Gigamon®

See More. Secure More.

Pervasive 가시성 확보를 위한 보안 전달 플랫폼 구축

인성디지탈
신동엽 (dyshin@isd.co.kr)

보는 수준이 다르니

네트워크 구석구석 들여다볼 수 있는 '가시성 솔루션' 시장 개척

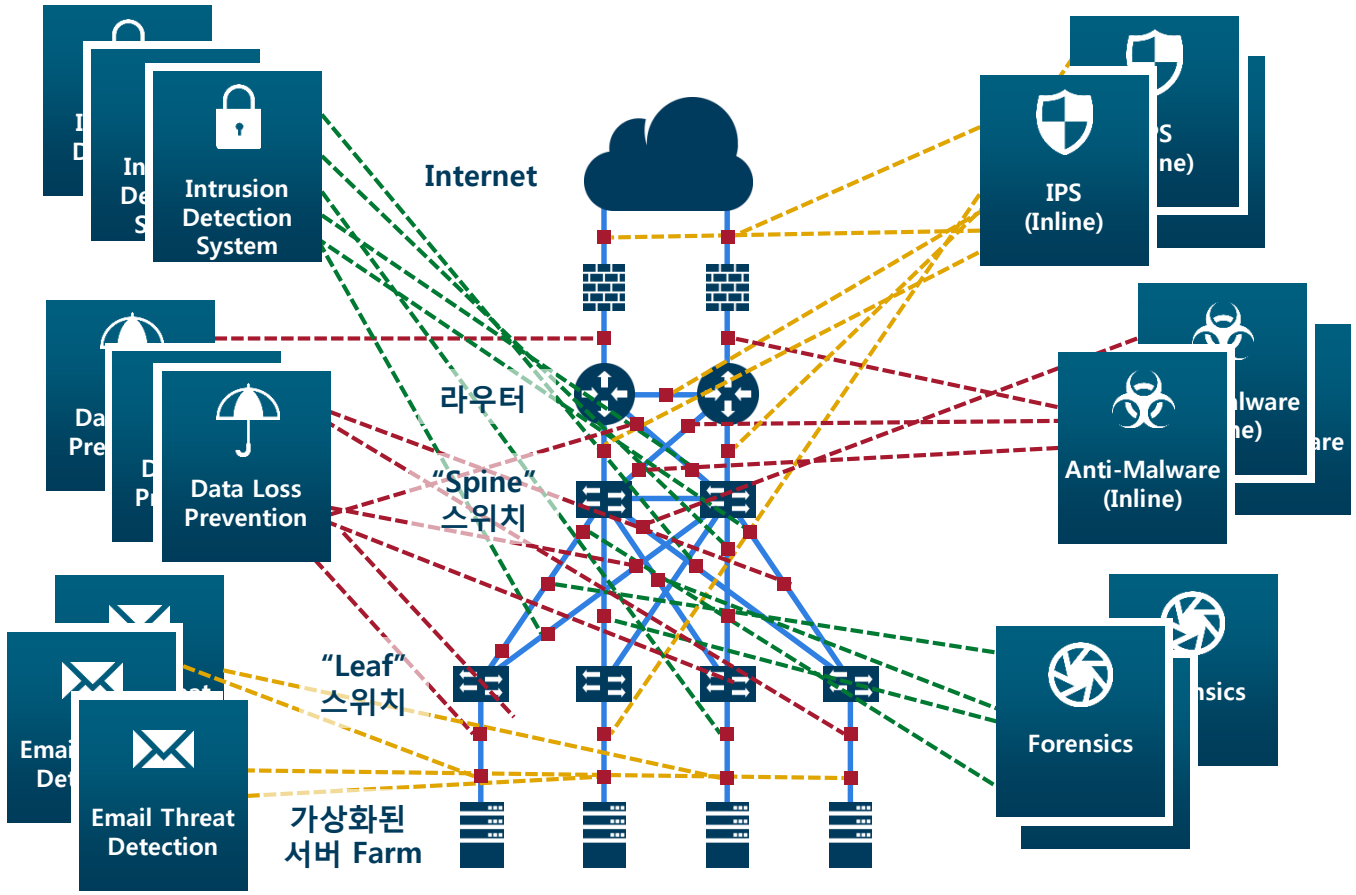
보안 수준이 다르다

누가 들어왔는지 뭘 했는지 바로 파악…해커들에겐 '공포의 대상'

1.
보안 솔루션 투자 효과, 가시성 플랫폼이 높인다

현재, 보안 장비에 트래픽는 어떻게? (제한적 가시성)

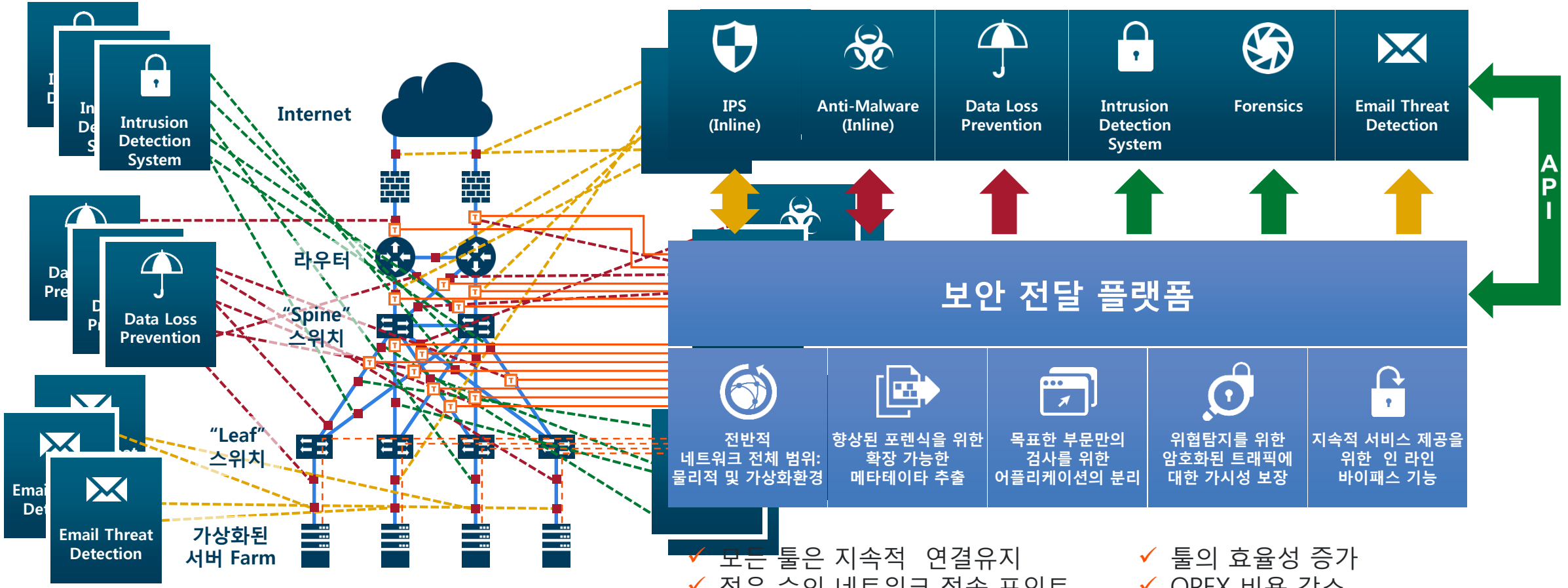
모니터링 인프라의 복잡성 : 너무 많은 모니터링 패스와 방어 포인트



복잡성	네트워크가 확장되면서 모니터링 솔루션 구성이 점차 복잡
개별관리	네트워크 모니터링 및 분석 솔루션들이 팀 단위/부서 단위로 구축되고 개별로 관리되어 중복투자 발생
사각지대	Span 또는 Mirror 포트 구성 제약으로 인해 네트워크 전 구간의 모니터링 불가, 사각지대 발생
운용의 비효율성	모니터링 솔루션의 중복 투자로 CAPEX/OPEX 증가로 인한 비용증가

향후, 보안 전달 플랫폼: “See Everything”

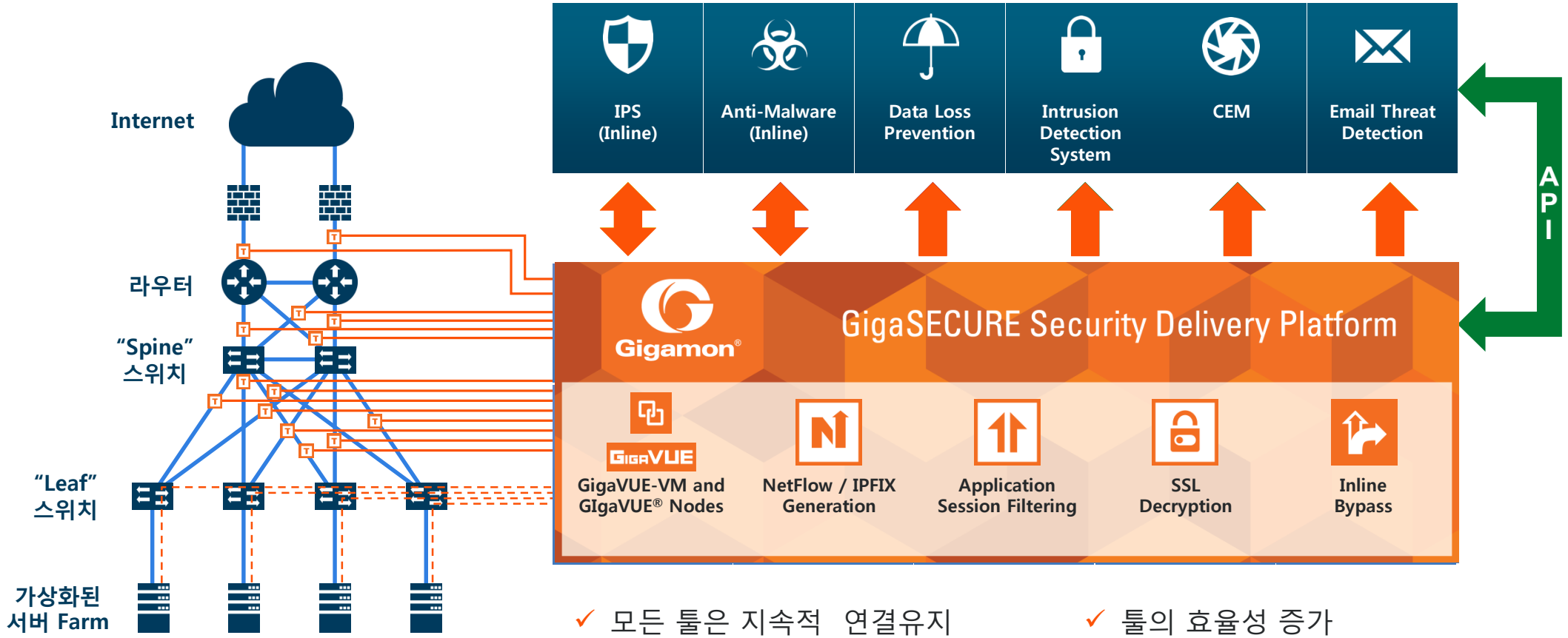
효과적인 보안을 위한 기본적인 빌딩 블록(BUILDING BLOCK)



- ✓ 모든 툴은 지속적 연결유지
- ✓ 적은 수의 네트워크 접속 포인트
- ✓ 툴의 효율성 증가
- ✓ OPEX 비용 감소

보안 전달 플랫폼: “See Everything”

산업계 최초의 보안 전달 플랫폼 (SECURITY DELIVERY PLATFORM)



- ✓ 모든 툴은 지속적 연결유지
- ✓ 적은 수의 네트워크 접속 포인트
- ✓ 툴의 효율성 증가
- ✓ OPEX 비용 감소

기가몬 주요 협력 파트너 사 (Ecosystem Partners)

We Fight Smart!

It's time to turn the tables on cybercrime.

Today, organizations around the world are fighting a growing enemy – and losing.

Cybercriminals have breached almost every major corporation and government department.

Despite our defenses, they are not just getting through, they are staying undetected for longer.

The reality is that none of us can be sure that our personal information is still private, or that our bank accounts are still safe.

No corporate leader can be sure that he or she will not be paraded in front of the media by the end of the day.

Even our energy and transport networks are under constant threat.

We are all in the crosshairs.

As leaders in business and government, it's time for us to fight smarter, and together.

And we can. New technology gives us the visibility to see what's really happening in our increasingly complex networks.

Working together, we can see threats earlier, isolate and eliminate them faster.

