




글로벌 엣지 기반의 WAAP 를
이용한 Website Protection 전략

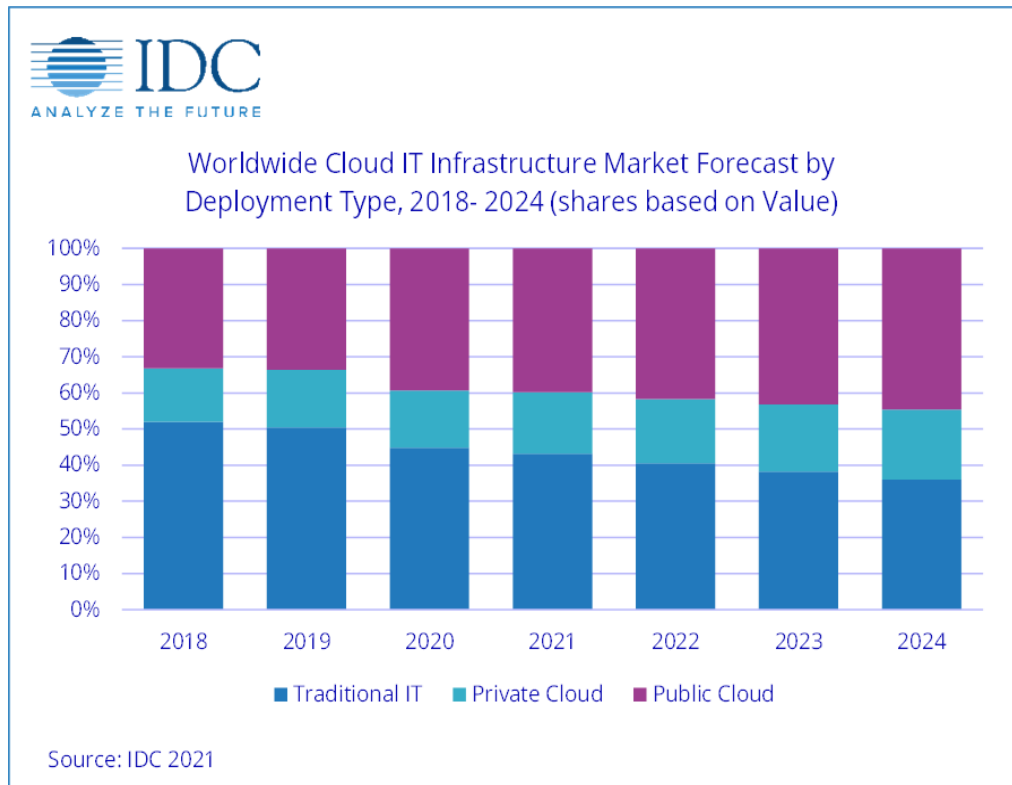


Contents

1. 웹 애플리케이션이 직면한 위협 요소
2.  AIONCLOUD Website Protection

❖ Migrate data and applications to the cloud

- 데이터와 애플리케이션의 위치가 클라우드로 전환

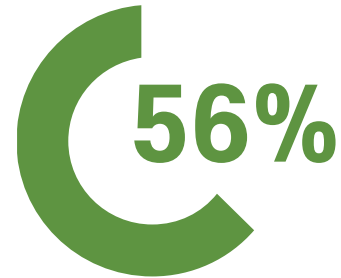


- 프로덕션 환경의 멀티·하이브리드 클라우드화
- 기업의 94%가 클라우드를 사용
 - 기업 워크로드의 83%가 클라우드에 위치
 - SMB의 94%가 클라우드로 전환 후 보안 이점 보고
 - 2025년까지 클라우드 저장 데이터 100ZB 예상

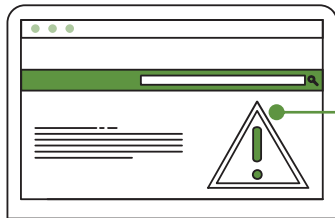
❖ Security Threats Faced by Business - Website



