VIRTUAL
INTEGRATED
APPLICATION
SECURITY
FAIR 2021 (9th)

SASE & ZTA 기반의 Secure Internet Access

모니터랩 연구소
김 현 목 전무

MONITORAPP

CONTENTS

01

Covid19/Cloud 시대의 보안 환경 변화

01 Covid19/Cloud 시대의 보안 환경 변화

❖ Covid19로 인한 사무환경 변화와 보안위협 증가

위험도가 높은 APP과 웹사이트 접근이 Covid19 이전에 비해 161% 증가...

전체 인원의 **64%** 가 원격근무중

148% Covid19 이전에 비해 증가

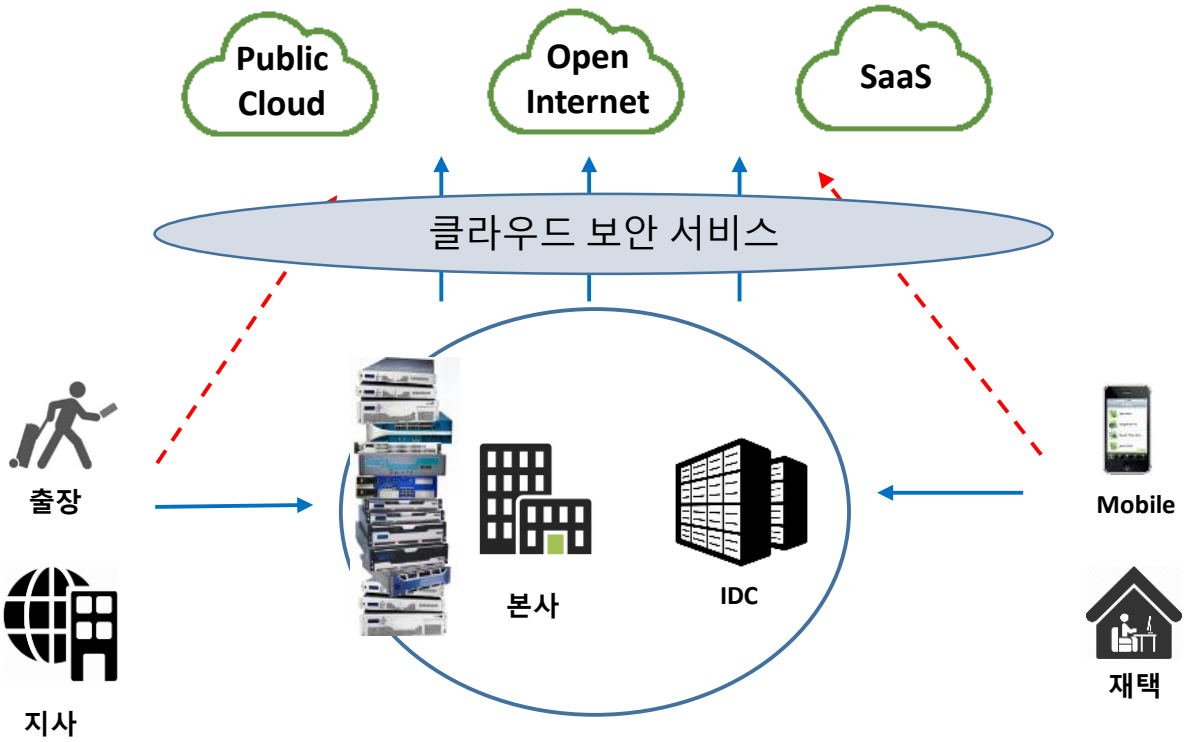
업무용 Device 개인용도 사용율 **97%**

80% 기업용 협업툴 사용율

-TechTarget 2020

01 Covid19/Cloud 시대의 보안 환경 변화

❖ 환경 변화에 따른 위협



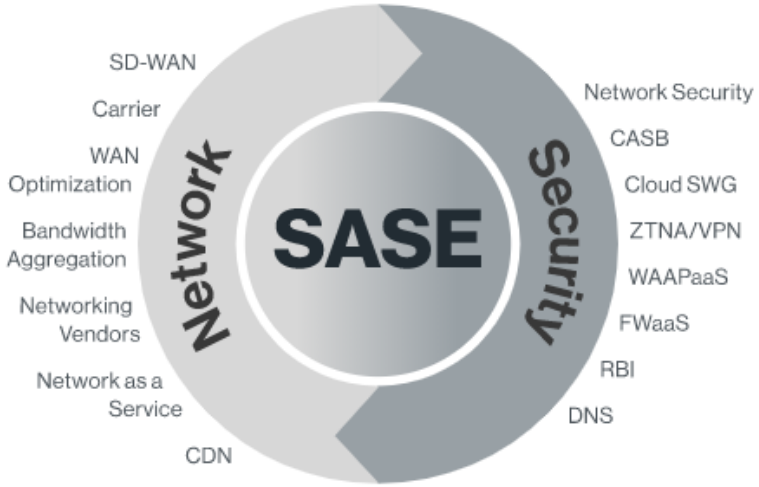
- 외부 외부 위협에 대한 경계선 방어
- 내부에 위치한 네트워크 자원
- 내부자의 위협으로부터 보호

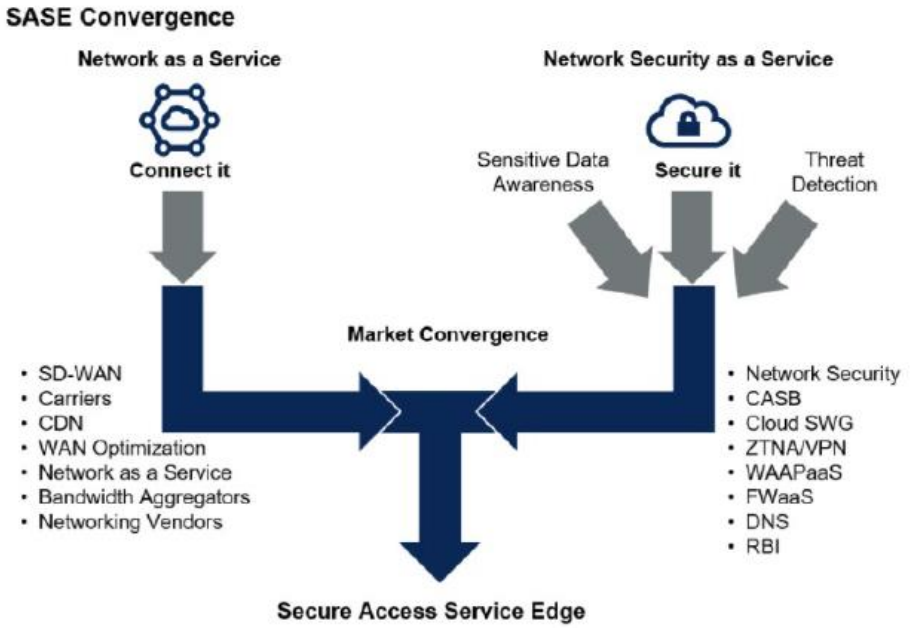
- 리모트 접속이 기본
- 기업 내 외부에 워크로드 위치
- 조직별로 사용하는 인프라 사이
- Multi Cloud 인프라 사용

01 COVID19/CLOUD시대의 보안환경 변화

❖ ~as-a-Service와 SASE(Secure Access Service Edge)의 활용

- SASE는 클라우드와 식별된 사용자 ID 기반의 네트워킹/보안 통합 아키텍처
- SASE를 통해 Security Anywhere 서비스 가능





-Gartner 2019

01 COVID19/CLOUD시대의 보안환경 변화

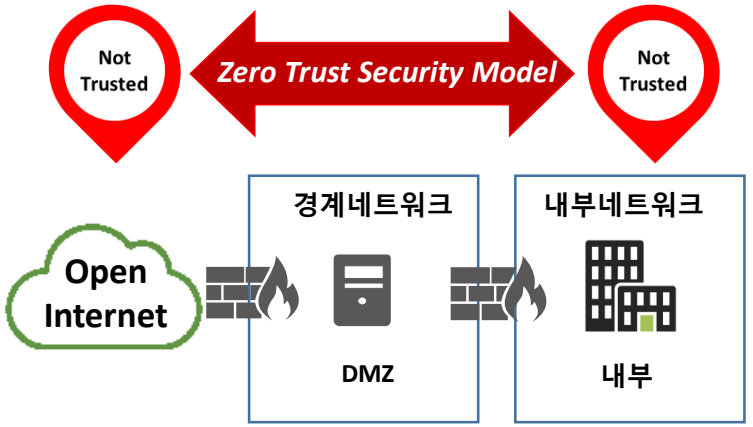
❖ ~as-a-Service와 SASE(Secure Access Service Edge)의 활용

- 네트워크 중심 → 사용자 중심으로
- 네트워크 보안 → 사용자 보안
- 보안기능 중심 → 정책관리 중심
- 보안 장비 별 관리 --> 서비스 및 정책 통합관리

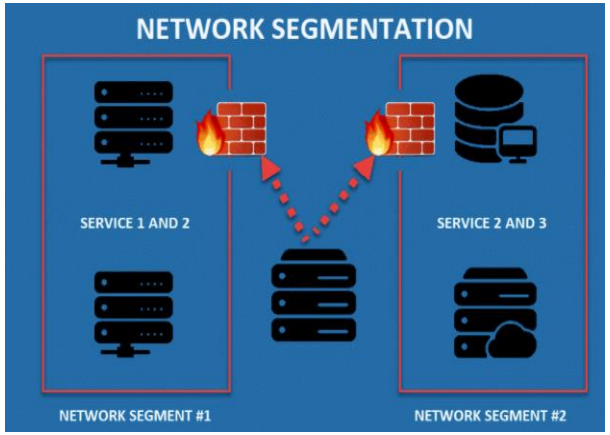
01 COVID19/CLOUD시대의 보안환경 변화

❖ ZTA (Zero Trust Access)

