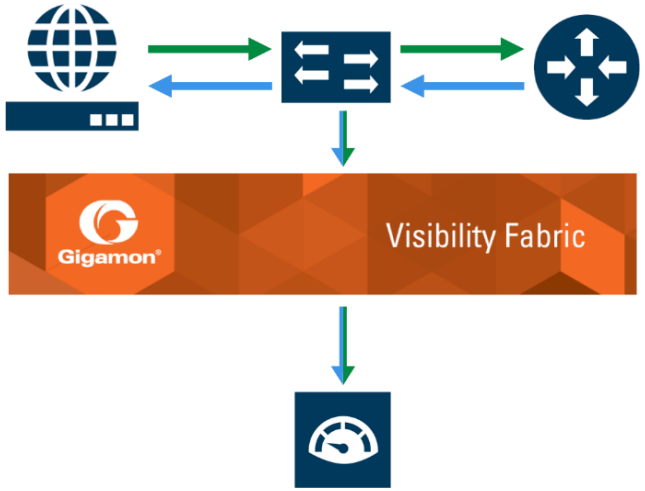
See More Secure More

클라우드 환경에서의 보안 구현을 위한 Software Defined Visibility

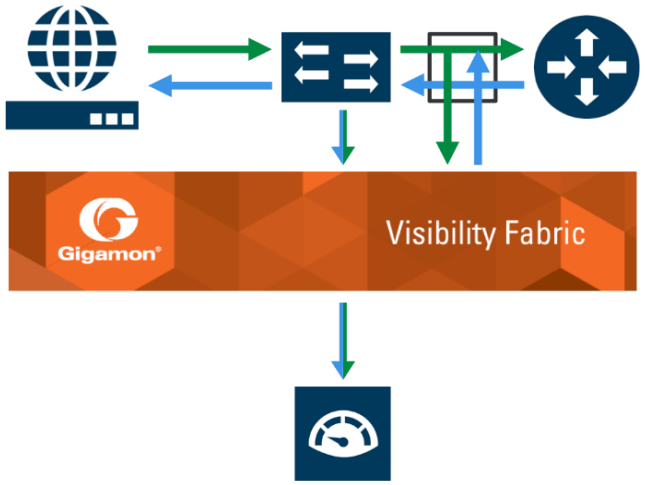
Minhyung Lee
SE, Gigamon Korea

The First Step to Visibility : SPAN vs. TAP

- SPAN(Switch Pot ANalyzer) : Software

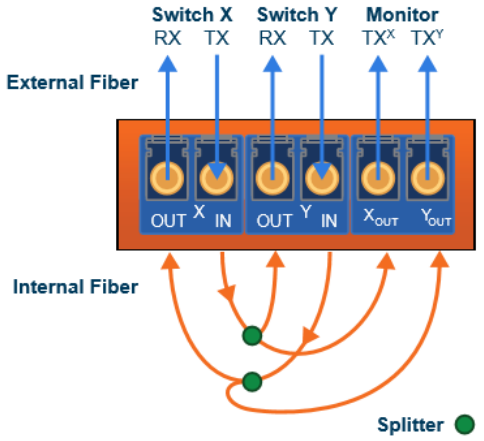


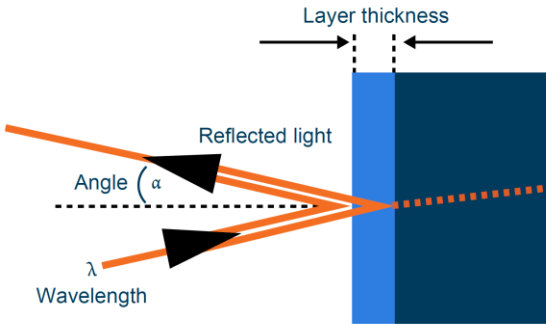
- TAP(Test Access Point) : Hardware

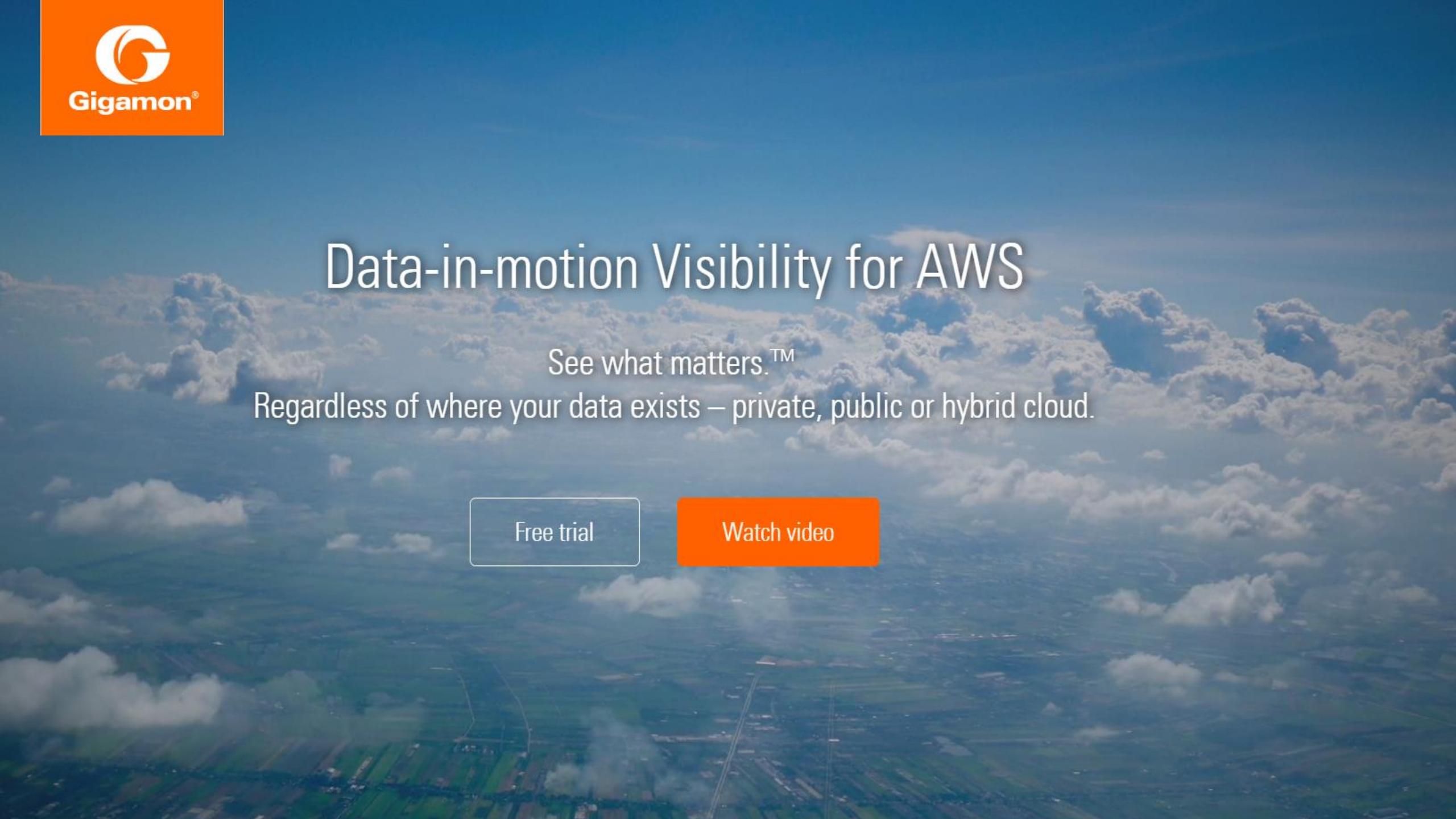


TAP s are preferred because:

1. SPAN ports are easily oversubscribed and can often result in dropped packets
2. The SPAN is processor intensive and can negatively impact the switch (possibly affecting network traffic)
3. Because SPAN traffic is easily reconfigured, SPAN output can change from day to day (resulting in inconsistent reporting)
4. TAPs forward all packets (including errors) at line rate





