Intelligent SECaaS Platform with Global Presence

AiONCLOUD

MONITORAPP

Contents

1. AIONCLOUD 가 필요한 이유

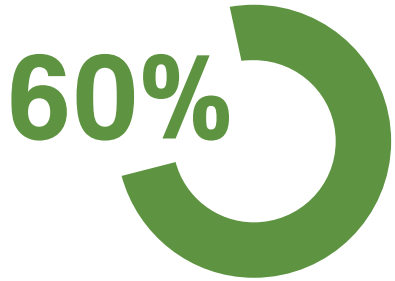
2. AIONCLOUD 개요

3. Website Protection

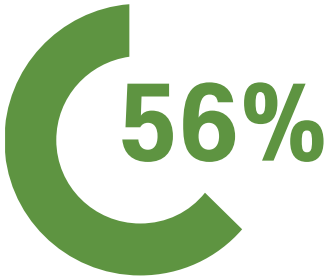
4. Secure Internet Access

1. AiONCLOUD가 필요한 이유

❖ 비즈니스가 직면한 보안 위협 - 웹 취약점



60%의 웹사이트 취약점에 항상 노출



심각한 취약점 중 **56%**만이 해결

62%는 취약점을 이용한 해킹

196

심각한 취약점이 해결되는데
걸리는 시간, **196일**

WhiteHat Security Website Security Statistics Report 2019

❖ Security Threats Faced by Business - Malware

669 million
New malware

2019년 새롭게 발견된 악성코드 수
6억 9천만 개

1 in 13

전체 URL중
7.8%의 멀웨어 발견

1242
Ransomware
per day

2019년 하루 평균 발생한
랜섬웨어 1242 여 개

Symantec Internet Security Threat Report 2019

❖ 원격근무 확산에 따른 보안위협 증가

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

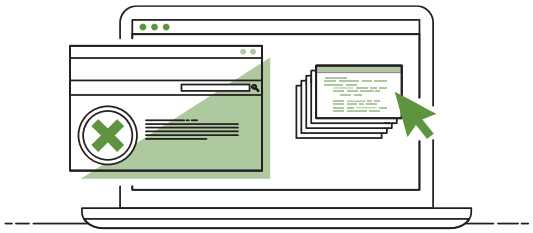
전체 인원의 **64%** 가 원격근무중

148% C19 이전에 비해 증가

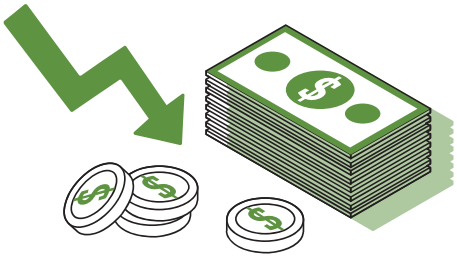
- 전체 직원중 64% 가 원격 근무, 코로나 이전 대비 148% 증가
- 위험한 App이나 사이트에 대한 접근이 161% 증가
- 성인 컨텐츠 트래픽이 600%증가
- 업무용 Device의 개인용도 사용율이 97%증가
- 기업용 협업툴 사용율이 80%증가
- 클라우드 기반의 악성코드 전파가 63% 증가

-TechTarget 2020

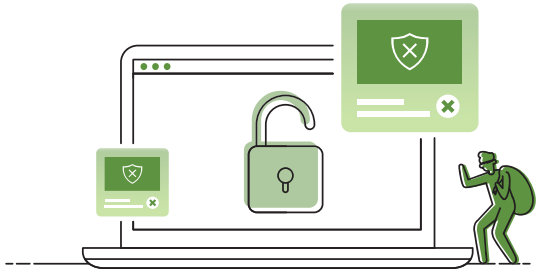
❖ 웹 취약점/악성코드가 기업에게 끼치는 피해



서비스 장애



재정적 손실



개인정보 도난/분실

신뢰도 하락

❖ 웹 보안에 직면한 과제

As Is : 웹 보안에 직면한 과제

- 번거로운 설치

  - 장비 배송, 네트워크 구성, 설치, 테스트 등 번거 로운 설치 과정 요구

- 높은 Total Cost of Ownership (TCO)

  - 초기 투자 비용
  - 도입 후 운영/유지보수 비용
  - 하드웨어, 소프트웨어 구매 비용
  - 트레이닝 및 기술지원 비용

To Be : "Security as a service" 의 이점

- 간편한 서비스 신청

  - 하드웨어, 소프트웨어 설치 불필요
  - 번거로운 설치/테스트 과정 불필요

- 낮은 Total Cost of Ownership (TCO)

  - 초기 투자 비용 불필요
  - 유지보수 비용 불필요
  - 하드웨어, 소프트웨어 구매 불필요
  - 트레이닝 및 기술지원 비용 최소화

직면한 과제의 해결 방법

비용이 저렴하고 쉽게 이용/운영 가능한 **"Security as a Service"**

❖ SECaaS 도입시 고려사항

- ✓ 정말 비용이 절감 되는가 : SW/HW 투자 및 운영 인력 비용
- ✓ 서비스 도입의 용이성 : 핵심 서비스의 영향을 최소화 하여 신속하게 도입
- ✓ 확장성 : 서비스 볼륨과 글로벌 확장의 용이성
- ✓ 전문성 : 보안 전문가의 컨설팅과 사고 발생시 도움
- ✓ 향후 몇 개의 사업자로 구성할 것인가? / 인,아웃바운드 트래픽의 통합 관리?
  어느 부분의 보안 영역까지 Cover할 것인가
- ✓ 네트웍 서비스의 필요성
- ✓ SaaS 보안인증 필요성(국내)

2. ONCLOUD Overview

❖ AIONCLOUD (Application Insight on Cloud) 서비스 소개

AIONCLOUD는 풀 스택 네트워크 보안을 제공하는 첨단 머신러닝 위협 인텔리전트 시스템과 결합한 SASE 플랫폼입니다.

