VIRTUAL
INTEGRATED
APPLICATION
SECURITY
FAIR 2020 (8th)

AiONCLOUD Website Protection & Secure Internet Access

01 | 모니터랩 | 윤승원 상무

MONITORAPP

CONTENTS

01 COVID19/CLOUD시대의 보안환경 변화

❖ Covid19로 인한 사무환경 변화와 보안위협 증가

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

전체 인원의 **64%** 가 원격근무중

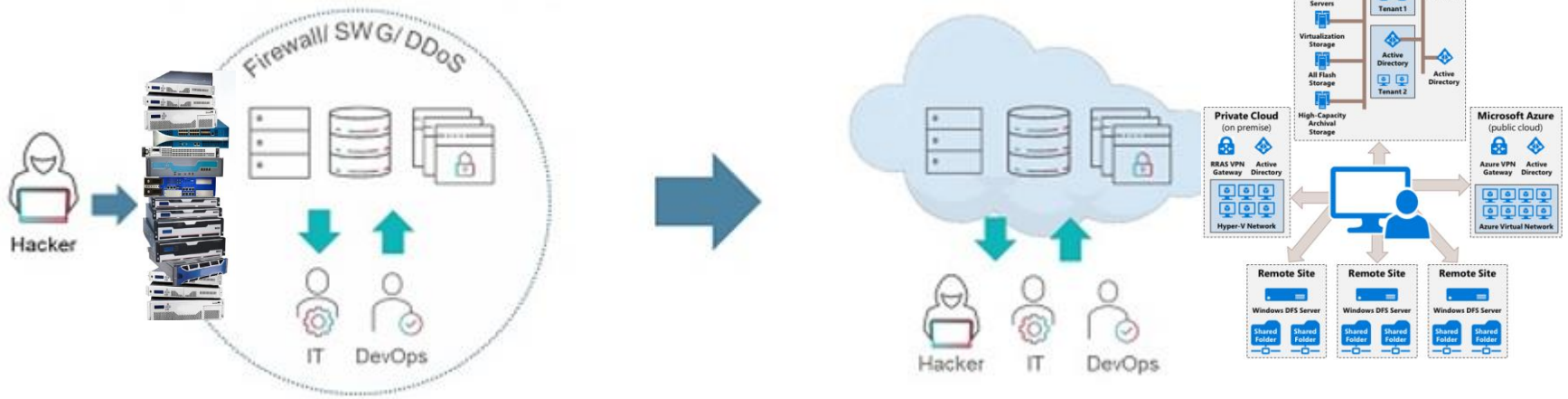
148% Covid19 이전에 비해 증가

- 전체 직원중 64% 가 원격 근무, 코로나 이전 대비 148% 증가
- 위험한 App이나 사이트에 대한 접근이 161% 증가
- 성인 컨텐츠 트래픽이 600%증가
- 업무용 Device의 개인용도 사용율이 97%증가
- 기업용 협업툴 사용율이 80%증가
- 클라우드 기반의 악성코드 전파가 63% 증가

-TechTarget 2020

01 COVID19/CLOUD시대의 보안환경 변화

❖ 재택과 함께 클라우드 확대로 기존의 경계선 보안으로는 사실상 보안이 불가한 시대

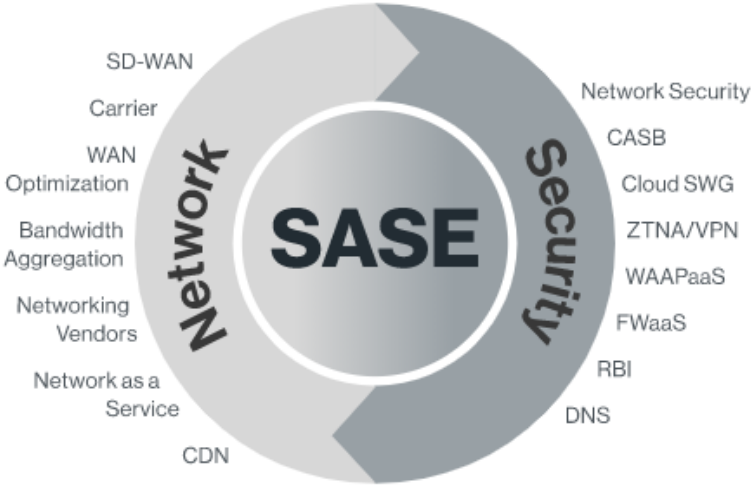


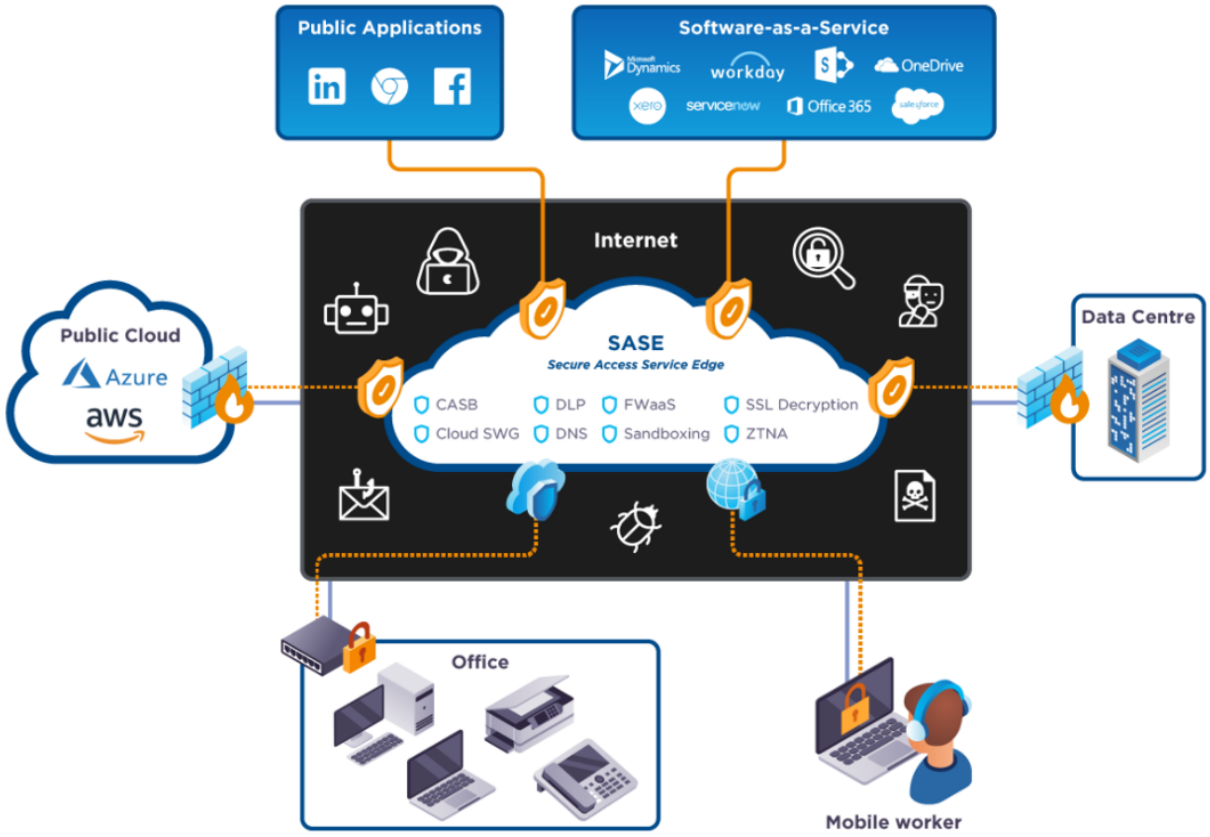
- 외부 위협에 대한 경계선 방어
- 내부에 위치한 네트워크 자원
- 내부자의 위협으로부터 보호