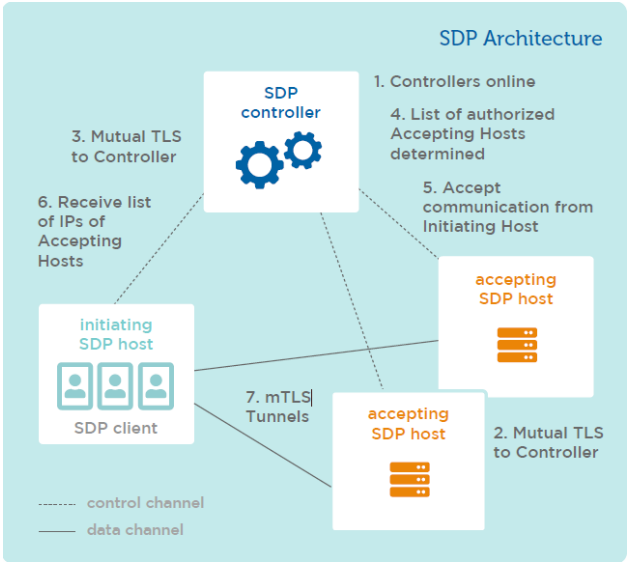
- ZT (Zero Trust) : 모든것을 신뢰하지 않는다
- ZTA (Zero Trust Access) : 네트워크에 접근하는 사람과 기기
- ZTNA (Zero Trust Network Access) : 애플리케이션 접근 중점



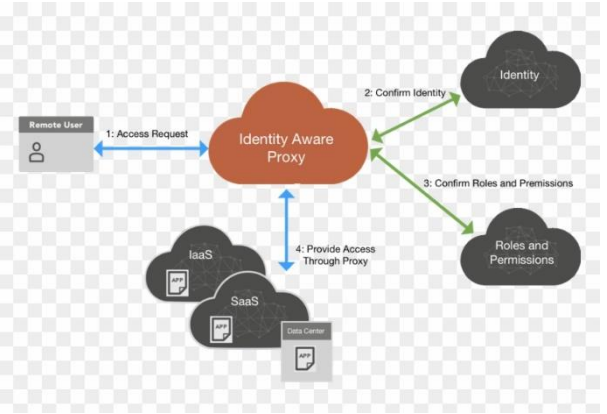
❖ Network Segmentation



❖ SDP(Software Defined Perimeters)



❖ IAP(Identify Aware Proxys)



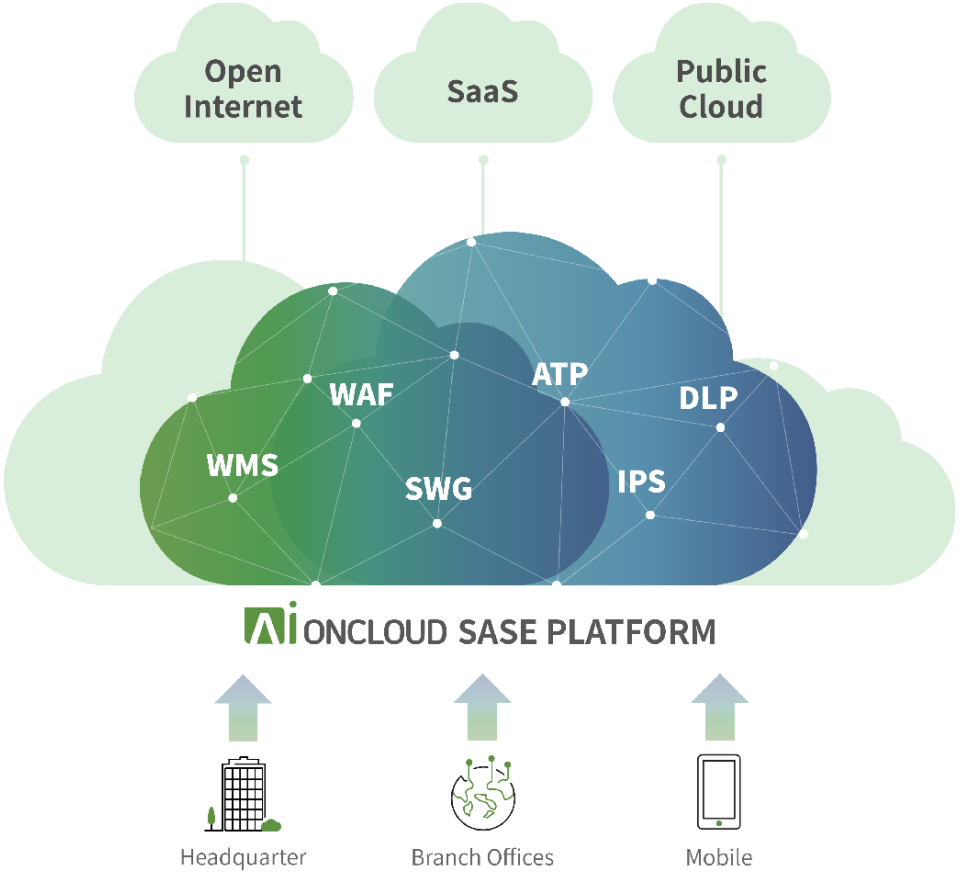
02

모니터랩 SASE 플랫폼 AIONCLOUD

02 모니터랩 SASE 플랫폼 AIONCLOUD

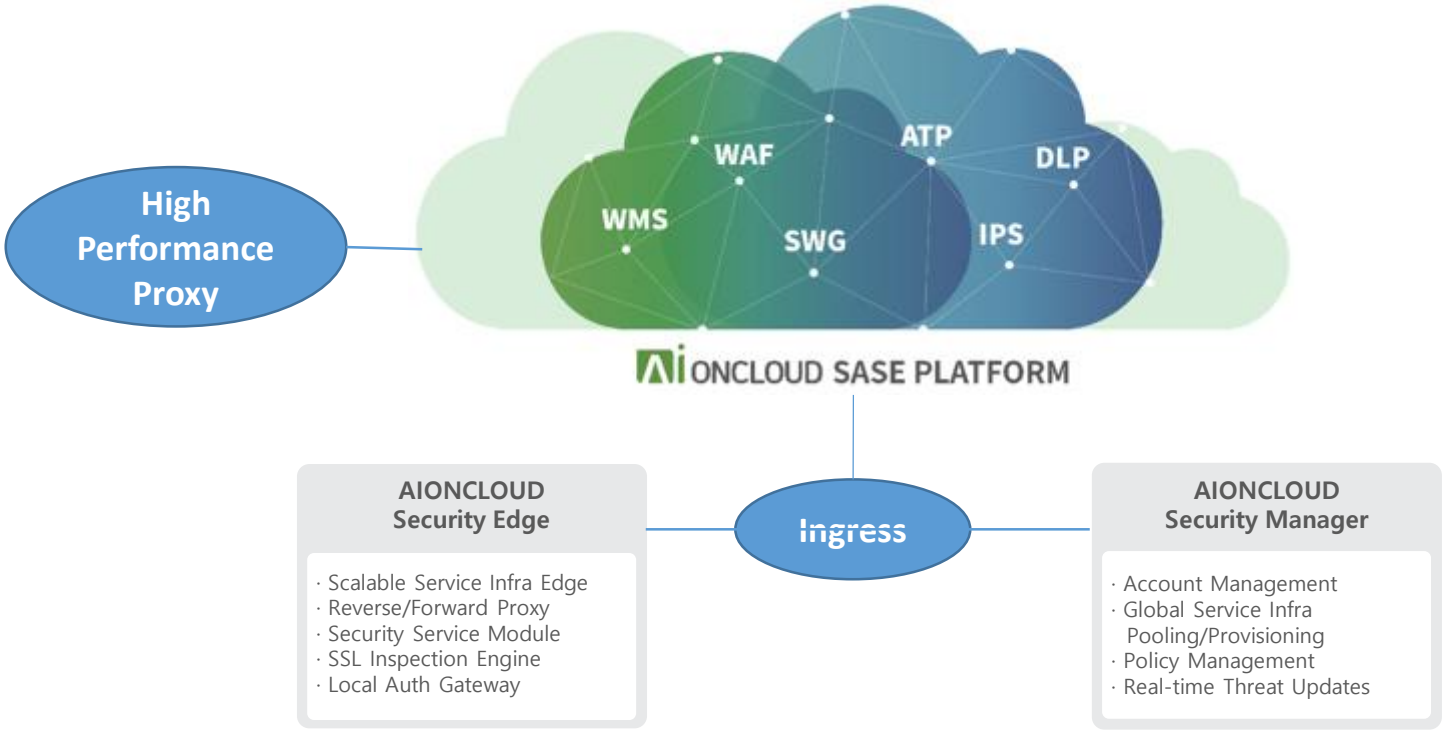
❖ AIONCLOUD (Application Insight on Cloud)

- AIONCLOUD는 모니터랩이 제공하는 SASE(Secure Access Service Edge) 플랫폼
- 인공지능 기술이 결합된 Threat Intelligence 기반의 Full Stack 네트워크 보안 서비스 제공 목표



