CLOUDFLARE

금융을 위한 보안 다시 생각하기

황성환 이사
Cloudflare

Agenda

1. Cloudflare 소개
2. 금융IT보안의 복잡성과 어려움
3. 효율화 방안
4. Cloudflare 솔루션 Key Value

Cloudflare 글로벌 클라우드 네트워크

Cloudflare는 웹사이트와 인터넷 애플리케이션의 보안, 성능, 안정성 향상을 목표로 다양한 서비스를 제공합니다.

DNS, DDoS, WAF, CDN, Serverless computing ..

- ChatGPT

12,000+

ISP, 클라우드 공급자, 대기업 등 Cloudflare에

207 Tbps

네트워크 에지 용량 규모

310+

100여 개국의 도시 수

1,260 억

매일 차단하는 보안 위협 건수

95%

전 세계 사용자 중, 50ms 이내로 Cloudflare 네트워크에 연결되는 비율

All services are available in each Cloudflare city

Cloudflare city

Approximate area inside which Cloudflare's network is reachable within 50ms via the Internet

Cloudflare 포트폴리오

클라우드플레어 플랫폼

1 클라우드플레어 원

제로트러스트 서비스

- Zero Trust Network Access
- Secure Web Gateway
- Cloud Access Security Broker
- Cloud Email Security
- Remote Browser Isolation
- Data Loss Prevention

네트워크 서비스

- WAN-as-a-Service
- Firewall-as-a-Service
- **L3 & L4 DDoS Protection**
- Network Interconnect
- Smart Routing
- IDS/IPS [1]

어플리케이션 서비스

- WAF with API Protection
- Rate Limiting
- Load Balancing
- Bot Management
- L7 DDoS Protection
- CDN and DNS

클라우드플레어 엣지개발플랫폼

Workers | Pages | R2 | Workers KV | Durable Objects | Images | Stream

클라우드플레어 글로벌 네트워크

Compliance/Privacy: FedRAMP, ISO, SOC, PCI, GDPR compliant, Logs & Analytics, Data Localization Suite

aws

3% → 17%

Microsoft Azure

Google Cloud

DATA CENTER

금융 IT 담당자의 어려움

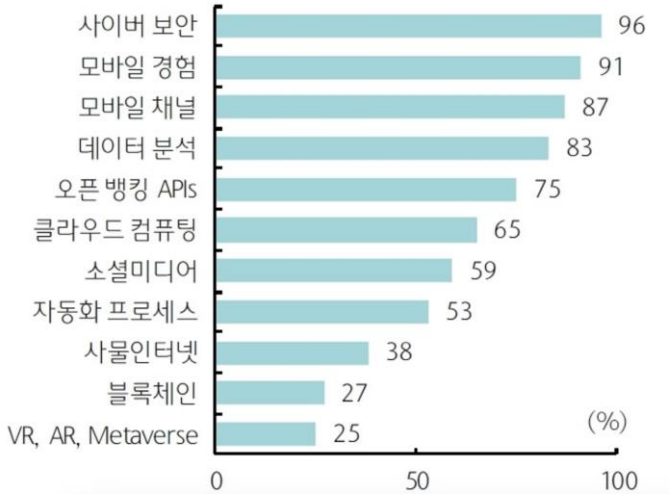
멀티클라우드 보안 ?
하이브리드 클라우드 ?
글로벌 비즈니스 확장?

HW 입고는
언제 ?
운영관리 ?
업데이트?

Zero Trust ? WAAP ?
AI 기술과 보안?
장애 대응 ? 모니터링 ?

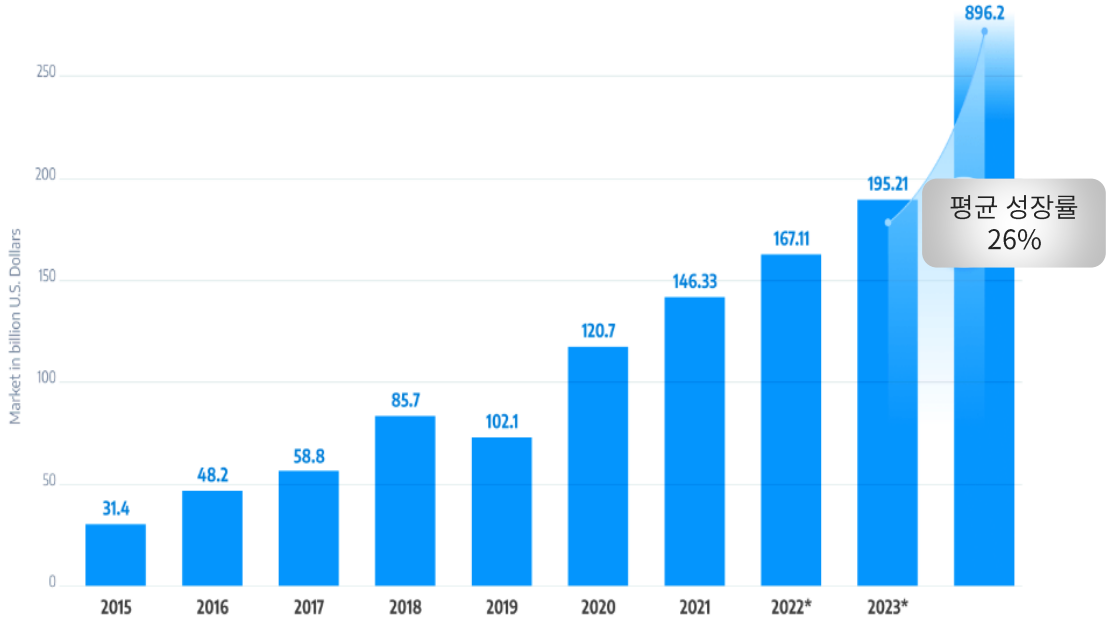
보안 관련 규제
MSA 프로젝트?
비용 절감 ?

