VIRTUAL
INTEGRATED
APPLICATION
SECURITY
FAIR 2021 (9th)

Global Edge를 이용한 Website Protection

모니터랩 연구소
김 현 목 전무

MONITORAPP

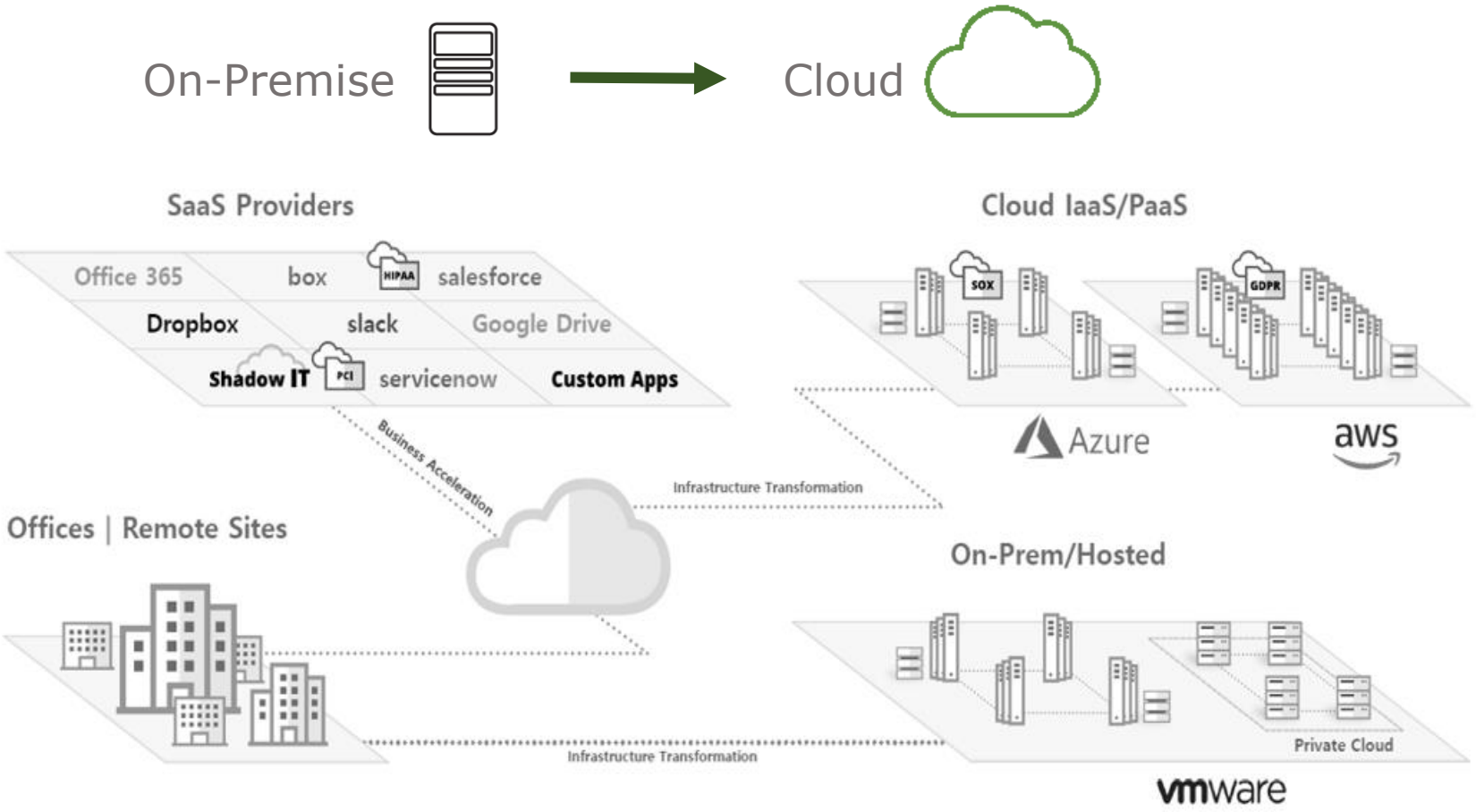
CONTENTS

01

Security as a Service

01 Security as a Service

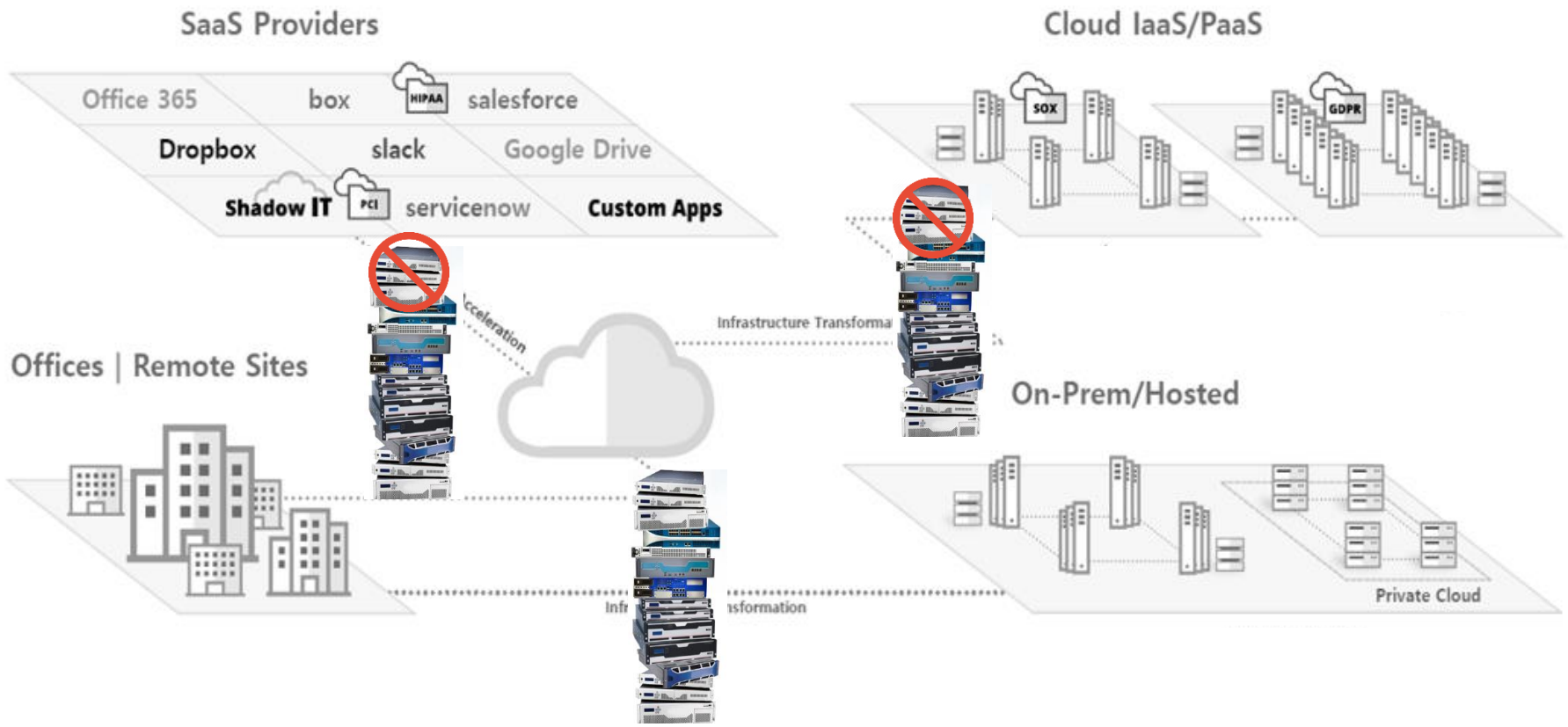
❖ 기업 IT 환경 변화



Cloud는 선택이 아닌 필수이며 , Cloud 전환에 보안은 가장 큰 고려 요소

01 Security as a Service

❖ 기업 IT 환경 변화



본사/지사 환경과 On-Prem / IaaS / SaaS 이용 증가로 보안 환경 변화
기존 경계선 보안만으로는 한계

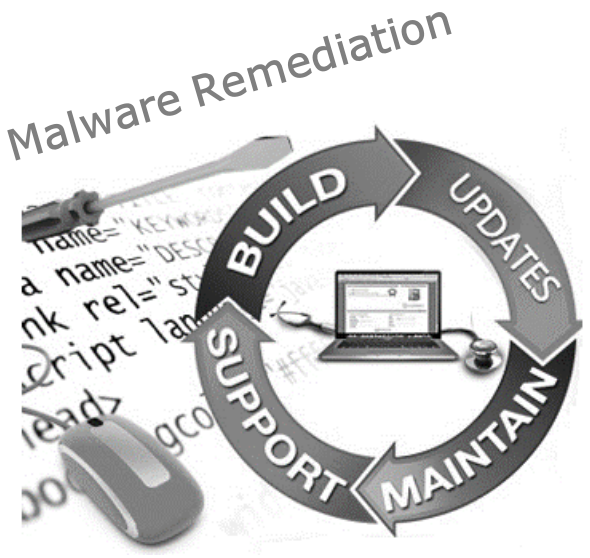
01 Security as a Service

❖ 보안 서비스의 변화

- 다양한 Edge of Internet 에 대한 보안시스템 구축,운영이 비용/시간/위험 증대 초래

Multiple appliances at
every internet gateway

- NG Firewall
- Intrusion Prevention System
- Web Application Firewall
- Advanced Persistent Threat
- Zero Day
- Data Loss Prevention
- URL Filtering
- Anti-Virus
- Cache/Proxies