- 기업 내외부에 워크로드 위치
- 조직별로 사용하는 인프라가 상이
- Multi Cloud 인프라 사용
- 리모트 접속이 기본

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

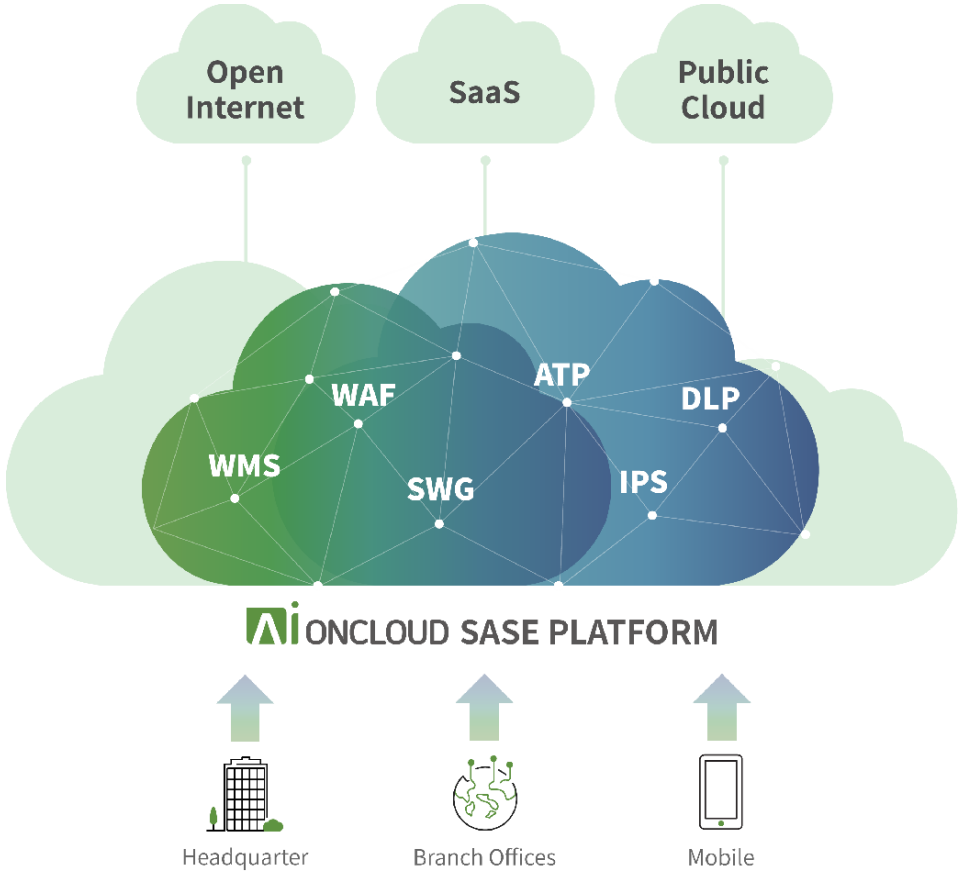
- SASE는 클라우드와 식별된 사용자 ID기반의 네트워킹/보안 통합 아키텍쳐





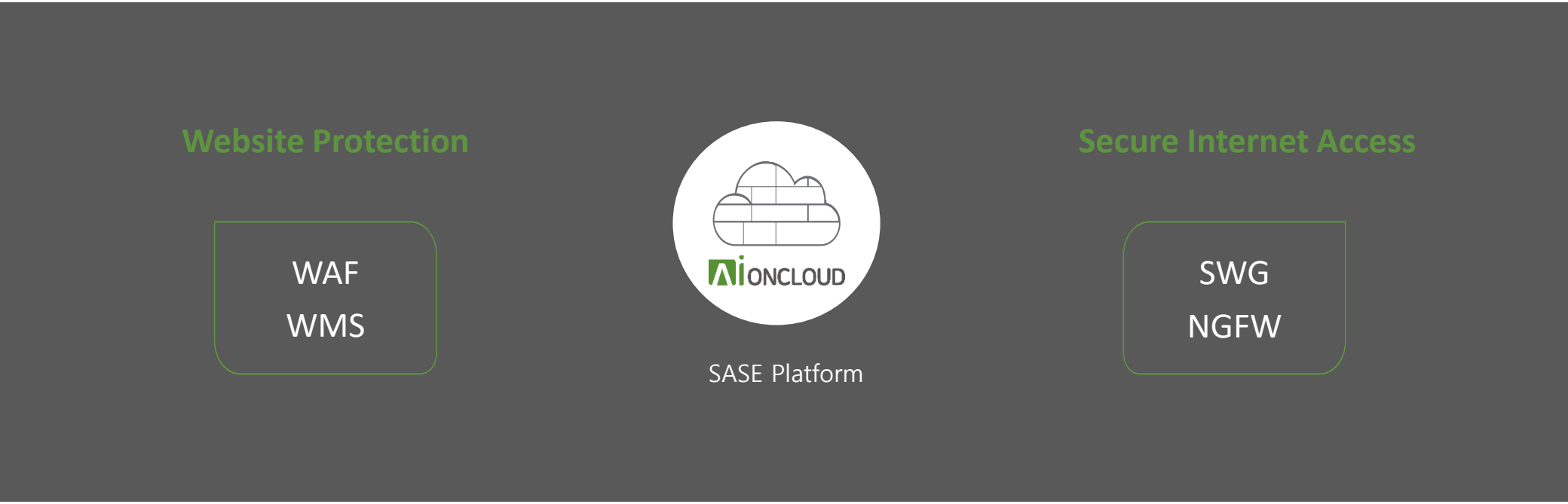
❖ AIONCLOUD (Application Insight on Cloud)

AIONCLOUD는 AI(인공지능)기술이 결합된 Threat Intelligence 기반에서 다양한 네트워크 보안 서비스를 제공을 목표로하는 SASE(Secure Access Service Edge) 플랫폼입니다.