Digital 금융의 경제와 최우선 과제



Source: 향후 3~5년간 디지털 전환의 최우선 과제
[자료=하나금융경영연구소]

Digital Transformation - SaaS First



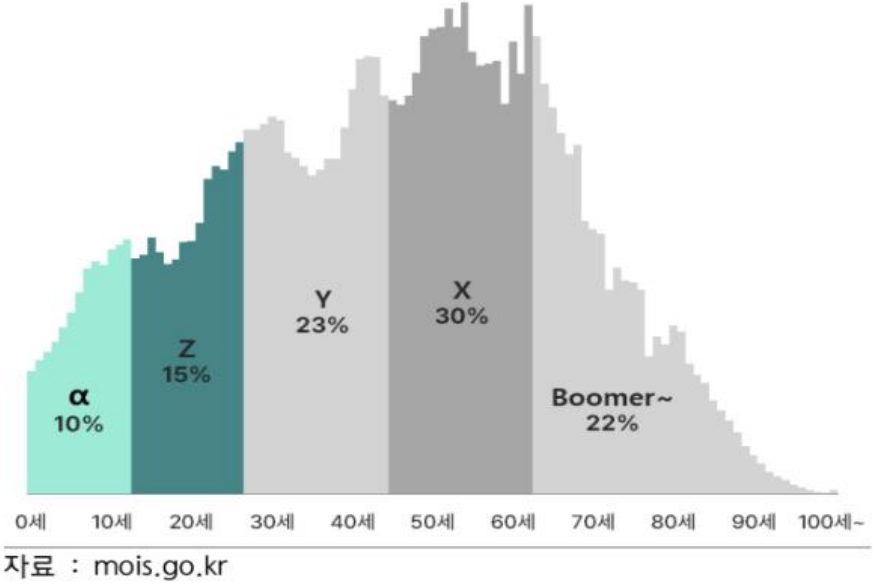
Source: statista.com, verifiedmarketresearch.com

SaaS 솔루션의 장점

1. 즉시 최신의 서비스 지원 가능
2. 개발 비용의 절감
3. 자동화에 따른 업무 효율성 향상
4. 편리한 글로벌 비즈니스 진출

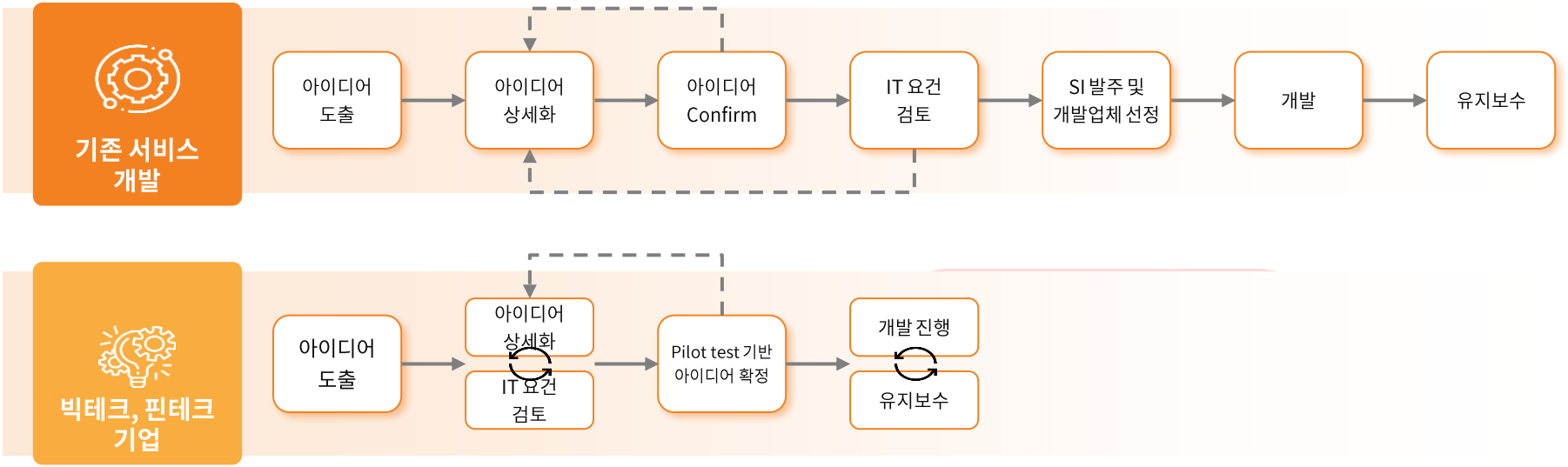
금융 고객 세대의 변화

- Z, Alpha 세대 대두
- Digital & Mobile native 세대, AI & 디지털 경험을 중시함
- 기존 금융사에 대한 충성도가 낮음