01 Security as a Service

❖ 보안 서비스의 변화

Multiple appliances at
every internet gateway

Security Management
- **Appliances**
- **VM Based**
- **Container Based..**

Shadow IT and…
- **SaaS?**
- **Cloud Access Control?..**

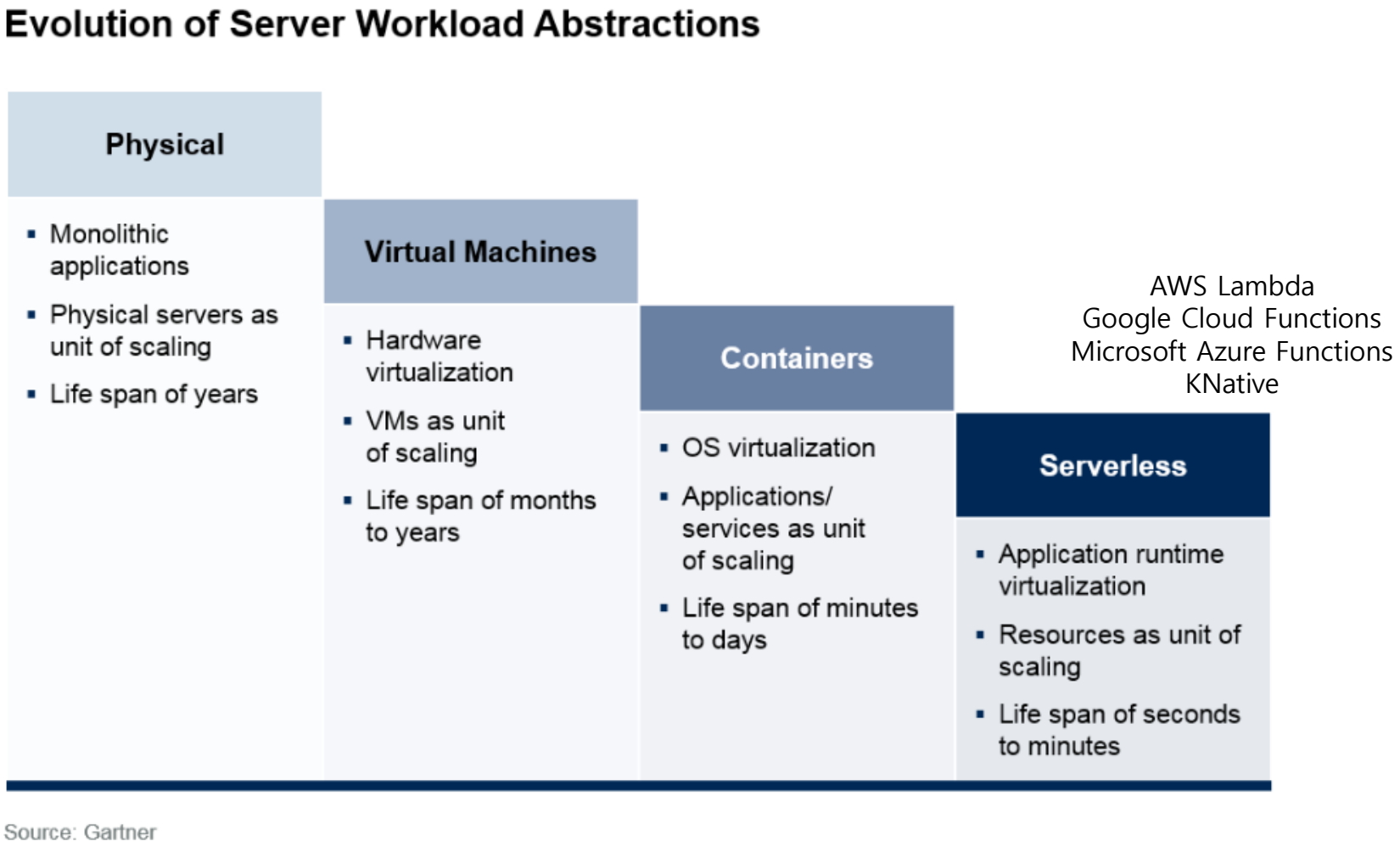
Hybrid

and

01 Security as a Service

❖ 보안 서비스의 변화

- 컴퓨팅 환경의 변화에 따른 다양한 보안 고려 요소



Source: Gartner

01 Security as a Service

❖ 보안 서비스의 변화

- 클라우드 환경에서의 해킹 사고 – 사람과 관리의 문제가 99%

- 2019년 3월 유출 후 7월 확인

- 전 AWS 직원에 의한 오픈소스 WAF 환경설정 오류 이용

- 1억 6백만개 신용카드 정보 유출(미국/캐나다)

01 Security as a Service

❖ 보안 서비스의 변화

- 클라우드 환경에서의 보안 책임 확인 필요

클라우드의 영역 별로 필요한 보안 요소가 무엇인지 파악. ☐ 고객 책임 ▢ 클라우드 공급자 책임

Shared Security Responsibility Model			
Private/ On-Premise	IaaS	PaaS	SaaS
Users	Users	Users	Users
Data	Data	Data	Data
Applications	Applications	Applications	Applications
Operating System	Operating System	Operating System	Operating System
Network	Network	Network	Network
Hypervisor/ Virtualization	Hypervisor/ Virtualization	Hypervisor/ Virtualization	Hypervisor/ Virtualization
Infrastructure	Infrastructure	Infrastructure	Infrastructure
Physical	Physical	Physical	Physical

01 Security as a Service

❖ 보안 서비스의 변화

Security-as-a-Service (SECaaS)

An outsourced, subscription-based model for security management delivered over the Internet

SECaaS

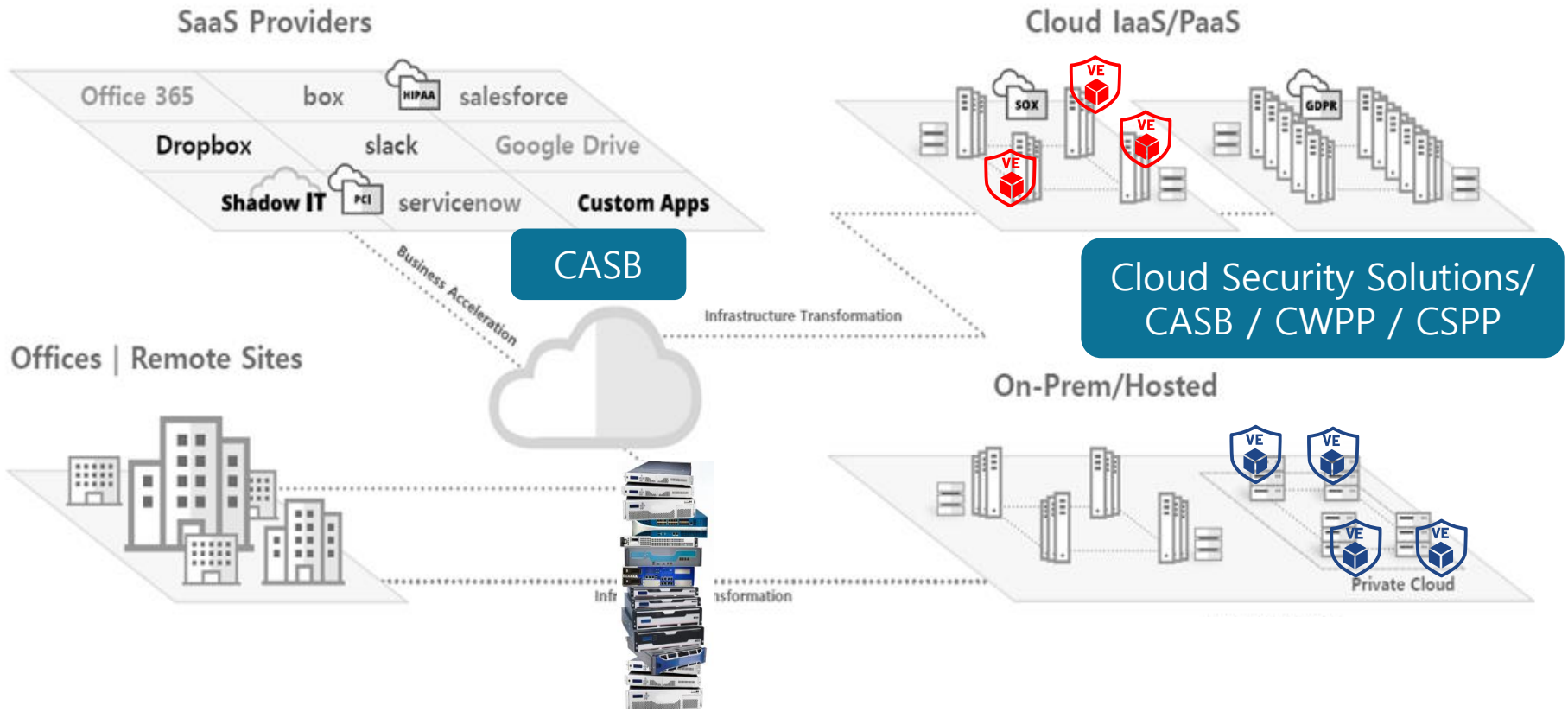
Unnecessary

A CUMBERSOME PROCEDURE

- Hardware
- Physical Server
- Physical space
- Continuous monitoring &maintenance
- Tremendous cost &human resources

