Gigamon®

보안 이제는 플랫폼이다!

(기가몬 보안 전달 플랫폼/패킷 전달 플랫폼 소개)

기가몬 코리아

이민형

Agenda

1.보안전달플랫폼 소개

2.핵심기술

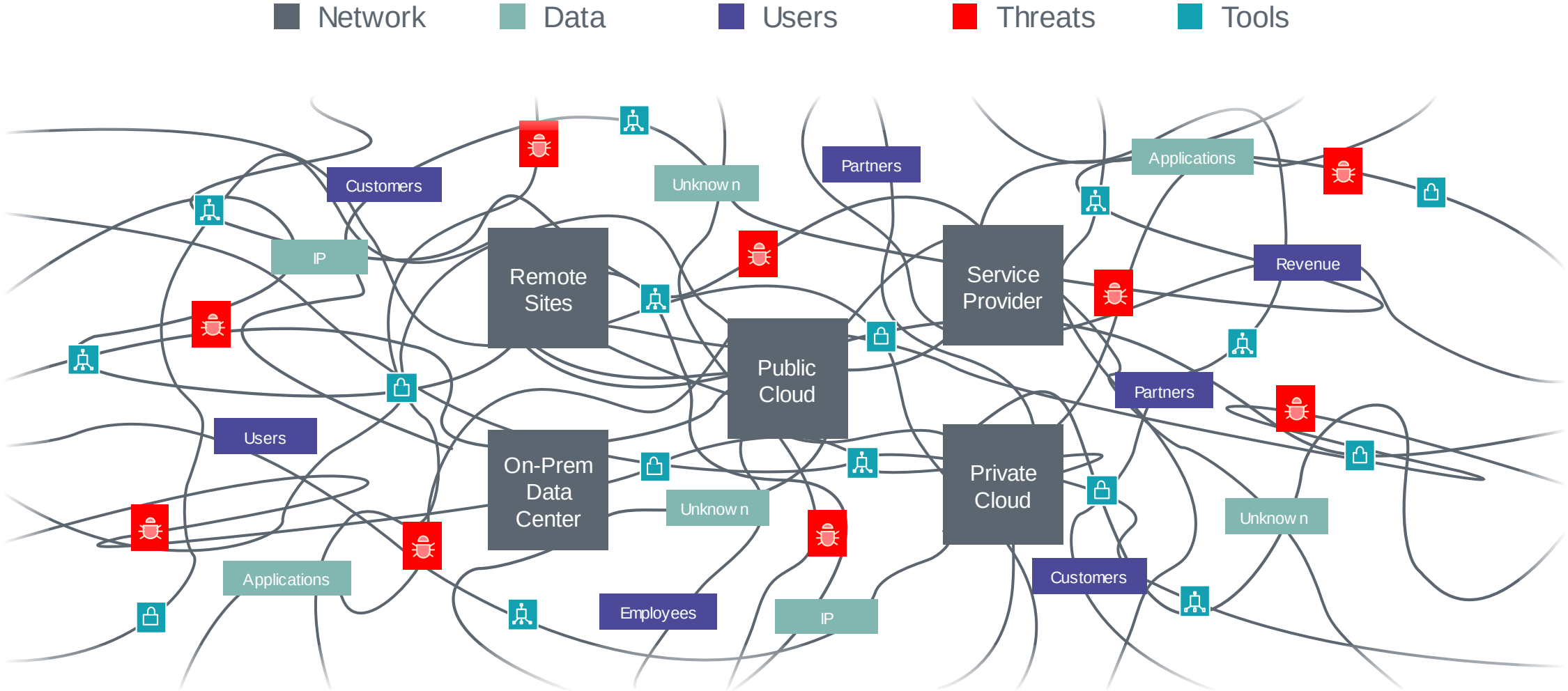
3.활용방안

4. 고객사례

5.제조사 소개

1. 보안전달플랫폼 소개

In Reality - DATA in EVERYWHERE(본사, 지사, 데이터 센터, 클라우드 등)



1. 보안전달플랫폼 소개

보안 관련 이슈 사항 – 변화되는 보안위협

You cannot secure/manage what you cannot see!

*Trustwave Holdings, Inc. "Trustwave Global Security Report.". **FireEye. "MAGINOT REVISITED: More Real-World Results from Real-World Tests.".

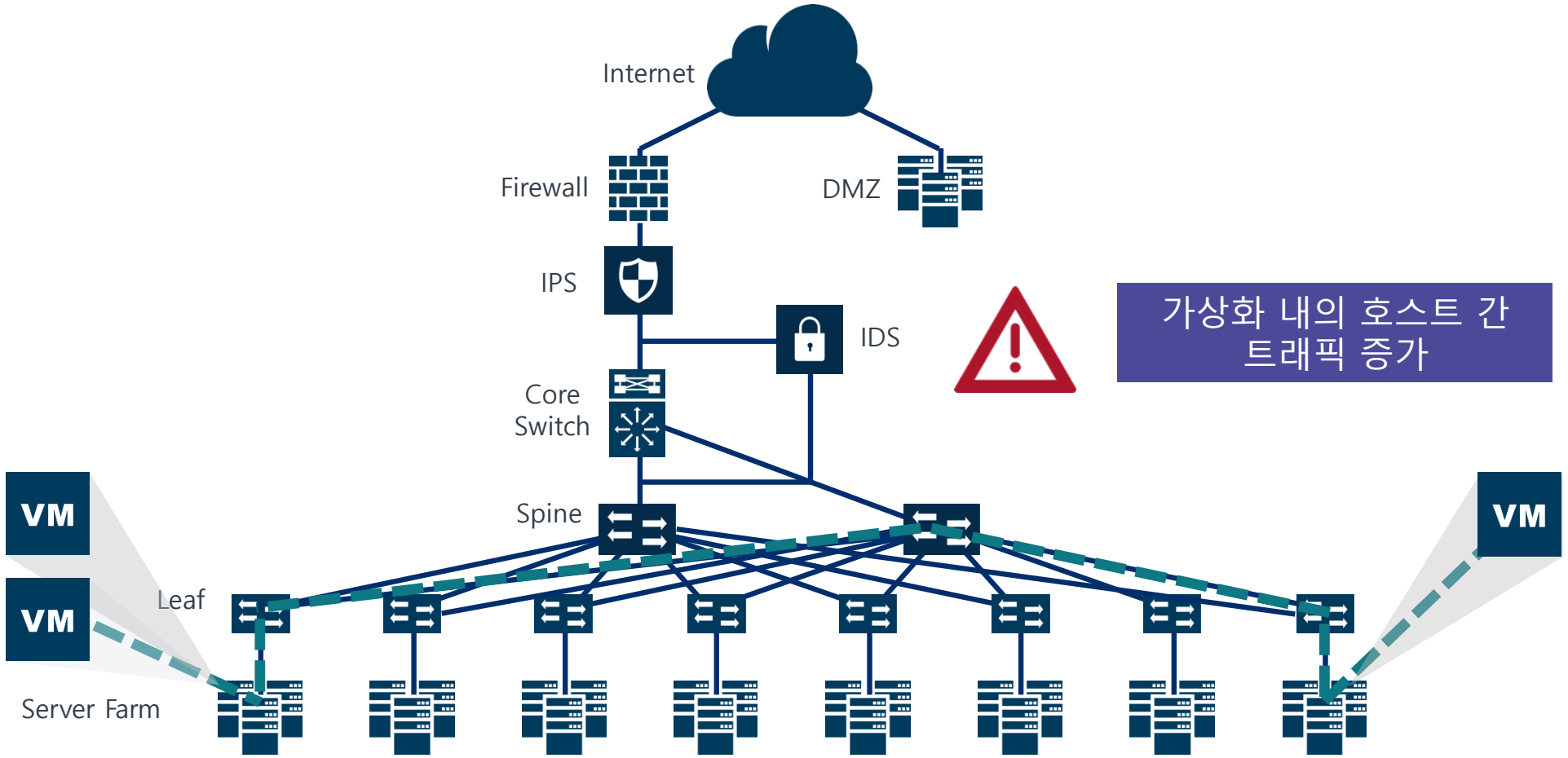
Gigamon

1. 보안전달플랫폼 소개

보안 관련 이슈 사항 – 너무나 많은 데이터량

1. 보안전달플랫폼 소개

보안 관련 이슈 사항 - 트래픽 패턴의 변화



1. 보안전달플랫폼 소개

보안 관련 이슈 사항 – 암호화 트래픽(SSL)의 증가

SSL 트래픽 (현재) : 기업 트래픽의 25%-35% [1]

보안 및 관리 툴은 SSL 트래픽을 인지 못 하거나, 복호화 시 과부화가 발생

Large (2048b) ciphers 는 SSL 복호화 장비의 **81%** 성능 감소를 유발 [1]

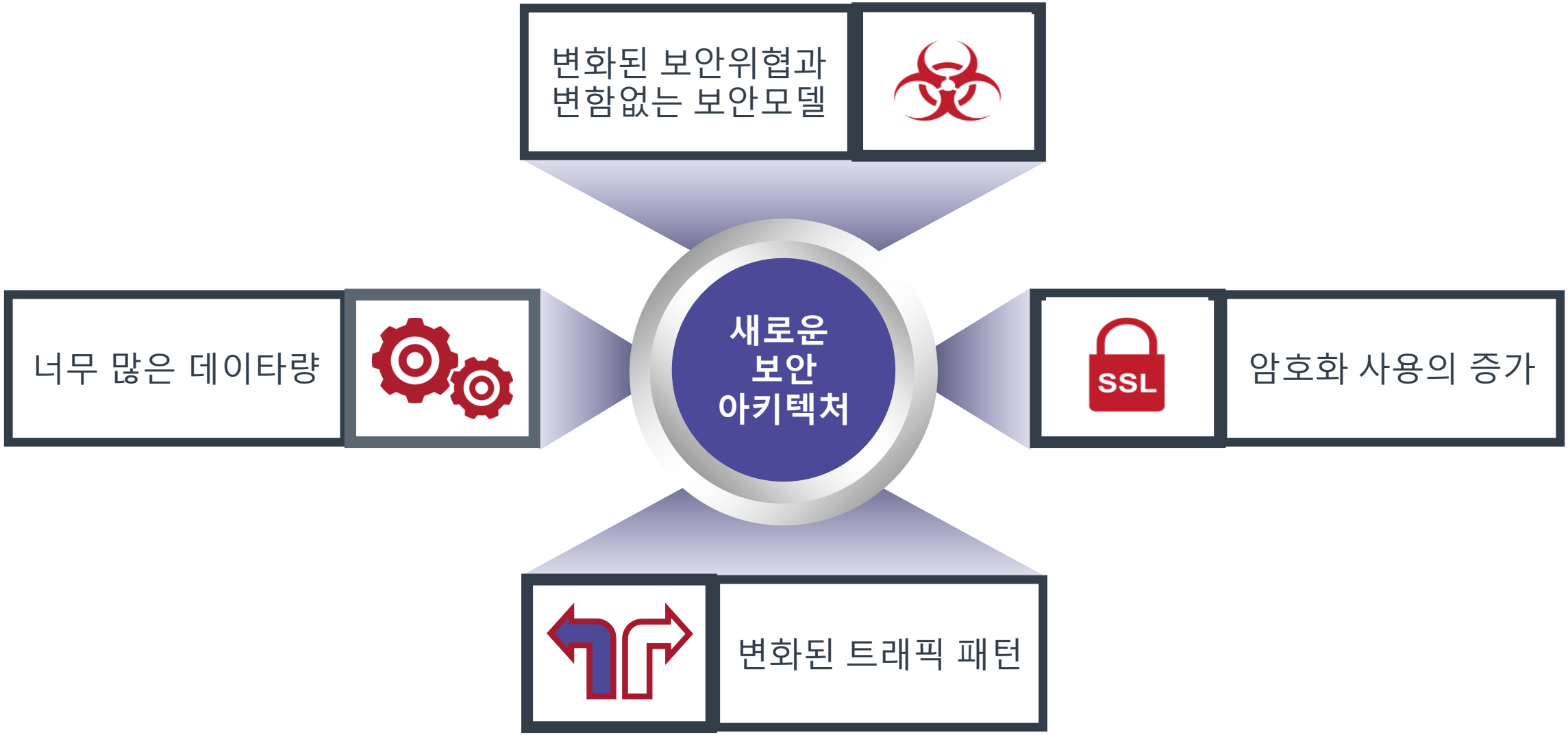
늘어나는 암호화된 트래픽에 대응 할 방법은?

[1] NSS Labs : 보안솔루션 전문 테스트 기업
[2] Gartner

Gigamon

1. 보안전달플랫폼 소개

보안 아키텍처의 재고



1. 보안전달플랫폼 소개

고객의 PAIN POINTS

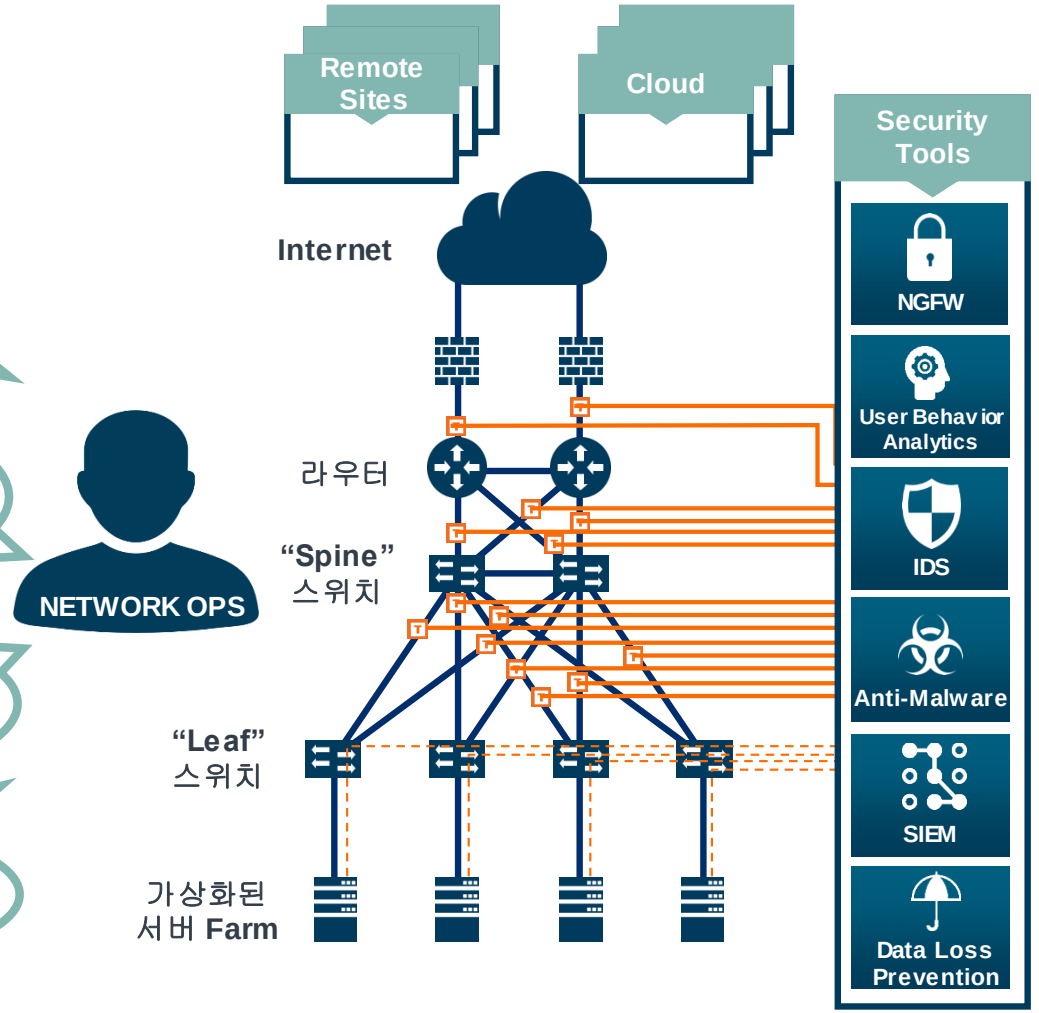
Network Operations

보안 툴로 인해 네트워크 장애나 지연시간 증가가 발생할까 걱정입니다

보안 툴 구성을 위한 미러 포트가 부족합니다

보안 툴 업그레이드에 따라 네트워크 가용성이 훼손됩니다

라우팅 변경없이 네트워크 트래픽 경로를 변경할 수 있습니까?



Security Operations

보안 강화를 위해 네트워크 전체 트래픽을 받아야 합니다

SECURITY OPS

트래픽 확보를 위해 네트워크팀의 신속한 협조가 필요 합니다.

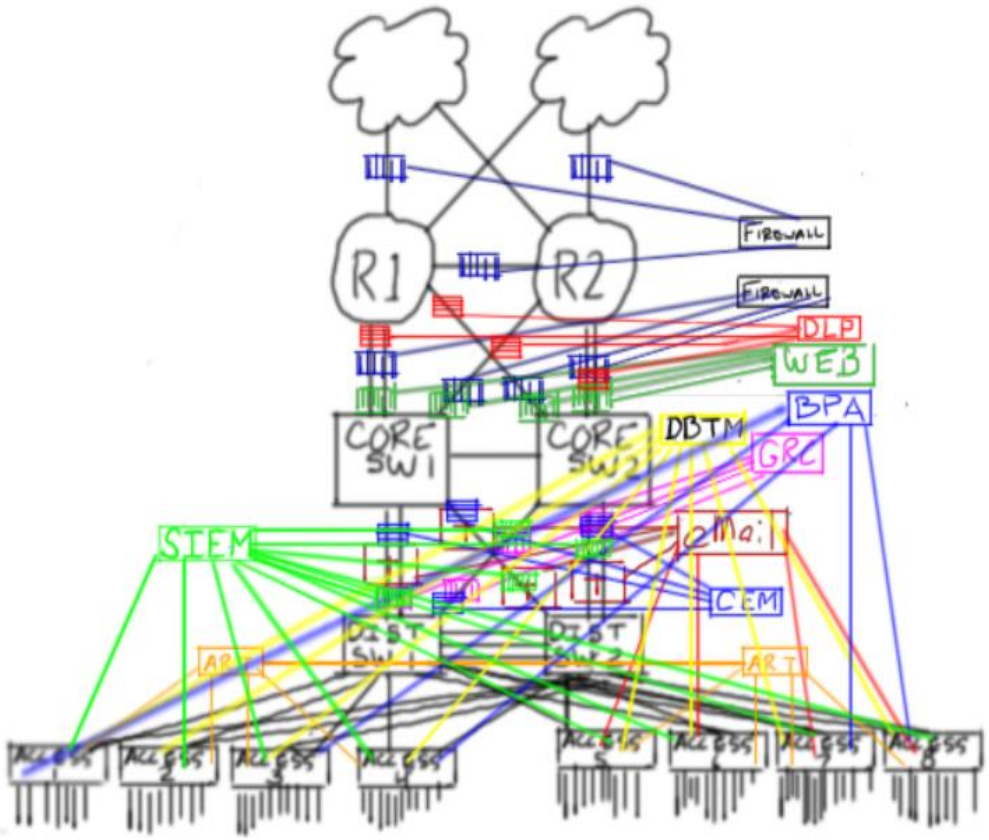
늘어나는 SSL트래픽을 효율적으로 검사할 수 있습니까?

빅데이터 및 IoT 를 위한 보안방법은 인라인 또는 OOB 구성입니까?