Website Protection

WAF
WMS

Secure Internet Access

SWG
NGFW

AIONCLOUD AISASE

AIONCLOUD의 AI-SASE(Secure Access Service Edge)는
네트워크 및 보안을 위한 원스톱 서비스 플랫폼

❖ AIONCLOUD 주요 기능

Website Protection

1

웹 보안 향상

2

웹 공격/악성코드
탐지 및 방어

3

웹 사이트 성능 최적화


SSL 가시성

Secure Internet Access

1

네트워크 보안 향상

2


인터넷 접근 제어

3

작업 생산성 향상

❖ AIONCLOUD Global Network

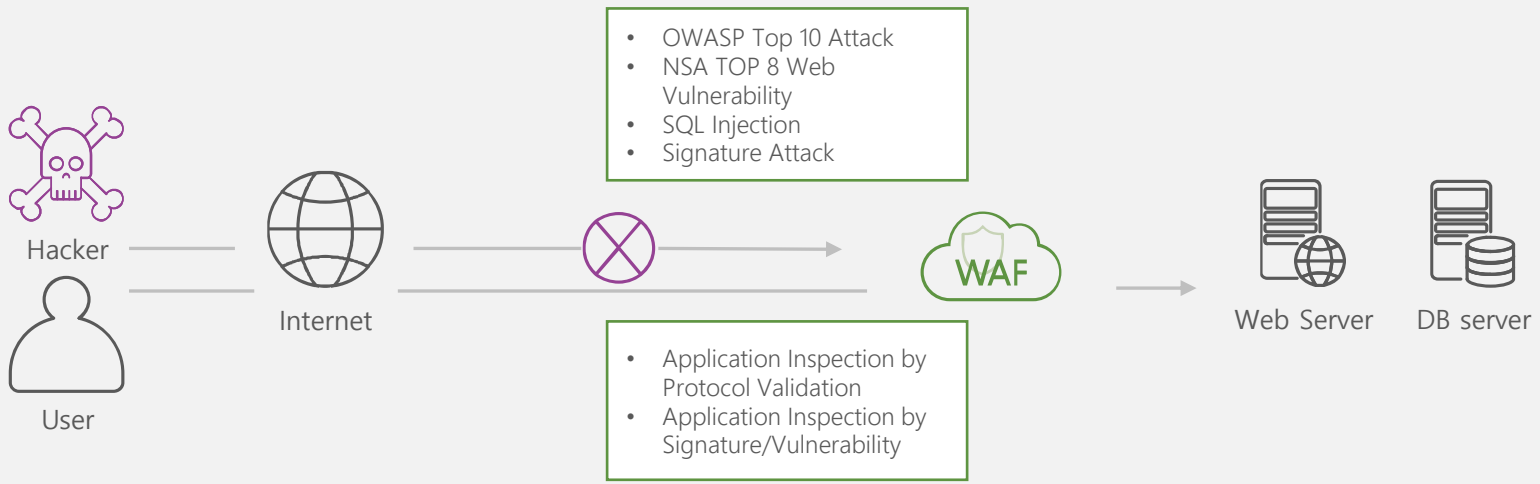
- AIONCLOUD는 전세계 15개 지역의 40개 데이터센터에 서비스 인프라를 보유하고 있습니다.

3. Website Protection

❖ WAF (Web Application Firewall) 서비스 소개

- 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

WAF Diagram



❖ 왜 WAF를 선택해야 할까요?

Robust Security Service

클라우드 기반의 보안 서비스로서 오늘날 가장 위협적인 공격에 대한 완벽한 보안 제공

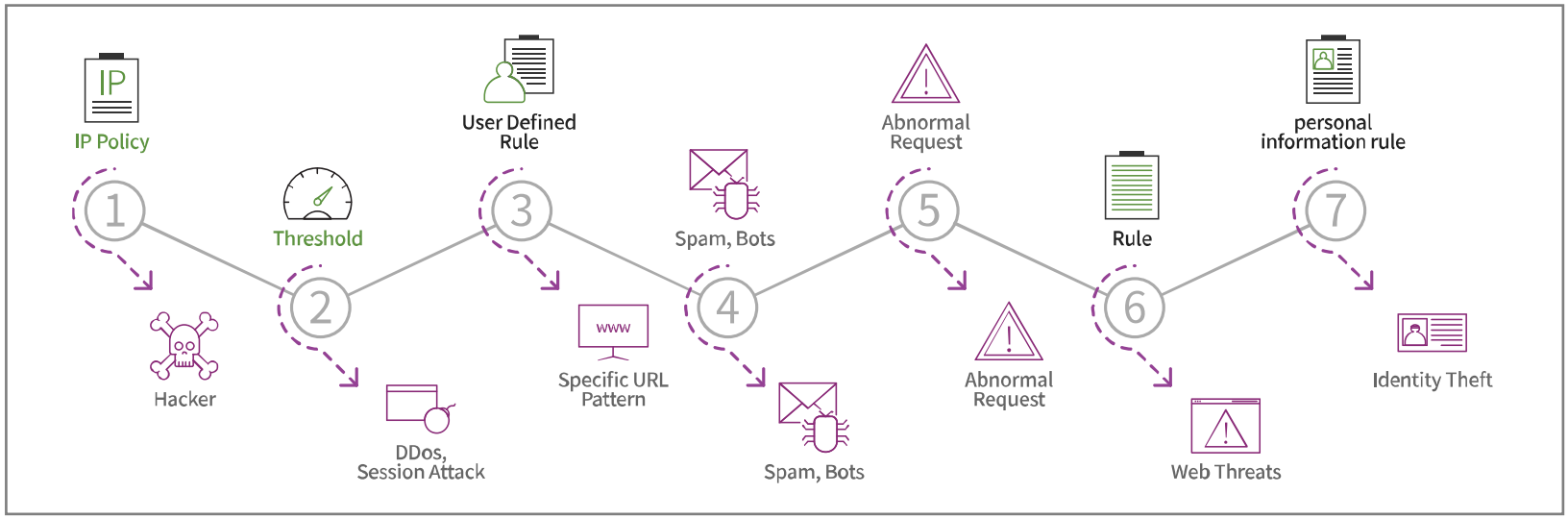
Simple Management

IT 전문 지식이 부족하더라도 쉽게 모니터링 및 방어 할 수 있도록 간편한 보안 정책 설정 및 직관적인 UI 제공

Cost Effective

사용한만큼 지불하는 Pay-as-you-go 가격 정책으로 비용에 대한 부담 없이 서비스 이용

❖ 강력한 보안 서비스



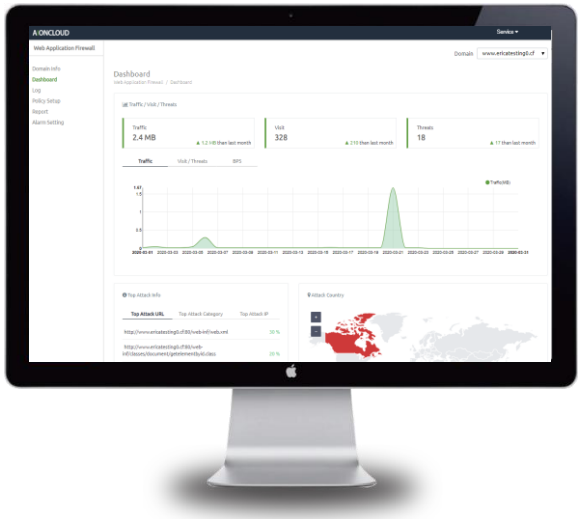
- WAF 는 오늘 날 웹 사이트에 영향을 미치는 가장 위협적인 공격들을 방어합니다.

