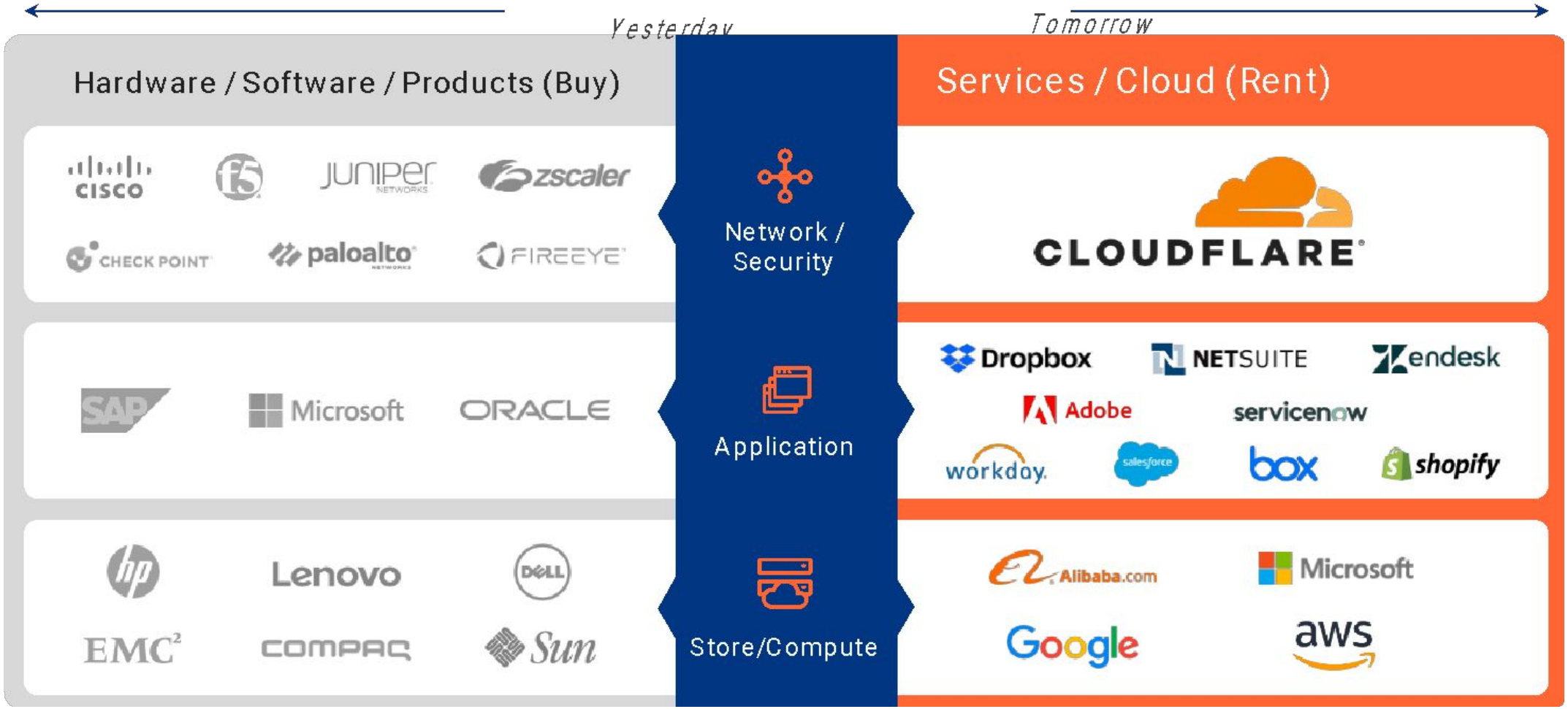
CLOUDFLARE

새로운 SASE 보안 강자
Cloudflare One & 제로트러스트

전창우 | 클라우드플레어 기술이사 | 2023

CLOUDFLARE

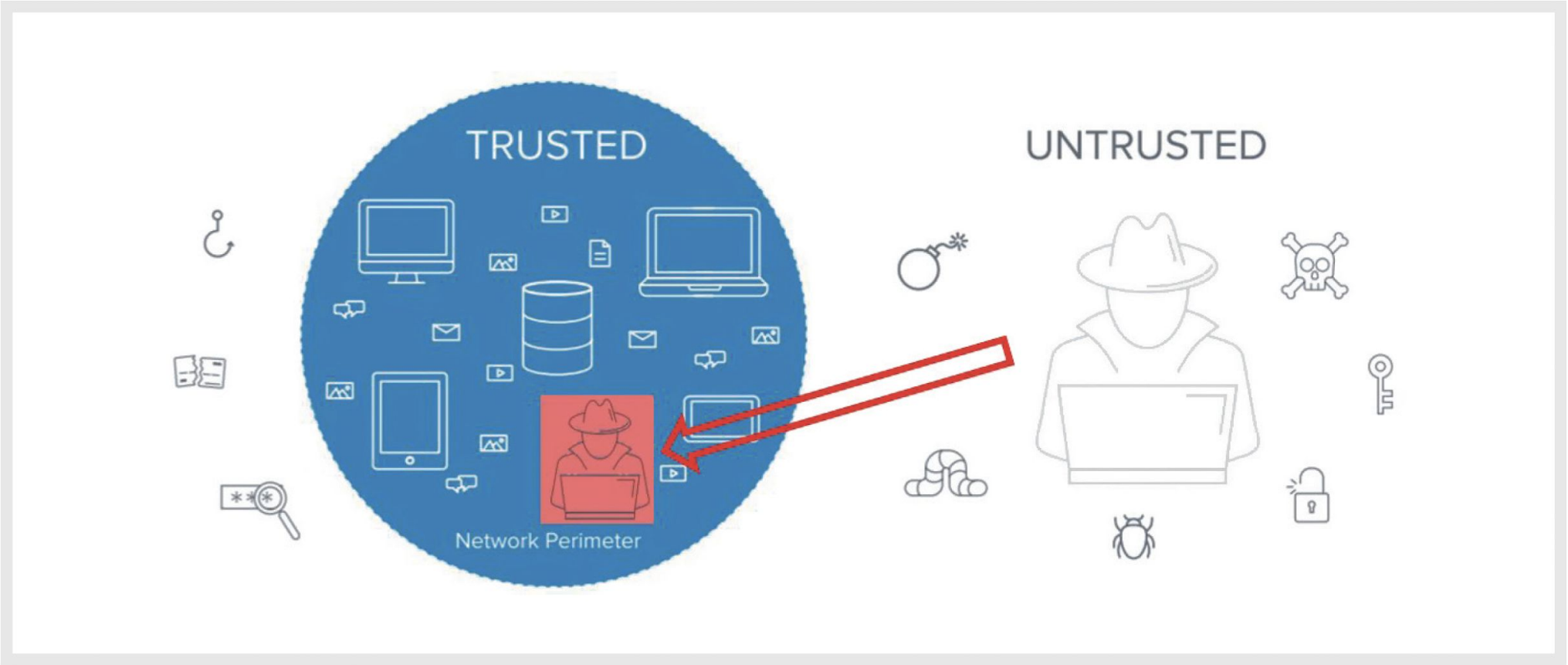
기업의 인프라는 **On-Prem** 에서 클라우드로 빠르게 전환되고 있습니다.



CLOUDFLARE

대부분의 해킹 및 침해사고는 기업 내부망에서 자의/타의에 의해 발생합니다.

〈경계 기반 보안모델의 한계 상황〉

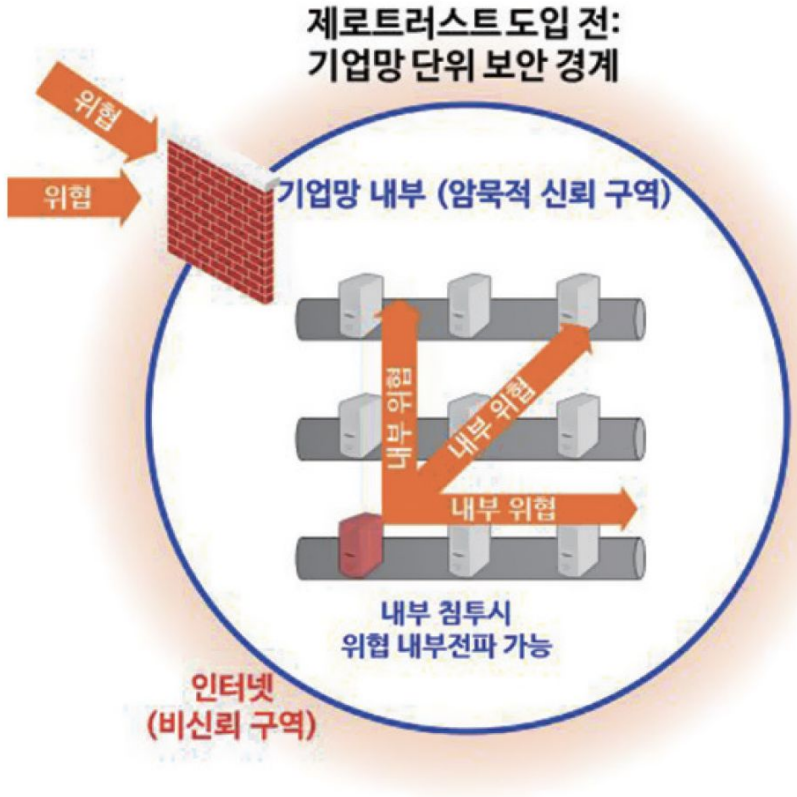


[What is Zero Trust Security / Okta 재구성]