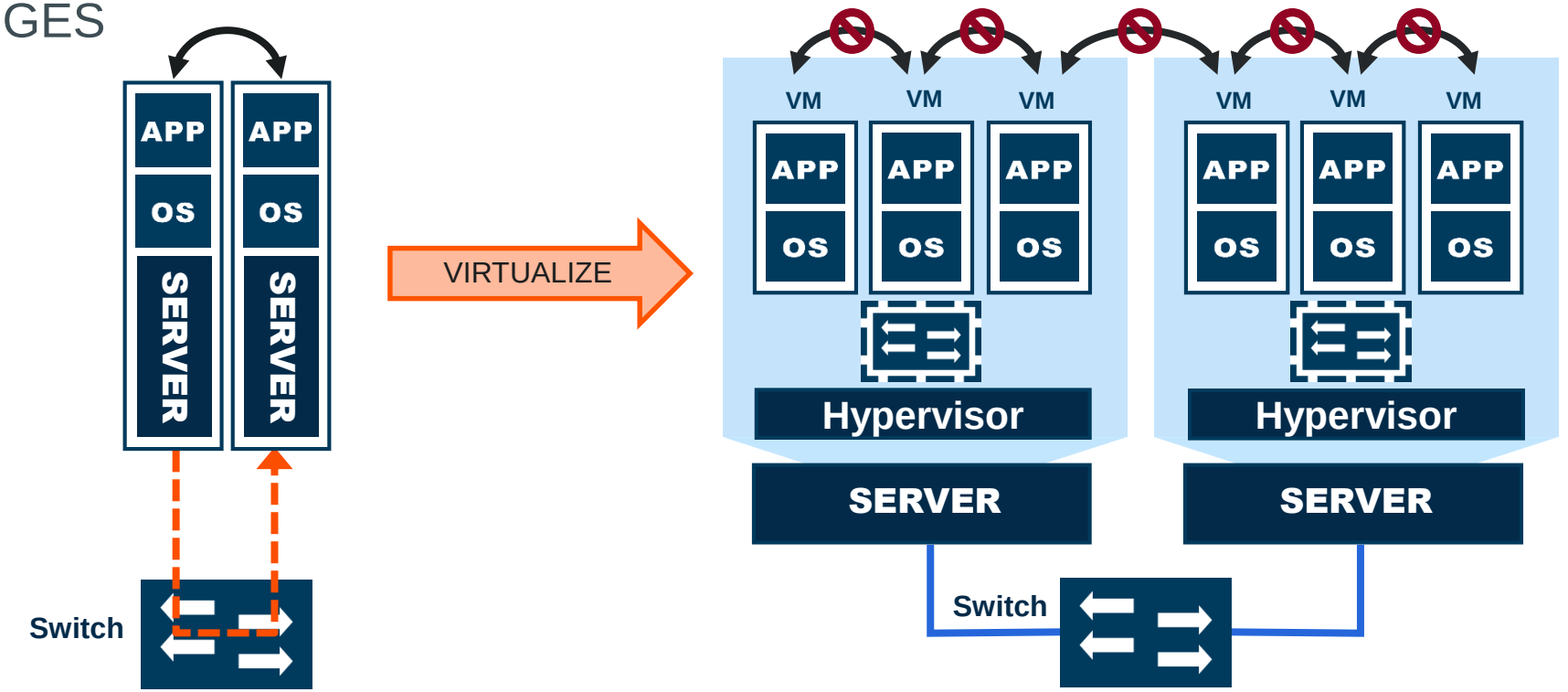

Gigamon®
Data-in-motion Visibility for AWS
See what matters.™
Regardless of where your data exists – private, public or hybrid cloud.
Free trial
Watch video

클라우드 시장 변화

단계	서버가상화	프라이빗 클라우드	퍼블릭 클라우드
			• Salesforce • Microsoft Office365 • AWS • Workday • VMWare vCloud • Microsoft Azure, etc.
선택 기술	• VMware ESX • KVM • Microsoft Hyper-V	• Server virtualization • Orchestration: OpenStack, VMware vRealize Automation • Network: Cisco ACI, VMware NSX • Containers: E.g. Docker	• SaaS: Software-as-a-Service *[E.g. SFDC, Workday, …]* • PaaS: Platform-as-a-Service *[E.g. Amazon Elastic Beanstalk]* • IaaS: Infrastructure-as-a-Service *[E.g. AWS, Microsoft Azure]*
잇점	• Break application silos • Increase asset utilization • Decrease cost	• Automate virtualization • Gain economies of scale across organization • Agility: on-demand services	• Agility • Pay-per-use • Minimize infrastructure investment