01 Security as a Service

❖ 보안 서비스의 변화



01 Security as a Service

❖ SECaaS를 이용한 웹보안 서비스

- SECaaS 형태의 보안 서비스 고려 사항

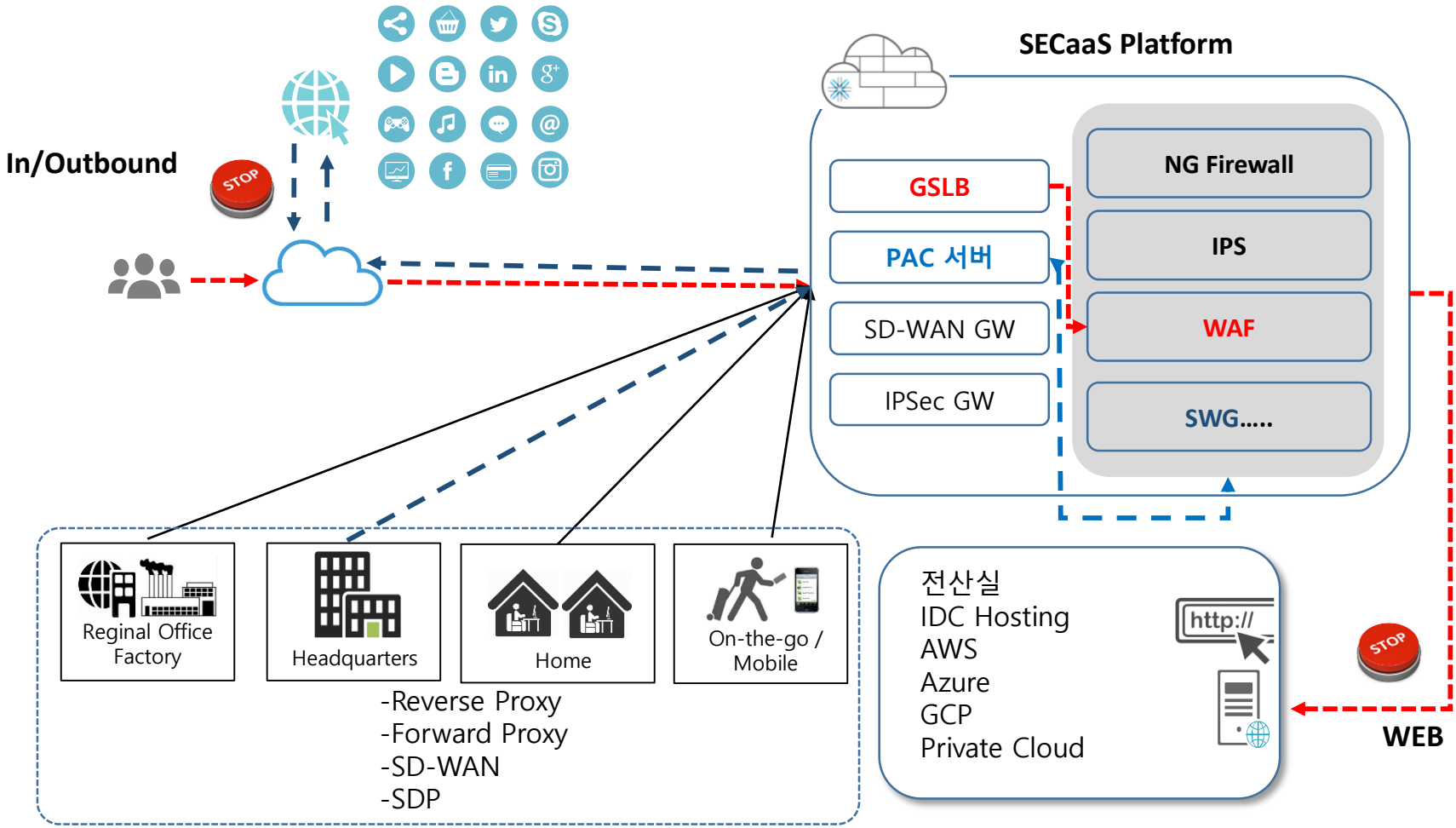
- ***Traffic Forwarding***
  - **Reverse/Forward Proxy**
  - **SD-WAN**
  - **IPSec**

- ***Multitenancy / Scalability***
  - **Tenant Based Service Architecture**
  - **Global One Platform**
  - **IX/ISP/Datatacenter Transit**

01 Security as a Service

❖ SECaaS를 이용한 웹보안 서비스

- 다양한 보안서비스를 SECaaS 플랫폼에서 제공하기 위한 Reverse/Forward Proxy/SDWAN/IPSec 지원



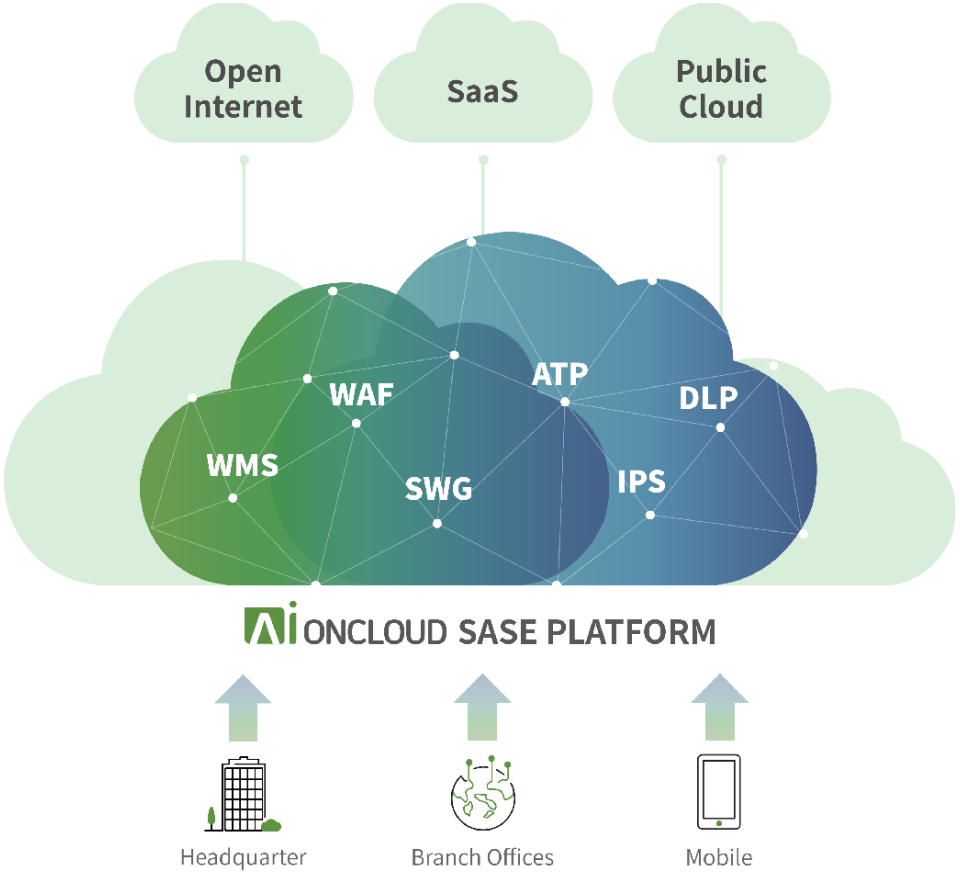
02

Global Edge Platform AIONCLOUD

02 Global Edge Platform AIONCLOUD

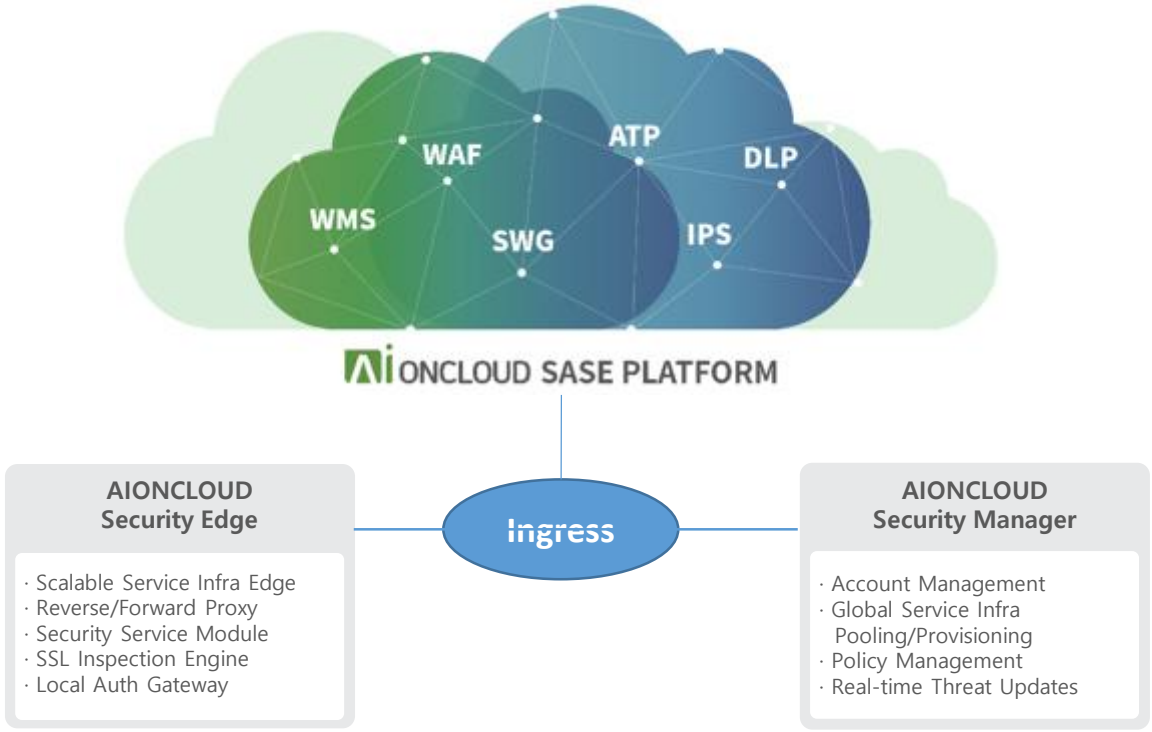
❖ AIONCLOUD (Application Insight on Cloud)

- AIONCLOUD는 클라우드 기반 통합 보안 서비스를 제공 하는 All-In-One Platform
- 고성능 프록시 기술 기반으로 WAF, SWF, DLP 등 보안 서비스 제공