60%의 웹사이트 취약점에 항상 노출



심각한 취약점 중 56%만이 해결



62%

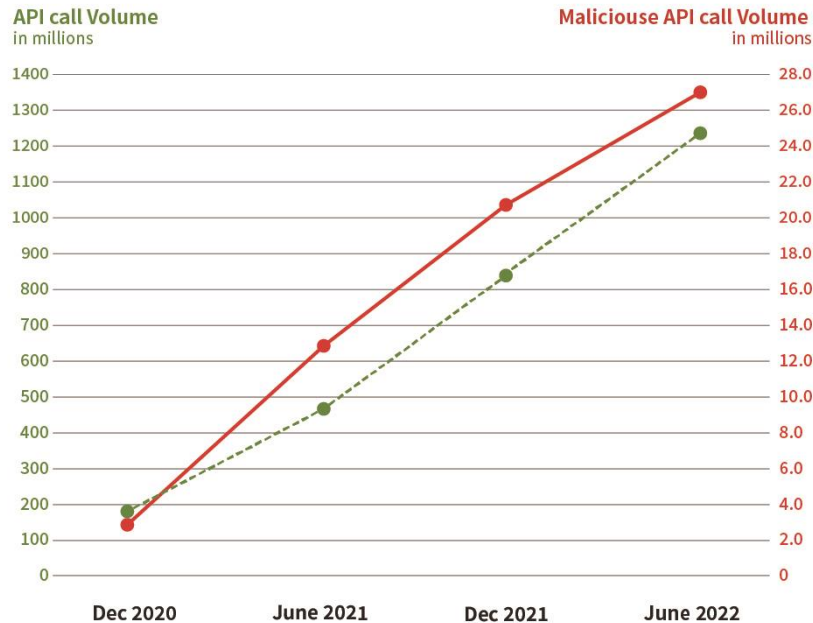
62%는 취약점을 이용한 해킹

196

심각한 취약점이 해결되는데
걸리는 시간, 196일

WhiteHat Security Website Security Statistics Report 2021

❖ The explosive growth of API & API security need



OWASP API Security Top 10 2023 RC

- 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: Server Side Request Forgery
- API 7: Security Misconfiguration
- API 8: Lack of Protection from Automated Threats
- 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

❖ OWASP API Security Top 10 2023 RC (Ex no.1)

- **Broken Object Level Authorization (손상된 개체 수준 권한 부여)**

시나리오)

온라인 상점을 위한 전자 상거래 플랫폼은 호스팅 상점의 수익 차트가 포함된 목록 페이지를 제공합니다. 공격자는 브라우저 요청을 검사하여 해당 차트 및 해당 패턴의 데이터 소스로 사용되는 API End-point를 식별할 수 있습니다.

/shops/**honggildong**/revenue_data.json.

/shops/**hocheolpark**/revenue_data.json.

다른 API End-point를 사용하여 공격자는 모든 호스팅 상점 이름 목록을 얻을 수 있습니다.

❖ OWASP API Security Top 10 2023 RC (Ex no.2)

- **Broken Object Property Level Authorization (손상된 개체 속성 수준 권한 부여)**

시나리오)

데이트 앱을 사용하면 사용자가 다른 사용자의 부적절한 행동을 신고할 수 있습니다. 이 흐름의 일부로 사용자가 "신고" 버튼을 클릭하면 다음 API 호출이 트리거됩니다.

```
POST /graphql
{
  "operationName":"reportUser",
  "variables":{
    "userId": 313,
    "reason":["offensive behavior"]
  },
  "query":"mutation reportUser($userId: ID!, $reason: String!) {
    reportUser(userId: $userId, reason: $reason) {
      status
      message
      reportedUser {
        id
        fullName
        recentLocation
      }
    }
  }"
}
```

API End-point는 인증된 사용자가 다른 사용자가 액세스해서는 안 되는 "fullName" 및 "recentLocation"과 같은 민감한 사용자 개체 속성에 액세스할 수 있도록 허용하므로 취약합니다.