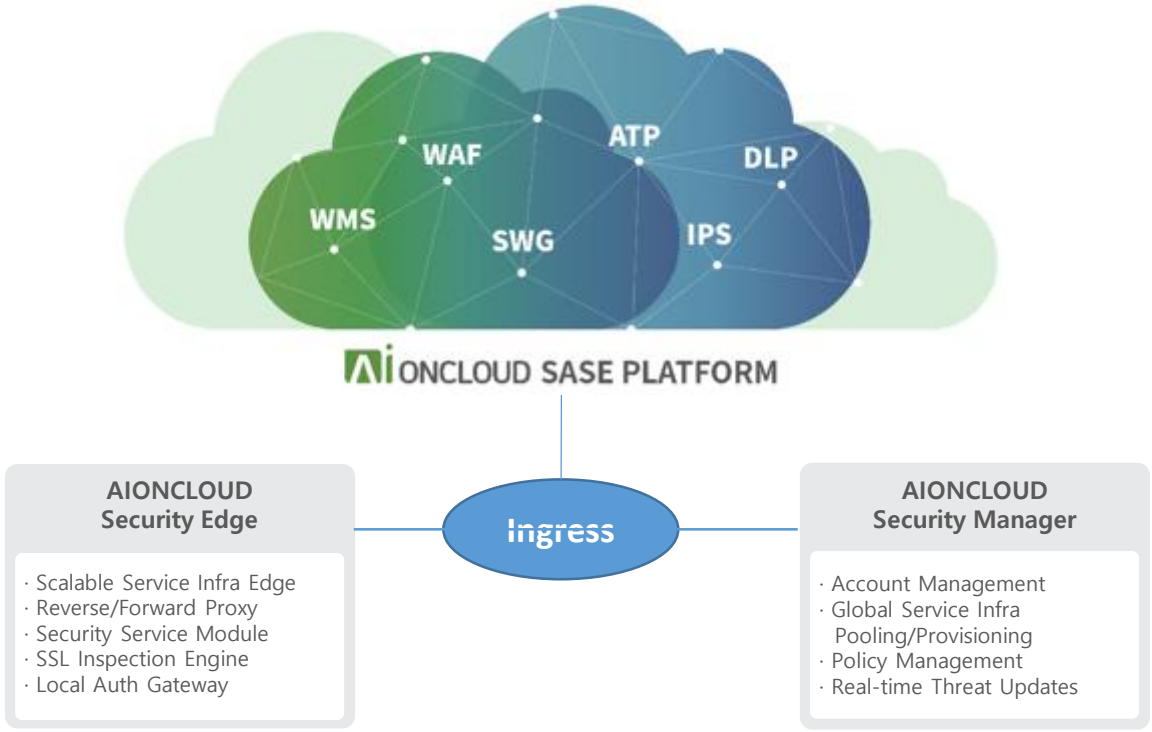
02 모니터랩 SASE 플랫폼 AIONCLOUD

❖ AIONCLOUD (Application Insight on Cloud)



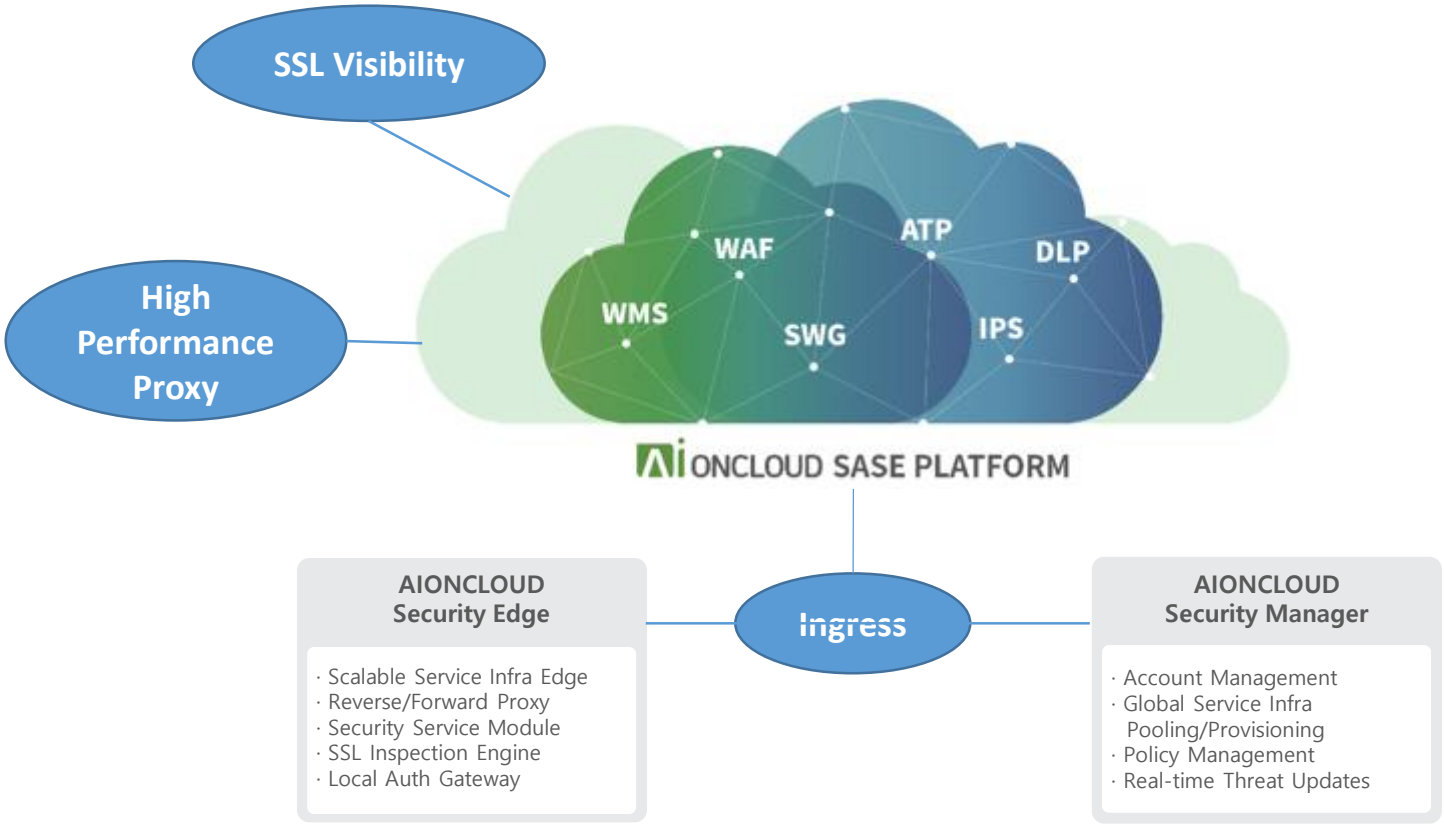
02 모니터랩 SASE 플랫폼 AIONCLOUD

❖ AIONCLOUD (Application Insight on Cloud)



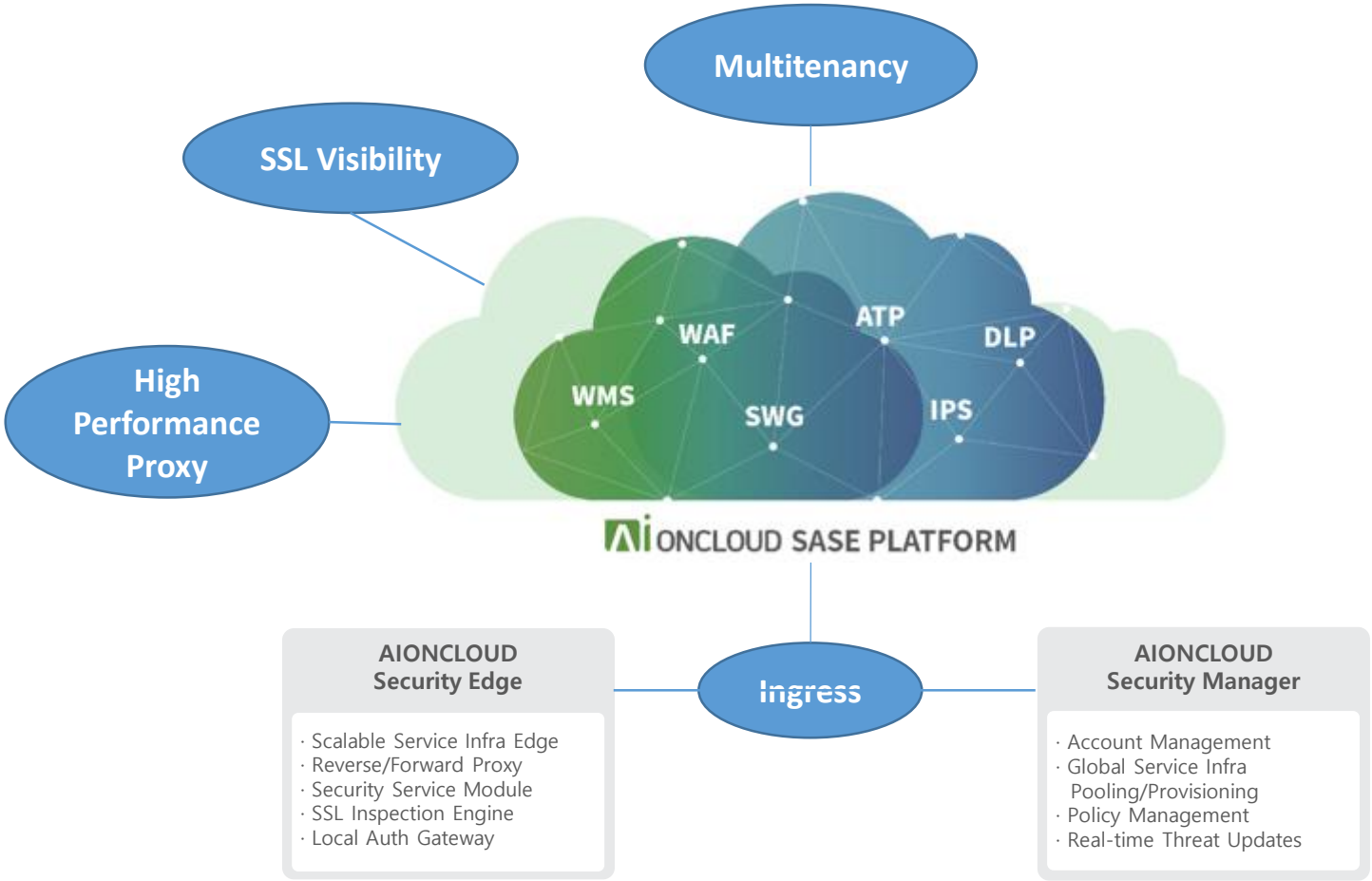
02 모니터랩 SASE 플랫폼 AIONCLOUD

❖ AIONCLOUD (Application Insight on Cloud)