클라우드 환경하에서 도전과제

CHALLENGES



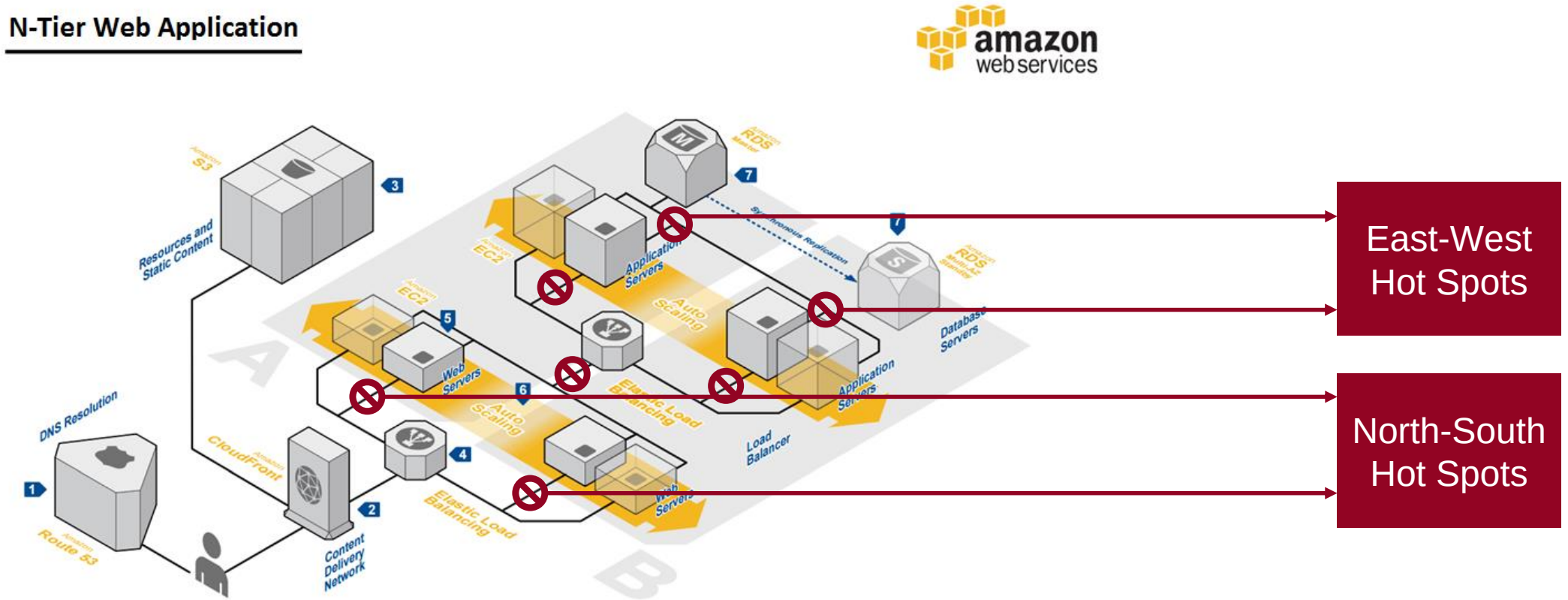
TRADITIONAL VISIBILITY

- **SPAN on Switch Ports**
- **Physical TAPs**

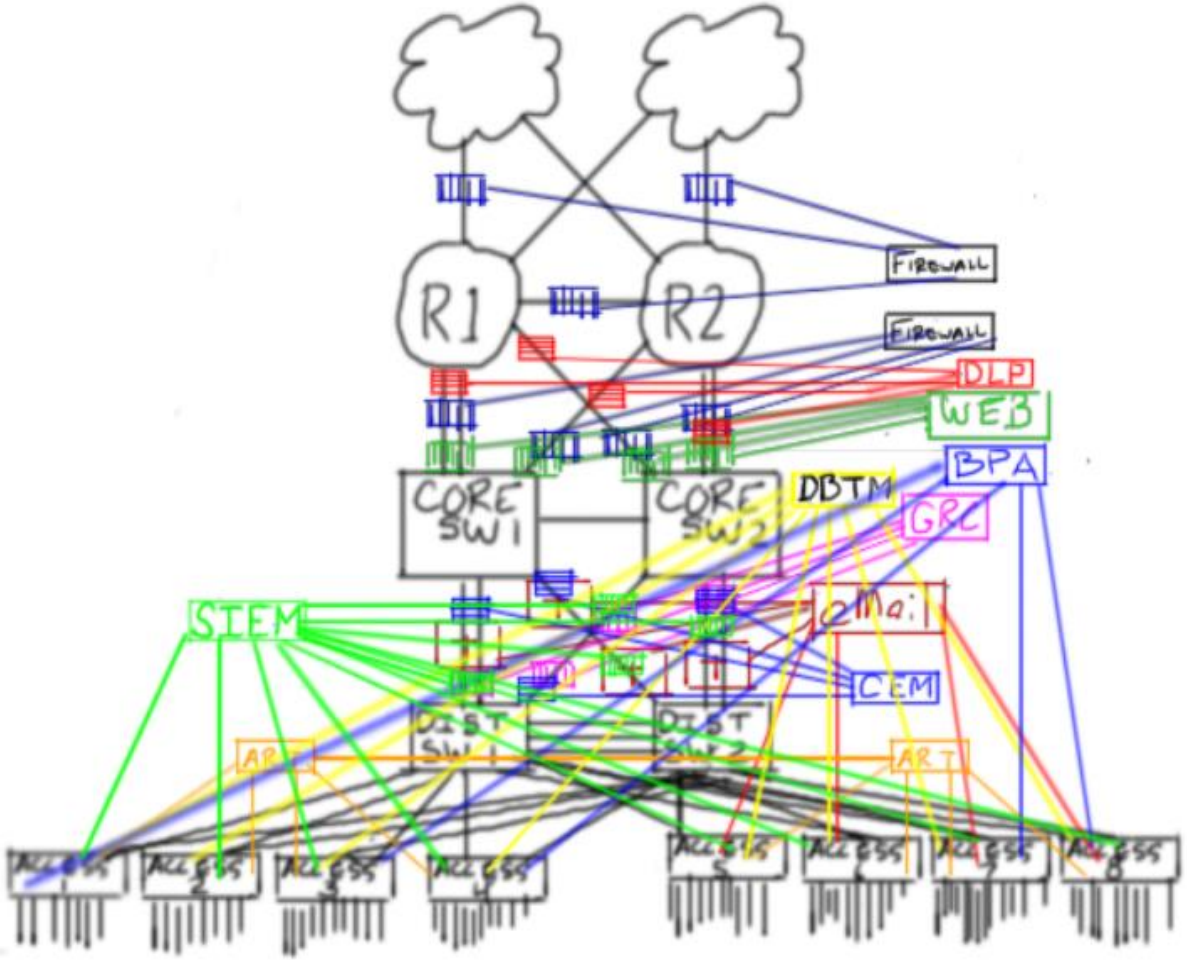
VIRTUAL VISIBILITY CHALLENGES

- **Blind spots for Inter-Host VM traffic**
- **Blind spots for Intra-Host VM traffic (blade center)**

클라우드 "핫스팟" – 웹 서비스 사례



클라우드 가시성을 위한 과제



- **Inability to access all traffic**
- **Discreet vendor monitoring agents per instance**
- **Impacts workload and VPC performance**
- **Increases complexity**
- **Static visibility with heavy disruption**

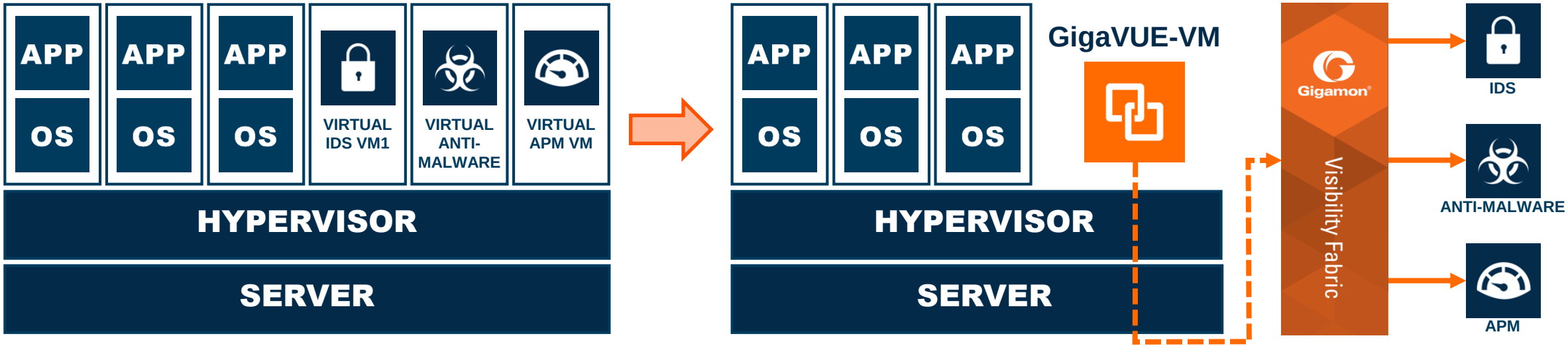
Elastic Load Balancing (ELB) Subnet Instances Tool Amazon Relational Database Service (RDS) Availability Zone (AZ)

교착상태 (Server, Network, Security Teams!)

클라우드 환경의 가시성

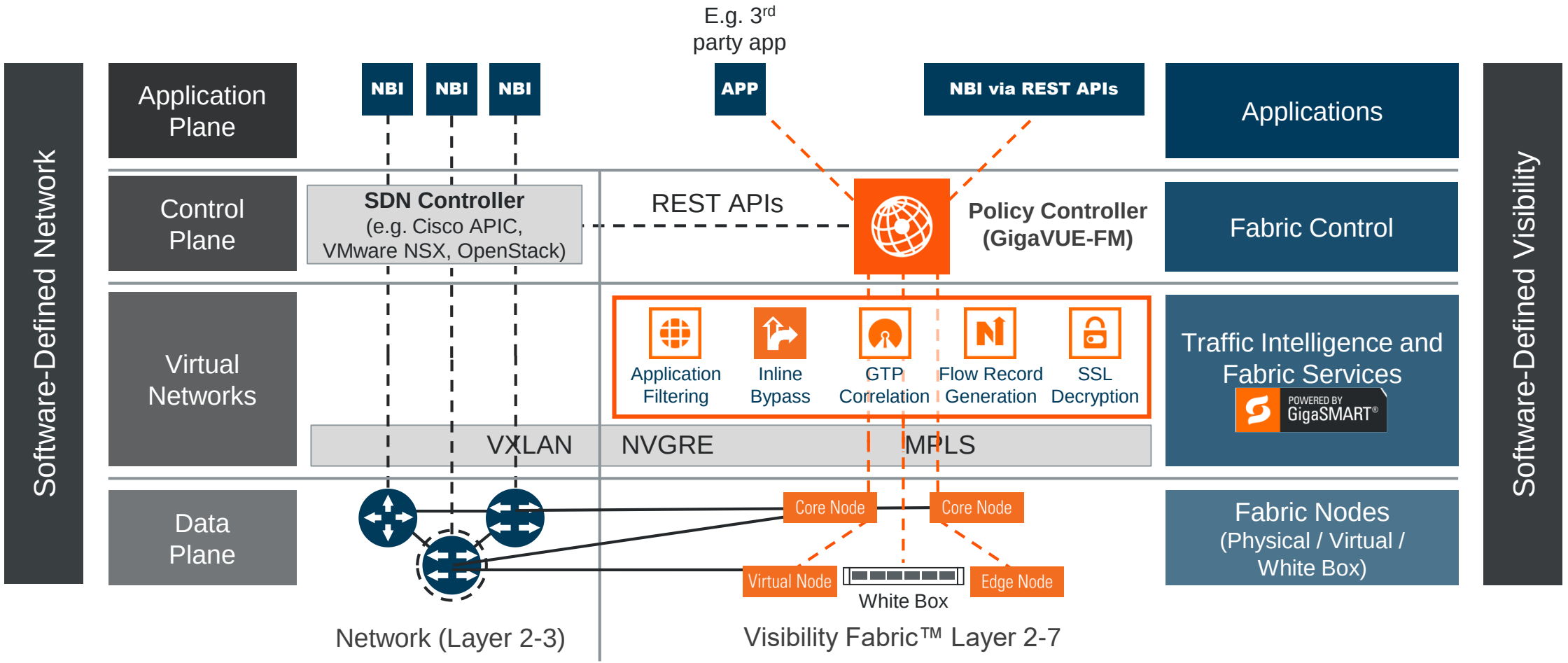
고객이 반드시 고려해야 하는 5가지 이유

1. 가상화 된 업무영역 내 보안요구 가속화.
2. 중요한 업무를 수행하는 VM 사용율의 증가.
3. 보안 및 어플리케이션 성능모니터링 도구를 위한 VM간 트래픽의 가시성 확보 필요.
4. 새로운 툴의 보안성 제공을 위한 가상 인스턴스의 생성이 시스템 업무 성능에 영향을 미침.
5. 가상 머신으로 전환 후 자동적인 가시성 확보 필요.