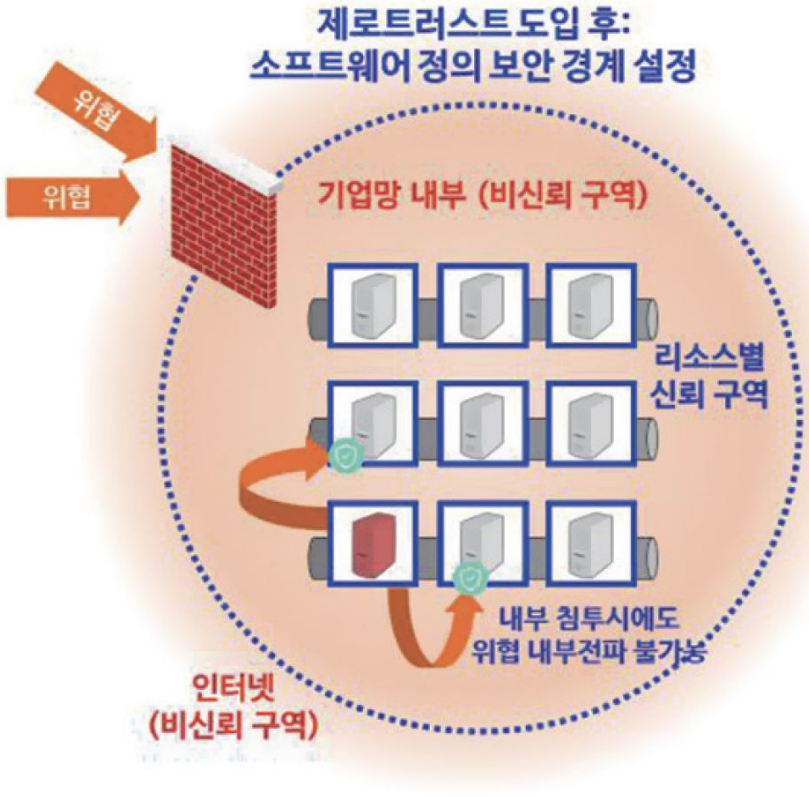
기존 경계 기반 보안과 제로트러스트 개념 비교

CLOUDFLARE

자원의 경계를 구분 -> 정해진 권한만큼만 활동이 가능 -> 인근 자원에 대한 추가 접속 요구 시 지속적 인증으로 침투 제한



▲ 기업망 내부에 접속한 이후 내부 자원에 대한 자유로운 접속 및 데이터 유출

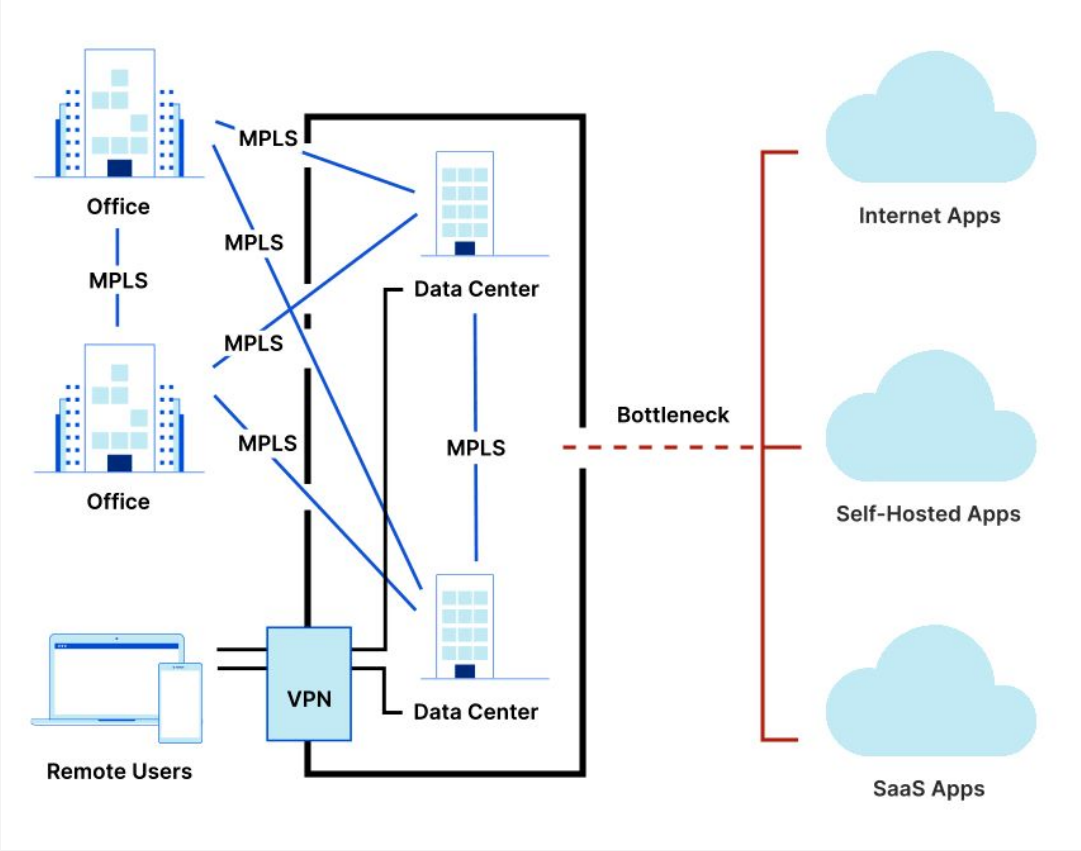


▲ 기업망 내부 모든 자원이 개별적으로 보호되고 선인증 후 접속 등 지속적인 접속 관리

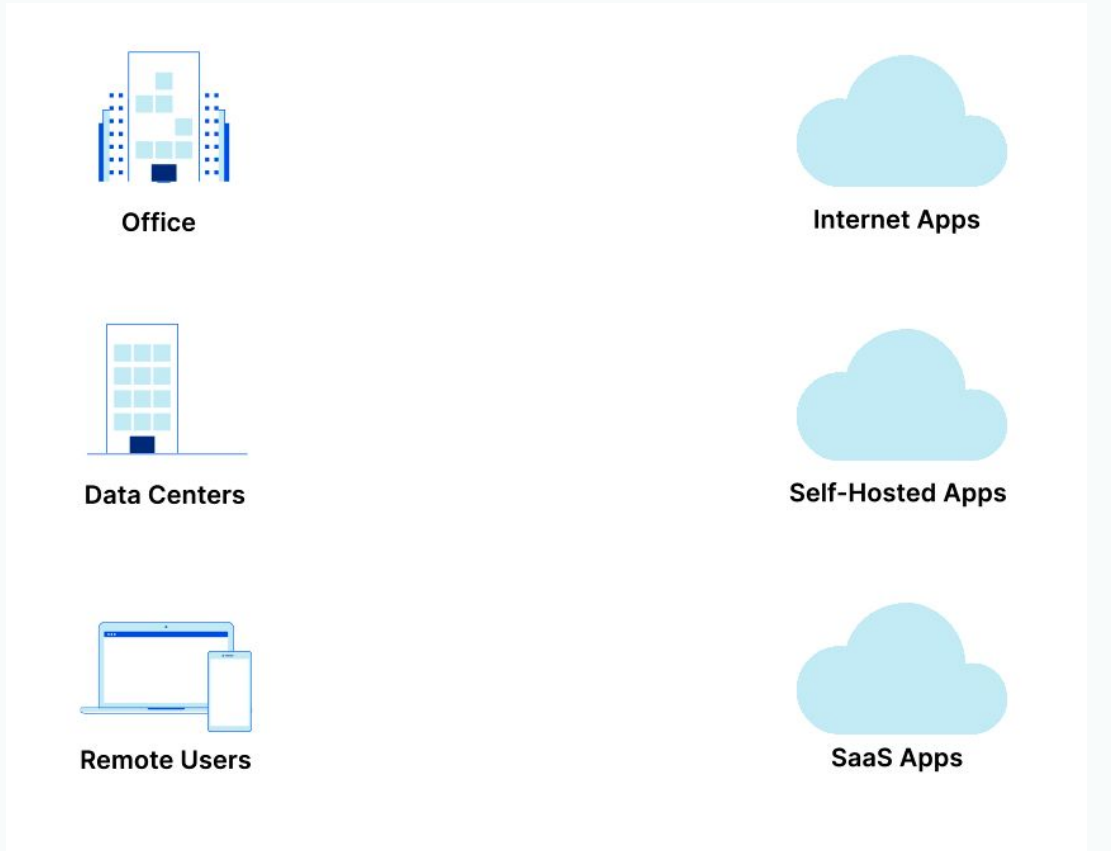
CLOUDFLARE

사용자에게 가장 근접한 CF PoP에 접속 -> “사용자 인증 + 데이터 접속 최소권한 + Full 암호화 접속 + 빠른 앱 접속” 까지 한 방에 해결

기존 DC 중심의 클라우드 및 인터넷 앱 접속 방식



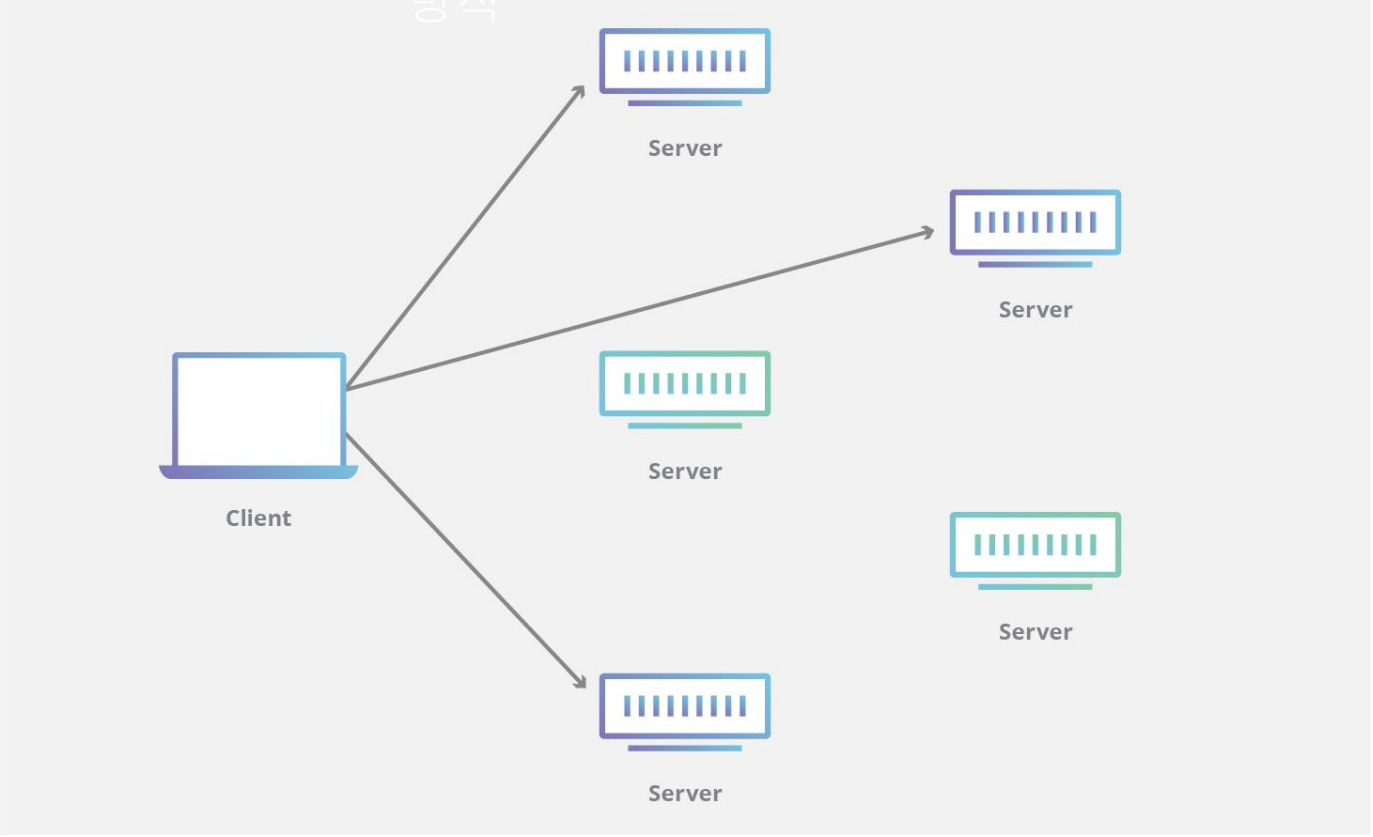
사용자 위치에 상관없이 Cloudflare 플랫폼의 보안 서비스 제공



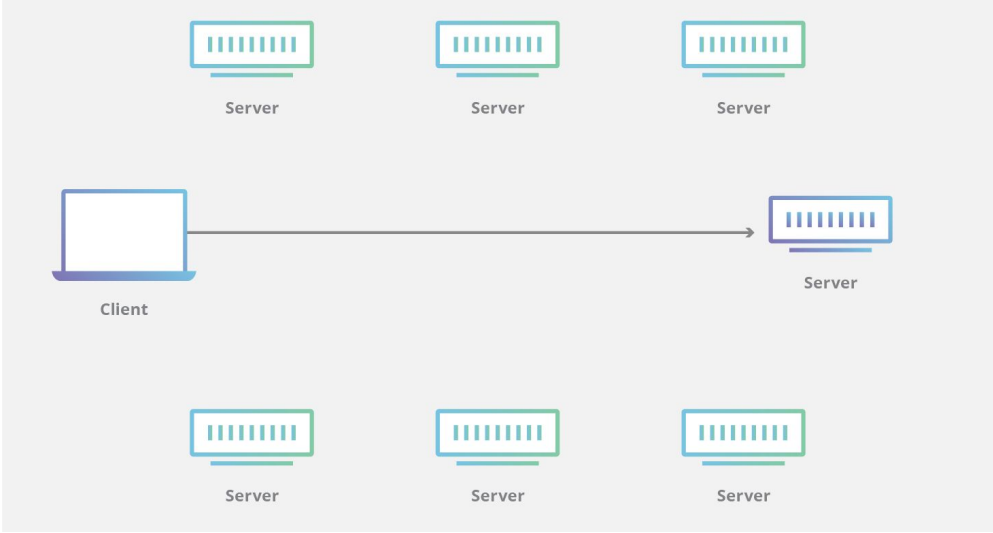
Anycast vs Unicast (클라우드 플레어의 최대 장점)

CLOUDFLARE

Cloudflare의 Anycast 방식



타사의 Unicast 방식



CLOUDFLARE

Cloudflare 전역 네트워크

세계에서 가장 빠른 네트워크 중 하나인 Cloudflare의 방대한 전역 네트워크는 수 백만 개의 웹 자산이 신뢰하고 있습니다.

거의 모든 서비스 공급자 및 클라우드 공급자와 직접 연결되는 Cloudflare 네트워크는 전 세계 인터넷 연결 인구의 약 95%에게 약 50ms 이내에 도달합니다.

300

도시 수(중국 본토를 포함한 100+ 개 이상의 국가)

12,500

Cloudflare에 직접 연결된 네트워크 수(모든 주요 ISP, 클라우드 공급자, 기업 포함)

209 Tbps

전역 네트워크 에지 용량(전환 연결, 피어링 및 사설 네트워크 상호 연결로 구성)

~50ms

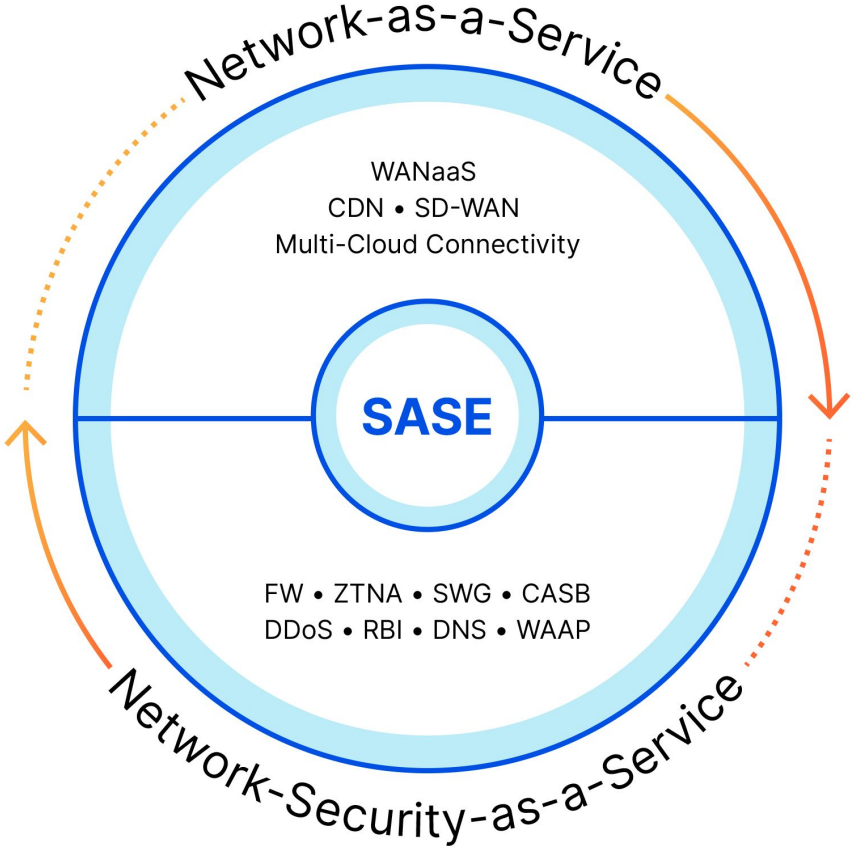
전 세계 인터넷 연결 인구 약 95%의 대기 시간

Cloudflare는 단일 벤더로서 SASE 통합 보안을 제공합니다.