❖ OWASP API Security Top 10 2023 RC (Ex no.3)

- **Unrestricted Resource Consumption (무제한 리소스 소비)**

시나리오)

공격자는 /api/v1/images에 POST 요청을 발행하여 큰 이미지를 업로드합니다. (업로드 완료 시 크기가 다른 여러 썸네일 생성)
업로드된 이미지의 크기로 인해 썸네일 생성 중에 사용 가능한 메모리가 소진되고 API가 응답하지 않게 됩니다.

로그인 시도에는 제한적인 속도 제한(분당 3회)이 적용 됩니다.
공격자는 이를 무력화 하기 위해 1회 요청을 아래와 같이 조작 하여 속도 제한을 우회 합니다.

```
POST /graphql
[
  {"query":"mutation{login(username:W"victimW",password:W"passwordW"){token}}"},
  {"query":"mutation{login(username:W"victimW",password:W"123456W"){token}}"},
  {"query":"mutation{login(username:W"victimW",password:W"qwertyW"){token}}"},
  ...
  {"query":"mutation{login(username:W"victimW",password:W"123W"){token}}"},
]
```


❖ API Security solution

API Discovery

Signature-based attack detection & Spec violation

Rate limit & enforced timeout

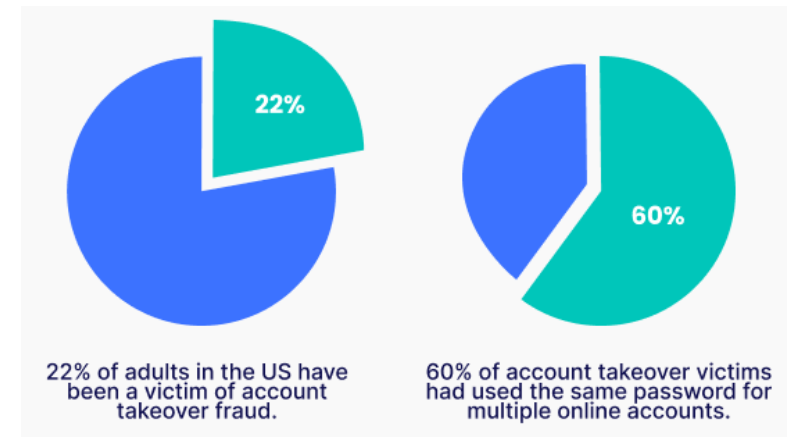
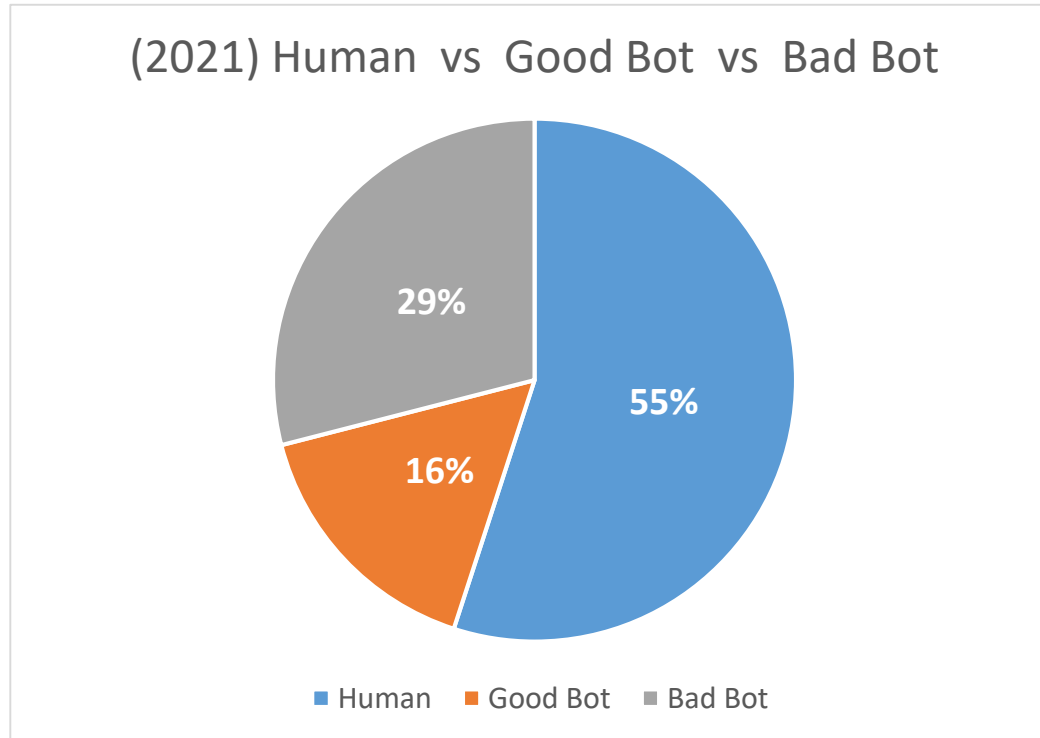
Access IP and Geolocation