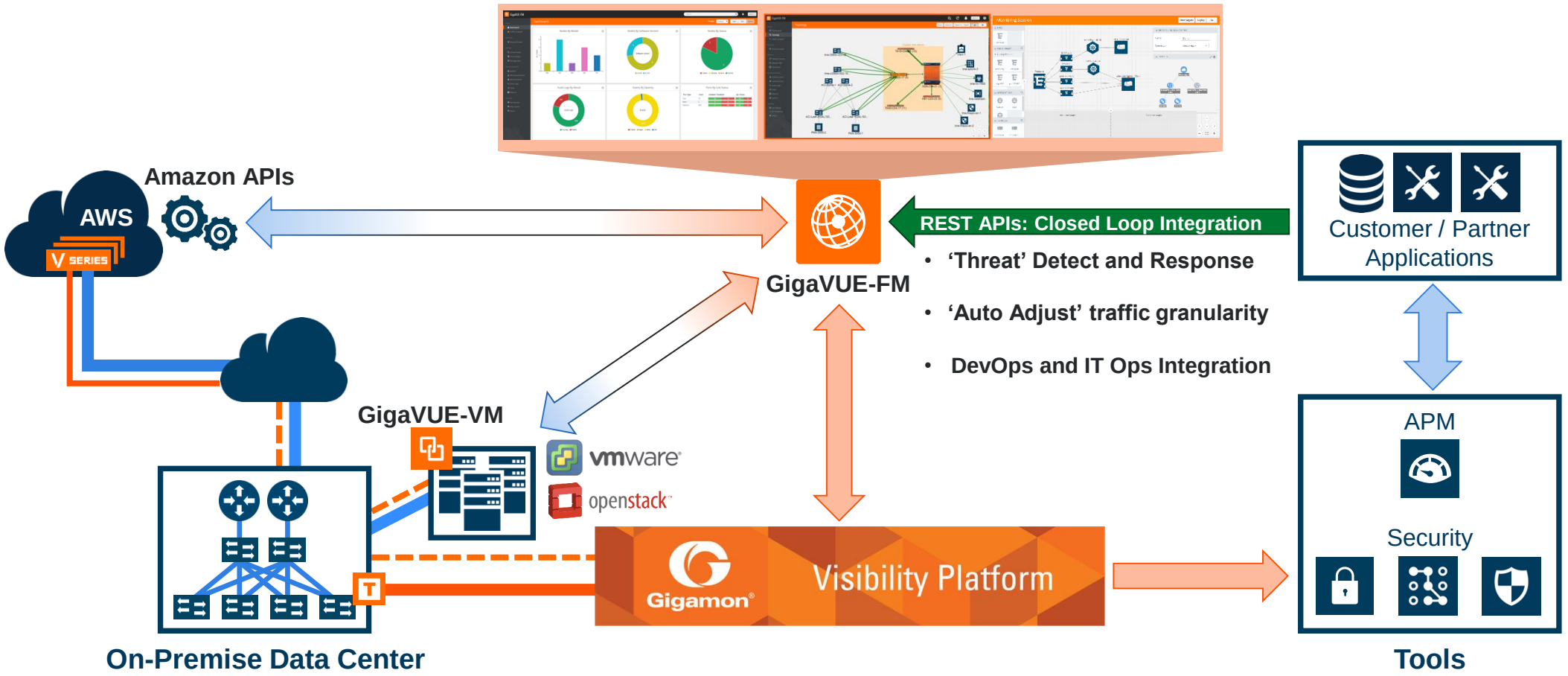
소프트웨어 정의 가시성(Software-Defined Visibility)

SDN 스택과의 상관성



Visibility Platform Orchestration

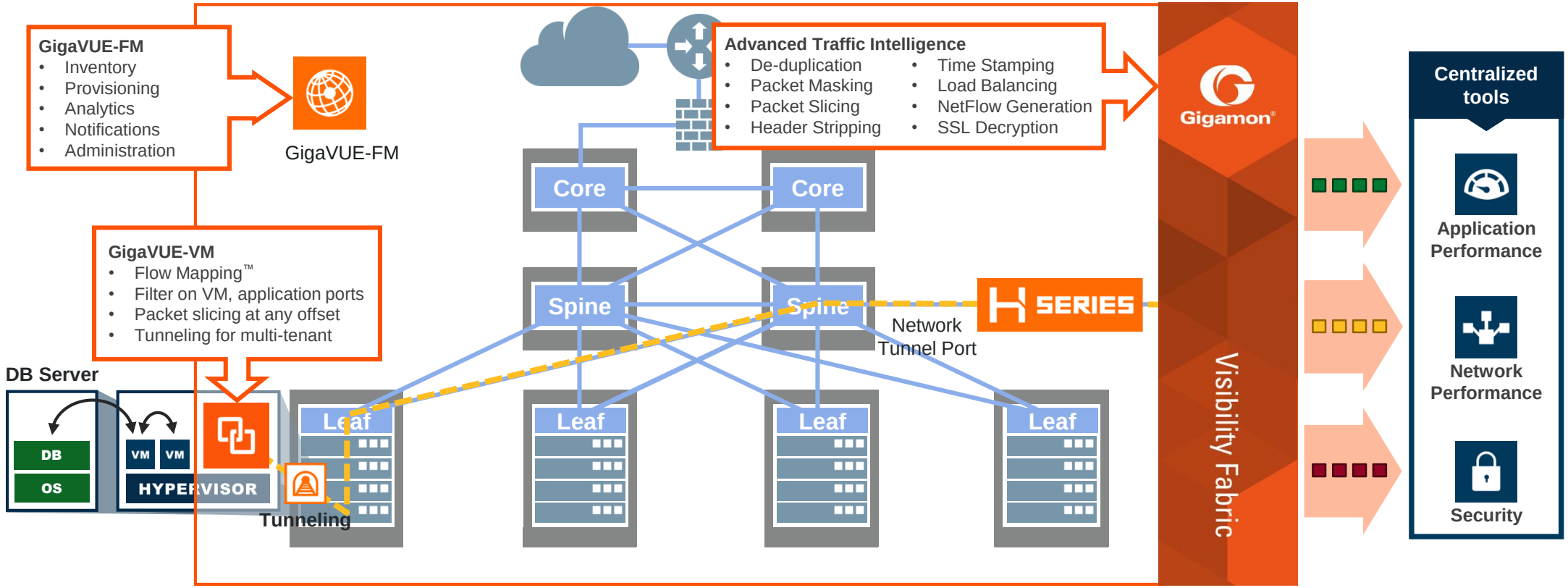
PUBLIC, PRIVATE AND HYBRID CLOUD VISIBILITY ORCHESTRATION



클라우드 가시성 확보 구성안

클라우드 내 트래픽 가시성 확보 가능

- 가상화 TAP(Virtual Tap)용 GigaVUE-VM을 통하여 호스트 어플리케이션간의 트래픽 분석
- 가상화 트래픽을 Flow Mapping 방식으로 분류 및 터널링을 통해 분석 장비로 전달



GigaVUE-VM 지원 하이퍼바이저 종류

VMware ESXi

- Virtual Visibility for VMware vSphere (vDS, vSS, Nexus 1000v)
- Manage/monitor 1000-nodes, 10 vCenters
- Support for 5.0, 5.1. 6.0

VMware NSX

- Integration with NSX Manager for “Gigamon Visibility Service” Insertion
- Enable ‘Traffic Visibility Policies’ for application security groups
- Automatically select, filter and forward virtual traffic to the Security and Monitoring Tools

OpenStack/KVM

- Extend Virtual Visibility to tenant traffic in private and SP clouds
- Deploy ‘Traffic Visibility Policies’ for virtual workloads and virtual network functions (VNFs)
- Support for Icehouse and above releases

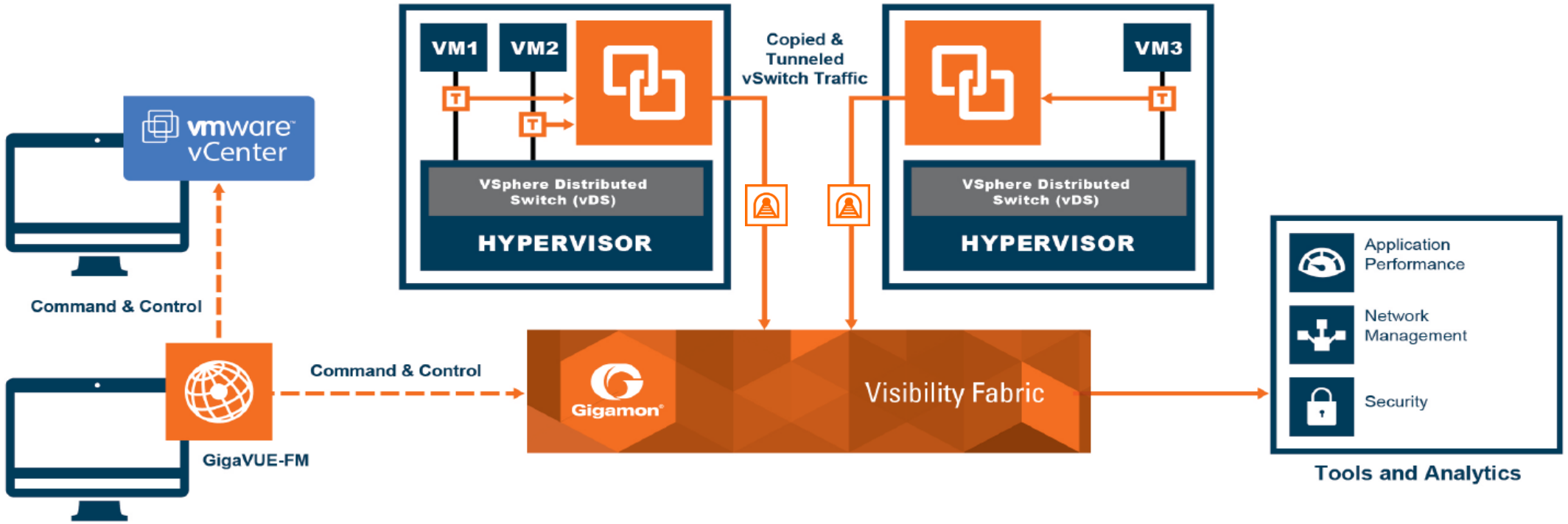
Management and Monitoring

- Centrally deployed and managed by GigaVUE-FM
- Workflows for creating virtual traffic policies
- Dashboards, Hot Spot Monitoring, Top/Bottom N Virtual Maps
- Historical trend analysis (up to a month), Reports

