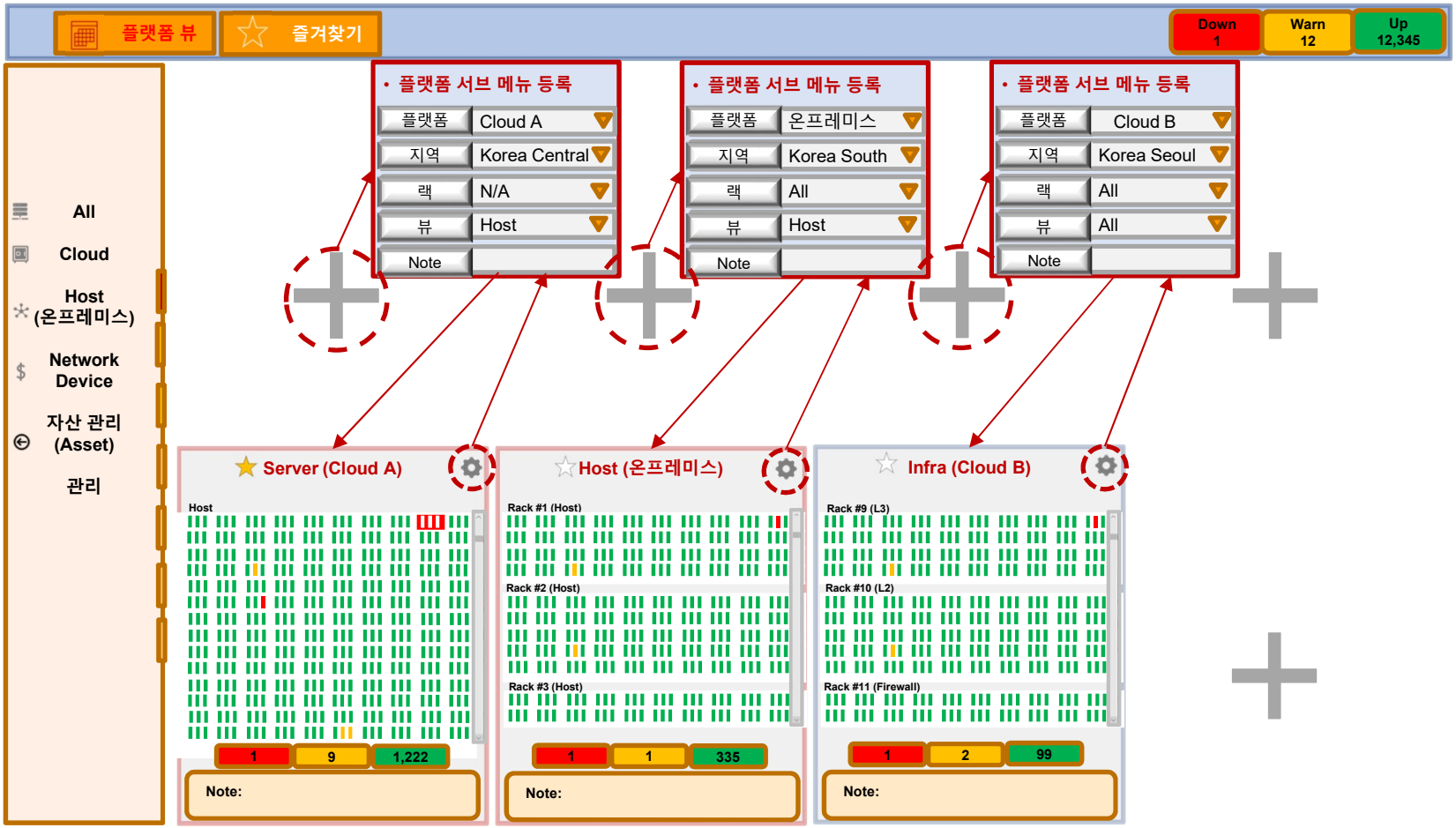
VI. 관리

❖ **Infrastructure-centric Silos to Application-centric Multi-cloud Strategy (VMware/AVI)**