❖ 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



❖ AIONCLOUD 주요기능

Website Protection

1

Bot/API/
Credential Stuffing

2

Web Security/
OWASP Top10

3

Optimize Website
Performance

Secure Internet Access

1

Network Security

2

Internet Access Control

3


DLP/APT

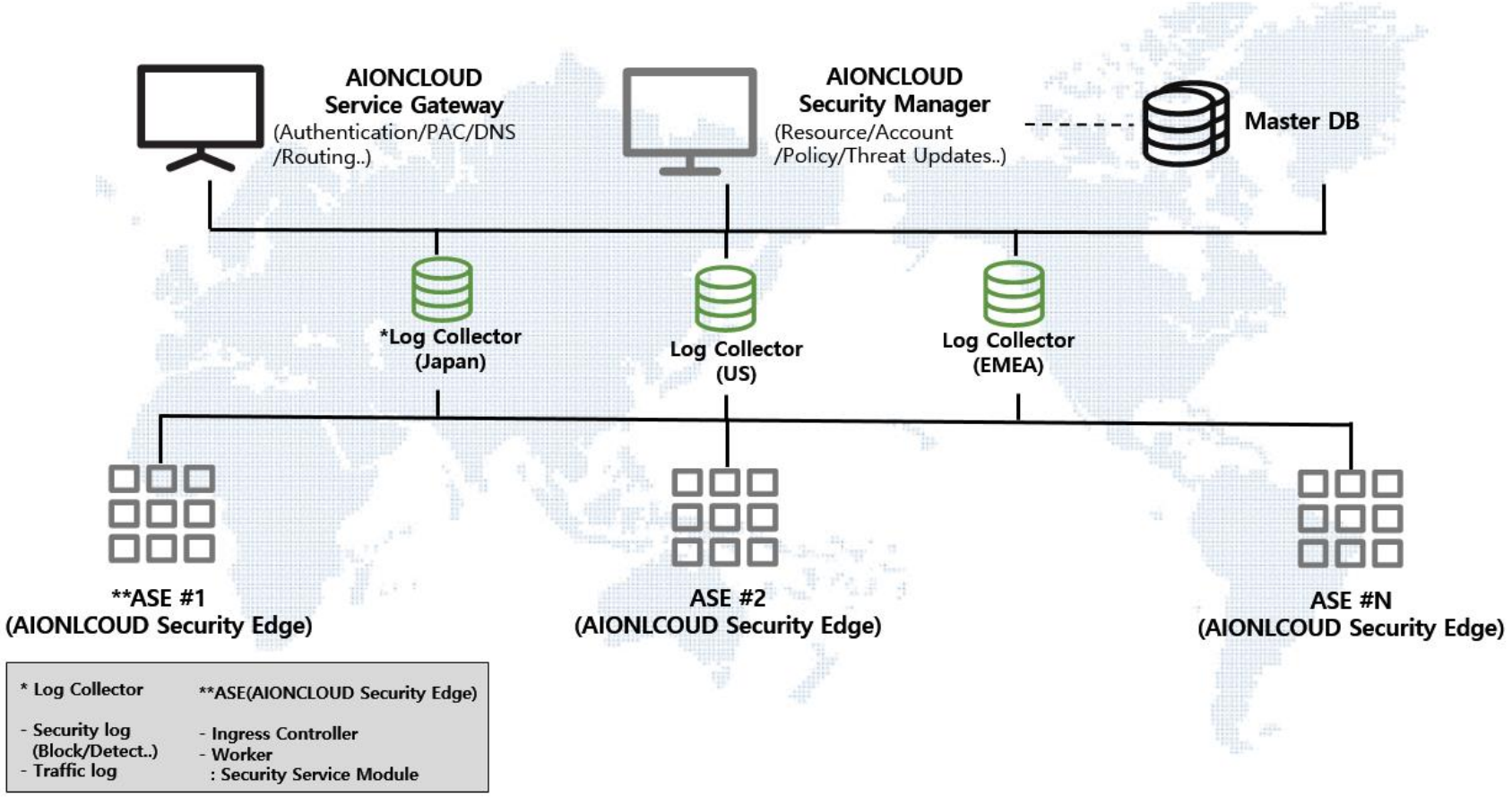

SSL Visibility

❖ AIONCLOUD Global Network

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

❖ AIONCLOUD 플랫폼 구성

AIONCLOUD Service Gateway / Security Manager / Security Edge



❖ AIONCLOUD 플랫폼 구성

AIONCLOUD Service Gateway

- Authentication
- Access Gateway
- DNS Service
- Service Routing

AIONCLOUD Security Manager

- Account Management
- Global Service Infra Pooling/Provisioning
- Policy Management
- Real-time Threat Updates