1 Cloudflare One

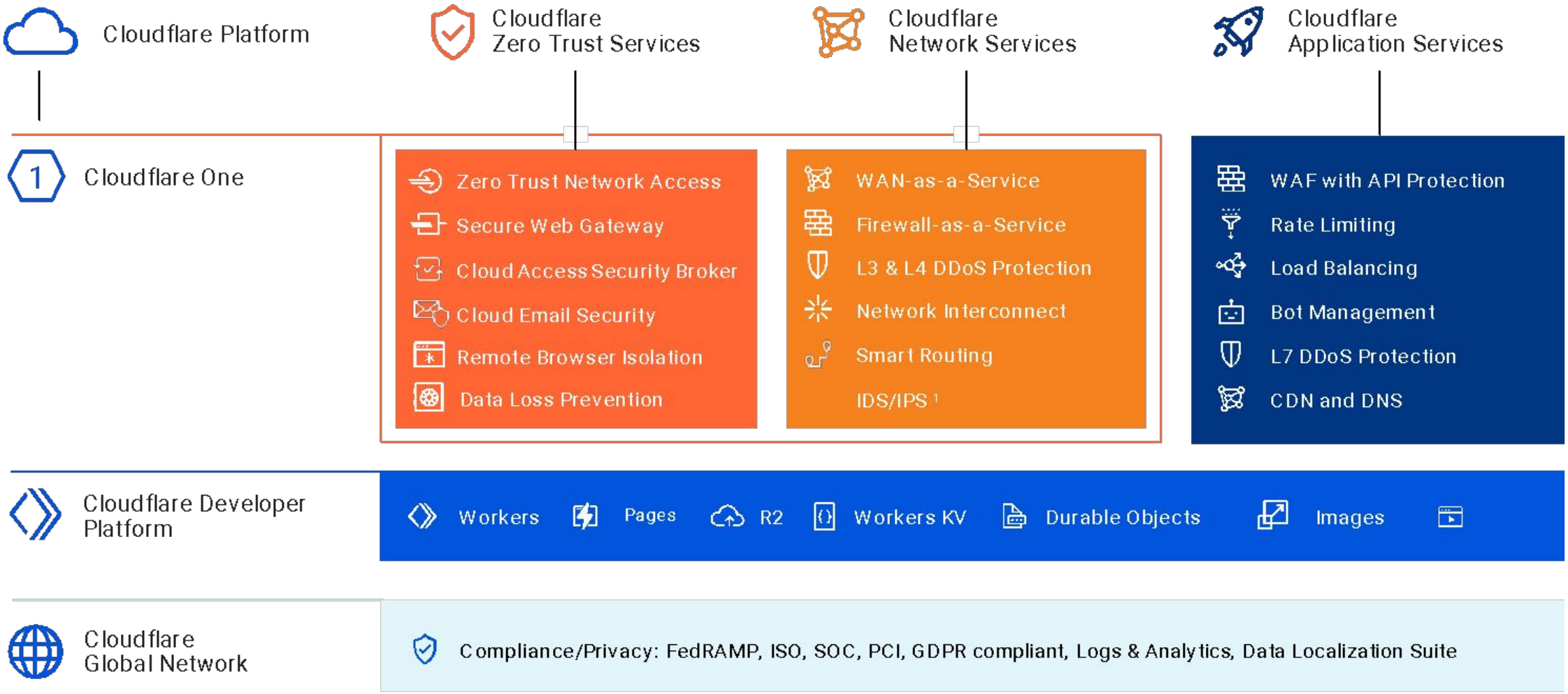
글로벌 클라우드 네이티브 서비스로
네트워크 부터 보안 서비스까지
모든 서비스를 **“클라우드 원”**으로
지원합니다.

=



Cloudflare One = SASE 통합 보안(전 세계 PoP에서 모두 동일하게 동작)

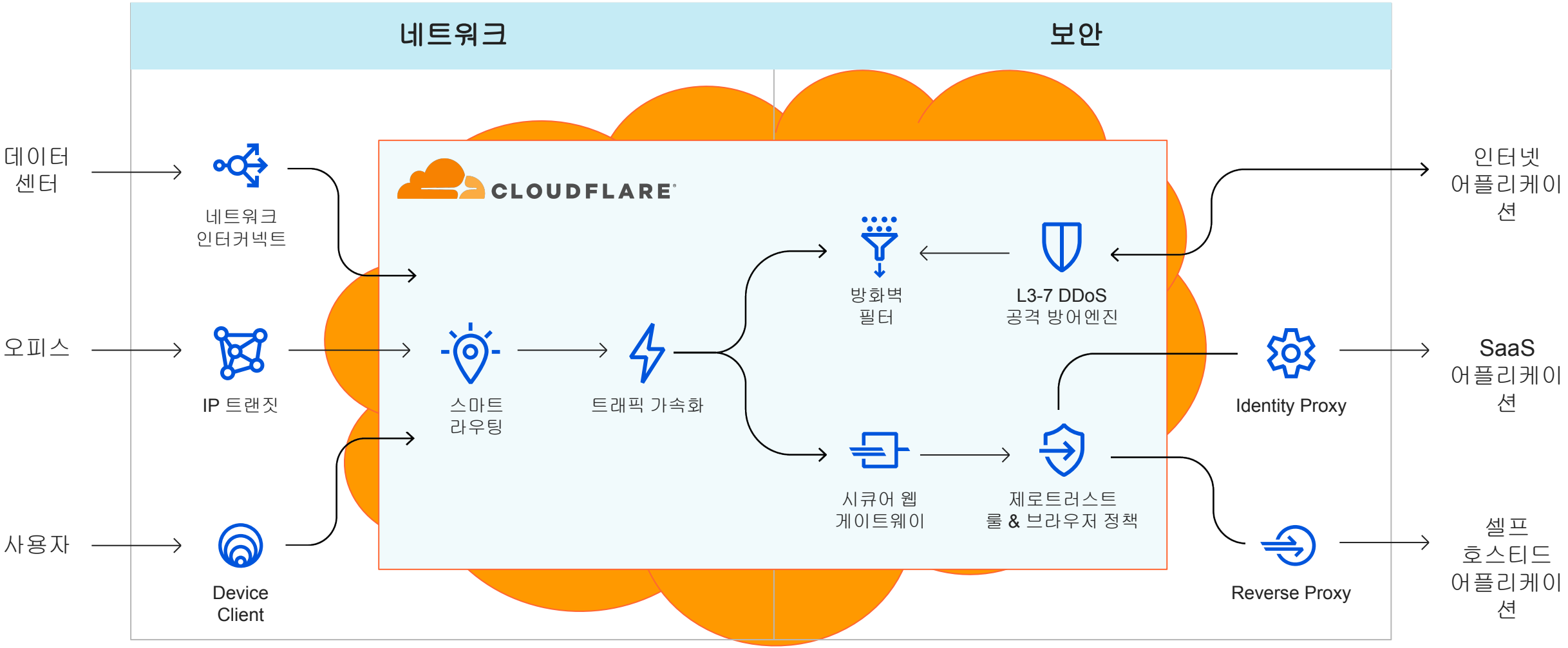
CLOUDFLARE



모든 레이어에서 트래픽 보안 연결 및 클라이드 네이티브 보안서비스 제공

CLOUDFLARE

트래픽의 인터넷 & 클라우드 연결 + 암호 & 가속화 + FWaaS 서비스 + 패킷 검사 + 안전한 트래픽만 기업 어플리케이션 연결



CLOUDFLARE

Cloudflare 제로트러스트는 클라우드 네이티브 보안 서비스를 제공합니다.

ZTNA(Zero Trust Network Access)
기존 VPN 보다 빠르고 높은 보안성 제공 가능

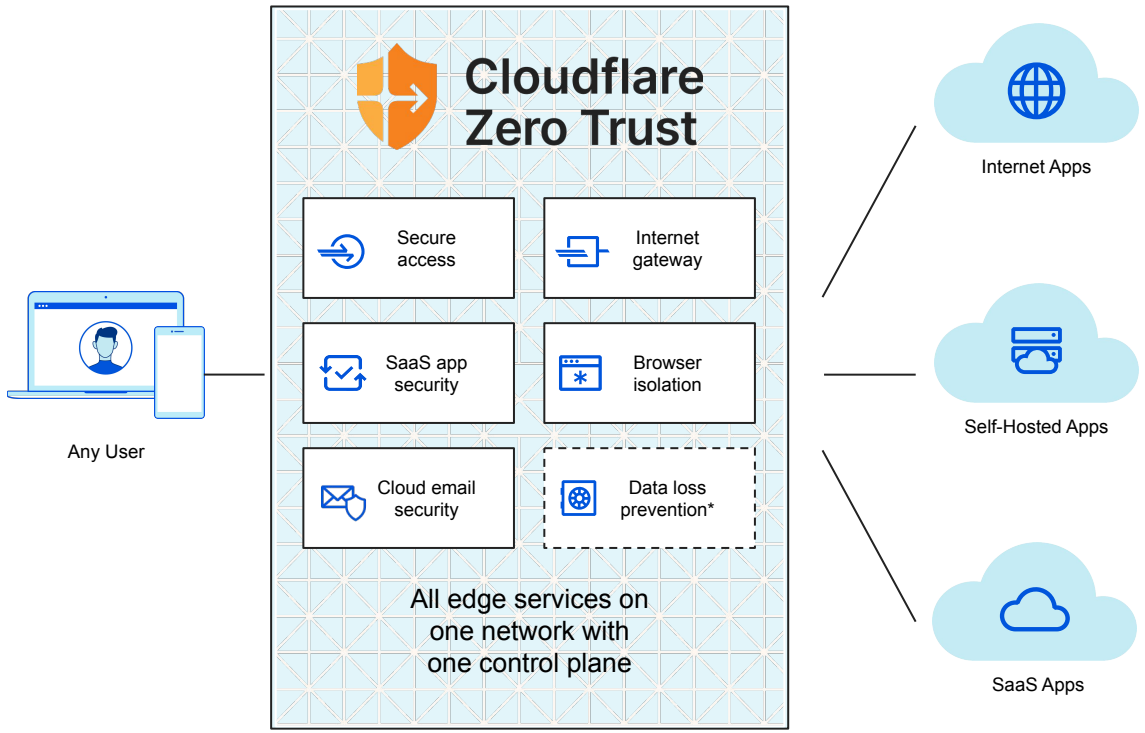
SWG(Secure Web Gateway)
인터넷 상의 멀웨어 감염 및 피싱등의 위협 방지 제공

RBI(Remote Browser Isolation)
악의적인 바이러스 등의 감염 및 데이터 유출 방지 제공

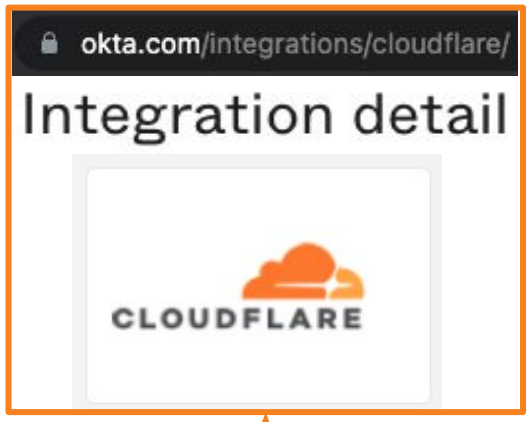
CASB(Cloud Access Security Broker)
안전한 SaaS 접근 및 사용을 위해 접근통제 및 위협탐지 제공

Cloud email security
악의적인 피싱 메일이나 이메일 손상(BEC) 등의 위협 방지 제공

DLP(Data Loss Prevention)
HTTP/S 통신과 문서파일의 민감정보 유출 탐지 및 방지 제공



Cloudflare Access



모든 사용자
모든 인증 가능한
단말장치

Internet

1. 사용자가 웹으로 인증 시도

2. IDP(인증공급자)에서 사용자 ID/PWD + MFA(SMS, Email 등)로 인증 성공
-> 단말 무결성 확인(e.g., AV실행, 방화벽, 기업필수프로그램 설치 및 실행 여부, 인증서 탐지 등)

Identity Providers

Device Posture

3. 인증된 사용자만 최소 권한으로 데이터 접근

Resources

Google Workspace
Microsoft 365
box
slack
GitHub
salesforce

CASB(Cloud Access Service Broker)
SaaS 서비스 이용 시 사용자에게 최소 권한만 부여하고 이상행위 탐지 시 즉시 차단하는 기능

Clientless vs Client(WARP

클라이언트리스 방식(Web 기반)	클라이언트 방식(에이전트 기반)
지원가능한 어플리케이션 ▪ HTTP/S ▪ Web SSH/VNC ▪ SaaS	지원가능한 어플리케이션 ▪ RDP and SMB ▪ SSH and VNC thick-client 지원 ▪ TCP/UDP 통신이 필요한 모든 C/S
특장점 ▪ 웹에서 직접 엑세스하기 때문에 매우 빠른 앱 접근 지원 ▪ 인브라우저 터미널을 통한 로깅방식 지원	특장점 ▪ VPN 모드 지원, IP기반으로 엑세스 가능한 세그먼트 분류 및 정책 설정 가능 ▪ VPN과 동시 사용가능(Split Tunnel) ▪ IDP인증시 단말 무결성 체크

모든 사용자
모든 인증 가능한
단말장치

WARP 에이전트
(PC, 모바일 지원)

1.1.1.1

The free app that makes your Internet safer.

