




WAAP로 진화하는 웹 애플리케이션 보호 솔루션 비교 및 선택 가이드

MONITORAPP | 박호철 팀장

Contents

CONTENTS

1. 웹 애플리케이션이 직면한 위협 요소
2.  IONCLOUD WAAP
(Web Application and API Protection)

WAAP (Web Application & API Protection)

WAF

API

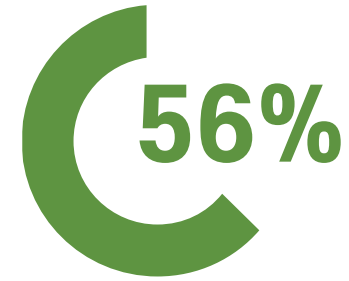
Bot

DDoS

Security Threats Faced by Business - Website



60%의 웹사이트 취약점에 항상 노출



심각한 취약점 중 56%만이 해결



62%

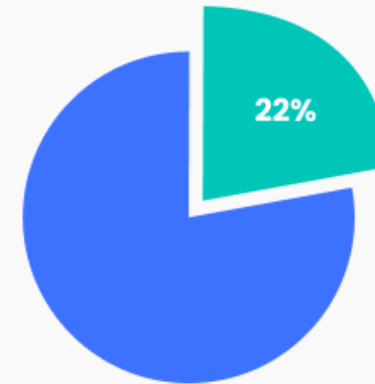
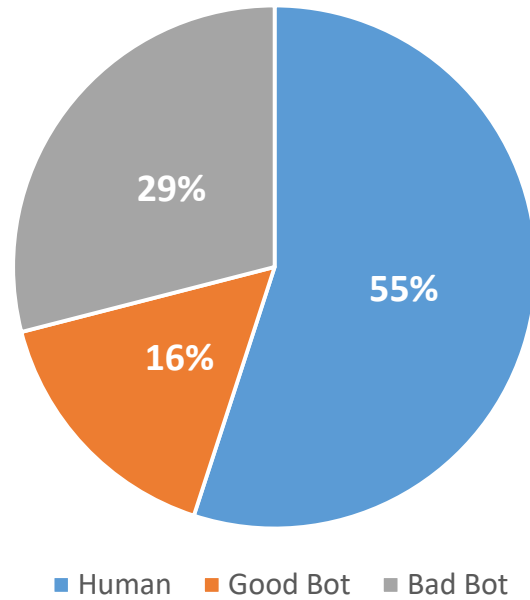
62%는 취약점을 이용한 해킹

196

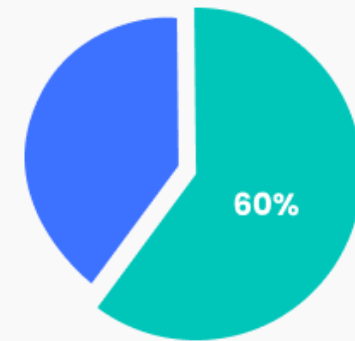
심각한 취약점이 해결되는데 걸리는 시간, 196일

Bot traffic and threat of Account Takeover

(2021) Human vs Good Bot vs Bad Bot



22% of adults in the US have been a victim of account takeover fraud.



60% of account takeover victims had used the same password for multiple online accounts.

Bot 기반의 공격 빈도, 강도 및 복잡성은 지속적으로 증가하며
계정 탈취(Account Takeover) 위협은 매우 심각한 위험 요소

Bot traffic and threat of Account Takeover

65% of people reuse the passwords

73% of users use same password both personal and work accounts

34% of the overall authentication traffic is malicious(by OKTA)

44Millions accounts are vulnerable(by Microsoft)

0.2%~1% , Success rate of credential stuffing attack

Credential Cracking(brute force) : **Credential Dictionaries, Randoms & Brute Forcing**