Log Collector

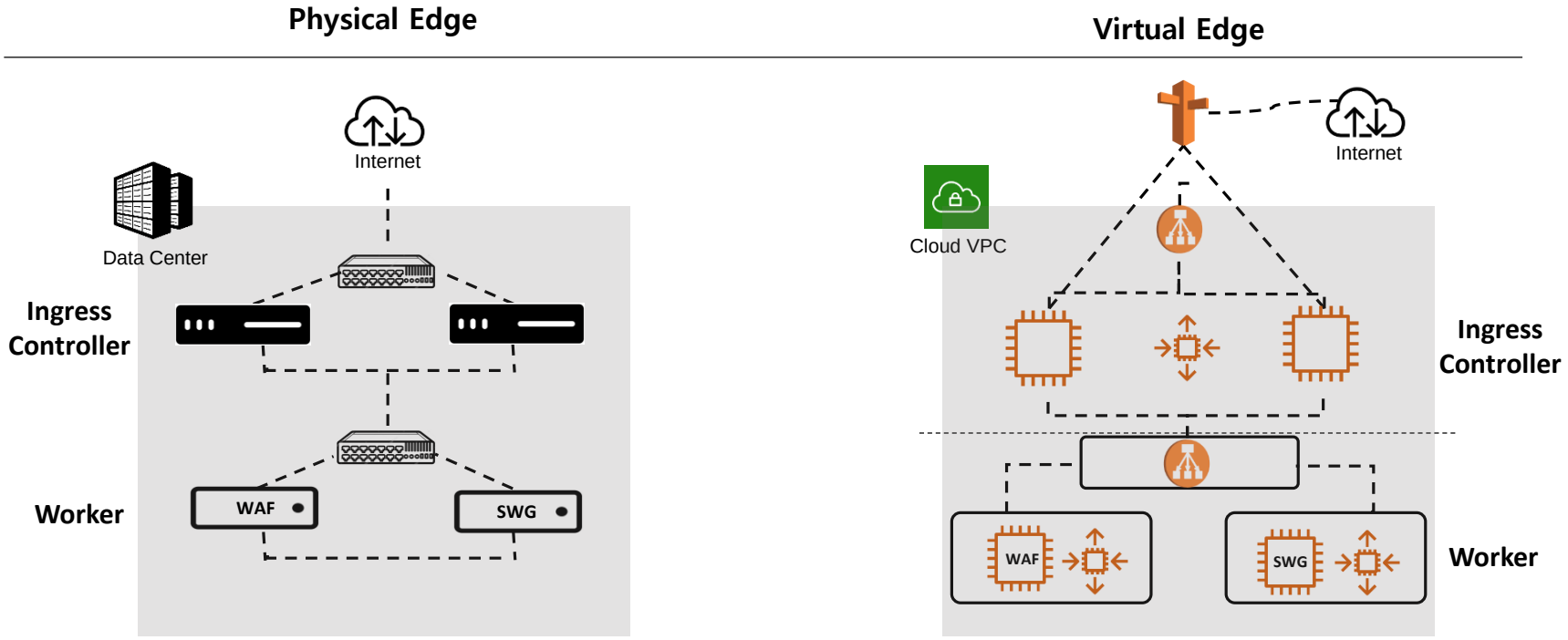
- Distributed Database system
- User Logs Consolidation
  - Security / Traffic log
- Interworking with User's SIEM

AIONCLOUD Security Edge

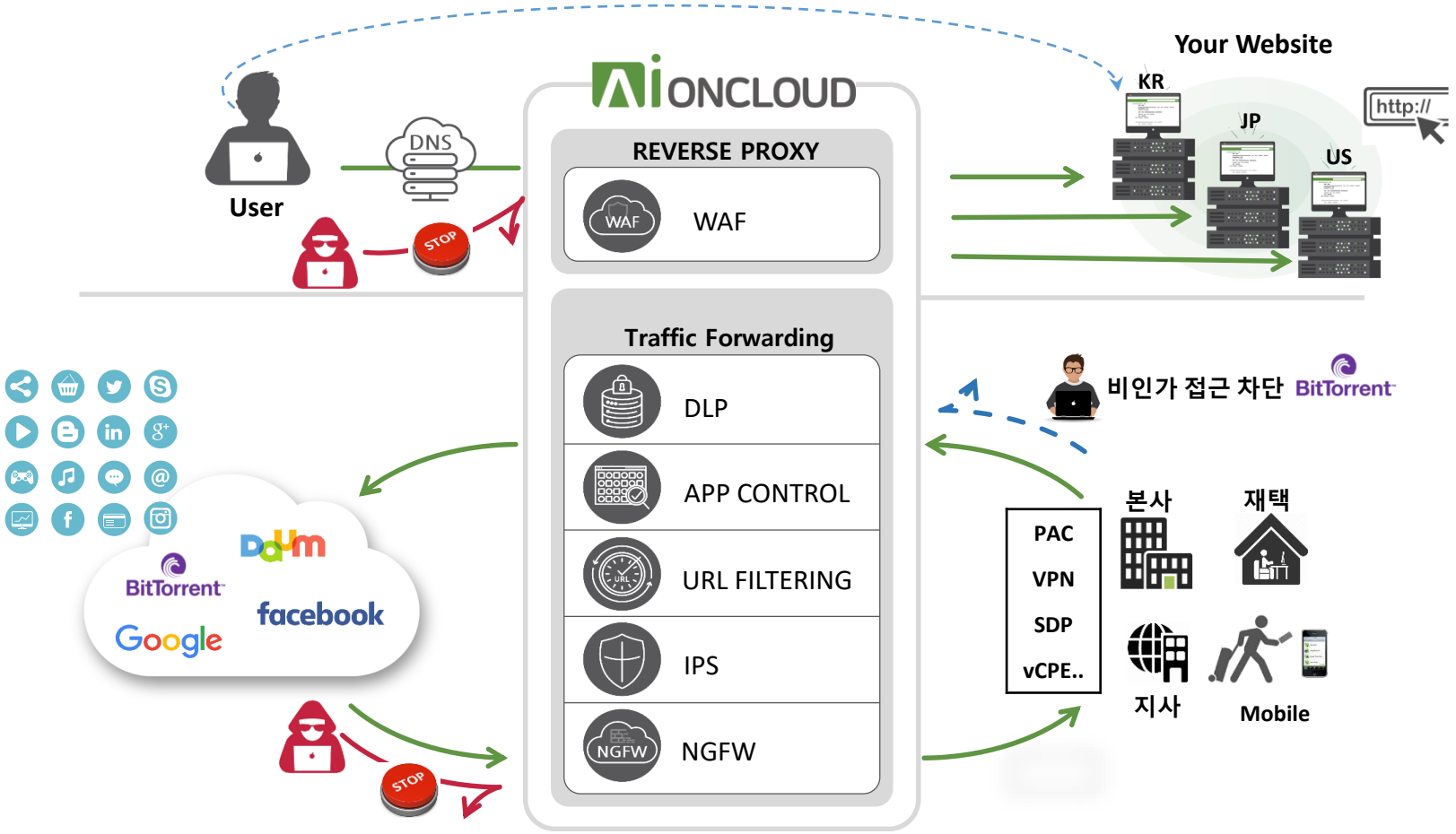
- Ingress Controller
  : FW,LB,DDoS
- Reverse/Forward Proxy
- Security Service Module
- SSL Inspection Engine

