MONITORAPP

MONITORAPP

회 사 소 개 서

Application Security Leader

목차

01

회사소개서

- 일반현황
- 연혁 및 실적
- 조직 및 인원현황
- 주요기술
- 사업영역
- 인증 및 수상내역
- 해외 사업 현황
- 국내 사업 현황

02

솔루션 라인업

AI Product Suit :

- AIWAF
- AISWG
- AISVA
- AIDFW

03

AIONCLOUD

- WAF
- WMD

Section 1. 회사 소개

1. 일반현황

Vision

Be a leading application security solution provider in the world

Mission

Pursue the progress of information and communication technology and strive for a world in which people and knowledge by bringing people together

Strategy

- Application Layer 집중
- Profiling & Correlation 기술을 통한 Application Layer에 최적화된 보안기술 구현
- Big Data 분석을 통한 Threat Intelligence & Business Intelligence 구현
- On-Premise와 In the Cloud를 통한 Delivery

Core Value

- 고객 중심의 서비스 정신
- 따뜻하고 꾸밈없는 소통
- 뜨거운 동료애
- 적극적인 참여
- 과감한 도전
- 투철한 책임감
- 창의성
- 끊임없는 자기계발

주 요 사 업 분 야

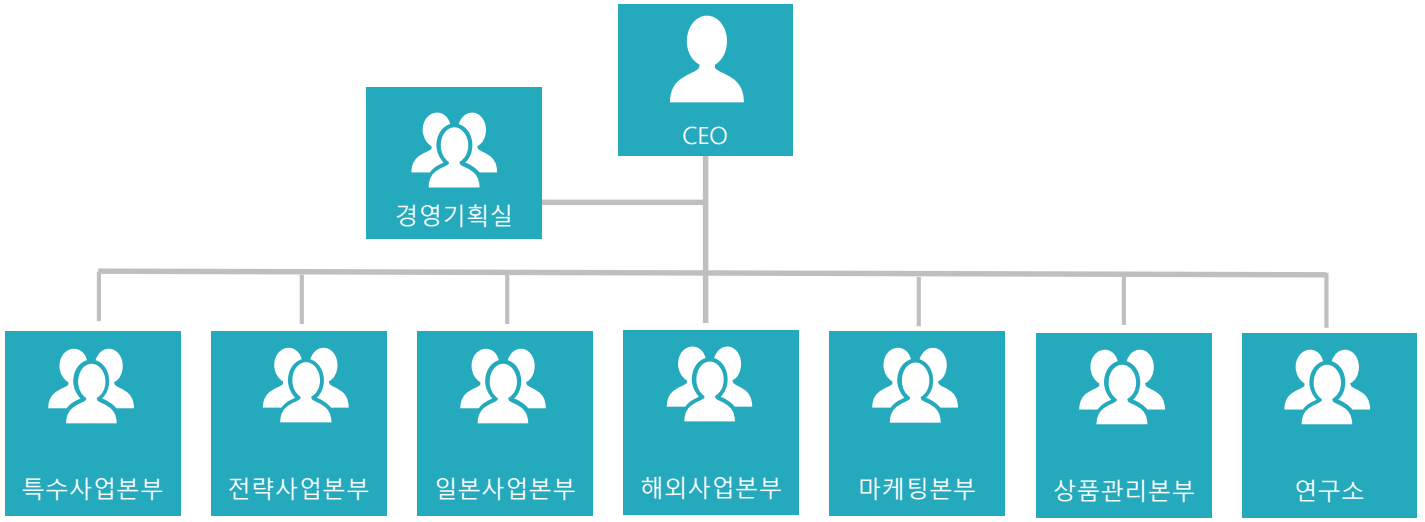
- 웹방화벽 (AIWAF)
- 시큐어 웹게이트웨이 (AISWG)
- SSL 가시성 장비 (AISVA)
- DB 접근제어 (AIDFW)
- -클라우드 기반 웹보안 서비스 (SECaaS (Security as a Service)) (AIONCLOUD)
- 애플리케이션 전문 보안관제 서비스
- 애플리케이션전문 취약점진단 및 보안컨설팅

2. 개요 & 주요연혁

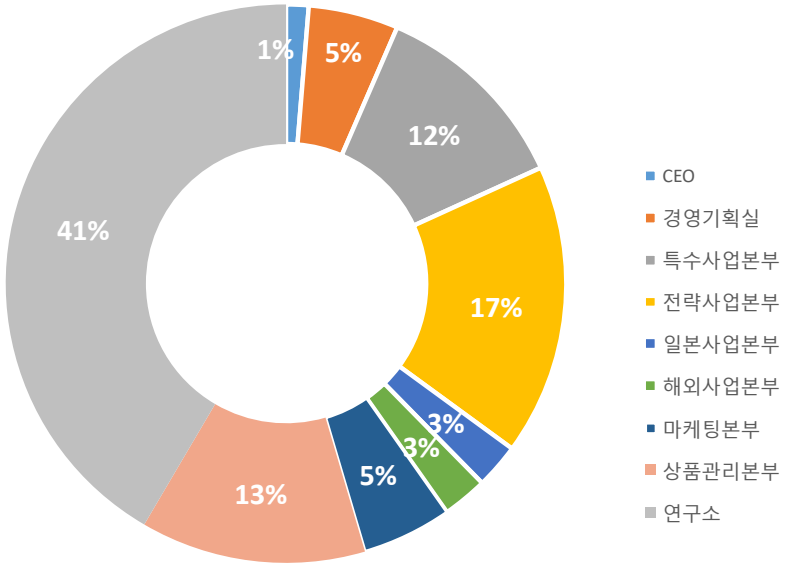
회 사 명	(주)모니터랩 (MONITORAPP)	설 립 일	2005년 2월 22일
인원/매출액	75명(2019년) / 100억 (2019년)	사업 종목	소프트웨어자문, 개발및공급, 정보보안솔루션
본점 소재지	서울시 구로구 디지털로 27가길 27	서비스URL	www.monitorapp.com