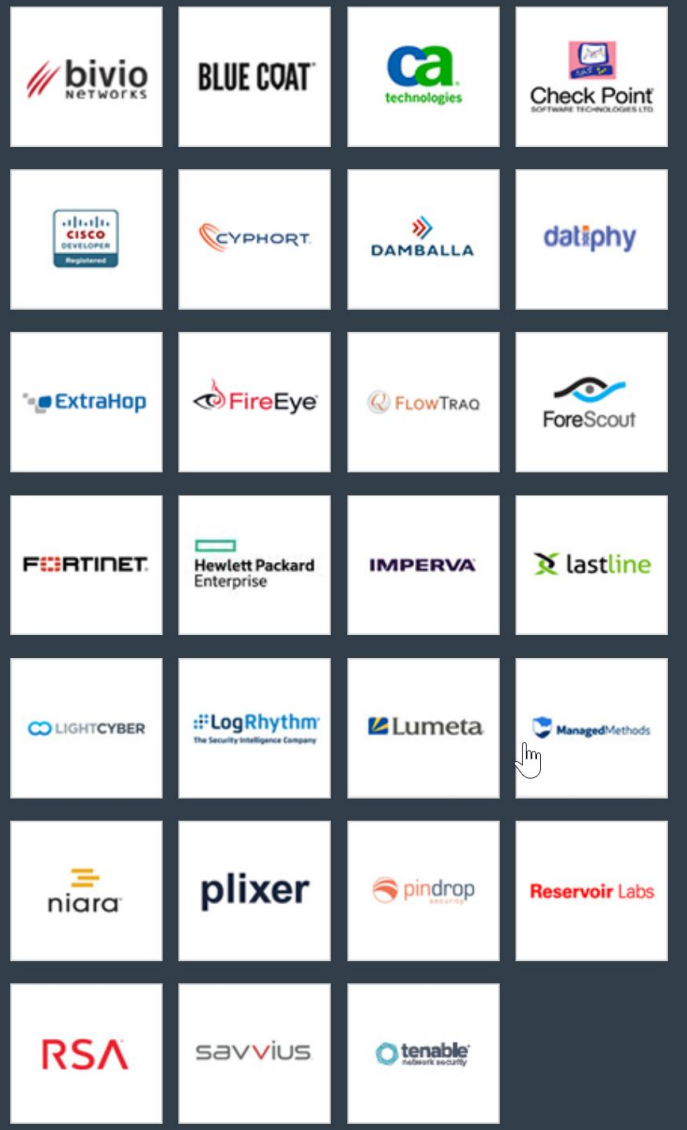
Last year we delivered the world's first Security Delivery Platform, an innovation that makes the world's most effective security tools even stronger.

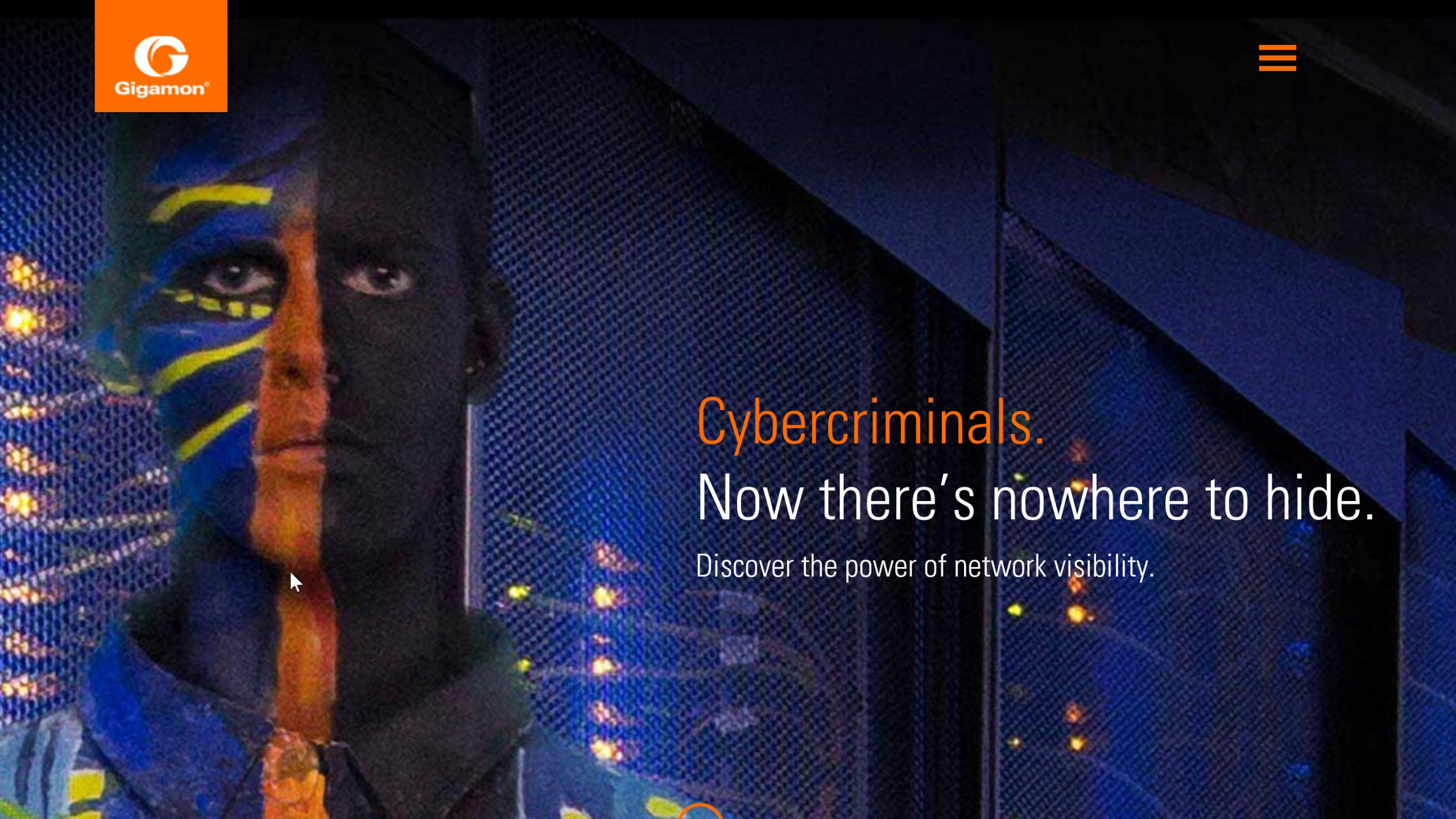
Today we stand united, ready to turn the tables on our attackers.

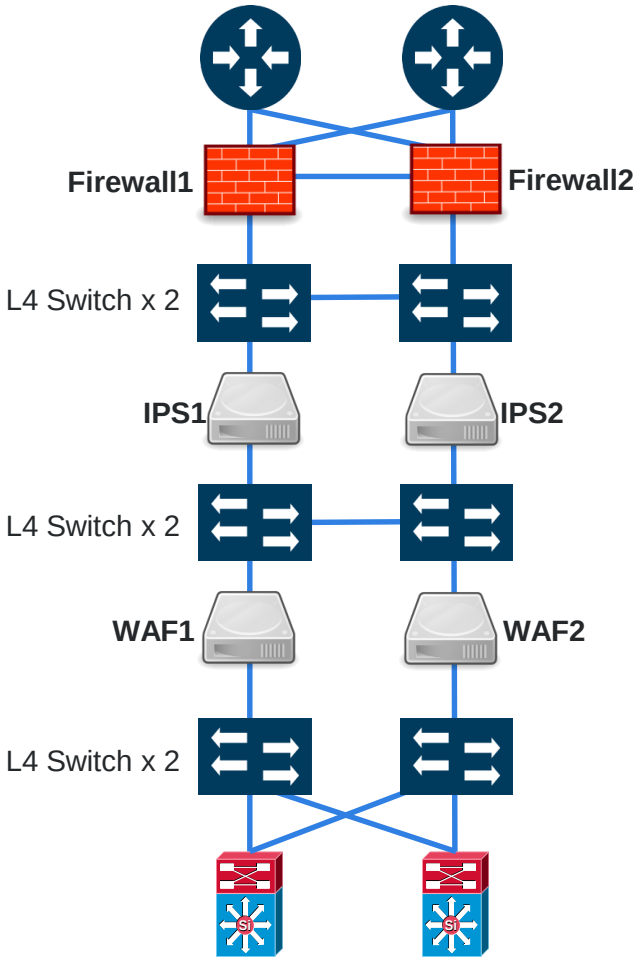
Join us, at #wefightsmart

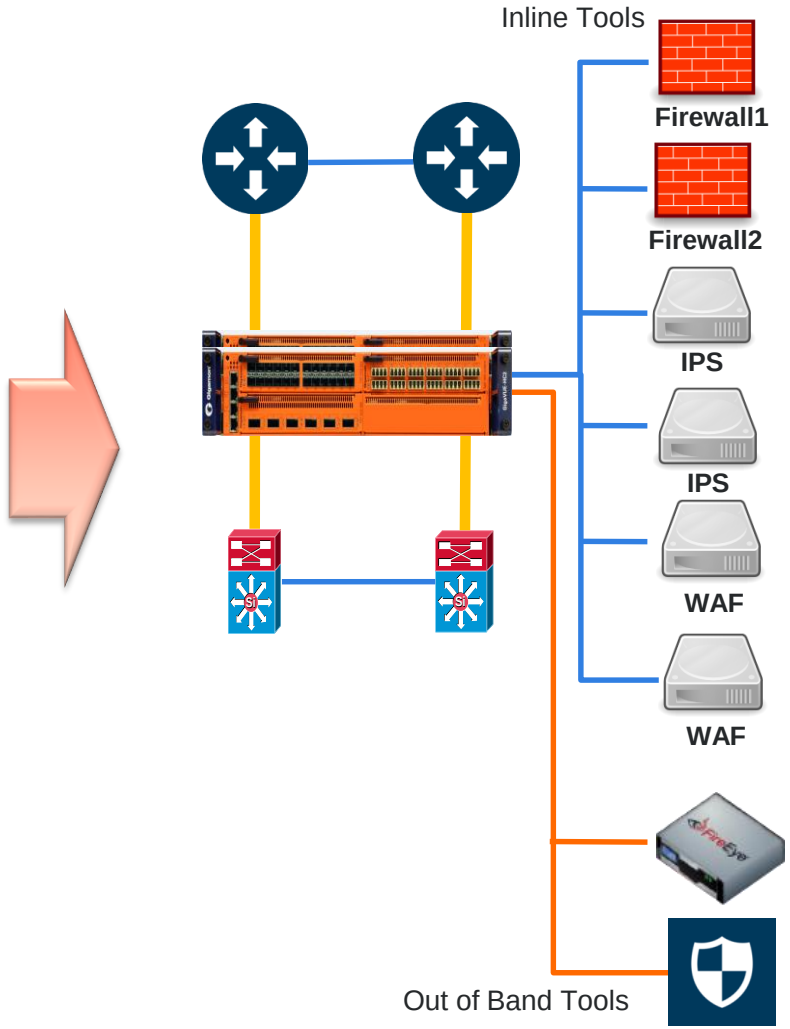
Paul Hooper

CEO, Gigamon



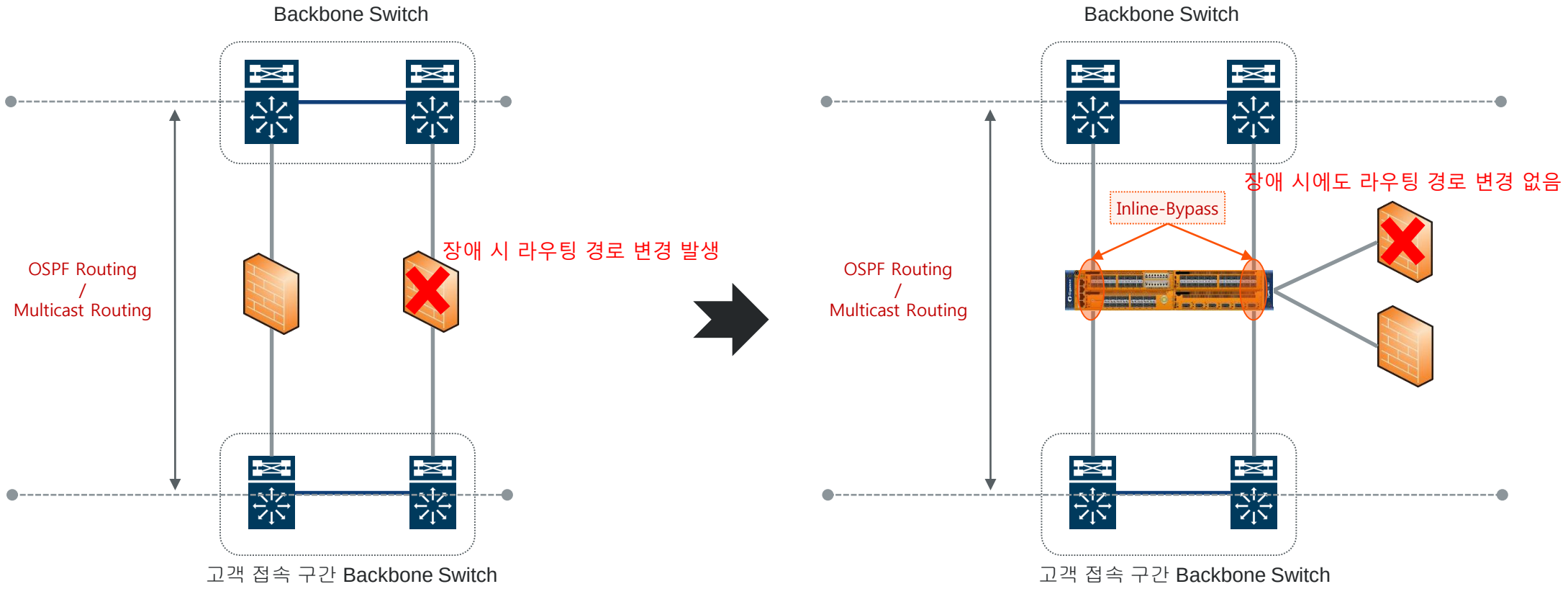

Gigamon
Cybercriminals.
Now there's nowhere to hide.
Discover the power of network visibility.