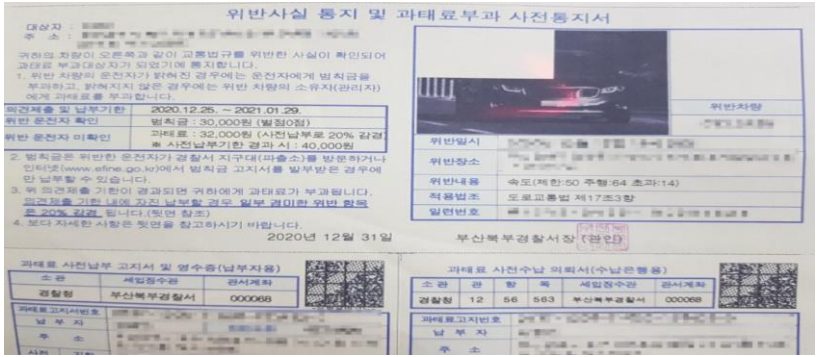


자료 : mois.go.kr

신규 서비스 구축 프로세스 차이점



AI 서비스에서 데이터의 중요성이란?



위반사실 통지 및 과태료부과 사전통지서

대상자 :
주 소 :

귀하의 차량이 오른쪽과 같이 교통법규를 위반한 사실이 확인되어 과태료 부과대상자가 되었기에 통지합니다.

1. 위반 차량의 운전자가 밝혀진 경우에는 운전자에게 범칙금을 부과하고, 밝혀지지 않은 경우에는 위반 차량의 소유자(관리자)에게 과태료를 부과합니다.

의견제출 및 납부기한	2020.12.25. ~ 2021.01.29.
위반 운전자 확인	범칙금 : 30,000원 (벌점0점)
위반 운전자 미확인	과태료 : 32,000원 (사전납부로 20% 감경 ※ 사전납부기한 경과 시 : 40,000원

2. 범칙금은 위반한 운전자가 경찰서 지구대(파출소)를 방문하거나 인터넷(www.efine.go.kr)에서 범칙금 고지서를 발부받은 경우에만 납부할 수 있습니다.

3. 위 의견제출 기한이 경과되면 귀하에게 과태료가 부과됩니다. 의견제출 기한 내에 자진 납부할 경우 일부 경미한 위반 항목은 20% 감경 됩니다.(뒷면 참조)

4. 보다 자세한 사항은 뒷면을 참고하시기 바랍니다.

2020년 12월 31일

부산북부경찰서장 (인)

위반일시	
위반장소	
위반내용	속도(제한:50 주행:64 초과:14)
적용법조	도로교통법 제17조3항
일련번호	

과태료 사전납부 고지서 및 영수증(납부자용)

소관	세입징수관	관서계좌
경찰청	부산북부경찰서	000068

과태료 사전수납 의뢰서(수납은행용)

소관	관	항	목	세입징수관	관서계좌
경찰청	12	56	563	부산북부경찰서	000068

과태료고지번호
납 부 자
주 소

과태료부과 사전통지서

대상자:
주 소:

귀하에 대하여 도로교통법 제160조와 제161조에 따라 아래와 같이 과태료를 부과하고자 하오니 의견이 있으시면 기한내 의견을 제출하여 주시기 바랍니다.

위반일시	2017-08-03 15:08	위반장소	장산아파트 사거리
위반내용	주·정차 위반	적용법령	도로교통법 제32~34조
과태료금액	40,000 원	의견제출기한	2017년 08월 23일

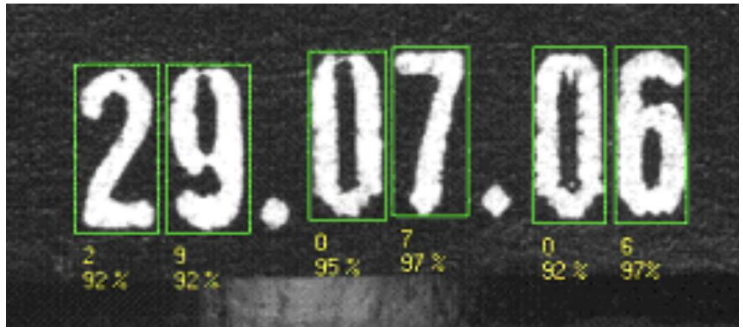
귀하께서 위 의견제출기한 내에 이의제기 없이 과태료를 납부하고자하는 경우에는 아래의 과태료 납부고지서를 이용하여 납부하실 수 있습니다. 기한 내에 자진납부하는 때에는 과태료가 20% 감경됩니다.