Now available for even more devices.

App Store | Google Play

macOS | Windows | Linux

Internet

SaaS 서비스

Google Workspace

Microsoft 365

slack GitHub

box salesforce

CloudflareD 데몬 설치
- 터널(QUIC) & SW GW 역할
- Win, OSX, Linux, Container 지원

IaaS

AWS Azure

암호화된 터널 구간 생성
(아웃바운드 Only)

암호화된 터널 구간 생성
(아웃바운드 Only)

DC & 온프램

CloudflareD 데몬

K8 온프램

SSH

RDP

SMB

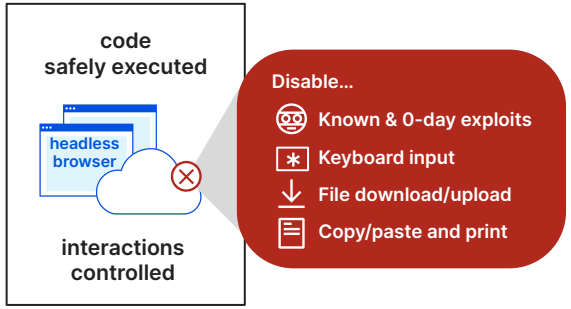
1. OnPrem, IaaS 환경에 CloudflareD 터널을 설치
2. 터널을 통해 각 서버 서비스 및 프로토콜, 포트에 접속 가능
3. 터널은 설치 직후 글로벌 CF PoP으로 자동 연결 -> 외부 스캔 및 접근 차단
4. 고객 방화벽에서 NAT에 아웃바운드 Rule 추가작업없이 전구간 암호화 연결됨

Cloudflare Gateway(SWG)

DLP (Data Loss Prevention)

기업데이터가 외부로 Web을 통해 유출되지 않도록 템플릿을 통해 개인정보, 민감/중요정보들을 사전에 지정하여 외부 유출 시도시 자동탐지 및 즉시 차단하는 기능

Internet



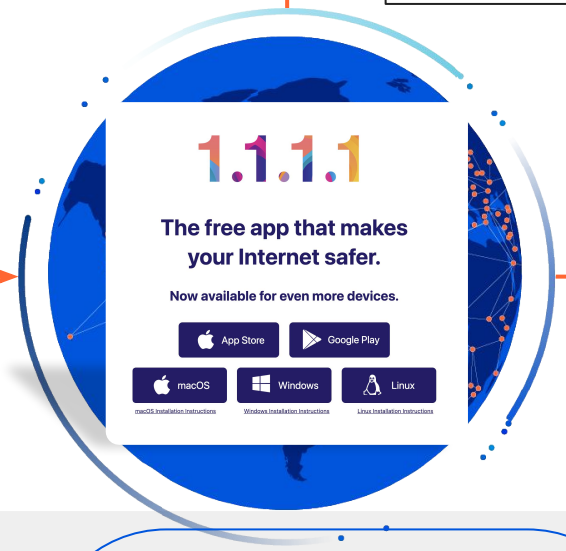
RBI (Remote Browser Isolation)

사용자가 실제 단말이 아닌 가상 브라우저 상에서 모든 코드를 실행하며 웹 이용 -> 제로데이 공격 원천 방지, 키보드 입력제한, 파일 다운로드/업로드 제어, 복사/붙여넣기, 출력 제어 지원

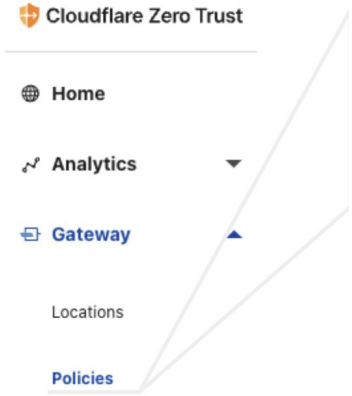
모든 사용자
모든 인증 가능한
단말장치

사내: **GRE/IPSEC or WARP** 에이전트

사외: **WARP** 에이전트 (PC, 모바일 지원)



Resources

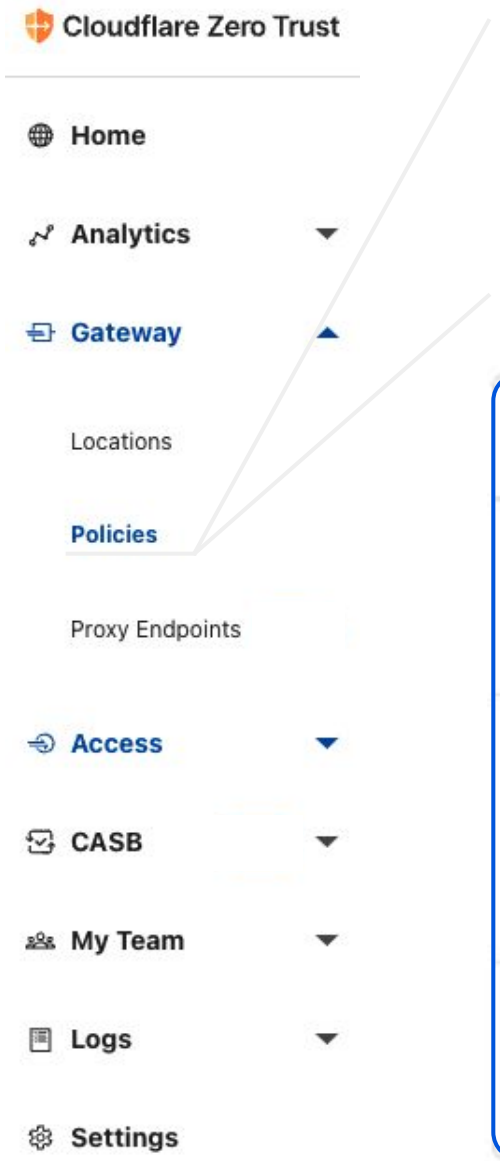


DNS	Network	HTTP
Domain	IP/Port/FW (L3/4)	HTTP/S (L7, Payload)

Cloudflare Gateway(SWG)

CLOUDFLARE

전 세계 20% Live 트래픽 기반의 최대 Threat Intel DB를 통한 Reputation 보호(e.g., 악성IP&Domain, C2C, Botnet, DNS, Mal



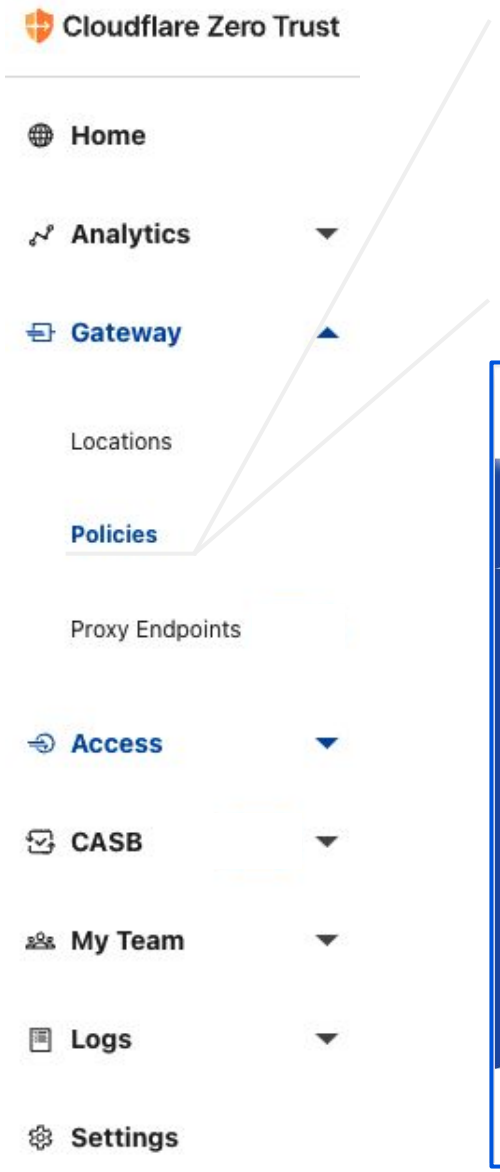
DNS **Network** **HTTP**

Domain

Category	Definition
Anonymizer	Sites that allow users to surf the Internet anonymously.
Command and Control & Botnet	Sites that are queried by compromised devices to exfiltrate information or potentially infect other devices in a network.
Malware	Sites hosting malicious content and other compromised websites.

Cloudflare Gateway(SWG)

FwaaS 서비스와 같은 네트워크 방화벽 기능 지원(e.g., IP/Port/Protocol/Country 등 비인가된 모든 L3/L4 조건값을 활용하여 연결 차단)



DNS Network HTTP

IP/Port/FW (L3/4)

	Policy name	Action	Enabled	Last edited
1	Permit RDP 85d71f08-f227-41cf-81ec-a75642de6208	ALLOW	✓	July 29, 2022 • 6:19 PM

Policy description
Permit RDP from approved subnets

Date created
July 29, 2022 • 6:19 PM

Selector	Operator	Value
Source IP	in	172.16.0.0/12
Destination Port	is	3389

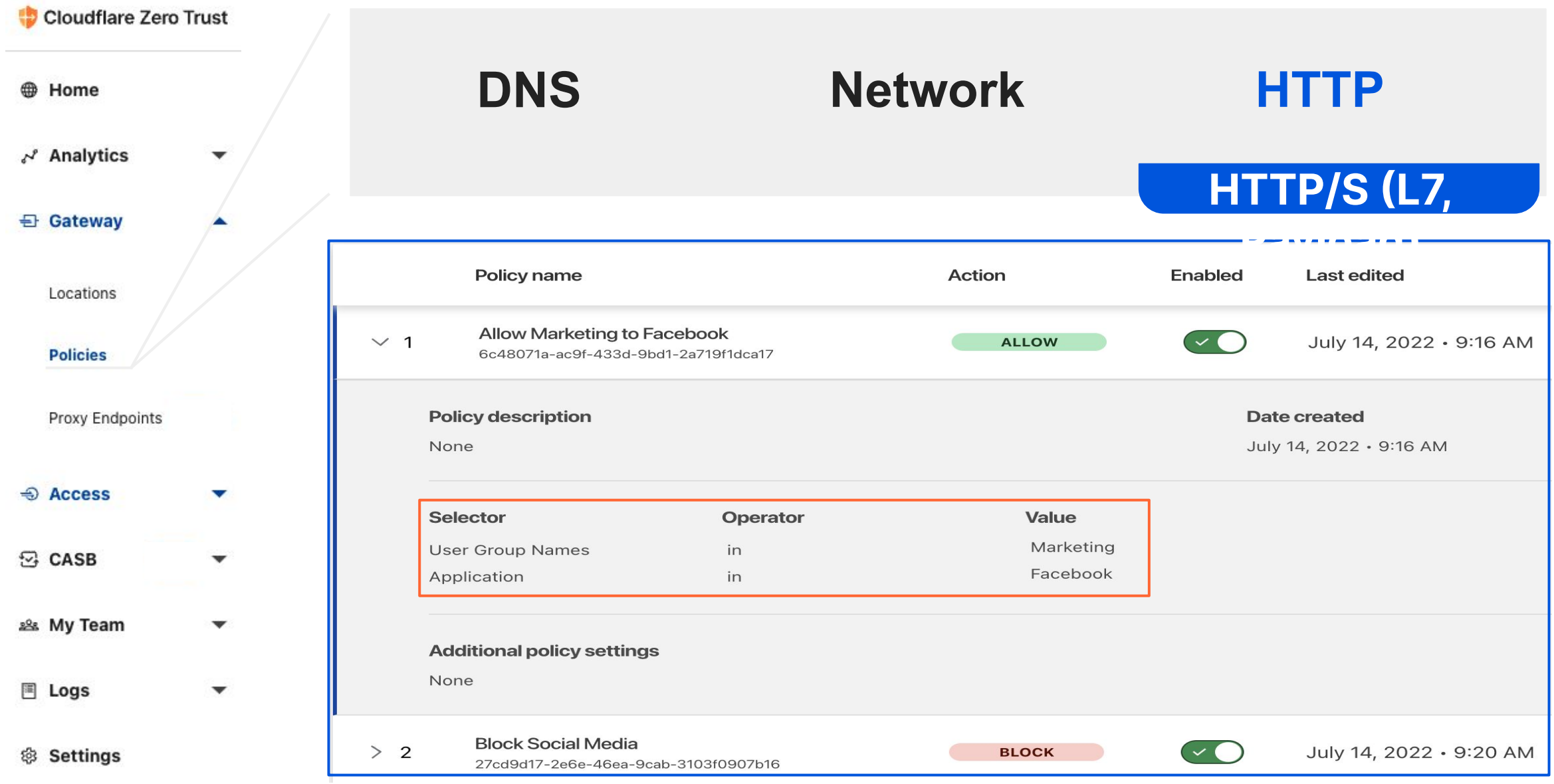
Additional policy settings
None

2	Block RDP dcbeca71-1850-4b80-9fa1-160f21ae09ed	BLOCK	✓	July 29, 2022 • 6:20 PM

Cloudflare Gateway(SWG)