2.
네트워크와 보안을 분리하다.

Simple Network Secure Network



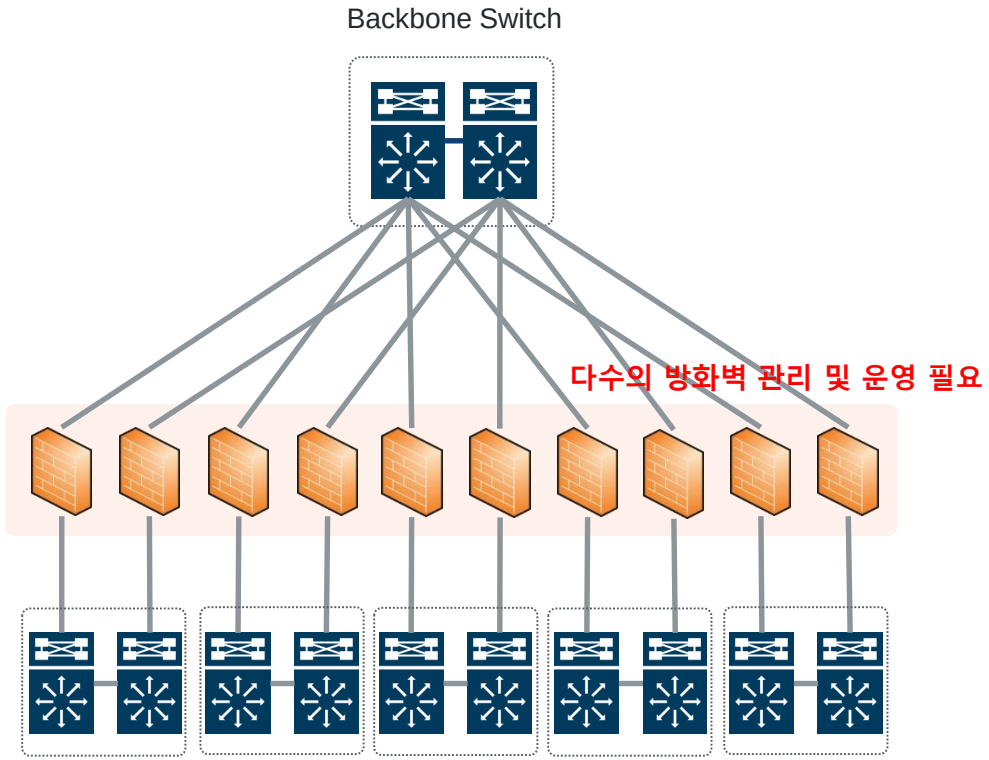
방화벽 장애 시 불필요한 라우팅 경로 변경 발생

- 방화벽 장애 발생 시 불필요한 라우팅 경로 변경에 따른 서비스 안정 저하
- 방화벽 홀딩 발생 시 트래픽 처리 불가에 따른 트래픽 손실 발생

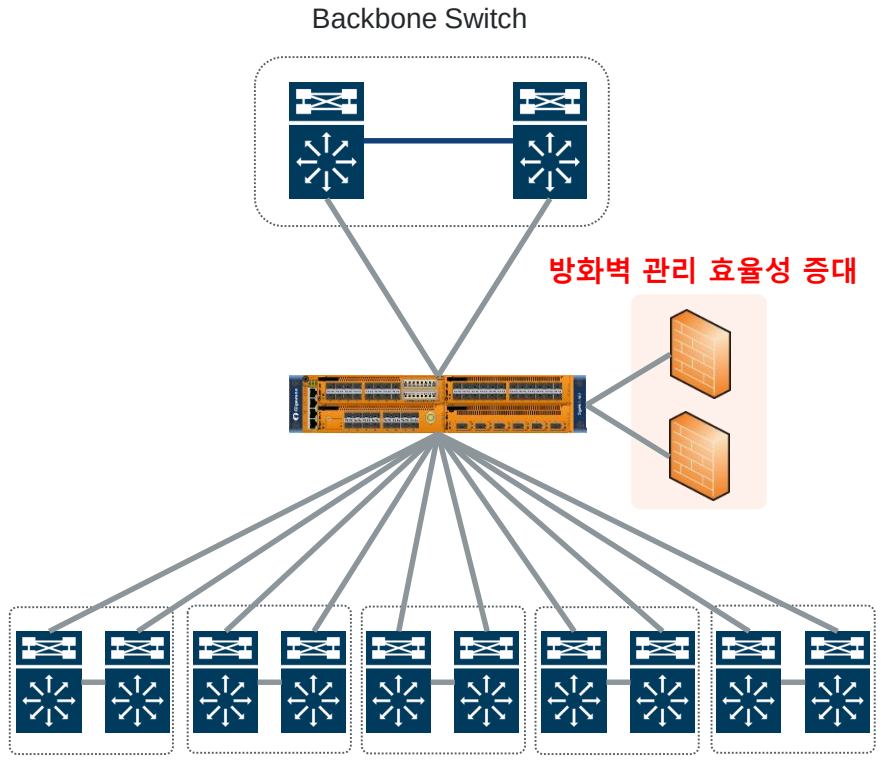
방화벽 장애 시에도 라우팅 경로 변경 없음

- 방화벽 장애 발생 시 기가몬 장비에서 트래픽 바이패스를 통한 정상 처리
- 기존 운영 네트워크망에서 불필요한 라우팅 경로 발생이 없음

Simple Network Secure Network



다수 접속 구간 Backbone Switch



다수 접속 구간 Backbone Switch

다수의 방화벽 도입으로 비효율적인 운영 및 투자

- 주요 서비스 구간 내 인라인으로 다수의 방화벽 운영으로 장애 요소 증가
- 고객접속구간 각 라인 별 방화벽 도입에 따른 비효율적인 투자

소수의 대용량 방화벽 도입으로 효율적인 방화벽 관리

- 소수의 대용량 방화벽 운영으로 장애 요소 최소화 및 효율적인 통합 보안 관리
- 방화벽 장애 시에도 기가몬 바이패스 동작으로 장애 요소 삭제

Case Study : E-Commerce

100G LOAD BALANCING

GigaVUE-HD8

GigaVUE-HD4

Background & Challenge

- 다수의 100G 링크의 트래픽을 10G 링크의 분석 장비 그룹으로 수용할 필요성
- 로드 밸런스(Load Balance) 필요

Solution

- 기가몬 적용 솔루션 : GigaVUE-HD4 & HD8
- 분석 장비는 A사 보안 팀에서 자체 제작

Results & Key Benefits

- Flow Mapping 기술로 100G 트래픽의 로드 밸런싱
- GigaSMART의 Applicaton Session Filtering 적용으로 분석 플로우의 L7 filtering
- 100G 링크의 분석 방법 제공으로 기존 10G 솔루션 활용 및 CAPEX 절감 효과

Case Study – 엔터프라이즈/제조

INLINE AND OUT-OF-BAND MONITORING

도입배경

- Inline Tools : SourceFire (now Cisco FirePOWER) IPS, Imperva WAF,
- Out-of-Band tools: FireEye, ExtraHop
- 인라인 및 OOB툴의 통합 구성 및 다계층 보안 요구

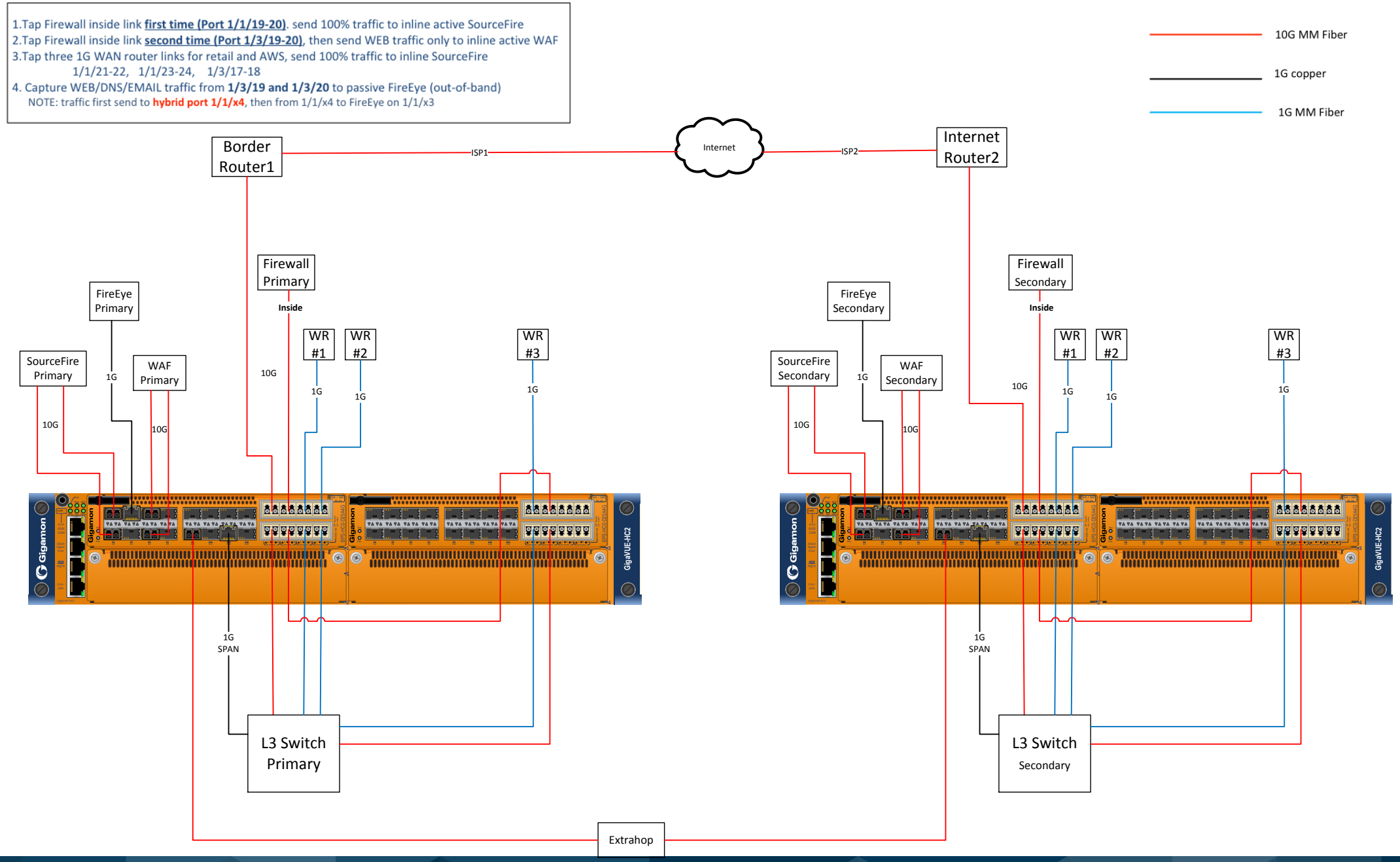
적용솔루션

- Inline 감시 구성을 위한 GigaVUE-HC2 bypass 기술 (1 x 10Gb & 3 x 1Gb links)
- Web 트래픽 감시 성능 향상을 위한 APP aware feature
- 확보된 동일 인터넷 트래픽을 OOB 툴 FireEye 와 ExtraHop 향 동시 전달