- SQL Injection
- Web Server Vulnerability
- Malicious File
- System File Access
- Cross Site Script
- Application Vulnerability
- Directory Listing
- Directory Traversal
- Scanner & Bot
- CSRF
- Command Injection

❖ 간단한 관리

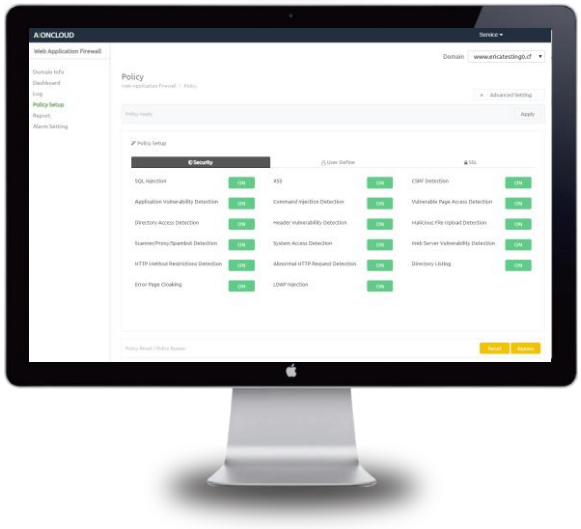
❑ Intuitive UI

- 사용자 친화적인 인터페이스 제공
- 실시간 모니터링
- 유형 별/ 시간 별/ 일자 별 로그 통계 및 보고 기능



❑ Simple security setting

- 3가지 운영모드 제공 (Bypass/ Detect/ Block)
- 스위치 타입의 쉬운 정책 설정

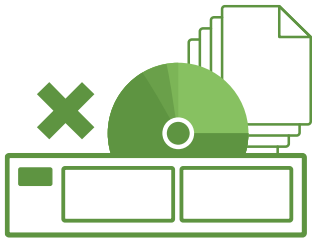


❖ Cost effective

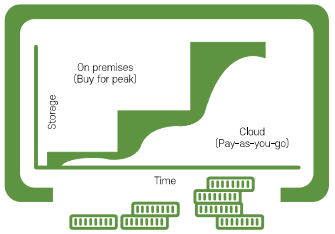
- 5GB까지 무료 서비스
- Pay-as-you-go 가격 정책으로 사용한 만큼만 지불하는 종량제 서비스
- 별도의 하드웨어나 소프트웨어 설치 비용 절감
- 추가적인 초기 비용 불필요

Cost Reduction of WAF

초기 비용 불필요 ☑



하드웨어 소프트웨어 설치 불필요 ☑



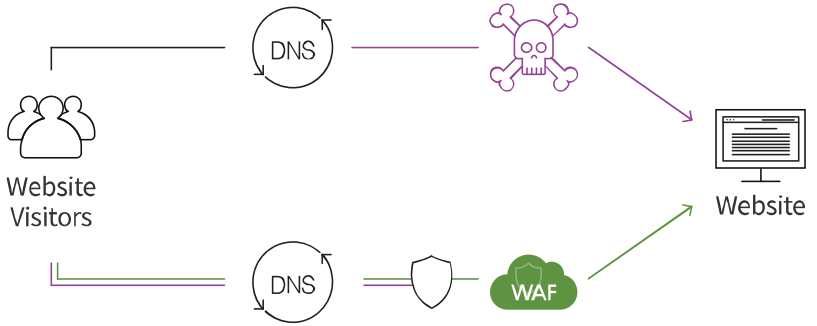
사용한 만큼만 요금 지불 ☑

❖ AIONCLOUD WAF 사용법

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

❖ WMS (Website Malware Scanner) 서비스 소개

- 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

WMS의 분석 과정

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

❖ 왜 WMS를 선택해야 할까요?

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

❖ WMS의 주요 기능

웹사이트 진단

- 감염 확인 결과 및 세부 정보 보기
- 직접 진단 기능
- 탐지 시간 / 서버 IP / 서버 포트 / 탐지된 URL / 응답 데이터 / 응답 데이터 크기 에 대한 정보 제공
- 사용자는 평판을 볼 수 있습니다.

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

❖ 멀티 레벨 분석

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

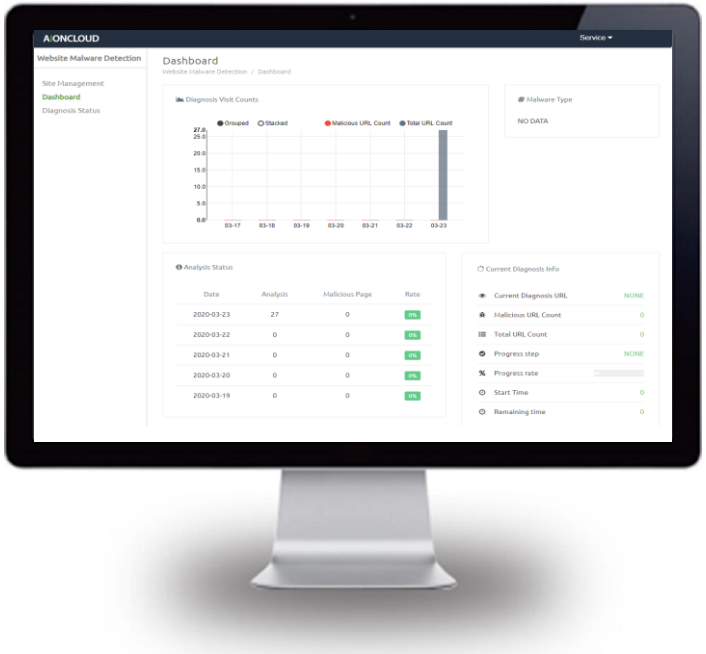
❖ WMS는 멀티 레벨 탐지/분석을 수행하여 악성코드를 탐지

- 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

❖ 악성코드 진단 서비스

- **Granular Report**
  - 진단 URL/ 악성 URL 수/ 진단 URL 수 표시
  - 기간 별 악성코드 분석 통계 정보 제공
  - 도메인 진단 범위 설정 (외부/ 내부 도메인)