2005	02	㈜모니터랩 설립
2006	02	웹방화벽 WISG (AIWAF의 구버전) 출시
	04	수출유망 중소기업 선정 (중소기업청)
	06	WISG 제품 CC 및 GS 인증 취득
2007	03	'프로파일링 기반 웹 서비스 보안 시스템' 기술 특허 등록
	05	'원격 웹 서비스 보안 시스템' 기술 특허 등록
	11	AIDFW, DB 방화벽 출시
2008	05	'프로파일링 기반 DB 보안 시스템' 기술 특허 등록
	06	AIDFW, DB 방화벽 GS 인증 취득
2009	02	AIVFW, VoIP 방화벽 출시
	04	AIWAF 및 AIDFW 제품 CC 인증 취득
	05	'투명 프록시 시스템 및 패킷 처리 방법' 기술 특허 등록
2010	01	'웹-DB 간 로그 데이타 상관관계 추적에 의한 통합 보안' 기술 특허 등록
	05	AIVFW, VoIP 방화벽 CC 인증 취득
2011	08	태국 SI 업체 BlueZebra 와 총판 계약
2012	01	클라우드 용 웹방화벽 AIWAF-VE 출시
	04	태국 국회에 AIDFW 공급
2013	02	말레이시아의 보안 전문 업체 TechLab Security 와 총판 계약
	09	유해 사이트 차단 솔루션 AISWG 출시
2014	02	국제웹보안표준기구 OWASP 기업회원 가입
2015	03	AIWAF-VE 제품을 AWS(아마존웹서비스) 마켓플레이스에 게시
	11	SSL 가시성 장비, AISVA 출시
	12	AISWG 제품 GS 인증 취득
2016	08	일본 법인 설립
	09	베트남의 ISP 업체 Netnam 과 총판 계약
	10	SECaaS 플랫폼 AIONCLOUD 출시
	11	인도네시아의 NI 업체 RML 과 총판 계약
2017	02	일본 NI 업체 Artiza Networks 와 AISVA ODM 계약 체결
	03	나라장터 조달 시스템 SSL 가시성 분야에 AISVA 등록
	07	'데이터 마이닝을 통한 웹-DB 사용자 추적 방법' 기술 특허 등록
	12	AhnLab 및 아토리서치와 AIONCLOUD에 대한 White Label 파트너십 체결
2018	03	'보호 대상 서비스 자동 인식 방법' 기술 특허 등록
	04	AIONCLOUD에서 WMD 서비스 출시
	05	AIONCLOUD가 NIPA의 클라우드 품질 및 성능 인증 획득
	08	웹방화벽 제품 AIWAF 에 대한 CC 인증 획득
	11	메가존 클라우드와 AIONCLOUD에 대한 파트너십 체결
	12	UAE 벤더 ABS Mena와 AIWAF 에 대한 파트너십 체결
	12	일본 벤더 Secure Innovation과 AIONCLOUD에 대한 White Label 파트너십 체결
2019	04	미국 법인 설립
	06	일본 보안업체 앳시그널(@SIGNAL)과 SECaaS 공동사업 협약 체결
	07	'보안장치 경유 SSL 접속 불가 사이트 접속 지원 방법 및 시스템' 특허 등록

3. 조직도 및 인원현황



Division	Number
CEO	1
경영기획실	4
특수사업본부	9
전략사업본부	13
일본사업본부	2
해외사업본부	2
마케팅본부	4
상품관리본부	10
연구소	32
합계	**77**



4. 주요기술

APPLICATION INSIGHT 기술은 모니터랩의 주요 기반 기술로서 OSI 7 Layer 중 7번째 계층인 애플리케이션을 보호한다. APPLICATION INSIGHT는 패킷 드라이버를 통한 드라이버 조정과 AI_SOCK를 통해 트래픽 조절이 가능한 AIOS Platform을 통해 구현된다. MONITORAPP 사용자들은 AIOS Platform과 통합 관리 인터페이스를 통해 APPLICATION INSIGHT 기술을 사용함으로써 애플리케이션 계층 보호/관리가 가능하다.

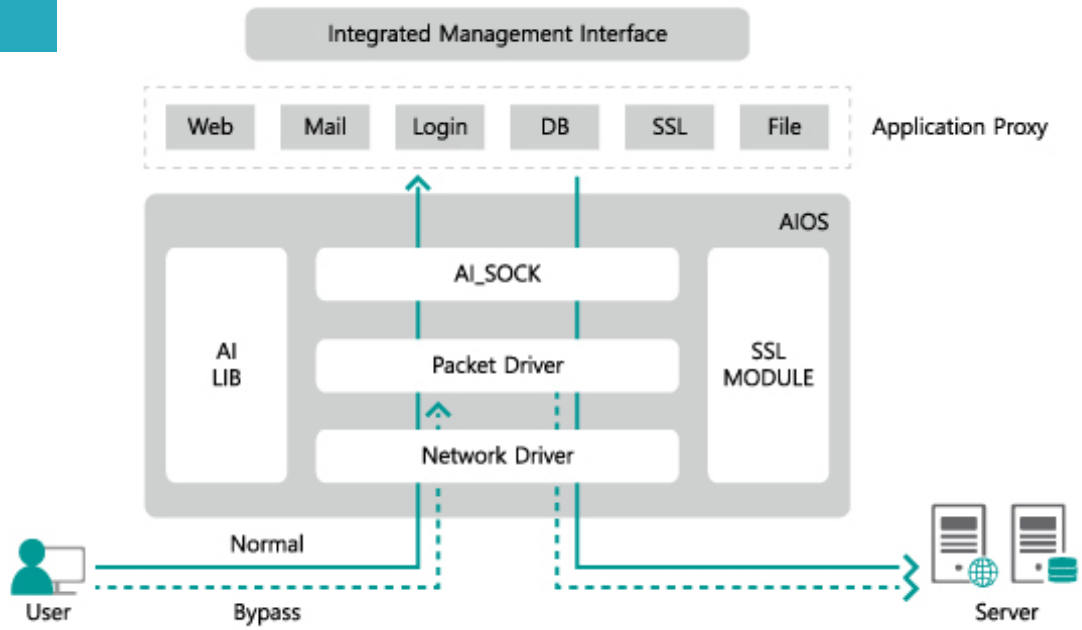
4. 주요기술

AIOS Platform

AIOS(APPLICATION INSIGHT OPERATING SYSTEM)는 모니터랩 모든 제품에 공통되는 플랫폼이다.

- Packet Driver
  - ✓ 보호대상 트래픽 유무를 판단 하며 보호대상 트래픽은 AI_SOCK 로 전달하고 보호대상이 아닌 트래픽은 bypass
  - ✓ 구성모드 설정에 따라 eth1(Client)로 유입된 패킷을 eth2(Server) 또는 eth1(Client/Server) 전송
- AI_SOCK : 최적화된 TCP/IP Stack으로 보호대상으로 분류된 트래픽을 Proxy 엔진으로 전달하며 패킷에 대한 기본적인 흐름제어 및 상태체크
- Application Proxy: 기본모드 및 조건에 대한 설정과 Product 별 보호대상 Traffic에 대한 탐지 및 차단
  - ✓ 구성 모드에 따른 처리 모듈 분류 : Sniffing, Mirroring, SYN_TP, Transparent Proxy, Reverse Proxy 등