❖ AIONCLOUD Security Edge

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



❖ AIONCLOUD(Application Insight on Cloud)서비스 트래픽 Flow



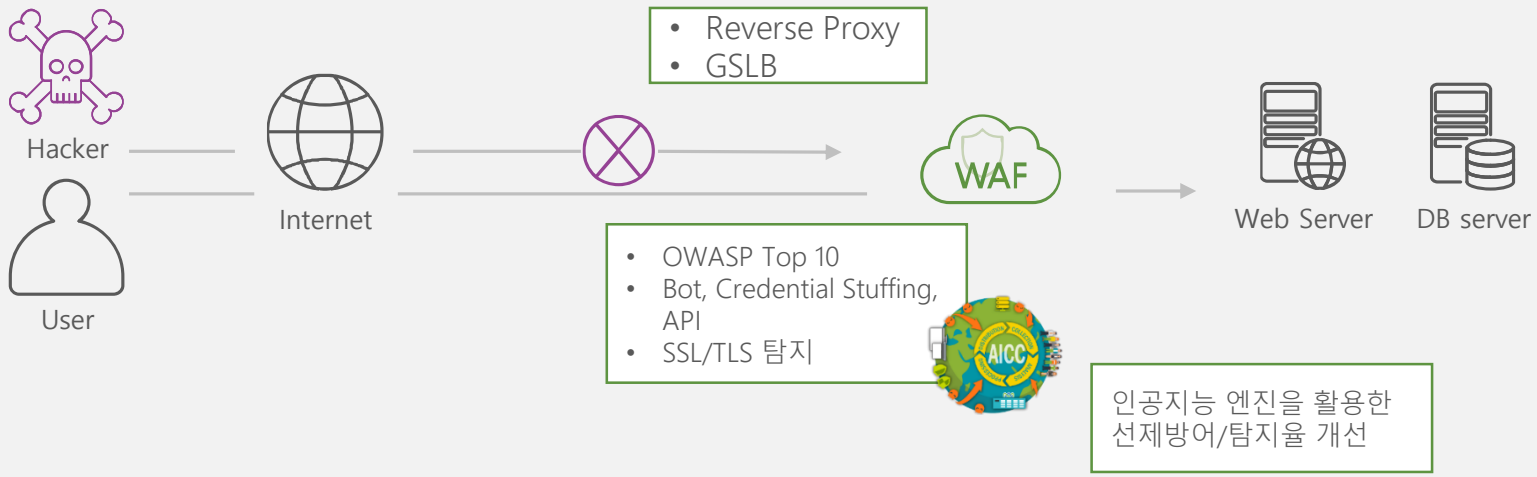
Website Protection

- **WAF (W**eb **A**pplication **F**irewall**)**
- **WMS (W**eb **M**alware **S**canning**)**

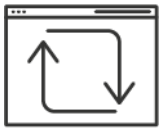
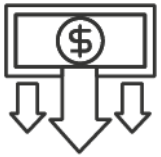
❖ AIONCLOUD WAF 서비스

- HW / SW 설치, 유지보수, 라이센스가 필요 없는 강력한 웹 보안과 성능 최적화를 제공
- 5,000여개 이상의 국내외 사이트에서 국내 시장점유율 1위 웹방화벽의 검증된 신뢰성 높은 웹보안 서비스
- SECaaS 플랫폼을 통한 간편한 신청 / 설치 / 설정 / 관리

WAF 서비스 구성



❖ AIONCLOUD WAF의 Key Service Factor

 **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

❖ AIONCLOUD WAF – 강력한 보안 서비스

01

OWASP Top 10 취약점 방어

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

❖ AIONCLOUD WAF – 강력한 보안 서비스

02

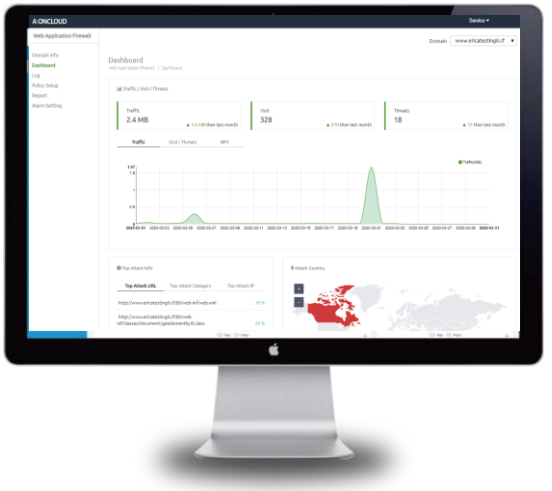
악성 봇 공격 방어

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

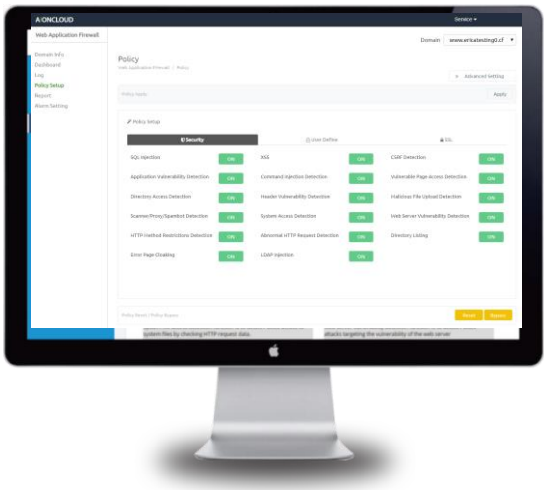
❖ AIONCLOUD WAF – 강력한 보안 서비스

❖ 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

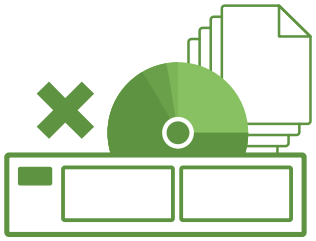
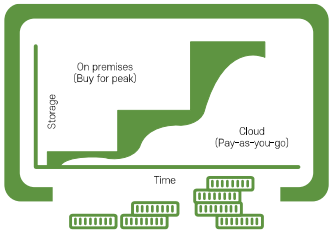


- **Simple Security Policy Setting**
  - Detect/Block/Bypass 운영모드 제공으로 운영의 편의성 제공
  - 웹공격 유형별 스위치 타입의 간편한 정책 설정 제공



❖ AIONCLOUD WAF-Cost Effective

- 현재 5GB까지 무료 서비스
- Pay-as-you-go 가격 정책으로 사용한 만큼만 지불하는 종량제 서비스
- 별도의 하드웨어나 소프트웨어 설치 비용 절감
- 추가적인 초기 비용 불필요
- 24X365로 운영되는 Managed Service로 고객 보안 인력 최소화 가능