※ 가상계좌번호 : 790106-35-468737 농협

2017년 08월 08일

진 천 군

증거번호: 차량등록번호:



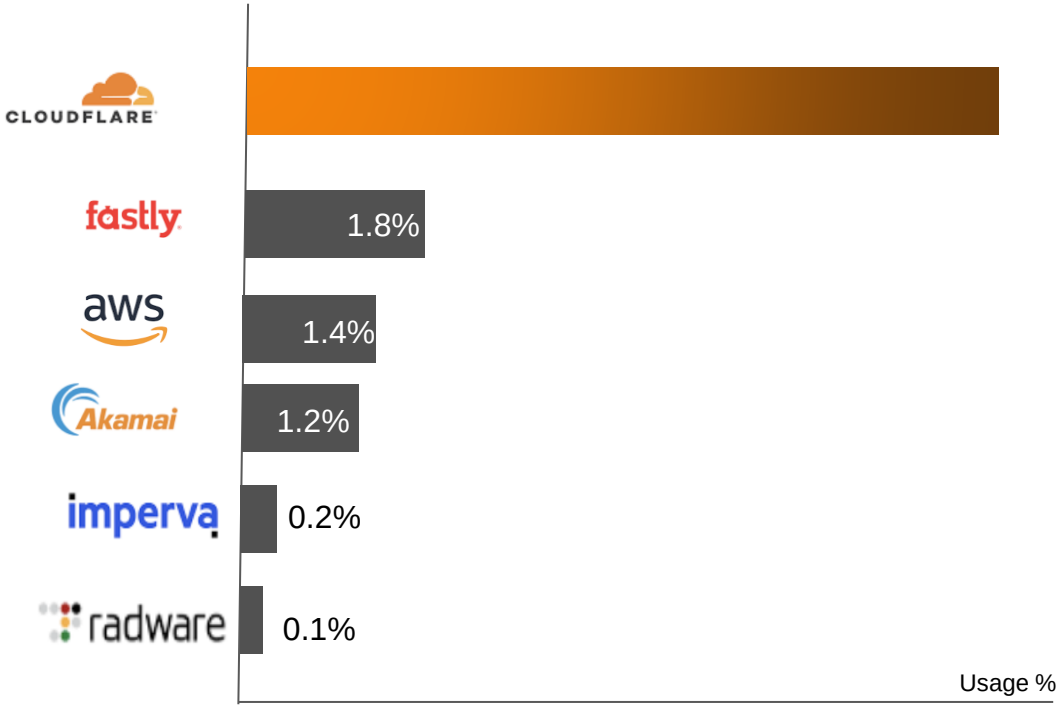
8/16に新居に引っ越しするため、8/17以降の配達でお願い致します。

8/16に新居に引っ越しするため、8/17
以降の配達でお願い致します。

〒106-00与32

〒106-0032

전 세계 인터넷 웹사이트 트래픽 처리 현황



18.7%

77.8%

Source: W3Techs.com, 13 Nov 2023

Market research 자료

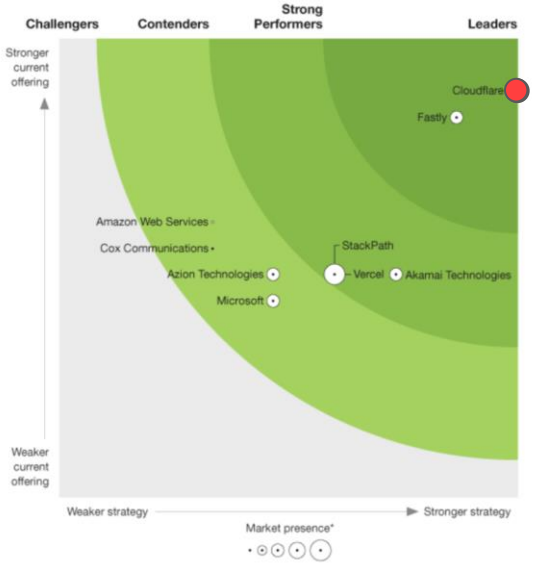
The Forrester Wave™:
Web Application Firewalls
Q3 2022

Source: Forrester Research, Inc.

2022 Gartner Magic Quadrant
for WAAP
August 2022

Source: Gartner

The Forrester New Wave™:
Edge Development Platforms
Q4 2021



Source: Forrester Research, Inc.