결과 및 핵심이점

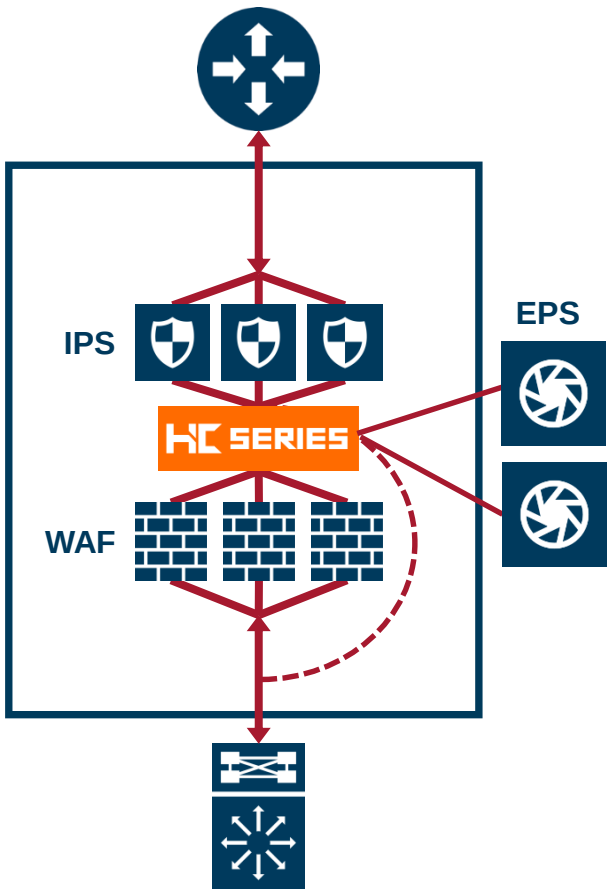
- 서로 다른 4개의 물리적 링크에 하나의 OOB 툴 활용 가능
- 인라인 및 OOB의 통합 구성 및 적은 비용으로 다계층 보안 구성 가능

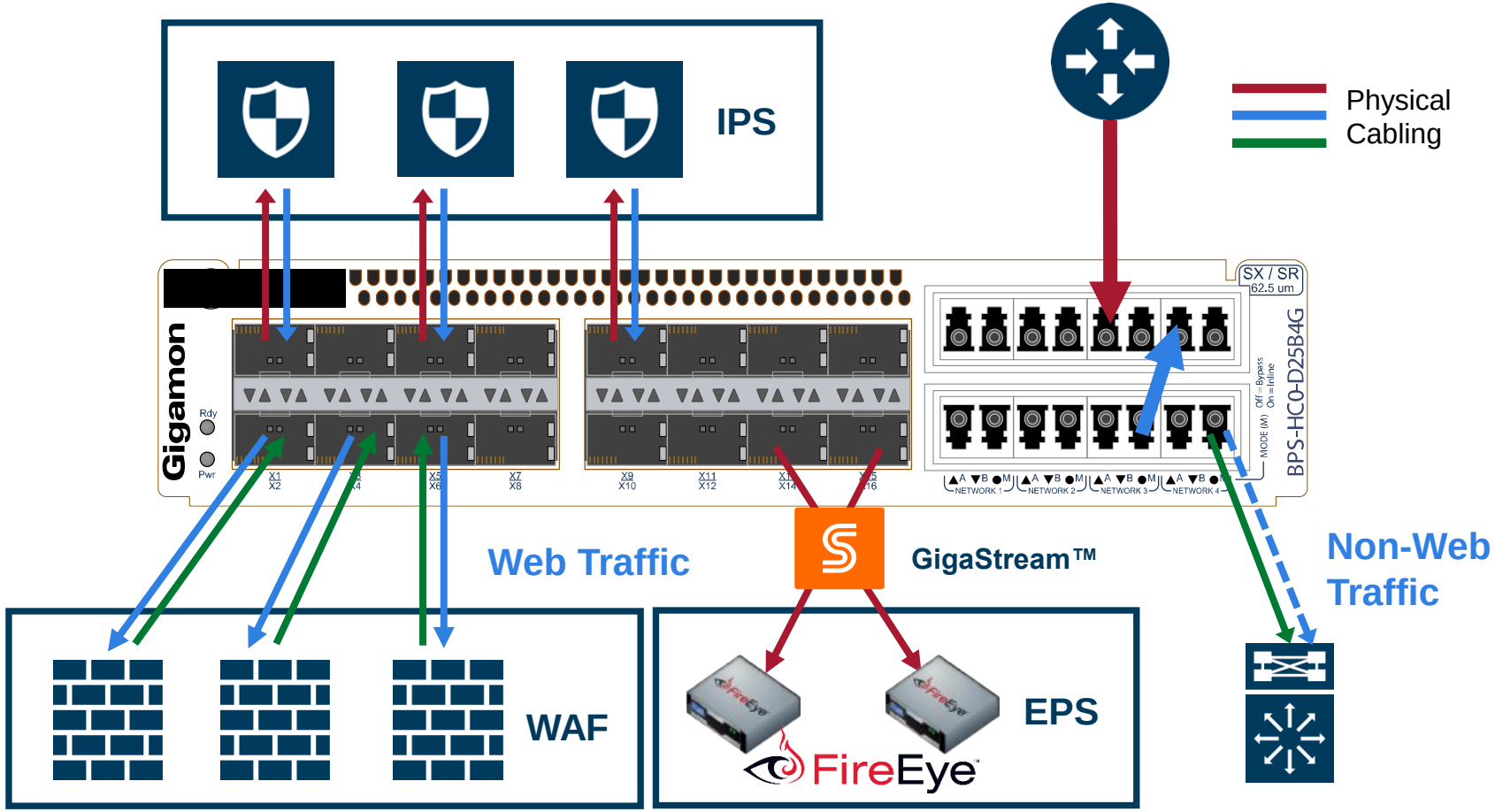
1.Tap Firewall inside link **first time (Port 1/1/19-20)**. send 100% traffic to inline active SourceFire
2.Tap Firewall inside link **second time (Port 1/3/19-20)**, then send WEB traffic only to inline active WAF
3.Tap three 1G WAN router links for retail and AWS, send 100% traffic to inline SourceFire
1/1/21-22, 1/1/23-24, 1/3/17-18
4. Capture WEB/DNS/EMAIL traffic from **1/3/19 and 1/3/20** to passive FireEye (out-of-band)
NOTE: traffic first send to **hybrid port 1/1/x4**, then from 1/1/x4 to FireEye on 1/1/x3



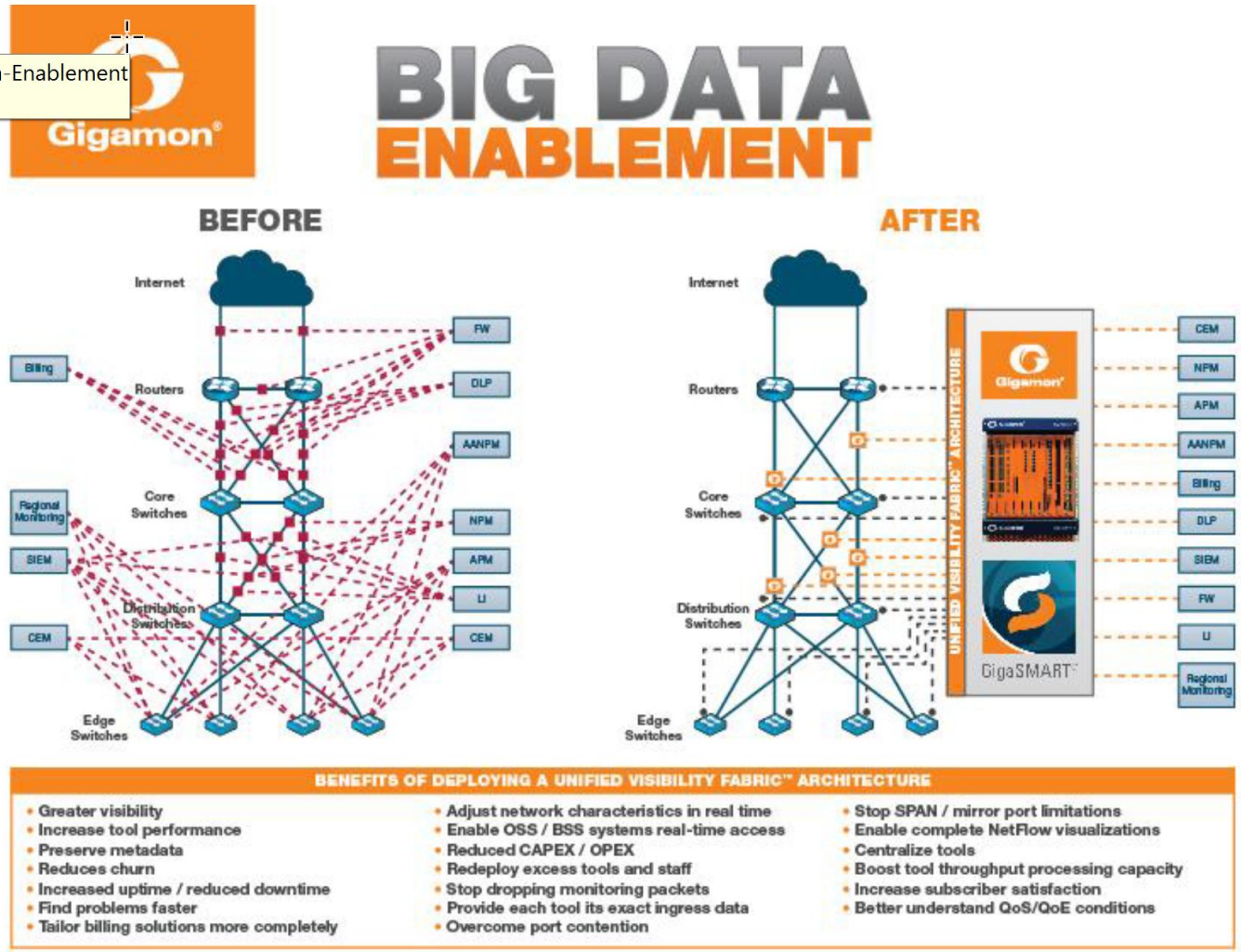
Case Study - 필요한 트래픽만 검사하자!