Credential Stuffing : **Stolen Login Credentials**

Bot traffic Abuse

유형	목적	주요 대상
Price Scraping	경쟁 업체 대비 가격 경쟁력 확보	<ul style="list-style-type: none"> • 전자 상거래 • 도박 • 항공사 • 여행
Content Scraping	컨텐츠 도난	<ul style="list-style-type: none"> • 채용 공고 • 마켓 플레이스 • 디지털 출판 • 부동산
Denial of Inventory	상품 독점 후 재판매	<ul style="list-style-type: none"> • 항공사 • 티켓 • 수강신청
Account Creation	무료 계정 생성을 통한 크레딧(돈, 포인트 등) 획득	<ul style="list-style-type: none"> • 소셜 미디어 • 데이트 사이트 • 커뮤니티 • 도박
Account Takeover (Credential Stuffing)	계정 도용	<ul style="list-style-type: none"> • 로그인 되는 모든 웹 사이트

Bot mitigation solution

Rate Limiting (**USER Identification = IP, XFF IP, Fingerprint, SESSION ID, Header value...**)

CAPTCHA

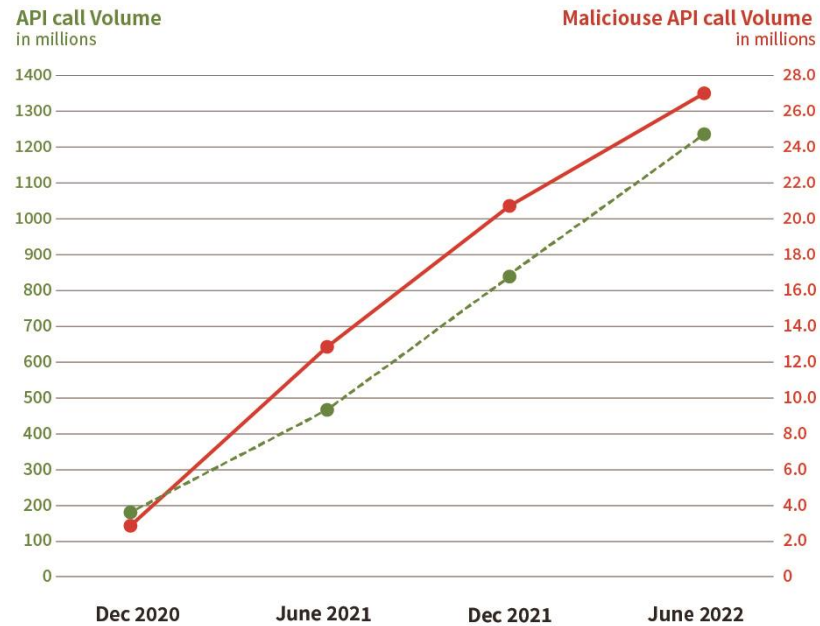
Honeypot Trap

Java Script Challenge (Human Interaction Challenge / Device Fingerprinting ...)

leaked credential DB

...

The explosive growth of API & API security need



OWASP API Security Top 10 2023

- API 1: Broken Object Level Authorization
- API 2: Broken Authentication
- API 3: Broken Object Property Level Authorization
- API 4: Unrestricted Resource Consumption
- API 5: Broken Function Level Authorization
- API 6: Unrestricted Access to Sensitive Business Flows
- API 7: Server Side Request Forgery
- API 8: Security Misconfiguration
- API 9: Improper Inventory Management
- API 10: Unsafe Consumption of APIs

클라우드 및 마이크로서비스 아키텍처 등장으로 다양한 서비스와 애플리케이션 연결을 위한 API는 필수요소

폭발적인 API 성장에 따른 **API 취약점 공격 및 부정 접근 완화를 위한 전문적인 보안 솔루션 필요**

API Security solution

API Discovery

Signature-based attack detection & Spec violation

Rate limit & enforced timeout

Access IP and Geolocation

File upload size and extension limit

Validate – JWT (JSON Web Token)

Validate – Claim & Component

...