File upload size and extension limit

Authentication server integration

...

❖ Bot traffic and threat of Account Takeover



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

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

CAPTCHA

Honeypot Trap

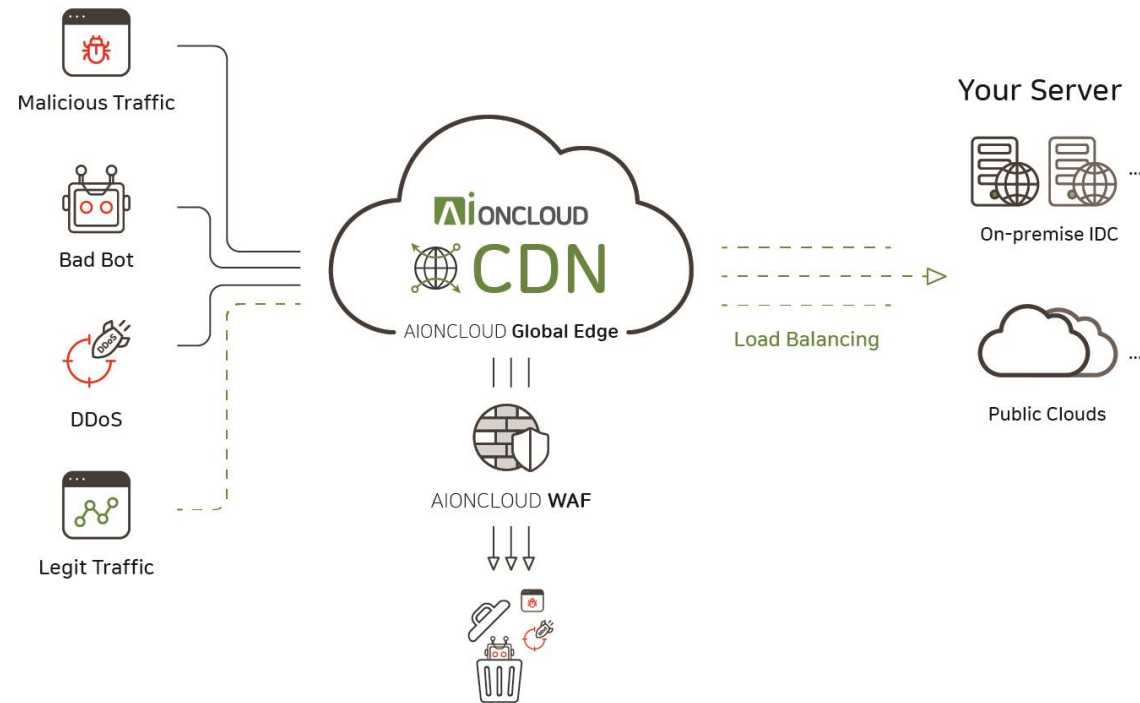
Java Script Challenge

Human Interaction Challenge

Device Fingerprinting

...