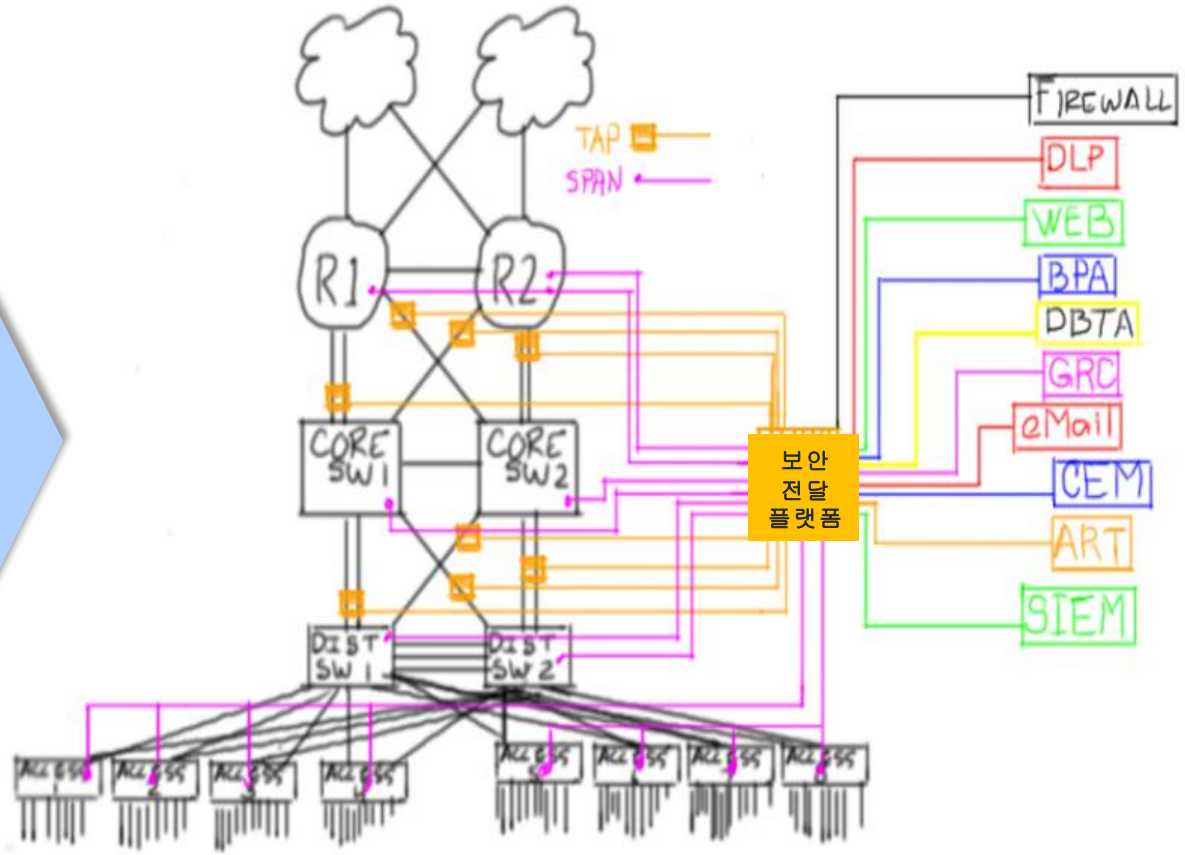
1. 보안전달플랫폼 소개

보안전달 플랫폼 – 도입 전, 후

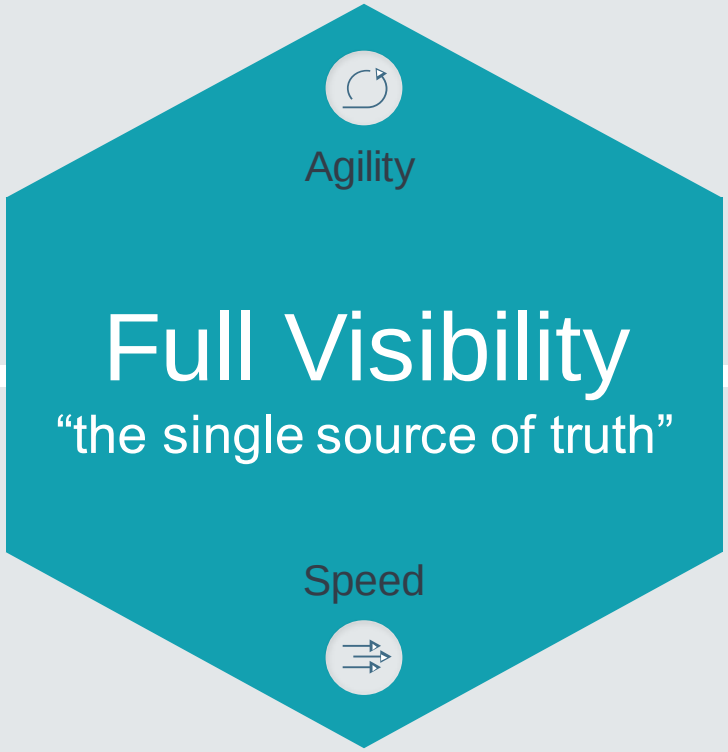
As-Is (전통적인 접근방식)



To-Be (보안 전달 플랫폼)

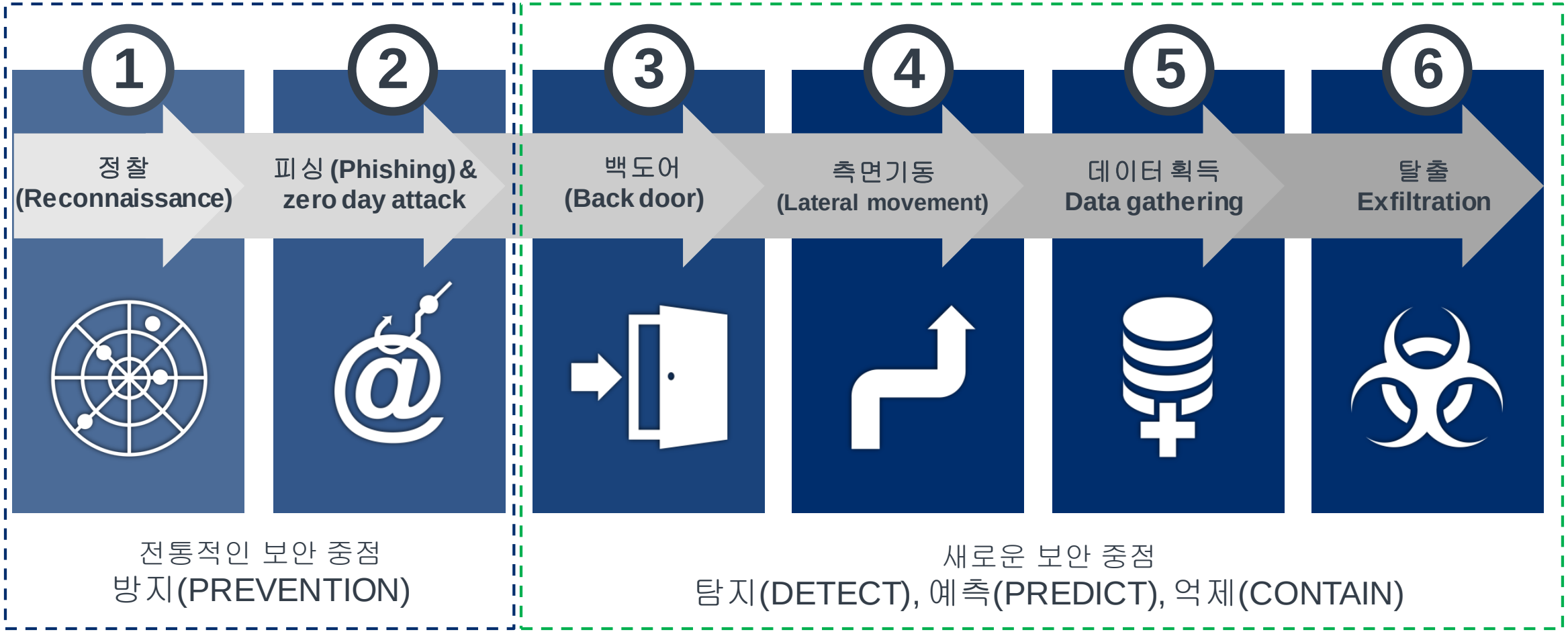


1. 보안전달플랫폼 소개


Security Stack
Agility
Full Visibility
“the single source of truth”
Speed
Network
Physical, Virtual and Cloud Infrastructure

1. 보안전달플랫폼 소개

보안전달 플랫폼 – 목적

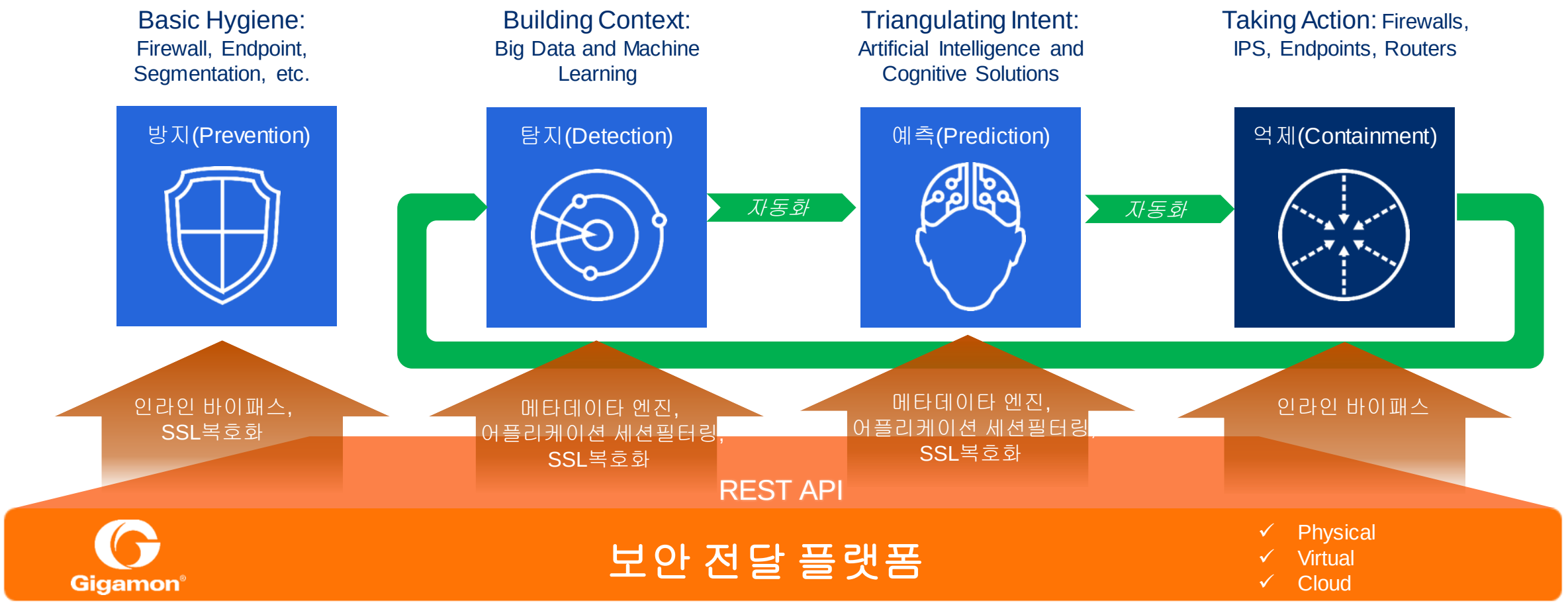


BREAK THE CHAIN, DON'T JUST TRY TO PREVENT IT

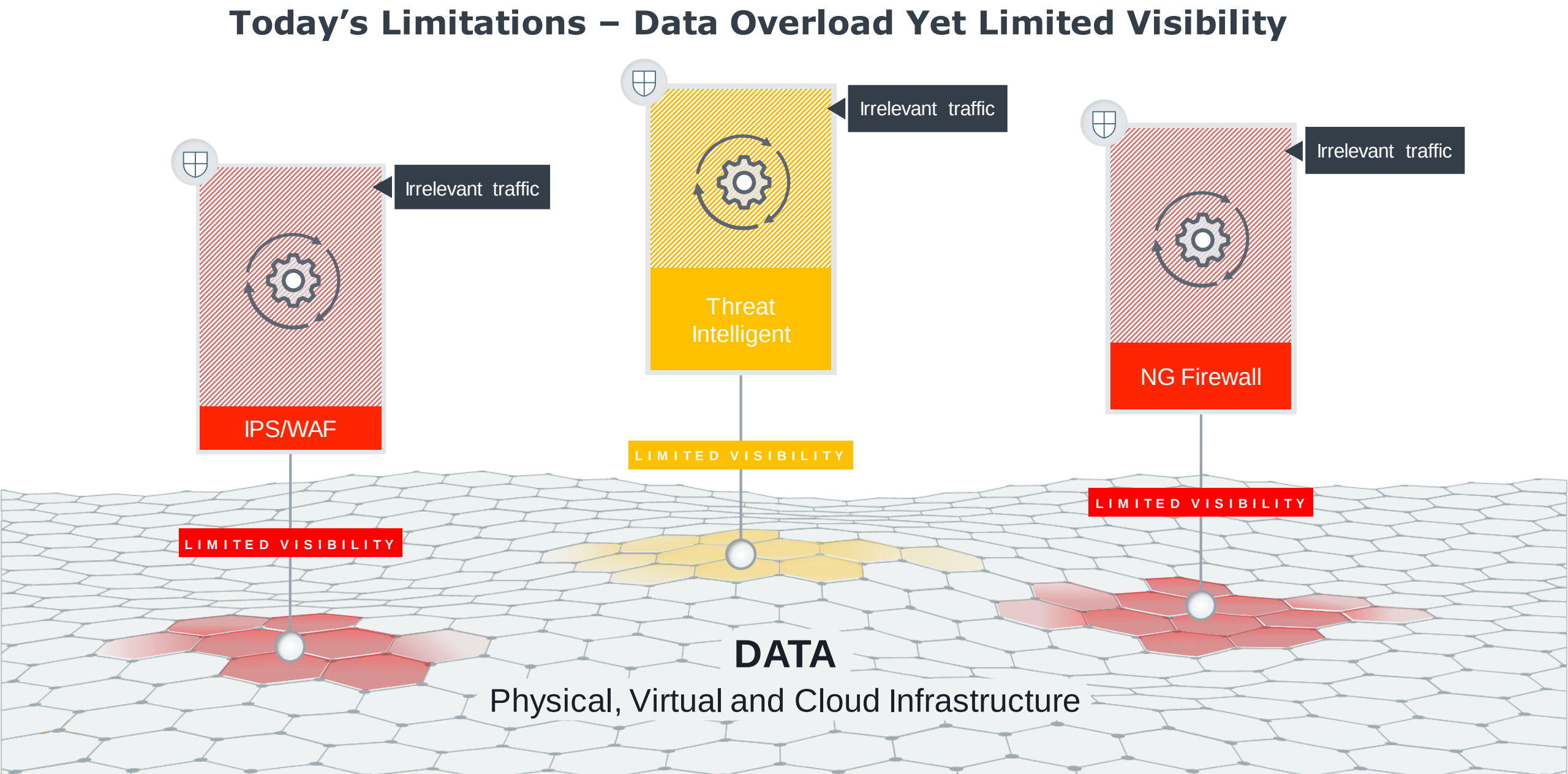
Gigamon

1. 보안전달플랫폼 소개

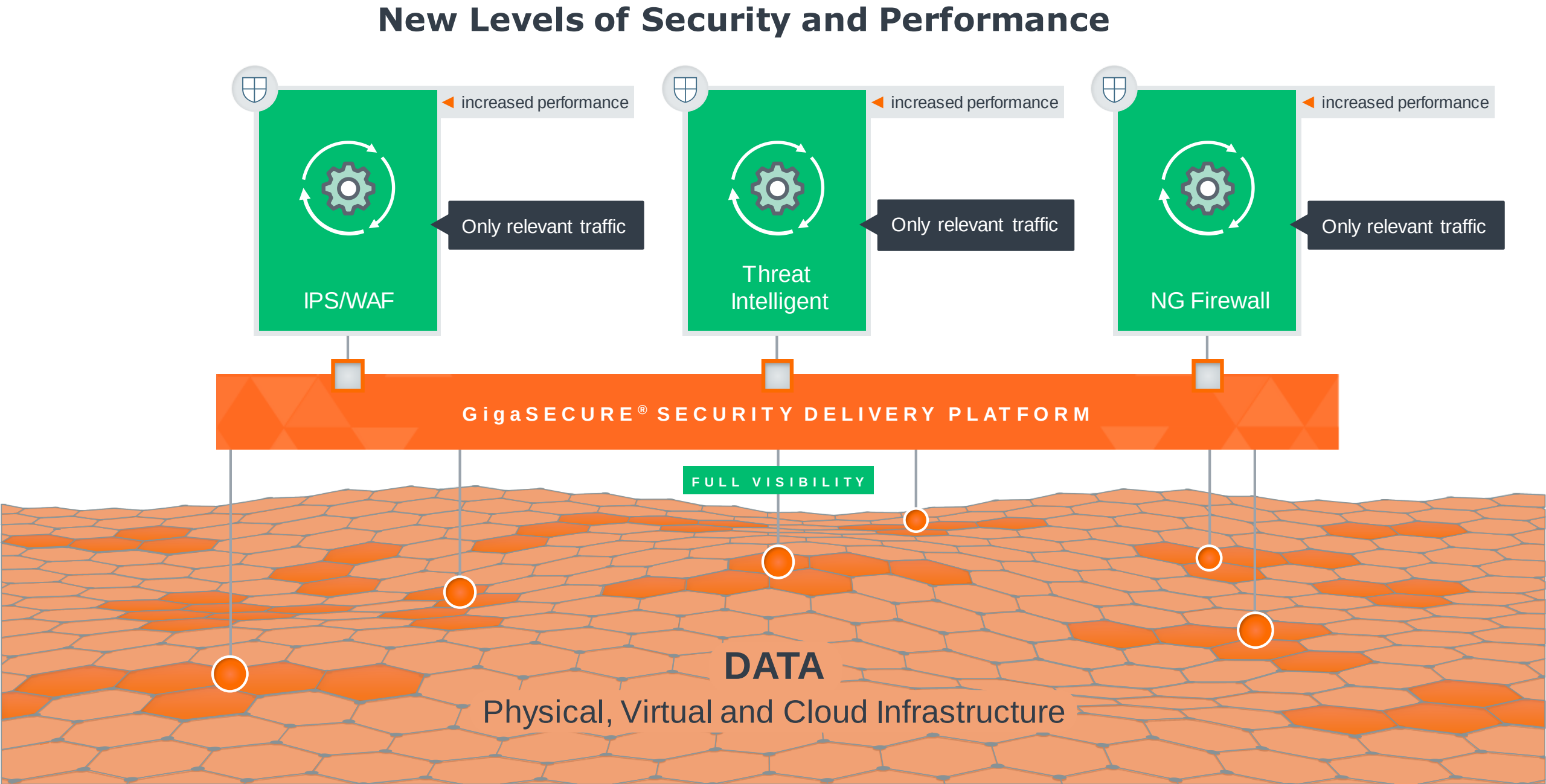
보안전달 플랫폼-구성(TO BE)



1. 보안전달플랫폼 소개


Today's Limitations – Data Overload Yet Limited Visibility
Irrelevant traffic
IPS/WAF
LIMITED VISIBILITY
Irrelevant traffic
Threat Intelligent
LIMITED VISIBILITY
Irrelevant traffic
NG Firewall
LIMITED VISIBILITY
DATA
Physical, Virtual and Cloud Infrastructure

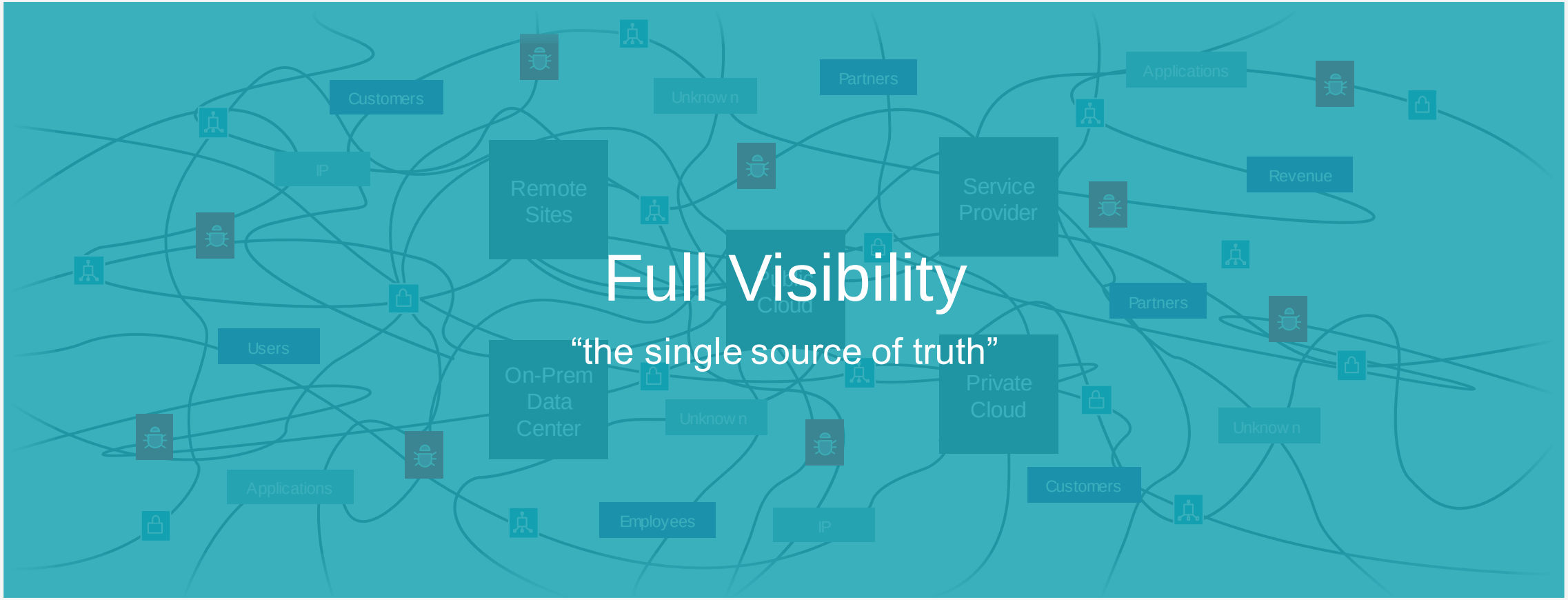
1. 보안전달플랫폼 소개


New Levels of Security and Performance
increased performance
Only relevant traffic
IPS/WAF
increased performance
Only relevant traffic
Threat Intelligent
increased performance
Only relevant traffic
NG Firewall
GigaSECURE® SECURITY DELIVERY PLATFORM
FULL VISIBILITY
DATA
Physical, Virtual and Cloud Infrastructure