AIOS Platform



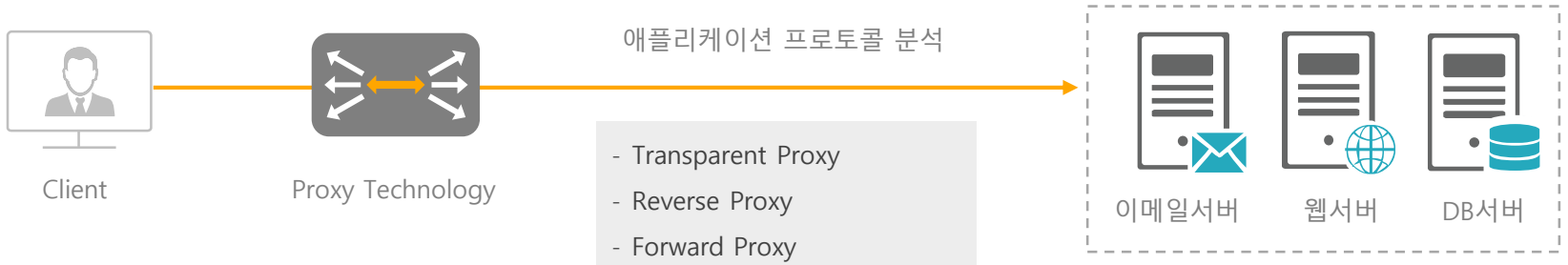
4. 주요기술

High Performance Proxy Technology

핵심 특허기술 중 하나인 Transparent Proxy 는 Application 보안을 위하여 안정적이며, 높은 수준의 Inspection 을 수행한다.

- WEB, Database, UC 개별 Application 프로토콜에 대한 완벽한 해석을 바탕으로 깊이 있는 수준의 보안을 제공하는 Application Proxy로서의 기능을 고성능으로 제공
- 네트워크 구조상 투명성 보장으로 기존 네트워크 변화 없이 구축 가능
- Bypass기능 제공을 통한 안정성과 신뢰성 제공

Proxy Technology



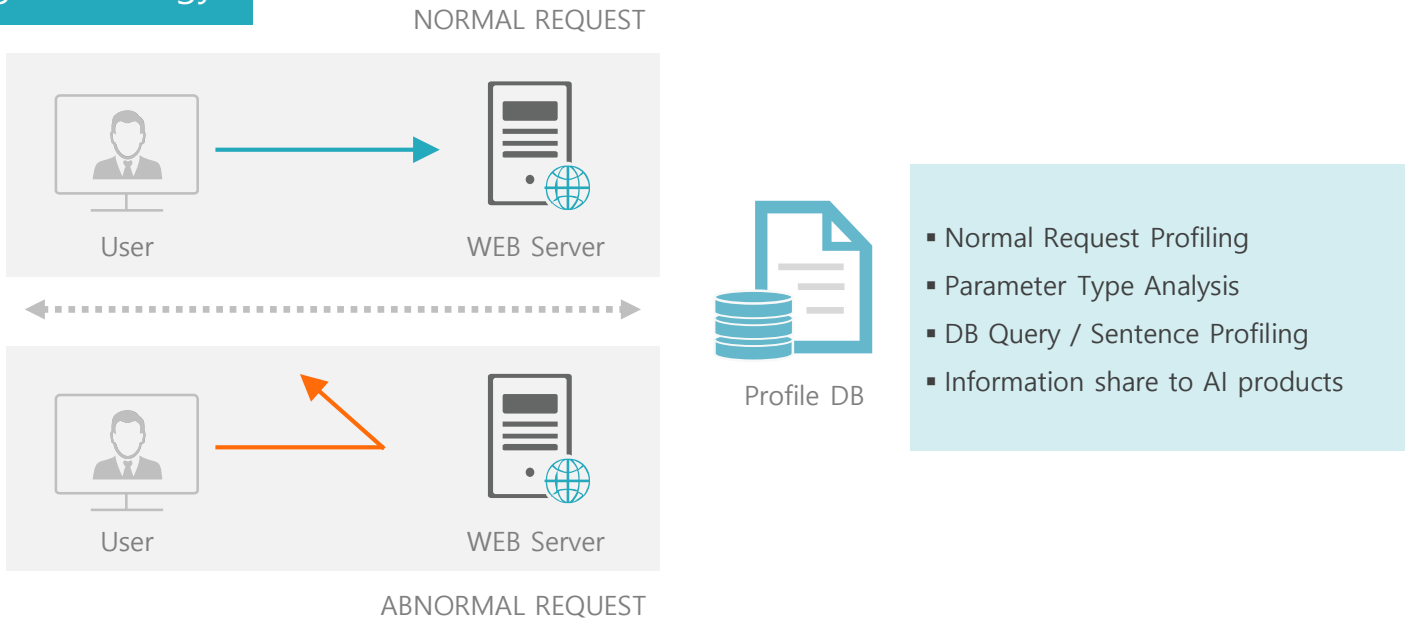
4. 주요기술

Adaptive Profiling Technology

Profiling 기술을 이용하여, 알려져 있지 않는 공격을 차단하거나, 복잡한 보안 정책을 자동으로 수립할 수 있도록 지능적인 보안 기술을 제공한다.

- 웹 사용자 행위 중 정상 응답 유발 Request 프로파일링
- 개별 Parameter에 대한 유형 분석
- DB 쿼리 / 문장 프로파일링
- SIP 지문, 시퀀스 프로파일링

Adaptive Profiling Technology



4. 주요기술

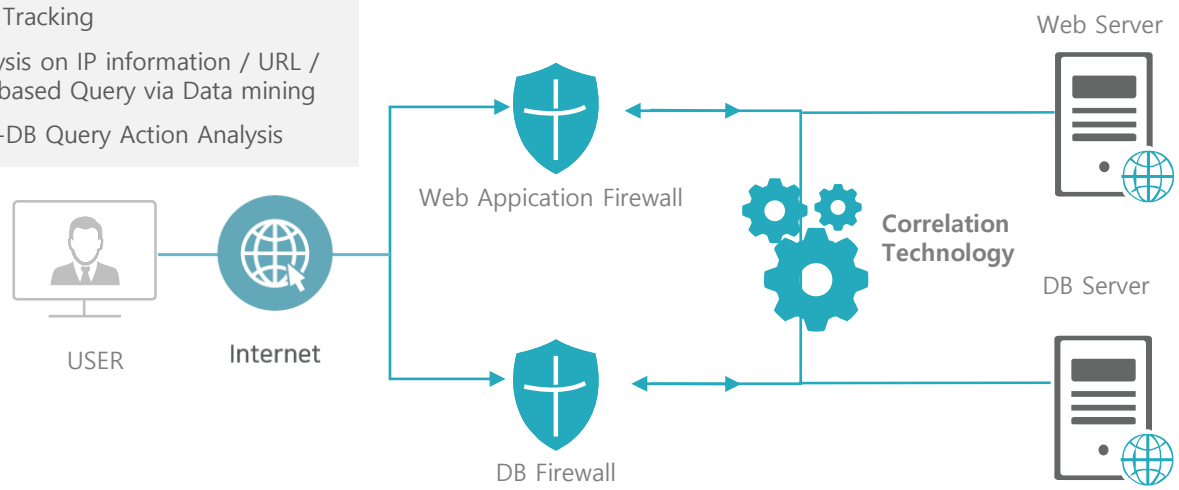
Correlation Technology

Correlation Technology 을 통해 서로 다른 애플리케이션간의 연관 관계 분석으로 추가 보안 정보를 제공한다.