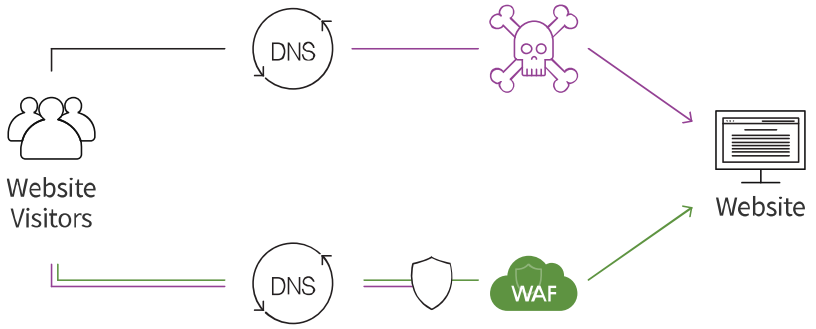
Cost Reduction of WAF		
		
초기 비용 불필요 ☑	하드웨어 소프트웨어 설치 불필요 ☑	사용한 만큼만 요금 지불 ☑

❖ AIONCLOUD WAF 이용 절차

1. 도메인 등록

- 대상 웹사이트 등록 (domain)
- 하나의 어카운트로 다수의 웹사이트 등록 가능

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

❖ AIONCLOUD WMS(Website Malware Scanner)서비스

WMD는 고객의 웹사이트를 주기적으로 방문하여 악성코드 감염 여부를 진단 정적/동적 분석을 수행하며 웹사이트의 악성코드 감염 및 경유지, 유포지 활용 여부를 판단하고, 분석된 정보는 리포트 및 알림을 통해 제공함으로써 침해 사고 조기 대응 가능

모니터랩의 Threat Intelligence 플랫폼 AICC와 연동하여 AI 기술 기반의 악성 URL판단 및 악성 파일 프로파일링을 통해 탐지율 및 속도 향상

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

❖ 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

❖ AIONCLOUD WMS 이용 절차

1. 도메인 등록

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

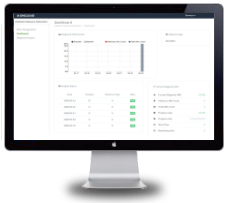
2. 진단 스케줄 설정

- 진단 주기 설정 (시간, 일, 주, 월 주기로 설정 가능)

3. 알림 설정

- 악성코드 탐지 알림 설정 (이메일 or SMS)

4. 모니터링 및 관리



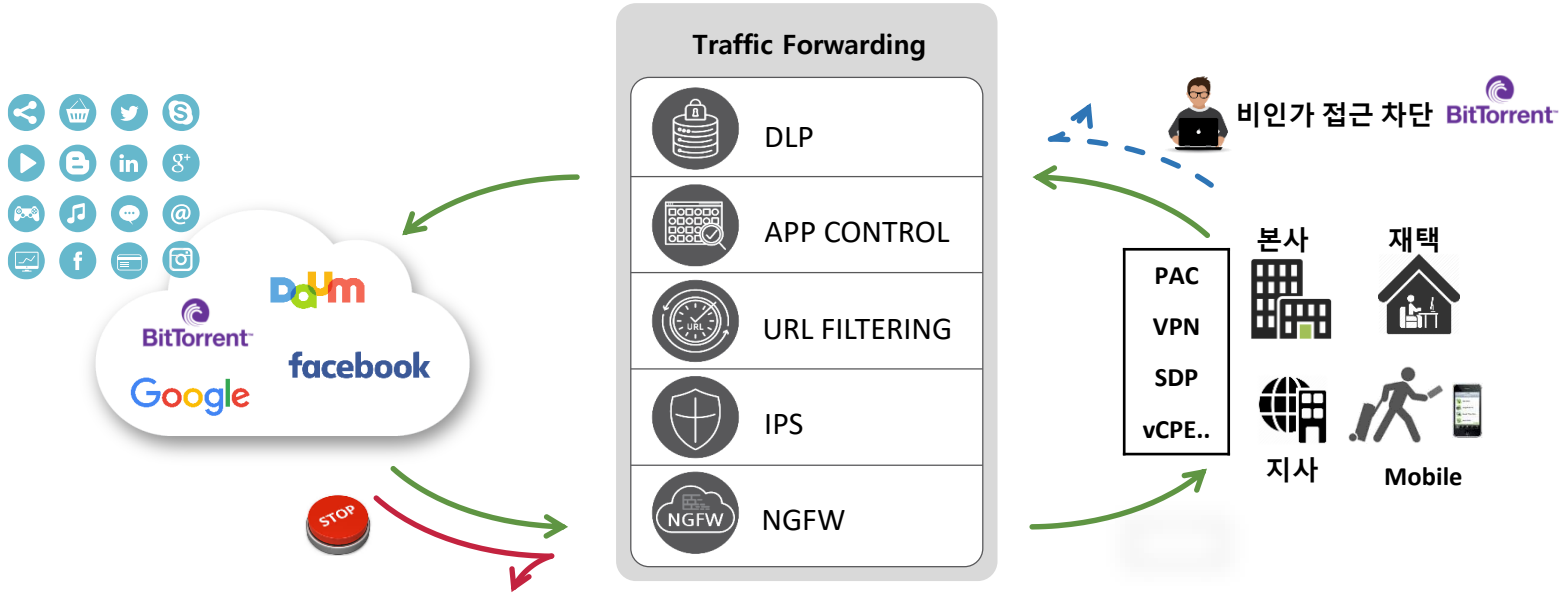
- 직관적인 UI를 통한 쉬운 모니터링 및 정책 설정 가능

Secure Internet Access

- SWG (Secure Web Gateway)