1. 보안전달플랫폼 소개

Security Landscape is Always Changing

Network Data Users Threats Tools



2. 핵심기술

2.1 패킷 수집, 분류 및 전달 (Flow Mapping)

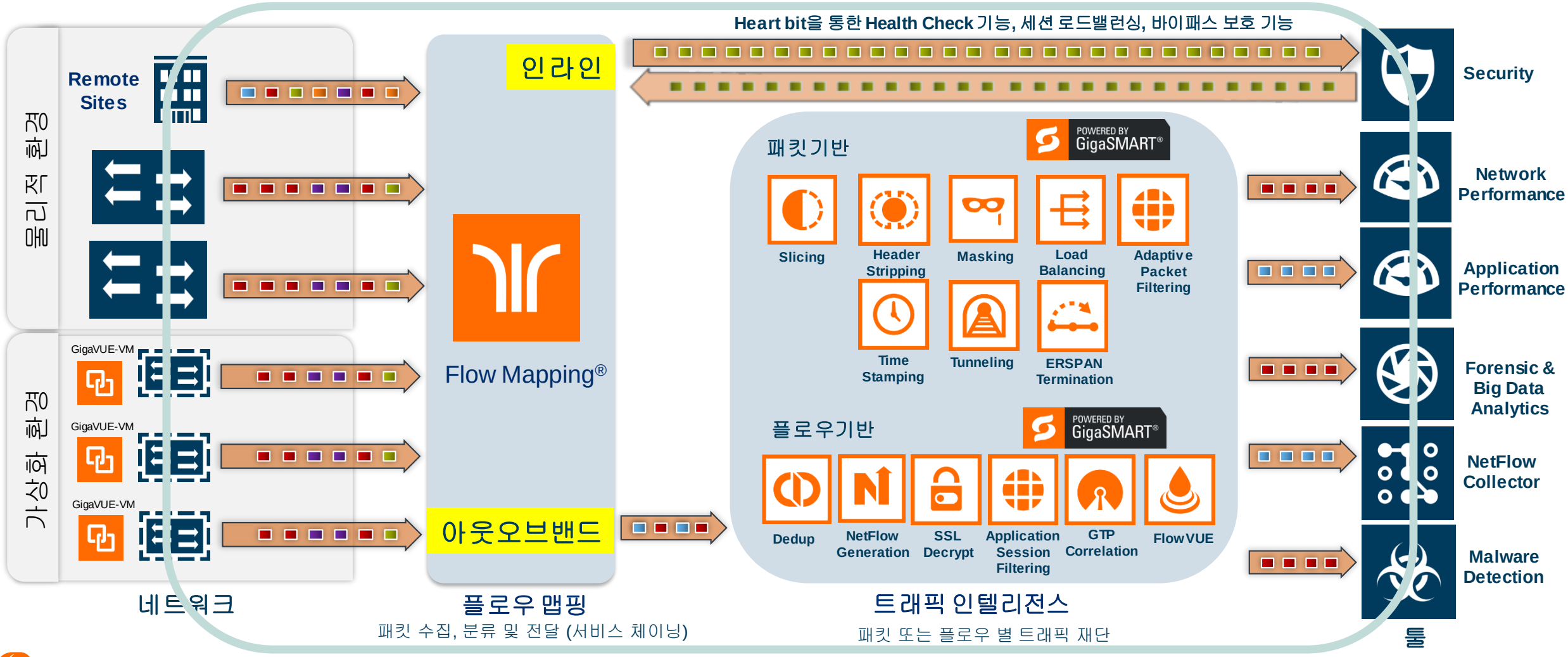
2.2 인라인 보안 툴 안정성 확보 (Heartbeat, Bypass)

2.3 OOB툴 효율성 향상을 위한 패킷재단 (GigaSMART®)

2.4 가상화 환경의 가시성 확보 (SDN, Public & Private)

2. 핵심기술

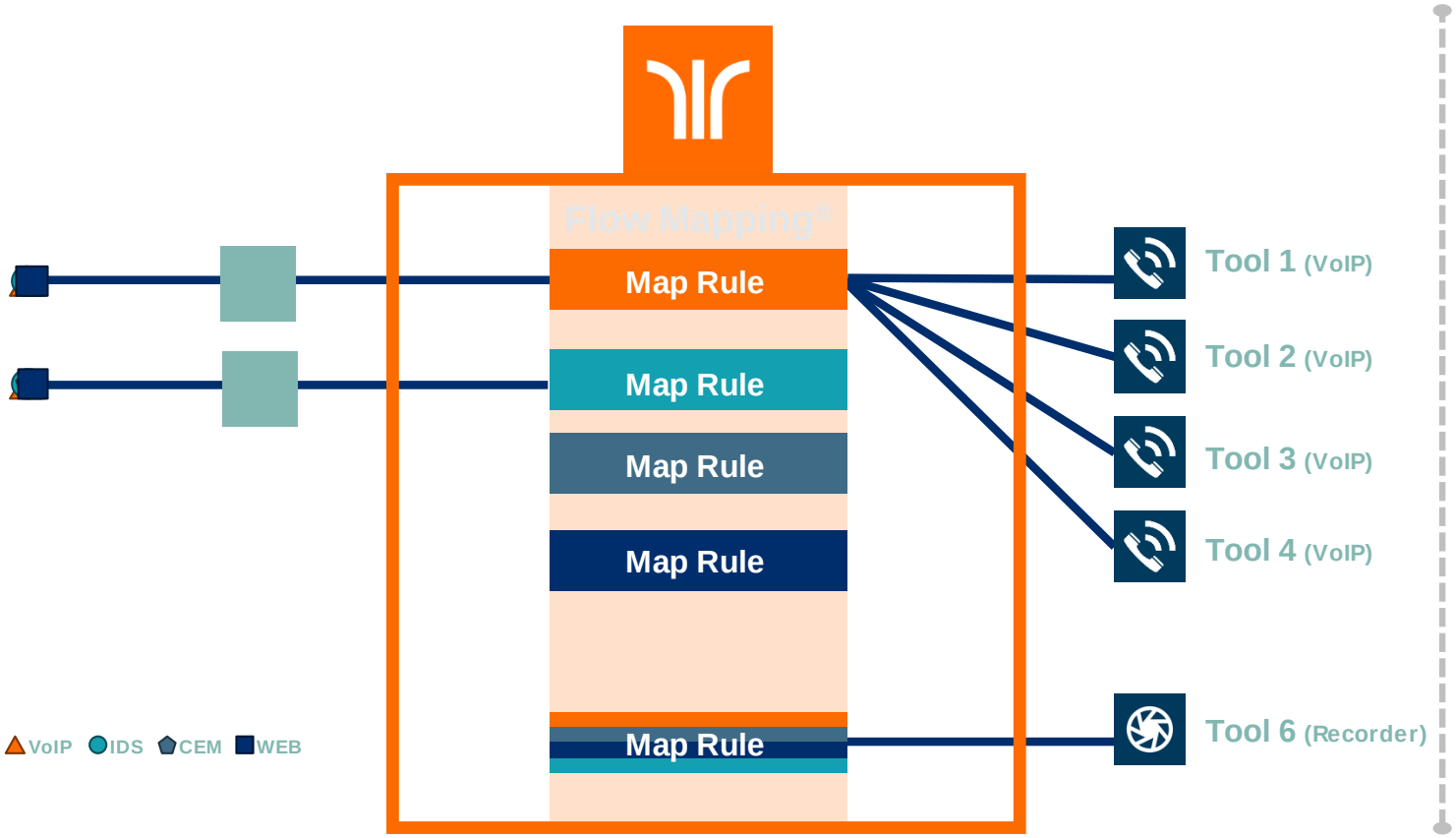
물리적 또는 가상화 네트워크->패킷 수집,분류 및 전달(서비스 체이닝)→필요시,패킷 재단→ 툴

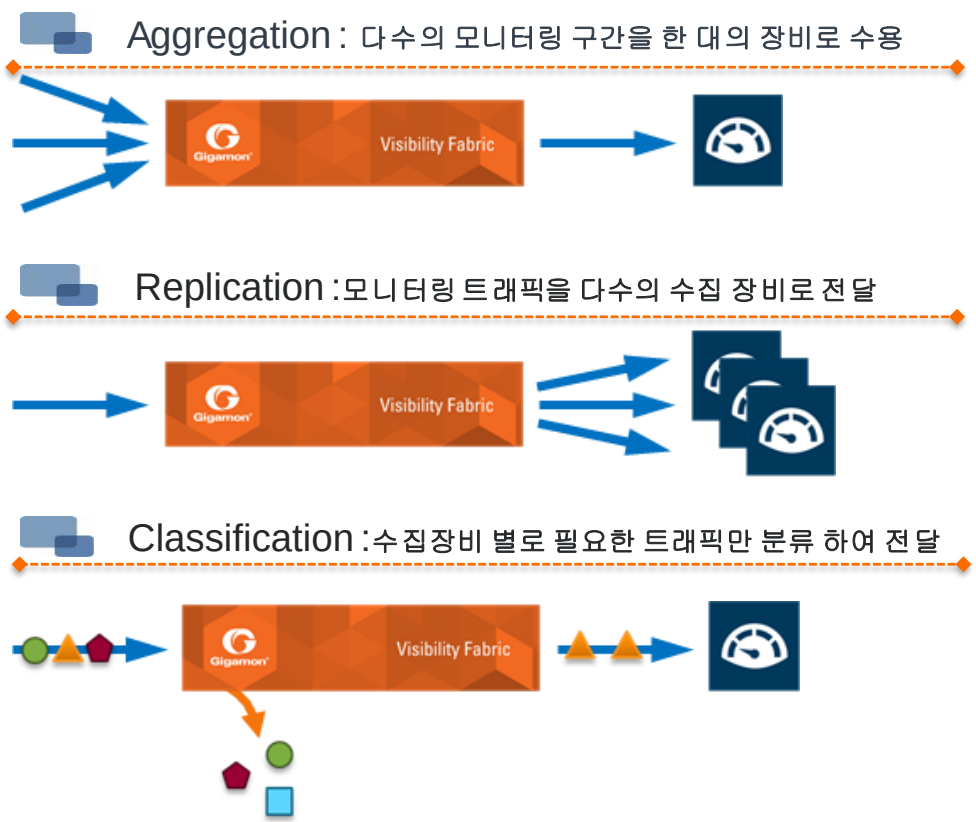


2. 핵심기술

2.1 패킷 수집, 분류 및 전달 (Flow Mapping)

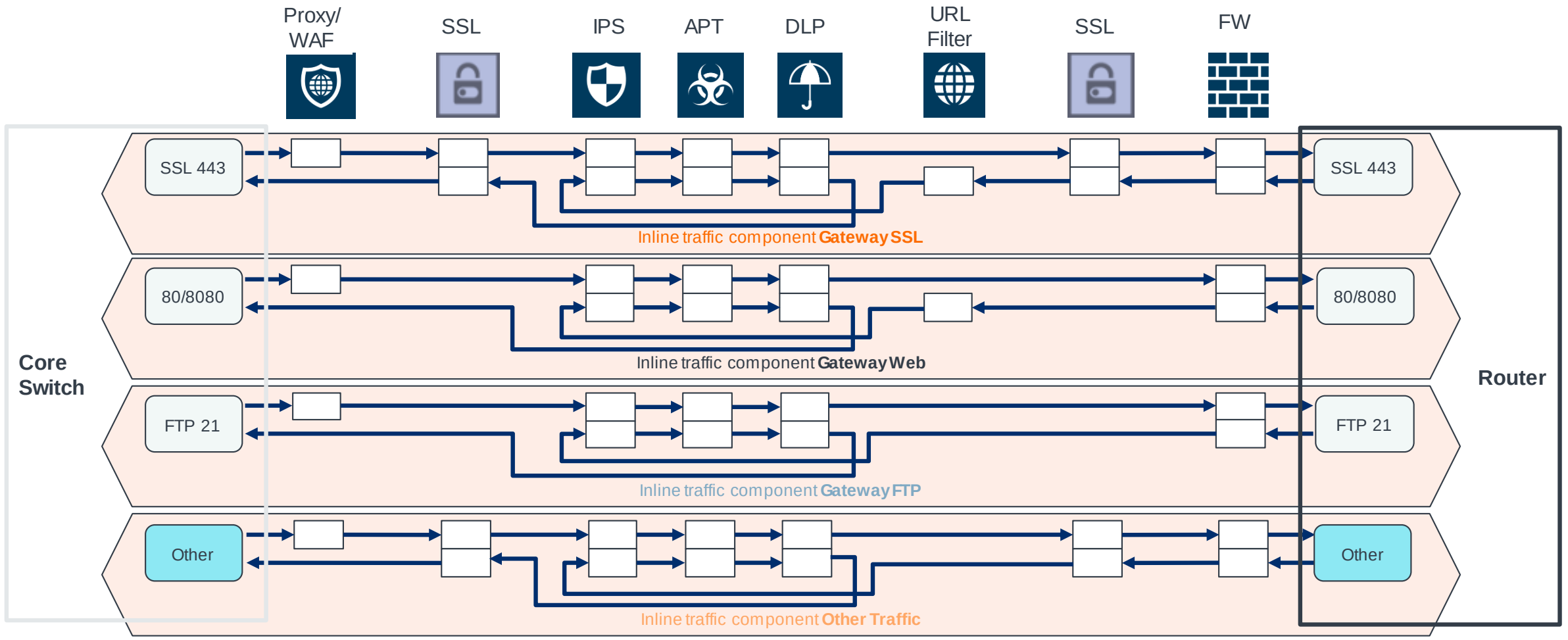
✓ 기가몬의 혁신적인 **"Flow Mapping"** 기능은 IPv4/IPv6, L2, L3 및 L4 레이어,VLAN ID, MAC 주소 등 **30개 이상**의 **사전 정의된 항목**을 통하여 운영자가 **원하는 트래픽**을 다수의 **모니터링 장비**로 **분배** 및 **전달**함으로써 모니터링 장비의 부하가 감소하여 **효율**적인 보안장비/모니터링 **장비 운영**이 가능합니다.





2. 핵심기술

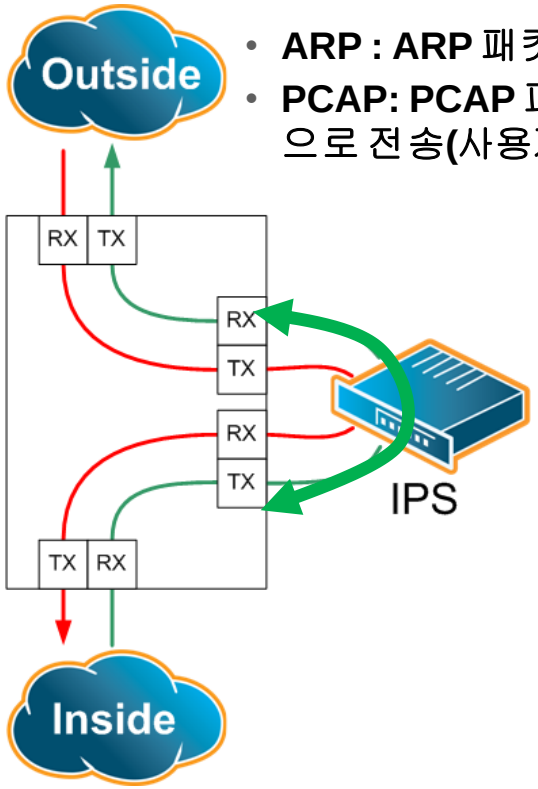
2.1 패킷 수집, 분류 및 전달 (보안 서비스 체이닝)



2. 핵심기술

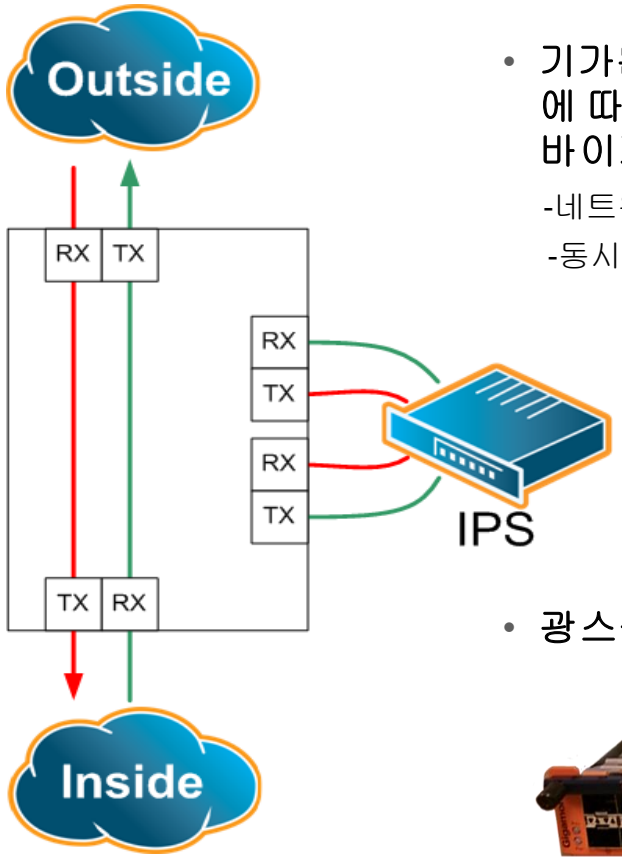
2.2 인라인 보안 툴 안정성 확보 (Heartbeat, 물리적 & 논리적 Bypass)

- **Heartbeat 기능**



- **ARP : ARP 패킷을 양방향으로 전송**
- **PCAP: PCAP 파일에 있는 패킷을 양방향으로 전송(사용자 Customizing 가능)**