❖ 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

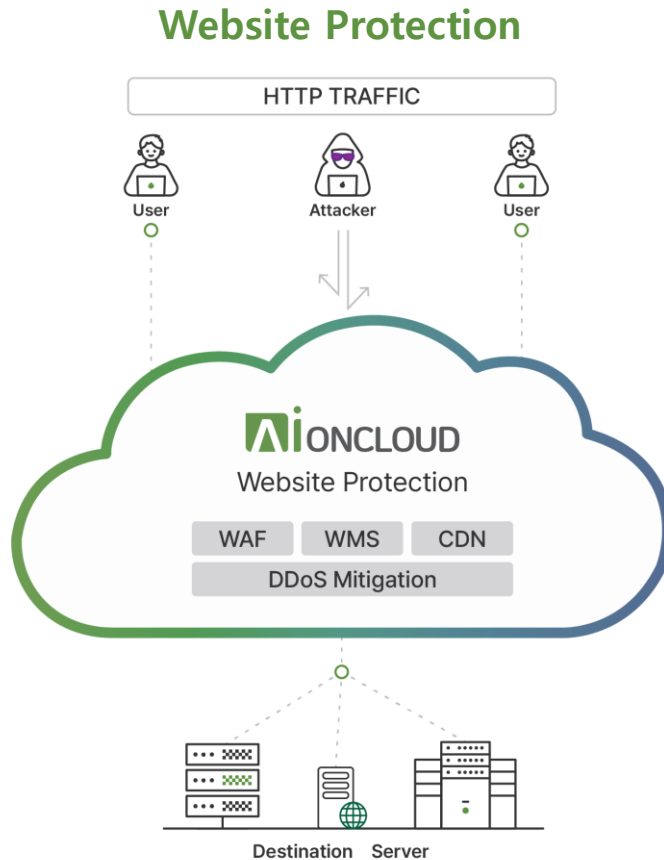
❖ AIONCLOUD WAF Vs CSP Native WAF

	AIONCLOUD WAF	CSP A사 WAF	CSP G사 WAF
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	Maximum 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

 **IONCLOUD Website Protection**

❖ AIONCLOUD Service Category

- Website Protection : 기업 데이터센터에 대한 “WAAP” 보안 서비스
- Secure Internet Access : 기업 직원의 안전한 인터넷 연결을 보장하는 “SSE” 기반 보안 서비스



❖ 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

❖ 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.



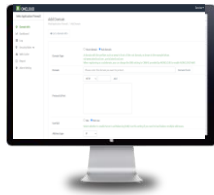
■ 복잡성 및 비용 절감

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

18

❖ How to subscribe Website Protection

1. 도메인 등록



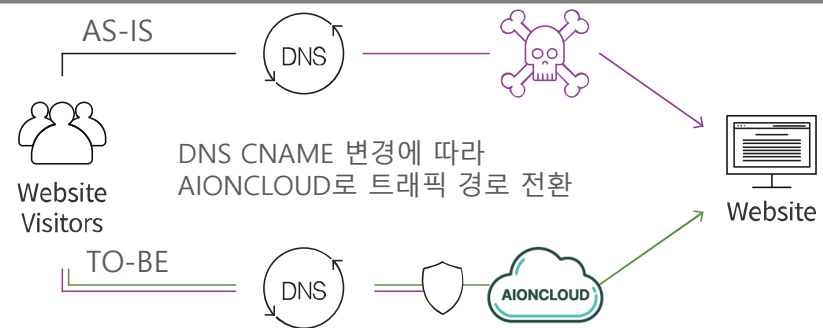
- 대상 웹사이트(도메인) 등록
- 단일 계정으로 여러개의 웹사이트 보호