Validate – Claim & Component

Encoded PASTE A TOKEN HERE

```
eyJhbGciOiJIUzI1NiIsInR5cCI6IkpXVCJ9.eyJzdWIiOiIxMjM0NTY3ODkwIiwibmFtZSI6IkpvaG4gRG91IiwiaWF0IjoxNTE2MzY0MDUyfQ.Sf1KxwRJSMeKKF2QT4fwpMeJf36P0k6yJV_adQssw5c
```

Decoded EDIT THE PAYLOAD AND SECRET

HEADER: ALGORITHM & TOKEN TYPE
<pre>{ "alg": "HS256", "typ": "JWT" }</pre>
PAYLOAD: DATA
<pre>{ "sub": "1234567890", "name": "John Doe", "iat": 1516239022 }</pre>

```
PUT /api/2.2/sites/9a8b7c6d-5e4f-3a2b-1c0d-9e8f7a6b5c4d/users/9f9e9d9c-8b8a-8f8e-7d7c-7b7a6f6d6e6d HTTP/1.1
HOST: my-server
X-Tableau-Auth: 12ab34cd56ef78ab90cd12ef34ab56cd
Content-Type: application/json

{
  "user": {
    "fullName": "John Doe",
    "siteRole": "ViewerWithPublish"
  }
}
```

Value 일치 여부 검증

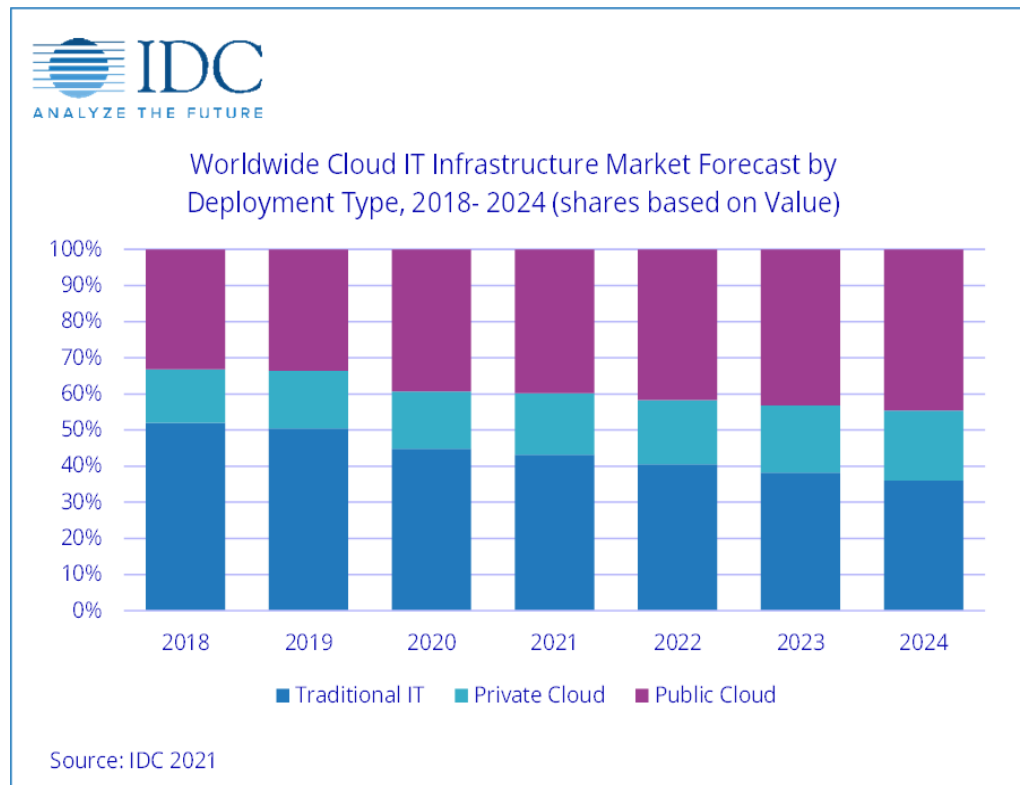
→

지정한 컴퍼넌트(path, 파라미터, 쿠키, 헤더 등)에 클레임이 존재 하는가?