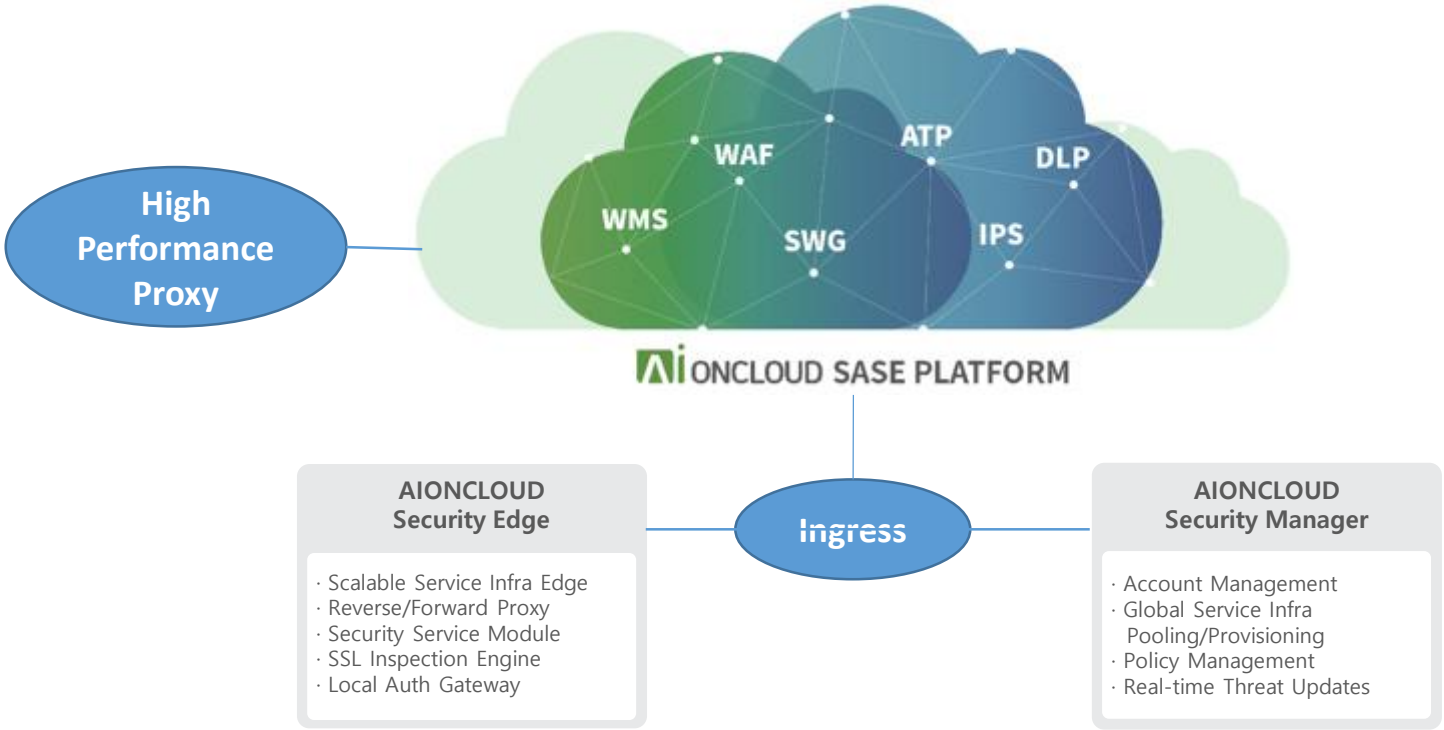
02 모니터랩 SASE 플랫폼 AIONCLOUD

❖ AIONCLOUD (Application Insight on Cloud)



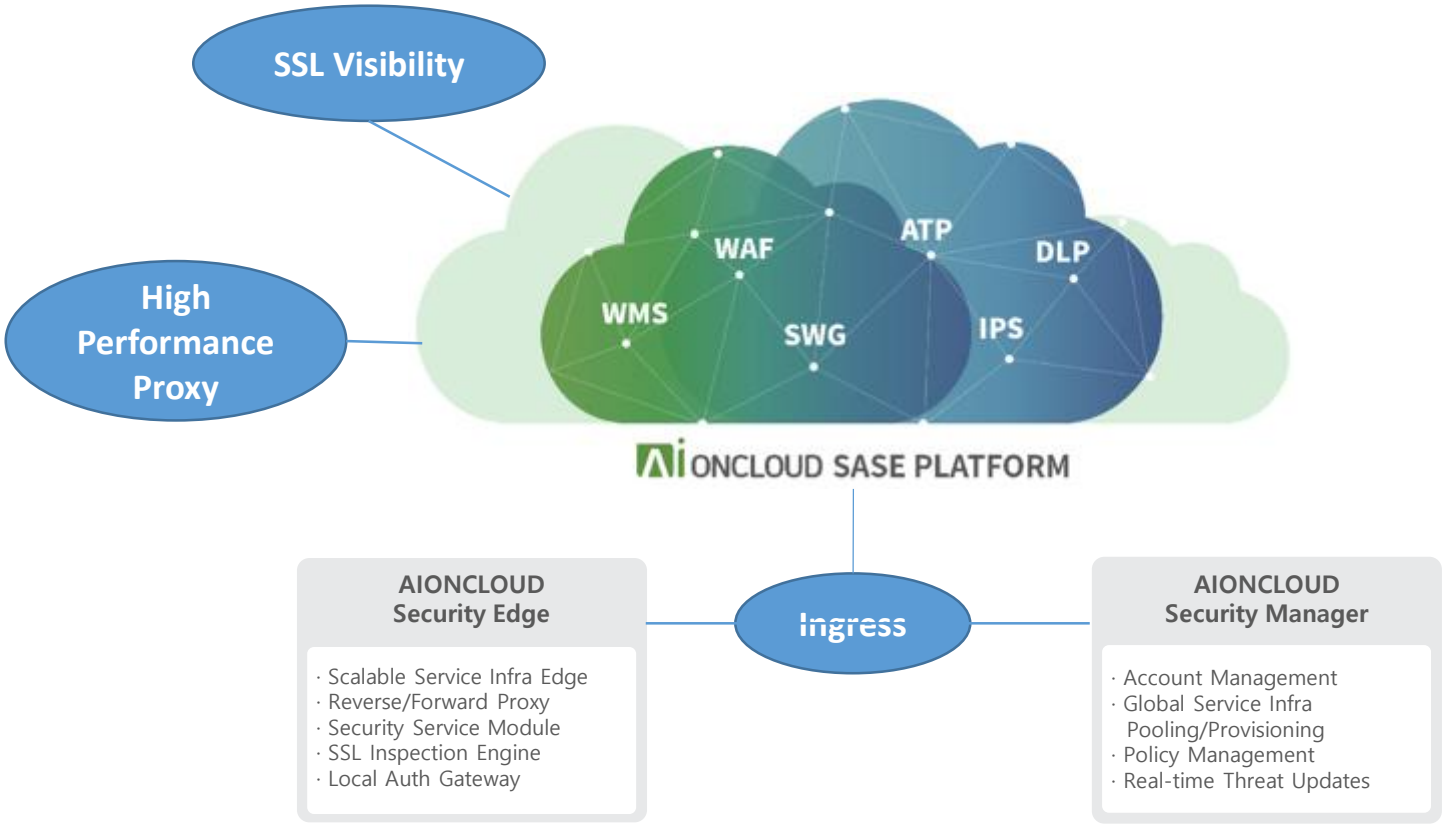
02 모니터랩 SASE 플랫폼 AIONCLOUD

❖ AIONCLOUD (Application Insight on Cloud)



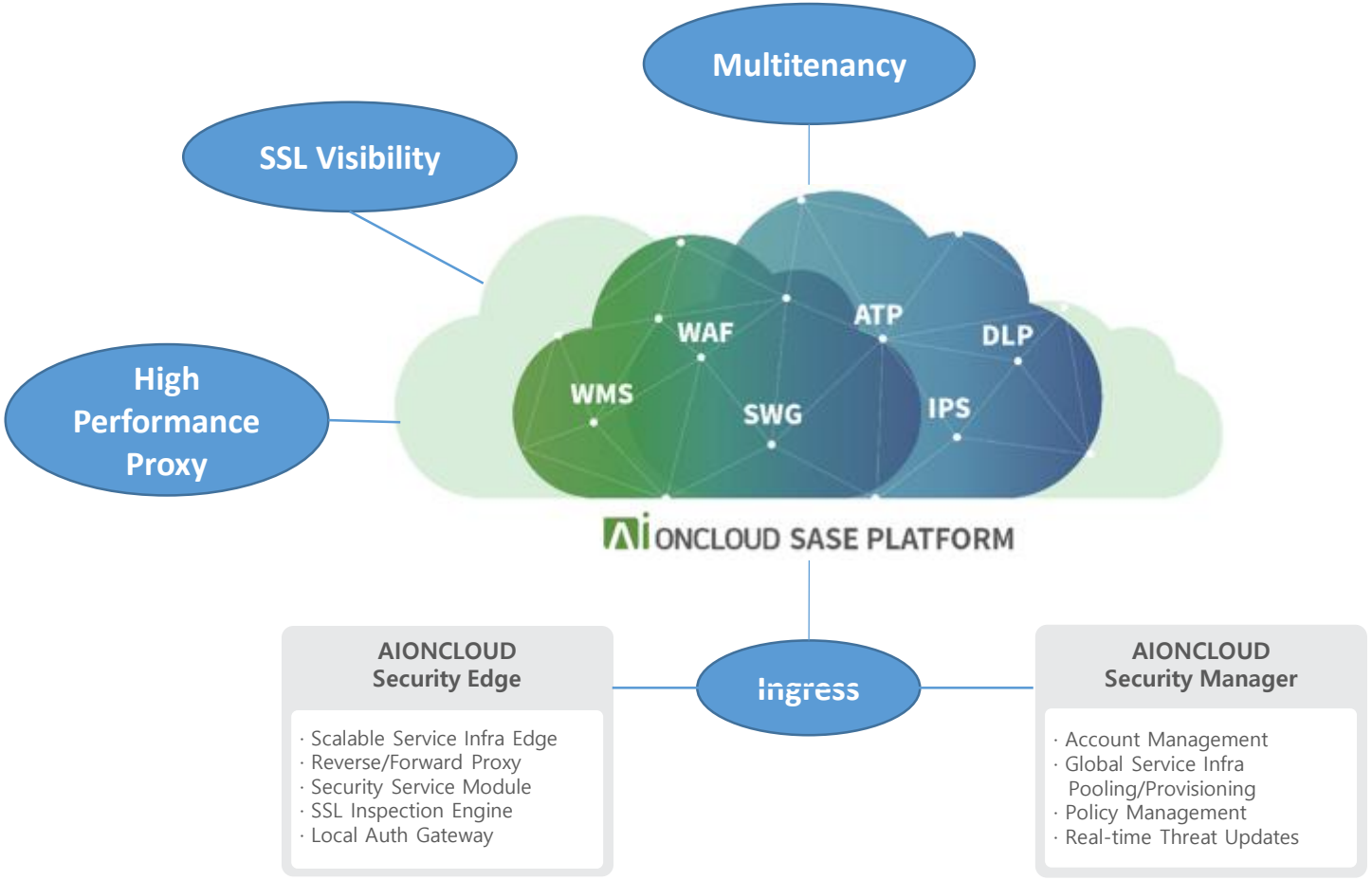
02 모니터랩 SASE 플랫폼 AIONCLOUD

❖ AIONCLOUD (Application Insight on Cloud)