3. 모니터링 & 관리



- 보안 이벤트 모니터링
- 보안 규칙 관리

2. DNS 변경 설정



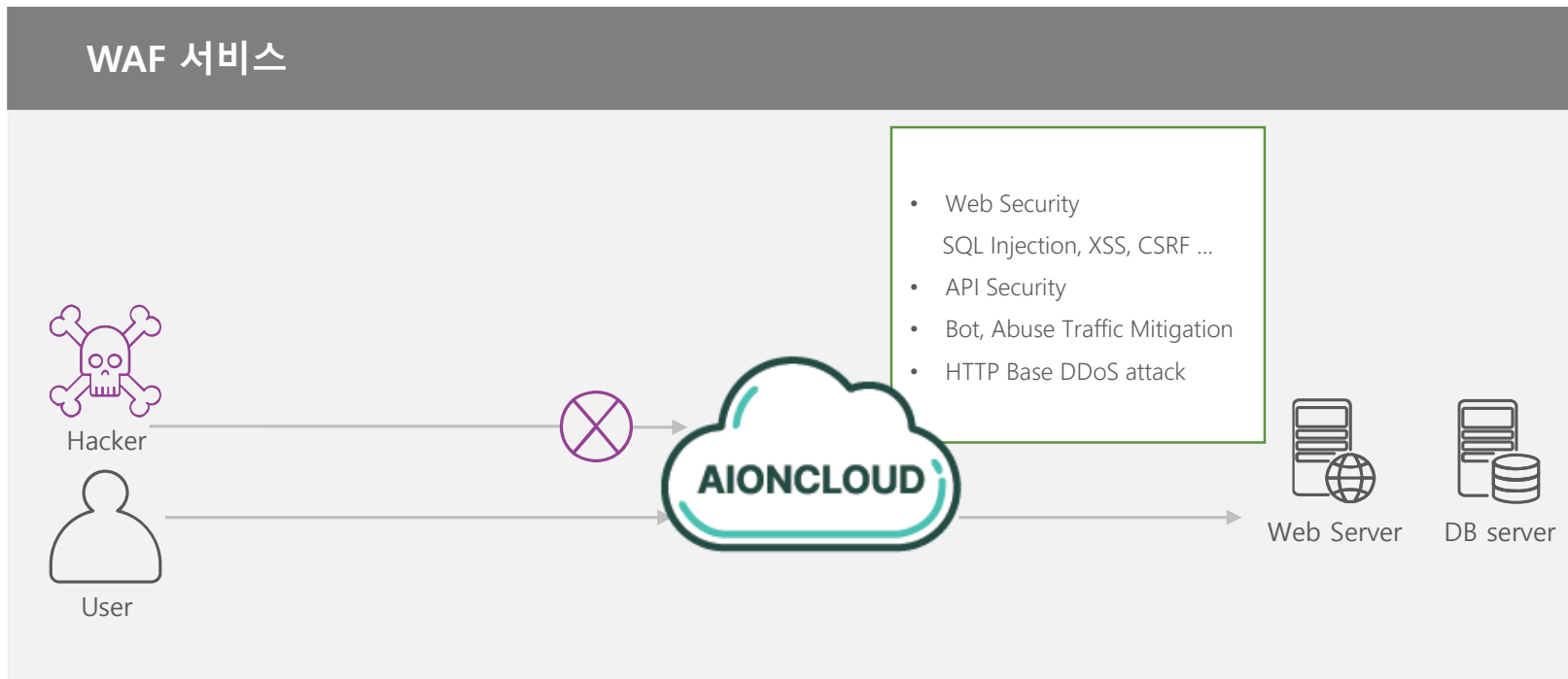
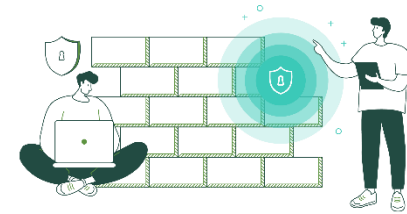
- DNS(Domain Name Server)의 CNAME 정보를 AIONCLOUD에서 안내하는 주소 값으로 변경

▪ 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 WAF 서비스를 경유하며 안전하게 보호 받습니다.