- Correlation Probe와 분석기를 통해 사용자 추적
- 데이터 마이닝 기법을 통해 URL, IP 기반 정보와 SQL 기반 쿼리 정보 분석
- WEB-DB 쿼리 액션 분석
- SIP-RTP correlation 분석
- SIP-DB correlation 분석

Correlation Technology

- User Tracking
- Analysis on IP information / URL / SQL based Query via Data mining
- Web-DB Query Action Analysis



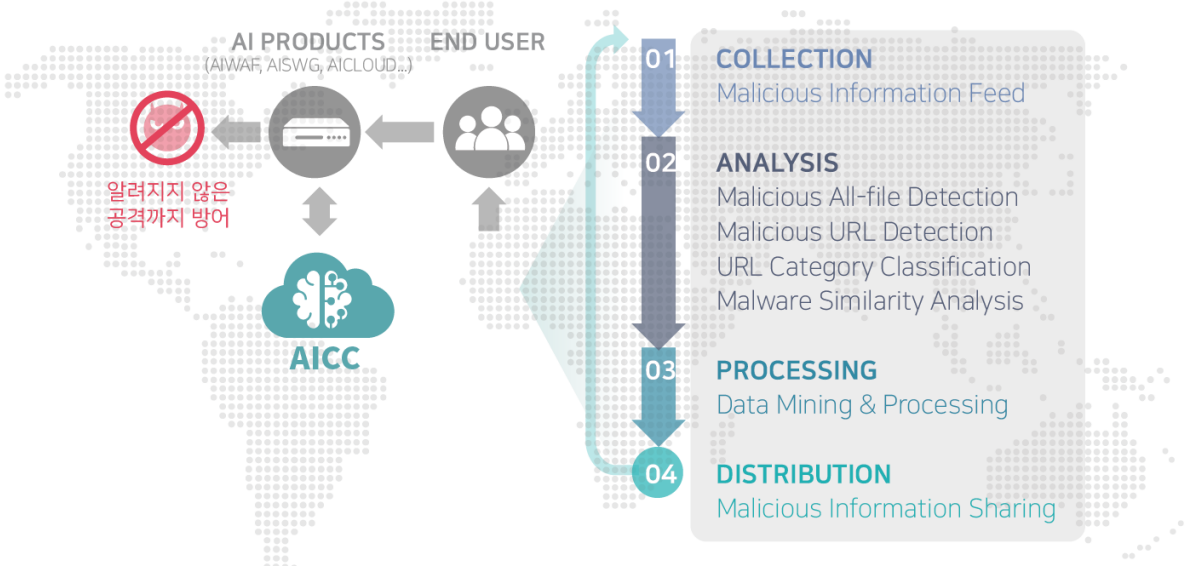
4. 주요기술

Threat Intelligence

Threat Intelligence : 기존의 보안에 인텔리전스 개념을 도입하여 전세계 위협을 빠르게 수집, 분석, 공유하여 진화하는 위협에 즉각 대응 가능하다.

- 평판 탐지
- 시그니처 탐지
- 트래픽 전수 검사
- 행위 기반 탐지
- 실시간 정보수집
- 기기 간 연동
- 데이터 마이닝
- 빅데이터 분석

AI CLOUD Center for Threat Intelligence (AICC)

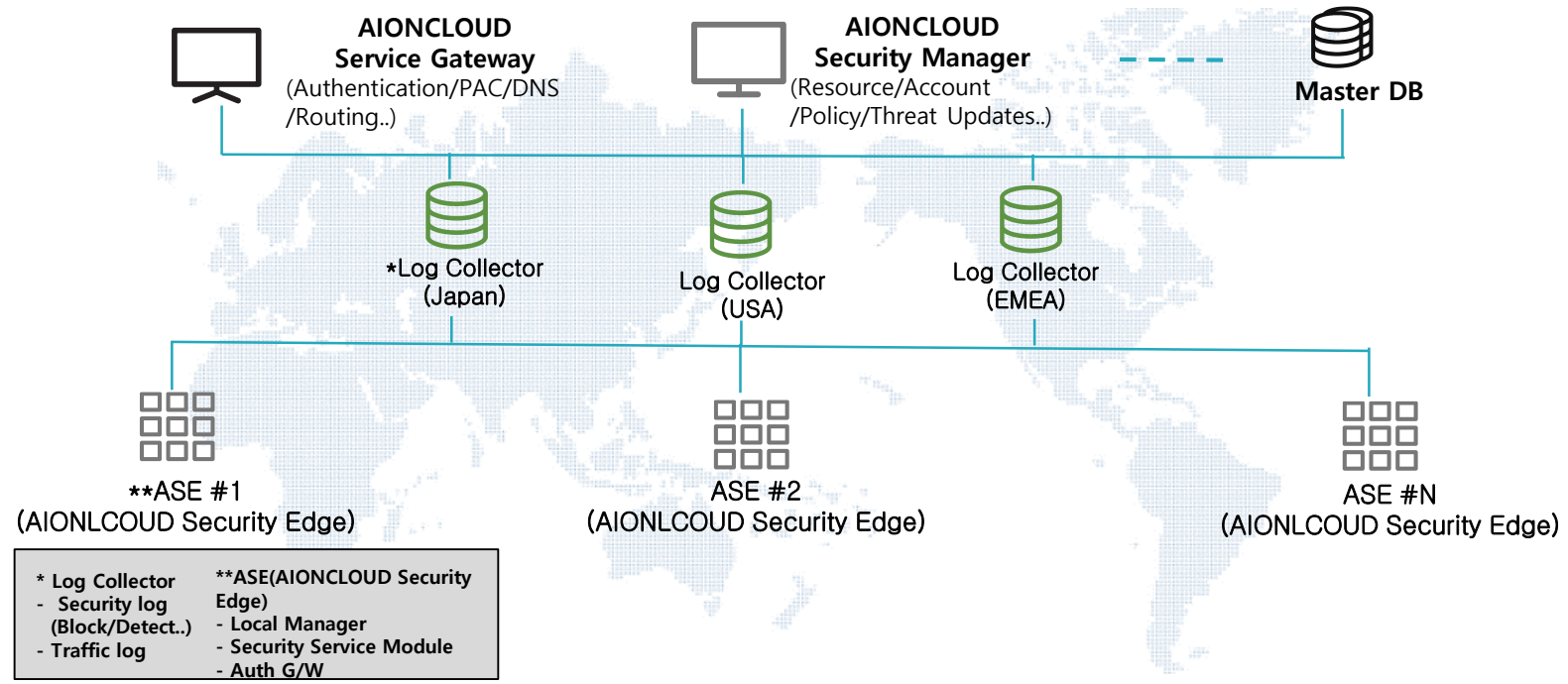


4. 주요기술

SECaaS Platform

모니터랩은 SECaaS 비지니스에 최적화 Cloud Security Platform을 보유하고 있다. SECaaS Platform은 Service Gateway, Security Manager, Security Edge, Log Collector의 상호 연계를 통해 멀티테넌시 기반의 서비스 인프라를 구성하고 있으며, 다양한 Security Service Module을 통해 보안 서비스를 SECaaS 형태로 제공한다. 모니터랩의 SECaaS 브랜드인 AIONCLOUD를 통해 16개 Global Region 40개 Datacenter 서비스 인프라를 기반으로 Cloud WAF, Website, Cloud SWG 서비스를 제공하고 있으며 제공되는 보안 서비스는 지속적으로 추가될 예정이다.