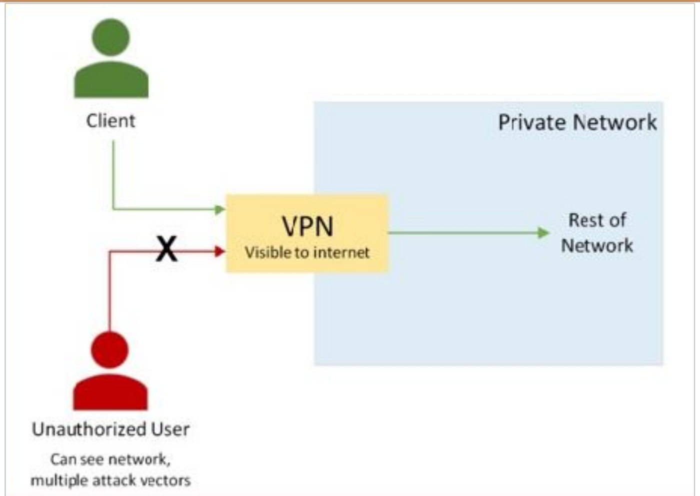
CLOUDFLARE

HTTP/S 트래픽 검사 지원(e.g., Payload 검사를 통해 유해사이트, 컨텐츠별 허용/차단, 검색, 다운로드/업로드 차단 등)



고객 성공사례 1) 소프트웨어 개발 및 공급 B사

MPLS & VPN ▯▯ ▯ ▯▯▯▯ ▯▯▯ ▯▯▯▯▯▯ SSO▯▯ ▯ ▯▯ (Azure AD ▯▯)

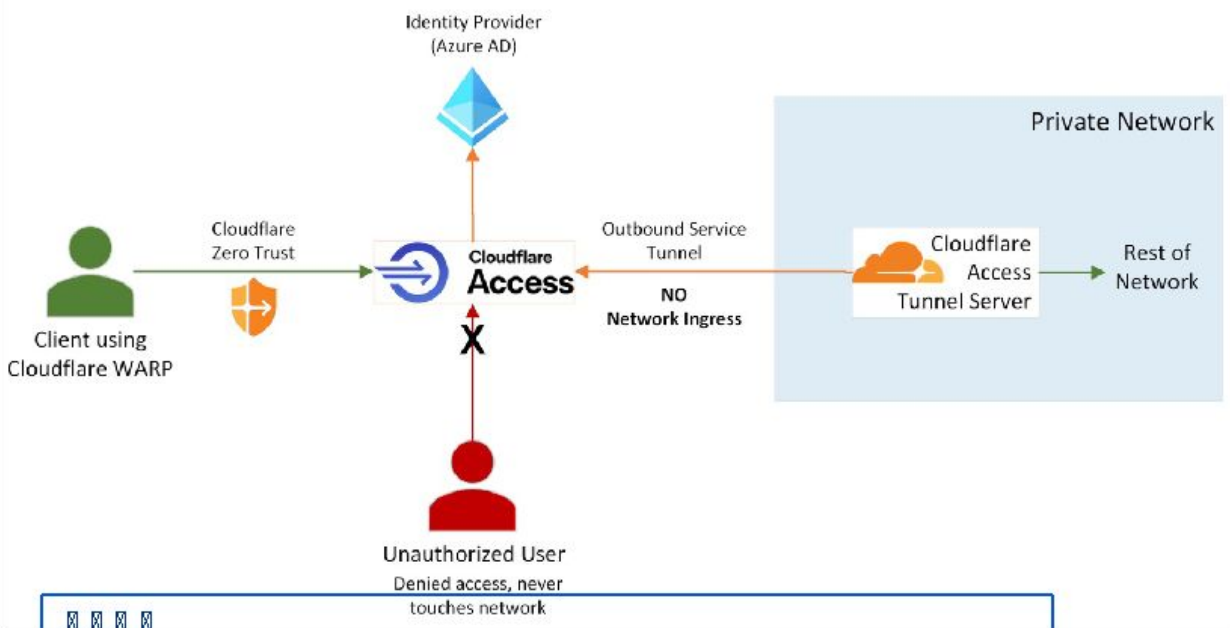


▯▯ ▯▯▯

1. F▯▯ SSL VPN ▯▯▯ ▯ 7▯▯ ▯▯▯▯ ▯▯▯▯▯ ▯▯ ▯▯ ▯▯ ▯▯ ▯▯▯ ▯▯▯▯▯▯ ▯▯ -> ▯▯ ▯▯ ▯▯ ▯▯▯▯, ▯▯▯, ▯▯▯ ▯▯▯▯▯ ▯▯ ▯▯▯ ▯ ▯▯▯▯ ▯▯

2. ▯▯▯ ▯▯▯▯ ▯▯ & ▯▯▯▯ ▯▯▯▯▯ ▯▯▯▯ ▯▯▯▯▯ ▯▯▯▯▯▯ ▯▯ -> ▯▯▯ ▯▯▯ VPN▯ ▯▯▯ ▯▯ ▯▯, ▯▯▯, ▯▯▯▯ ▯▯ ▯▯▯▯▯▯ ▯▯ ▯▯ ▯▯

3. MPLS & VPN▯ ▯▯▯ ▯▯ ▯▯ ▯▯ ▯ ▯▯ ▯▯ ▯▯



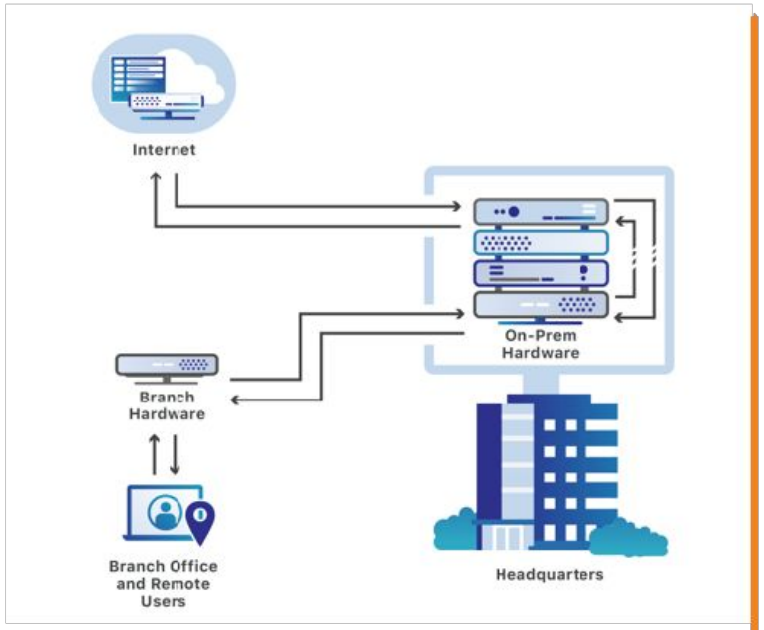
▯▯▯▯

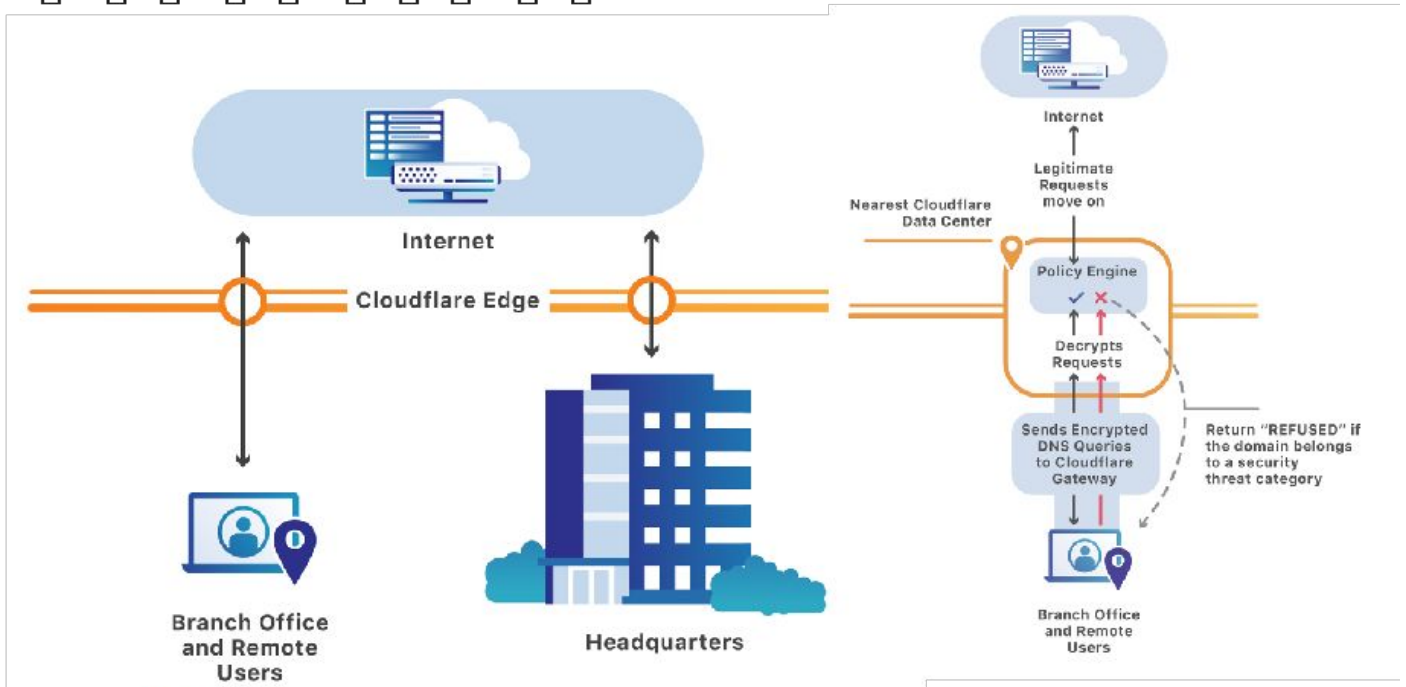
1. ▯▯▯ ▯▯▯ Cloudflare WARP ▯▯▯▯ ▯▯ -> ▯▯/▯▯▯ ▯▯ Application(*▯, C/S, SaaS▯)▯ ▯▯▯▯▯ ▯▯▯ ▯▯ ▯▯ ▯▯ -> ▯▯ SSL VPN ▯▯ 42% ▯▯ ▯▯ ▯▯ (*PoC▯ ▯▯▯ ▯▯▯ App ▯▯ ▯▯▯▯ ▯▯)

2. Azure AD▯ ▯▯▯▯ ▯ ▯▯▯▯ AD Group▯ Role▯▯▯ Access▯▯ ▯▯ ▯▯ -> ▯▯▯▯ AD▯ ▯▯▯▯▯▯ ▯

3. L7▯▯ ▯▯▯▯ ▯▯ VPN▯▯ ▯▯▯▯▯ ▯▯ ▯▯▯ ▯▯ ▯▯▯ ▯▯▯ ▯▯▯▯ ▯▯▯▯▯▯ -> L3▯▯ ▯▯ ▯▯▯ ▯▯ ▯▯▯ ▯▯▯

고객 성공사례 2) 글로벌 물류 유통 D사





1. (e.g. ,IPS, Email, VPN)
->

2.