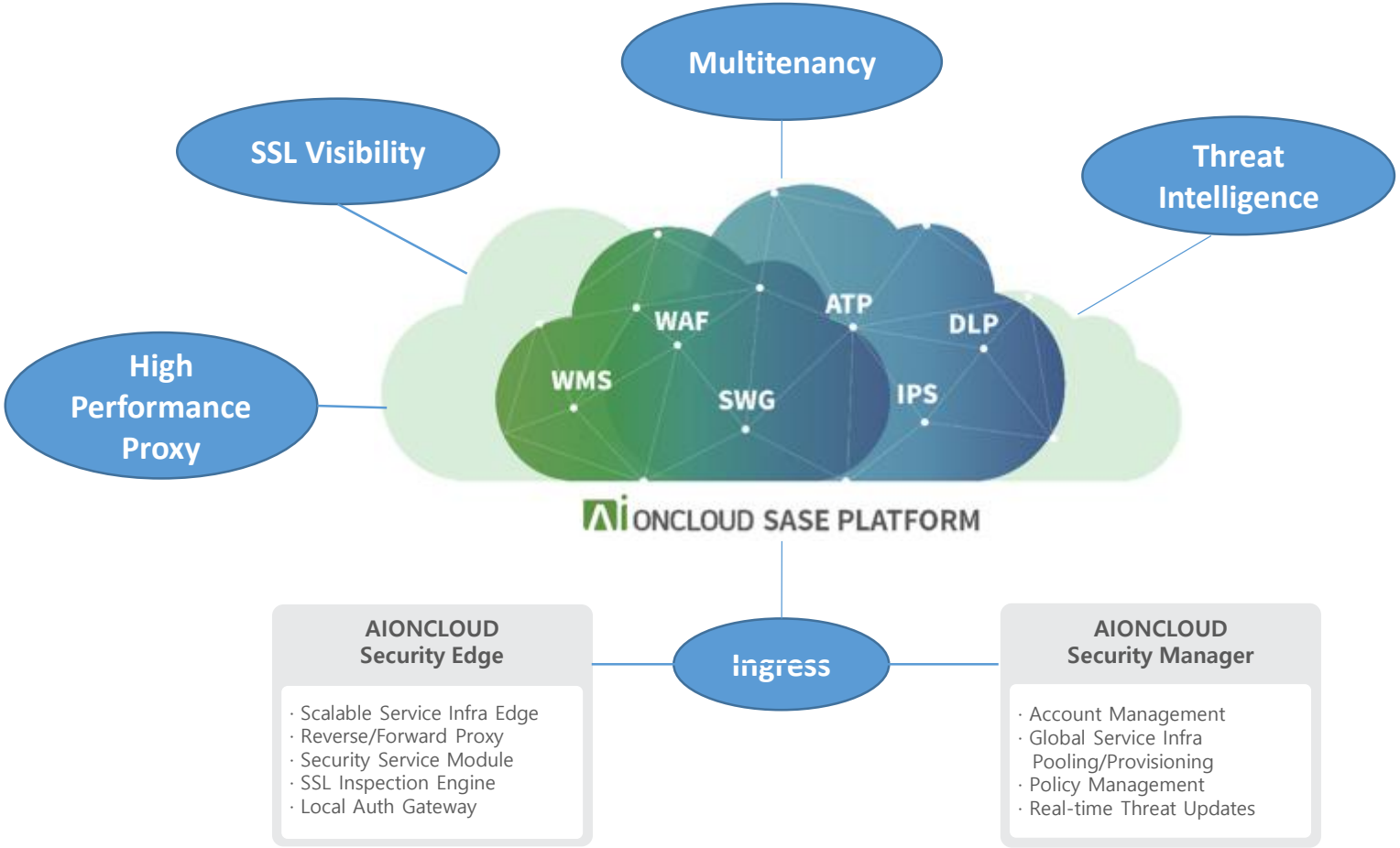
02 모니터랩 SASE 플랫폼 AIONCLOUD

❖ AIONCLOUD (Application Insight on Cloud)



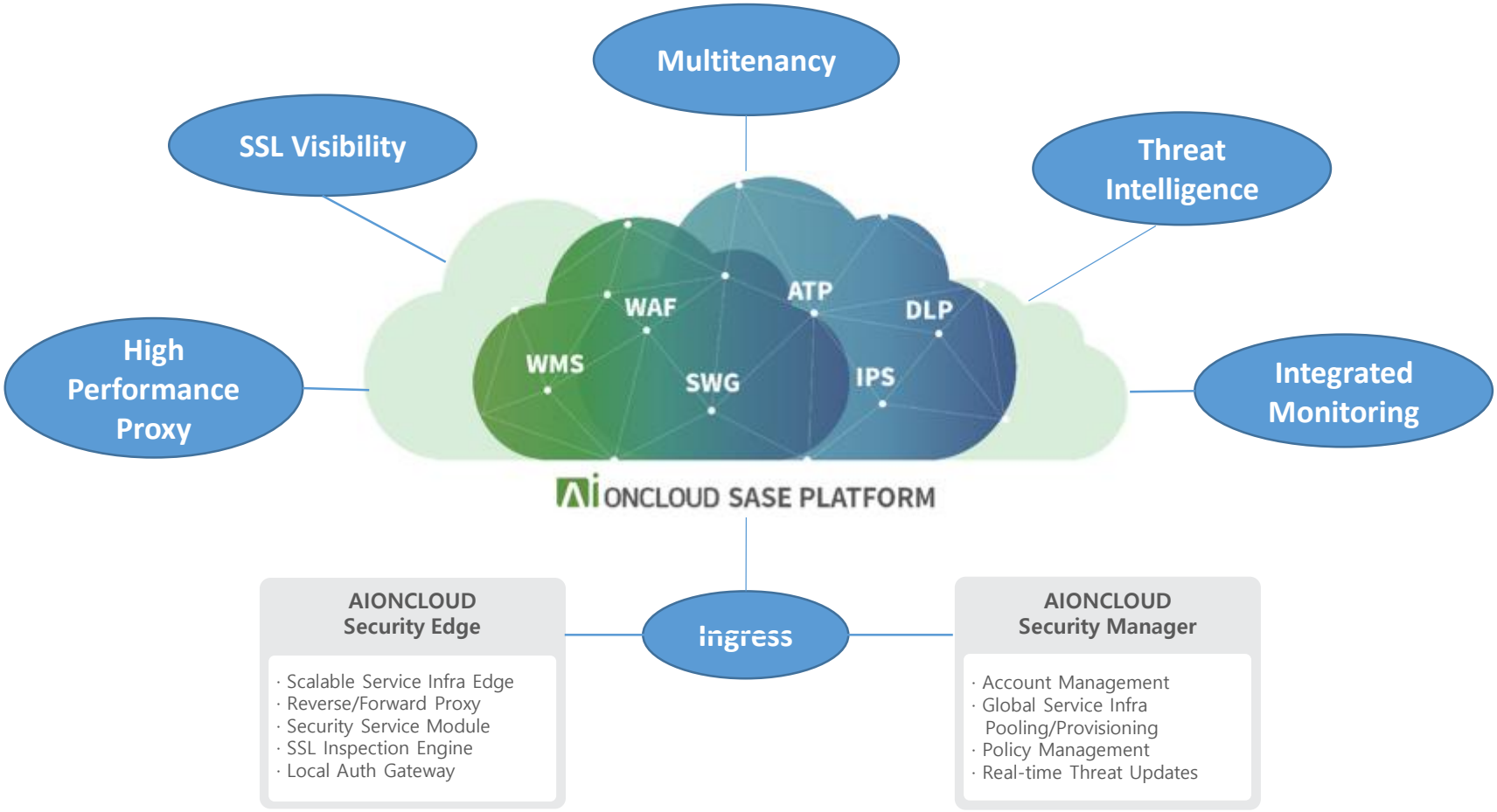
02 모니터랩 SASE 플랫폼 AIONCLOUD

❖ AIONCLOUD (Application Insight on Cloud)