- **Malware Alert**
  - 진단 결과 자동 보고서 발송
  - 악성코드 탐지 시 이메일 알림 기능 제공



❖ AIONCLOUD WMS 사용법

1. 도메인 등록

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

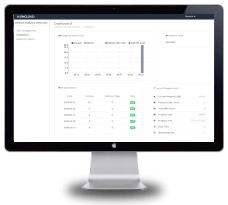
2. 진단 스케줄 설정

- 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

4. Secure Internet Access

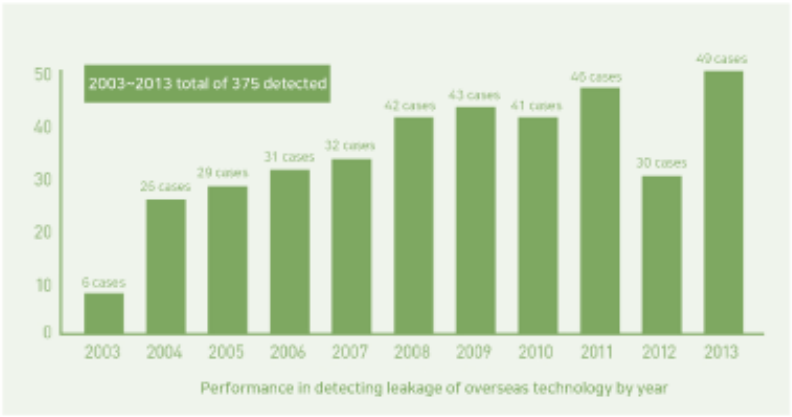
❖ DLP(Data leak protection)솔루션 필수

- **기밀 데이터 유출로 인한 기업 손실**

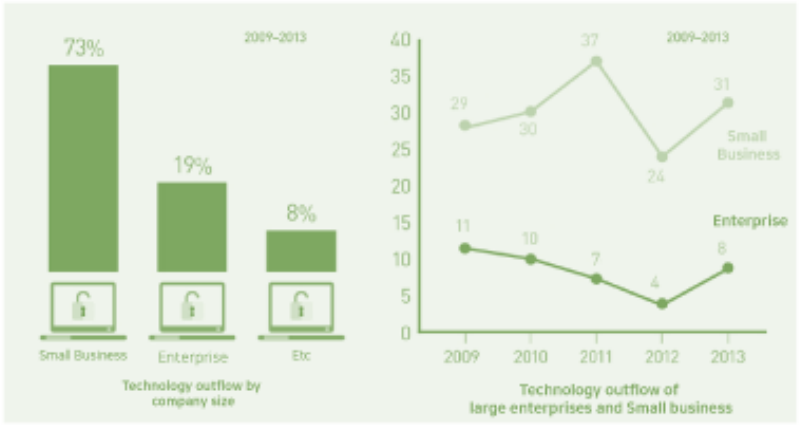
  → 기업의 85%가 데이터 유출 경험이 있으며, 이 중 80%는 내부 사용자에 의한 유출

"산업 스파이는 21 세기의 가장 큰 사업 중 하나이며
결코 사라지지 않을 것입니다."

- Alvin Toffler



Source: Industrial Confidentiality Protection Center



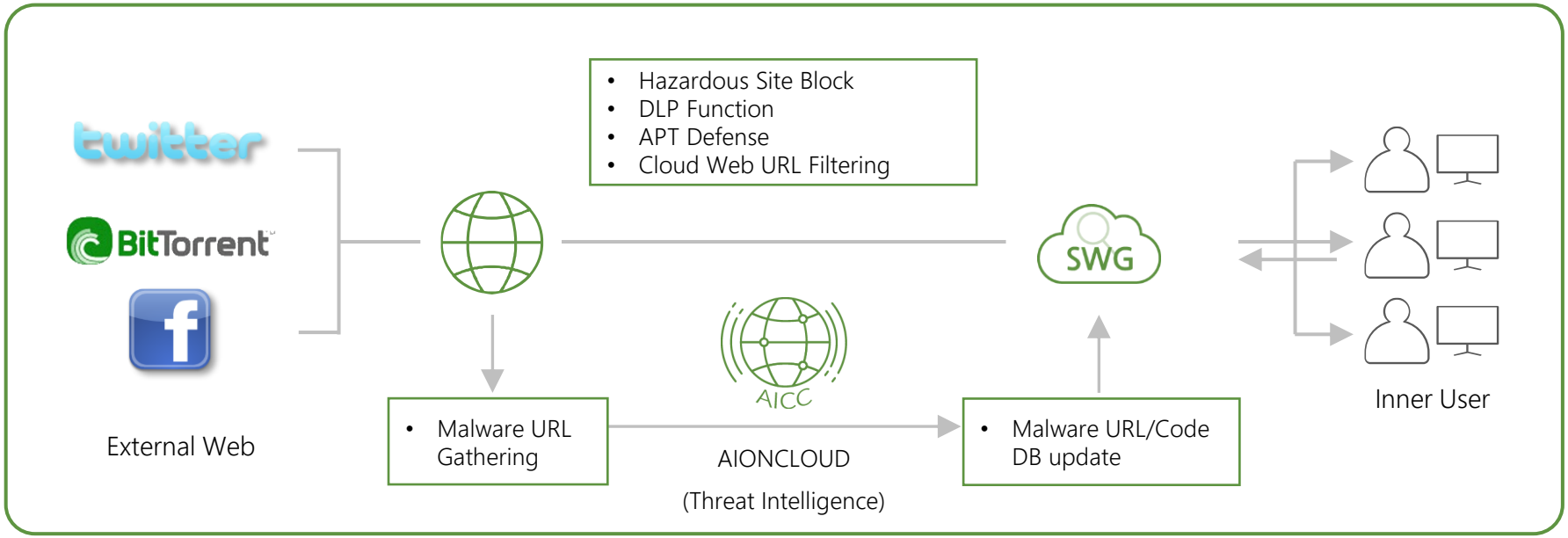
Source: Industrial Confidentiality Protection Center

IT 기술의 발달로 인간이 사용하는 거의 모든 재료와 시스템이 디지털화되고 관리되고 있습니다.

→ 해킹 및 데이터 유출로 인한 장애가 용이해짐

❖ SWG (Secure Web Gateway) 서비스 소개

AIONCLOUD SWG 서비스를 통해 직원의 웹 활동을 모니터링, 차단 및 보고할 수 있습니다. SWG는 네트워크가 알려진 악성 사이트에 액세스하지 못하도록 보호하여 네트워크를 안전하게 유지하면서 기업의 생산성을 높여줍니다.



양방향 악성 트래픽 탐지

❖ 왜 SWG를 선택해야 할까요?