WITH MANUAL SERIAL INLINE CONFIGURATION





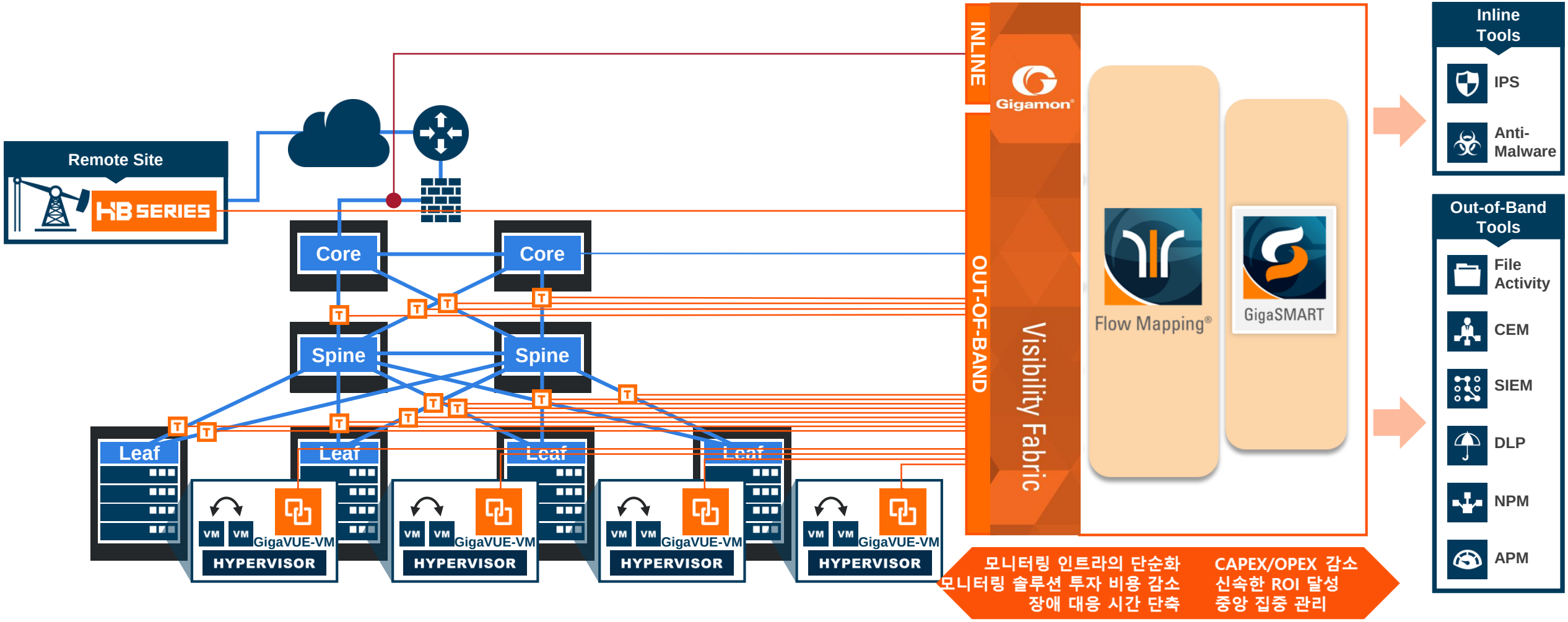
3.
Big Data 대한 대비



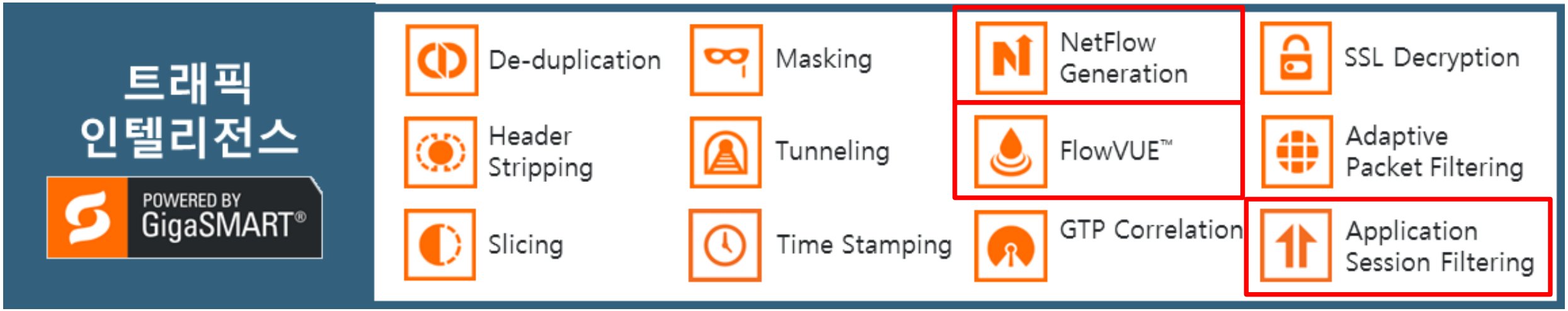
빅 데이터 vs. 보안

너무 많은 데이터 량 (TOO MUCH DATA)

Visibility Fabric™ 구성도



지능형 트래픽 제단 기능 – GigaSMART



ASF: DPI 기반 특정 어플리케이션 세션 필터링

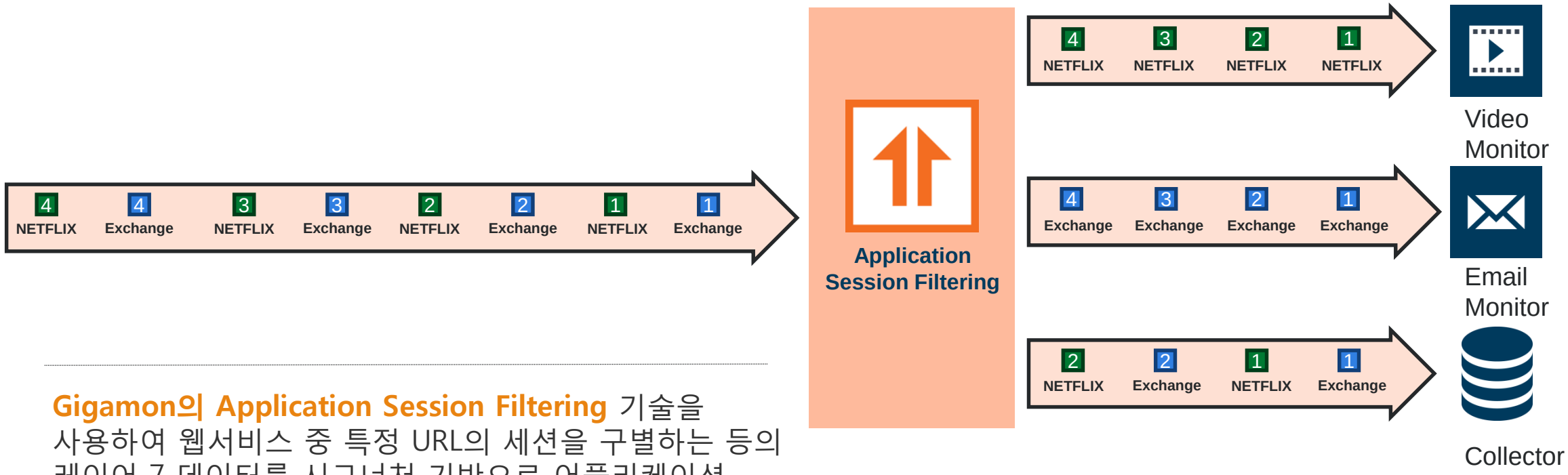
LIMITATIONS OF PORT BASED APPROACH TO APPLICATION VISIBILITY

Protocol	HTTP	SMTP	FTP	TELNET	NTP	BGP
TCP/UDP Port #	80	25	20/21	23	123	179

Protocols?
All Web 2.0 use port 80 & 443

ASF: DPI 기반 특정 어플리케이션 세션 필터링

L7 기반 세션 필터링, APPLICATION SESSION FILTERING



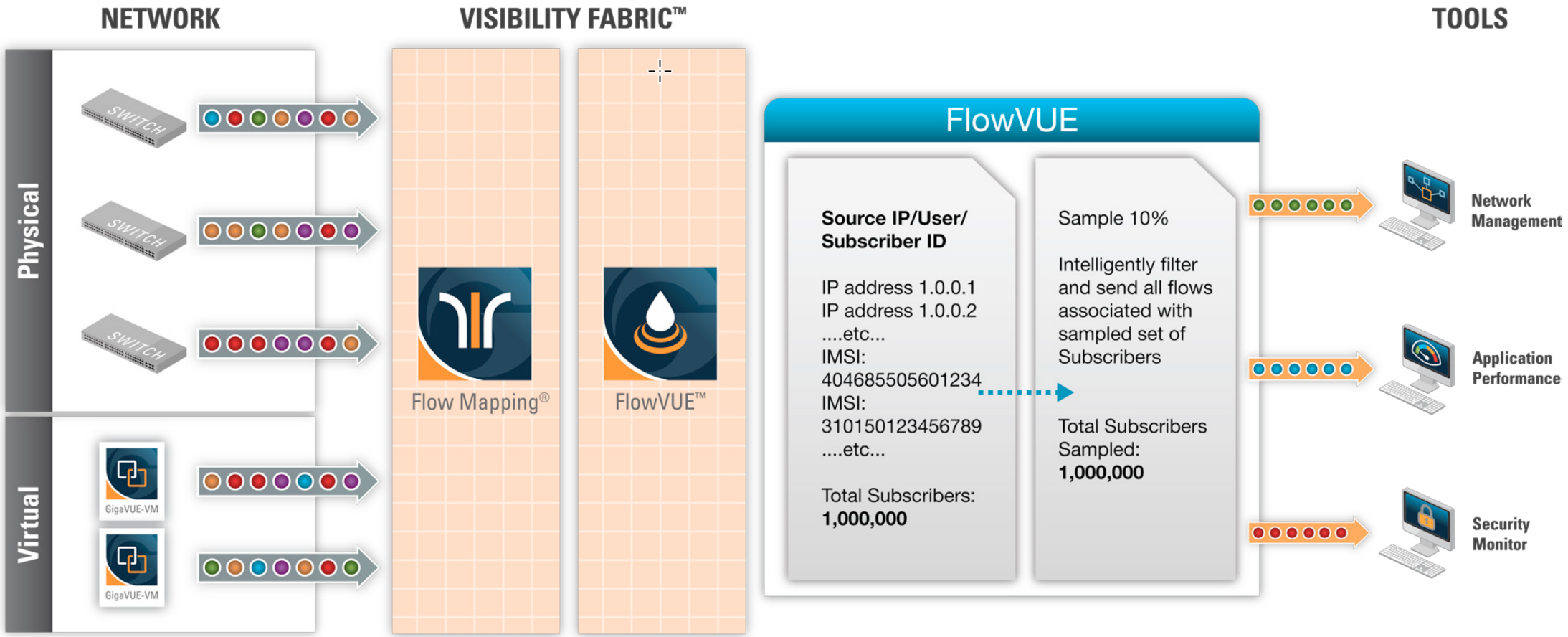
Gigamon의 Application Session Filtering 기술을 사용하여 웹서비스 중 특정 URL의 세션을 구별하는 등의 레이어 7 데이터를 시그너처 기반으로 어플리케이션 세션을 분류 할 수 있음. 이를 통해 제한된 모니터링/분석 도구를 효율적으로 사용할 수 있는 경제성을 제공

GigaSMART® : Adaptive Packet Filtering

L7 기반 패킷 필터링

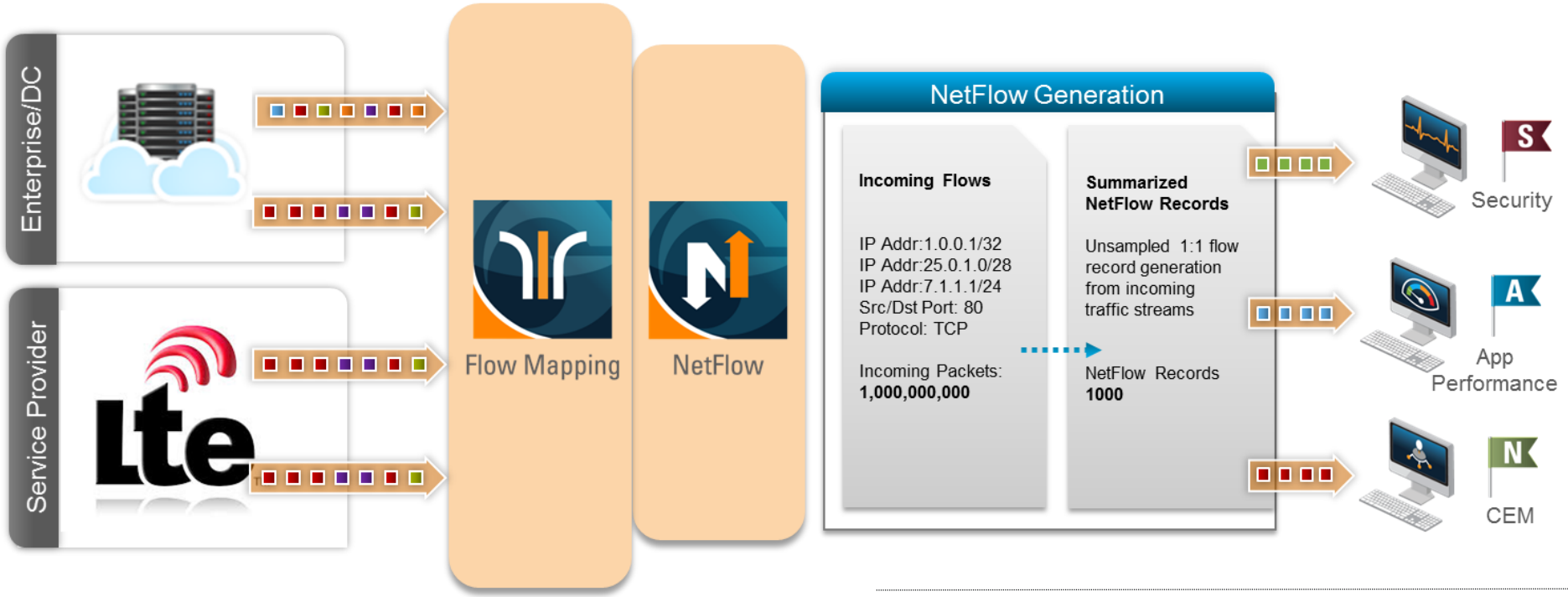
FlowVUE

세션/FLOW 기반 샘플링



NetFlow Generation

전수 트래픽(UNSAMPLED) NETFLOW 생성 기능

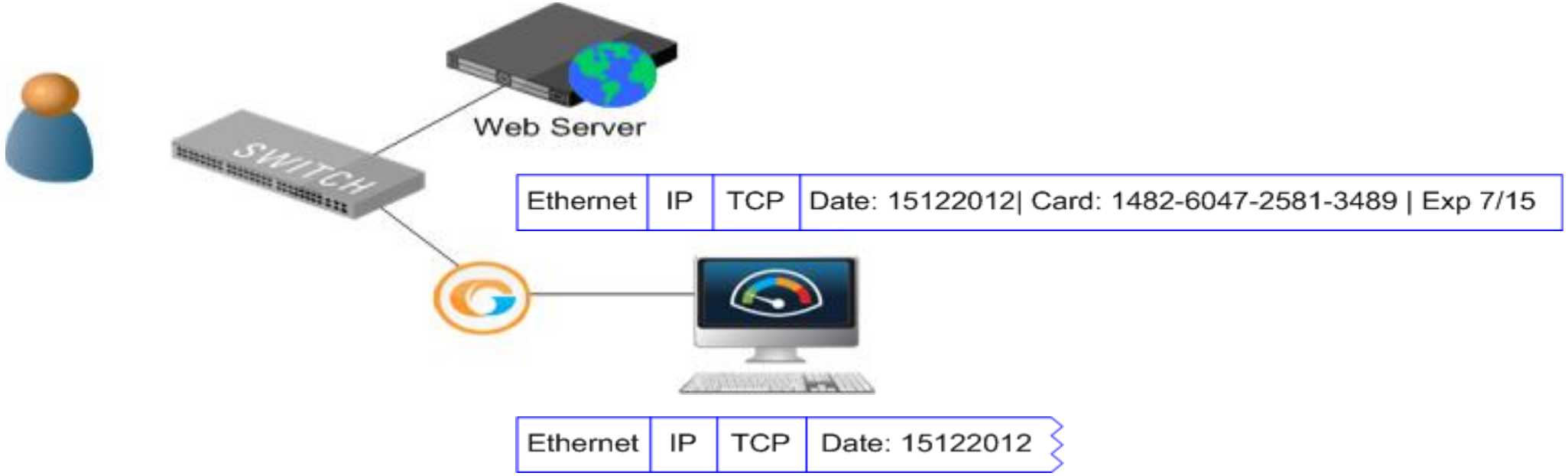


Gigamon의 NetFlow 생성 기능을 사용하여 전수 트래픽의 모니터링 분석 이 가능하며, 동시에 6개의 수집 서버로 NetFlow 전송 가능. 지원 버전 : NetFlow v5, v9 및 IPFIX