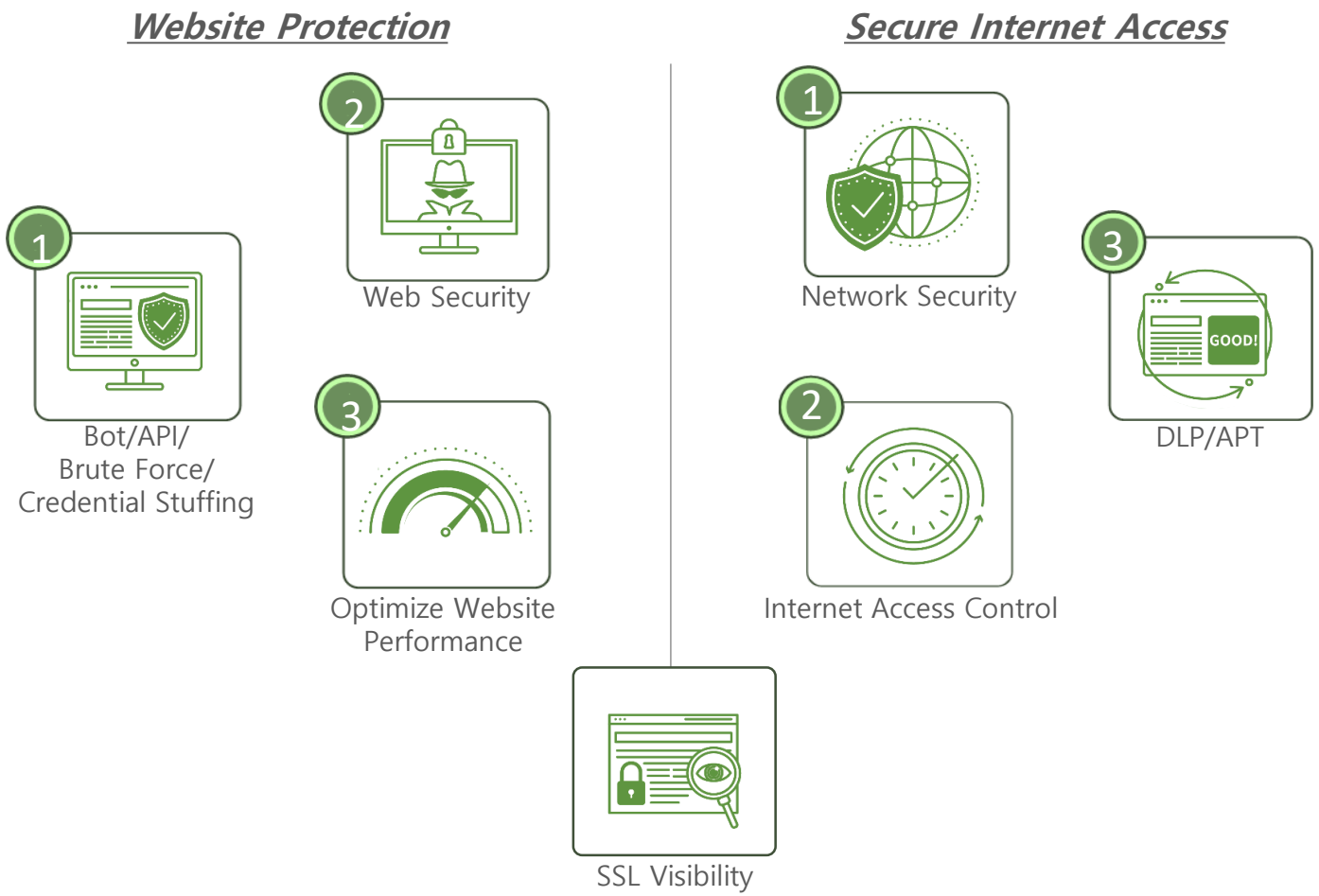
02 모니터랩 SASE 플랫폼 AIONCLOUD

❖ AIONCLOUD (Application Insight on Cloud)



02 Global Edge Platform AIONCLOUD

❖ AIONCLOUD 주요기능



02 Global Edge Platform AIONCLOUD

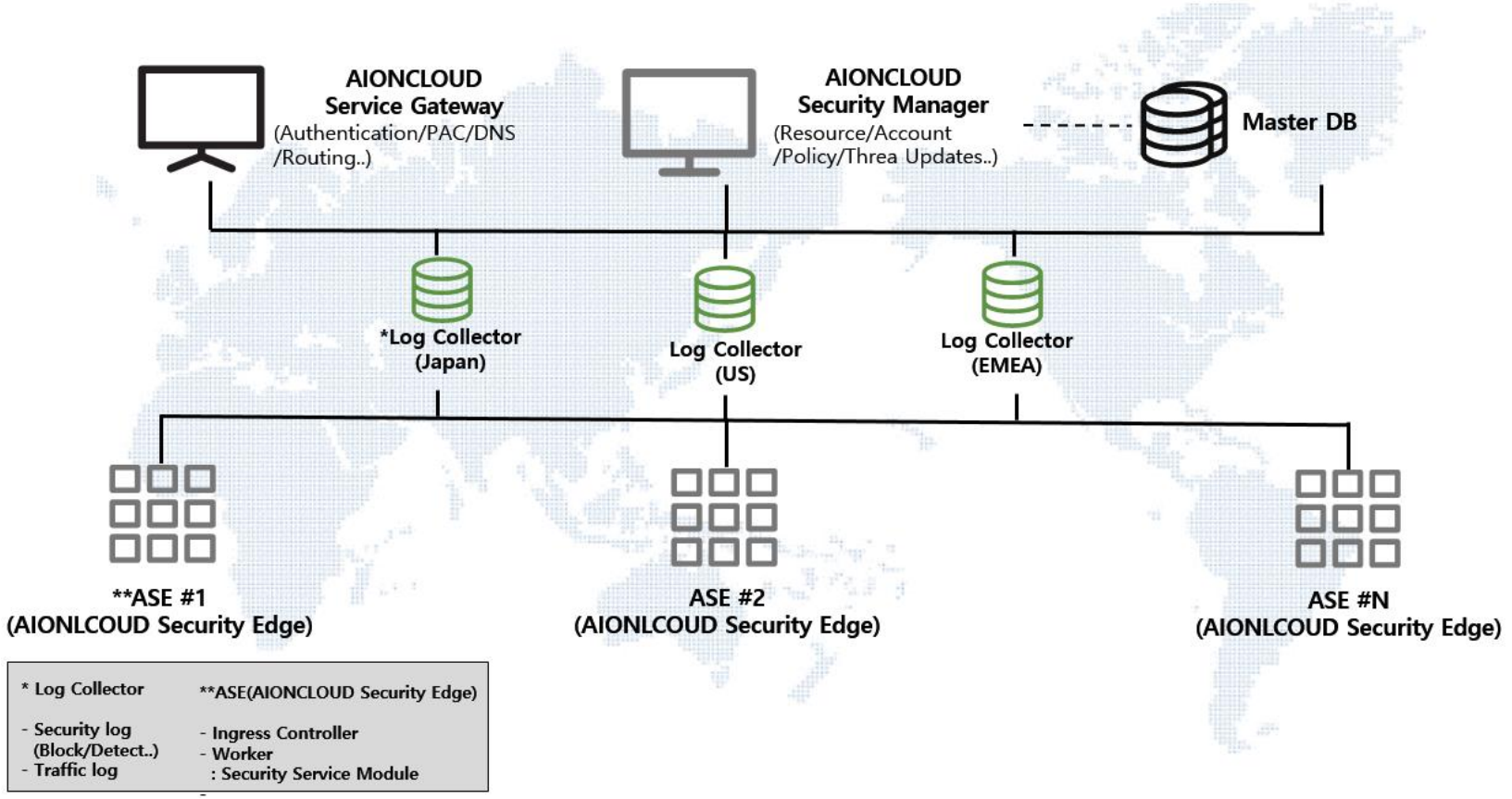
❖ AIONCLOUD Global Network

- AIONCLOUD는 전세계 15개 지역의 40개 데이터센터에 Physical/Virtual 서비스 인프라를 보유하고 있습니다.

02 Global Edge Platform AIONCLOUD

❖ AIONCLOUD 플랫폼 구성

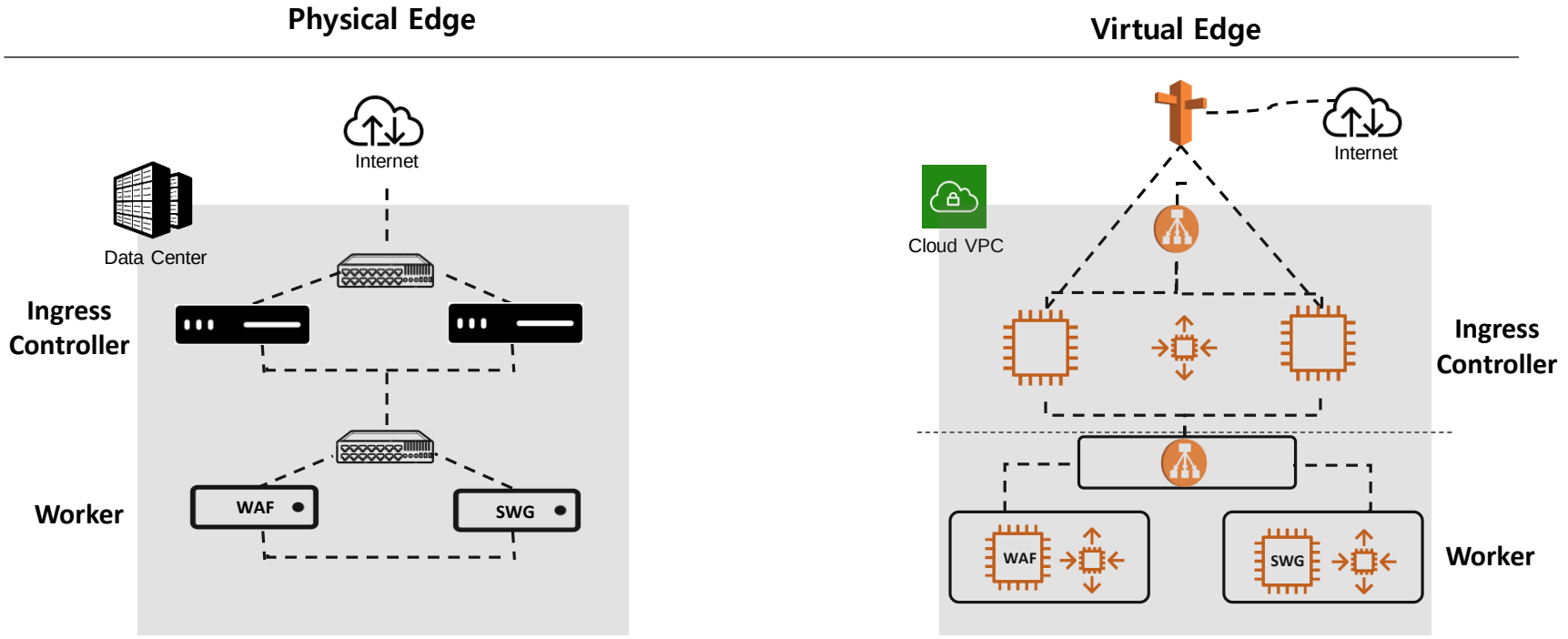
AIONCLOUD Service Gateway / Security Manager / Security Edge