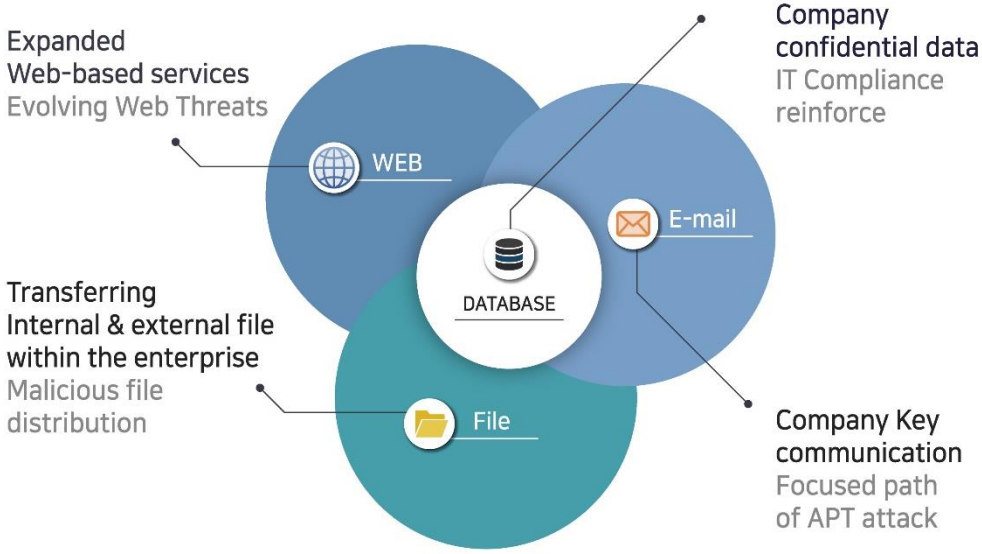
SECaaS Platform



5. 사업영역

MONITORAPP

Application



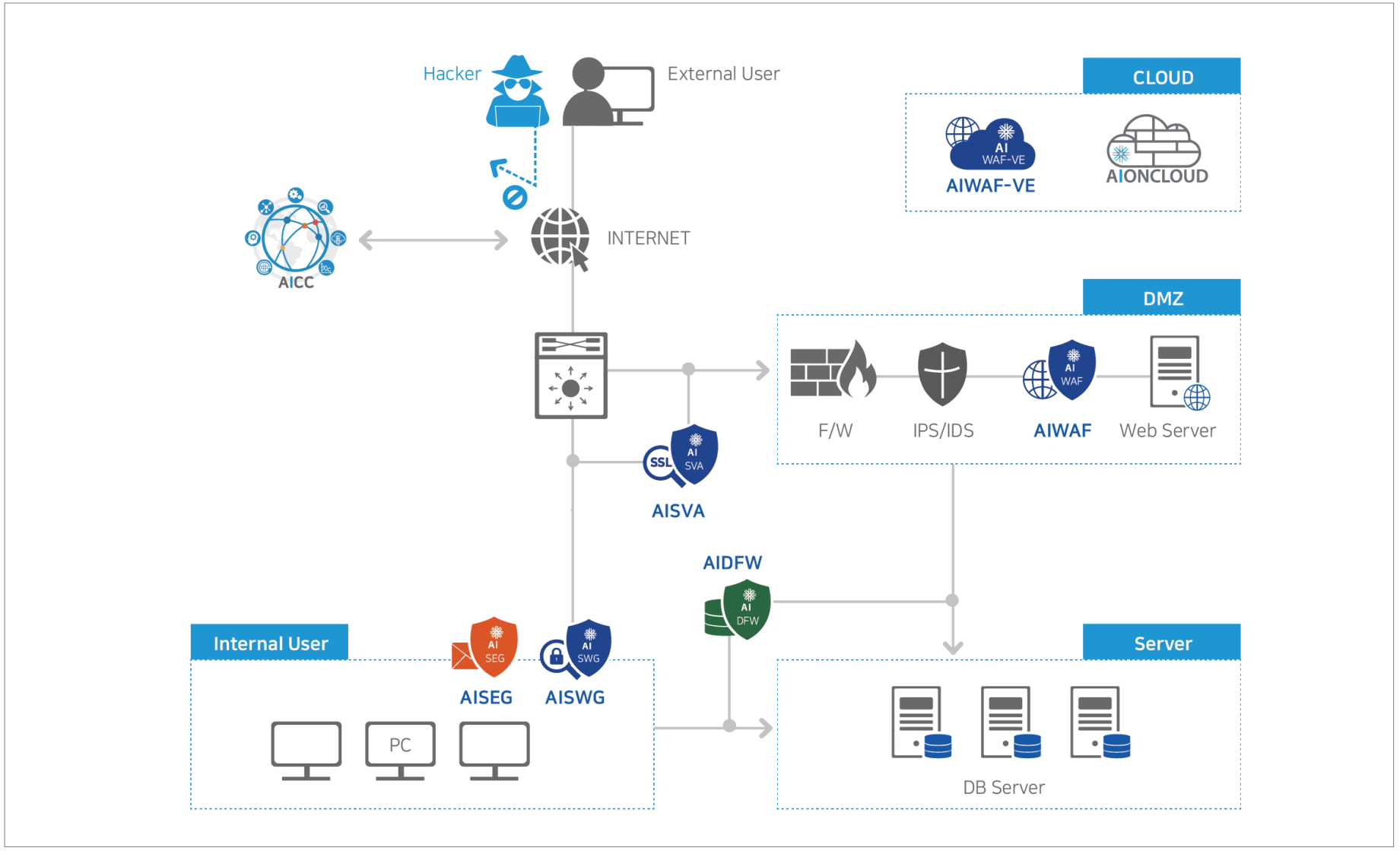
Delivery Platform

Appliances
- Enterprise
- High Performance

Virtual / IoT
- Private/Public Cloud
- AWS, MS Azure

SECaaS
- Global One Platform
- Subscription Based

6. Product Map



7. 인증 및 수상내역

MONITORAPP
Application Delivery Leader

모니터랩은 지식경제부를 포함하여 공공기관 및 기업 중심으로 약 3,000 이상의 고객을 보유하고 있으며, 다양한 애플리케이션 보안 특허를 통해 시장 영역을 넓혀가고 있다.