쉬운 설치

간단하고 쉬운 설명을 따라 트래픽을 구성할 수 있음

유연한 정책 설정

사용자 또는 부서별로 유연하고 자세한 정책 설정 가능

경제적 합리적 솔루션

사용자 수에 따라 필요한 만큼만 지불 가능

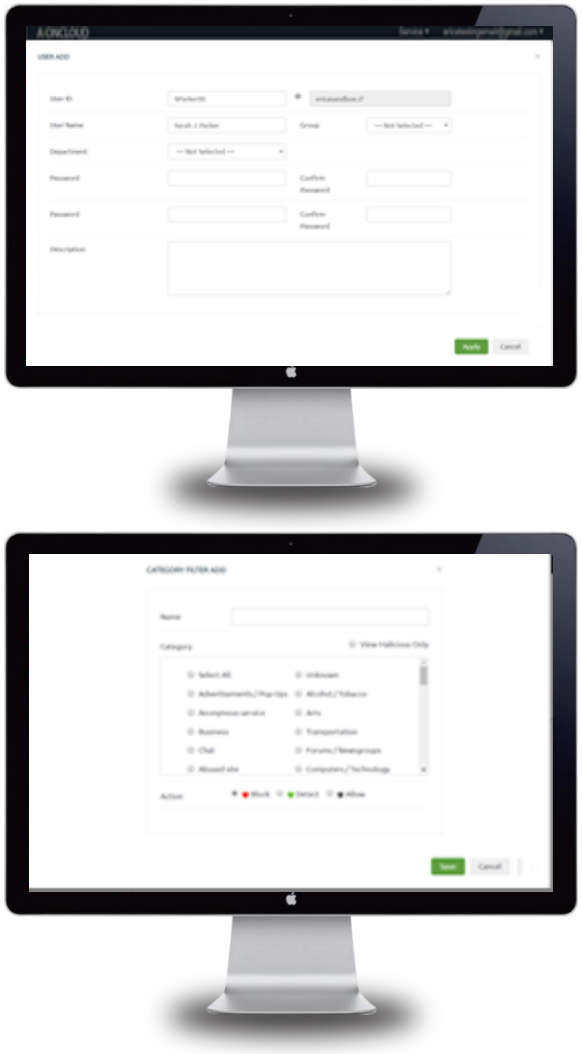
❖ 간단한 관리

❑ 간편한 사용자 설정

- 자세한 사용자 설정
- 부서 설정 가능

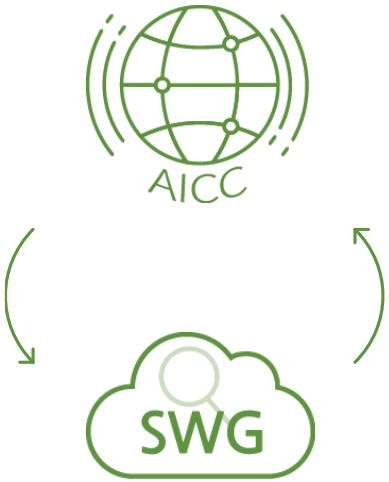
❑ 단순 정책 설정 및 범주 필터

- 3가지 작동 모드(바이패스/탐지/블록)
- 클릭 한 번의 정책 설정으로 사용할 수 있는 카테고리 필터링



❖ 위협 인텔리전스 분석으로 60여개 카테고리 분류

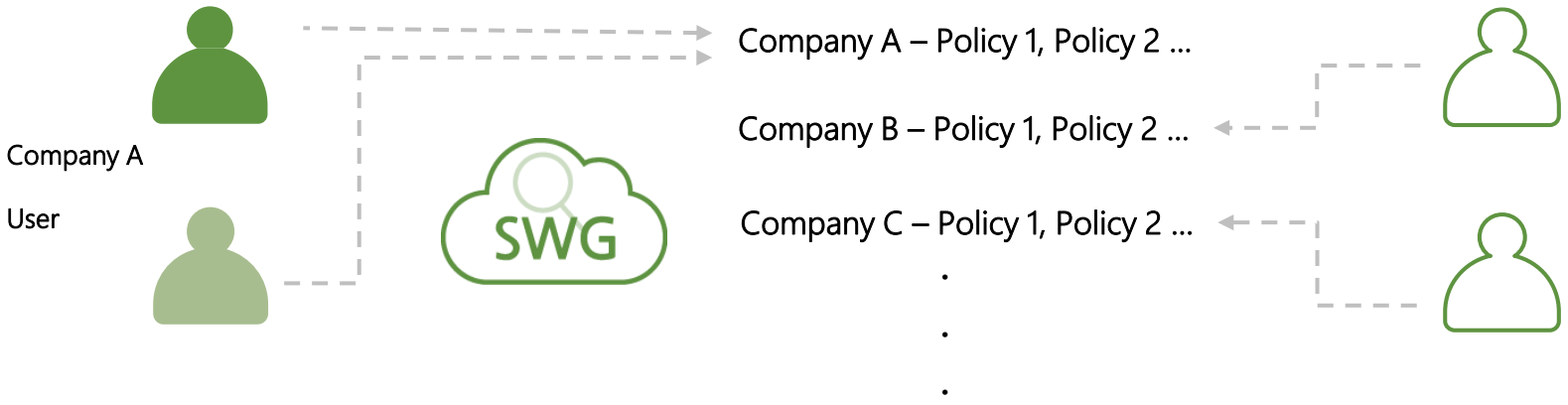
- **카테고리 필터링은 신종 위협 스트레스로부터 자유롭게 해줍니다.**



- AICC는 머신러닝 및 샌드박스 기술을 통해 수집된 수많은 위협 사건에 대한 동적 및 정적 분석을 수행하여 공격자를 식별하고 공격의 목적, 목표 및 행동에 대한 정보를 파악합니다.

- AICC의 데이터는 AIONCLOUD의 SWG에서 지속적으로 업데이트되어 새로운 악성 악성 악성 프로그램 및 사이트를 최신 상태로 유지하여 최신 위협으로부터 사용자를 보호합니다.

❖ 다중 사용자 그룹 관리



- **사용자 중심 정책 설정**
  - 보안 정책 생성을 위한 다중 규칙 결합 (enable / disable / exception handling, etc.)
  - 사용자 또는 그룹별로 생성된 보안 정책 적용
- **다중 사용자 그룹 관리**
  - 특정 조직의 정책 설정 및 운영 범위 제한 능력
  - 기업규모가 크거나 복잡하거나 관리부서 간 보안담당관이 다른 경우도 유연한 정책 설정 가능
  - 다중 사용자 그룹 관리를 통해 고객(또는 조직)별로 논리적으로 완전히 분리된 정책 수립

❖ AIONCLOUD SWG 사용법

1. Register ID and domain

- 정보 등록
- 사용할 도메인 이름 등록

2. Change PAC settings

- AIONCLOUD에 제공된 지침에 따라 PAC 설정 변경

3. Policy setting

- 정책 설정을 생성하거나 AIONCLOUD에서 제공하는 60개 이상의 범주에서 선택

4. Set policy by user or department

- 사용자 또는 부서에 정책할당
- 이제 AIONCLOUD의 관적인 대시보드에서 모든 활동을 모니터링할 수 있습니다.

❖ 위협 인텔리전스

- 전 세계적으로 발생하는 위협을 수집하고 분석하여 진화하는 위협에 대응
- 사이버 보안 위협에 대한 사전 예방적 예측
- 유사성 분석을 통한 신종 및 변종 위협 탐지