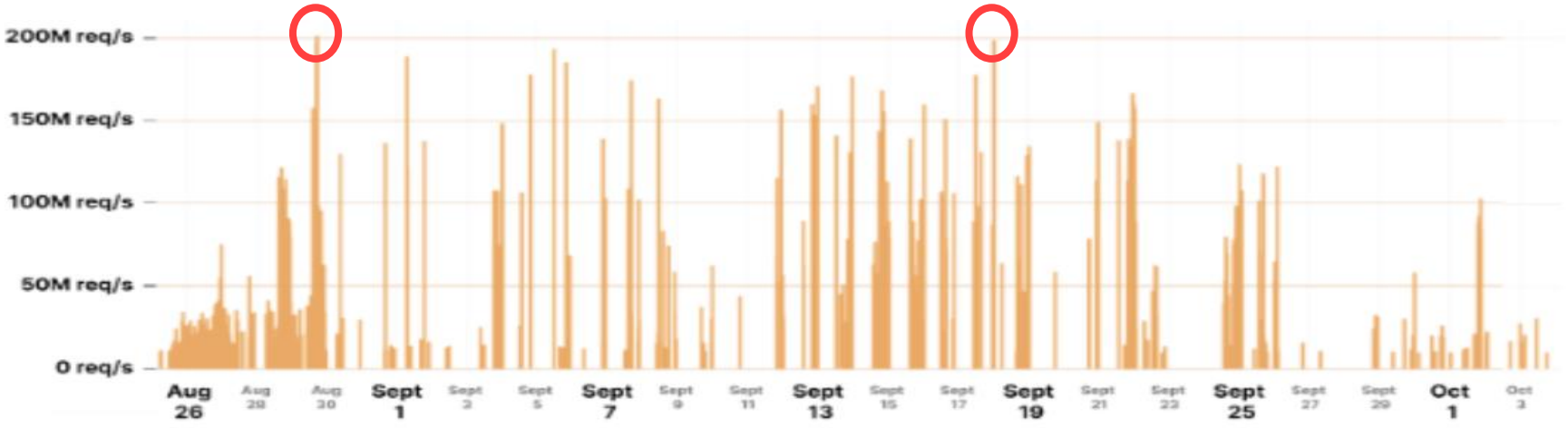
긴급 보안 업데이트 대응 사례

Cloudflare는 Log4J 취약점 발생시
신규 4개의 Ruleset를 몇 시간안에 Test
완료하여 배포 진행함

Confluence CVE-2022-26134
취약점 발견 후 약 30분 안에 대응 업데이트
버젼 배포 진행함
취약점을 목표로 한 해커 공격은 약 3.5시간 후에
진행됨

글로벌 최대의 DDoS 공격 - “Rapid Reset”

- HTTP2 취약점 기반 공격
- 기존 대비 약 3배 이상의 201MM RPS 공격
- Cloudflare 공격 방어 (AWS, Google과 협업)



전 세계가 주목하는 Cloudflare의 이점

현대화된 SASE 아키텍처

- 209 Tbs 방어 용량을 갖춘 Anycast 기반 단일 글로벌 네트워크
- 통합된 L3-7 방어
- 스크러빙 센터 기반이 아니고 자체 개발 소프트웨어 사용
- 서비스 형태로 제공하고 모든 클라우드플레어 서비스와 통합 사용 가능

종합적인 방어 제공

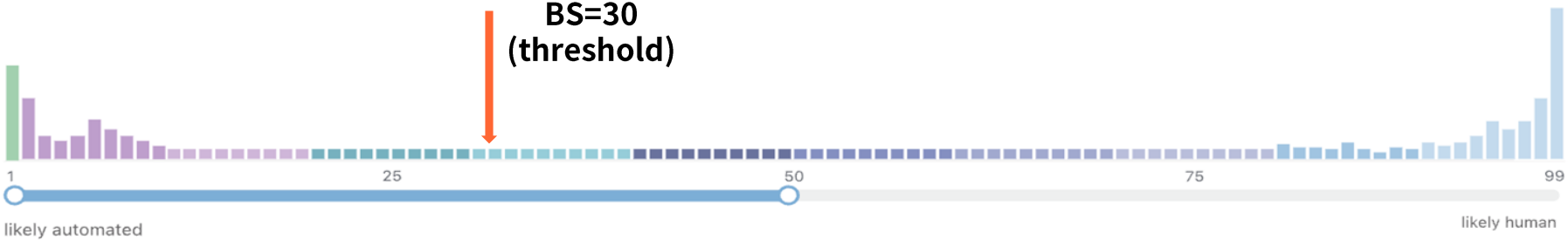
- 플러그&플레이 방어
- 실시간 핑거프린팅 정보 제공
- 복잡한 TCP 공격 방어(TCP Stat) 트래픽 프로파일링
- 높은 수준의 Configuration 제공
- Time to mitigate <3 sec

사용 편의성

- 셀프 서비스 가능, 관련 가이드/제품설명서 공개
- 전문가 커뮤니티
- API/Terraform 자동화, SIEM연동
- 분석 및 관리를 위한 단일 패널 사용