[07/03/01]
프로파일링 기법을 적용한 능동형 웹 애플리케이션 보안 기술

[07/05/01]
인터넷을 통한 원격 웹 애플리케이션 서비스 보안 시스템 및 시스템 제공 방법

[08/05/01]
프로파일링 기반 데이터베이스 보안 시스템 및 방법

[09/05/12]
투명 프록시 시스템 및 그외 패킹 처리 방법

[10/01/07]
웹-데이터베이스 공격 탐지 로그 데이터 상관 관계 추적에 의한 통합 보안 시스템 및 방법

[17/07/03]
데이터마이닝을 이용한 웹-데이터베이스 사용자 추적 방법 및 시스템

[18/03/14]
보호 대상 서비스 자동 인식 시스템 및 방법

[19/07/05]
보안장치 경유 SSL 접속 불가 사이트 접속 지원 방법 및 시스템

8. 해외 사업 현황

해외 레퍼런스

모니터랩은 2009년부터 고성능 애플리케이션 프락시 기술을 바탕으로한 우수한 보안 솔루션으로 글로벌 시장에 진출해 빠른 성장세를 보이며 가시적인 성과를 도출해냈다. 태국, 말레이시아, 베트남, 인도네시아 등 동남아에 글로벌 파트너와 안정적인 세일즈망을 갖고 2016년 일본에 법인을 설립해 활발한 수출이 이뤄지고 있으며 두바이와 시리아 등 중동지역에 진출해 신규 세일즈를 확보해 나가고 있다. 2019년 미국에 법인을 설립하고 클라우드 기반 웹 보안 서비스 AIONCLOUD를 판매하고 있으며 이를 기반으로 유럽 시장 진출을 목표로 하고 있다.

9. 국내 사업 현황

국내 레퍼런스

모니터랩은 웹방화벽 시장을 필두로 국내 애플리케이션 보안 시장에서 지속적인 성장을 하고있다. 웹 보안 의식이 강화되면서 대한민국 공군, 대법원 등에 AIWAF가 활용되고 있으며, 개인정보보호법이 시행으로 인한 DB접근제어가 필수가 된 기업을 대상으로 한 AIDFW 또한 시장점유율을 높여가고 있다. 유해사이트차단 솔루션 AISWG는 효율적인 APT 공격 차단 기능으로 시장 전반여에 걸쳐 사용되고 있기도 하다.

Section 2. 솔루션 라인업

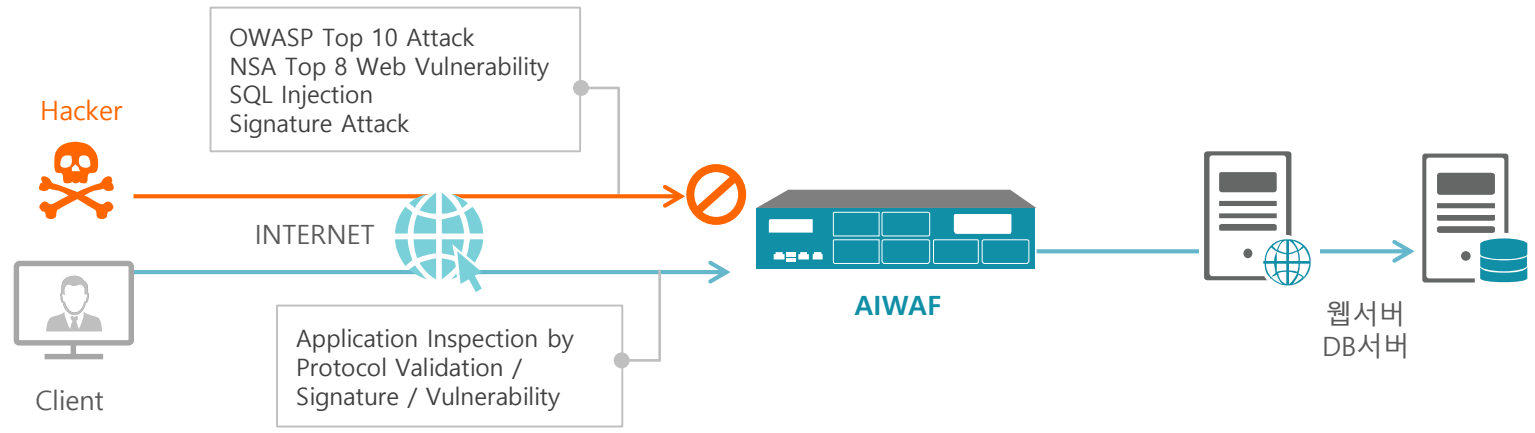
AIWAF | APPLICATION INSIGHT WAF | 웹방화벽

AIWAF (APPLICATION INSIGHT WEB APPLICATION FIREWALL)은 완전한 HTTP Protocol 해석을 기반으로 Profile 기반의 자동화된 보안 정책과 주기적인 업데이트를 포함하는 정규화된 시그니쳐(Signature) 기반의 보안정책을 지원하며, 다양한 부가 기능을 통해 외부의 해킹으로부터 웹 서비스를 보호해주는 전용 웹방화벽 제품이다.

- 핵심 기술

- Threat Intelligence Platform 연동을 통한 다양한 웹 공격 위협 (Black Client IP, C&C IP 등) 에 대한 선제적 대응
- 시스템 상태에 따른 자동 바이패스
- Non HTTP 트래픽 제어
- 모든 탐지로그에 요청 외 응답 데이터 로깅
- 도메인 별 독립적인 대시보드 제공
- 웹 서비스 별 상태(가용률, 응답속도, 상태) 모니터링
- Bot Detection / CAPTCHA
- 우회 목적의 트래픽에 대한 Normalization 수행
- 탐지 여부 검증을 위한 셀프 테스트 기능 제공

APPLICATION INSIGHT WAF Function



AISWG | APPLICATION INSIGHT SWG | 웹 게이트웨이 (URL 필터링 솔루션)

