CLOUDFLARE

Cloudflare가 제안하는 AI로 금융 데이터 보안 강화

홍순권 고객 대표
Cloudflare

AI 시대의 보안 구현?

AI 기반 위협 탐지와 대응

- 머신러닝과 딥러닝을 활용해 비정상적인 트래픽, 행동 패턴, 데이터 이상치를 실시간으로 분석

제로 트러스트 아키텍처

- AI는 사용자의 신원 및 접근 요청을 지속적으로 평가, 내부 네트워크에서도 철저히 검증된 사용자와 장치만이 접근 보장

예측 보안 (Predictive Security)

- 과거 데이터를 학습, 사이버 공격을 예측하고 사전에 방어책 마련.
- DDoS, 랜섬웨어 등 다양한 공격 유형에 대해 빠르게 경고를 제공하고, 자동화된 대응으로 피해를 최소화

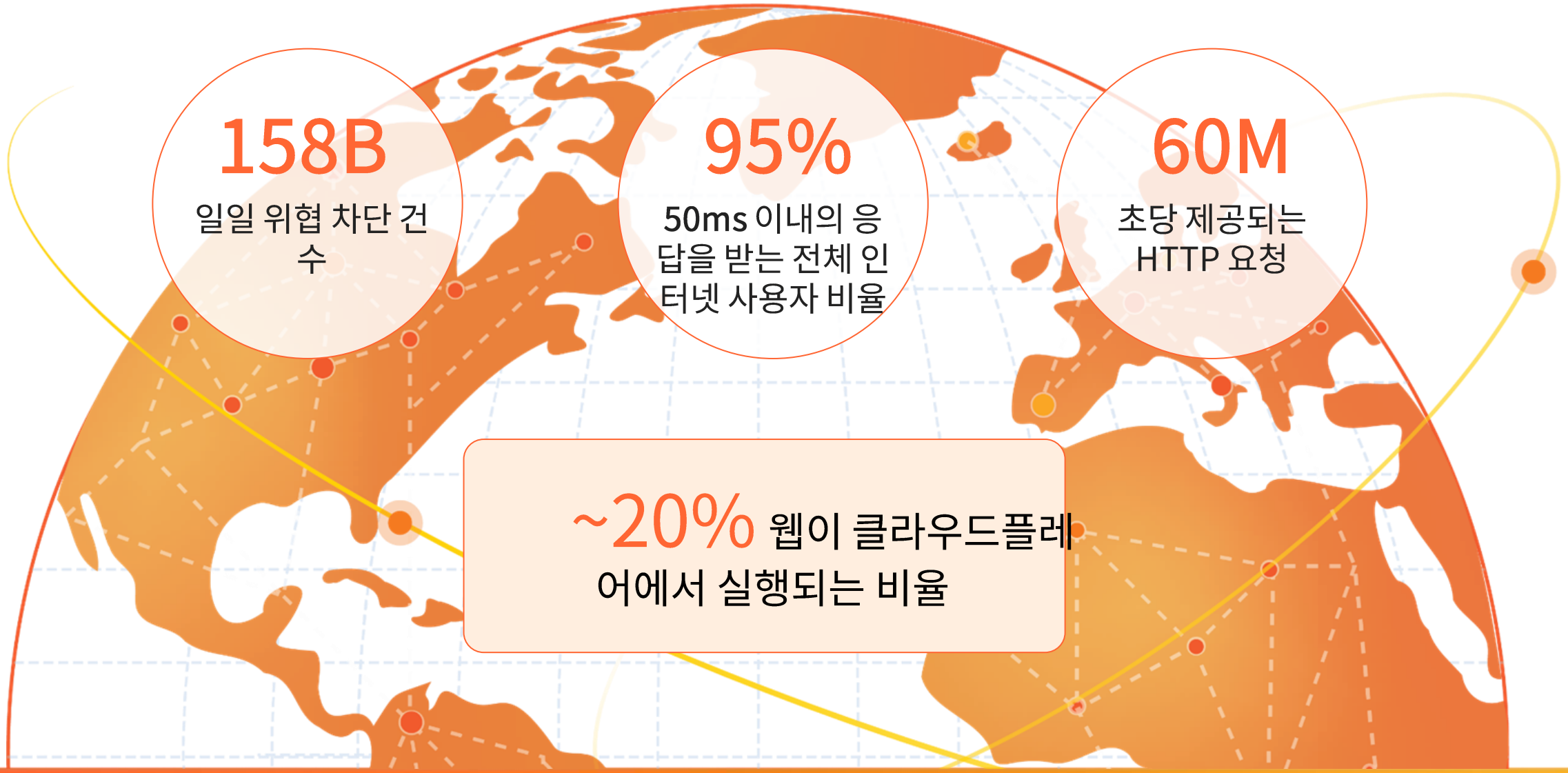
자율 방어 시스템

- AI는 보안 운영센터(SOC)의 일부 역할을 자동화하여, 즉각적인 위협 분석 및 방어를 실행합니다. 이를 통해 수동으로 대응하기 어려운 대규모 공격에도 빠르게 대처할 수 있습니다.