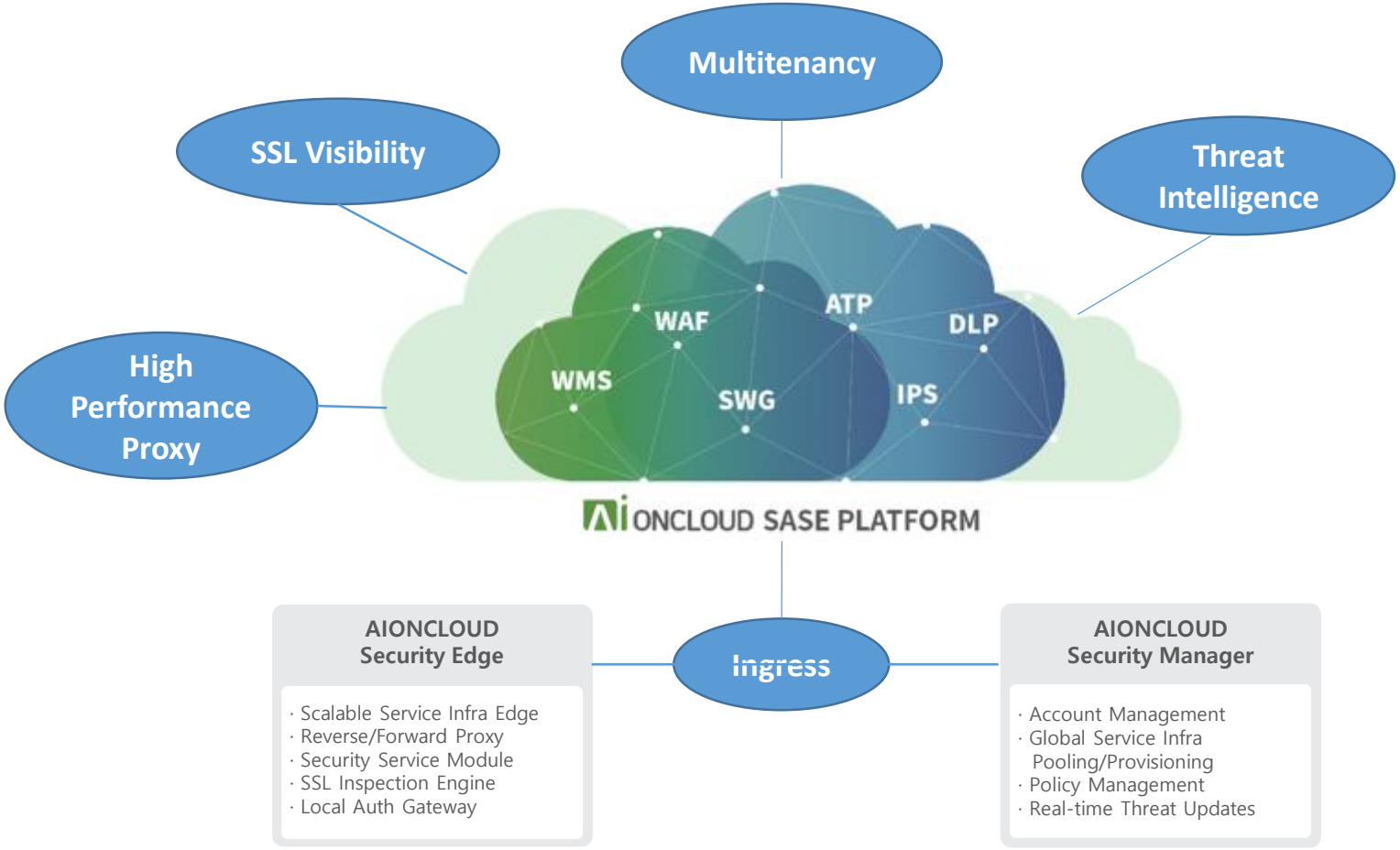
02 모니터랩 SASE 플랫폼 AIONCLOUD

❖ AIONCLOUD (Application Insight on Cloud)



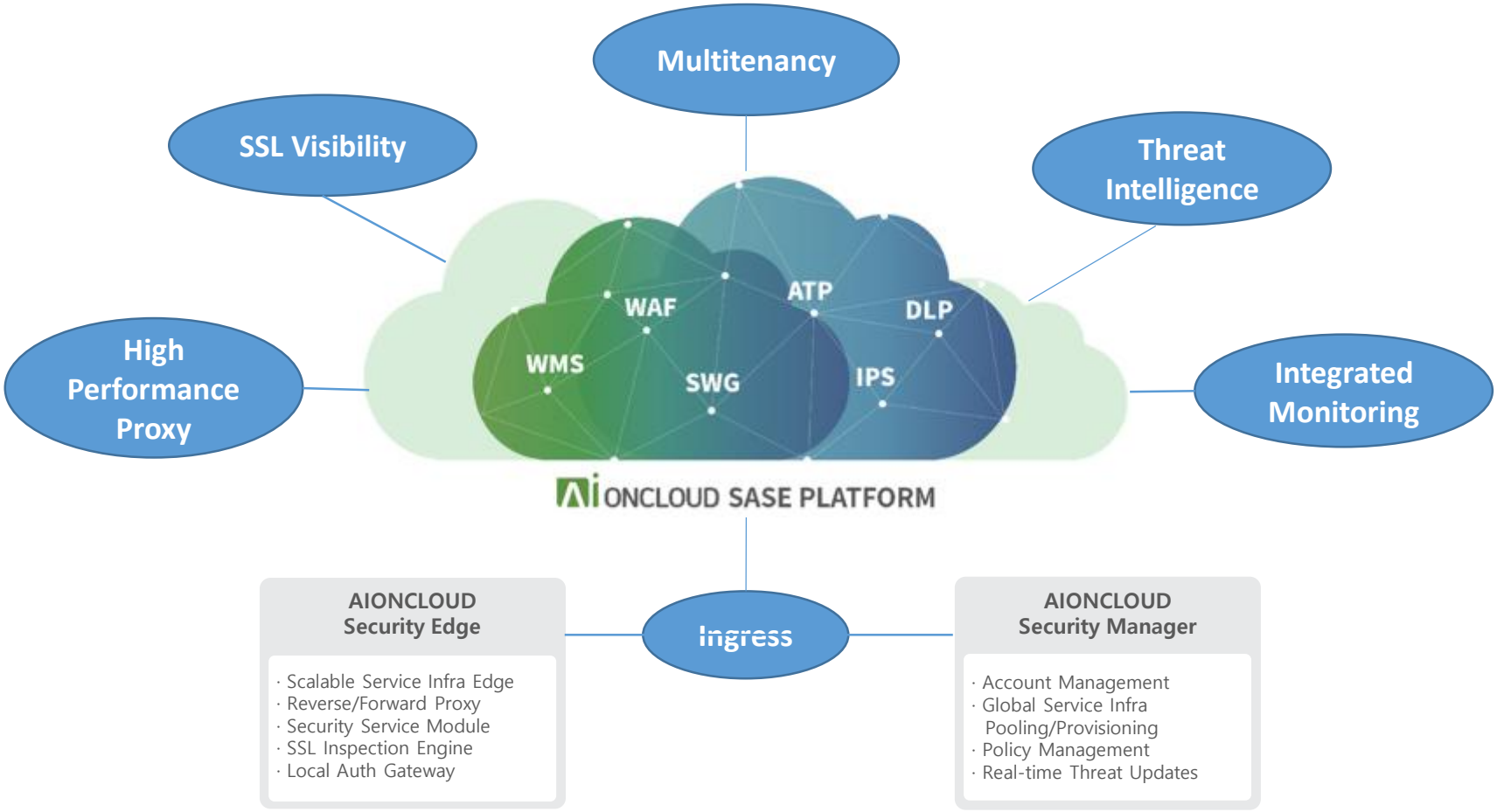
02 모니터랩 SASE 플랫폼 AIONCLOUD

❖ AIONCLOUD (Application Insight on Cloud)



02 모니터랩 SASE 플랫폼 AIONCLOUD

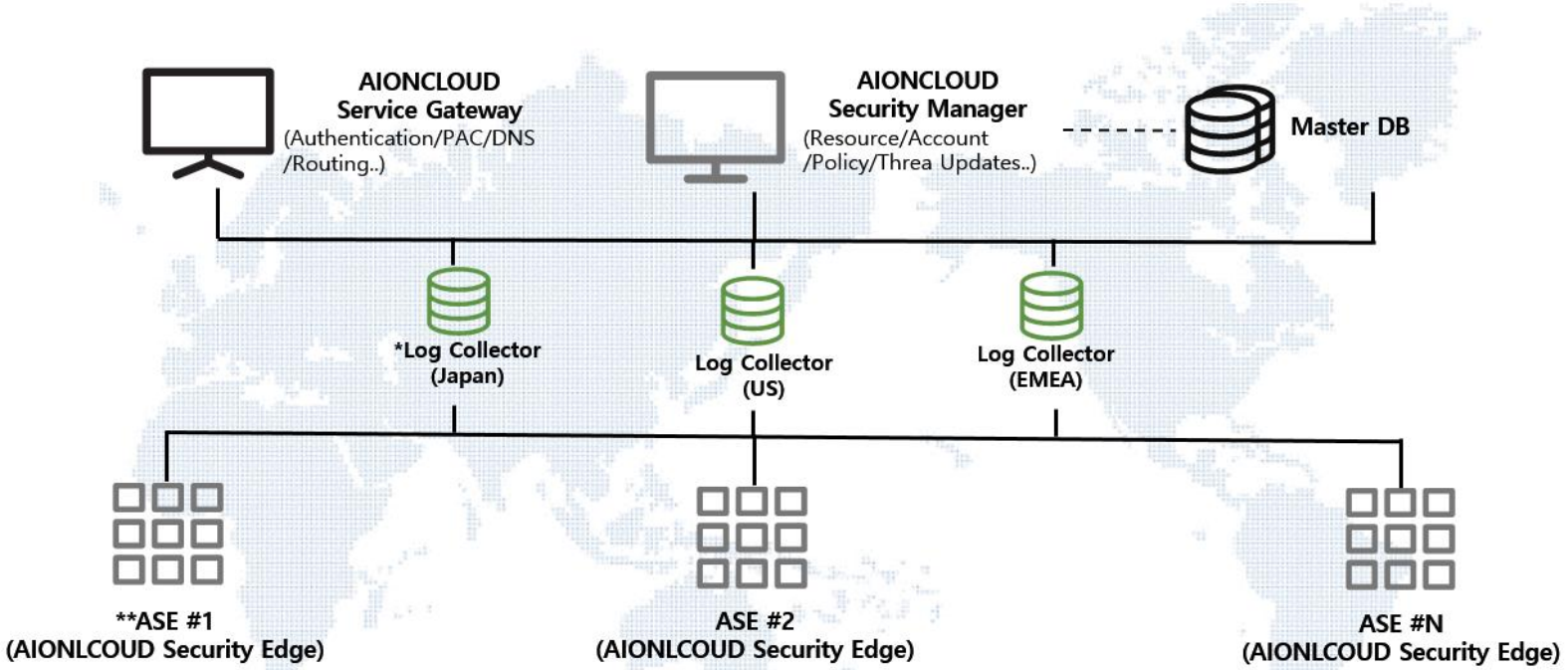
❖ AIONCLOUD (Application Insight on Cloud)