클레임 이름과 지정 컴퍼넌트 이름이 다름에 유의

Migrate data and applications to the cloud

- 데이터와 애플리케이션의 위치가 클라우드로 전환



- 프로덕션 환경의 멀티·하이브리드 클라우드화

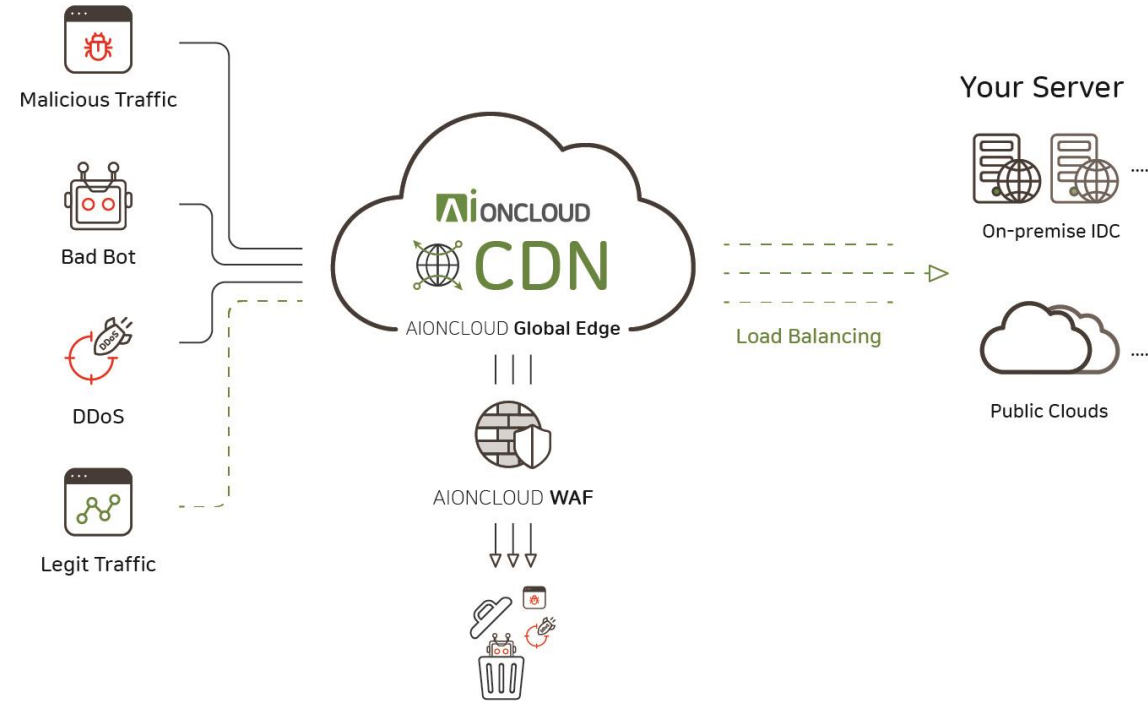
- 기업의 94%가 클라우드를 사용

- 기업 워크로드의 83%가 클라우드에 위치

- SMB의 94%가 클라우드로 전환 후 보안 이점 보고

- 2025년까지 클라우드 저장 데이터 100ZB 예상

Single-Point Security for Hybrid · Multi-Cloud



Cloud는 선택이 아닌 필수이며 Cloud 전환에 보안은 가장 큰 고려 요소

웹 애플리케이션 프로덕션 환경과 독립적인 단일 지점에서 강력한 보안을 구성하고 관리

SECaaS WAAP Vs APPLIANCE WAAP

■ SECaaS(Security as a Service)

- 보안 솔루션을 클라우드 서비스로 이용(구독)하는 방식

■ APPLIANCE(Physical / Virtual)

- Physical : On-premise
- Virtual : Public Cloud 또는 Private Cloud에 Virtual APPLIANCE 가상머신을 배치/구성하는 방식

	SECaaS WAAP	APPLIANCE WAAP
배치	Reverse Proxy (DNS 변경)	In-Line Reverse Proxy (DNS 변경)
트래픽 비용	사용한 만큼 과금	비용 증가 없음 (East-West)
보안 상품 구성	보안 상품별/기능별 구독	제공 되는 모든 기능 사용
보안 설정	심플하고 직관적 (Provider가 최적의 템플릿 제공)	상세한 보안 설정 (운영자의 유연한 규칙 설정)
운영 및 관리 (패치/업데이트 등)	Provider가 관리	직접 운영 및 관리