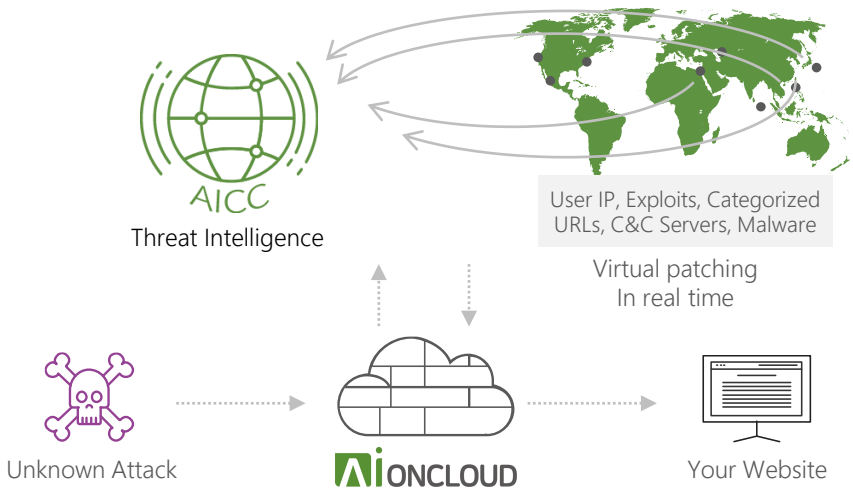
◈ Virtual Patching

- 알려진 악성정보 및 위협 인텔리전스가 수집한 악성 정보에 대한 패턴을 생성하여 실시간으로 패치

◈ Machine Learning

- 신속하고 정확한 위협 자동 분석 및 악성여부 판별
- 알려지지 않은 공격 및 신종/ 변종 공격에 대한 대응

Profiling Technology



5. AIONCLOUD 무상체험 신청하기(SCK)

AIONCLOUD 무상체험 신청하기

❖ AIONCLOUD 신청 Process

체험 신청 › 전문 파트너사 가이드 › AIONCLOUD 등록 › 회원가입 › 사이트 등록

AIONCLOUD

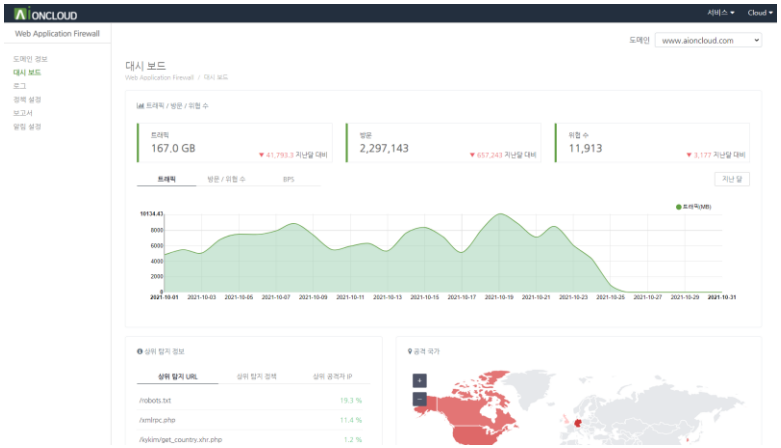
사이트 방어 및 관리자 체험 ‹ 방역 결과에 대한 가이드 ‹ 유상전환 프로모션 참여 ‹ 안전하고 성공적인 Business 도약

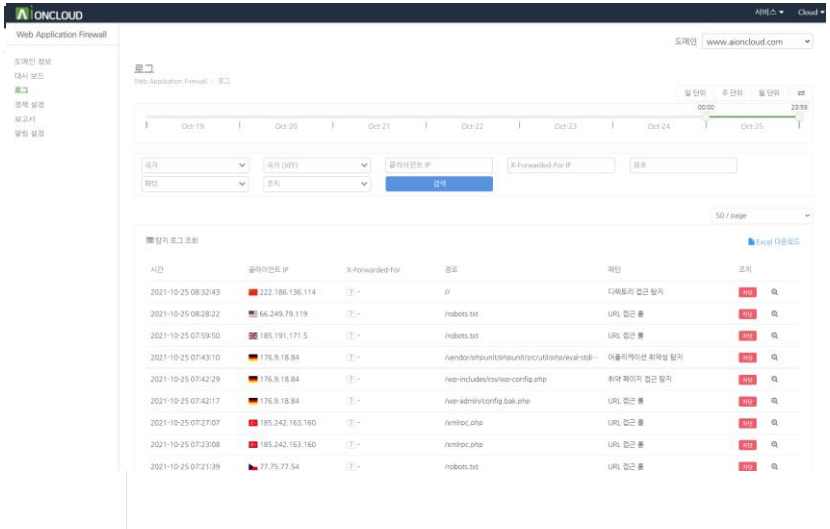
유상전환 프로모션 참여
3개월 무상 서비스(25% 할인)
구독 금액에 따른 상품 지급

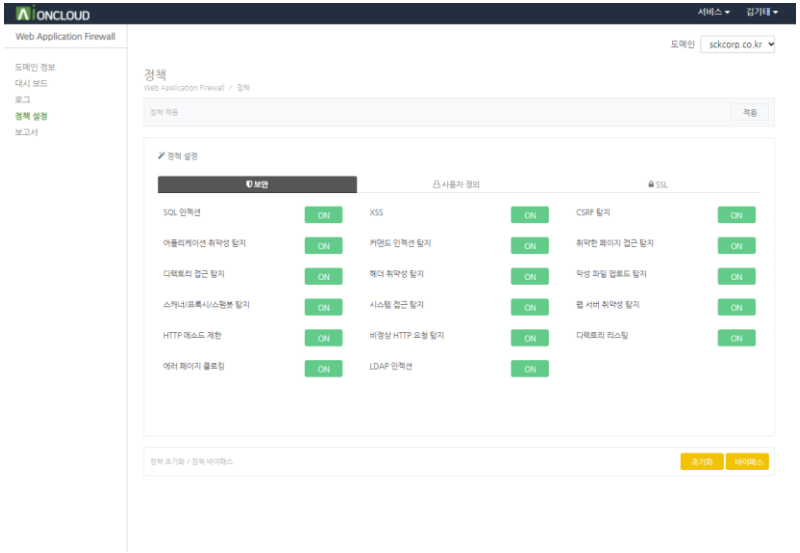
* 프로모션은 이번 웨비나를 통해 신청 하신 고객사에 한하여 특별히 제공 되는 프로그램 입니다.