1. (*DNS, URL, Payload)

2. 74%

3. (Location, Onsite/Offsite)
Whitelist/Blacklist

CLOUDFLARE

감사합니다

CLOUDFLARE

Cloudflare 클라우드 보안

클라우드 활용한 디도스 방어 및 어플리케이션 보안

이계경 | 클라우드플레어 솔루션 엔지니어

클라우드플레어 제공 서비스

CLOUDFLARE

클라우드플레어 플랫폼

1 클라우드플레어 원

클라우드플레어 제로트러스트 서비스

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

클라우드플레어 네트워크 서비스

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

클라우드플레어 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

1. Contact us to request access

보안 인텔리전스

초당 46백만건(평균), 64백만건(피크) http 요청 처리

초당 26백만(평균) 일간 2.2조(평균) DNS 조회 건 처리

2.5 Tbps 디도스 공격 방어('22년 3분기)
초당 71백만 https 디도스 공격 방어 ('23년 2월)

일평균 14백억 사이버 위협 차단('23년 2분기)

300+
도시 수(중국 본토를 포함한 100개 이상 국가)

12,500+
Cloudflare연결된 네트워크 수 (모든 주요 ISP, 클라우드 공급자, 기업 포함)

209 Tbps
네트워크 엣지 용량(트래짓, 피어링 및 사설 네트워크 상호 연결로 구성)

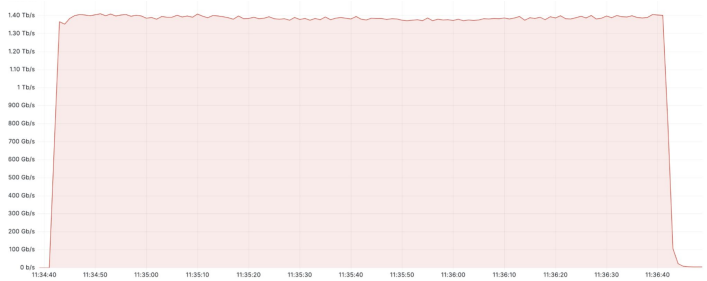
~50 ms
전 세계 인터넷 사용자의 95% 왕복지연시간

디도스 공격 방어

CLOUDFLARE

디도스 공격 동향 (‘23년 2분기) - VM 기반의 봇넷의 대두

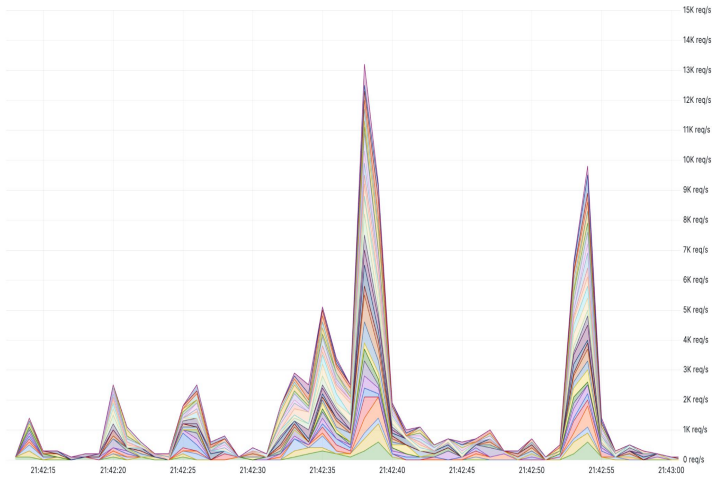
1.4 Tbps 의 볼륨 DDoS 공격



Attack stats:

- **Attack vector:** ACK Flood
- **Botnet:** Mirai-variant, 11K IPs
- **Rate:** 1.4 Tbps
- **Duration:** 2 minutes
- **Target**: American Service Provider

고도로 무작위화된 HTTP 디도스

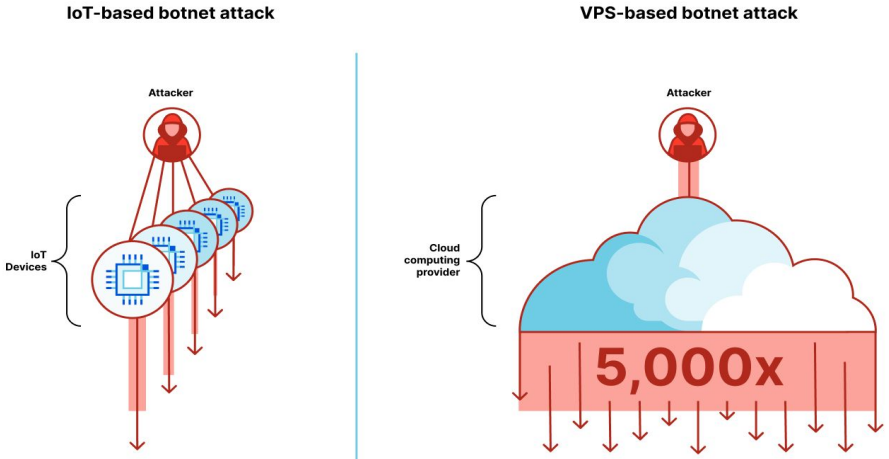


Attack stats:

- **Attack vector:** Random HTTP GET Flood
- **Botnet fleet size:** 15K
- **Rate:** 13K rps
- **Shortest peak**: 3 seconds
- **Duration**: 1 minute
- **Target**: Major VoIP provider
- **Randomization:**
  - 681 Client Hello fingerprints
  - 31 attack signatures

VM 기반의 강력한 봇넷 대두

(기존 IOT 봇넷 대비 5000배 용량)



HTTP/2 도입 확대로 인해 웹사이트 성능 뿐 아니라 봇넷의 성능도 증가

Virtual Machines 활용

IOT 기기 대비 5,000배의 용량

클라우드플레어는 클라우드 컴퓨팅 사업자와 위협의 최소화하기 위해 협업 중

CLOUDFLARE

자동화되고 상시 방어가 가능한 솔루션 선택 필요

- VM기반 봇넷을 활용한 공격, 더 커진 대역폭 및 컴퓨팅 파워를 이용한 대규모 공격

→ 공격자(사람)이 기획하고 봇을 통한 공격을 실행함으로 자동화된 트래픽 탐지하고 상시 방어 체계 필요

- 무작위화되고 복잡하고 높은 수준으로 잘 설계된 공격

→ 실시간 위협 인텔리전스, 공격 탐지하고 분류하는 데 기계 학습 활용, 지속적으로 트래픽 프로파일링

- 공격자가 사전에 공격 대상 네트워크 구성 및 취약점을 지속적으로 학습

→ 자사의 위협 요인을 이해하고 취약 부분에 대한 대비책 마련

CLOUDFLARE

디도스 방어 — 네트워크, 어플리케이션 레이어 방어

7	**Application Layer**
6	Presentation Layer
5	Session Layer
4	**Transport Layer**
3	**Network Layer**
2	Datalink Layer
1	Physical Layer

Cloudflare DDoS Protection
for Web Applications

Cloudflare Spectrum
for TCP/UDP applications

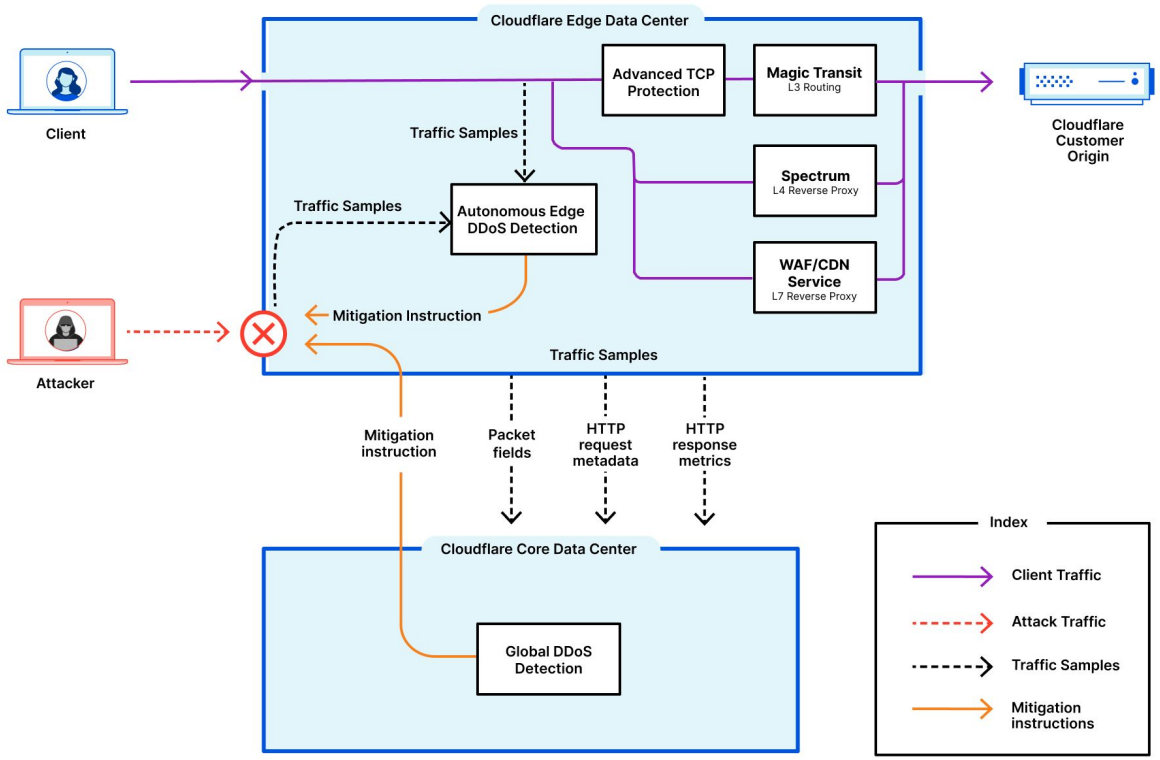
Cloudflare Magic Transit
for entire IP networks

Cloudflare DDoS Protection

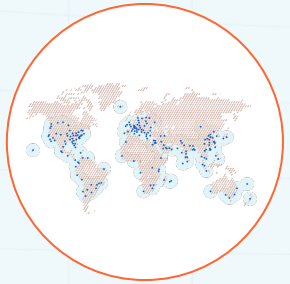
CLOUDFLARE

Cloudflare 네트워크 내 자동화된 DDoS 방어체계

- 엣지 자율 방어: *비중앙화* 전 세계 300여개 데이터 센터 분산된 엣지 서버에서 트래픽을 분석하고 디도스 공격 감지 시 자율적으로 방어 규칙을 생성하고 실행
- 글로벌 방어: *중앙화* 중앙 데이터 센터에서 글로벌하게 분산된 볼륨 디도스 공격을 탐지하고 자율적으로 방어 규칙을 생성하고 개별 데이터 센터로 전달하여 개별 데이터 센터 해당 규칙에 따라 디도스 방어
- 고급 TCP 방어: *TCP 상태 추적* , ingress 트래픽만을 클라우드플레어 통하여 처리되는 경우라도 복잡한 TCP 공격을 방어
- 프로파일링 기반 방어 : *트래픽 프로파일링* 트래픽 프로파일링을 통해 이상 트래픽을 감지하여 자동 방어 개시
- Magic Firewall: IP 화이트리스팅/블랙리스트, 보안 인텔리전스, 국가/지역별 차단 설정

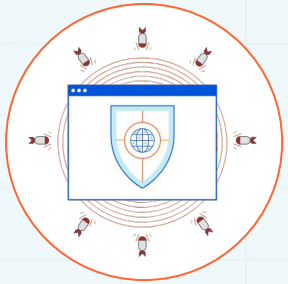


Cloudflare 디도스 방어 장점



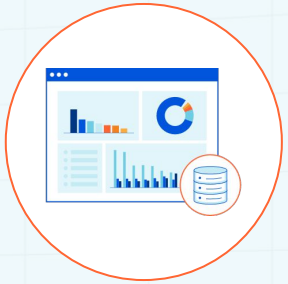
현대화된 SASE 아키텍처

- 209 Tbs 방어 용량을 갖춘 Anycast 기반 단일 글로벌 네트워크
- 통합된 L3-7 방어
- 스크러빙 센터 기반이 아니고 자체 개발 소트프웨어 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