- **물리적 바이패스 기능**



- **기가온 장비 장애 발생시, 운용자 사전 정의에 따라 네트워크 상의 트래픽을 자동으로 바이패스**

  -네트워크 중단없이 장비 업그레이드

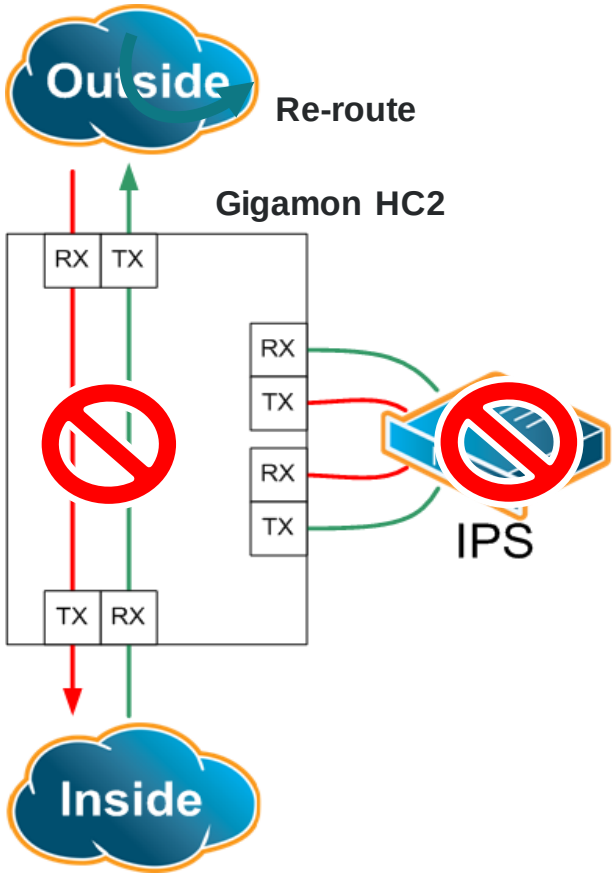
  -동시 다수 보안 툴 PoC 수행

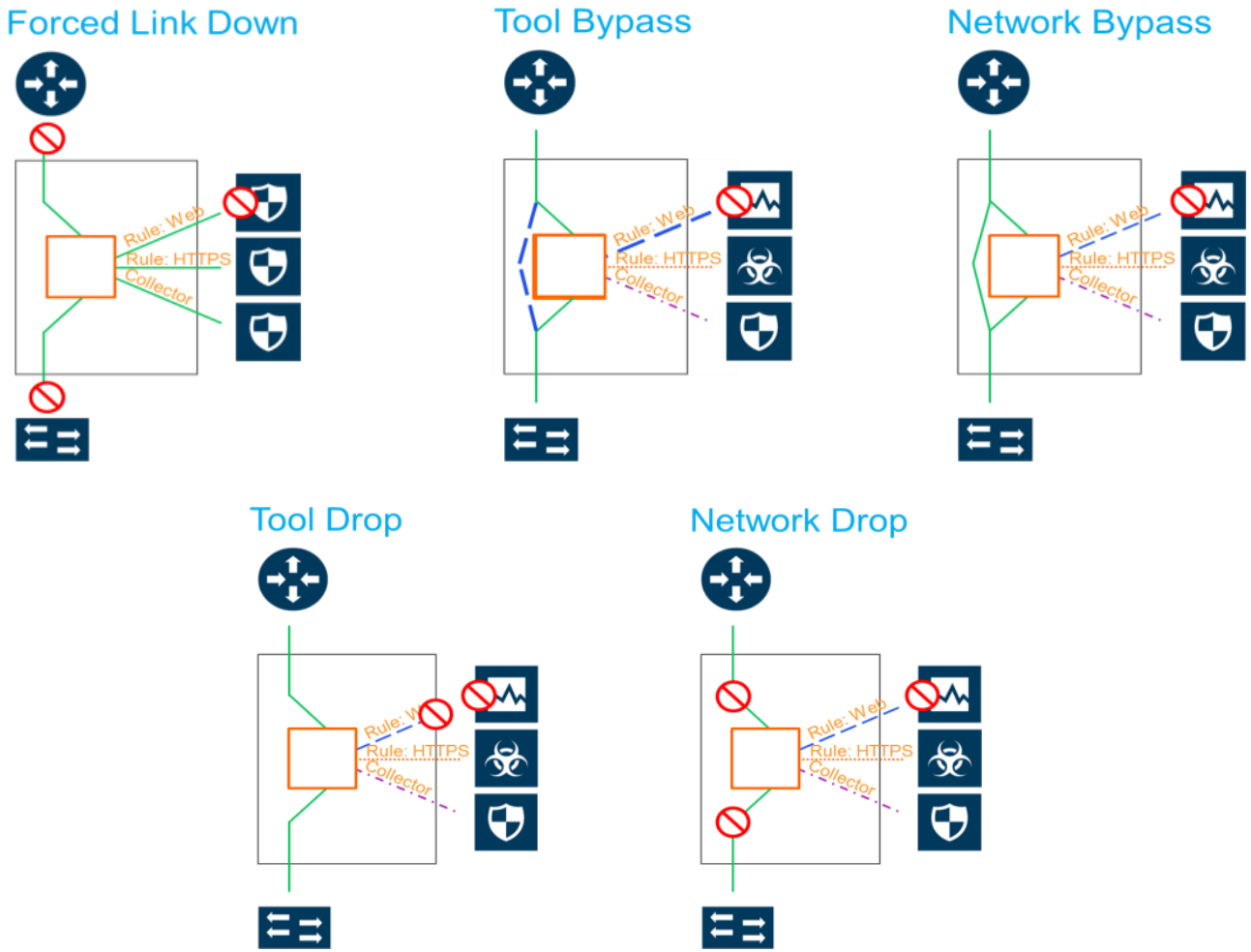
- **광 스플리터(수동소자)**

2. 핵심기술

2.2 인라인 보안 툴 안정성 확보 (Heartbeat, 물리적 & 논리적 Bypass)

- 논리적 바이패스 기능

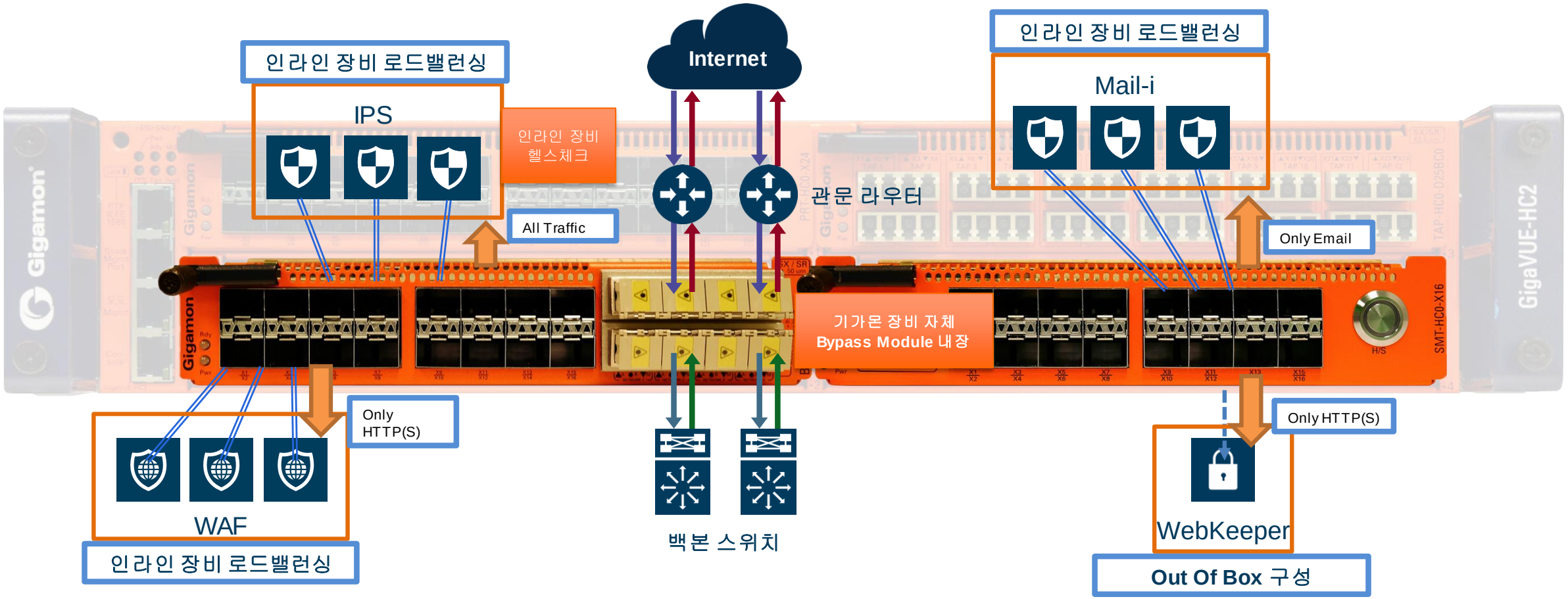




2. 핵심기술

2.2 인라인 보안 툴 안정성 확보

- 인라인 장비 상태 지속 체크 (Heart Beat), 최적화된 트래픽 전달
- 보안전달 플랫폼 내 연결된 장비 간 트래픽 세션 별 로드밸런싱 처리
- 운용자가 설정한 보안장비 통과 순으로 서비스 체이닝
- 동시에, 아웃오브밴드 툴로 트래픽 복사 전달(L7 로드밸런싱 가능)



2. 핵심기술

2.3 OOB보안장비의 효율성 확보 (GigaSMART® – Traffic Intelligence)

- 트래픽 재단 기능

기가스마트 기능

POWERED BY GigaSMART®

(영구라이선스 기반)

Packet Slicing
- 패킷 분할을 통한 패킷 사이즈 최적화

Masking
- 패킷 내부 개인 정보 마스킹

NetFlow & Metadata Generation
- 수집된 패킷에 대한 100% **NetFlow** 및 메타데이타 생성

SSL/TLS Decryption
- 암호화된 **SSL/TLS** 트래픽을 **복호화 (Inline or OOB)**

De-duplication
- 다중구간에서 수집된 **중복 패킷 제거**

Adaptive Packet Filtering
- L7 기반의 패턴 기반 트래픽 필터링**(패킷 단위)**

Application Session Filtering
- L7 기반의 패턴 기반 트래픽 필터링**(세션 단위)**

Tunneling/ ERSPAN Termination
- 본사/지사 간 암호화된 트래픽 전달 (L2GRE)

Header Stripping
- VLAN, VxLAN, MPLS와 같은 헤더 제거

Source Port Labeling
- 개별 패킷에 인입 포트라벨을 추가

GTP Correlation
- 통신사 가입자 기반 트래픽 필터링

FlowVUE™
- IP, User, 세션 기반 Flow –aware 트래픽 샘플링

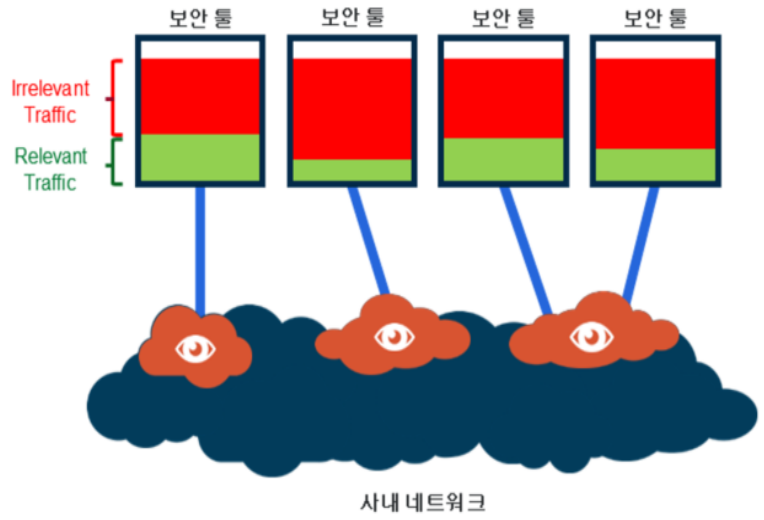
*참고 : 트래픽 인텔리전스 기능이 개발 중으로 지속적으로 추가 될 예정

Gigamon

2. 핵심기술

2.3 OOB보안장비의 효율성 확보 (GigaSMART® – Traffic Intelligence)

도입 전



불필요 트래픽 처리를 위해 보안장비 리소스 낭비
(CPU, 메모리 등)

도입 후

보안 툴이 처리 가능한 트래픽 내용과 양을
전달하여, 모니터링 구간 확대

2. 핵심기술

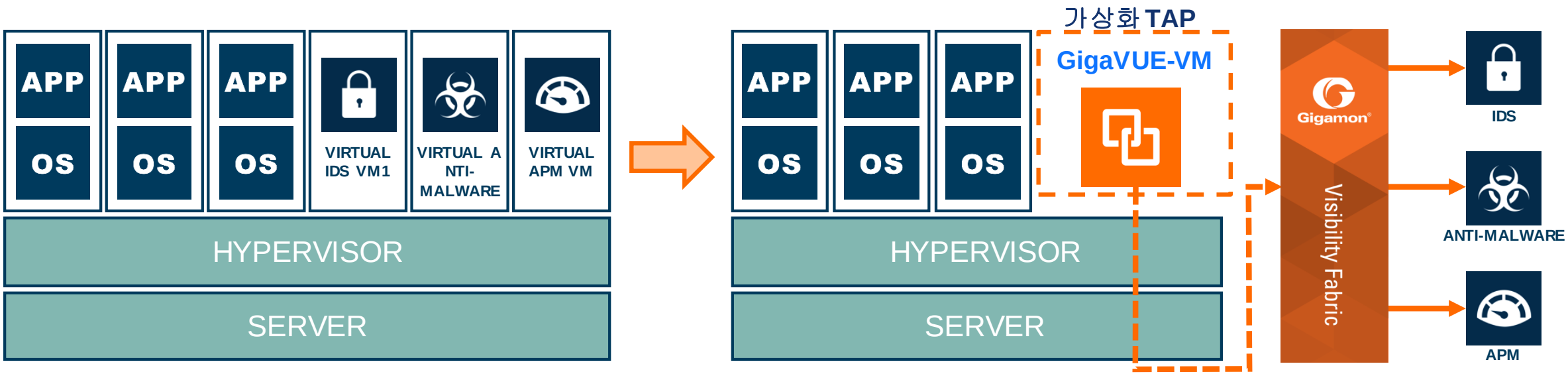
2.4 가상화 환경의 가시성

VIRTUAL VISIBILITY: MORE IMPORTANT THAN EVER

5 REASONS WHY YOU SHOULD CARE

1. 자원 효율화를 위한 가상화 자원에 중요 업무 위치증가
2. CAPEX 및 OPEX 향상을 위해 VM Density 증가가 필요.
3. VM-VM 간 트래픽에 대한 보안성 확보를 위해 보안 VM 도입이 증가 됨.
4. 보안 VM, 가상 툴 인스턴스를 생성하면 컴퓨팅 자원이 소모됨
5. 업무VM 마이그레이션 경우, 자동화된 가시성 확보 필요

- SDN환경의 가시성 확보 > VMware NSX, Cisco ACI
- Private 클라우드 : VMware ESX, OpenStack
- Public 클라우드 : Amazon Web Services (AWS), Microsoft Azure



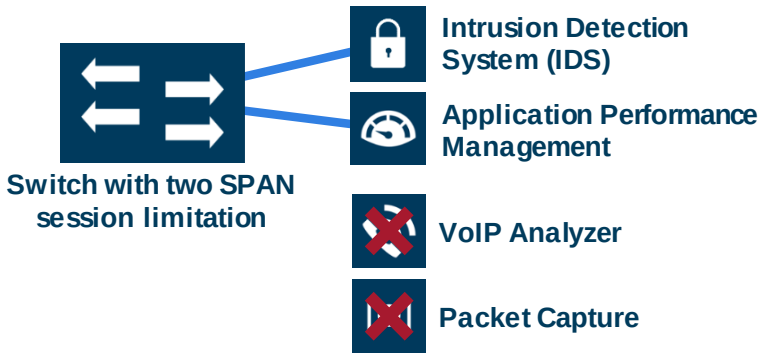
3.활용방안

3. 활용방안

3.1 네트워크 트래픽 수집제약 해소

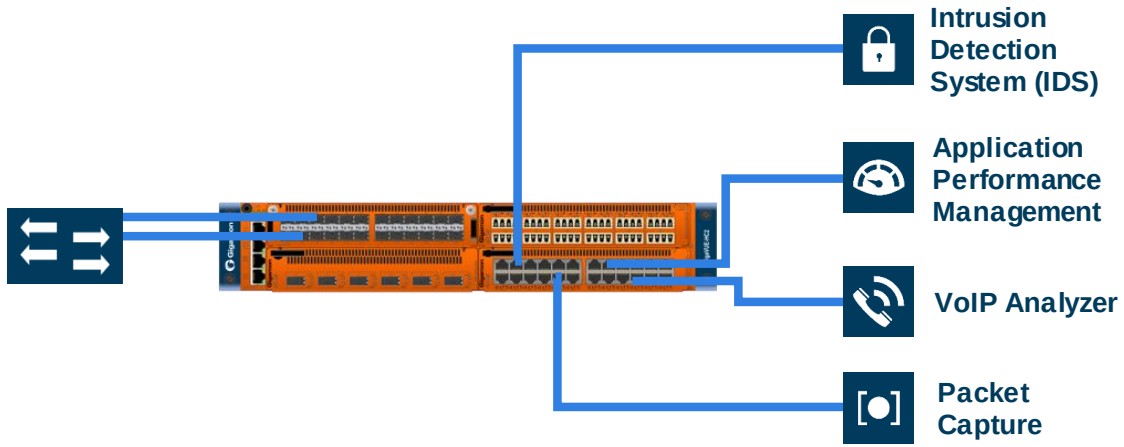
- 모니터링 구간 통합 및 트래픽 필터링

도입 전



고객이 모든 도구를 사용할 수 없습니다

도입 후



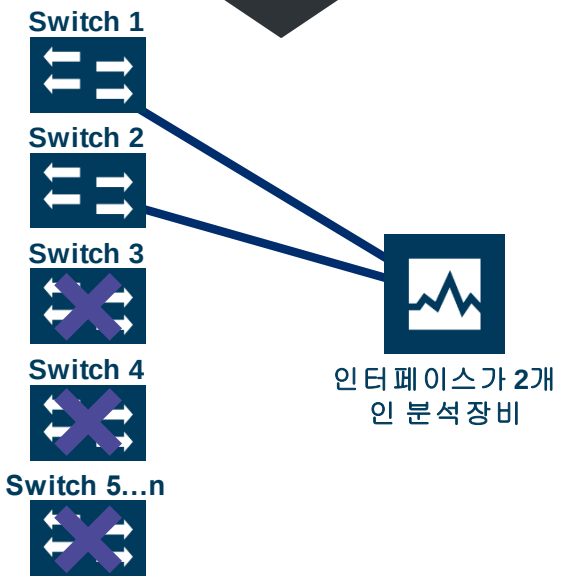
고객은 모든 도구를 완벽하게 파악할 수 있습니다

3. 활용방안

3.2 보안 분석 장비 가시범위 향상

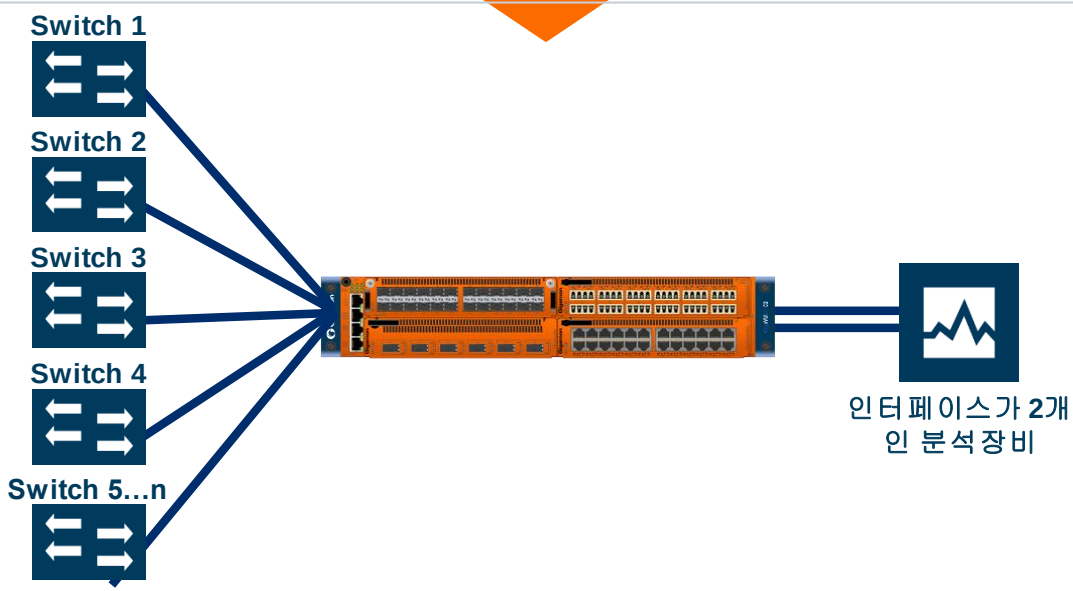
- 모니터링 구간 확대 및 트래픽 필터링을 통한 효율성 향상

도입 전



- 보안 및 분석 장비의 인터페이스 제약으로 제한적 구간의 트래픽 모니터링

기가몬 도입 후



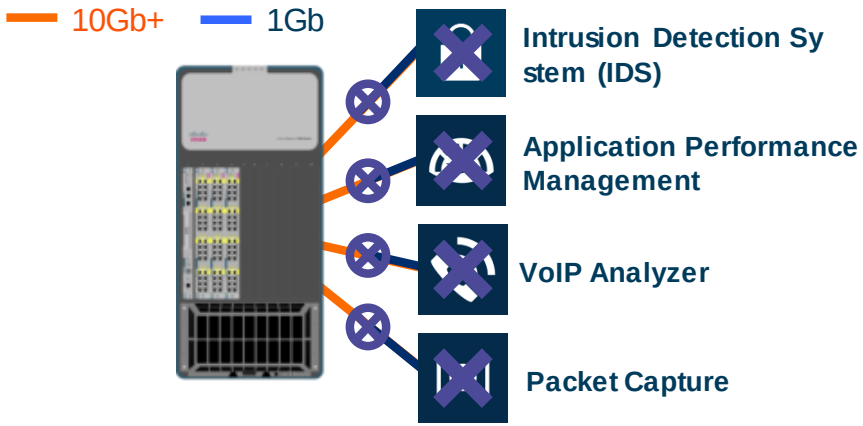
- 경제성 및 전 구간 가시성 확보

3. 활용방안

3.3 보안장비 라이프사이클 연장

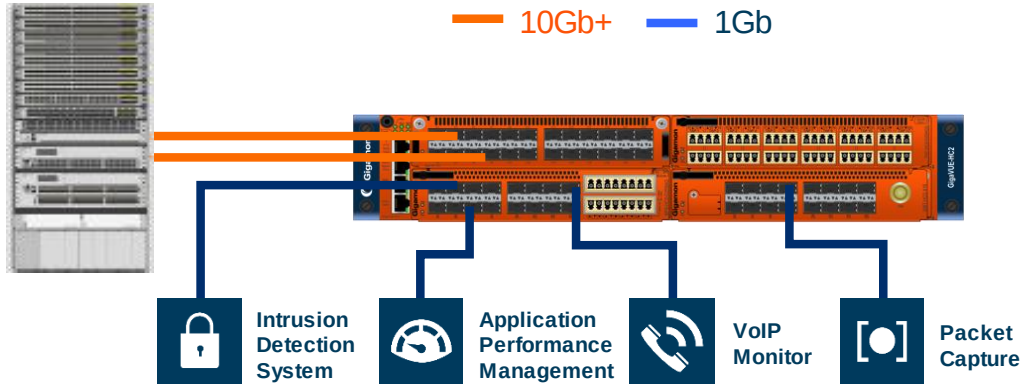
- 네트워크과 보안장비 속도 불 일치에 따른 보안장비 사용연장

도입 전



- 네트워크 업그레이드에 따라 기존 보안 및 분석 솔루션 업그레이드 필요

기가몬 도입 후



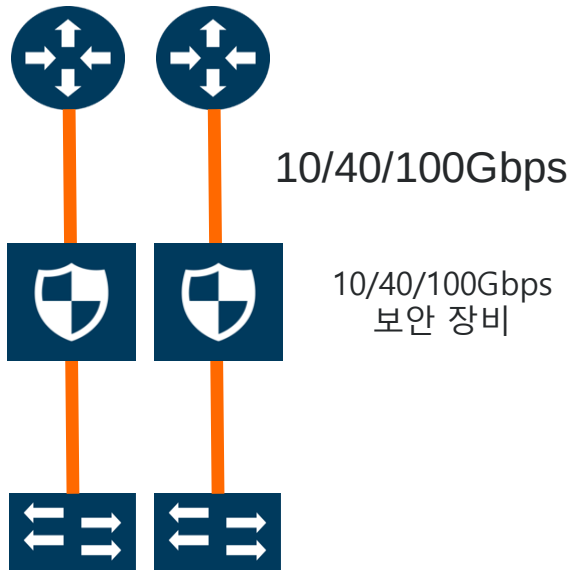
- 보안 및 분석 솔루션의 라이프사이클 연장 및 투자 규모 시기의 탄력적 계획 가능