02 모니터랩 SASE 플랫폼 AIONCLOUD

❖ AIONCLOUD 플랫폼 구성

AIONCLOUD Service Gateway / Security Manager / Security Edge



02 모니터랩 SASE 플랫폼 AIONCLOUD

❖ AIONCLOUD에서 제공하는 보안 서비스

- **Website Protection**
  - Open된 기업 내부 웹 기반 시스템에 대한 보안 서비스 제공
- **Secure Internet Access**
  - 내부 사용자의 안전한 외부 인터넷 사용을 지원하는 보안 서비스 제공

Web Application Firewall

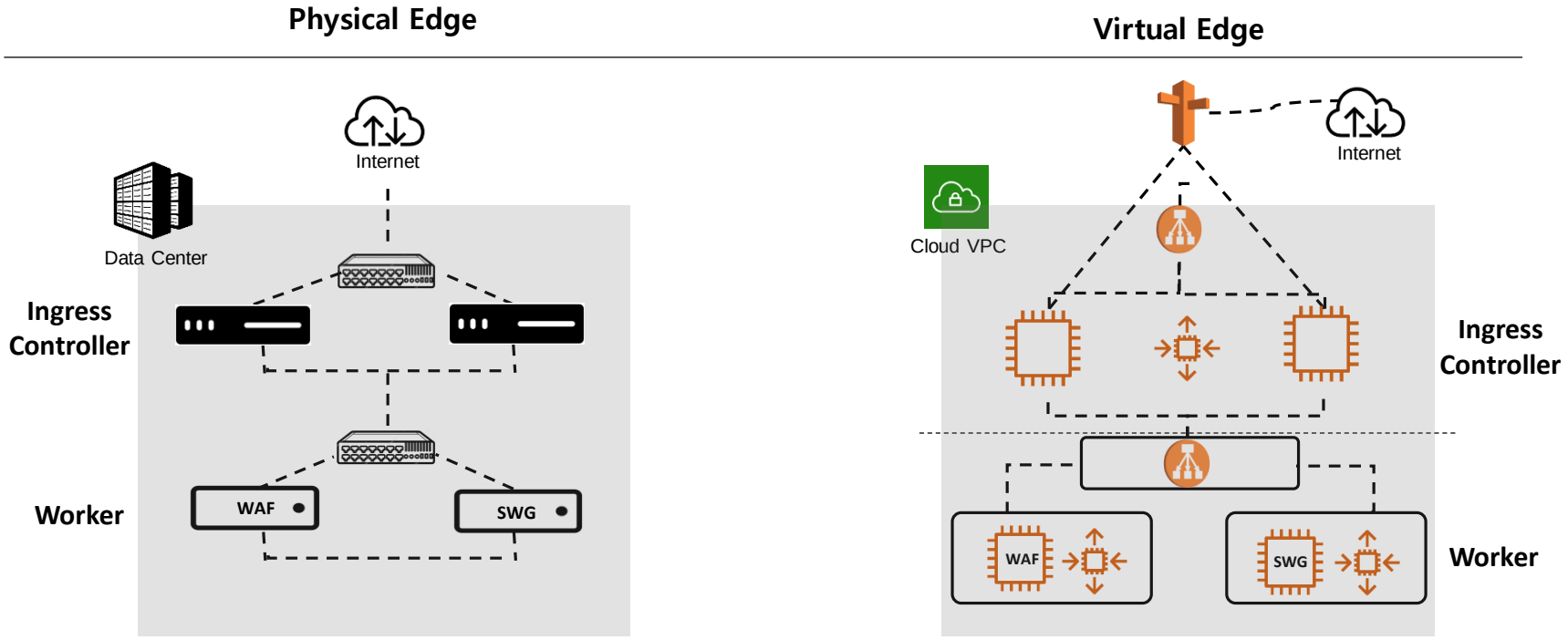
Website Malware Detection

Secure Web Gateway

02 모니터랩 SASE 플랫폼 AIONCLOUD

❖ AIONCLOUD Security Edge

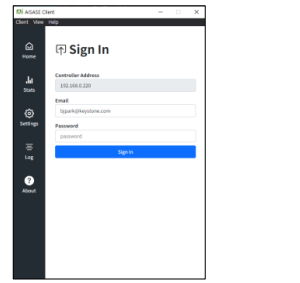
- Container Based Physical or Virtual Edge, AIONCLOUD Edge / White Label Partner Edge