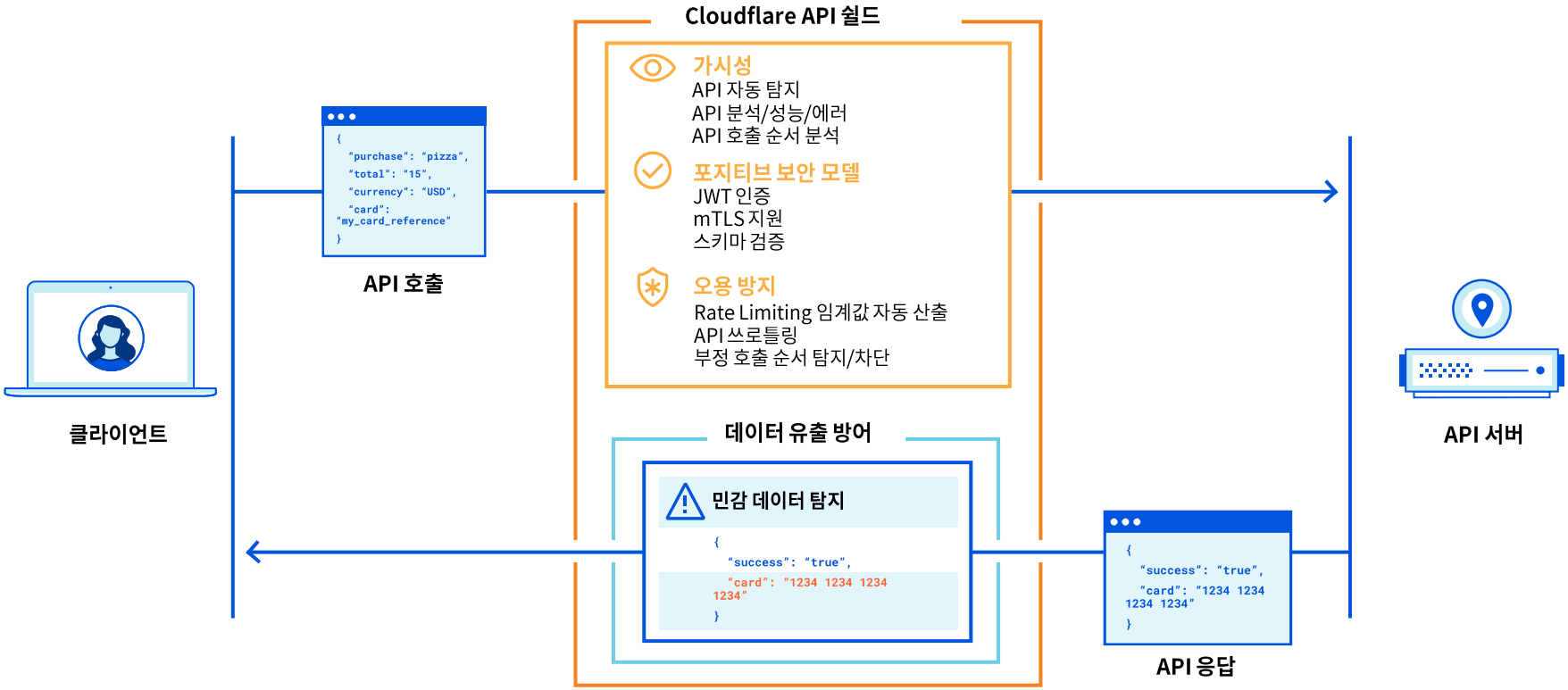
Bot 방어 솔루션 - Bot Scoring 기반

클라우드플레어 2,400만개 도메인의 위협 정보를 머신 러닝 및
핑거프린팅 분석 기법을 사용하여 위협 점수 제공

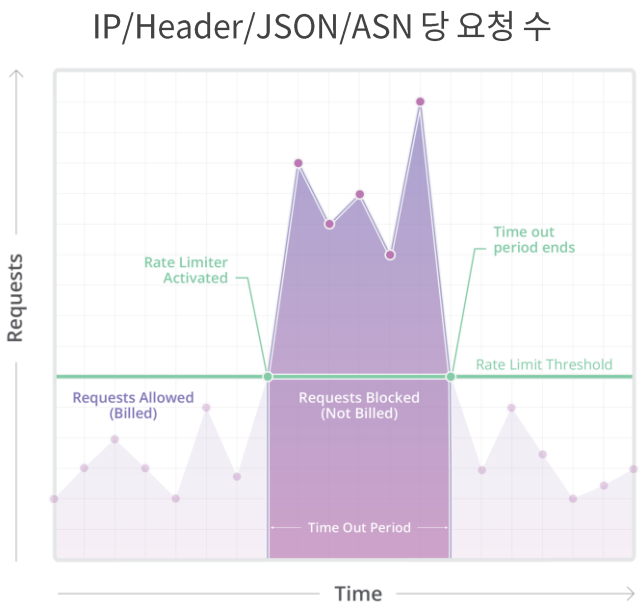


Heuristics	JavaScript Detections	Anomaly Detection	Machine Learning
시그니처, 패턴 기반의 봇 탐지	가벼운 자바스크립트 사용하여 헤드리스 브라우저, 정상 브라우저 유무 파악	사이트별 트래픽 프로파일링 하여 베이스라인을 만들고 기계학습을 통해 이상 패턴 감지	Cloudflare 모든 고객에서 수집되는 봇 트래픽 정보를 활용하여 지속적인 기계학습을 통해 봇 트래픽 스코어링

API 트래픽 관리 및 보안



API 트래픽 보안



Problem

- 과도한 API 호출에 따른 인프라 부담이 발생하고 전체적인 서비스 성능 영향을 줄 수 있어 API 에 대한 오남용을 효과적으로 방어할 수 있도록 사용자/세션/API키별로 호출 수를 관리하고 과도한 경우 제어할 수 있는 방안 필요

Solution

- 호출자의 다양한 특성(IP/HTTP header, Cookie/API 키값, JSON 변수)에 따라 호출 수를 측정 유지하고 정책에 따라 과도한 사용이 확인된 경우 차단(초,분,시간,일)등의 관리 조치

Qualification

- DDoS 공격 방어 필요
- API, 중요 end point URL에 대한 가용성 관리 필요

테슬라 자동차의 효율화?