사용의 편의성

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

어플리케이션 보안

CLOUDFLARE

CLOUDFLARE

봇 트래픽 비중

전체 인터넷 트래픽 중

30-40%

모바일 및 데스크탑 사이트 중

94% 써드파티 스크립트 사용

2021년

+20K

취약점 발견

API 트래픽 비중

HTTPS 트래픽중

55%

CLOUDFLARE

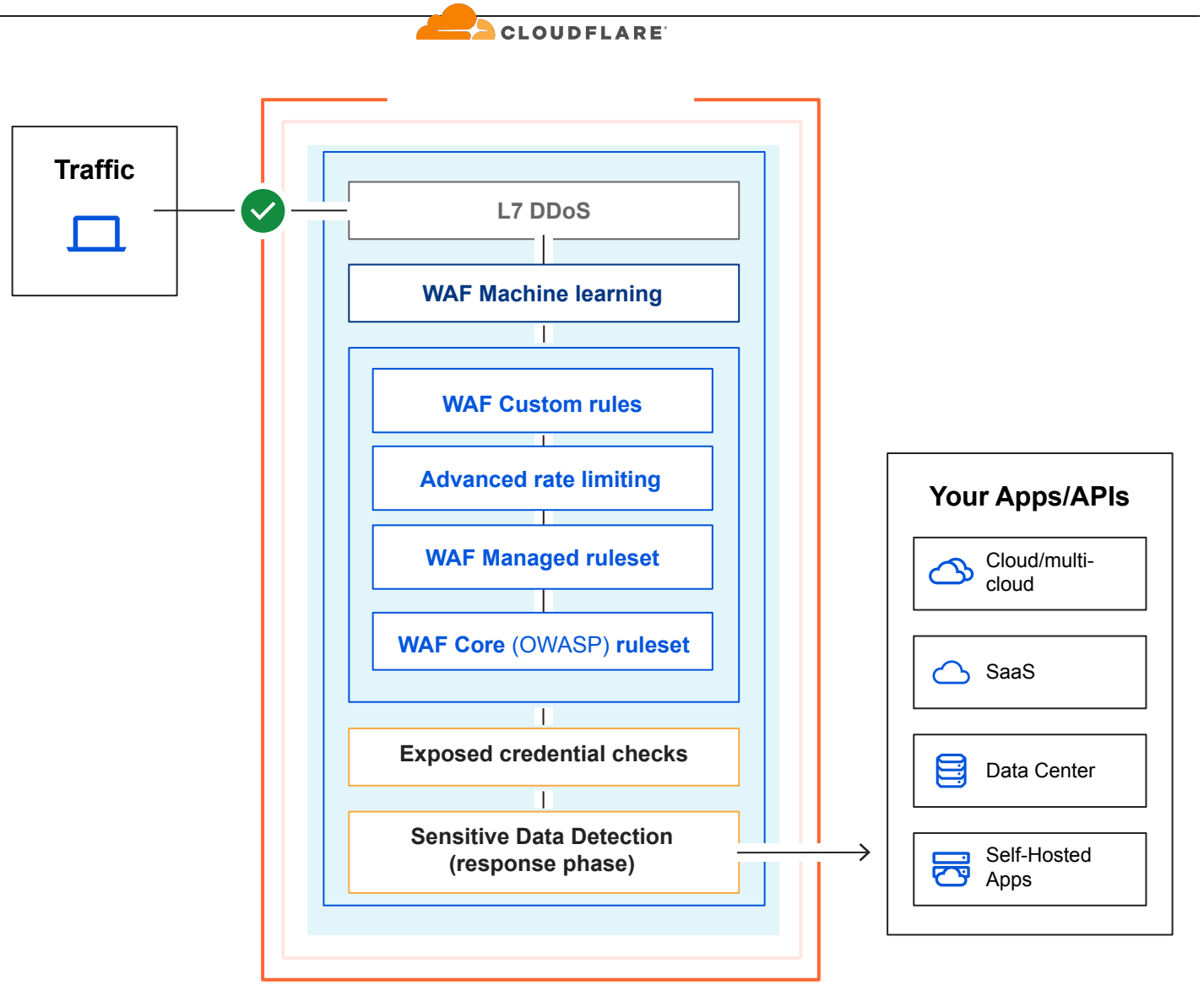
모든 요청에 대한 검사

신규 보안 취약점 및 위협에 대한 클라우드플레어 관리 보안 규칙을 통해 좀더 빠른 방어

보안 규칙을 우회하려는 바이패싱 공격에 대해 기계 학습을 통한 탐지

유출 암호 사용과 데이터 유출에 대해 손쉬운 탐지 및 차단 적용

API 호출에 다양한 조합의 호출 건수를 기록할 수 있는 고급 Rate Limiting

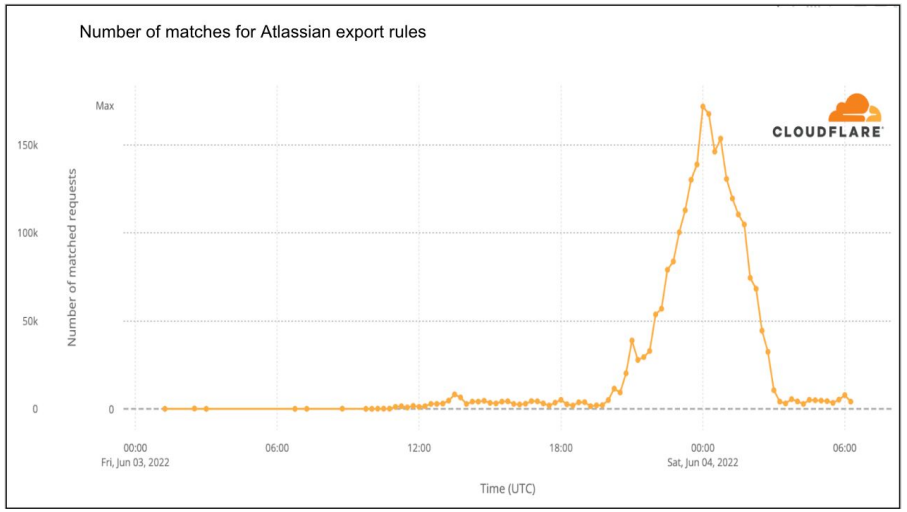


CLOUDFLARE

Confluence

30 분내에 보안 규칙 배포

공격 시작 3.5 시간 전 에 처리



2022-06-02 20:00 (UTC) 기준 아틀라시안사에서 긴급 보안 권고

원격코드실행(remote code execution) 취약점 Confluence 제품에서 발견

클라우드플레어 내부 보안팀 즉시 보안 조치 착수

- 23:38(UTC) 모든 고객사를 보호하기 위해 보안규칙 배포
- 내부 Confluence 서버 영향 여부 조사하고 영향 없음 확인

과거의 공격 이력 확인하여 잠재적으로 동일한 공격 위협을 '22년 05-26 00:33(UTC) 기준으로 확인했고, 취약점 보고 이전에 실제 공격이 작동한 사례가 있음 확인

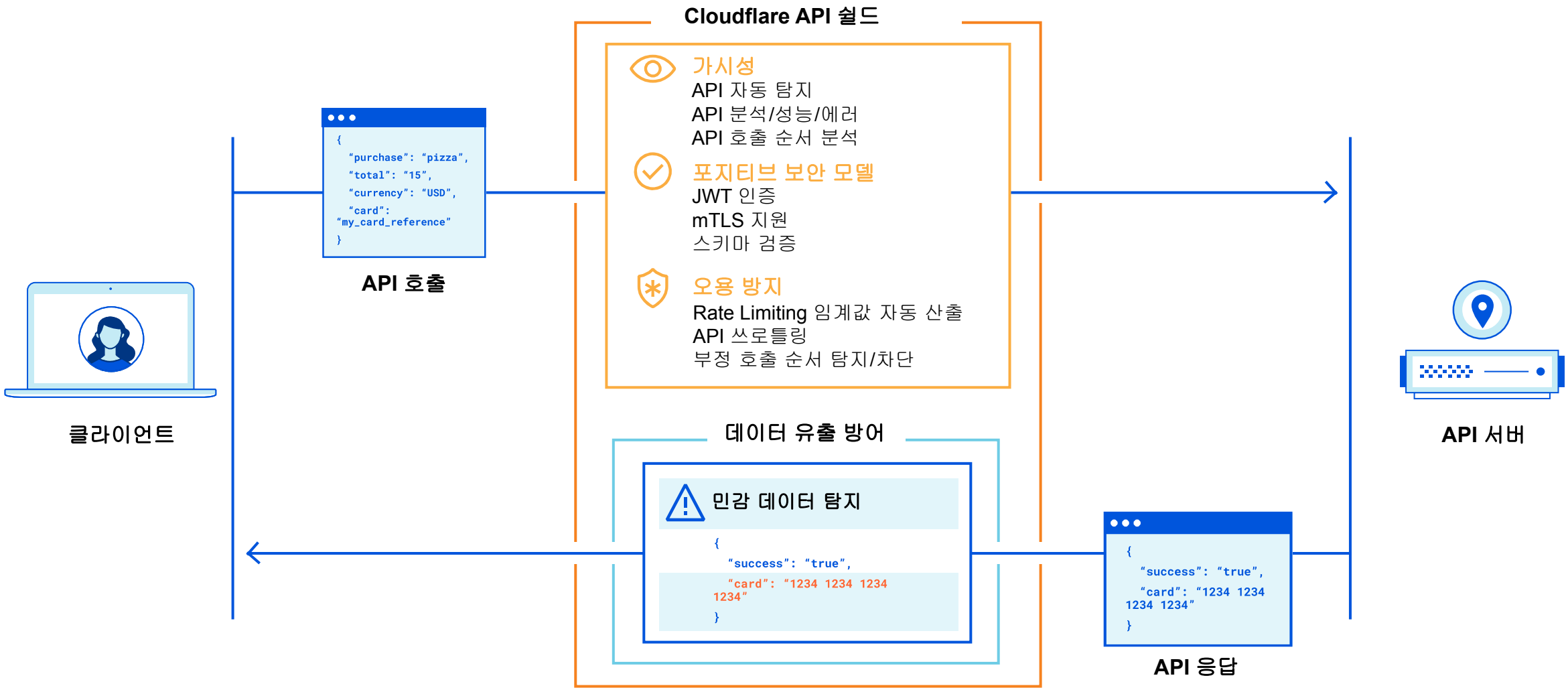
2022-06-03 10:30(UTC) 신규 WAF 규칙이 적용된 10시간 이후 최대 규칙 트리거링이 발생했고 이는 해당 취약점에 대해 확산되고 취약점 확인에 대한 테스트가 이루어진 시점과 일치. 해당 시간 대 공격자들이 해당 취약점에 대한 스캐닝을 시작한 최대화된 시점으로 보임

이때 정확한 취약점과 일치하지 않는 공격성 트래픽이 많이 유입된 것으로 보안 공격자들이 정확한 취약점을 스캐닝 한 것으로 보이고, 이후 WAF 규칙을 수정한 이후 2022-06-23 23:00(UTC) 이후 트리거링 수가 급격히 감소함.

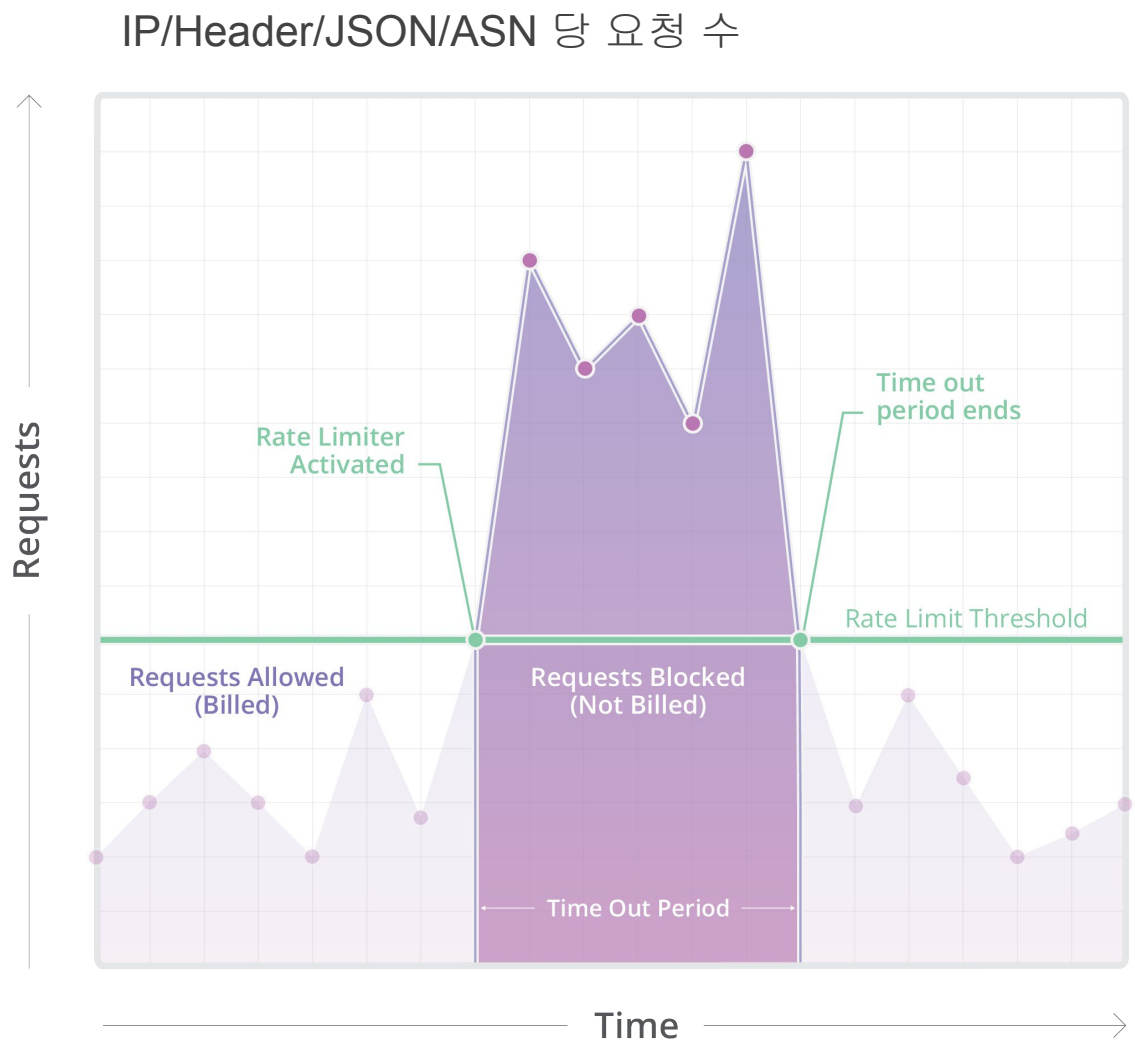
좀더 자세한 이야기는 **blog.cloudflare.com** 보실 수 있습니다.