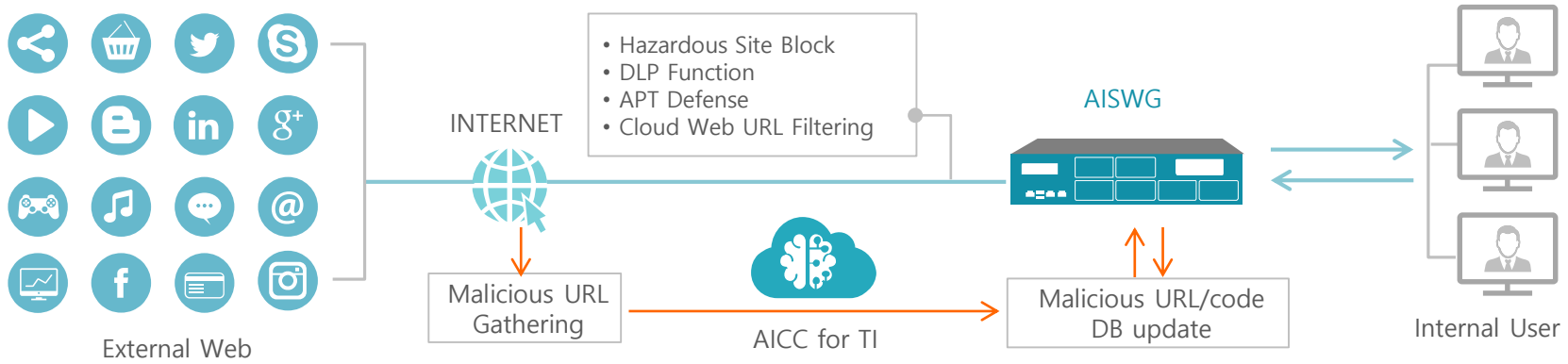
AISWG(APPLICATION INSIGHT SECURE WEB GATEWAY)는 비즈니스 요구사항에 필요한 유연성을 제공하며, APT공격 등 다양하고 진화하는 웹 공격 위협으로부터 기업 내부 웹 사용자를 보호하고 기업 내부 사용자의 안전한 웹 사용환경을 보장하는 전용 어플라이언스 기반의 보안 웹 게이트웨이 장비다.

- 핵심 기술

- Threat Intelligence(AICC) 연동을 통한 실시간 정보 업데이트
- SSL/TLS 암호화 트래픽 지원
- NAT/DHCP 환경 지원 (사용자 인증)
- 요청 및 응답 데이터 분석 (상세한 웹 서비스 제어)

- URL 필터링 (65개 카테고리 분류)
  > 비업무 사이트 접속 제어 (59) + 악성 사이트 접속 제어 (6)
- HTTP 프로토콜에 대한 Full Parsing
  - 데이터 내 악성코드 유입 탐지
  - 기밀·주요 정보 유출 탐지
  - 웹 메일 서비스 기능별 통제

APPLICATION INSIGHT SWG Function



AISVA | APPLICATION INSIGHT SVA | SSL/TLS 가시성 솔루션

MONITORAPP

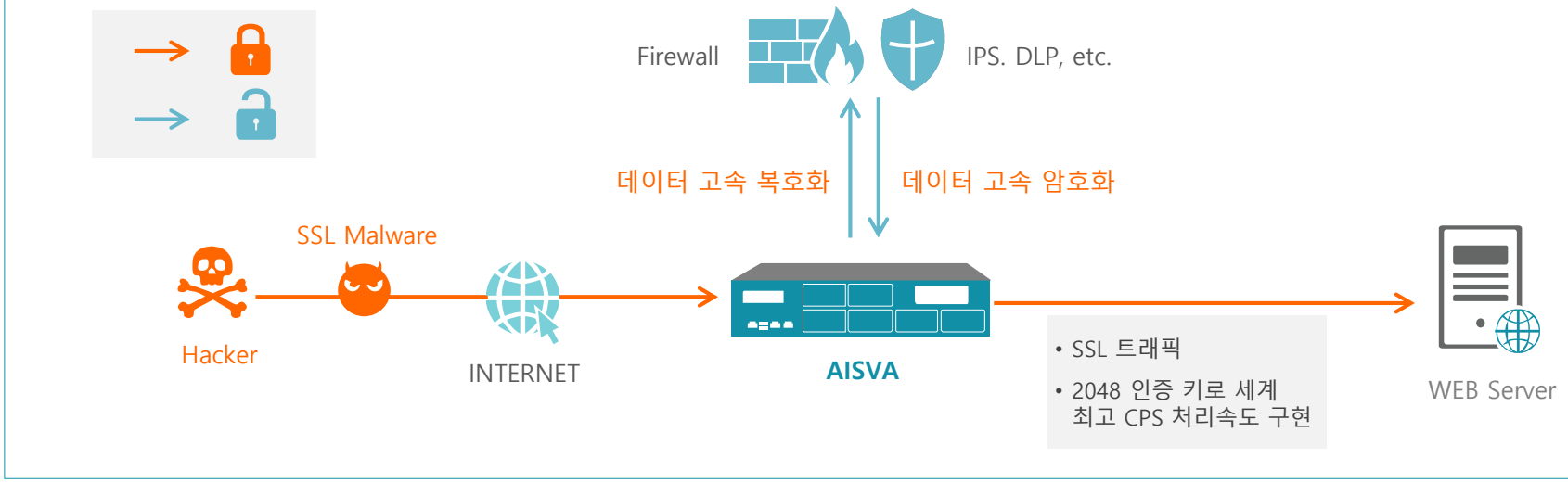
AISVA(Application Insight SSL Visibility Appliance)는 SSL Traffic에 대한 복호화 및 암호화를 제공함으로써 기존 보안 장비에서 암호화된 트래픽에 대해서도 강력한 보안정책이 적용 될 수 있도록 SSL트래픽에 대한 가시성을 제공하는 전용 어플라이언스 제품이다.

- 핵심 기술

- 인바운드 복호화 : 서버 IP:PORT, 인증서 및 개인키 등록
- 아웃바운드 복호화 : 인증서 및 개인키 직접 생성 및 관리
  암호화 트래픽 자동 선별
  (별도의 복호화 대상 설정 불필요)

- Application 유형과 무관하게 모든 SSL/TLS에 대한 복호화
- 양방향 (인바운드/아웃바운드) 복호화 동시 수행
- NAT, 비동기 네트워크 환경 지원
- 복호화 불가 웹 사이트 자동 (로컬 학습 / DB업데이트) 관리
- 보안시스템 연동 구간 Health Check