비용 절감 효과

- 생산공정 로봇 : 1,000대 중 300대 절감
- 컨베이어 벨트 면적: 20% 절감
- 생산단가 : 40% 절감

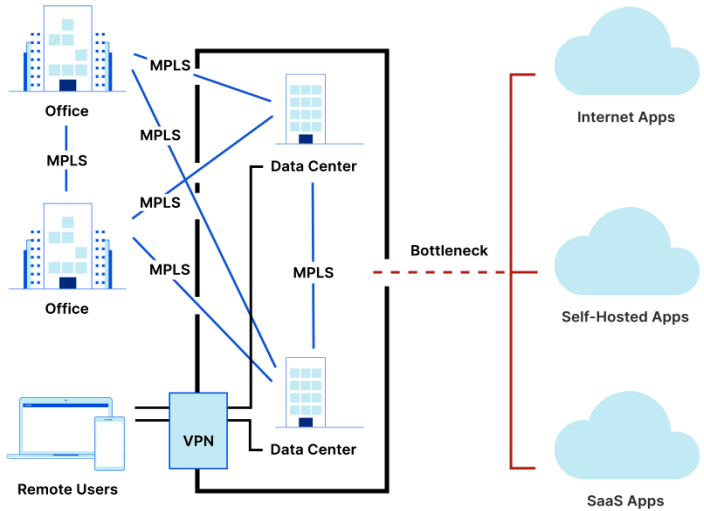
생산효율 극대화

- 대량생산 가능: 장비 1대당 1,000대 생산
- 부품 조립에 따른 결함, 오작동 줄어듬
- Supply 공급망 이슈 해결

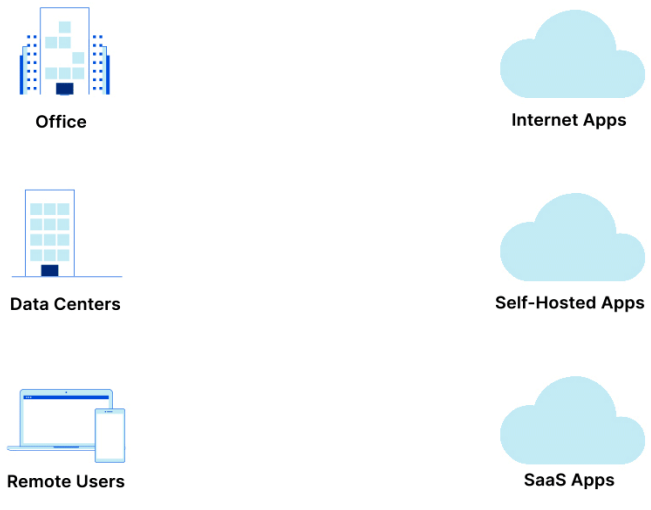
효율화 방안 I - 통합 솔루션 제공

사용자에게 가장 가까운 PoP(Edge)에서 처리, “사용자 인증 + 보안 + Application 성능 향상” 까지 한 번에 해결

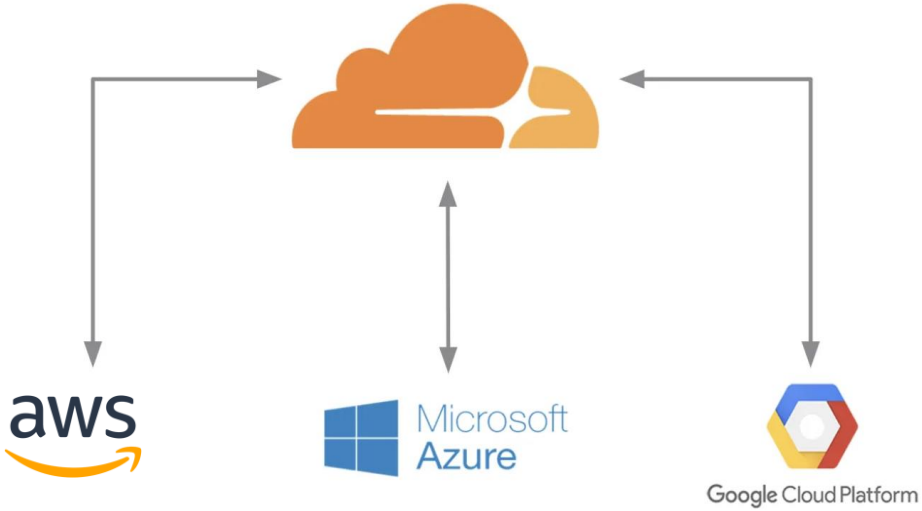
기존 IDC 중심의 클라우드 및 인터넷 앱 접속 방식



위치에 상관없이 Cloudflare 플랫폼의 보안 서비스 제공

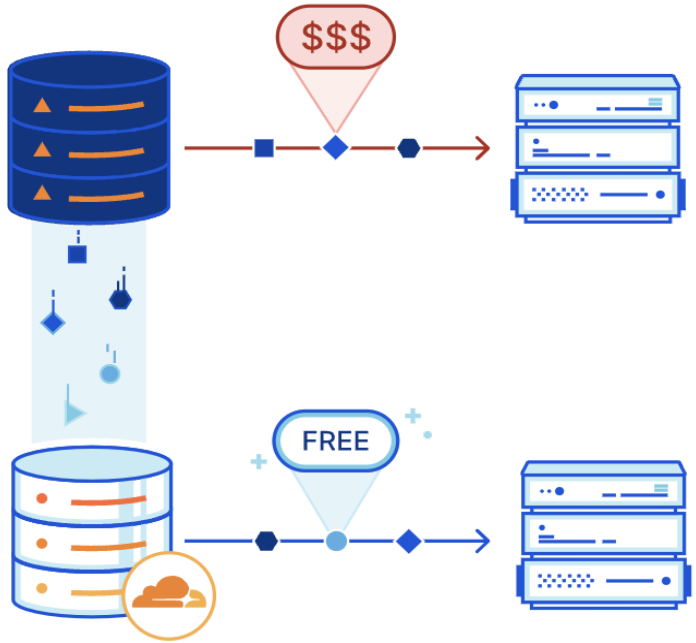


효율화 방안 II - Neutral Cloud 보안과 네트워크



1. 다양한 클라우드, On-Prem IDC와 간편한 통합
2. 보안과 개발 플랫폼 서비스 제공
3. 단일 대시보드에서 운영 및 관리

효율화 방안 III - Cloud-native Storage (R2) 활용



1. Low cost of storage
2. No Egress fee
3. Interconnect with Global CDN & DDos solution