VMware vSphere 상의 GigaVUE-VM

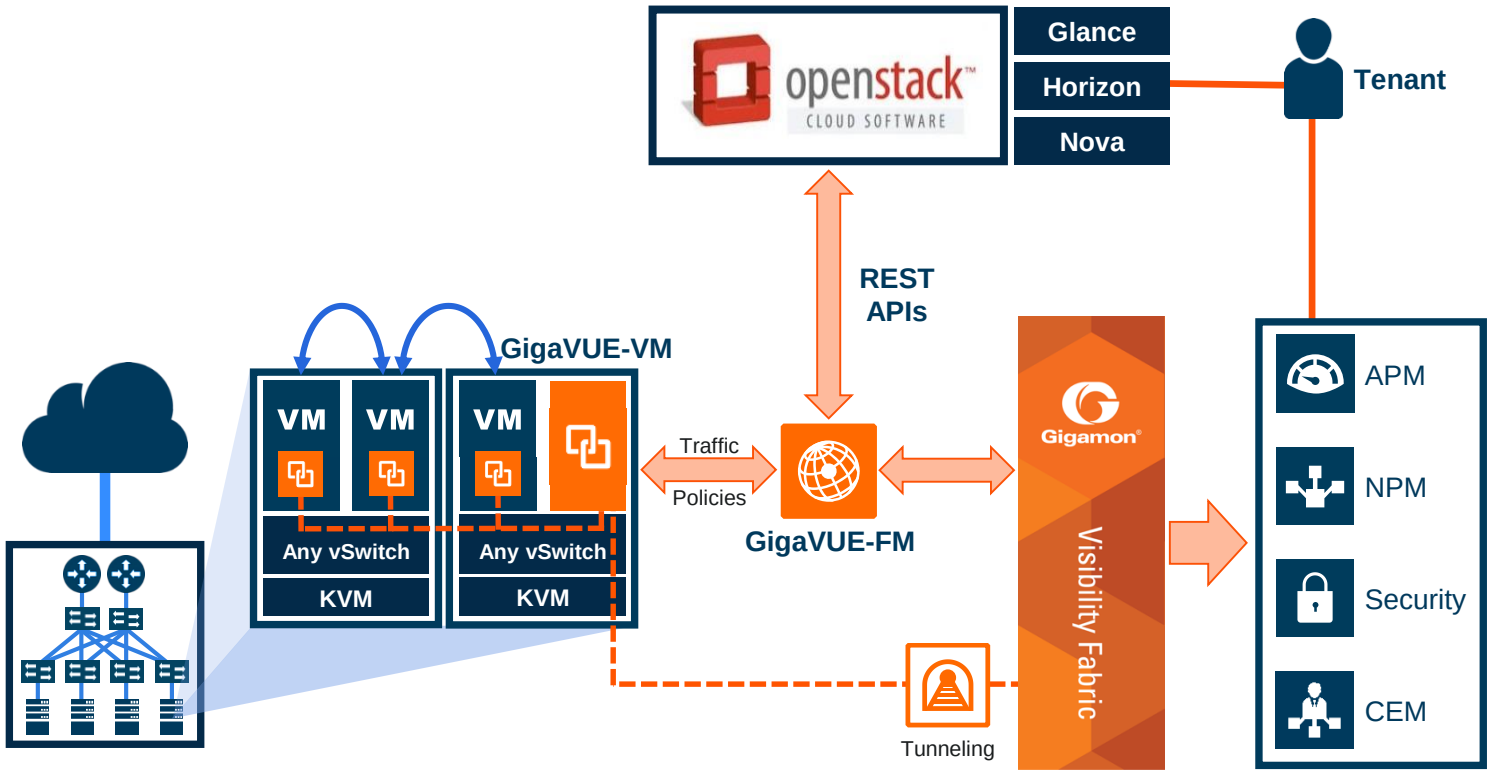
LIGHT FOOTPRINT VIRTUAL MACHINE, NOT KERNEL MODULE

Small Footprint: 1 vCPU, 2 GB RAM
Throughput (tested): 3 Gbps (mix packet sizes)



OpenStack 환경하에서 GigaVUE-VM

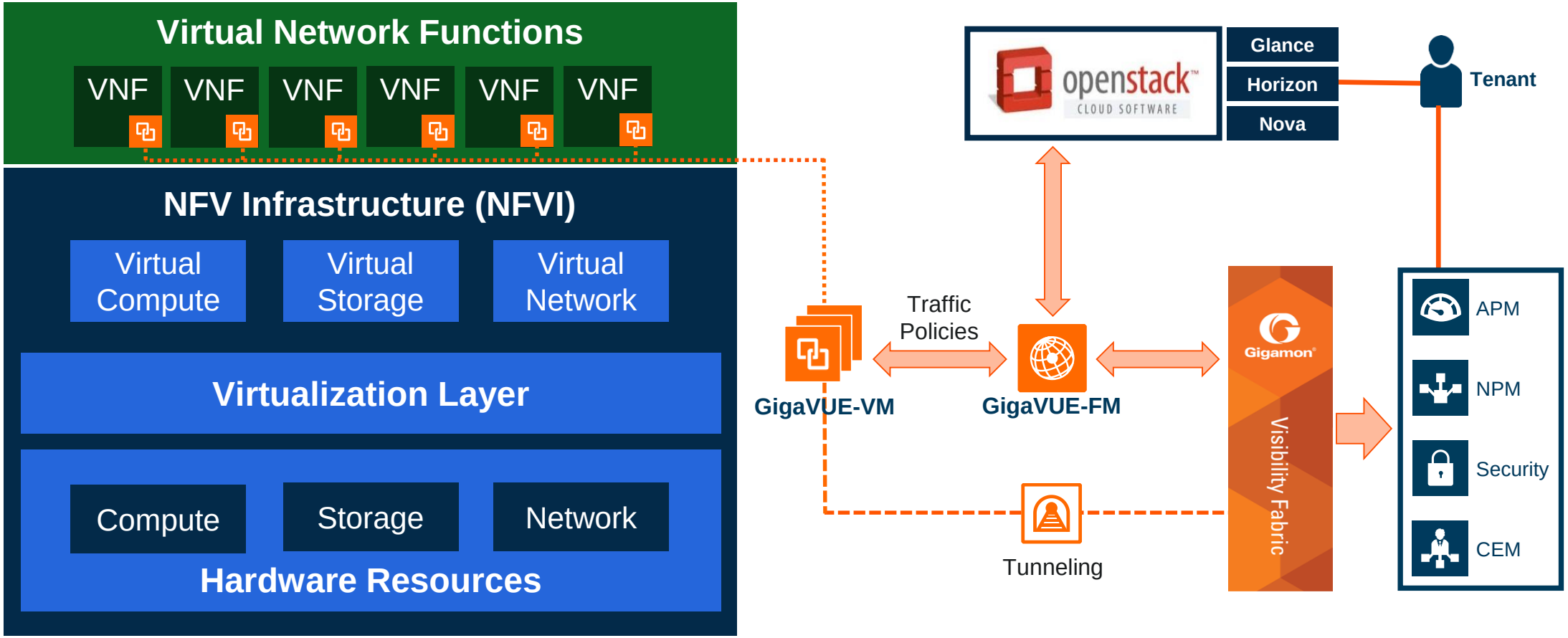
ALTERNATE APPROACH: MONITORING FROM WITHIN (MFW)



- Small footprint user-space application (G-vTAP) in the target VM
- Filters and delivers VM traffic to a Gigamon virtual appliance (GigaVUE-VM)
- GigaVUE-VM optimizes and delivers traffic to Visibility Fabric
- GigaVUE-FM for orchestration and management