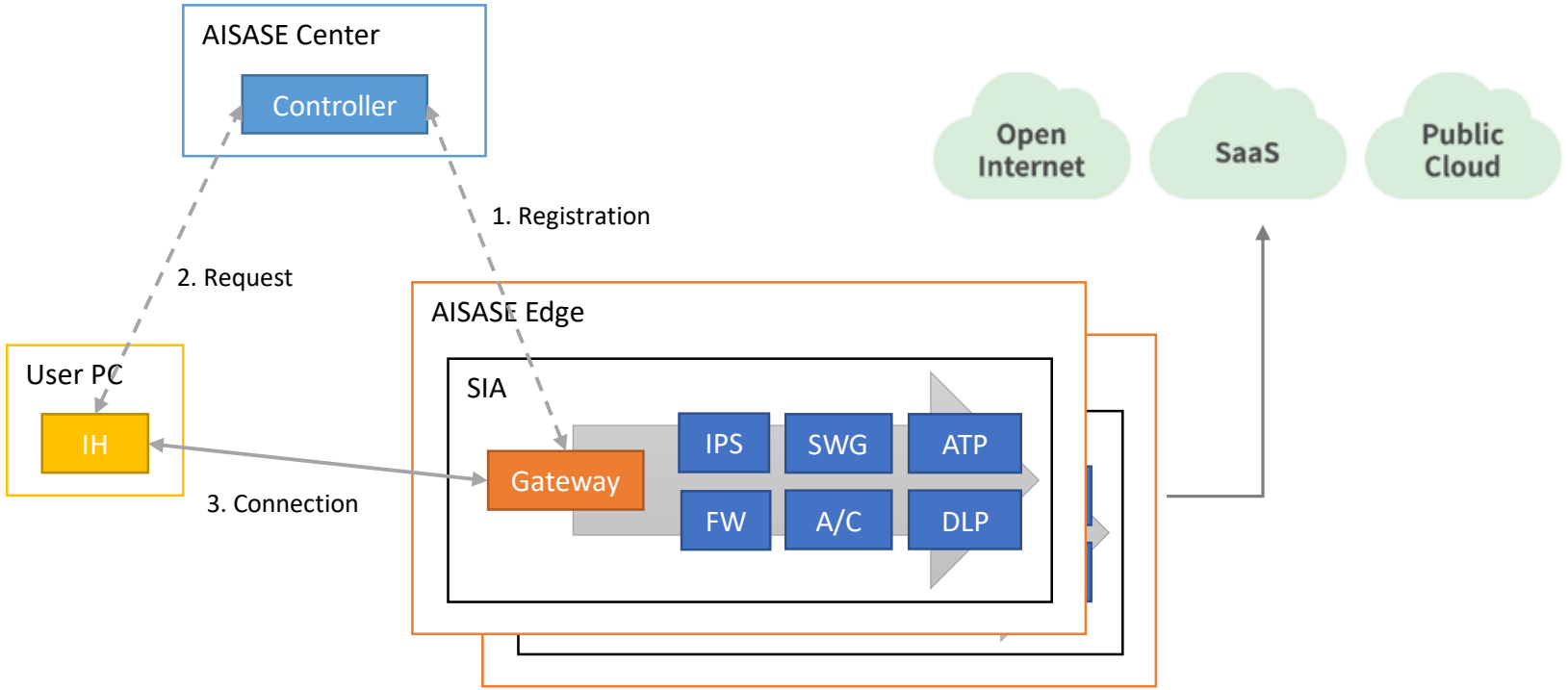


02 모니터랩 SASE 플랫폼 AIONCLOUD

❖ ZTA 기반 Secure Internet Access

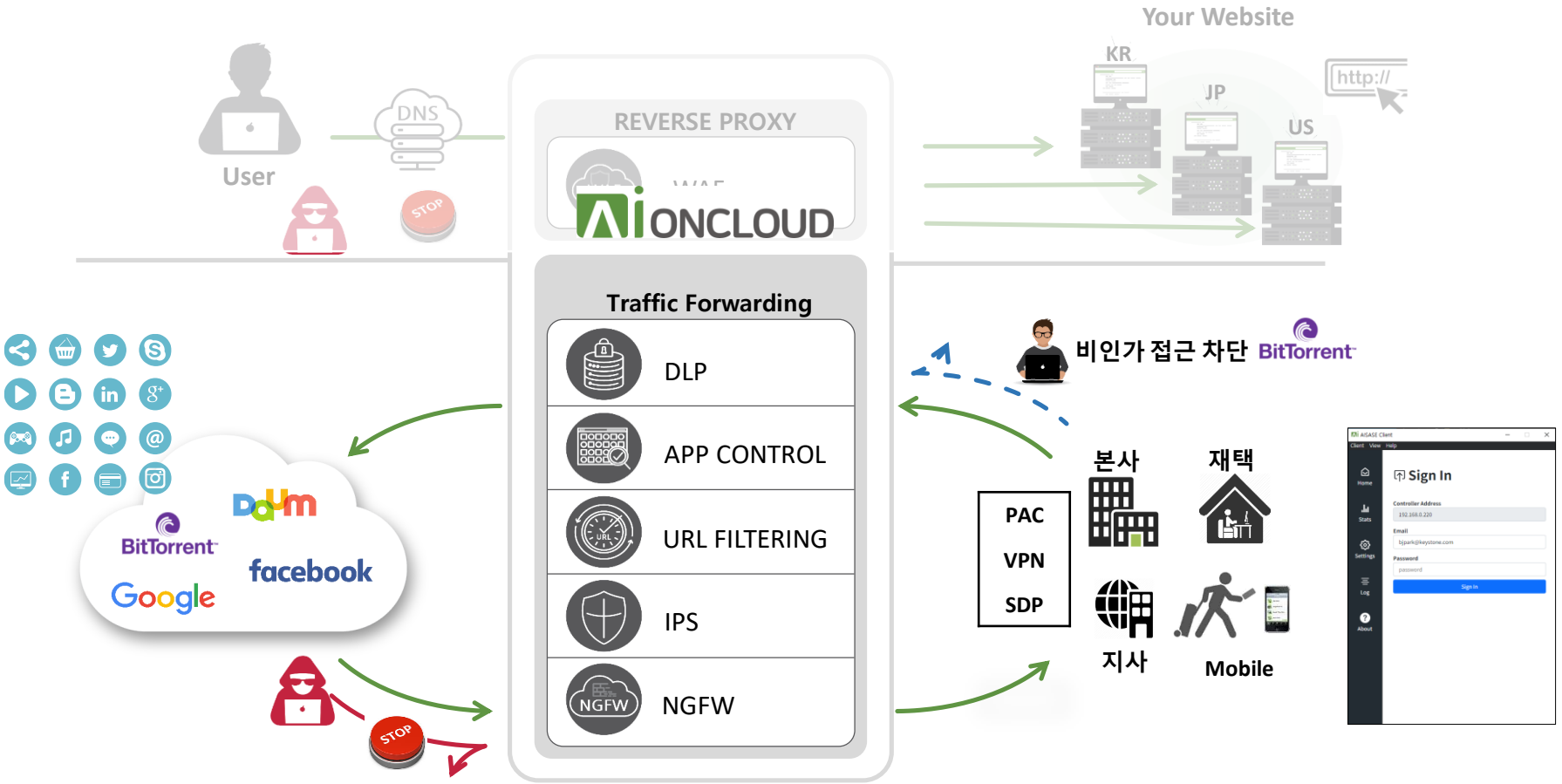
- SDP 를 통한 Zero trust Network Access 구현
- Single Packet Authorization 를 사용하여 Client(IH), Controller, AH간 인증에 사용.





02 모니터랩 SASE 플랫폼 AIONCLOUD

❖ AIONCLOUD(Application Insight on Cloud)서비스 트래픽 Flow



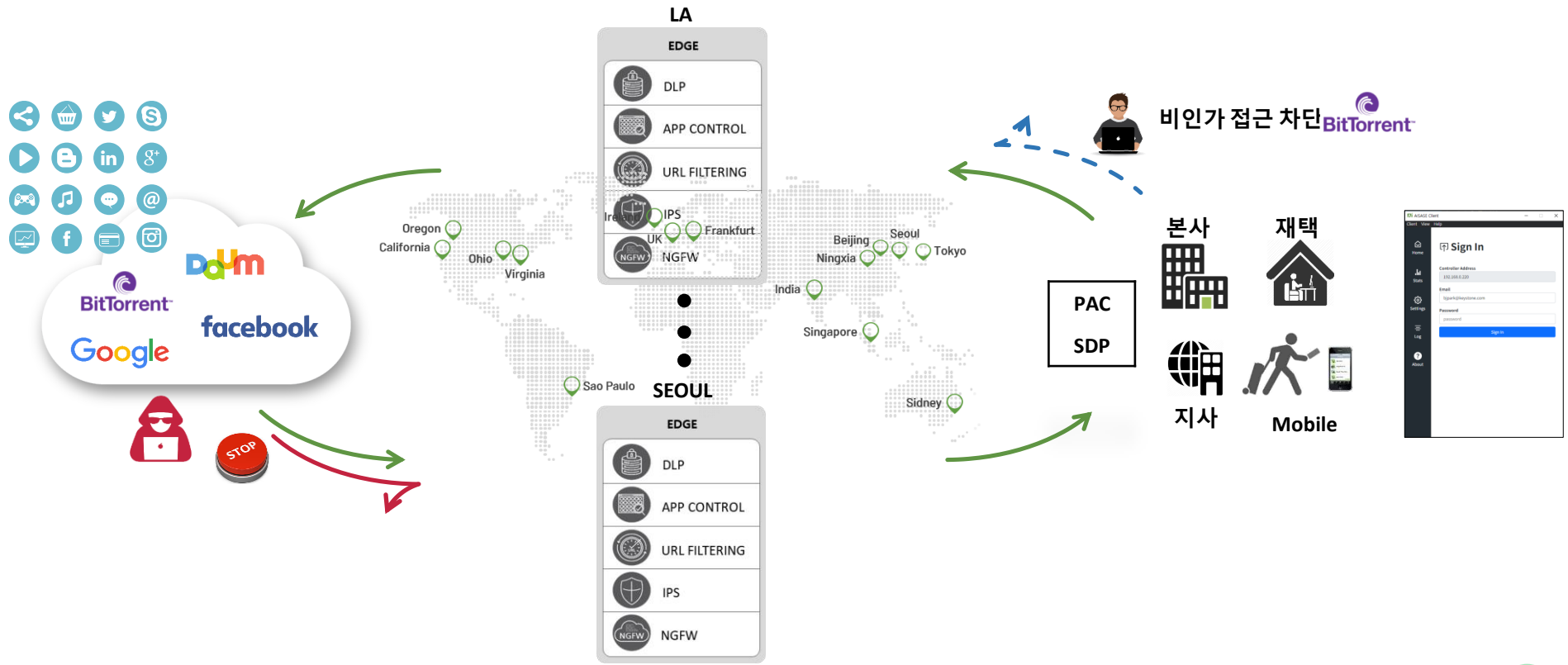
03

ZTA 기반 Secure Internet Access

03 ZTA 기반 Secure Internet Access

❖ Secure Internet Access Service

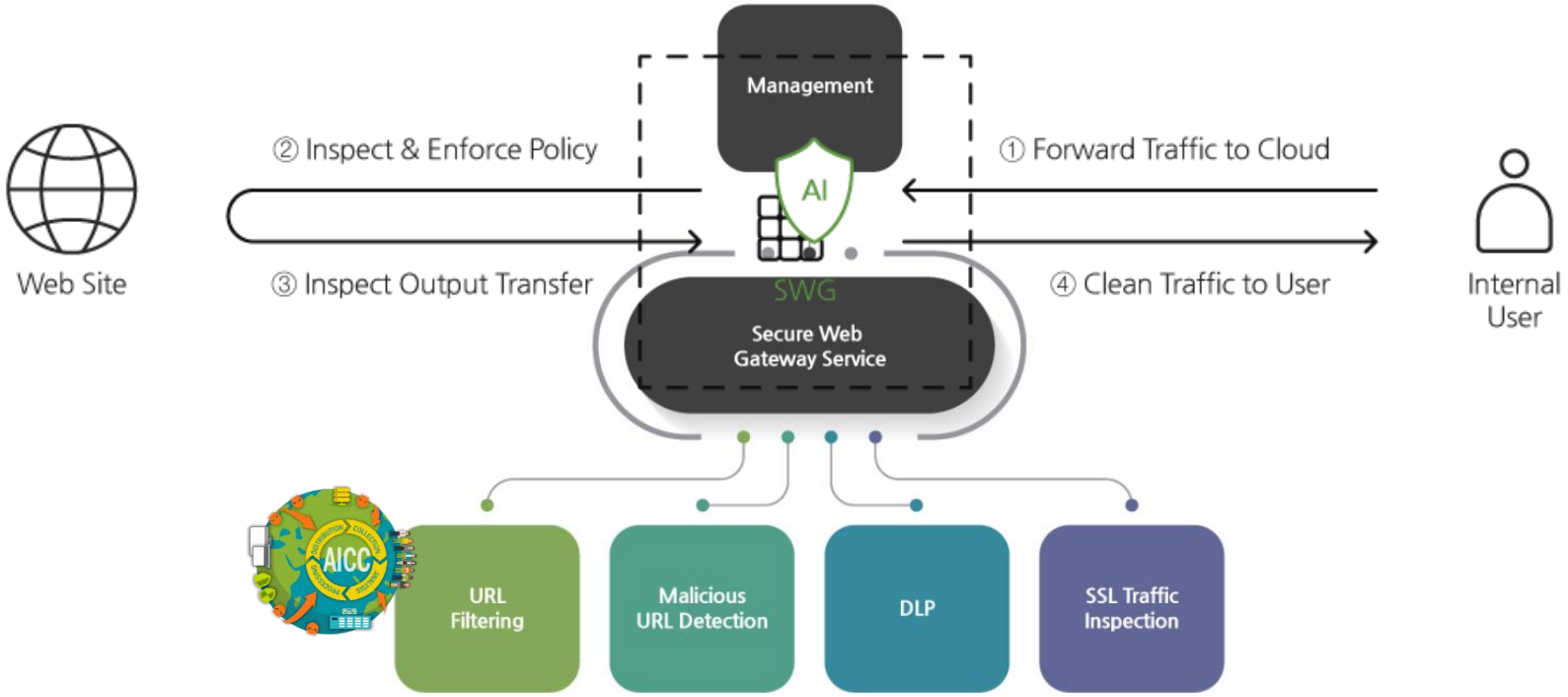
- 사용자가 외부 인터넷 이용 시 발생할 수 있는 보안 위협을 제거 및 방어
- SDP(Software Defined Perimeter) / SWG(Secure Web Gateway) / NGFW 등의 서비스로 구성.
- ZTA 를 통해 언제 어디서든 일관된 보안 서비스 제공 및 이용 가능