GigaSMART® : Packet Slicing

대역폭, 스토리지 보호를 위한 패킷 사이즈 조정 기능

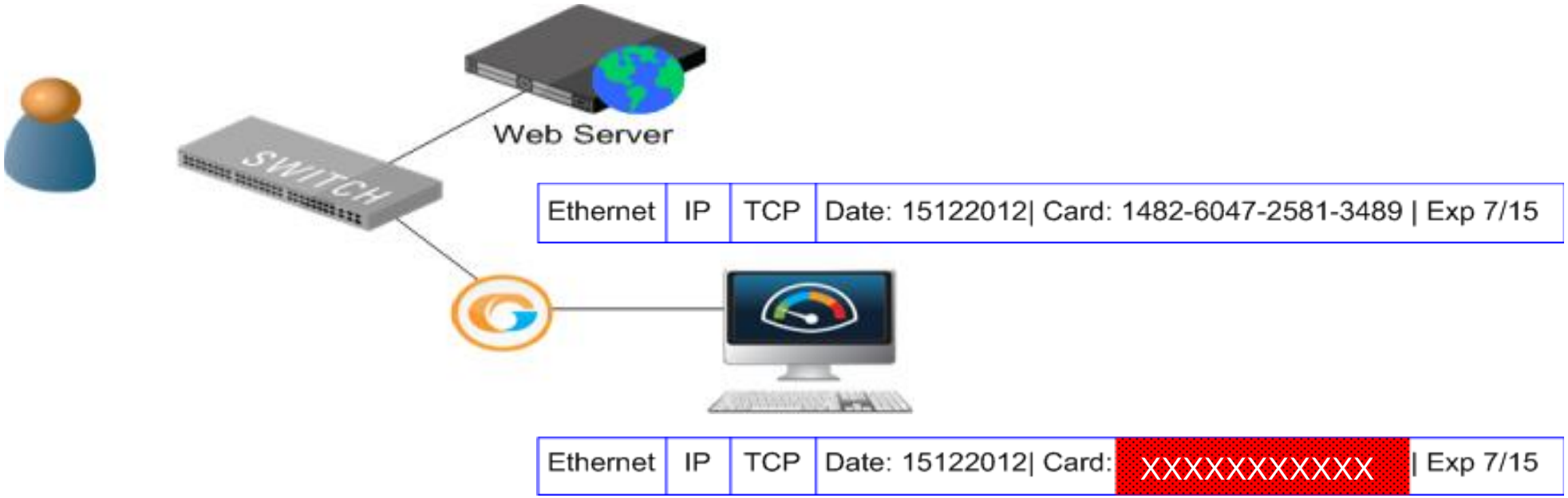
- **FLOW MAPPING 룰에 따라, 다양한 사이즈로 패킷 사이즈를 조정**
- **패킷헤더 정보 및 필요한 정보만 저장하여 패킷 저장 장치의 스토리지 최적화**



GigaSMART® : Packet Masking

개인 정보 등 데이터 마스킹 기능 제공

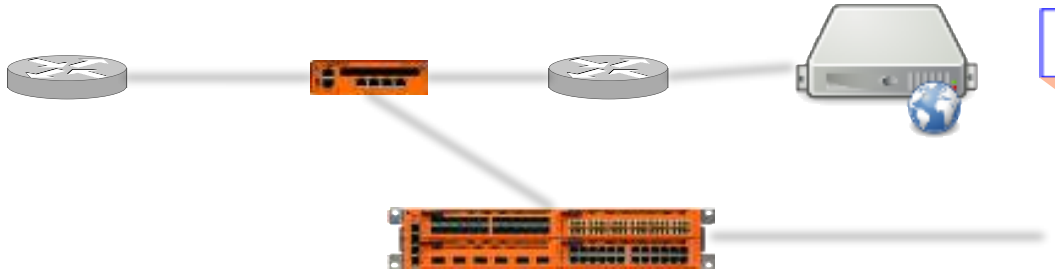
- **패킷의 PAYLOAD에 포함된 개인정보 등 민감한 데이터를 마스킹하는 기능을 제공**
- **마스킹할 패턴을 정의하고 인입 포트에 마스킹 룰을 적용**

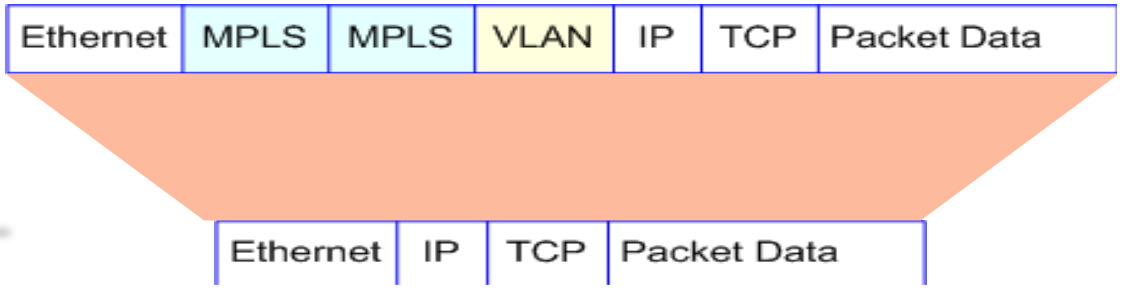


GigaSMART® : Packet Header Stripping

패킷 해더 제거

- VLAN, MPLS, VN-Tags, VXLAN, Cisco FabricPath, GTP tunnels, ISL tunnels, GRE 등 분석/모니터링 장비에서 인식할 수 없는 패킷 헤더 정보 제거하는 기능 제공
- 패킷 구분을 위하여 VLAN tag 정보를 추가하는 기능 제공





GigaSMART® : De-Duplication

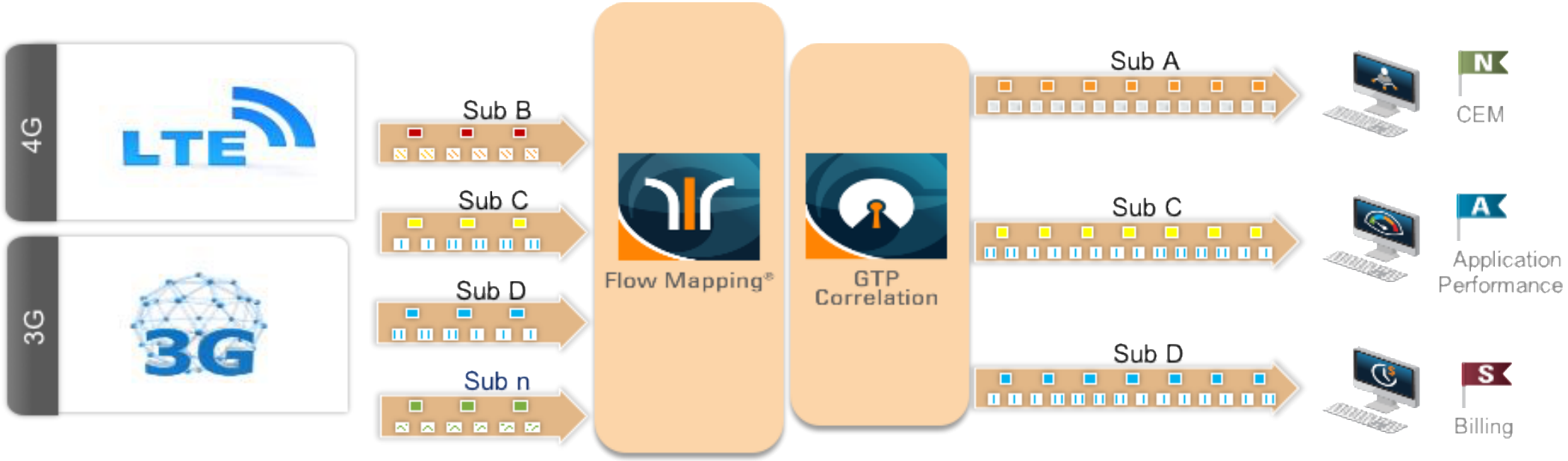
중복 패킷 제거로 툴 장비 자원 보호 및 신뢰성 있는 분석 결과 제공

- 분석/모니터링 장비의 정확성을 위하여 중복 패킷 제거
- 중복 패킷 제거 혹은 카운팅 제공

GigaSMART®: GTP Correlation

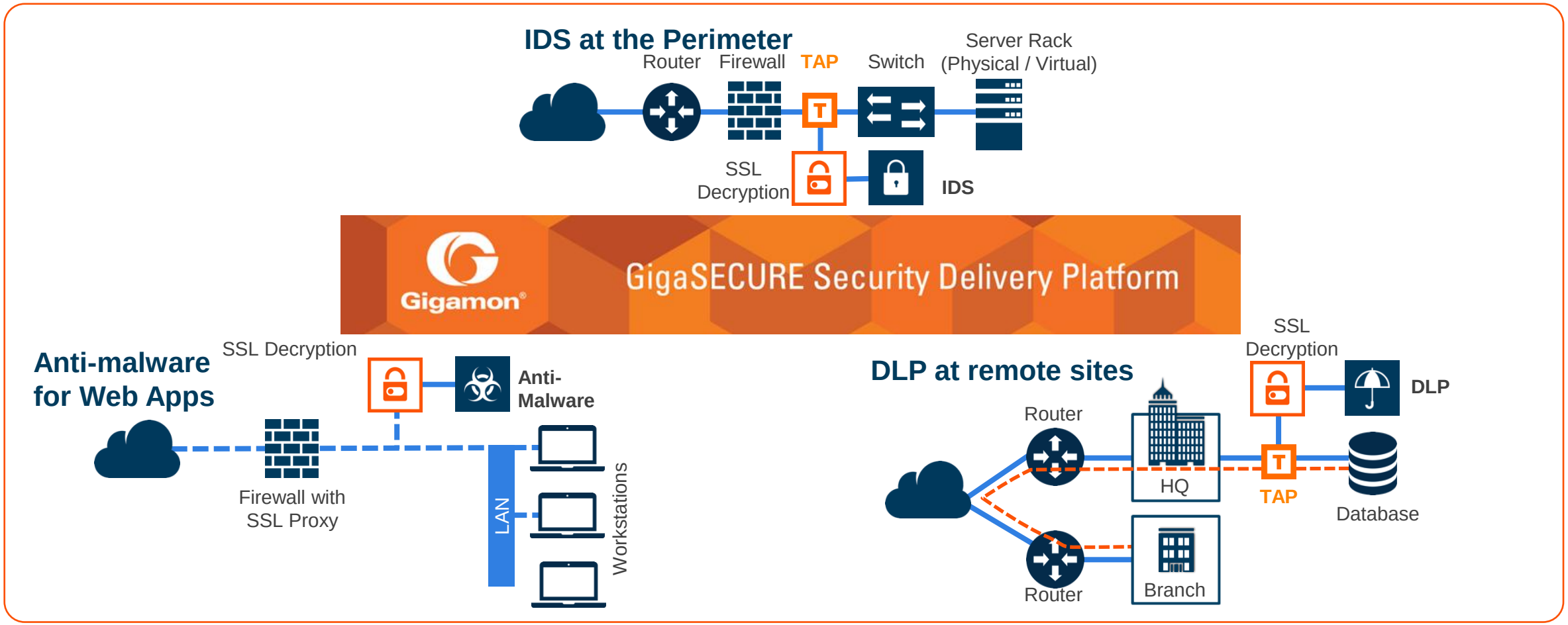
3G 또는 LTE 망 내 GTP-u & GTP-c 패킷의 연관성 제공

- GTP-u/GTP-c 연계 분석을 위하여 동일 분석 Tools로 전달
- 가입자 기반의 플로우 샘플링 기능 제공
- White List 제공으로 특정 가입자의 Tracking 기능 제공