서비스사업자 내 NFV 가시성 확보

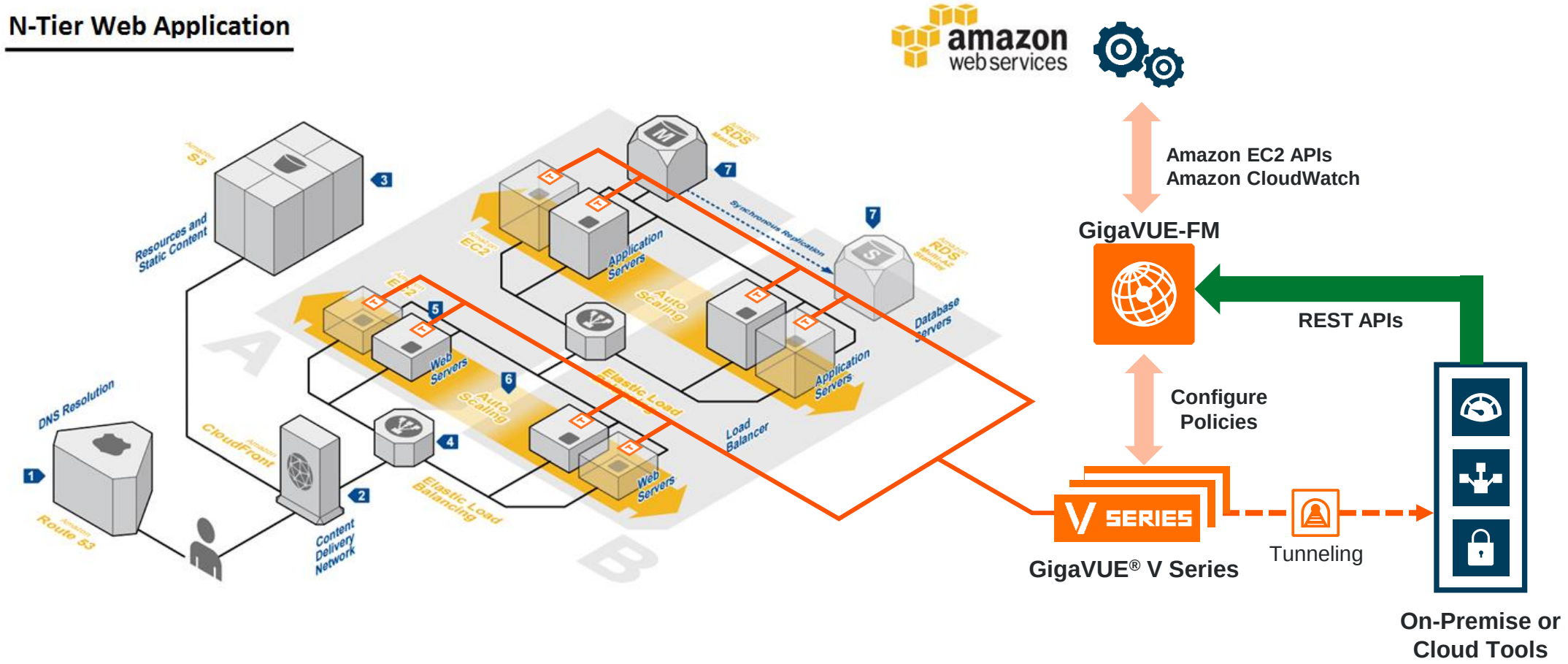
GIGAMON OPENSTACK SOLUTION MAINTAINS VISIBILITY DURING NFV TRANSITION



Reference: ETSI publication GS NFV 002: Network Functions Virtualization (NFV); Architectural Framework

아마존 상의 Gigamon Visibility Platform

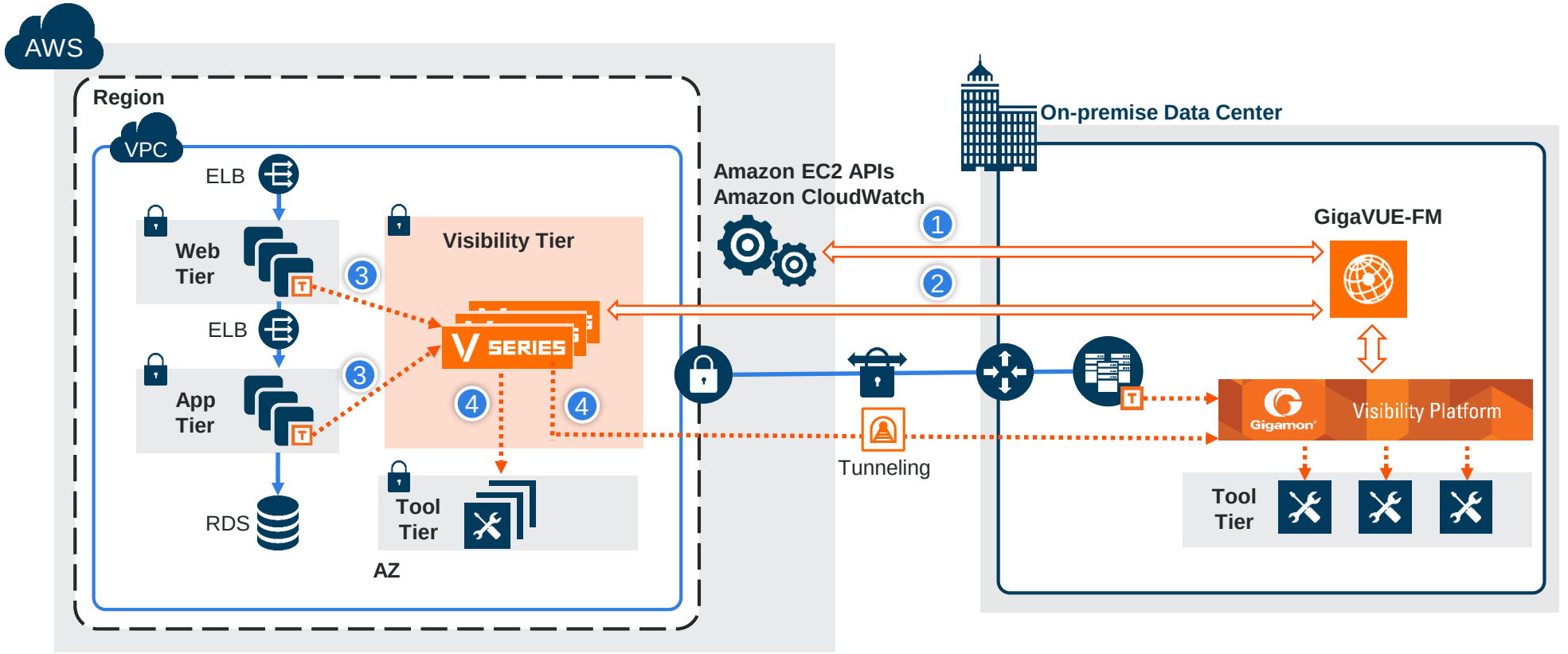
- Sample Web Application – AWS Reference Architecture



Reference Picture: AWS Best Practices

하이브리드 형태 (Hybrid Cloud Visibility)

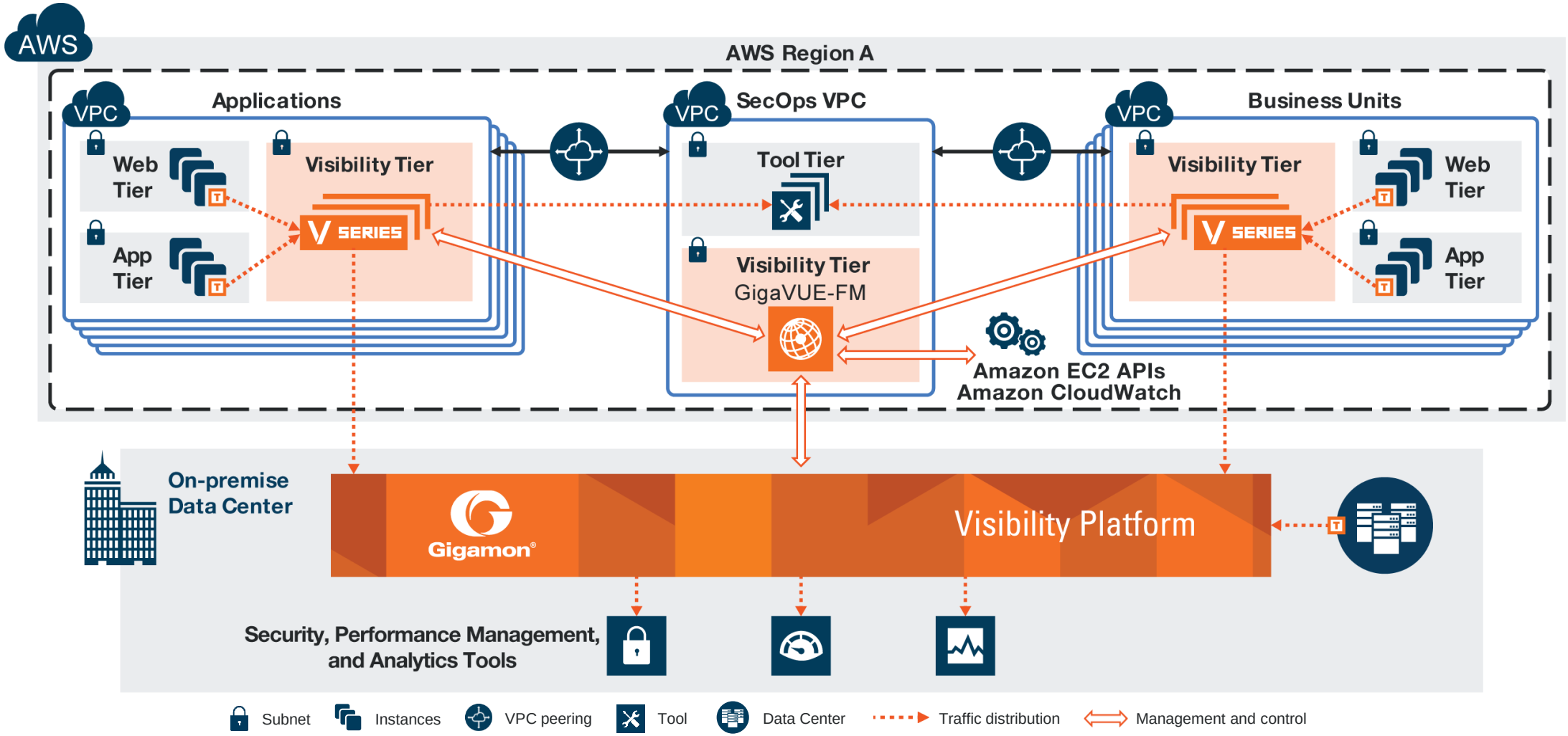
- Preserve Tool Investment



1. Integrate with Amazon APIs
2. Deploy Visibility Tier
3. Copy EC2 instance traffic
4. Aggregate and distribute customized traffic to tools