03 ZTA 기반 Secure Internet Access

❖ AIONCLOUD SWG 주요 보안기능

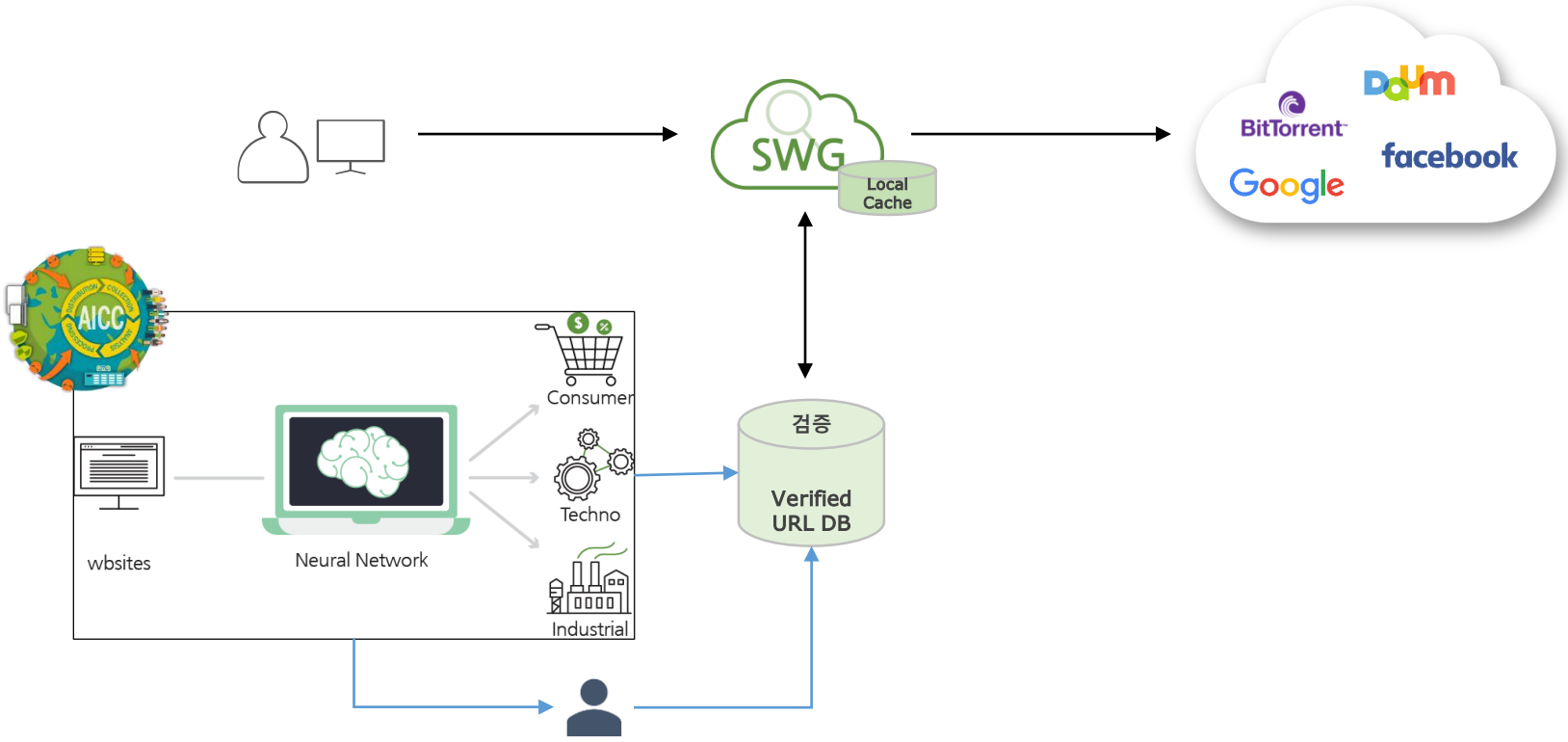
- URL 카테고리 필터링
- 악성 사이트 필터링 및 악성 코드 탐지
- 정보유출방지 (압축파일 및 파일첨부를 통한 개인정보 등 기업비밀 자료 유출 방지)
- HTTPS 트래픽 제어(SSL 가시성 제공, SSL Pinning 사이트 Bypass, 인증서 자동배포)



03 ZTA 기반 Secure Internet Access

❖ AIONCLOUD SWG 주요 보안기능

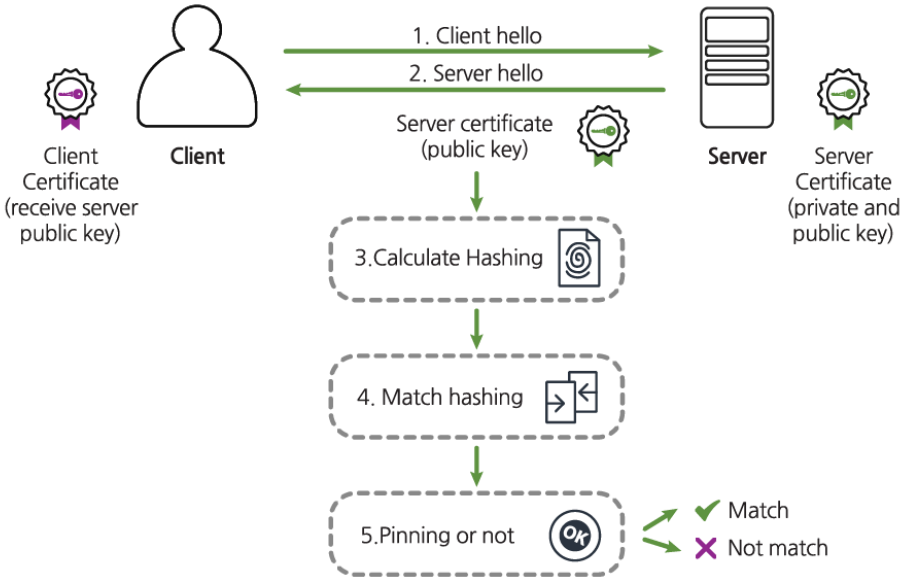
- 머신러닝 기반 카테고리 자동 분류 및 탐지 (Threat Intelligence : AICC)
- 악성 URL 및 악성 파일 탐지 및 차단



03 ZTA 기반 Secure Internet Access

❖ AIONCLOUD SWG 주요 보안기능

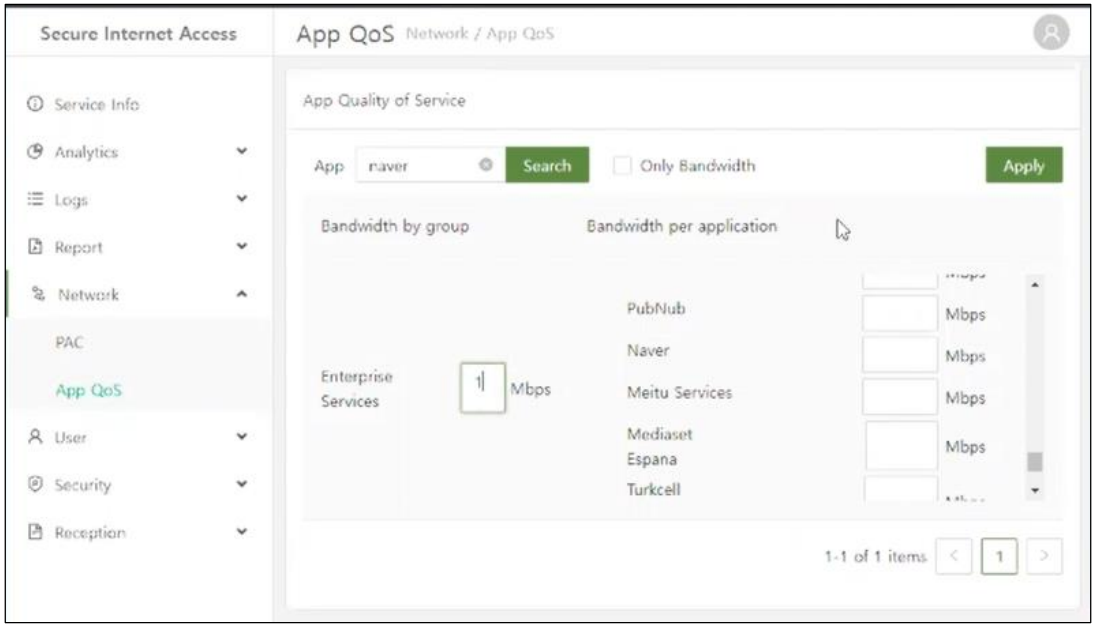
- HTTPS 복호화를 위해 AISWG가 통신에 개입하는 경우 인증서 고정으로 인해 정상적인 통신 불가
- AISWG가 제공한 공개 키와 클라이언트 애플리케이션에 내장된 공개키가 불일치 하여 MITM 공격으로 간주
- PKP List를 정기적으로 업데이트하여 해당 목적지 트래픽에 대한 선택적 바이패스

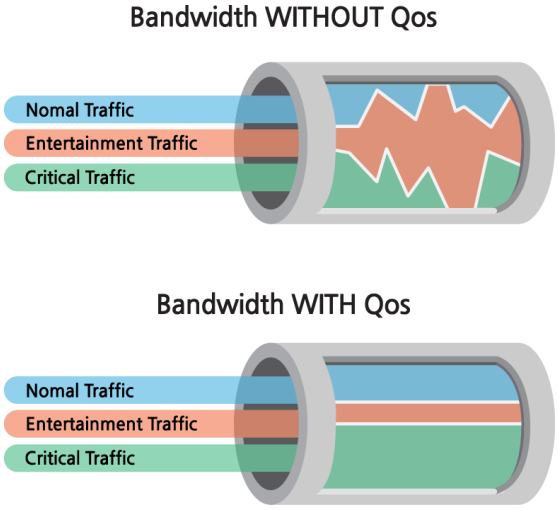


03 ZTA 기반 Secure Internet Access

❖ AIONCLOUD SWG 주요 보안기능

- Application 과 그룹에 대해 사용자 그룹별, 사용자별 대역폭 제어 기능
- 사용자에 따른 Application 별 사용량 제어
- Application 별 QoS 대역폭 제한 설정