02 Global Edge Platform AIONCLOUD

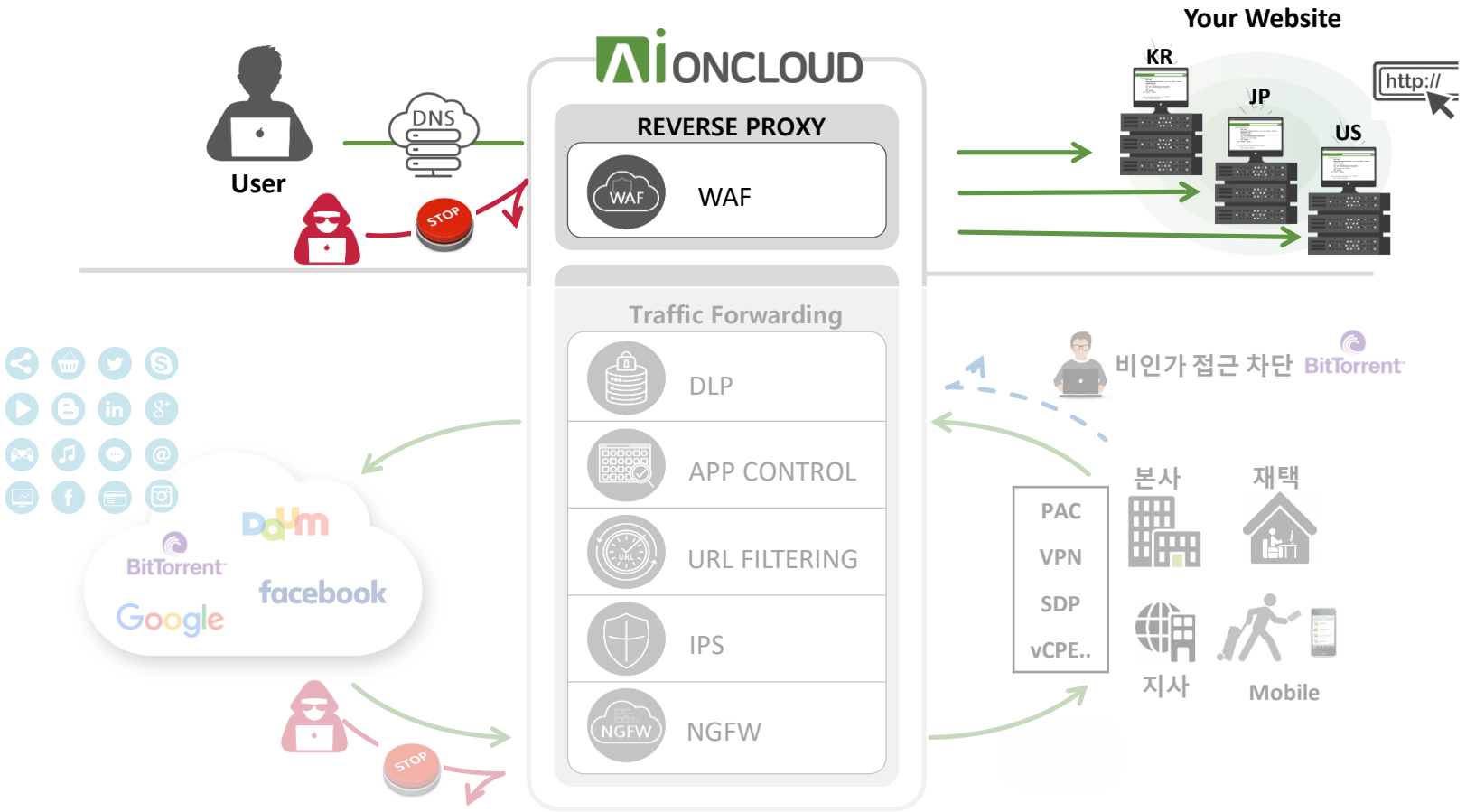
❖ AIONCLOUD Security Edge

- Container Based Physical or Virtual Edge, AIONCLOUD Edge / White Label Partner Edge



02 Global Edge Platform AIONCLOUD

❖ AIONCLOUD(Application Insight on Cloud)서비스 트래픽 Flow



03

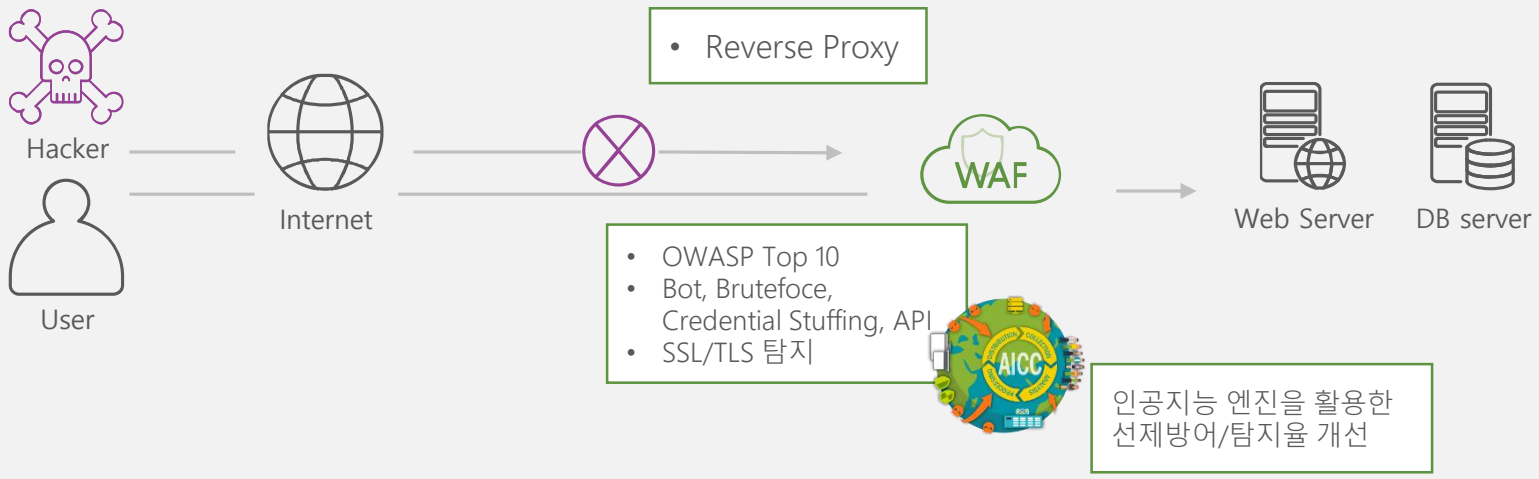
Website Protection

03 Website Protection

❖ AIONCLOUD WAF 서비스

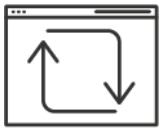
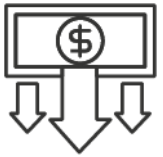
- HW / SW 설치, 유지보수, 라이센스가 필요 없는 강력한 웹 보안과 성능 최적화를 제공
- 5,000여개 이상의 국내외 사이트에서 검증된 신뢰성 높은 웹보안 서비스
- SECaaS 플랫폼을 통한 간편한 신청 / 설치 / 설정 / 관리

WAF 서비스 구성



03 Website Protection

❖ AIONCLOUD WAF의 서비스 특징

 **SECURITY** 웹 사이트 보안 강화	 **PERFORMANCE** 웹 사이트 성능 최적화	 **LOWER COST** TCO 절감 (Total Cost of Ownership)
 **SCALABILITY** 클라우드 기반의 서비스 인프라	 **EASY to USE** 직관적인 UI/UX	 **UPDATE** 최신 보안 기능 실시간 업데이트

03 Website Protection

❖ AIONCLOUD WAF – 강력한 보안 서비스

01

OWASP Top 10 취약점 방어

SQL 인젝션, XSS, CSRF 같은 가장 심각한 웹 취약점들을
다양한 정책으로 방어합니다.

02

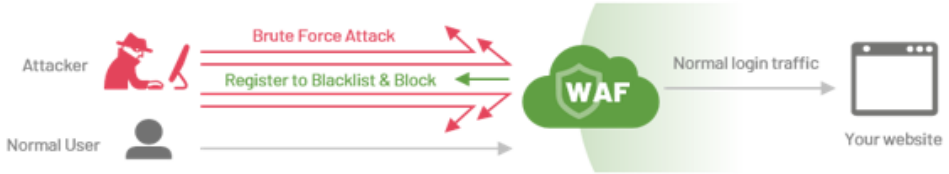
악성 봇 공격 방어

SPAM, 크롤링, 스크랩핑, 해킹툴과 같은 악성 Bot 공격을 방어합니다.
허니팟 URL 기능으로 임계치 기반 탐지 정책의 한계를 극복합니다.

03

Brute Force 공격 방어

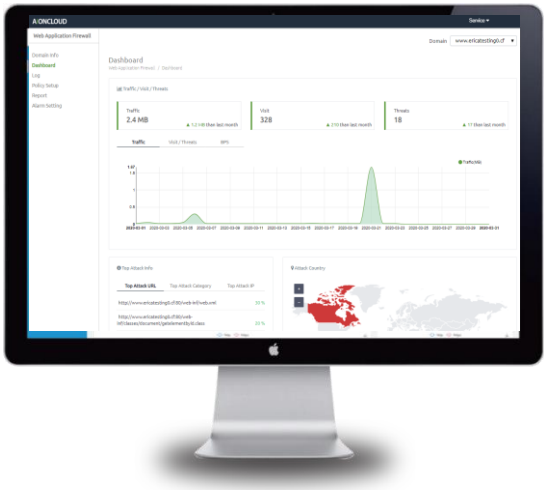
임계치 기반 정책으로 사용자의 대량 로그인 시도를 차단하고,
블랙리스트 IP로 등록합니다.



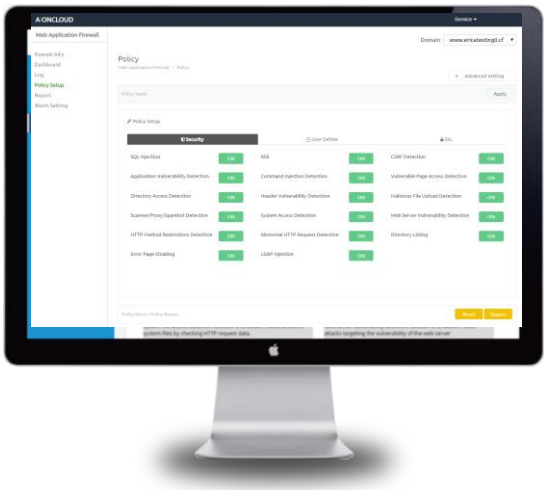
03 Website Protection

❖ AIONCLOUD WAF – 직관적이고 편리한 UI

- **Intuitive UI**
  - 사용자 친화적이고 직관적인 인터페이스 제공
  - 실시간 모니터링
  - 유형 별/ 시간 별/ 일자 별 로그 통계 및 보고 기능



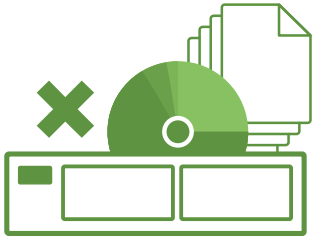
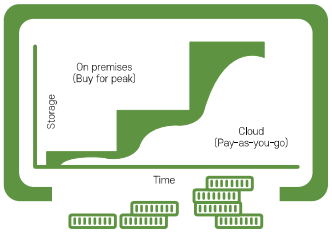
- **Simple Security Policy Setting**
  - Detect/Block/Bypass 운영모드 제공으로 운영의 편의성 제공
  - 웹공격 유형별 스위치 타입의 간편한 정책 설정 제공