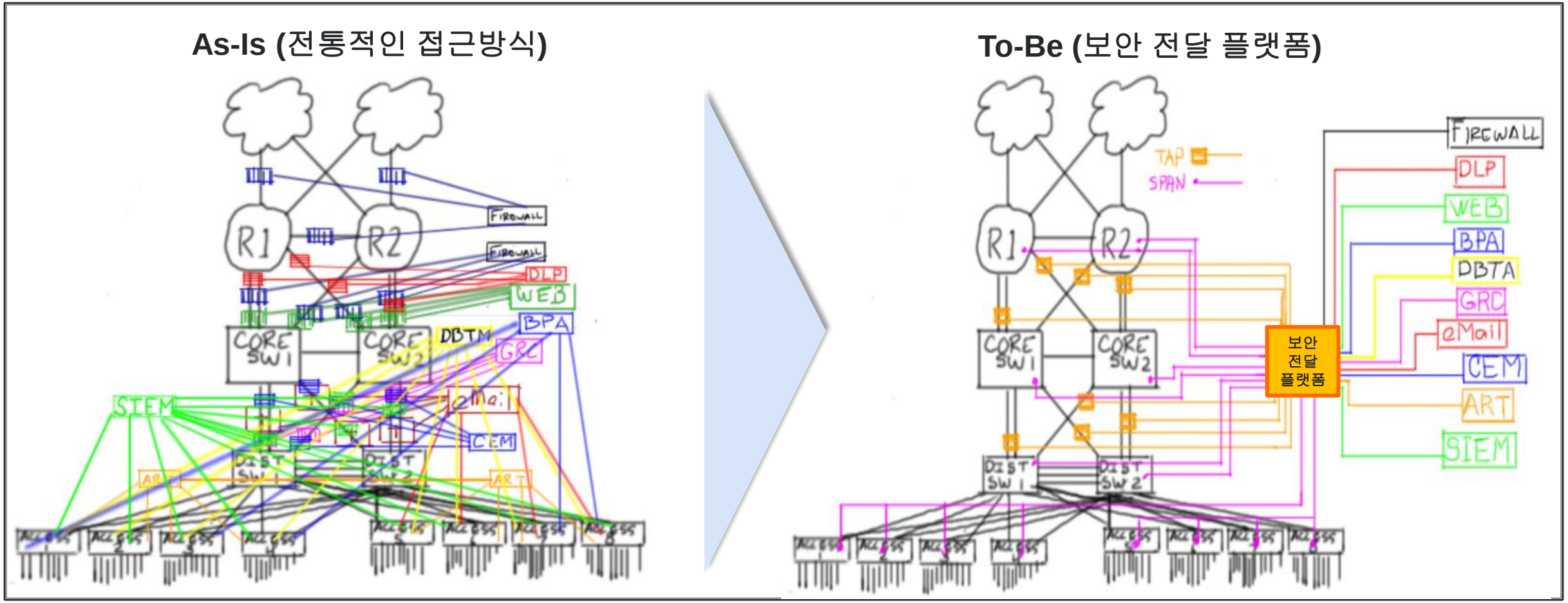
Elastic Load Balancing (ELB) · Subnet · Instances · Tool · Amazon Relational Database Service (RDS) · Availability Zone (AZ) · VPN Gateway · VPN Connection · Router · Data Center

멀티 VPC 형태(Multi-VPC Visibility)



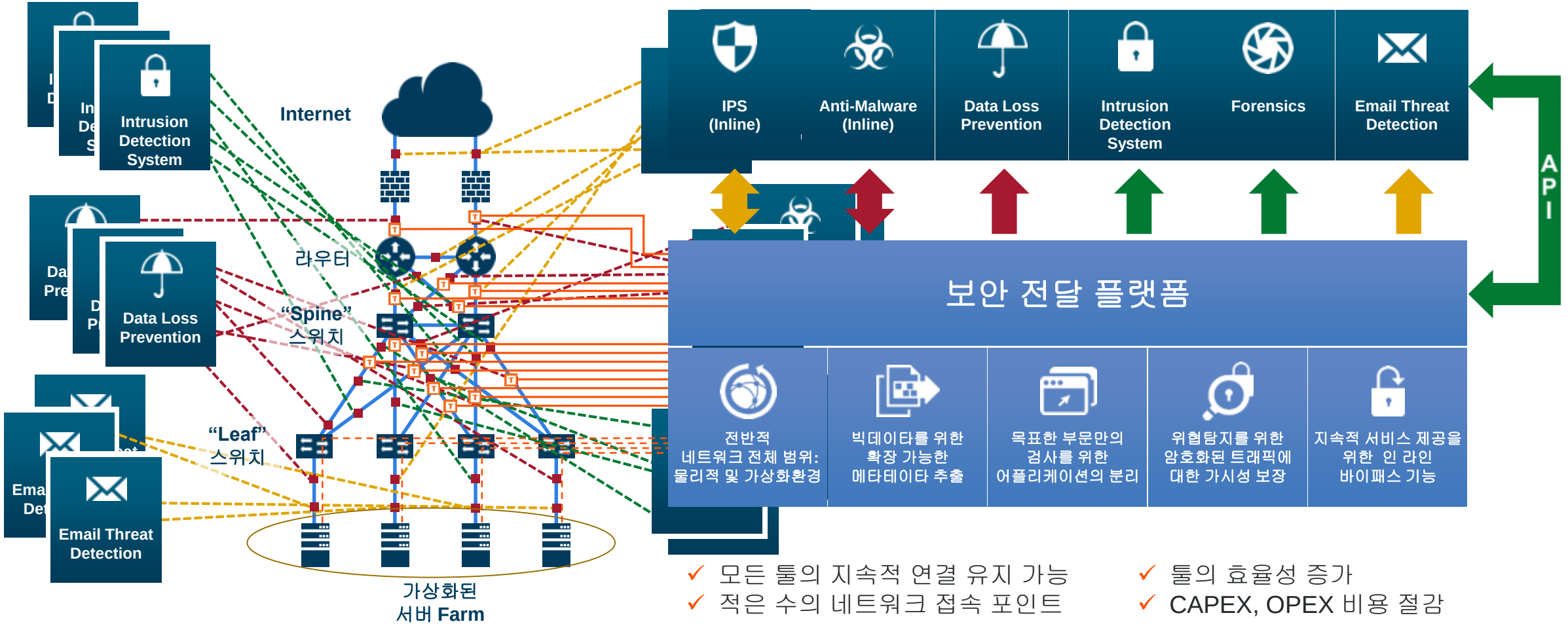
보안전달 플랫폼

단순화, 통합구성 및 관리 및 운영 효율, TCO 절감의 극대화



보안 전달 플랫폼: “See Everything”

효과적인 보안 구축을 위한 솔루션 블록화(BUILDING BLOCK)



- ✓ 모든 툴의 지속적 연결 유지 가능
- ✓ 적은 수의 네트워크 접속 포인트
- ✓ 툴의 효율성 증가
- ✓ CAPEX, OPEX 비용 절감

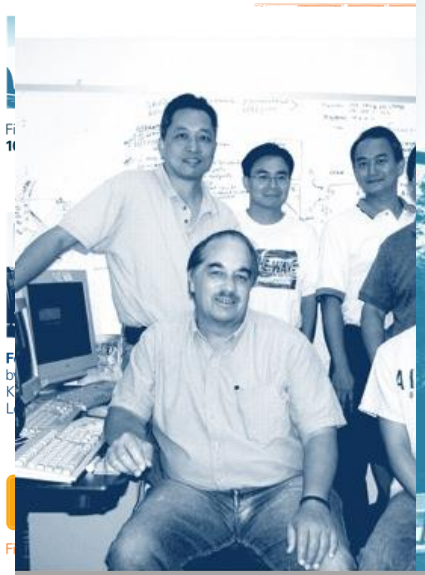
GIGABIT MONITORING

1Gigabit X 10 = 10Gigabit X 10 = 100Gigabit X 10 = 1 Terabit X 1000 = 1 Peta

기가몬 (Gigamon)