APPLICATION INSIGHT SVA Function



AIDFW | APPLICATION INSIGHT DFW | DB 방화벽

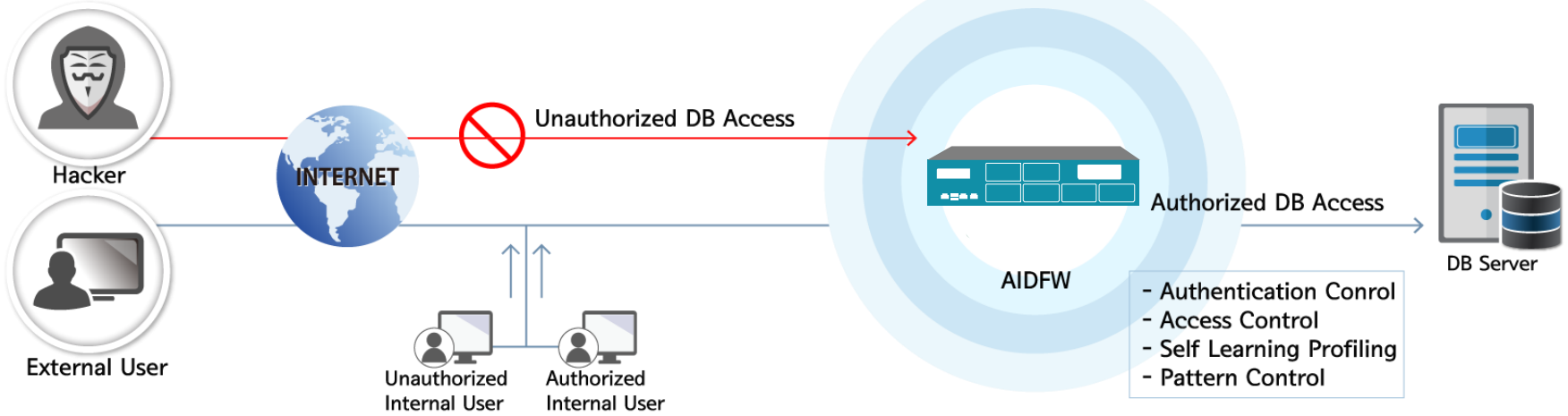
MONITORAPP

AIDFW (APPLICATION INSIGHT DB FIREWALL) 은 완전한 Query 분석을 기반으로 사용자 기반의 강력한 권한제어 및 접근제어, Profile기반의 자동화된 보안 정책을 제공함으로서 외부로부터의 비정상적인 DB접근을 통제하고, 접근 이력 관리를 통한 사후 감사기능으로 주요 내부 정보 자산을 보호해주는 전용 DB 방화벽 제품이다.

- 핵심 기술

- 고성능 패킷 처리 및 부하분산 알고리즘을 통한 대용량 트래픽 처리 성능 극대화
- SQL 패킷 처리 모듈과 대용량 로그 처리 모듈 분리를 통해 검색 및 로깅 성능 강화
- Proxy Gateway 대비 3배 이상 성능의 Sniffing Gateway
  - ✓ 별도의 Tap 장비가 불필요
  - ✓ Hybrid Mode를 지원
- 중단 없는 웹 서비스 제공을 위한 Fail-over 기능 제공
- WEB-Database 로그 연동 및 상관 관련 분석을 통한 실제 공격자 IP 탐지 및 차단
  - ✓ User Tracking 가능
  - ✓ Self-Learning Profiling 기술로 자동화된 DB 보안 정책 생성 및 적용

APPLICATION INSIGHT DFW Function



Section 3. AIONCLOUD

AIONCLOUD

MONITORAPP

AIONCLOUD

- AIONCLOUD 는 웹 보안 서비스를 제공하는 SECaaS 플랫폼 입니다.
- 웹방화벽 서비스 (WAF) 와 웹사이트의 악성코드 감염 진단 서비스 (WMD) 를 제공합니다.
- 웹에 대한 다양한 위협을 차단하여 웹 서버 보호와 성능 향상을 동시에 누릴 수 있습니다

WAF Service

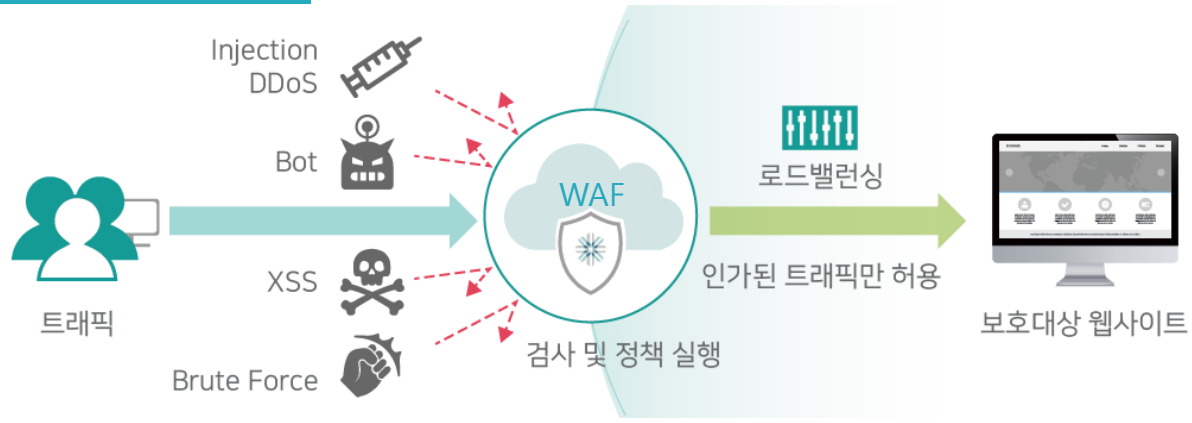
- HW / SW 설치, 유지보수, 라이센스가 필요 없는 강력한 웹 보안과 성능 최적화를 제공하는 서비스
- 다양한 형태의 웹 공격 / 비정상적인 접근 / 개인정보 유출 방지
- SECaaS 플랫폼을 통한 간편한 신청 / 설치 / 설정 / 관리

- 핵심 기능

- WAF 서비스는 웹사이트에 대한 다양한 공격을 방어합니다.
  - OWASP Top 10 취약점
  - Brute Force 공격
  - 악성 파일
  - 시스템 파일 접근
  - CSRF
  - 악성 봇, 스캐너
  - 애플리케이션 취약점
  - SQL / 커맨드 인젝션
  - HTTP DDoS 공격
  - 웹쉘 공격

- WAF 서비스는 웹사이트 운영 최적화 기능을 제공합니다.
  - 멀티 도메인 관리
  - 웹 캐싱으로 웹 가속화
  - SSL 인증서 발행

WAF 구성도



AIONCLOUD

WMD Service

- 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

- 핵심 기능

▪ 웹사이트 진단

- 감염 확인 결과 및 세부 정보 제공
- 직접 진단 기능
- 탐지 시간 / 서버 IP / 서버 포트 / 탐지된 URL / 응답 데이터 / 응답 데이터 크기 에 대한 정보 제공
- 평판 조회 기능

▪ 통계 정보

- 사용자 친화적인 인터페이스 제공
- URL 진단 결과 / 악성 판정 및 진단된 URL 수 / 진행 상태 표시
- 기간별 악성코드 분석에 대한 통계 정보

▪ 웹사이트 관리

- 사용자는 등록된 웹사이트 관리 가능
- 프로토콜 / 도메인 / 경로 / 진단 기간 / 자동 알림 설정 기능

▪ 위협 정보

- AICC (Application Insight Cloud Center)에서 수집한 위협 정보 제공
- 오랫동안 수집 및 처리된 악성코드 정보로 상관 관계 분석

WMD의 멀티 분석 과정

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

MONITORAPP

Thank you

- 서울특별시 구로구 디지털로 27길 27 아남빌딩 8층
- Tel : 02-749-0799
- Fax : 02-749-0798
- Email : sales@monitorapp.com
- Website : www.monitorapp.com