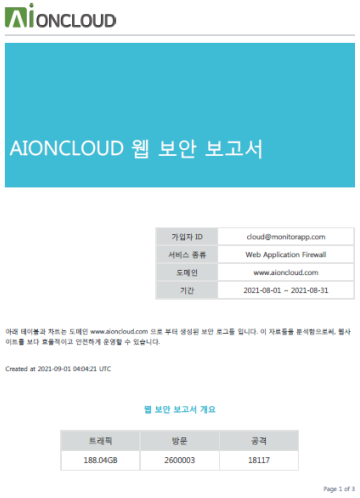
AIONCLOUD 무상체험 신청하기

❖ AIONCLOUD 결과 Report 예시





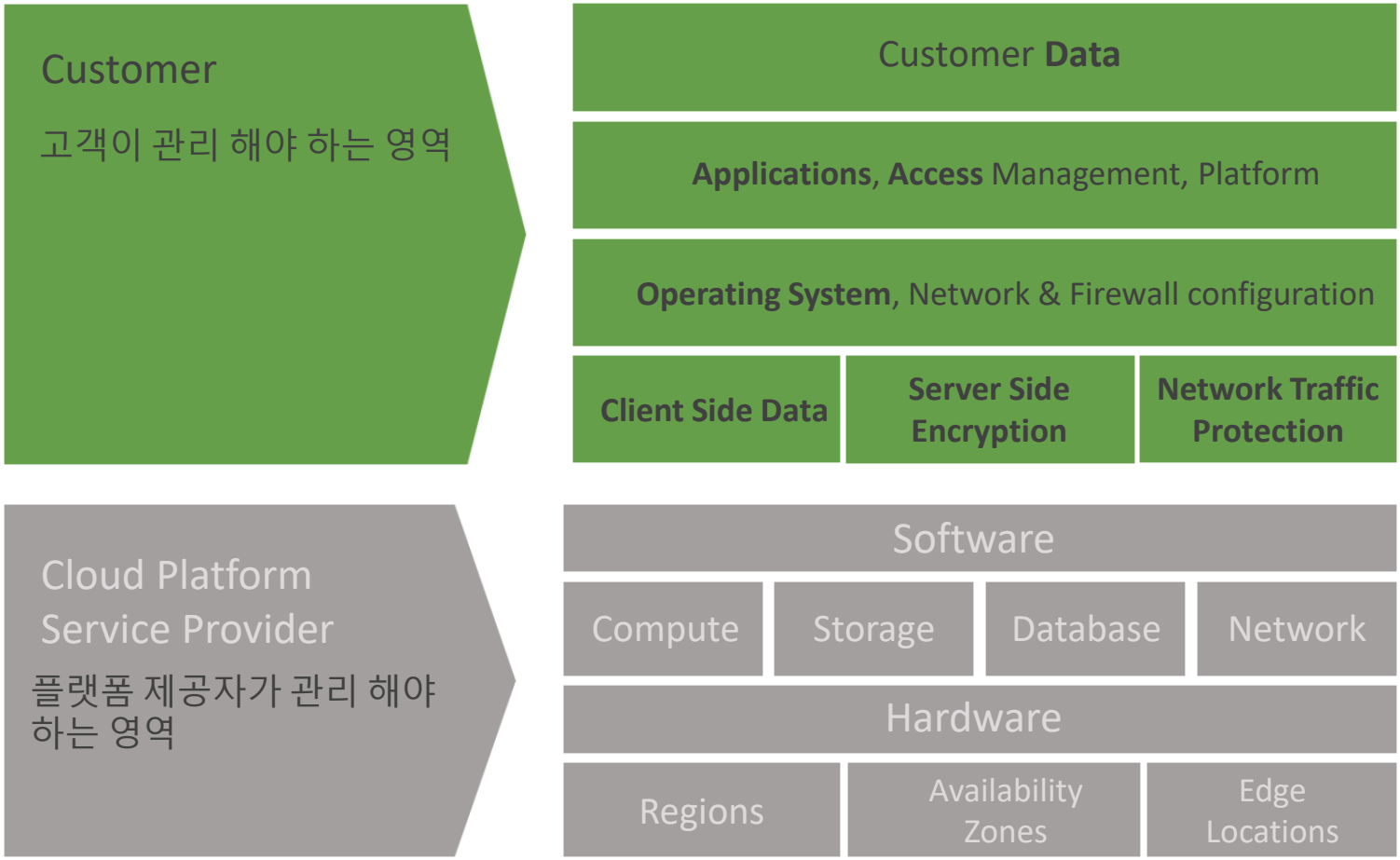




6. 안랩 CPP와 Office Security 소개

안랩 CPP와 Office Security 소개

❖ **왜 클라우드 보안이 필요할까?**



안랩 CPP와 Office Security 소개

❖ 클라우드 보안의 관리 포인트

1. Prevent data leakage

4. Visibility and threat detection

2. Strong authentication

5. Continuous compliance

3. Data encryption

6. Integrated security

안랩 CPP와 Office Security 소개

❖ 클라우드 보안의 통합 위협 관리 및 대응 플랫폼 CPP 간단 소개

“ 클라우드 엔드포인트 통합 보안을 위한 보안 모듈 제공 ”

Anti-Malware

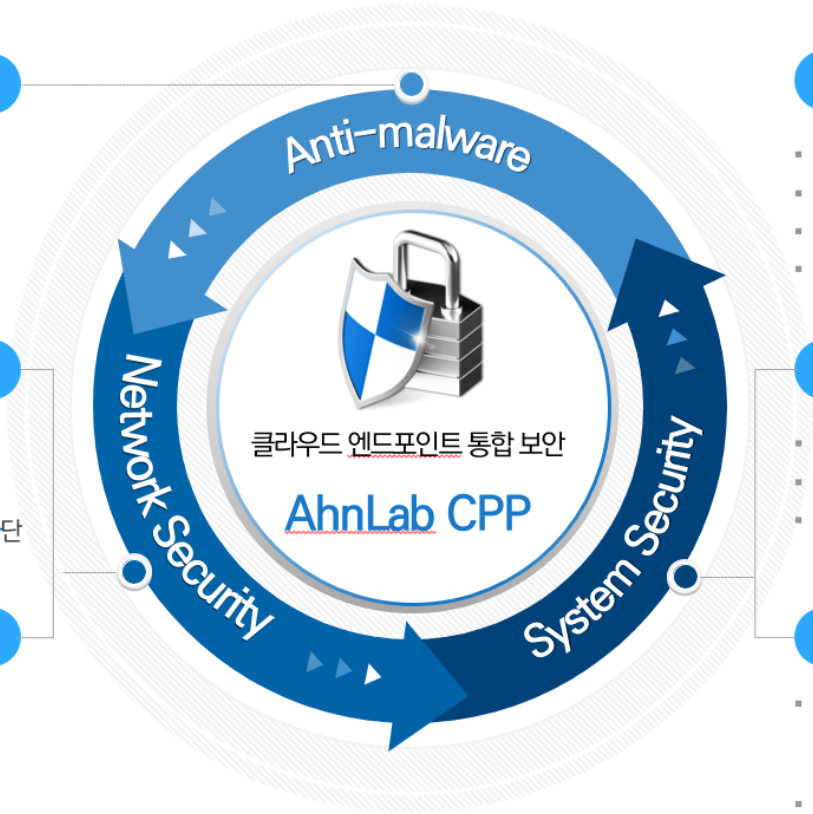
- 악성코드 실시간 검사
- Host, Container 탐지 및 가시성 제공
- 검사 성능/리소스 이슈 최소화

Host IPS

- 취약점에 대한 시그니처 추천 (가상패치)
- 네트워크 침입 공격에 대한 탐지 및 차단
- 내부 공격(Lateral Movement) 탐지 및 차단

Host Firewall

- IP, Port , 프로토콜 기반 통신 제어
- 국가 기반 차단 지원



Management

- 탐지 / 대응에 대한 실시간 가시성 제공
- 그룹별 관리자 권한 설정
- 서버 가용성을 위한 리소스 사용량 통제
- 상세 로그 및 리포팅 제공