- 최종 선택은 조직의 요구 사항, 예산, 보안 요건 및 확장성

AIONCLOUD WAAP Vs CSP Native WAAP

	AIONCLOUD	CSP A사	CSP G사
Type	SECaaS	CSP native product	CSP native product
Traffic route	Change DNS	in architecture	in architecture
Price	Traffic or Bandwidth	Rules and request count	Rules and request count
Protection perimeter	Any where	internal resources	internal resources
Feature capacity	Fully	1500 WCU	Security policy limits per project 10 Security rule limit per project 200
Access control	O	O	O
Rate limit	O	O	O
Web Attack - Injection, XSS, CSRF ...	O	△ (Need to managed rule)	ModSecurity Core Rule Set(CRS)
Security Rule Edit	Web UI	Web UI	Text base Editor
Bot Mitigation	O	O	add reCAPTCHA products (costs)
API Security	O	O	add API Security products (costs)
L7 DDoS Mitigation	O	O	O
Custom block page	O	O	X (only change HTTP Response code)
Content Caching	O	X	add CDN option (costs)
Log	3 Month(default)	3 Hours(default)	30 Days(default)
Forward events	SIEM (default)	add archive products (costs)	add archive&monitoring products (costs)
Dashboard / Report	O	add monitoring products (costs)	
API	O	O	O

| **AIONCLOUD** Website Protection

Website Protection

AISASE(Secure Access Service Edge) Platform



- 전체 네트워크 보안 스택을 클라우드 기반 서비스 플랫폼으로 제공
- 모든 사용자, 모든 엔드포인트, 모든 애플리케이션에 대한 액세스를 관리할 수 있는 싱글 포인트
- 15개국 40개 IDC에 배치된 AISASE 플랫폼 간 상호 연계를 통한 멀티테넌시 서비스 인프라

How to subscribe WAAP & Secure CDN

1. 도메인 등록



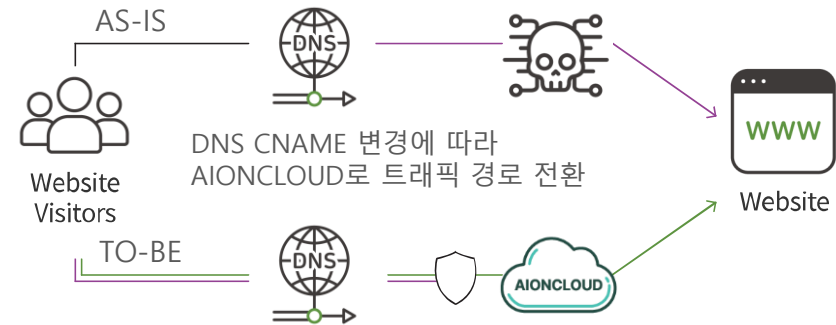
- 대상 웹사이트(도메인) 등록
- 단일 계정으로 여러개의 웹사이트 보호

3. 모니터링 & 관리



- 보안 이벤트 모니터링
- 보안 규칙 관리
- CDN 관리

2. DNS 변경 설정



- DNS(Domain Name Server)의 CNAME 정보를 AIONCLOUD에서 안내하는 주소 값으로 변경

▪ Example of changing CNAME ▾

- ① 보호대상 도메인 등록 후 " 210a7a86-.aioncloud.net " 와 같은 서비스 이용 도메인 정보를 발급 받습니다.
- ② 발급 받은 정보로 DNS의 CNAME 값을 변경합니다.
- ③ 변경 즉시 웹 트래픽은 AIONCLOUD 서비스를 경유하여 빠르고 안전한 서비스를 보장 받습니다.

Why need AIONCLOUD ?



■ 보안 강화

전세계에 배치된 Edge 플랫폼의 멀티테넌트와 오케스트레이션을 통해 급증하는 트래픽에 유연하고 민첩하게 대응 합니다.



■ 단일 지점 및 관리 콘솔

웹 애플리케이션 구성 시스템 및 네트워크와 관계없이 CDN, DDoS Mitigation, WAF, API Security, Bot Mitigation을 단일지점에서 all-in-one으로 관리하고 보호합니다.



■ 사용자 경험 개선

안전성과 유연성 그리고 성능까지 모두 갖춘 글로벌 수준의 Proxy 기술을 기반으로 네트워크 지연을 단축하고 사용자 경험을 개선 합니다.