AI로 강화된 인증 및 암호화

- 생체인식, 행동 분석, 암호화 키 관리를 AI로 지원

우리가 목격한 대규모 위협



CLOUDFLARE

글로벌 네트워크 전반에 걸쳐 공유된 인텔리전스는 위협에 대한 포괄적인 보호를 제공합니다.

글로벌 네트워크

수백만 명의 고객과 330개 이상의 지역에서 원격으로 측정

차단

격리

로그

<500ms 업데이트

위협의 타입

위협이 피해를 입히기 전에 차단

- 웹 공격
- 제로 데이
- 피싱 공격
- 악성코드
- 악성 URLs
- DDoS

보호를 위한 클라우드플레어 전반에 걸친 보안

사람
Secure Web Gateway
Cloud Email Security
Browser Isolation

애플리케이션
Web Application Firewall
Bot Management
L7 DDos Protection

네트워크
Firewall as a Service
L3/L4 DDoS Protection

한국을 포함한 아시아 태평양 지역 14개 시장의 보안 의사 결정자 약 4,000명을 대상으로 설문조사 실시

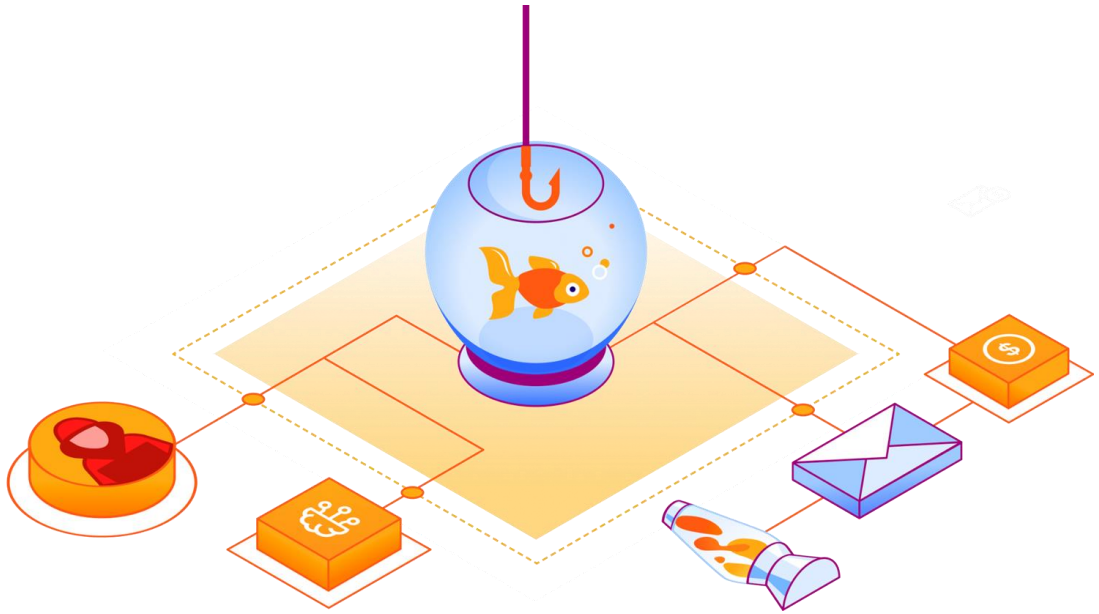
사이버보안 책임을 맡은 일반 관리 및 IT팀

직원의 규모가 250 – 2,500 명 이상인 기업 대상

교육, 금융 서비스, 정부, 의료, 관광, 제조, 미디어 및 통신, 소매 및 IT를 포함한 20개 이상의 산업 분야

사이버 보안 상태를 개선하기 위한 조치를 기반으로 사이버 보안 결과와 영향도에 대한 파악

한국 기업은 증가하는 사이버 보안 사고에 직면해 있습니다.



29%

지난 12개월 동안 한국의 위협 환경은 여전히 불안정했으며, 응답자의 29%가 데이터 유출을 경험했다고 답했습니다.