3. 활용방안

3.4 보안장비 CAPEX/OPEX 절감

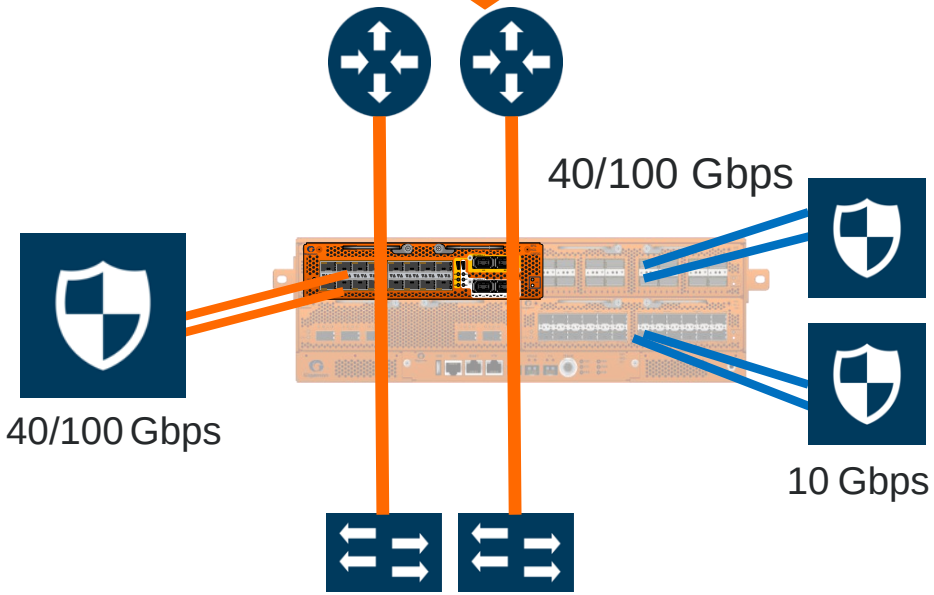
- 네트워크 마이그레이션에 따른 보안장비 신규 도입

도입 전



- 네트워크 회선 당 인라인 보안 및 분석 솔루션 구매

기가몬 도입 후



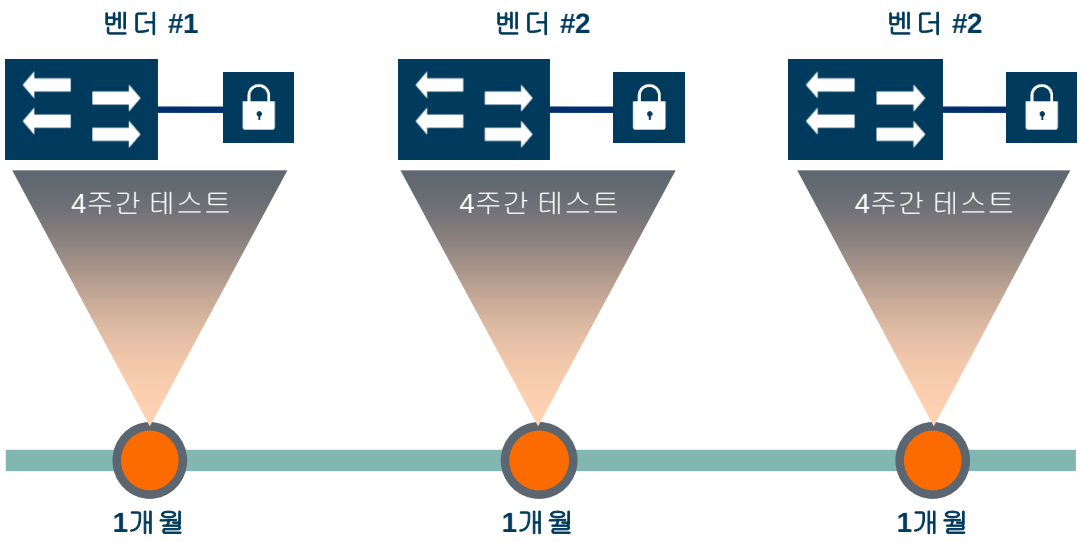
- 보안 및 분석 솔루션 도입 시 CAPEX, OPEX 절감 가능

3. 활용방안

3.5 인라인 장비의 효율적인 선택 및 운용

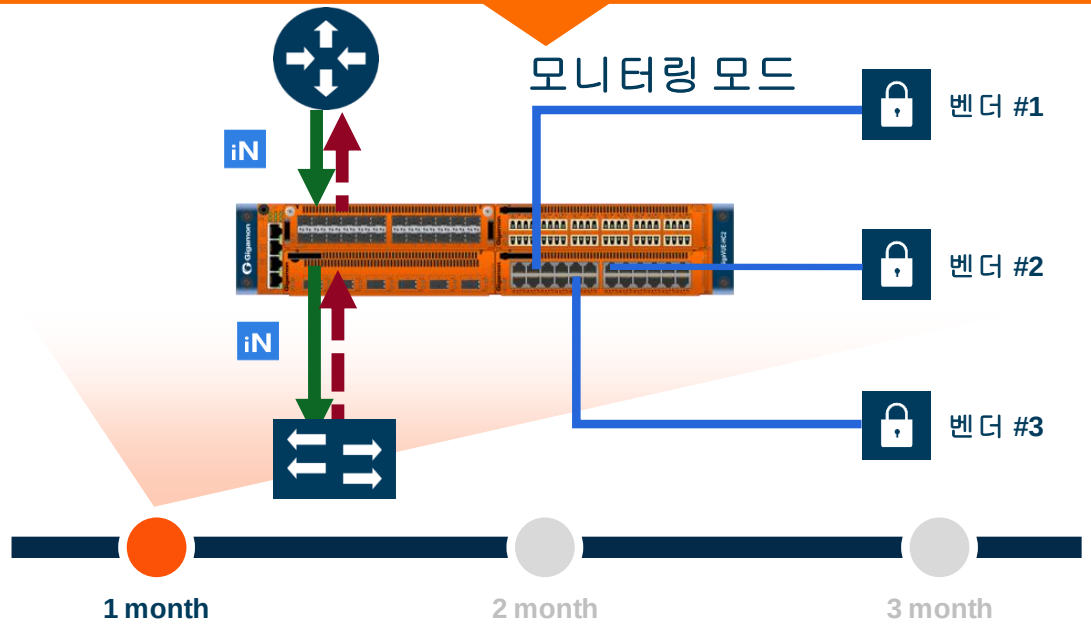
- 실망 영향 없는 인라인 장비 PoC(Proof Of Concept) 및 유지보수

도입 전



- 다른 시간대, 다른 트래픽을 대상으로 PoC 실시로 테스트 장비 비교 분석 어려움

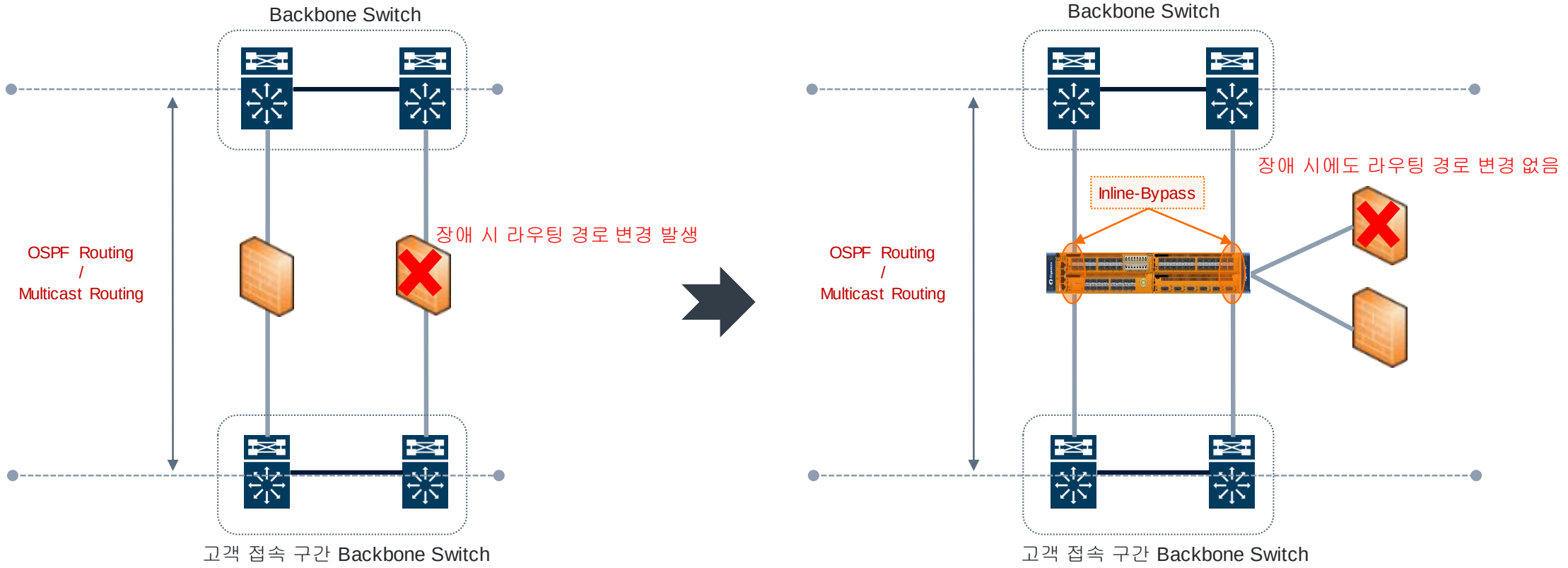
기가몬 도입 후



- 실 네트워크 영향 없이 동일 조건 PoC 수행
- 장비유지보수 시 모니터링 모드로 안정화기간 확보가능

3. 활용방안

3.6 안정적 인라인 보안장비 구성 및 운용



보안장비 장애 시 불필요한 라우팅 경로 변경 발생

- 장비 장애 발생 시 불필요한 라우팅 경로 변경에 따른 서비스 안정 저하
- 장비 내 트래픽 홀딩 시 트래픽 처리 불가에 따른 트래픽 손실 발생
- 보안 장비에 따라, Active-Standby 운용

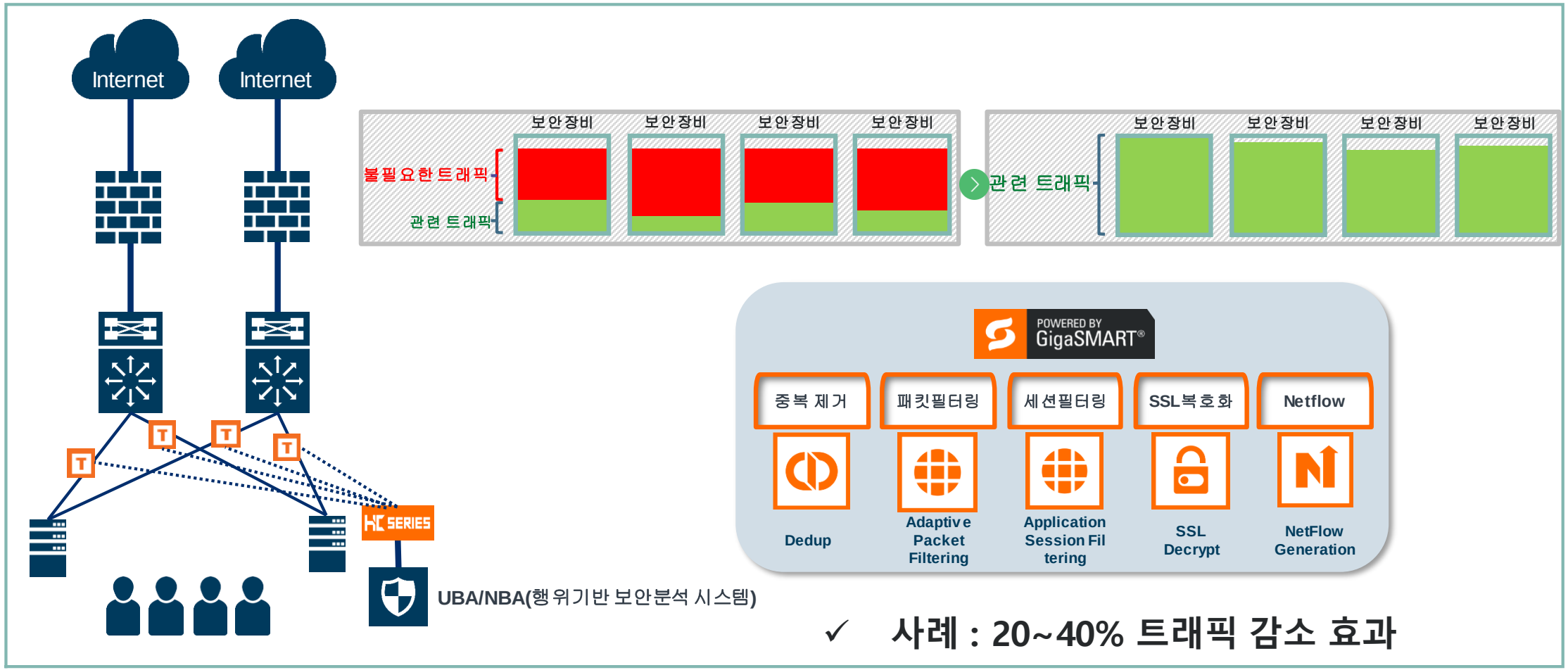
보안장비 장애 시에도 라우팅 경로 변경 없음

- 보안장비 장애 발생 시 기가온 장비에서 트래픽 바이패스를 통한 정상 처리
- 기존 운영 네트워크망에서 불필요한 라우팅 경로 발생이 없음
- 구성 변경없이 Active-Active 운용

3. 활용방안

3.7 UBA/NBA(사용자 행위분석) 시스템 협업

- 내부 사용자 구간의 중복 트래픽 및 불필요 트래픽 필터링을 통한 효율적인 시스템 활용

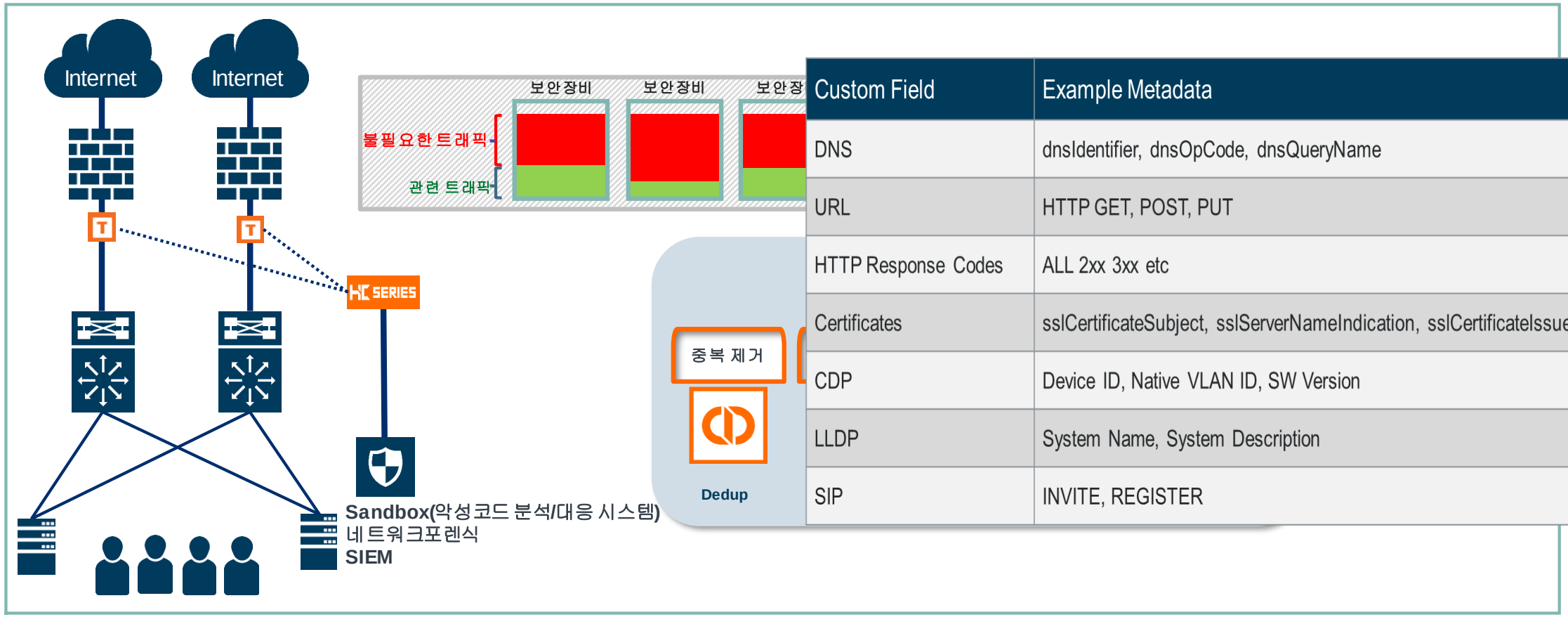


✓ **사례 : 20~40% 트래픽 감소 효과**

3. 활용방안

3.8 Network Forensic, APT, SIEM 솔루션과의 연동

- 불필요한 트래픽 필터링을 통한 연동보안제품의 리소스 활용증대 및 대응역량 향상, 차세대 SIEM 구축을 위한 전수 NetFlow 전달/메타데이타 활용