Application Control

- 화이트리스트 기반 애플리케이션 실행 제어
- 조건에 따른 애플리케이션 실행 허용
- 중요 파일에 대한 접근 제어

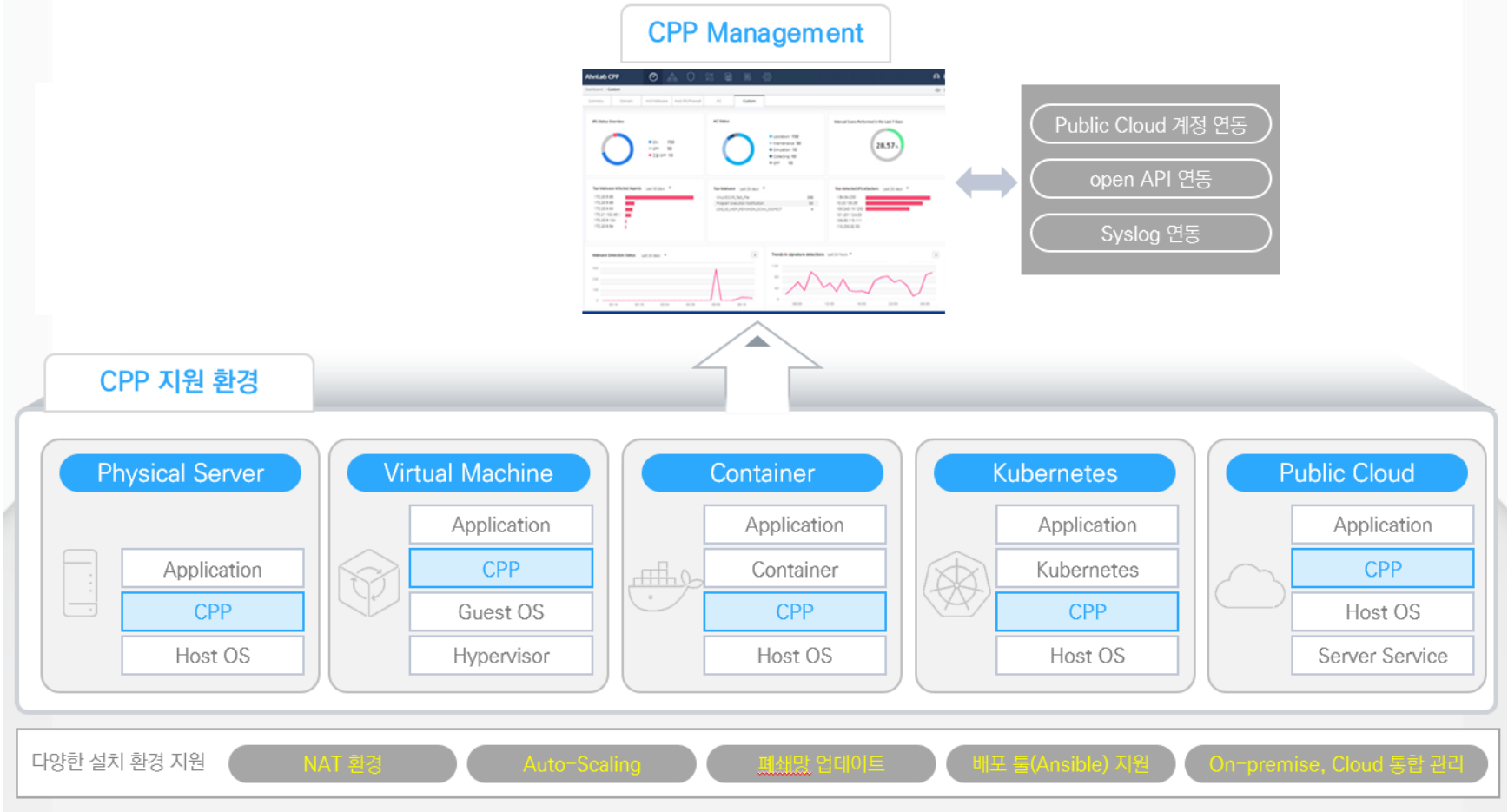
Integrity Monitoring

- 파일, 디렉토리, 서비스, 데몬, 프로세스, 레지스트리 키/값, 시작프로그램에 대한 무결성 모니터링
- 실시간 /수동/예약 검사 지원

안랩 CPP와 Office Security 소개

❖ 클라우드 보안의 통합 위협 관리 및 대응 플랫폼 CPP 간단 소개

“ 다양한 환경에 적용 가능하고 유연한 구성/연동 가능 ”



안랩 CPP와 Office Security 소개

❖ **SaaS 기반의 통합 보안 솔루션 Office Security 간단소개**

7. SCK 보안진단 프로그램 소개

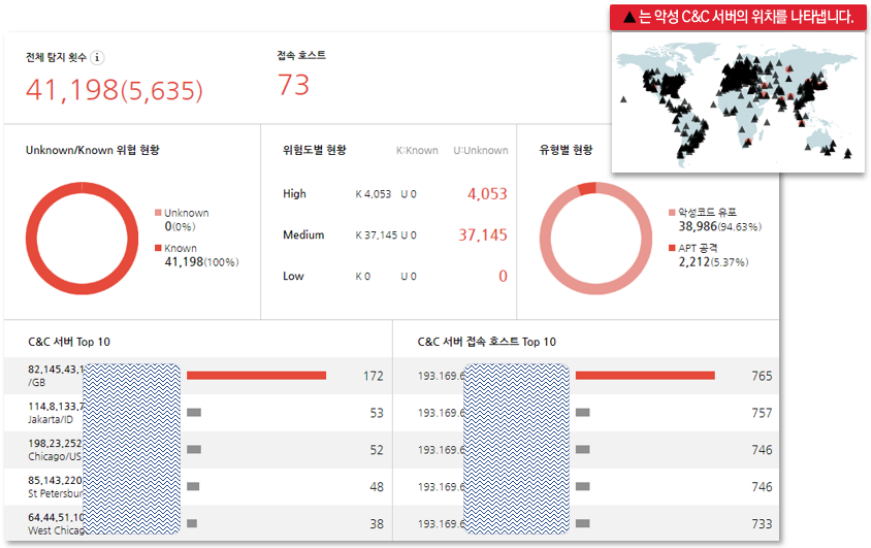
SCK 보안진단 프로그램 소개

❖ 보안 취약점을 가시화 하여 대응 방안 확보

사전 미팅 → 로그 수집 → 데이터 분석 → 리포트 전달 → 대응방안 확보 → 컨설팅 완료

[수집 가능 데이터]

1. Ransomware
2. Attack Initiation(공격유입)
3. Exploit(취약점 공격)
4. InfoStealer(정보유출)
5. AutoRun(자동실행 프로그램)
6. Injection Attack
7. System Manipulation(시스템 변조)
8. Anti-AV/Detour(보안솔루션 우회)
9. C&C/Malicious URL(네트워크연결)
10. Lateral Movement(내부 확산)



SCK 보안진단 프로그램 소개

❖ 보안 취약점을 가시화 하여 대응 방안 확보

[SCK 보안진단프로그램]

1. 진행 주체 : SCK, 전문 파트너사
2. 비용 : 무상
3. 기간 : 4주~6주
4. 내용
   1) 고객사 환경의 전반적인 위협 탐지
   2) 탐지된 위협에 대한 대응 방안 제시

[보안 정밀진단 프로그램]

1. 진행 주체 : AhnLab, SCK
2. 비용 : 유상
3. 기간 : 4주~6주
4. 내용
   1) 개별 시스템의 잠재적인 보안 위협 탐지
   2) 탐지된 위협에 대한 대응 방안 제시

THANK YOU

㈜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 |