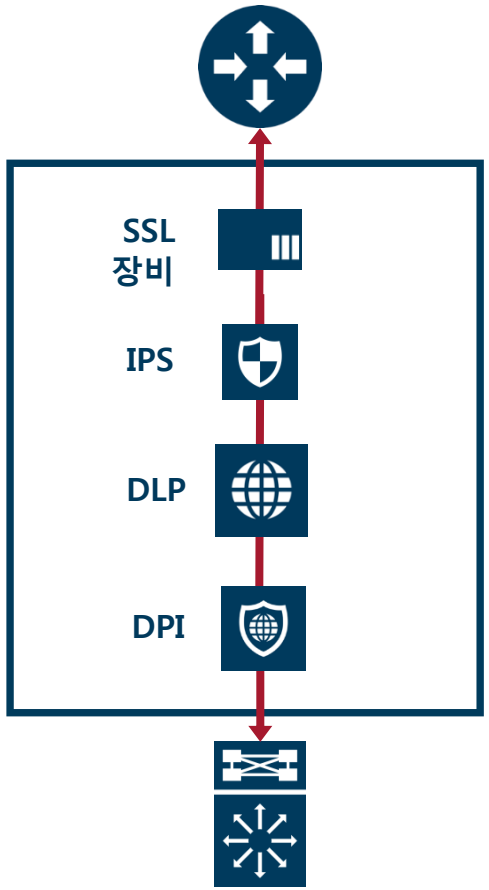
GigaSMART® : SSL Decryption (Out of Band)

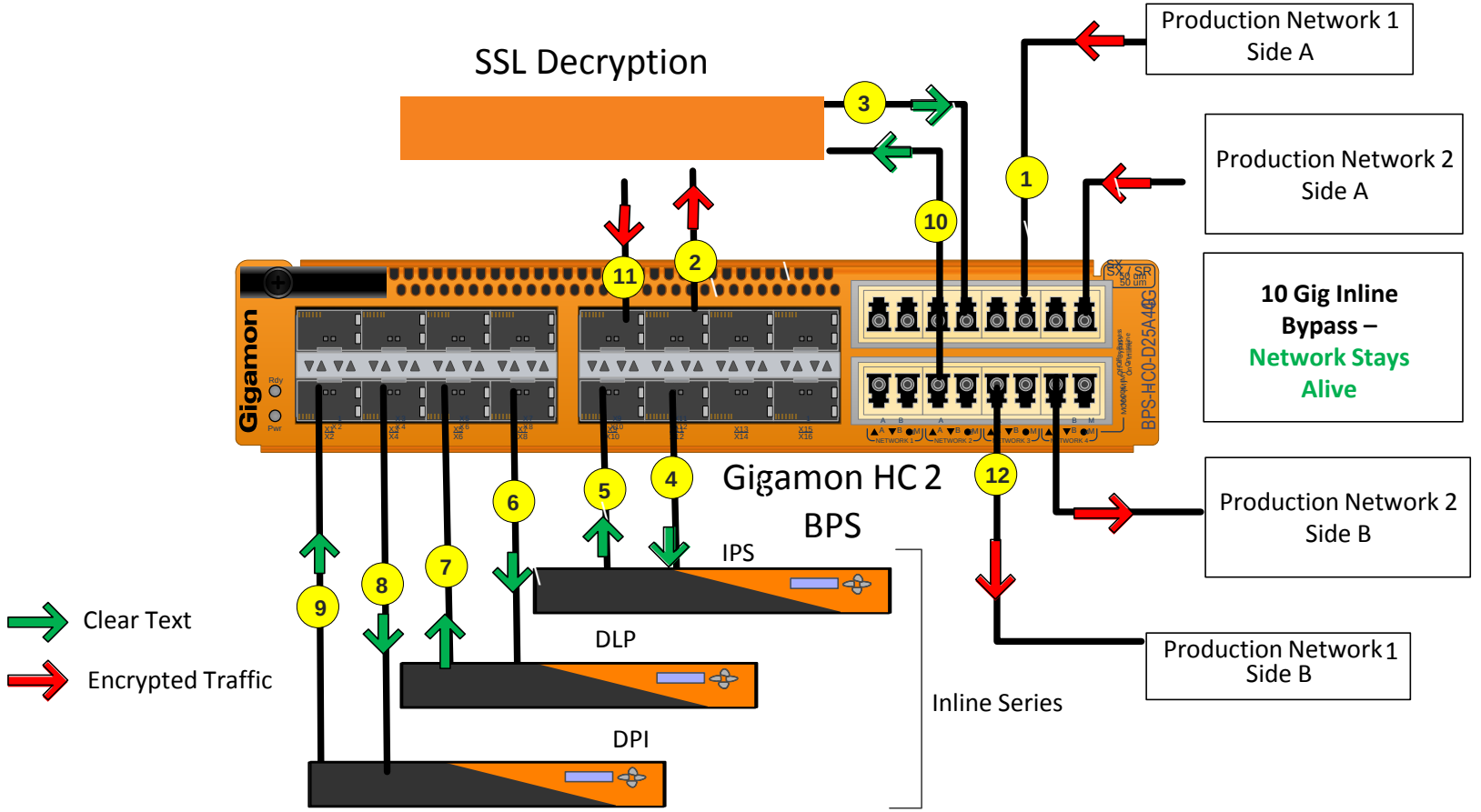
OUT-OF-BAND 방식으로 SSL 암호화 패킷을 복호화 기능 제공

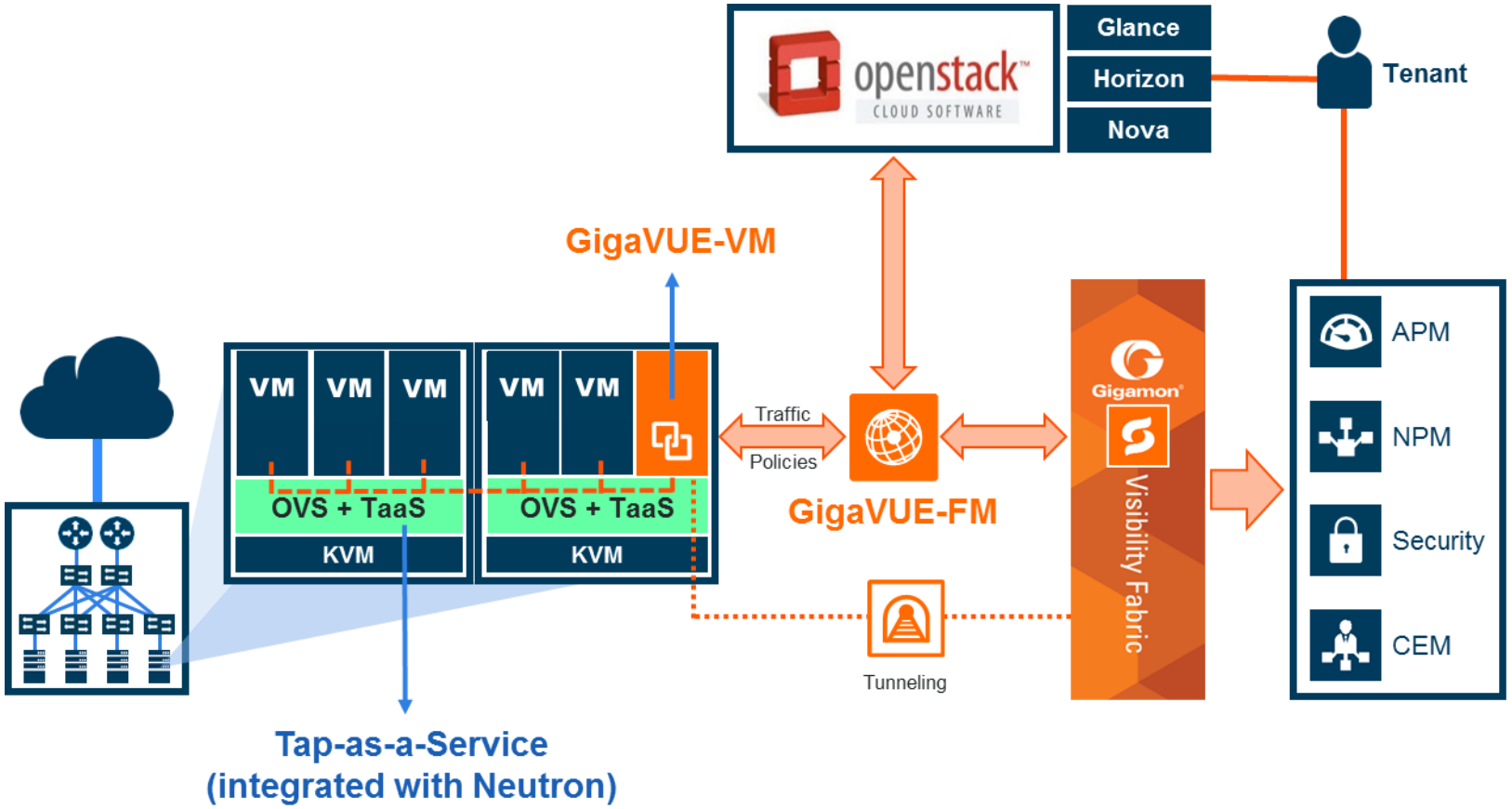


GigaSMART® : SSL Decryption (In-Line)

외장형 SSL DECRYPTION 솔루션 + DLP/IPS 결합 솔루션 :인라인 바이패스 보호,
이중화(HA), 로드밸런싱 제공으로 안정성 및 유연한 확장성 보장