❖ WAF(Web Application Firewall) Overview

- **기업 내부/데이터센터로 유입되는 HTTP(S)에 대한 포괄적 방어**
- 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



❖ Why need WAF ?



Web Security

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



API Security

- API 트래픽에 대한 완전한 구문분석을 수행하여 공격을 차단하고 접근 제한 규칙을 생성합니다.



Bot Mitigation

- 크리덴셜 스테핑, 콘텐츠 스크래핑 등 악의적인 목적의 Bot 트래픽을 식별하고 접속을 제한합니다.

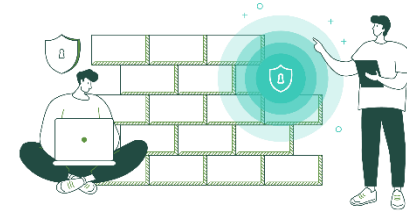


L7 DDoS Mitigation

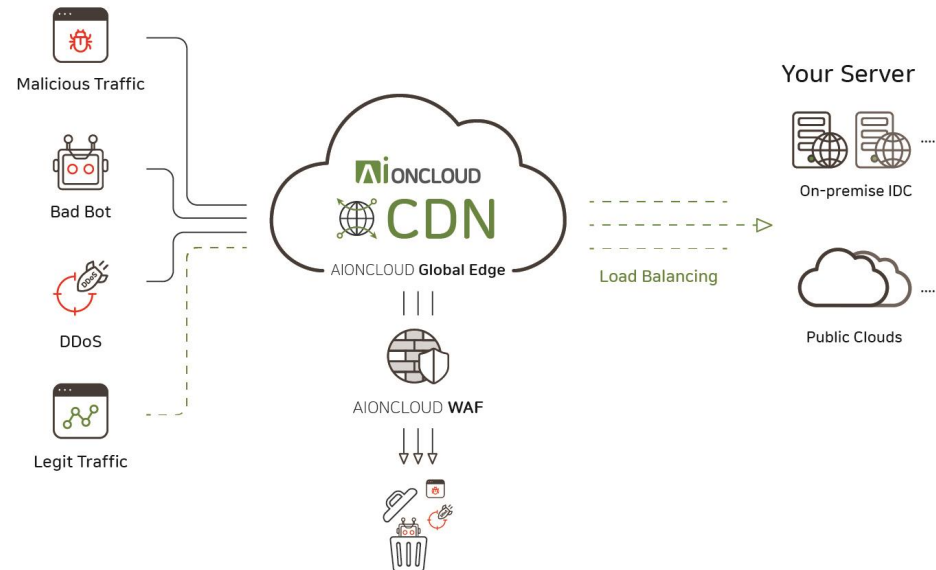
- GET 플러딩, RUDY, Slowloris 등 HTTP 기반의 서비스 거부 공격을 완화합니다.

❖ Secure CDN(Content Delivery Network) Overview

- **DDoS 완화 및 인터넷 콘텐츠의 빠른 전송**
- 웹 사이트 로드 시간 개선 및 트래픽 비용 절감
- DDoS 완화 및 높은 수준의 암호화 연결, 인증서 제공 등을 통한 보안 개선
- 사용한만큼 지불하는 Pay-as-you-go 가격 정책으로 비용 부담 해소



Secure CDN 서비스



❖ 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.

THANK YOU