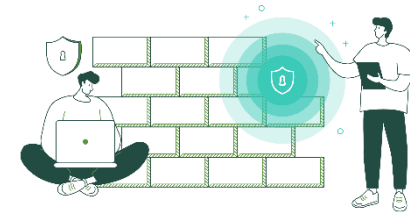


■ 복잡성 및 비용 절감

보안 서비스를 통합함으로써 IT 및 보안 팀의 복잡성을 줄이는 동시에 가시성과 관리 용이성을 높입니다.

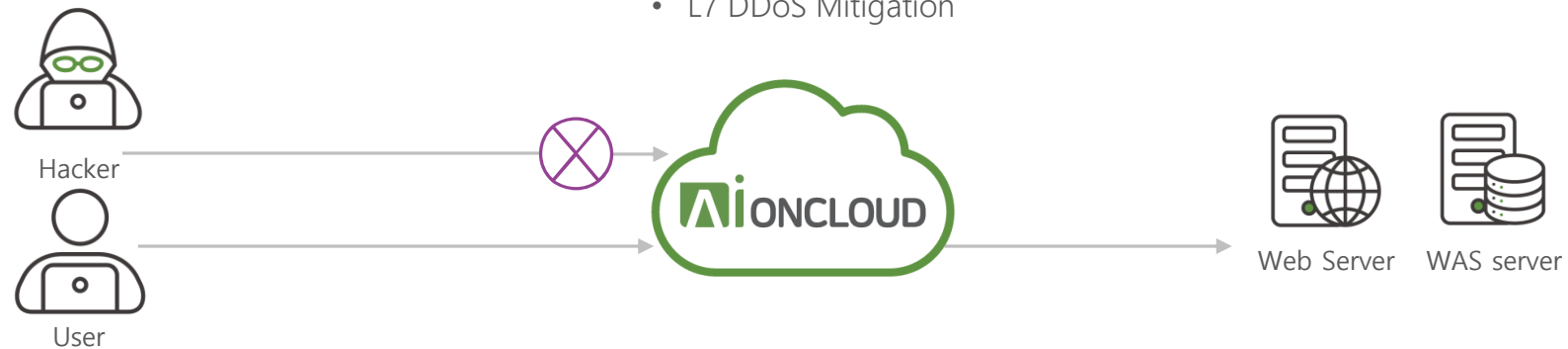
WAAP(Web Application and API Protection) Overview

- 웹 프로덕션 인프라에 대한 보안 서비스
- 멀티테넌트 아키텍처 기반으로 급증하는 트래픽에 대해서도 민첩하고 유연하게 대응
- 숙련된 보안 전문가 없이 최신/최적의 보안 체제 마련
- 사용한만큼 지불하는 Pay-as-you-go 가격 정책으로 비용 부담 해소



WAAP

- Web Security
- API Security
- Bot Mitigation
- L7 DDoS Mitigation



Why need WAAP ?



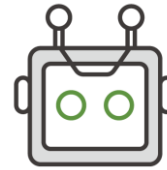
Web Security

- SQLi, Commandi, XSS, CSRF 등 웹 사이트에 직접적이고 위협적인 공격들을 차단합니다.



API Security

- API 트래픽의 완전한 구문분석과 토큰 무결성 검증을 통해 접근 제한 및 공격 차단, API Request 위변조를 감지 합니다.



Bot Mitigation

- 크리덴셜 스테핑, 콘텐츠 스크래핑 등 악의적인 목적의 Bot 트래픽을 식별 하고 접속을 제한 합니다.