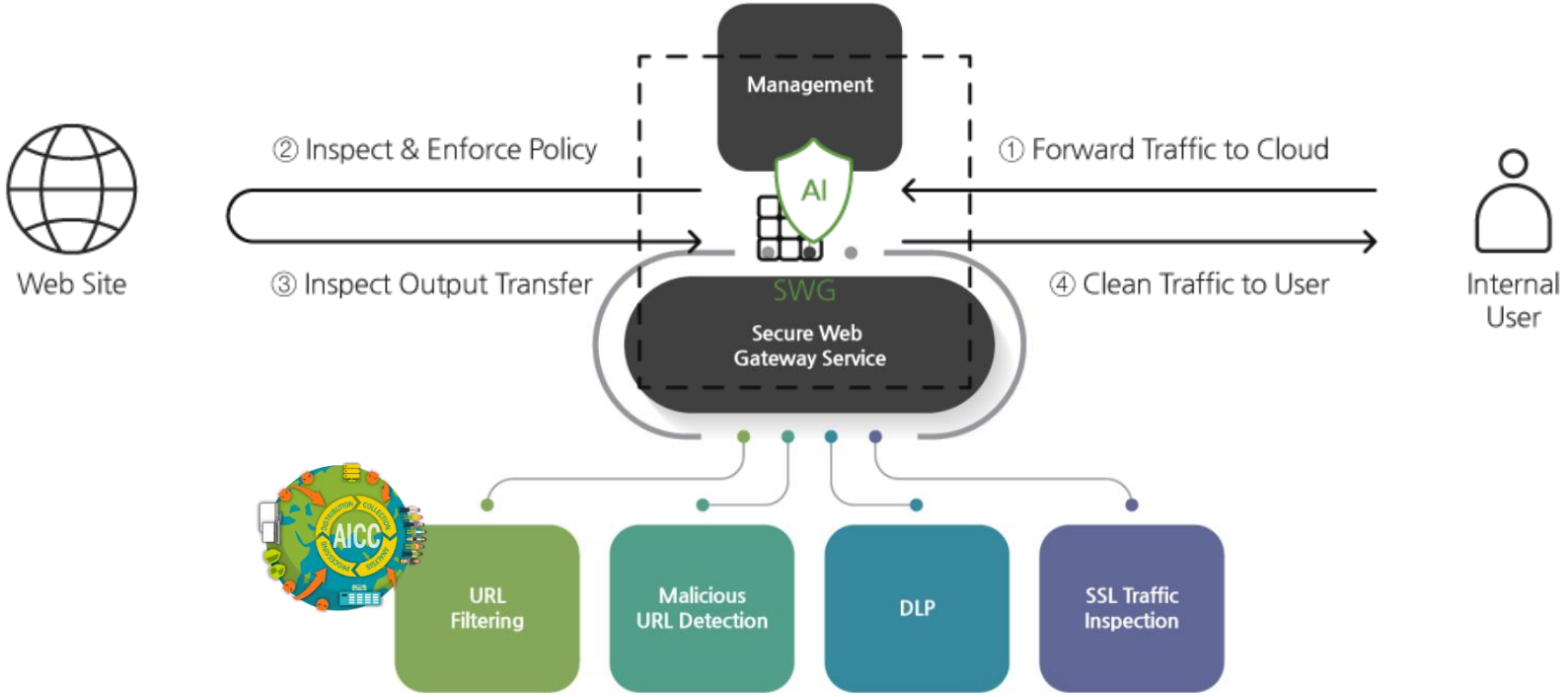
❖ Secure Internet Access

- Secure Internet Access 서비스는 내부 사용자의 외부 인터넷 이용시 발생할 수 있는 보안 위협을 제거 및 방어 할 수 있는 솔루션으로 구성되어 있으며, SDP(Software Defined Perimeter) / SWG(Secure Web Gateway) / NGFW 등의 서비스로 구성되어 있습니다.



❖ 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)

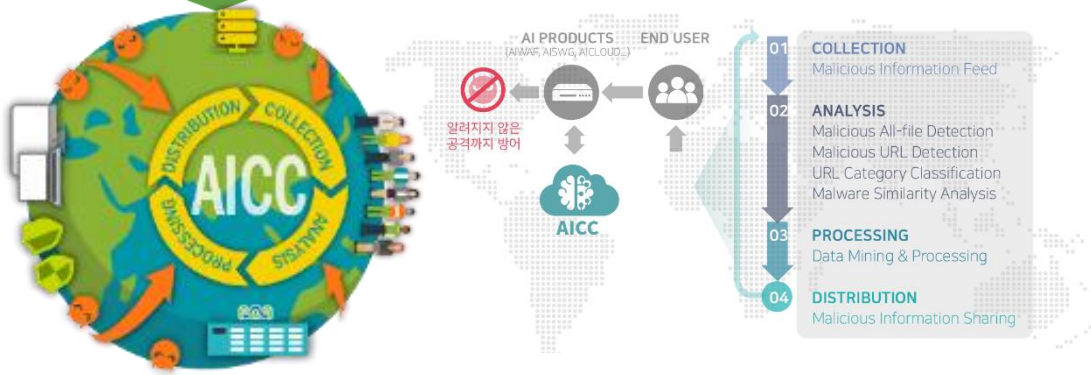


❖ AIONCLOUD Threat Intelligence Platform(AICC : Application Insight Cloud Center)

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.

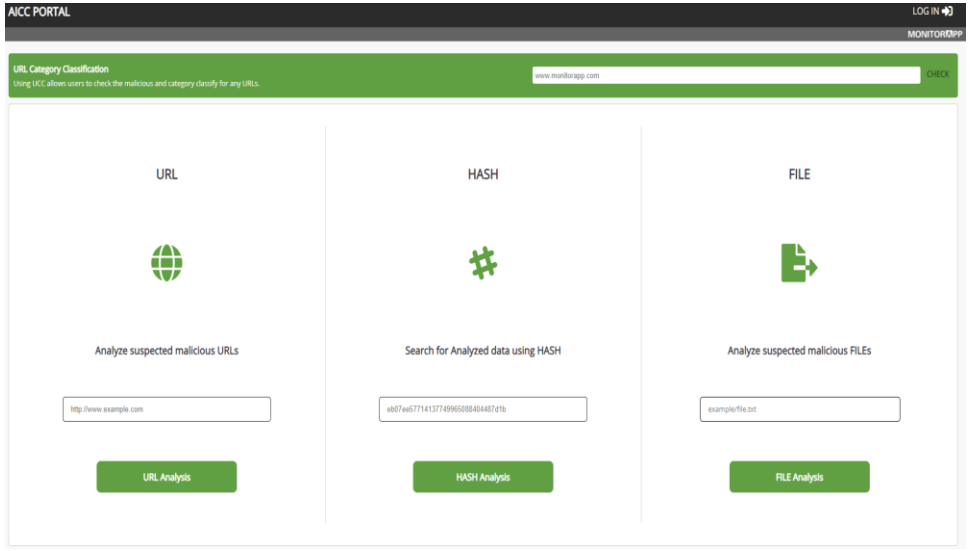
MUD	UCC	MAD	MSA
(Malicious URL Detection) 실 사이트 고속 동적 방문해 악성 URL 수집, 분석, 가공, 탐지	(URL Category Classification) URL 및 도메인에 대해서 분석을 통해 지정된 카테고리로 분류하는 시스템	(Malicious All File Detection) 웹 페이지에 첨부된 파일 등을 동적으로 분석해 악성코드를 포함한 악성 파일 식별	(Malicious Similarity Analysis) 대상 파일과의 유사도 분석을 통해 신종·변종 unknown 파일 탐지