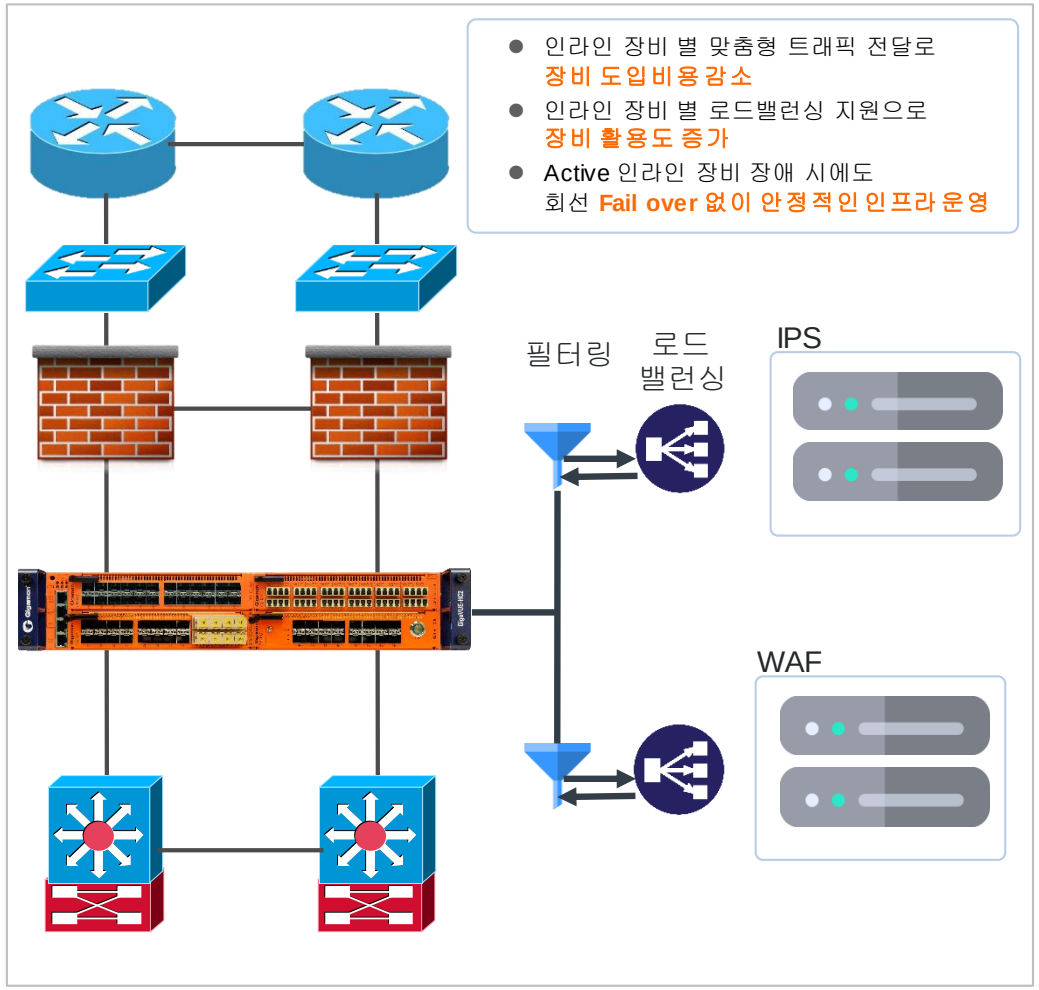


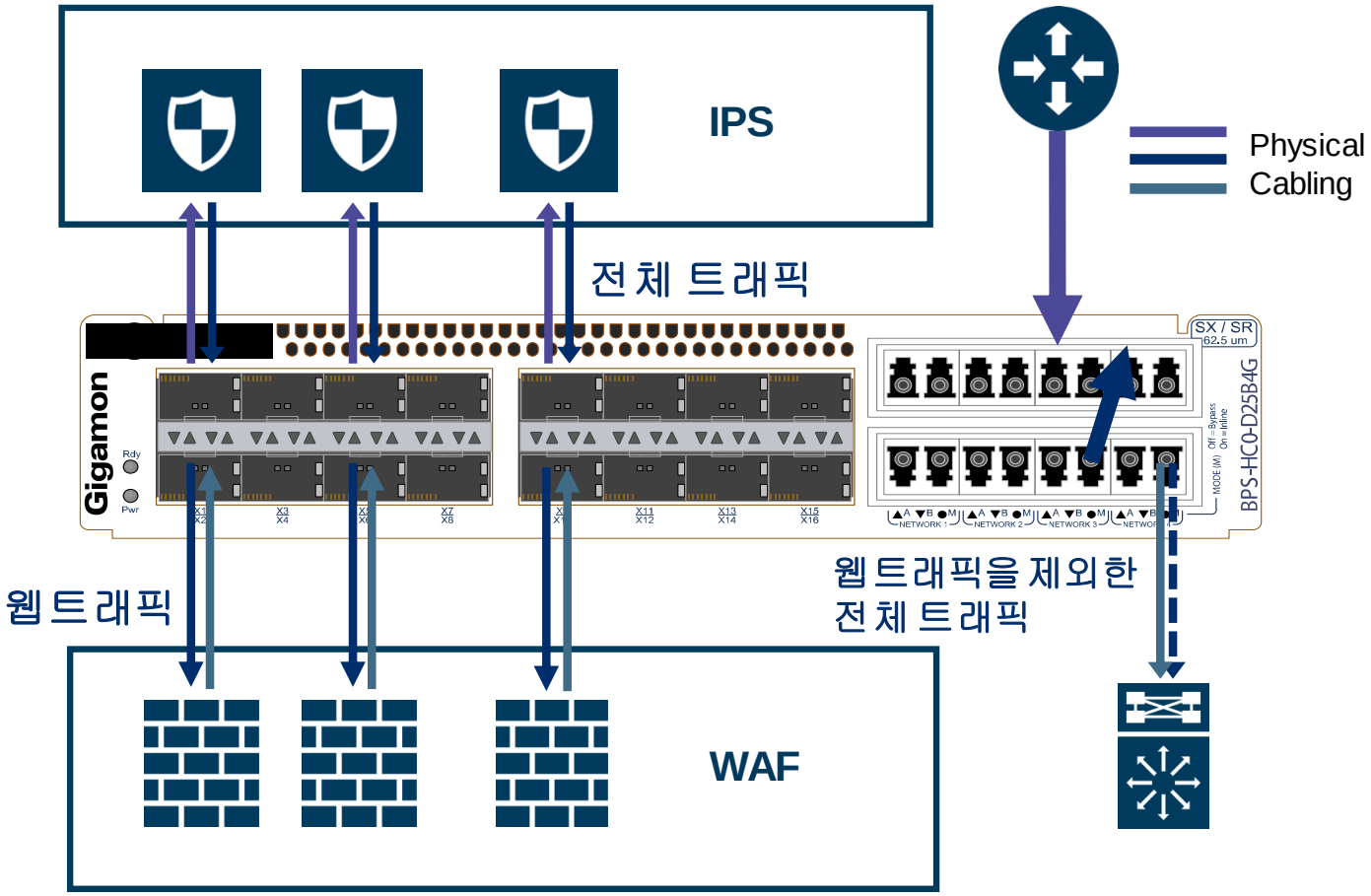
Custom Field	Example Metadata
DNS	dnsIdentifier, dnsOpCode, dnsQueryName
URL	HTTP GET, POST, PUT
HTTP Response Codes	ALL 2xx 3xx etc
Certificates	sslCertificateSubject, sslServerNameIndication, sslCertificateIssue
CDP	Device ID, Native VLAN ID, SW Version
LLDP	System Name, System Description
SIP	INVITE, REGISTER

3. 활용방안

3.9 웹방화벽 효율성 극대화

- WAF 효율적인 운영을 통한 CAPEX(투자비용) 최소화

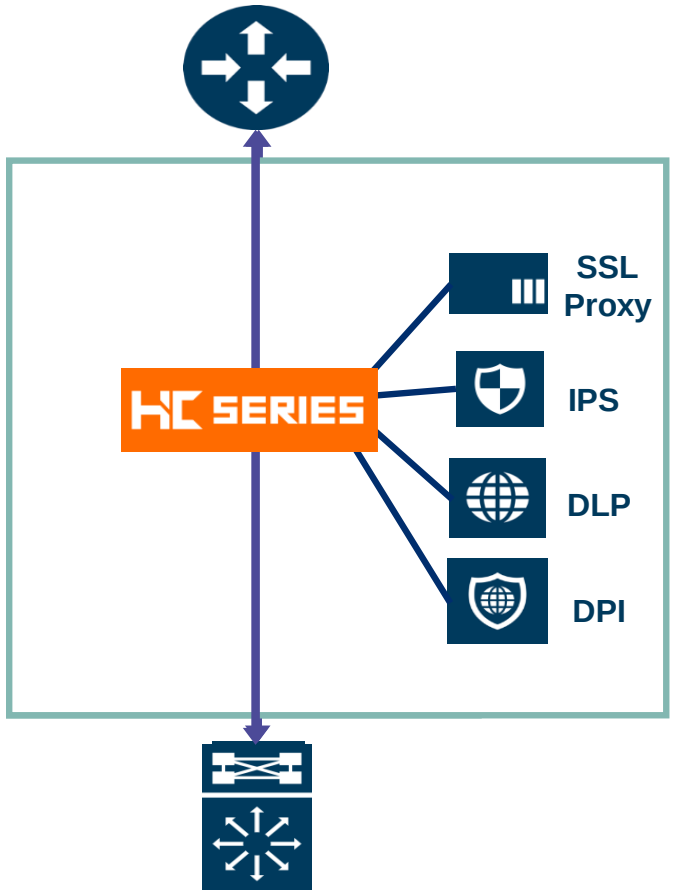


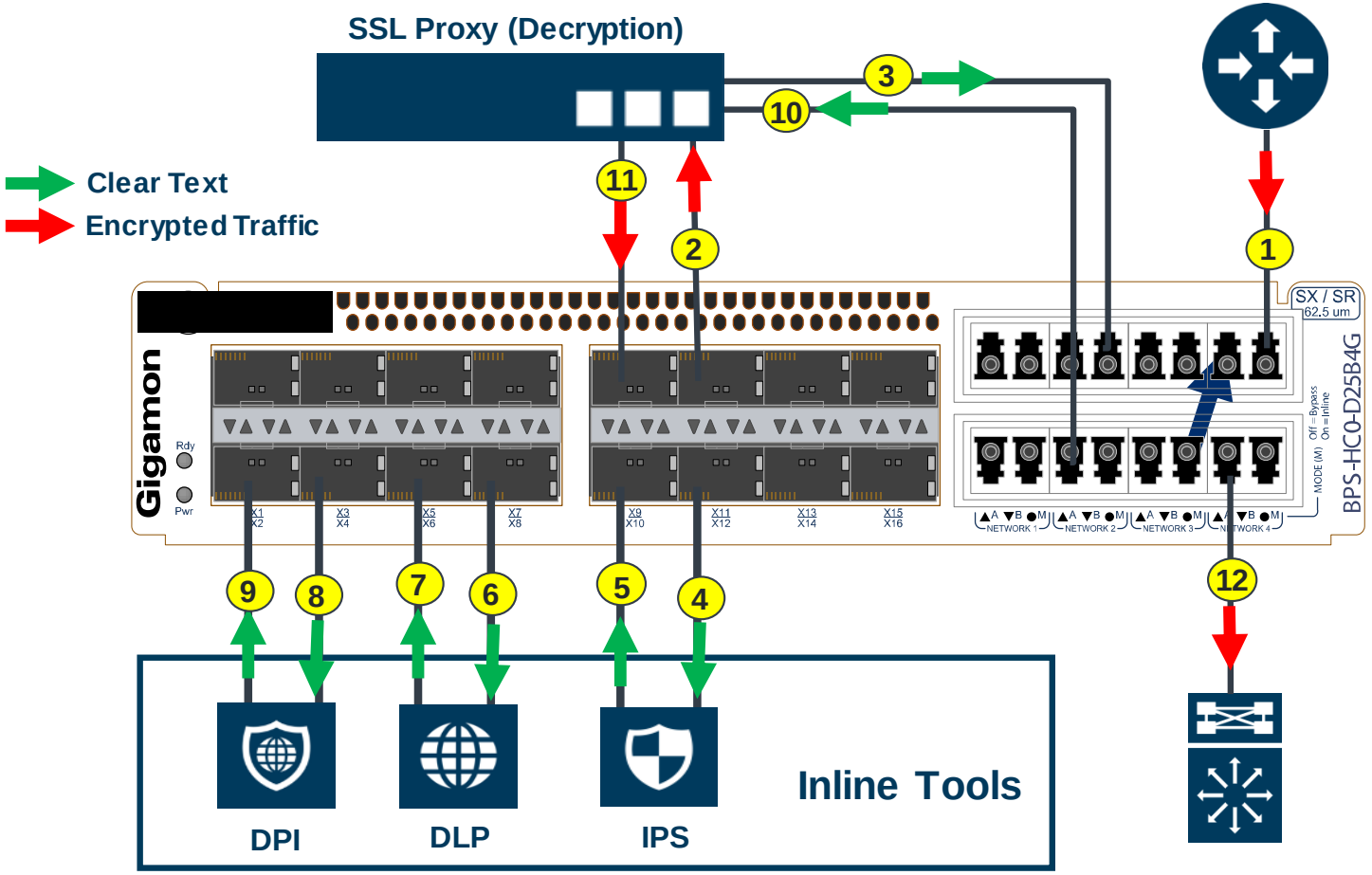


3. 활용방안

3.10 SSL복호화 솔루션 구성 시, 안정성 및 효율 성 극대화

- 외장형 SSL Decryption 솔루션 :인라인 바이패스 보호, HA & 로드밸런싱 기능 제공
- 통합 SSL Decryption 솔루션 (Security Delivery Platform + SSL Proxy), URL filtering 기능 번들