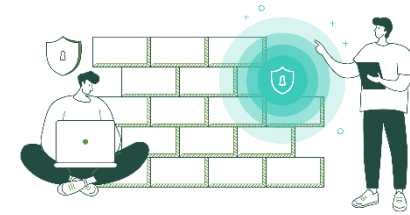


L7 DDoS Mitigation

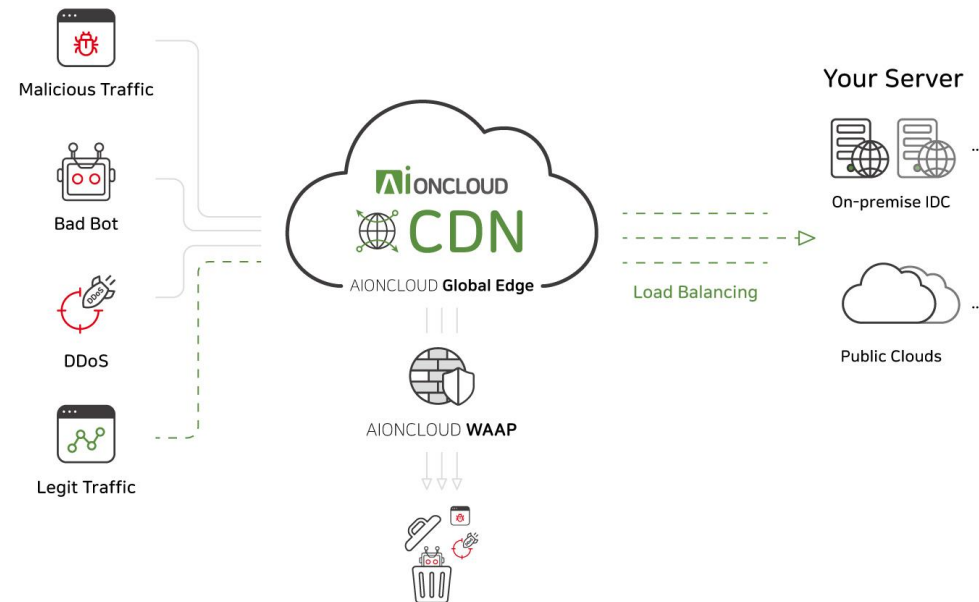
- GET 플러딩, RUDY, Slowloris, SlowRead 등 HTTP 기반의 서비스 거부 공격을 완화합니다.

Secure CDN(Content Delivery Network) Overview

- Network DDoS 완화 및 인터넷 콘텐츠의 빠른 전송
- 웹 사이트 로드 시간 개선 및 트래픽 비용 절감
- Network DDoS 완화 및 높은 수준의 암호화 연결, 인증서 제공 등을 통한 보안 개선



Secure CDN



Why need Secure CDN ?



Reduce load time

- 클라이언트와 가장 가까운 Edge에서 콘텐츠를 제공함으로써 사용자 경험을 향상시킵니다.



Bandwidth savings

- 캐싱 및 네트워크 최적화를 통해 대역폭을 절감시키고 원본 서버의 부담을 완화합니다.



Security improvement

- 높은 수준의 암호화 연결 및 인증서 제공, 보안 헤더 설정 등을 통해 SSL/TLS 환경의 보안을 강화합니다.



DDoS Mitigation

- Global Edge 인프라로 DoS 및 DDoS 공격으로부터 웹 사이트를 효율적으로 보호합니다.

Digital Service Mall

조달청 나라장터 종합쇼핑몰 혁신장터 벤처나라 서비스이음장터
e-고객센터 원격지원 원격지원(공센터)

조달청 디지털서비스몰

나라장터 인증서 로그인 (KONEPS Login)
이용하셔서 로그인하실 수 있습니다.

LOGIN

디지털서비스 상용 S/W 공개 S/W 데이터 거래

전체(규격,업체명 등) | 검색어를 입력하십시오

상세검색

디지털서비스몰

디지털서비스

- 클라우드서비스 ^
- SaaS(소프트웨어)
- PaaS(플랫폼)
- IaaS(인프라)
- API서비스
- 클라우드지원서비스 v
- 클라우드융합서비스 v

서비스 유형 v

클라우드구축방식 v

인증정보 v

서비스기술지원 v

초기화
선택검색

⚡

상품비교

보안클라우드서비스(SaaS)

업체명	주식회사 모니터랩	계약자/공급자 정보조회
계약방법	카탈로그계약	
규격명	보안클라우드서비스(SaaS), 모니터랩, AIONCL OUD Website Protection	
단위	식	
원산지	대한민국	
제조사	주식회사 모니터랩	
납품장소	수요기관 지정장소	

오늘의 상품
v

MONITORAPP

TOP

기업 추가정보

선택	디지털서비스번호	업체사업자번호	서비스타입명	서비스종류명
<input checked="" type="radio"/>	SAS40510632	2148766413	클라우드서비스	SaaS

THANK YOU

THANK YOU