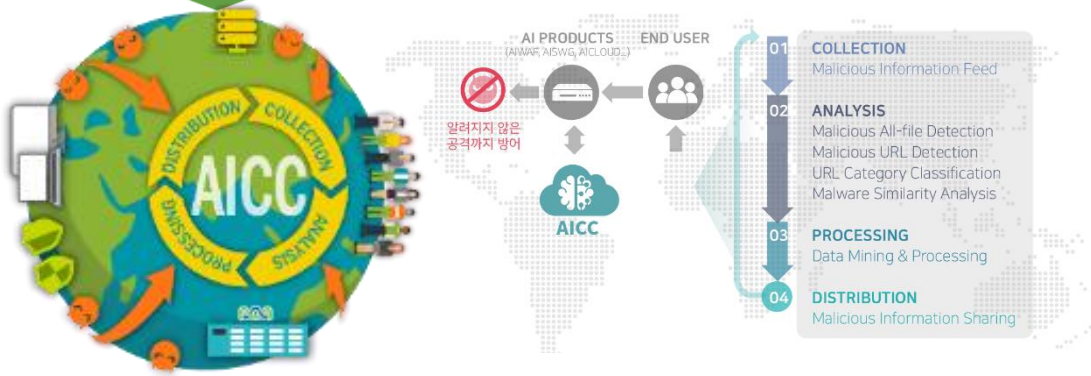
03 ZTA 기반 Secure Internet Access

❖ AIONCLOUD Threat Intelligence Platform(AICC : Application Insight Cloud Center)

모니터랩 보안 인텔리전스 AICC는 지능적이고, 변종의 알려지지 않은 공격에 대응하기 위해 AI(인공지능)엔진을 기반으로 전세계 위협정보를 수집-분석-가공하여 패턴 시그니처 정보와 함께 신뢰성 높은 보안 서비스를 가능하게 합니다.

MUD	UCC	MAD	MSA
(Malicious URL Detection) 실 사이트 고속 동적 방문해 악성 URL 수집, 분석, 가공, 탐지	(URL Category Classification) URL 및 도메인에 대해서 분석을 통해 지정된 카테고리로 분류하는 시스템	(Malicious All File Detection) 웹 페이지에 첨부된 파일 등을 동적으로 분석해 악성코드를 포함한 악성 파일 식별	(Malicious Similarity Analysis) 대상 파일과의 유사도 분석을 통해 신종·변종 unknown 파일 탐지

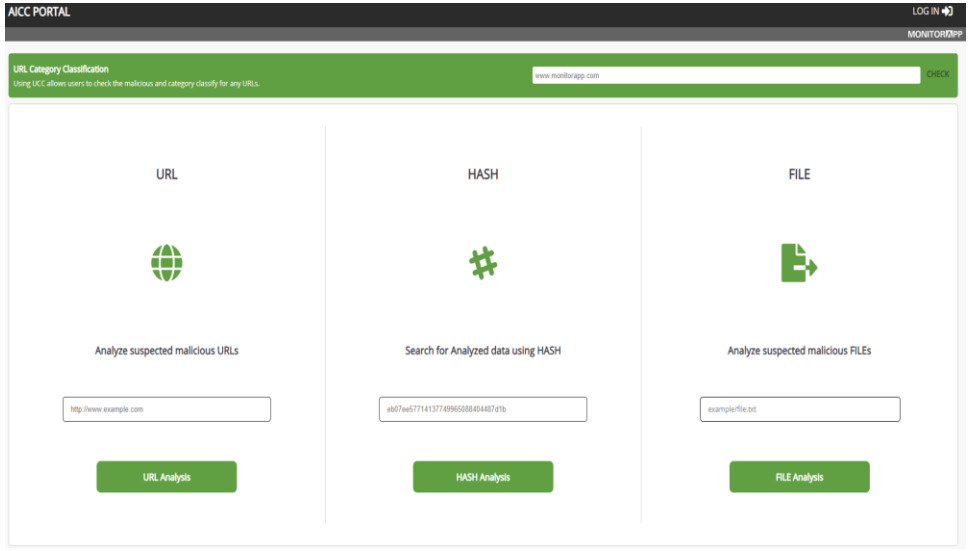
위협 인텔리전스 플랫폼 AICC (Application Insight Cloud Center)

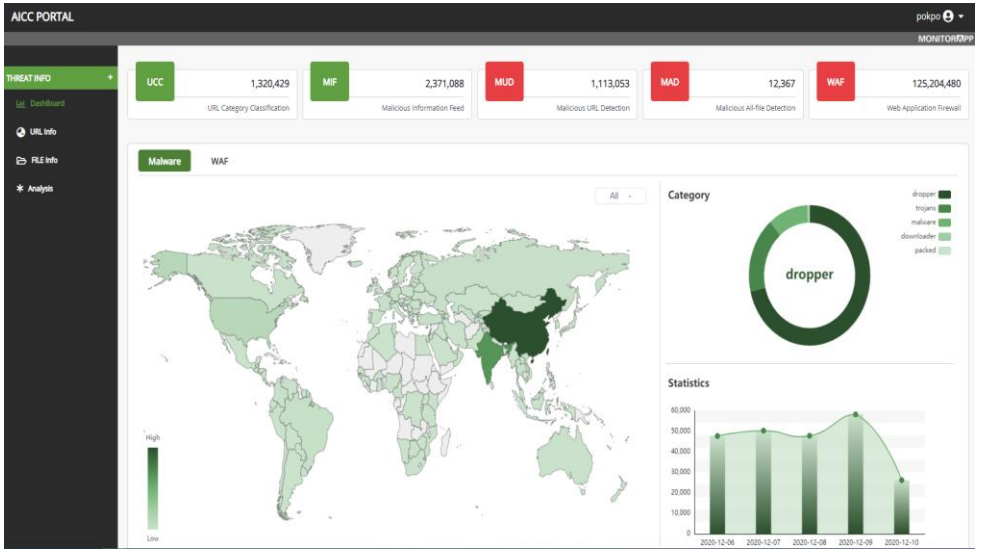


03 ZTA 기반 Secure Internet Access

❖ AIONCLOUD Threat Intelligence Platform(AICC : Application Insight Cloud Center)

Google VIRUSTOTAL



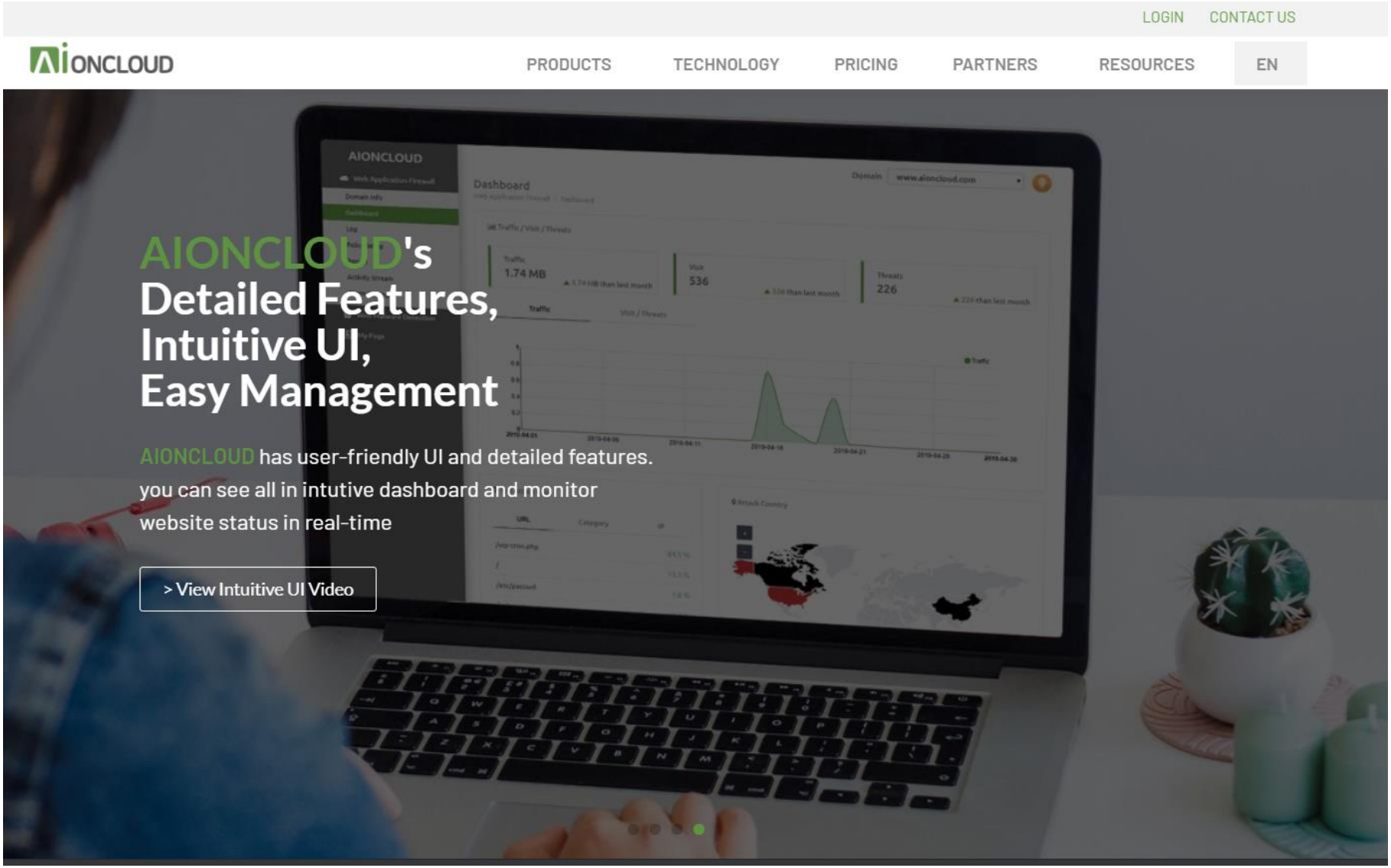


https://aicc.monitorapp.com

04

AIONCLOUD 서비스 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