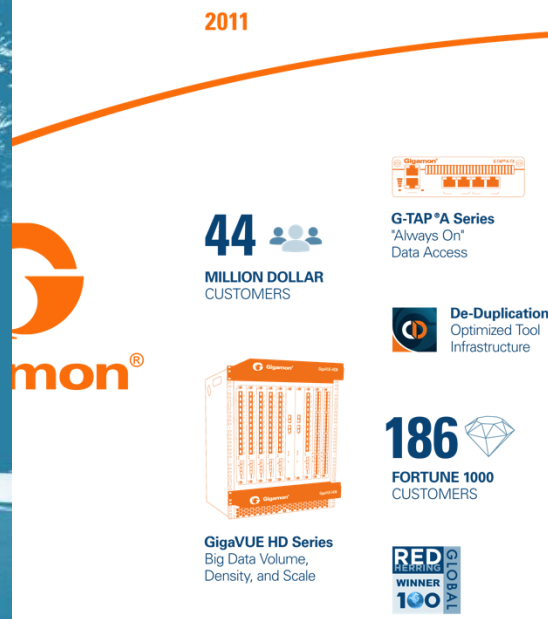
- 설립연도 : 2004년 (Pioneered Market)
- 기업공개 : 2013년 6월 (NYSE, GIMO)
- 본사위치 : 미국, 캘리포니아 Santa Clara

- 주요사업 : 보안 및 관리툴을 위한 가시성 시장의 1위 벤더 (약40%)*
- 사업분석 : 모바일(Mobile), 데이타센타 (Datacenter), 클라우드 (Cloud)
- 보유기술 : 35 개 핵심 특허권, 27개 특허권 출원 중**



2004년 창립기념 촬영사진

2015년 캘리포니아 본사 전경



2004 2005

*Gartner, **Customer and patent numbers FY16.

주요 국내외 고객 사

엔터프라이즈

TECHNOLOGY

monster, LINE, ebay, EMC², intel, REUTERS, Disney Online, LinkedIn, Apache, salesforce.com, Tech Data, Expedia.com

INDUSTRIAL

3M, MARATHON, NEC, BAKER HUGHES, Constellation Energy, SAMSUNG, Chevron, BNSF RAILWAY, aeso, LOCKHEED MARTIN, Genentech, HONDA, Schering-Plough

RETAIL

Sara Lee, ConAgra Foods, WAL★MART, LOTTE, SK broadband, BEST BUY, JCPenney, COSTCO WHOLESALE, General Mills

FINANCE

MasterCard, NYSE, DISCOVER FINANCIAL SERVICES, BARCLAYS, Mellon, NASDAQ, Fidelity, Bank of America, Standard Chartered SC제일은행, Deutsche Bank, Merrill Lynch, TD AMERITRADE, NYMEX, RBC Royal Bank, Capital One, STATE STREET

HEALTHCARE & INSURANCE

CardinalHealth, LEHIGH VALLEY HOSPITAL AND HEALTH NETWORK, CEDARS-SINAI, STANFORD HOSPITAL & CLINICS, National Institutes of Health, BJC HealthCare, APL, Medtronic

GOVERNMENT

SAIC, DARPA, SUPREME COURT OF THE UNITED STATES, NASA, New York City Transit, VITA, U.S. DEPARTMENT OF TREASURY

2300+ 글로벌 고객

Fortune-100 내 81+ 고객

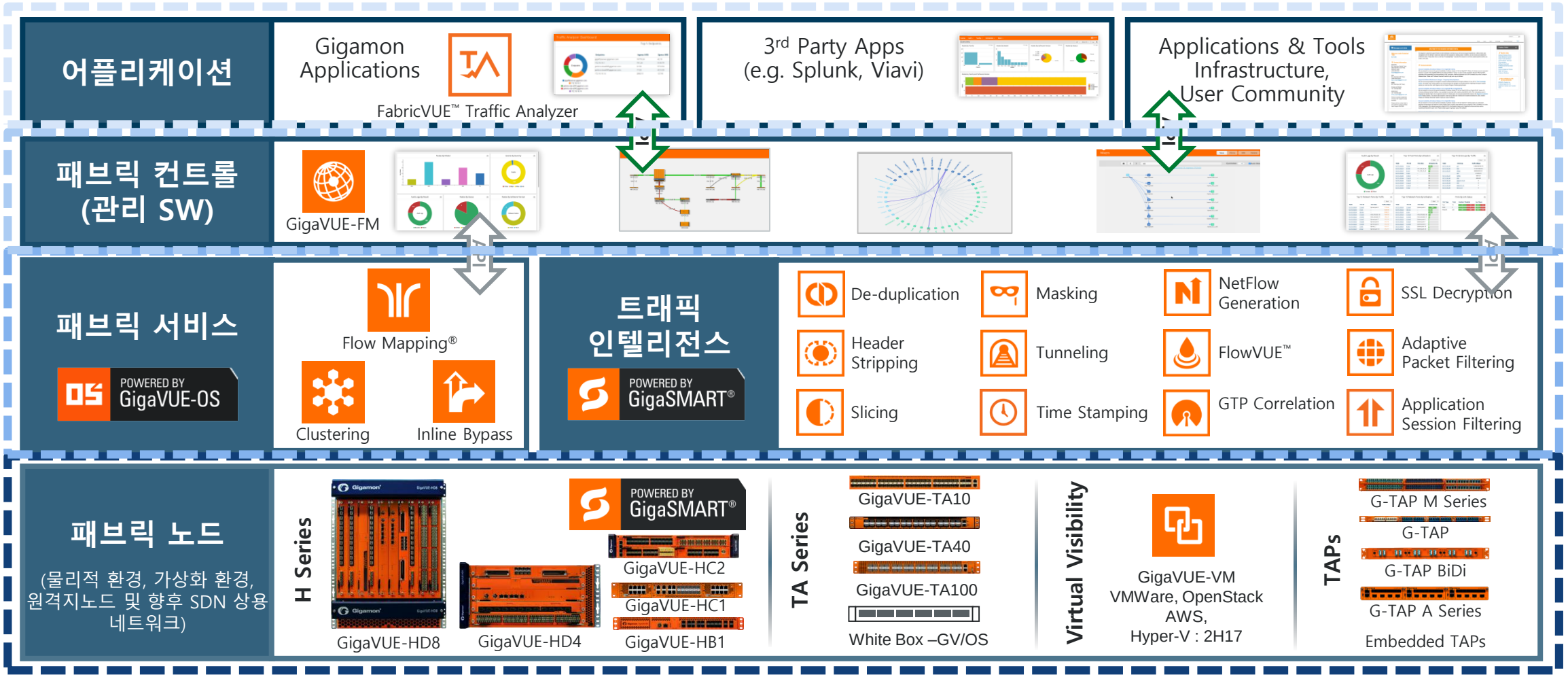
서비스 사업자

verizon, at&t, Sprint Together with NEXTEL, U.S. Cellular, comcast, NTT Communications, vodacom, vodafone, BT, TIME WARNER CABLE THE POWER OF YOU™, Telstra, Level (3) COMMUNICATIONS, Designing The Future KDDI, BCE, COX COMMUNICATIONS, kt

글로벌 TOP 100 SP 내 50+ 사업자

주요 에코 파트너사

보안전달 플랫폼 통합 포트폴리오



보안전달 플랫폼 주요 장비 사양

Visibility Nodes	장비 모델명	장비 외관	Visibility Throughput	Port Density
H Series	GigaVUE-HD8		2.4 Tbps	100G : 48 ports 40G : 64 ports 10G : 256 ports 1G : 352 ports
	GigaVUE-HD4		1.28 Tbps	100G : 24 ports 40G : 32 ports 10G : 128 ports 1G : 176 ports
	GigaVUE-HC2		960 Gbps	100 : 8 ports 40G : 24 ports 1G/10G : 96 ports
	GigaVUE-HC1		284 Gbps	1G/10G : 12 ports 1G : 4 ports
	GigaVUE-HB1		56 Gbps	1G/10G : 4 ports 1G : 16 ports
Cloud	Public – AWS Private – VMWare, Openstack	GigaVUE-FM, GigaVUE-VM 외		

Thank You!

- **Contact Points**

-영업담당 : 노병완 전무 (010-7393-4196, brian.rho@gigamon.com)
김한기 이사 (010-4753-5448, hanki.kim@gigamon.com)
-기술담당 : 권혁인 이사 (010-3018-9461, hyukin.kwon@gigamon.com)
이민형 부장 (010-9636-8176, minhyung.lee@gigamon.com)

- **URL for downloading for e-Book (https://www.gigamon.com/resources/book/security-delivery-platforms-dummies-3197)**

Source: http://www.scality.com/blog/100-exabytes-makes-big-data-look-tiny/

Market Validation

THIRD-PARTY PERSPECTIVES

Gartner

"Gigamon is the market share leader…delivering Layer 2 through Layer 7 visibility, filtering and correlation via its GigaSMART platform."

- Market Guide for Network Packet Brokers, January 2016

"The Gigamon Visibility Platform enables our customers to accelerate …migration of their existing applications and workloads, while gaining greater visibility into network traffic for richer content inspection and protection of their mission-critical workloads and data."

- Tim Jefferson, Global Ecosystem Leader-Security, Amazon Web Services, Inc., November 2016

amazon web services

ESG

"A Security Delivery Platform helps eliminate many of the security architectural deficiencies that have led to so many high-profile breaches."

- Jon Oltsik, Senior Principal Analyst, ESG, July 2015