API 트래픽 관리 및 보안

CLOUDFLARE



API 트래픽 보안 - Rate Limiting



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

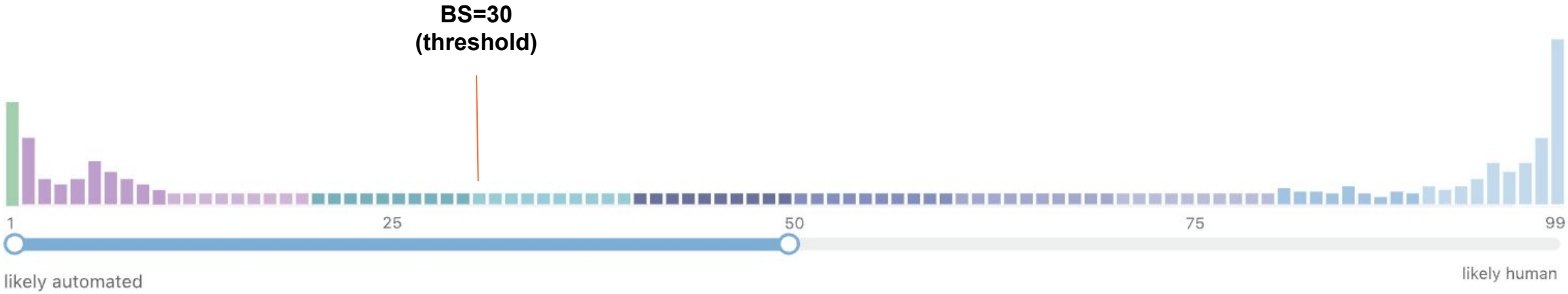
- 호출자의 다양한 특성(IP/HTTP header, Cookie/API 키값, JSON 변수)에 따라 호출 수를 측정 유지하고 정책에 따라 과도한 사용이 확인된 경우 차단(초,분,시간,일)등의 관리 조치

Qualification

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

CLOUDFLARE

봇스코어링 클라우드플레어 2400만개 도메인의 위협 정보를 머신 러닝 및 핑거프린팅 분석 기법을 사용하여 위협 점수 제공



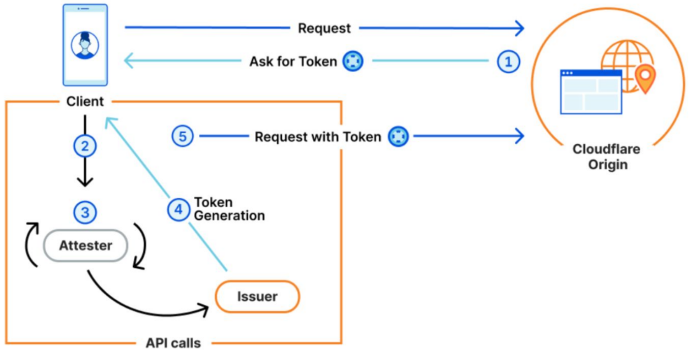
Heuristics	JavaScript Detections	Anomaly Detection	Machine Learning
시그니처, 패턴 기반의 봇 탐지	가벼운 자바스크립트 사용하여 헤드리스 브라우저, 정상 브라우저 유무 파악	사이트별 트래픽 프로파일링 하여 베이스라인을 만들고 기계학습을 통해 이상 패턴 감지	Cloudflare 모든 고객에서 수집되는 봇 트래픽 정보를 활용하여 지속적인 기계학습을 통해 봇 트래픽 스코어링

CLOUDFLARE

CAPTCHA 없는 세상

관리형 챌린지

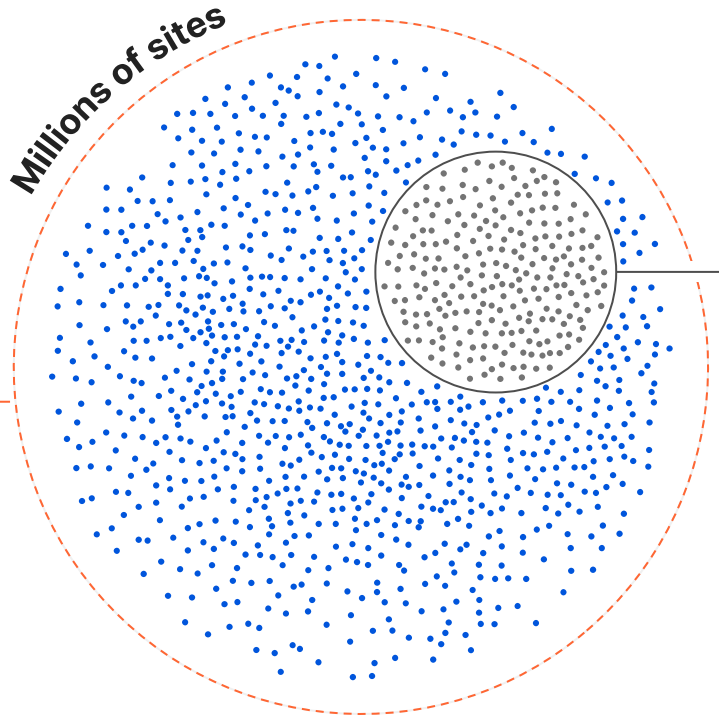
Private Access Tokens



JavaScript 챌린지

Workers 대체 컨텐츠 서빙

Cloudflare 봇탐지 장점 - 전체 트래픽에 대해 봇 탐지

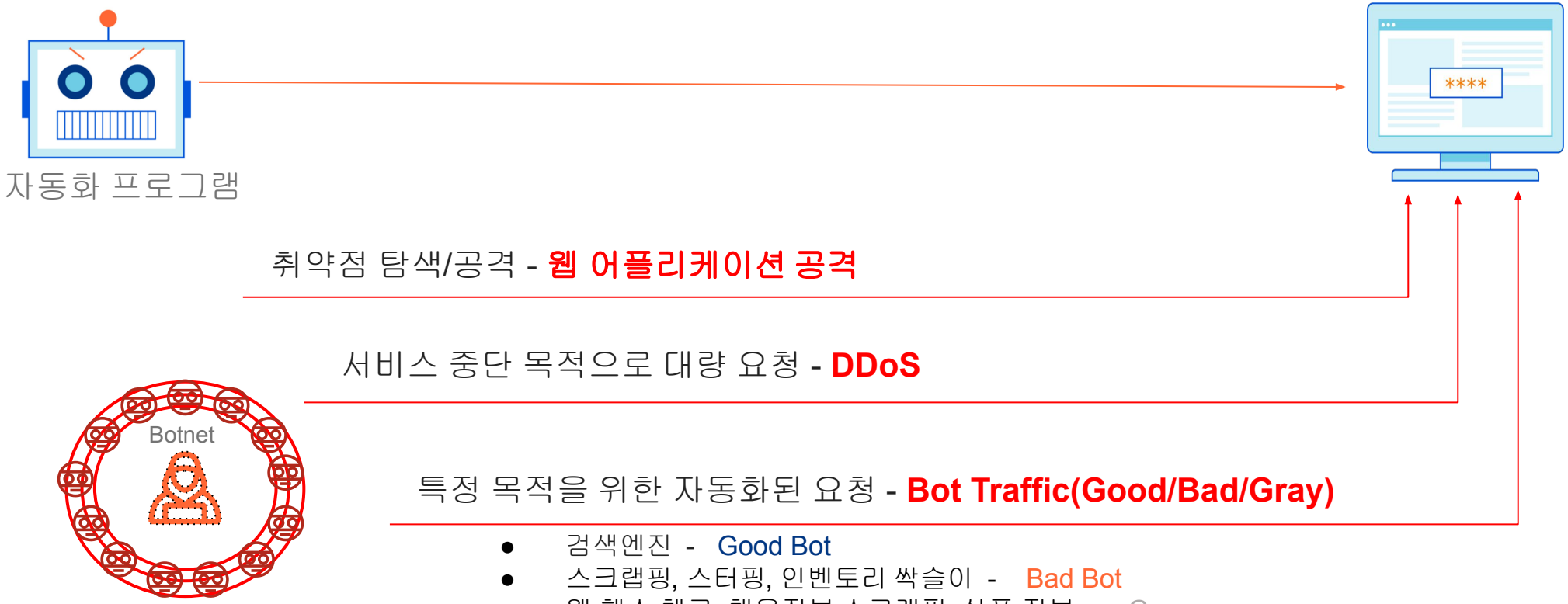


봇 관리 서비스
가입 고객

Cloudflare 차별점

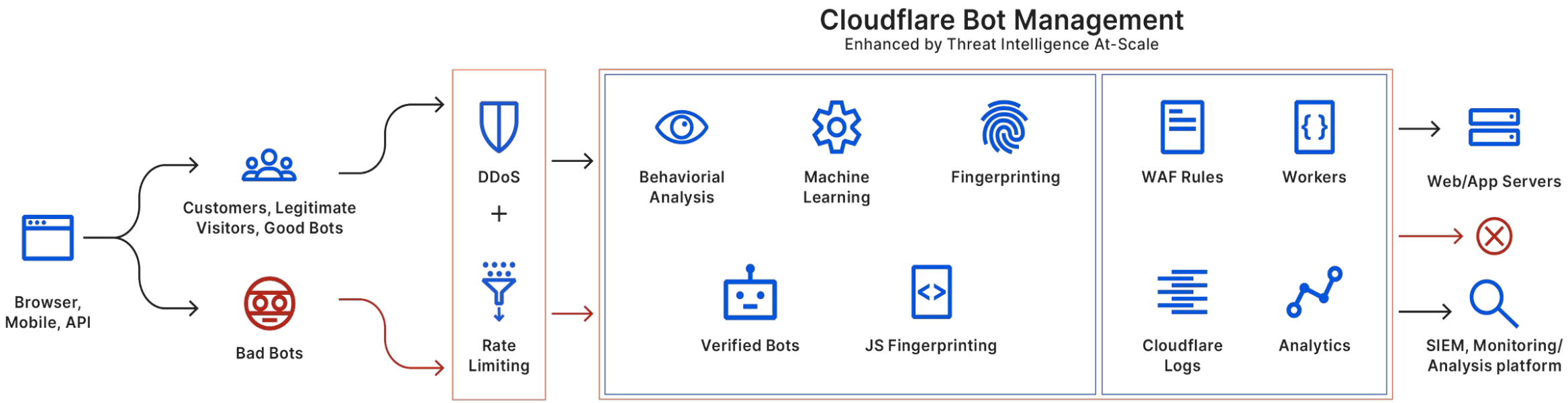
봇 관리 가입 고객뿐 아니라 무료/유료 고객
포함 모든 고객에 대해 봇 데이터 확보 및 학습

자동화된 트래픽 이해


자동화 프로그램
****
취약점 탐색/공격 - 웹 어플리케이션 공격
서비스 중단 목적으로 대량 요청 - DDoS
Botnet
특정 목적을 위한 자동화된 요청 - Bot Traffic(Good/Bad/Gray)
검색엔진 - Good Bot
스크랩핑, 스터핑, 인벤토리 싹슬이 - Bad Bot
웹 헬스 체크, 채용정보 스크래핑, 상품 정보 - Gray Bot

CLOUDFLARE

단일 플랫폼에서 통합 보안 서비스 및 WAF 서비스와 통합



보안 인텔리전스

초당 46백만건(평균), 64백만건(피크) http 요청 처리

초당 26백만(평균) 일간 2.2조(평균) DNS 조회 건 처리

2.5 Tbps 디도스 공격 방어('22년 3분기)
초당 71백만 https 디도스 공격 방어 ('23년 2월)

일평균 14백억 사이버 위협 차단('23년 2분기)

300+
도시 수(중국 본토를 포함한 100개 이상 국가)

12,500+
Cloudflare연결된 네트워크 수 (모든 주요 ISP, 클라우드 공급자, 기업 포함)

209 Tbps
네트워크 엣지 용량(트래짓, 피어링 및 사설 네트워크 상호 연결로 구성)

~50 ms
전 세계 인터넷 사용자의 95% 왕복지연시간

CLOUDFLARE

감사합니다

www.cloudflare.com – Sign-Up / Free Plan 통해 바로 사용 가능

- **developer.cloudflare.com** - 모든 서비스 문서
- **community.cloudflare.com** - 기술적인 문의 확인 커뮤니티 답변
- **blog.cloudflare.com** - 서비스 특징 및 아키텍처
- **www.cloudflare.com/learning** - 클라우드플레어 교육 컨텐츠
- **radar.cloudflare.com** - 디도스 분기별 보고서, 보안 및 인터넷 통계 제공