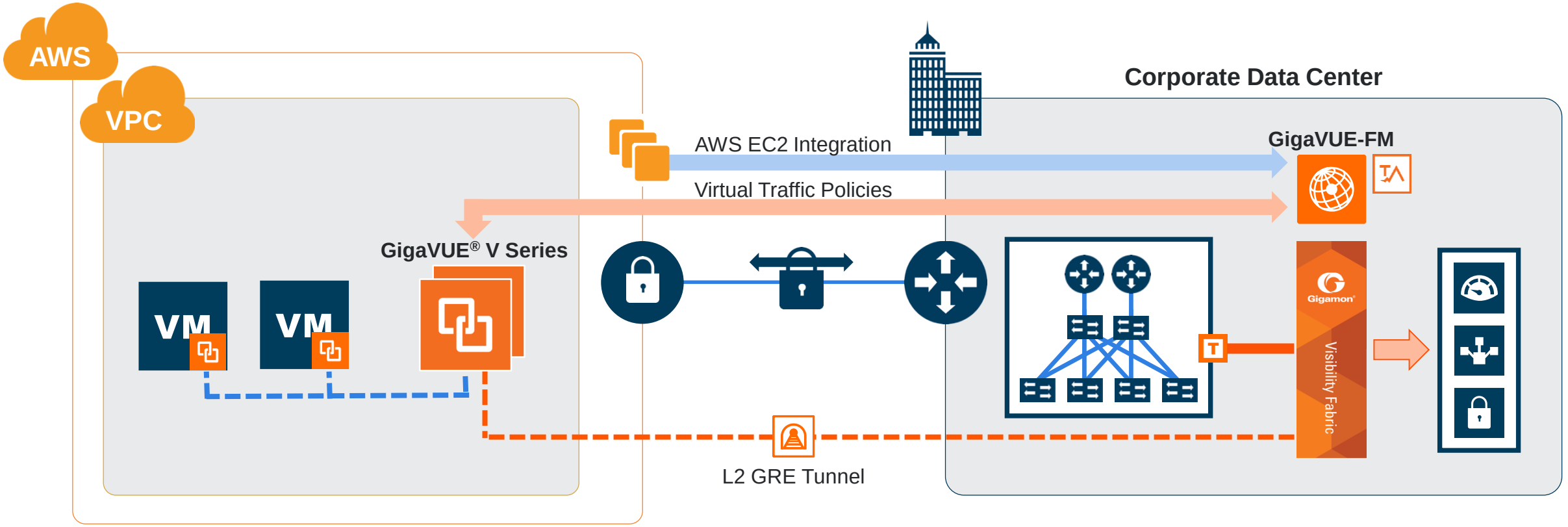




4. Cloud 가시성

Public Cloud 사례 – AWS

EXAMPLE USE CASE: TOOLS IN AN ON-PREM DATA CENTER

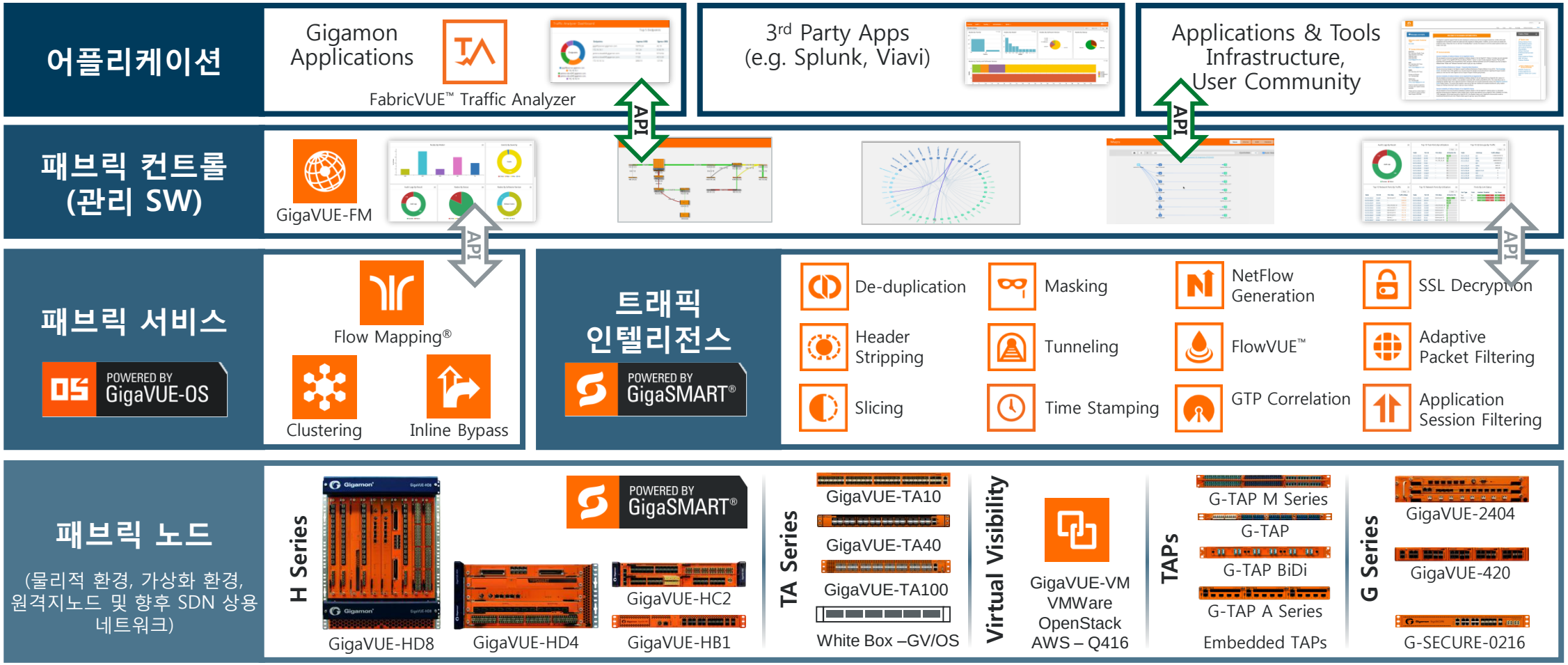


Public Could 의 트래픽을 자사 데이터센터의 보안 및 분석 장비로 전송

VPC: Virtual Private Cloud. Any forward-looking indication of plans for products is preliminary and all future release dates are tentative and subject to change.

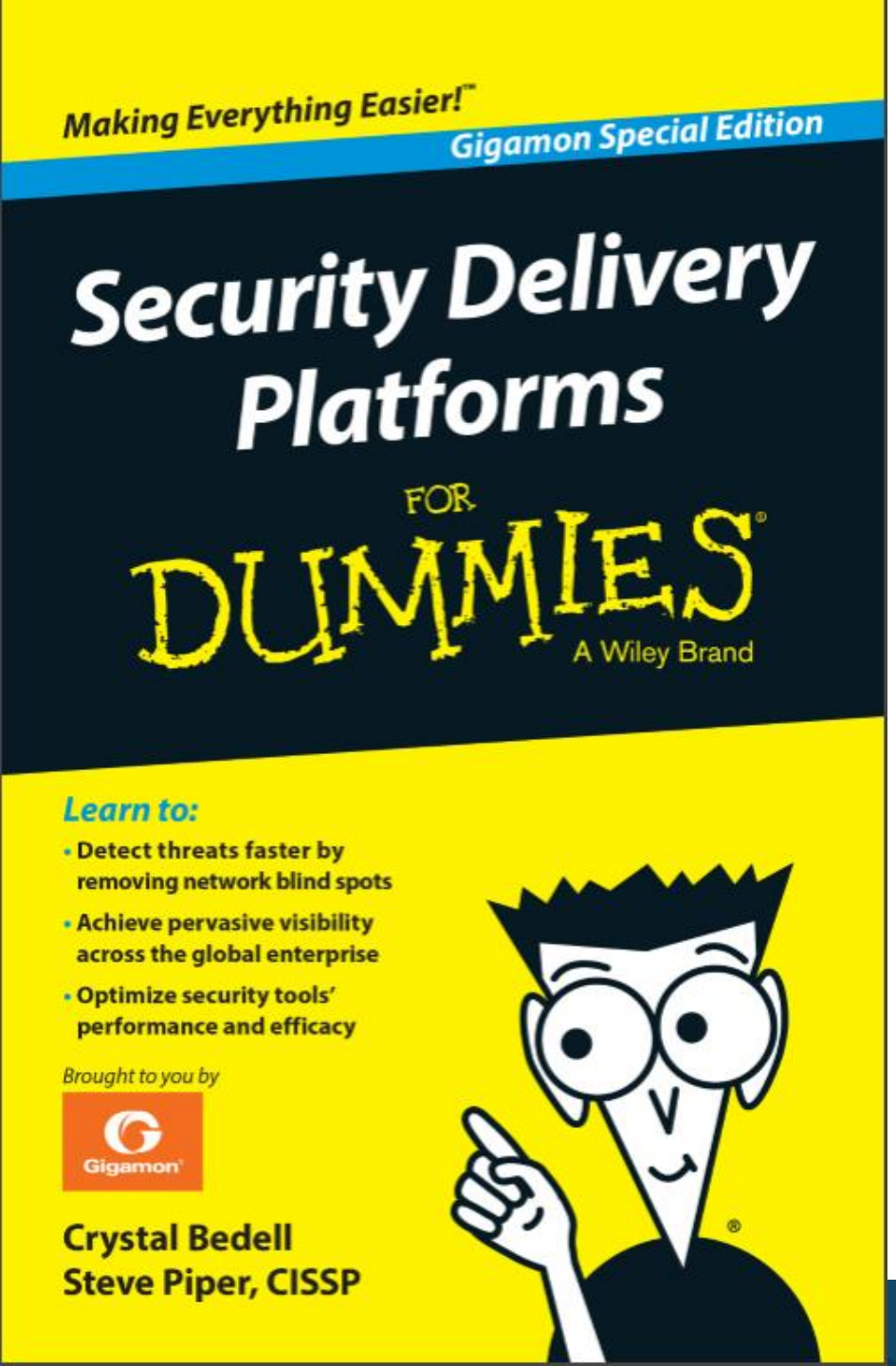
VISIBILITY MATTERS

Visibility Fabric™통합 포트폴리오



Visibility Fabric™ 주요 장비 사양

장비 모델명	장비 외관	Visibility Throughput	Port Density
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 10G : 96 ports (1G)
GigaVUE-HB1		56 Gbps	10G : 4 ports 1G : 20 ports
GigaVUE-TA10		640 Gbps	40G : 4 ports 10G : 48 ports



홈페이지 방문, E-Book을 신청하세요.
http://www.gigamon.com

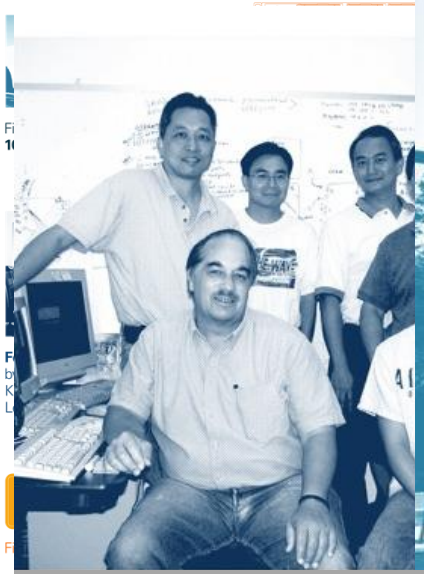
https://www.gigamon.com/resources/book/security-delivery-platforms-dummies-3197

기가몬 회사소개

Leader in Visibility for Security & Monitoring

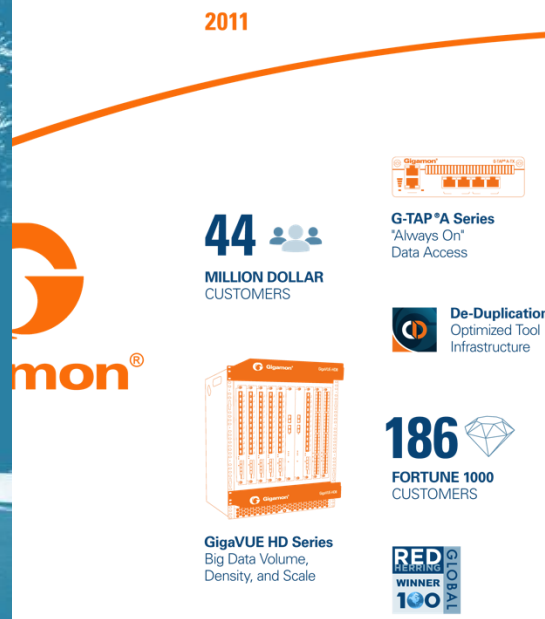
기가몬 (Gigamon) 소개

- 설립연도 : 2004년 (Pioneered Market)
- 본사위치 : 미국, 캘리포니아 Santa Clara
- 기업공개 : 2013년 6월 (NYSE, GIMO)
- 주요사업 : 보안 및 관리툴을 위한 가시성 솔루션/
  모바일(Mobile), 데이타센타 (Datacenter), 클라우드 (Cloud)
- 보유기술* : 26 개 핵심특허권, 28 개 특허 심사 중
- 시장점유율** : 약 40% (가시성 시장의 리더 및 Innovator)
- 주요고객 : 1700+ 고객(포춘 100대 기업 중 75개+, 전세계 글로벌 100대 통신사 중 50개+)



2004년 창립기념 촬영사진

2015년 캘리포니아 본사 전경



2004 2005

*Customer and patent numbers FY15Q2, **Gartner published on Jan 19th, 2016

기가몬 주요 고객 사

(기준 : 2015년 2사분기)

엔터프라이즈

TECHNOLOGY

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

INDUSTRIAL

3M, MARATHON, BAKER HUGHES, Constellation Energy, NEC, Chevron, BNSF RAILWAY, aeso, Lockheed Martin, Genentech, HONDA, Schering-Plough

RETAIL

Sara Lee, Target, ConAgra Foods, WAL★MART, Enterprise rent-a-car, BEST BUY, JCPenney, COSTCO WHOLESALE, General Mills

FINANCE

MasterCard, DISCOVER, NYSE, Mellon, BARCLAYS, NASDAQ, Fidelity, Deutsche Bank, Merrill Lynch, 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

1700+ 글로벌 고객

Fortune-100 내 75+ 기업

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

글로벌 TOP 100 SP 내 50개

A broad spectrum of brand-name customers.

요약 (Why Gigamon?)

포춘 지 선정 100대 기업 내 75+ 기업과 1,700 이상의 글로벌 고객에서 입증된 제품과 기술력

- 산업계 최초의 보안 전달 플랫폼 (Security Delivery Platform)
- SDN (Cisco ACI, VMware NSX)을 포함한 가상화 및 물리적 환경 내 전체적인 가시성 제공
- 특허 받은 Flow Mapping®기술을 통한 Zero Packet Loss 및 N:M 필터링 구현
- 클러스터링 (Clustering) 기술을 통한 구성관리의 단순화 및 유연한 확장성 보장
- 진보된 트래픽 인텔리전스와 서비스 연결성(Chaining)을 제공하는 탁월한 GigaSMART® 기능
- SSL 복호화 및 어플리케이션 세션기반 필터링 기능등의 통합된 가시성을 제공하는 유일한 회사
- 한층 넓고, 깊은 트래픽 인사이트 (Insight) 제공을 위한 전수 NetFlow / IPFIX 메타데이타 제공
- 고객과 파트너 성공에 100% 집중하는 회사

Customer numbers FY15Q2.

Gigamon®

Thank You!