03 Website Protection

❖ AIONCLOUD WAF-Cost Effective

- 5GB까지 무료 서비스
- Pay-as-you-go 가격 정책으로 사용한 만큼만 지불하는 종량제 서비스
- 별도의 하드웨어나 소프트웨어 설치 비용 절감
- 추가적인 초기 비용 불필요

Cost Reduction of WAF		
		
초기 비용 불필요 ☑	하드웨어 소프트웨어 설치 불필요 ☑	사용한 만큼만 요금 지불 ☑

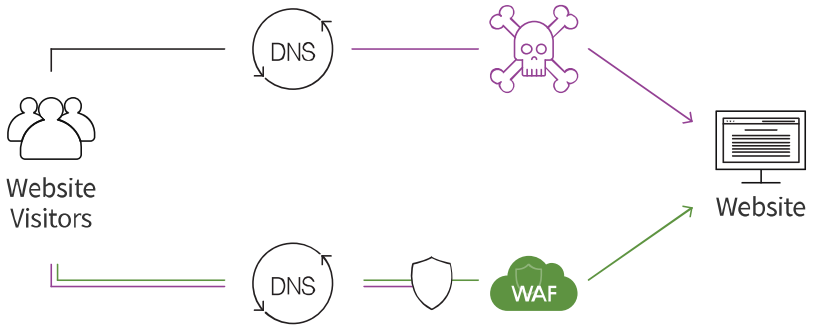
03 Website Protection

❖ AIONCLOUD WAF 이용 절차

1. 도메인 등록

- 대상 웹사이트 등록 (domain)
- 하나의 어카운트로 여러개의 웹사이트

2. DNS 변경 설정



- Domain Name은 웹사이트의 주소와 같은 역할을 하여 방문자는 도메인 주소를 이용하여 웹사이트에 접속 가능
- CNAME 변경을 통해 웹사이트의 주소를 AIONCLOUD의 주소로 변경하여 보안 적용
- Example of changing CNAME ▽

①WAF 서비스 신청 후 "210a7a86-.aioncloud.net"과 같은 WAF 전용 도메인 이름을 발급 받습니다.

②발행된 도메인 이름으로 CNAME을 변경합니다.

③CNAME 변경 후 바로 AIONCLOUD WAF 서비스를 이용할 수 있습니다.

3. 모니터링 & 관리

- 직관적 UI로 손쉬운 모니터링 & 정책 설정

03 Website Protection

❖ AIONCLOUD WMS(Website Malware Scanner)서비스

- 웹사이트의 악성코드를 탐지하는 진단 서비스
- 웹사이트를 정기적으로 방문하여 악성코드 감염을 진단하여 신속히 조기 대응하고 피해 최소화
- 정적 / 동적 분석 엔진 (MUD, Malicious URL Detection)을 사용하여 다단계 분석 실행

Multi-Level Inspection	Malware Awareness Service
정적/ 동적 분석을 통한 멀티 레벨 탐지/ 분석 기능으로 악성 코드 탐지율 강화	진단 결과 자동 보고서/ 알람 기능으로 침해사고 조기 대응 가능

1) 웹사이트 정기적 방문

2) 정적 분석을 통해 의심스러운 이벤트 발견

3) 동적 분석을 통해 악성코드의 실행 경로 탐지

4) 악성 URL 및 코드 추출

5) 웹사이트가 악성코드 유포지 / 경유지로 악용 여부 분석

6) 보고서/알림으로 분석결과 자동 전송

03 Website Protection

❖ AIONCLOUD WMS 악성코드 탐지 프로세스

- 정적 분석을 통해 발견된 의심스러운 이벤트는 동적 분석을 통해 심층적으로 악성코드 탐지
- 등록된 웹사이트 내의 깊이와 관계없이 모든 URL 검사
- 인코딩 및 난독화된 악성코드 분석
- 샌드박스 기술로 악성 사이트에 직접 방문하여 경유지 및 유포지 추적

STEP 01

사이트 방문하여 악성코드 검사

웹사이트를 정기적으로 신속히 방문하고 악성코드 감염을 진단하는 서비스

- 샌드박스 기술을 사용하여 악성 사이트를 직접 방문하여 악성코드를 추적합니다.
- 동적으로 신속히 대상 사이트 방문

STEP 02

MUD로 분석

MUD (Malicious ULR Detection) 엔진으로 정적 / 동적 분석

- 정적 분석을 통해 탐지된 의심스러운 이벤트는 동적 분석을 통해 심층적인 악성코드 탐지가 진행됩니다.
- 인코딩 되거나 난독화된 악성코드 분석
- 웹 취약점을 통한 Drive-by-down 이나 운영체제 이벤트를 통한 익스플로잇 탐지
- 등록된 웹사이트에 포함된 외부 링크 (링크된 광고 및 외부 스크립트 파일) 분석

STEP 03

자동 알림 및 공유

분석된 정보는 문자 / 이메일을 통해 보고서 및 알림의 형태로 전송됩니다.

- 악성 URL / 코드 추출
- 데이터 수집 및 저장
- 데이터 분석 및 시각화
- API 통한 데이터 공유

03 Website Protection

❖ AIONCLOUD WMS 이용 절차

1. 도메인 등록

- 보호할 웹사이트 (도메인) 등록
- 한 개의 계정에서 다수의 웹사이트 관리 가능

2. 진단 스케줄 설정

- 진단 주기 설정 (시간, 일, 주, 월 주기로 설정 가능)

3. 알림 설정

- 악성코드 탐지 알림 설정 (이메일 or SMS)

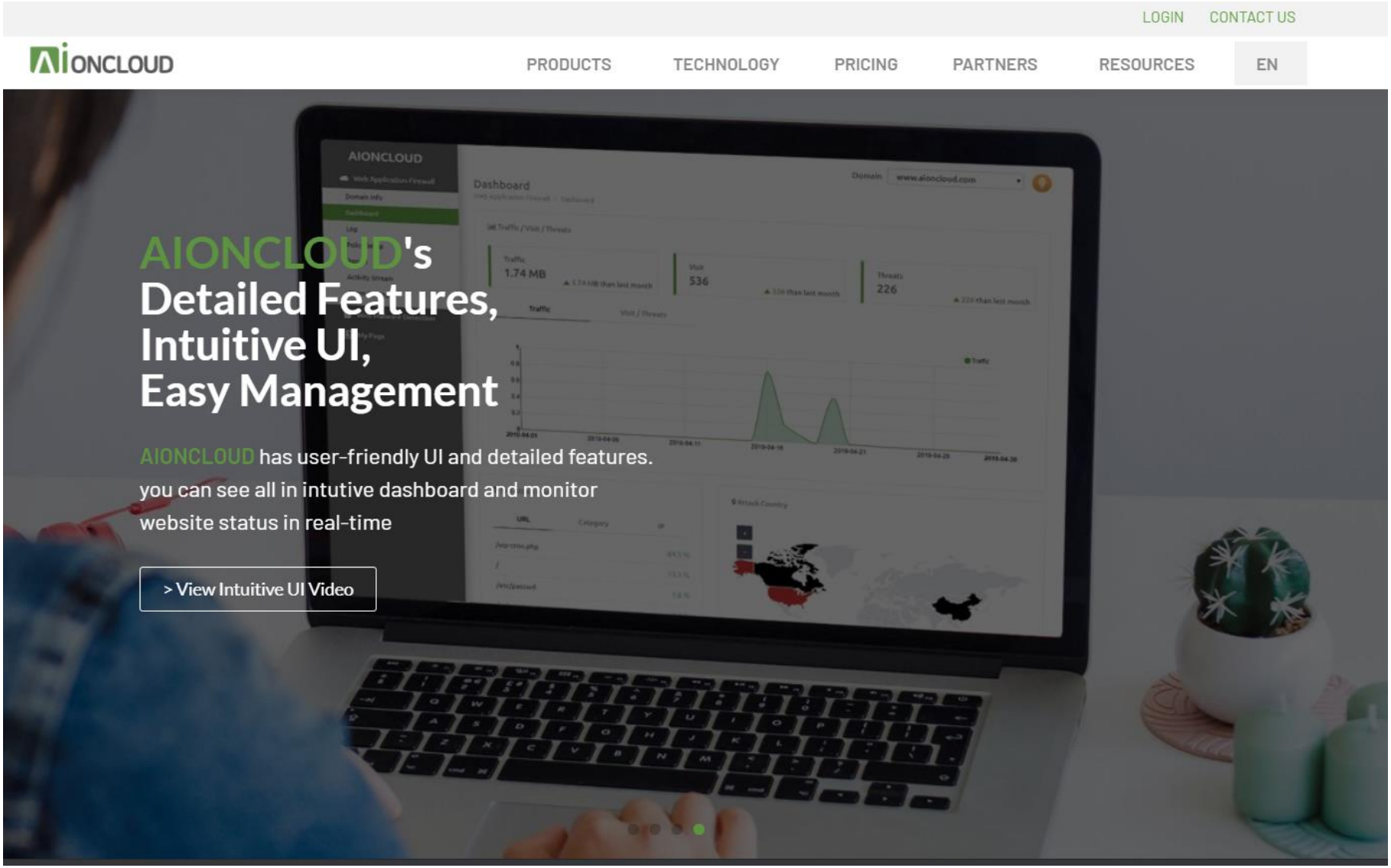
4. 모니터링 및 관리

- 직관적인 UI를 통한 쉬운 모니터링 및 정책 설정 가능

04

시연

04 AINCLOUD 서비스 시연



VIRTUAL
INTEGRATED
APPLICATION
SECURITY
FAIR **2021** (9th)

THANK YOU

AIONCLOUD

㈜모니터랩 | 주소 : 서울시 구로구 디지털로 27가길 27 아남빌딩 8,9층 08375 | Tel : 02-749-0799 | Fax : 02-749-0798 | Web : www.monitorapp.com
E-mail : sales@monitorapp.com | 사업자등록번호 : 214-87-66413