Cloudflare의 플랫폼 안정성과 타 솔루션 연계

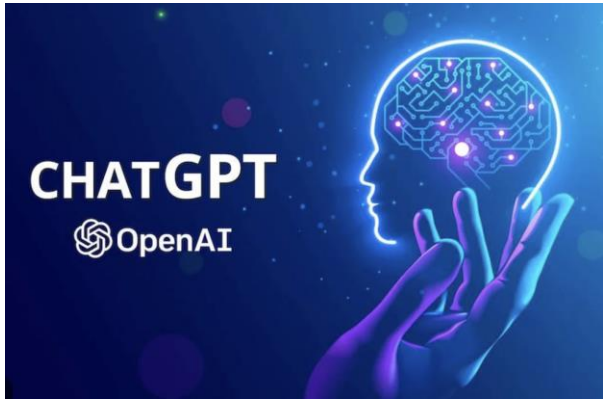
다양한 SIEM과 쉽게
연계가능하며
실시간 Log 제공으로 자체
모니터링 솔루션과 API 기반으로
데이터 제공

Terraform과 편리하게 연계하여
IAC 툴과 보안 연계

FedRAMP, SOC2 TYPE2
ISO27701등 최상위
보안인증으로 Cloudflare
플랫폼의 안정성 확보

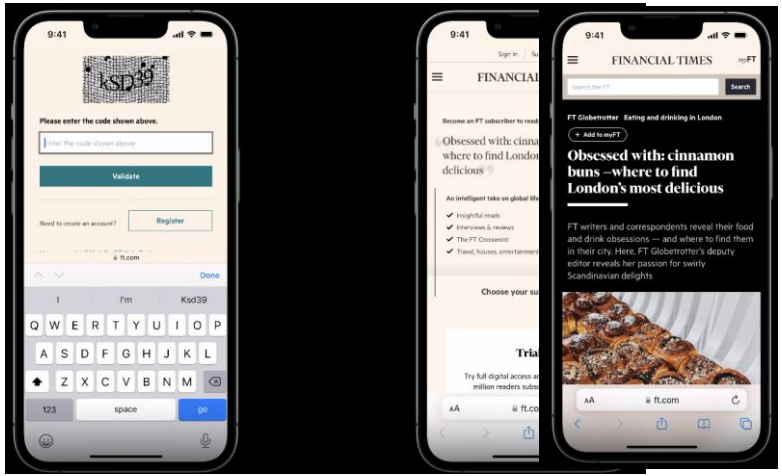
글로벌 고객사례 I - ChatGPT의 보안은?

- 가장 빨리 성장하는 애플리케이션 (1억명 사용자 / 다양한 Device)
- 비정형 API 트래픽 & Bot 트래픽 보안



글로벌 고객사례 II - CAPTCHA 없는 아이폰 & 맥북

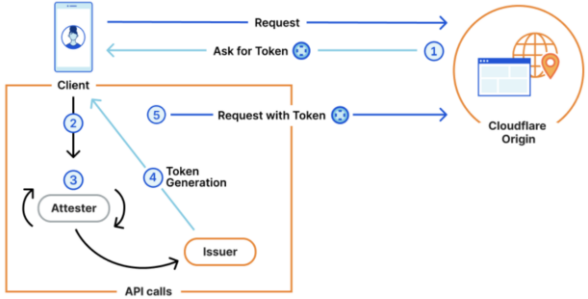
iOS 15 iOS 16



Cloudflare는 PAT 기능을 제공하여 iOS 사용자가 CAPTCHA 없이 웹사이트를 사용하도록 지원합니다.

(Private Access Token)

-iOS 16, iPad 16, and macOS 13



Thank you!

저희는 더 나은
인터넷 세상을 만드는데
주력합니다.

Thank you

sunghwan@cloudflare.com
www.cloudflare.com/ko-kr