VI. 관리

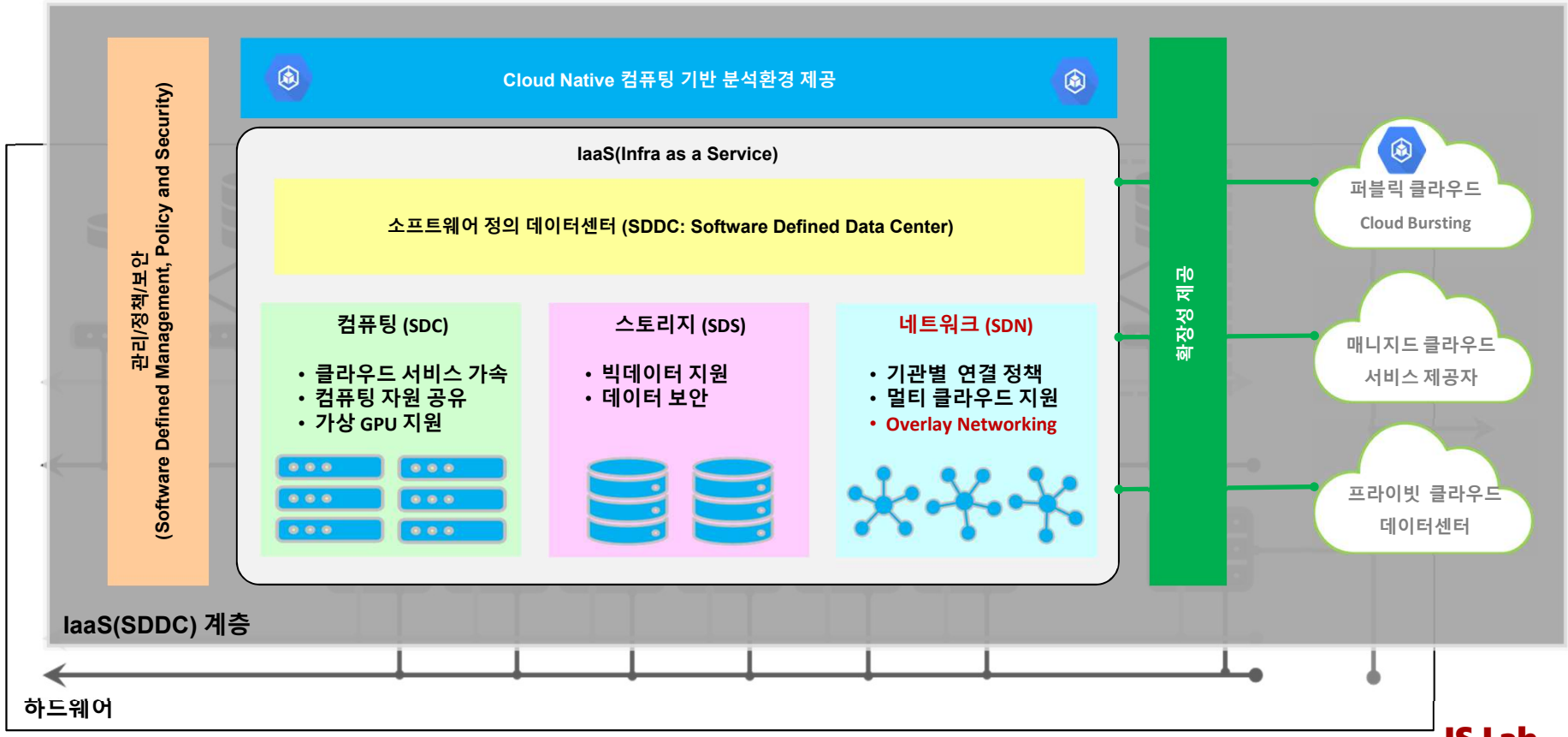
❖ 관리 개발 (예) - Management View Design 복잡성



VI. 관리

❖ 요약

- 하드웨어의 추상화 기반 IaaS 인프라 운영 (SDDC)
- 가상화 자원 제공
- 하이브리드(Hybrid)/멀티(Multi) 클라우드 인프라 서비스



james@jslab.kr