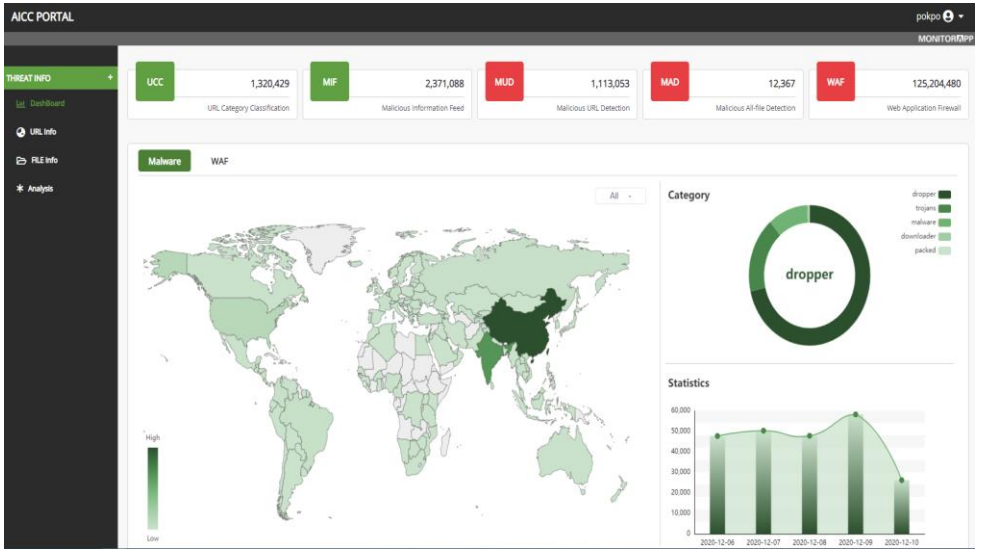
위협 인텔리전스 플랫폼 AICC (Application Insight Cloud Center)



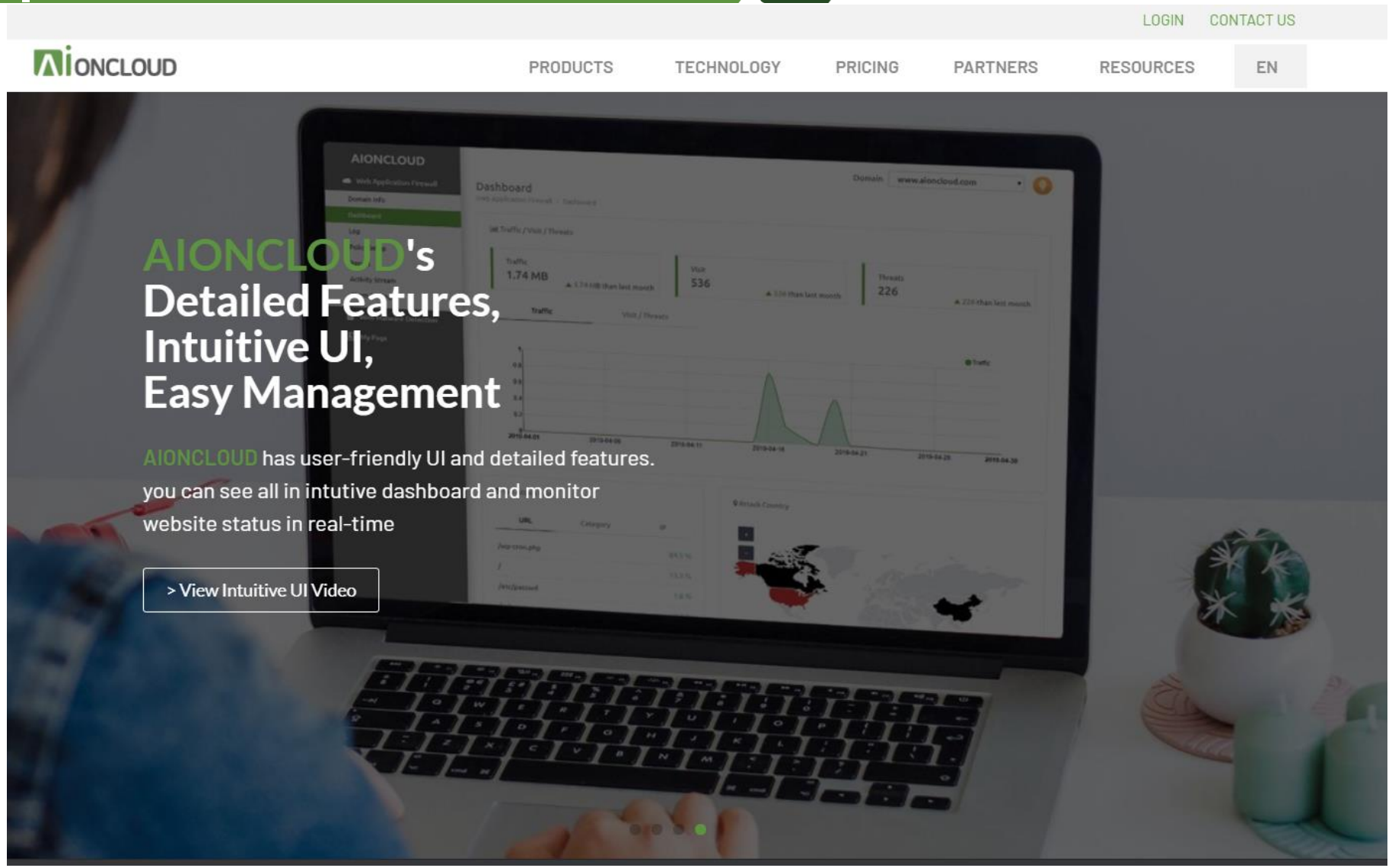
❖ AIONCLOUD Threat Intelligence Paltform(AICC : Application Insight Cloud Center)

Google VIRUSTOTAL





https://aicc.monitorapp.com


LOGIN
CONTACT US
AIONCLOUD
PRODUCTS
TECHNOLOGY
PRICING
PARTNERS
RESOURCES
EN
AIONCLOUD's
Detailed Features,
Intuitive UI,
Easy Management
AIONCLOUD has user-friendly UI and detailed features.
you can see all in intutive dashboard and monitor
website status in real-time
> View Intuitive UI Video

VIRTUAL
INTEGRATED
APPLICATION
SECURITY
FAIR **2020** (8th)

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