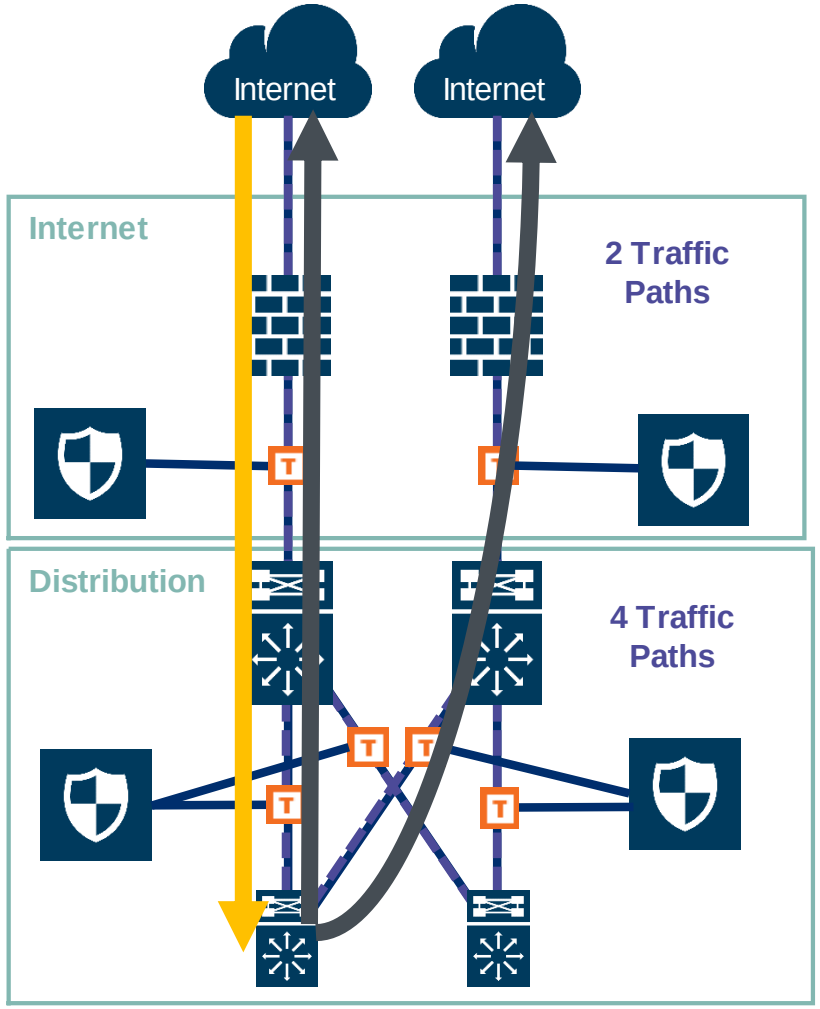


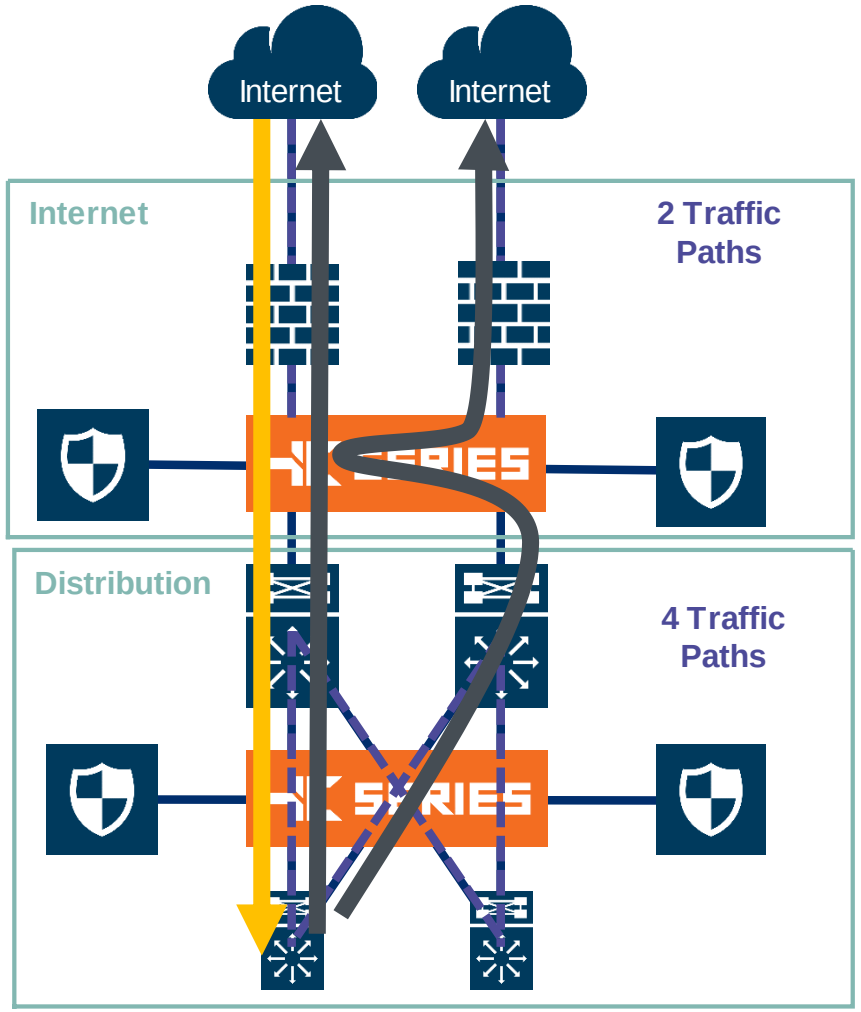


3. 활용방안

3.11 보안장비 구축 시 세션 제약 없는 유연한 FLB 구성

- Asymmetric 구성환경의 이중화(Active-Active) 지원 – 인라인/미러링 보안제품 연동

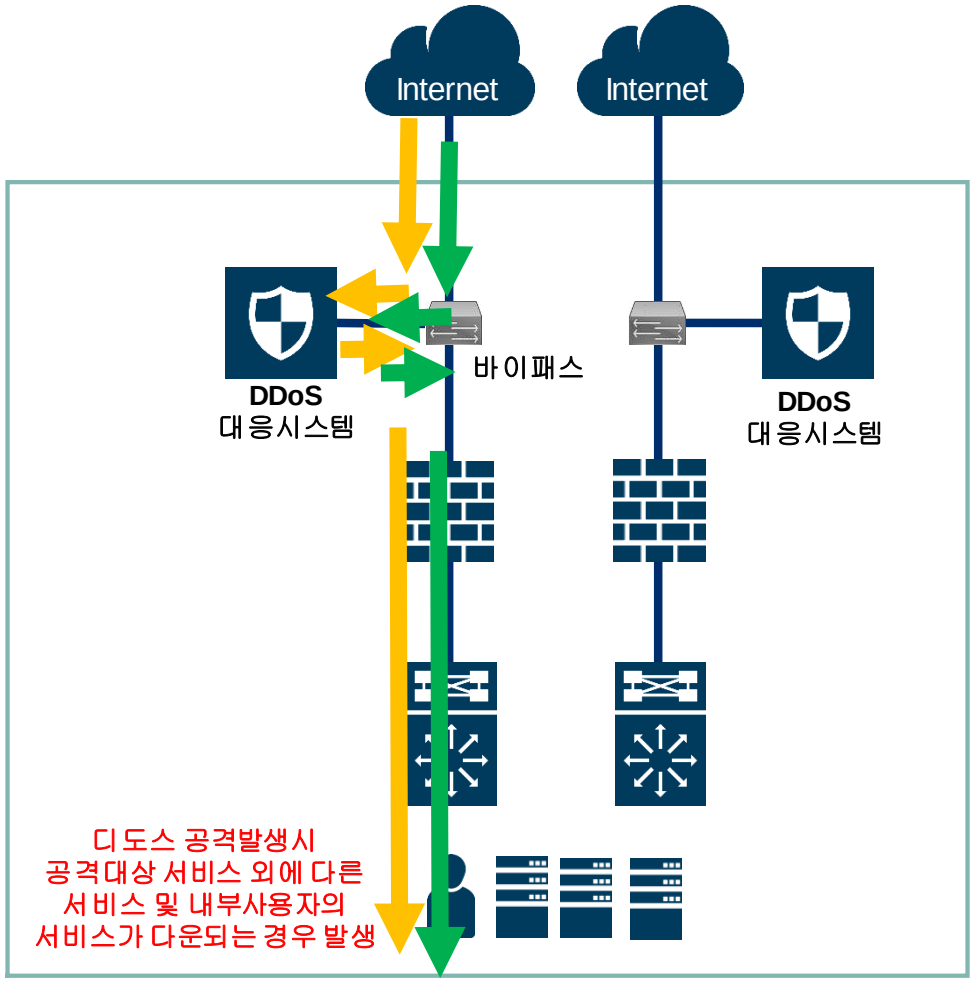


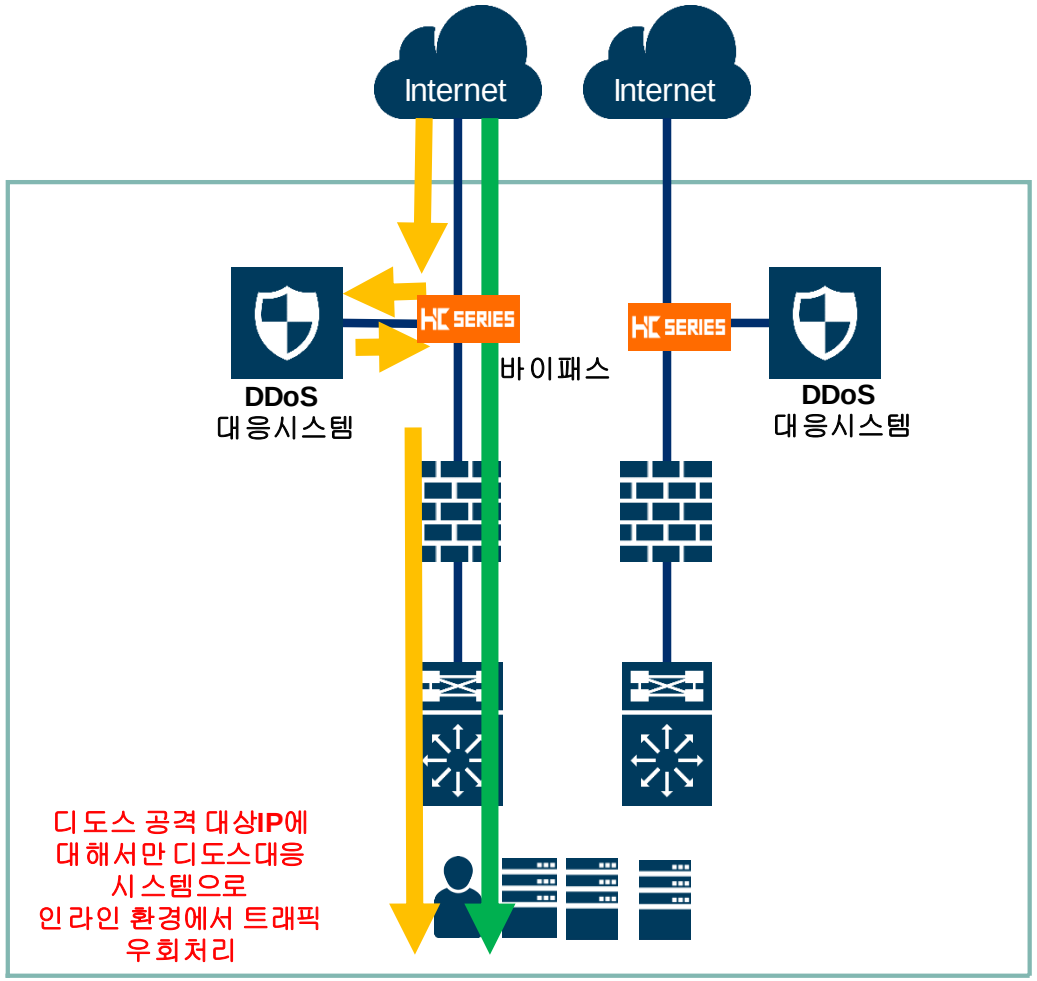


3. 활용방안

3.12 효과적인 DDoS 장비 연동

- DDoS 공격 발생시, 트래픽 우회를 통한 서비스 생존 성 보장



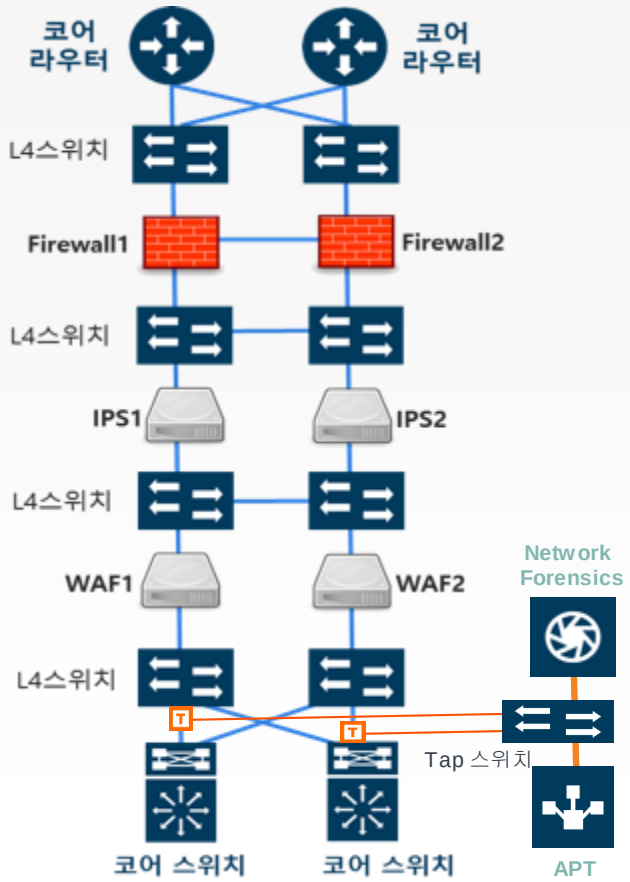


3. 활용방안

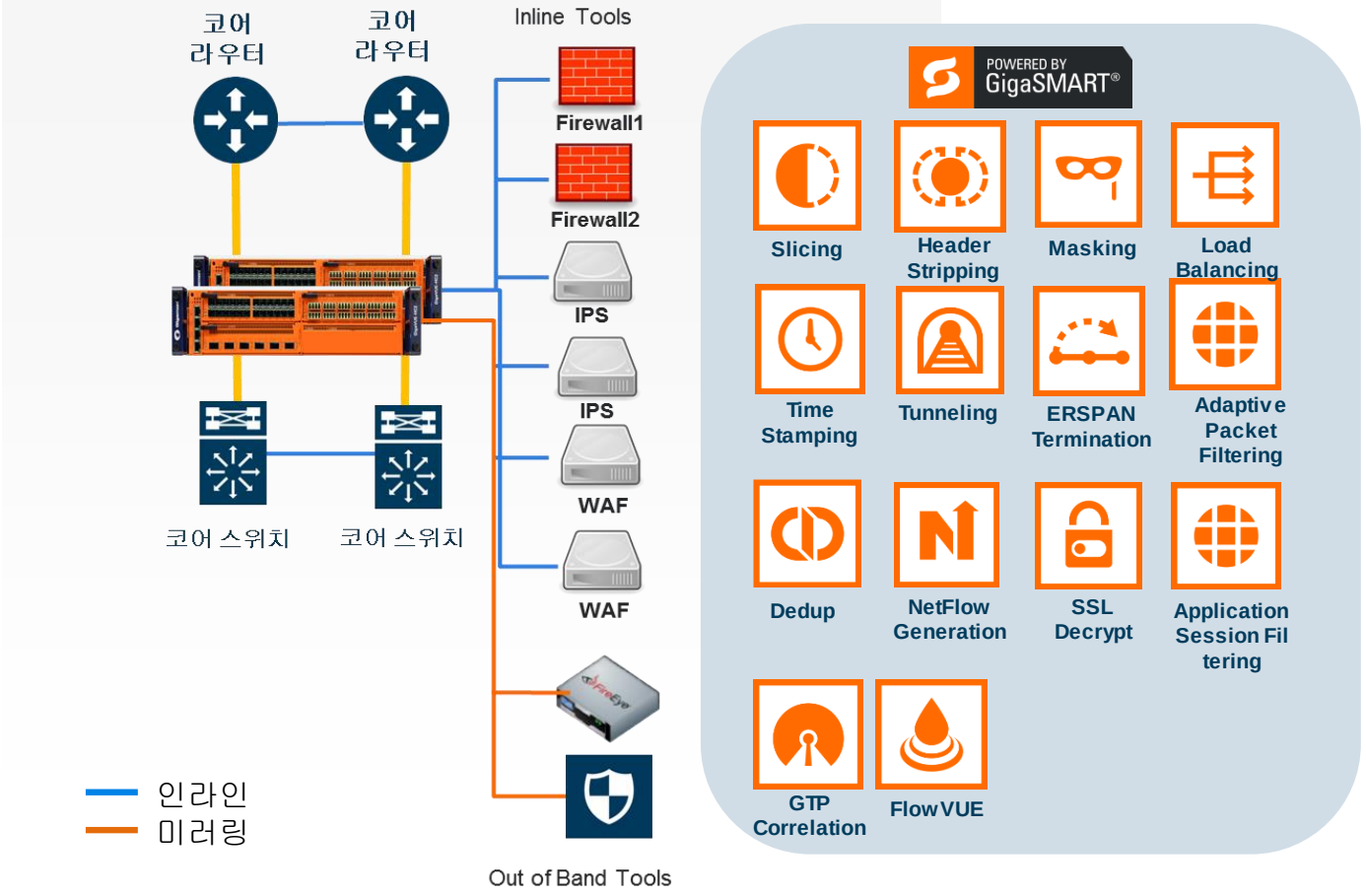
3.13 네트워크 인프라 환경 개선

- 효율적인 데이터센터 및 차세대 네트워크 인프라 환경개선

AS-IS



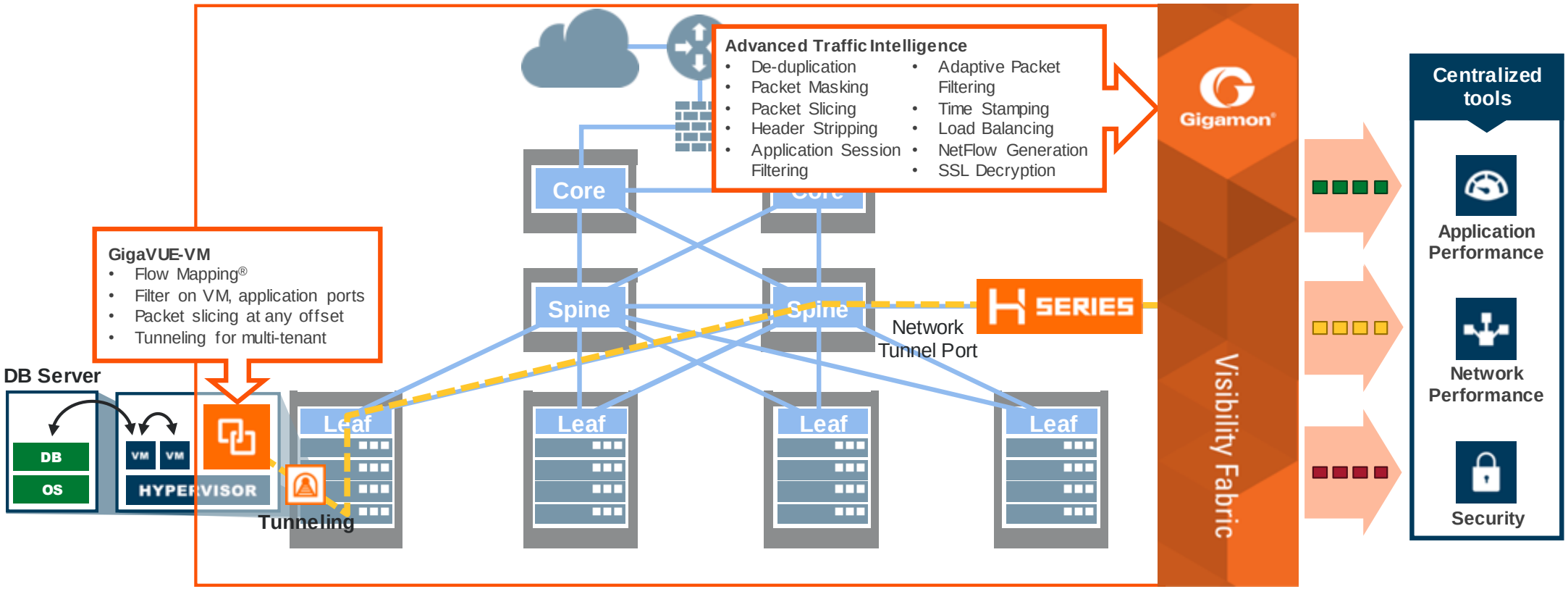
TO-BE



3. 활용방안

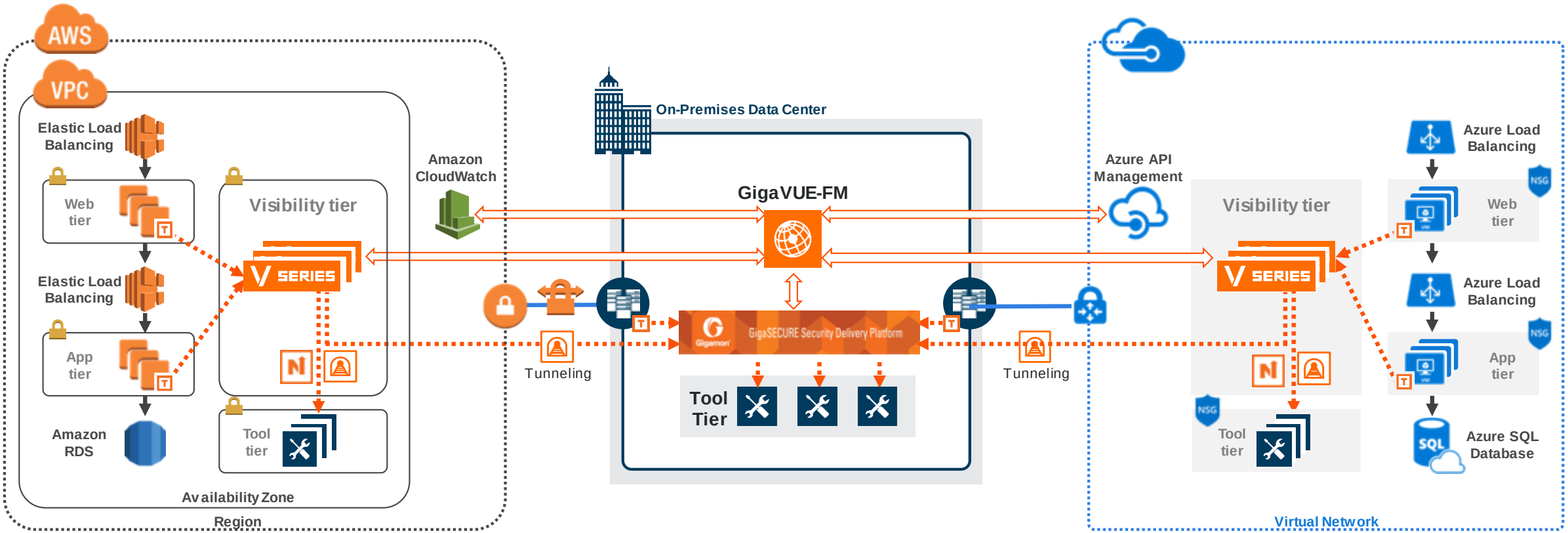
3.14 가상화 환경에서의 트래픽 모니터링(SDN, PRIVATE & HYBRID)

- 가상화 트래픽에 대한 가시성 확보



3. 활용방안

3.15 클라우드 환경의 보안 체계 수립

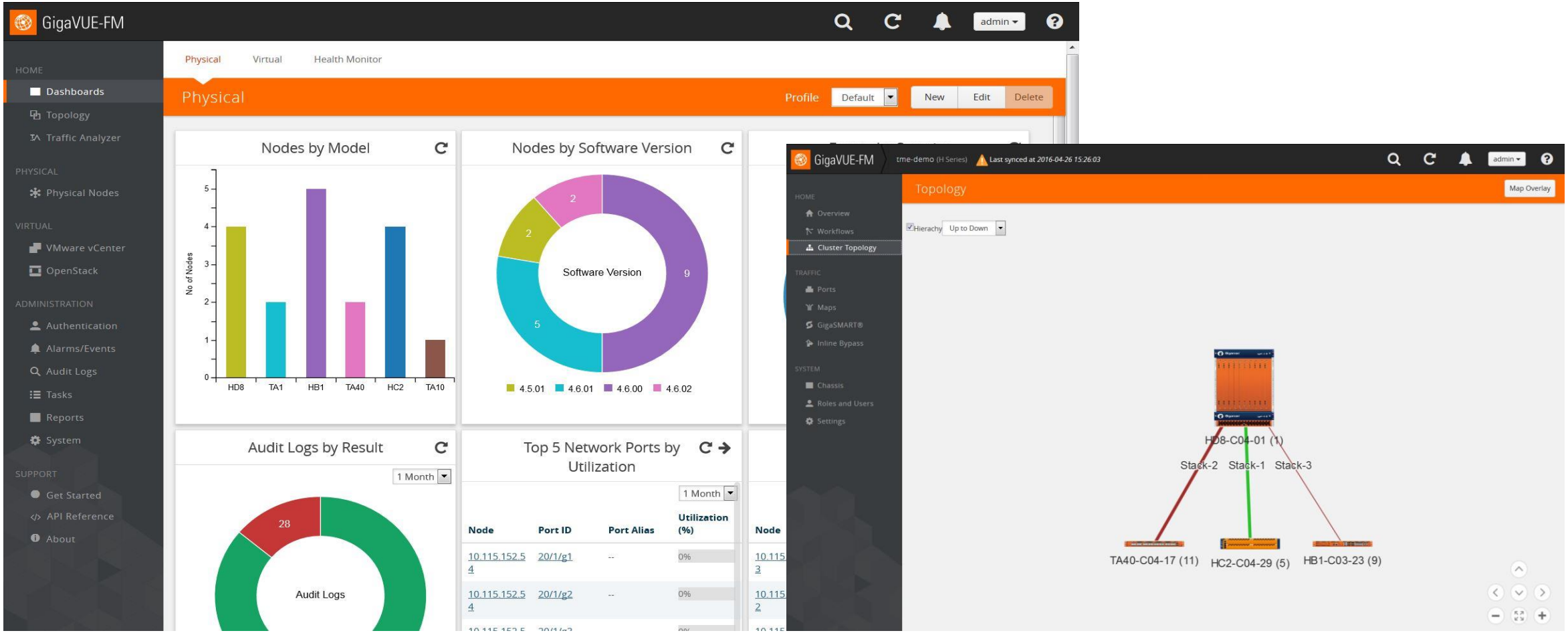


- 트래픽 모니터링 한계
- VM 인스턴스의 성능 이슈
- 멀티 밴더, 다수의 에이전트 설치 필요
- 복잡성, 관리 어려움

3. 활용방안

3.16 통합 관리 & ORCHESTRATION (PHYSICAL & VIRTUAL ENVIRONMENT)

- 효율적인 보안 및 네트워크 인프라 모니터링 제공

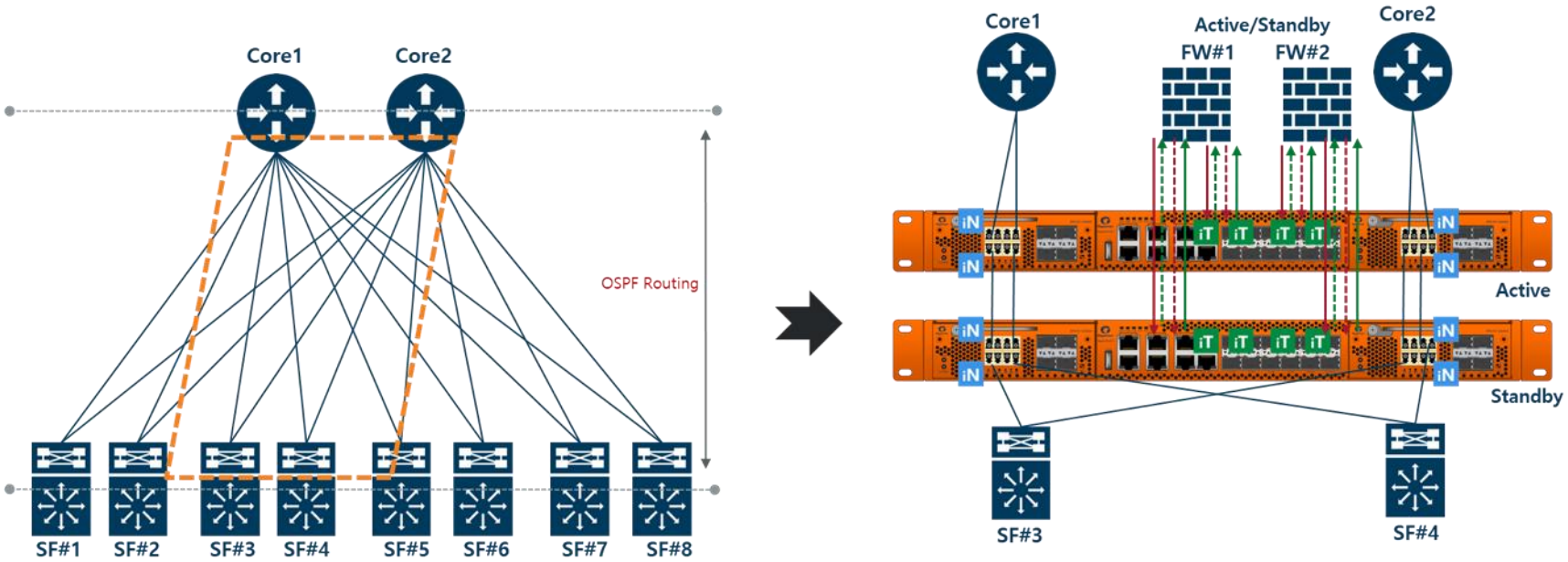


4. 고객사례

4. 고객사례

4.1 A사

- 다수의 링크와 ACTIVE/ACTIVE 네트워크 환경(ASYMMETRIC 라우팅 경로 발생)에서 방화벽을 효율적으로 도입

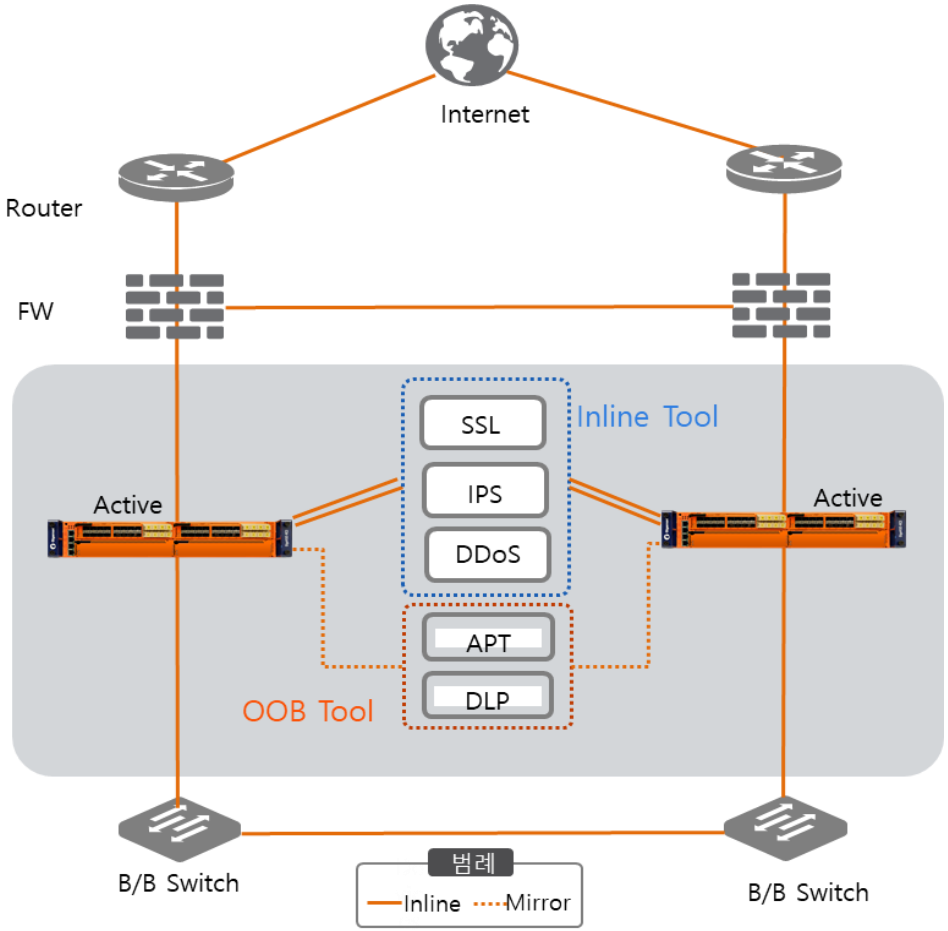


- ✓ 4~8개의 10Gbps 회선이 OSPF 라우팅으로 Active/Active 네트워크 환경이며, 방화벽을 Active-Standby 로 구성한 사례
- ✓ 네트워크회선을 Active-Active로 활용하면서 방화벽을 Active-Standby 혹은 Active-Active 로 자유롭게 적용 가능.
- ✓ 내부구간 트래픽 및 OSPF Control 패킷 등은 방화벽을 거치지 않고 Bypass

4. 고객사례

4.2 B사

- 다양한 보안 솔루션 수용 및 네트워크 구조의 단순화를 보안 존 구축

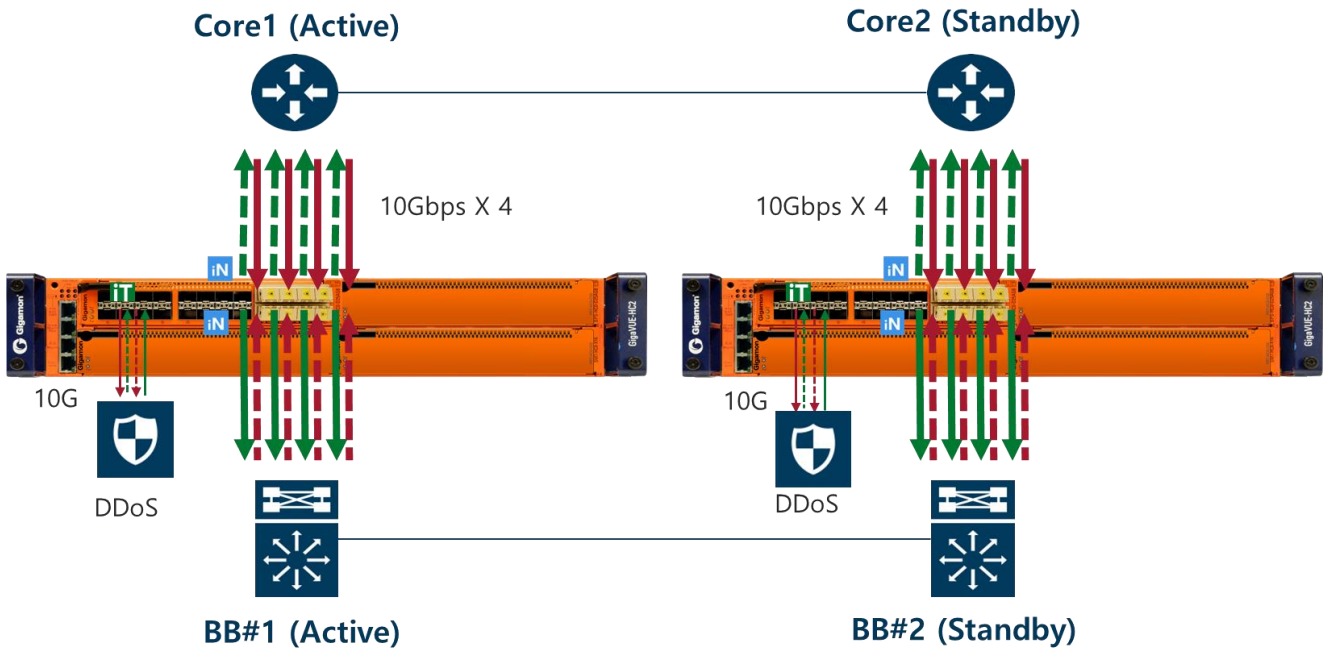


- ✓ 네트워크의 생존성 증대 및 보안 솔루션 확장성 증대
  -Heartbeat 이용, 각 Inline 보안 솔루션에 대한 실시간 Health Check 실시
- ✓ 자체 및 보안 솔루션 장애 시, 해당 솔루션 혹은 전체 네트워크에 대한 Bypass 구현
- ✓ 물리적 구성에 상관없는 다양한 Inspection Flow 구현(SSL → IPS → DDoS, IPS→ SSL → DDoS 등)
- ✓ 다양한 OOB 장비 수용 및 트래픽 복사/통합/재단 후 전달

4. 고객사례

4.3 E commerce

- 보안장비 효율성 극대화를 위한 다운링크 트래픽만 DDOS 장비로 전송, 업 링크 트래픽은 바이패스



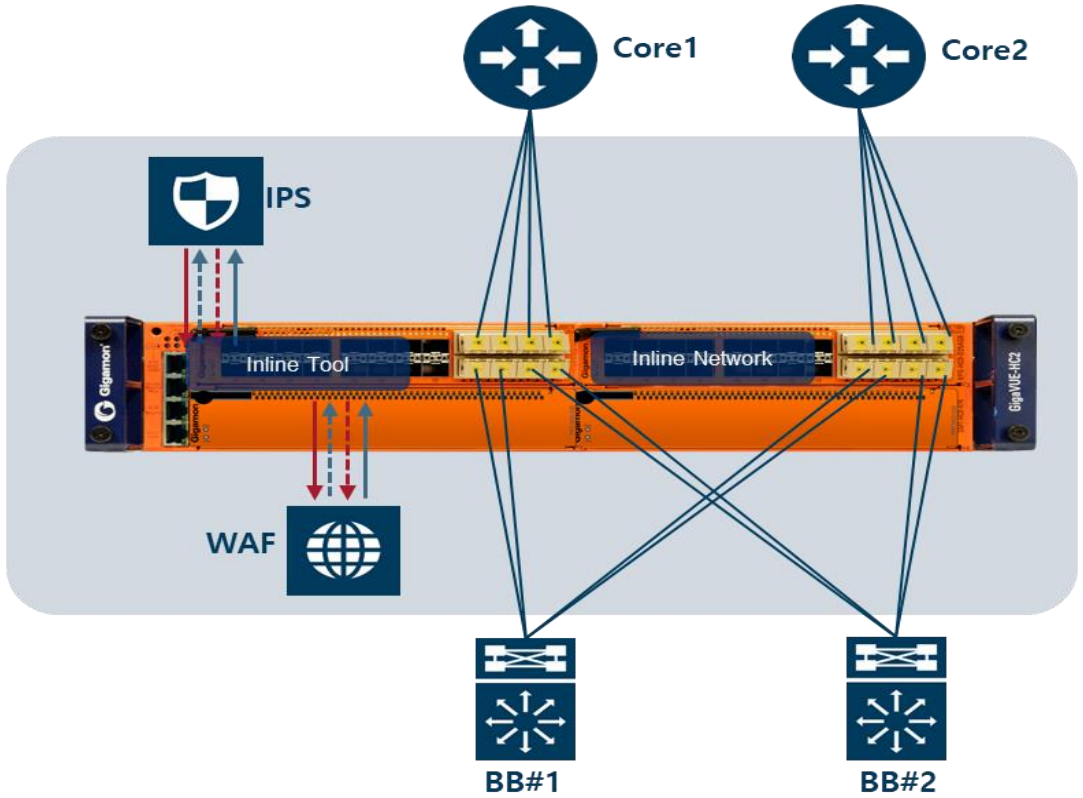
✓ 특장점 :
-A-to-B (Downlink) traffic 은 DDoS 장비로 전송
-B-to-A (Uplink) traffic은 Bypass

✓ 효과 :
Http response 패킷으로 인해 업 링크 트래픽 량이 다운링크 보다 4-5 배 많은 환경으로 효율적인 인라인 장비 배치 제공

4. 고객사례

4.4 N사 클라우드보안 서비스 사례

- IPS와 WAF 보안장비를 이용한 Security as a Service



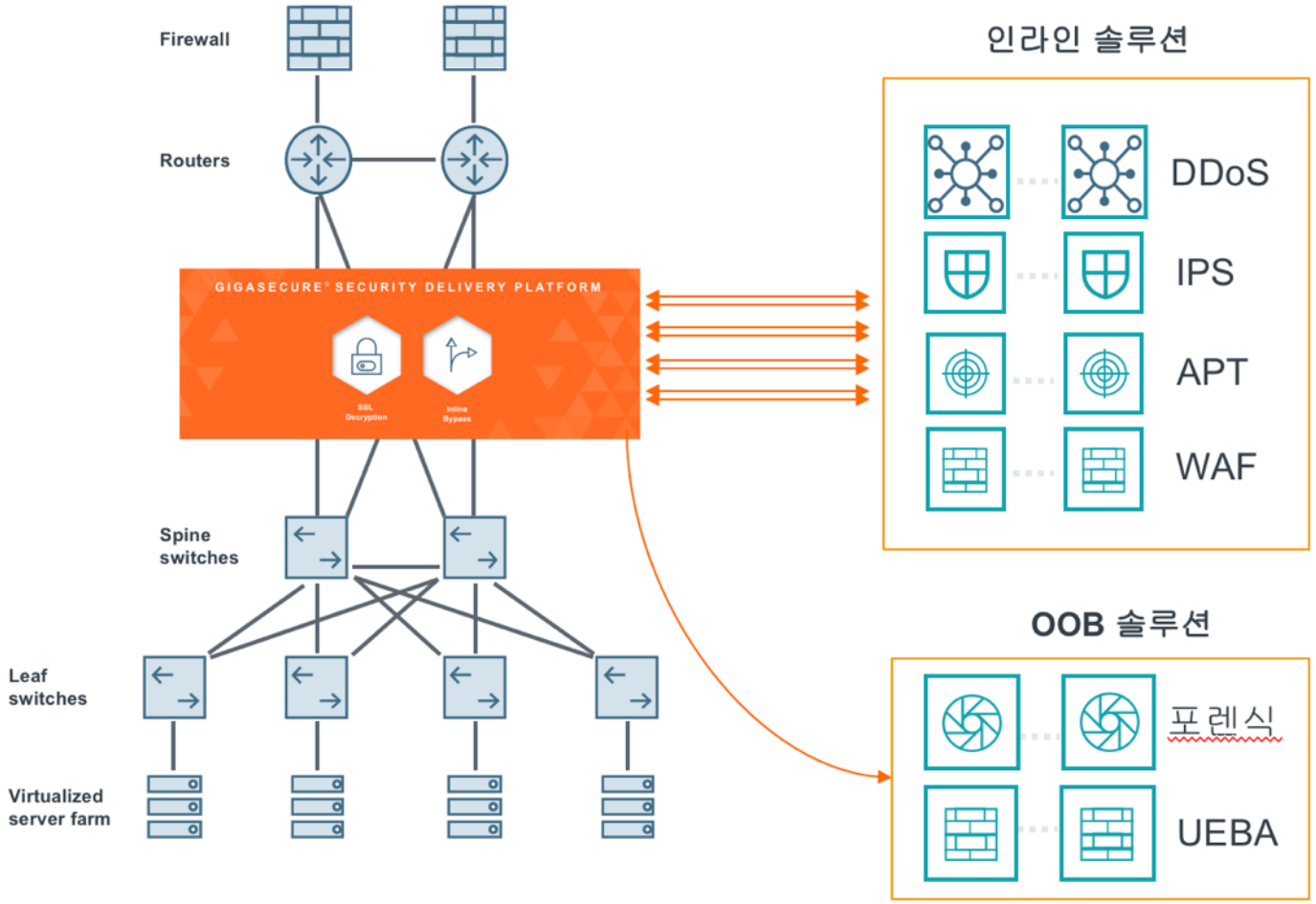
✓ 클라우드 서비스 이용자에 대한 보안 서비스를 구현하는 플랫폼으로 활용하는 사례

-보안 서비스 가입자 IP 패킷만 WAF/IPS 보안 장비로 전송
-그 이외의 트래픽은 바이패스

4. 고객사례

4.5 N원 Data Center

- 원활한 보안 서비스 제공을 위한 보안 존 구성 및 트래픽 선택 전달을 통한 CAPEX 및 OPEX 절감



✓ 서비스 체인 구성 예(인라인 솔루션)

-DDoS 의심 트래픽:

특정 IP 주소 트래픽(수시변경) → DDoS

-웹 트래픽:

TCP 80 & 443 → WAF

-전체 트래픽:

나머지 트래픽 → IPS → APT

5.제조사 소개

5. 제조사 소개

5.1 일반현황

- ✓ **설립연도**: 2004년 (Pioneered Market)
- ✓ **본사위치**: 미국, 캘리포니아 산타클라라
- ✓ **주요사업**: 보안 및 관리툴을 위한 가시성 시장의 리더 및 Innovator
- ✓ **사업분야**: 모바일(Mobile), 데이터센터(Datacenter), 클라우드(Cloud)
- ✓ **보유기술**: 26 개 핵심 특허권, 28 개 특허 심사 중
- ✓ **주요고객**: 2900+ 고객

  (포춘 100대 기업 중 83개+, 전세계 글로벌 100대 통신사 중 50개+)

- ✓ **2016년 기준 미국 기술기업 내 가장 빠르게 성장하는 기업 5위**

Fast Future Growth

Symbol	Company name	EPS estimate current yr % chg	Next yr % chg	Composite Rating	EPS Rating
PAYC	Paycom Software	93%	25%	99	99
FB	Facebook	73	29	99	99
SIMO	Silicon Motion Tech	56	17	99	93
HQY	HealthEquity	50	29	99	98
GIMO	Gigamon	45	21	99	95
NTES	NetEase	42	17	99	99
ESNT	Essent Group Ltd	33	18	97	99
AVGO	Broadcom Limited	25	19	99	95
GRUB	GrubHub	24	31	98	95

Deloitte. Technology Fast500

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

"기가몬은 복잡한 보안 아키텍처를 단순화 하는데 도움을 준다."

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

"기가몬은 전 세계 **NBP** 마켓의 **37.5%**를 차지하는 마켓 리더이다 "

amazon web services

"The Gigamon Visibility Platform enables our customers to accelerate …migration of their existing applications and workloads for richer content nspection and protection of their mission-critical workloads and data."
- Tim Jefferson, Global Ecosystem Leader-Security, Amazon Web Services, Inc., November 2016

"기가몬은 퍼블릭 클라우드 상에서 중요 데이터에 대한 가시성을 제공하여 클라우드 비즈니스로의 이전을 가능하게 한다. "

IHS Markit

Gigamon has a full portfolio of network monitoring equipment, addressing the whole range of deployments from small to very large.
- IHS Technology, Network Monitoring Equipment Annual Report (May 2017)

"기가몬은 마켓 리더로서, 네트워크 전반의 가시성을 제공하는 모든 제품군을 제공하고 있다."

52

Gigamon

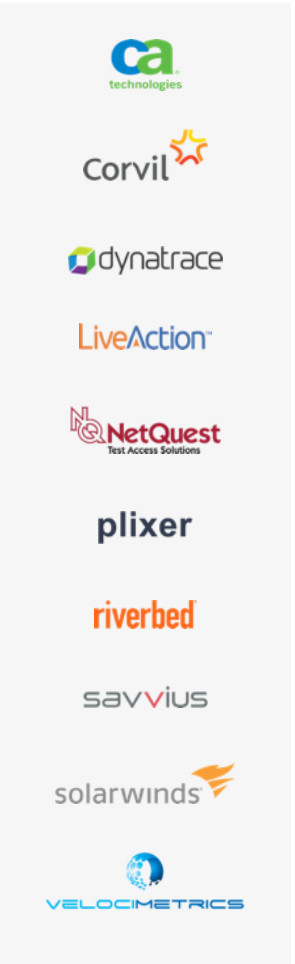
5. 제조사 소개

5.2 주요 에코 파트너사

Security and Vulnerability Management

Service Provider

Performance Management



Infra-structure

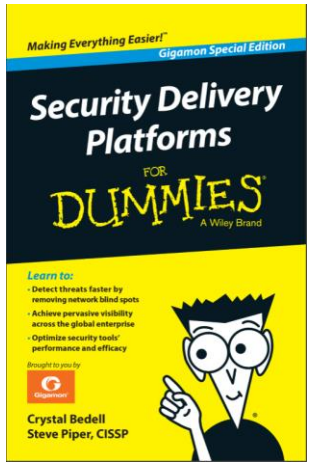
5. 제조사 소개

5.4 해외 레퍼런스

5. 제조사 소개

5.5 통합 포트폴리오

Thank you



- **Contact Points**

  -영업담당 : 노병완 전무 (010-7393-4196, brian.rho@gigamon.com)

  -기술담당 : 권혁인 이사 (010-3018-9461, hyukin.kwon@gigamon.com)

  이민형 이사 (010-9636-8176, minhyung.lee@gigamon.com)

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

Gigamon