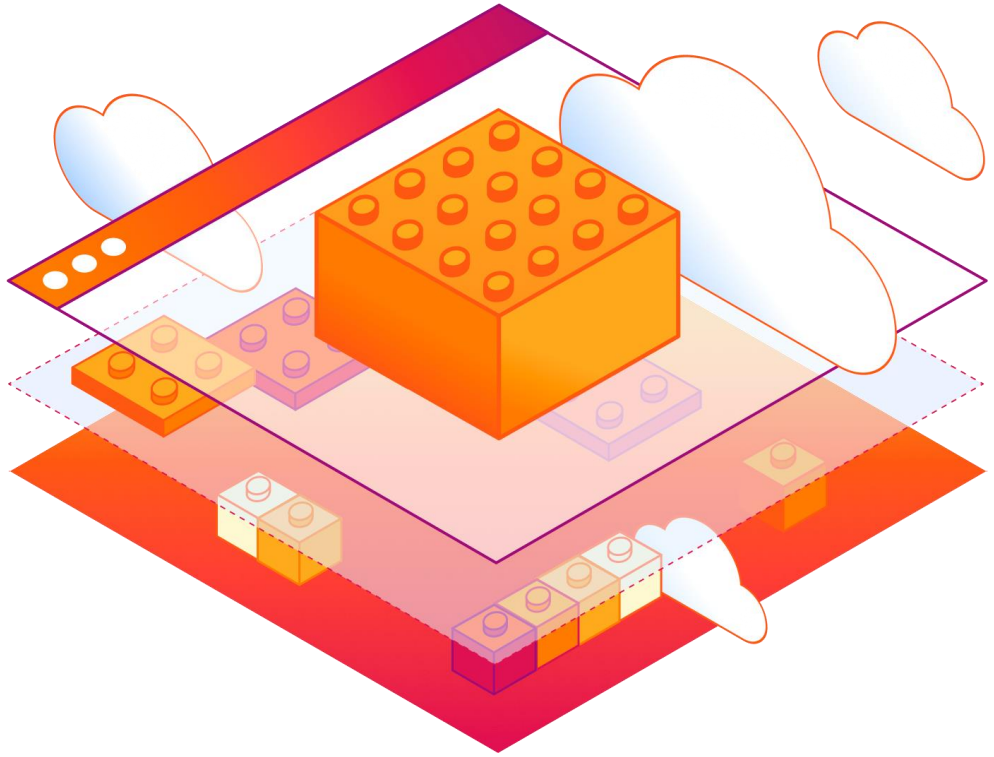
Source: *Cloudflare South korea Cybersecurity Readiness Survey 2024*

한국 기업이 직면한 광범위한 사이버보안 및 IT 문제

한국 보안 담당자의 사이버 보안 우선순위에 대한 비율

Source: *Cloudflare South korea Cybersecurity Readiness Survey 2024*

위협 벡터로서의 AI 가 여기 ~~오고있다~~ 왔다.

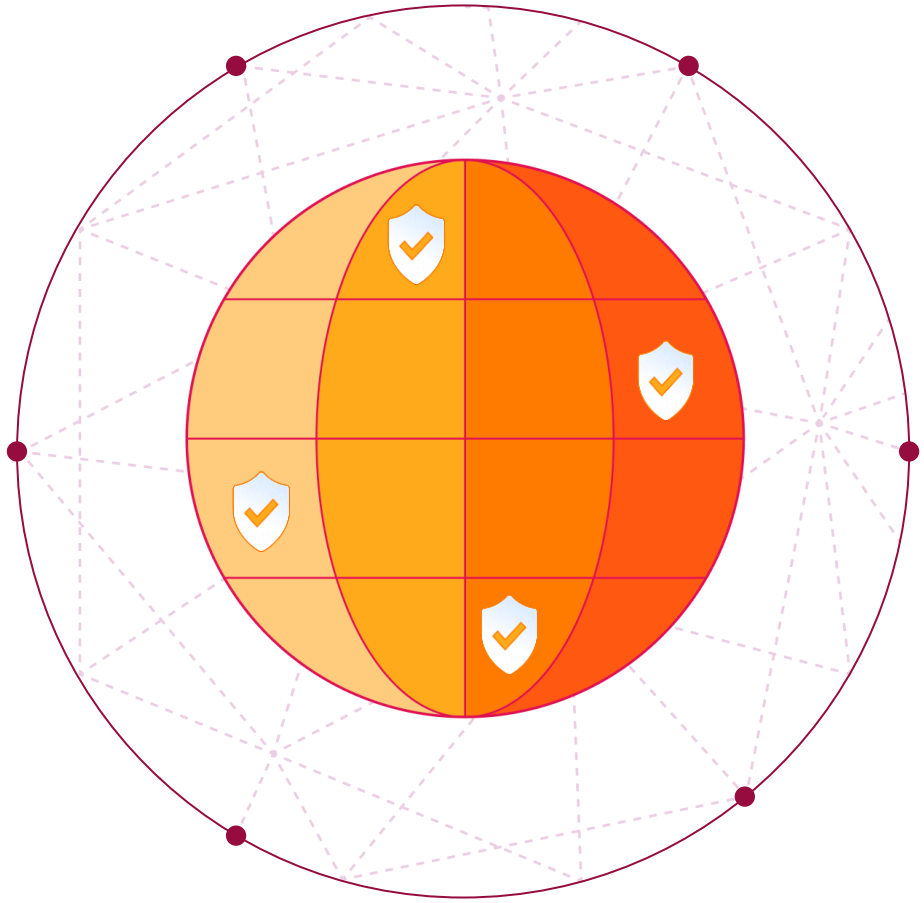


82%

AI 가 점점 더 정교해지고
침해가 심각해지는 것을
우려하는 응답자 비율

Source: *Cloudflare South korea Cybersecurity Readiness Survey 2024*

규정 준수 요구 사항이 증가함에 따라 정밀 조사가 강화



19%

업계 규제 요구 사항
및 인증에 맞춰 일주일
중 10% 이상을 소비

Source: *Cloudflare South korea Cybersecurity Readiness Survey 2024*

경계 기반 보안 모델에서 제로 트러스트 모델로 전환되는 시점

33%

33%

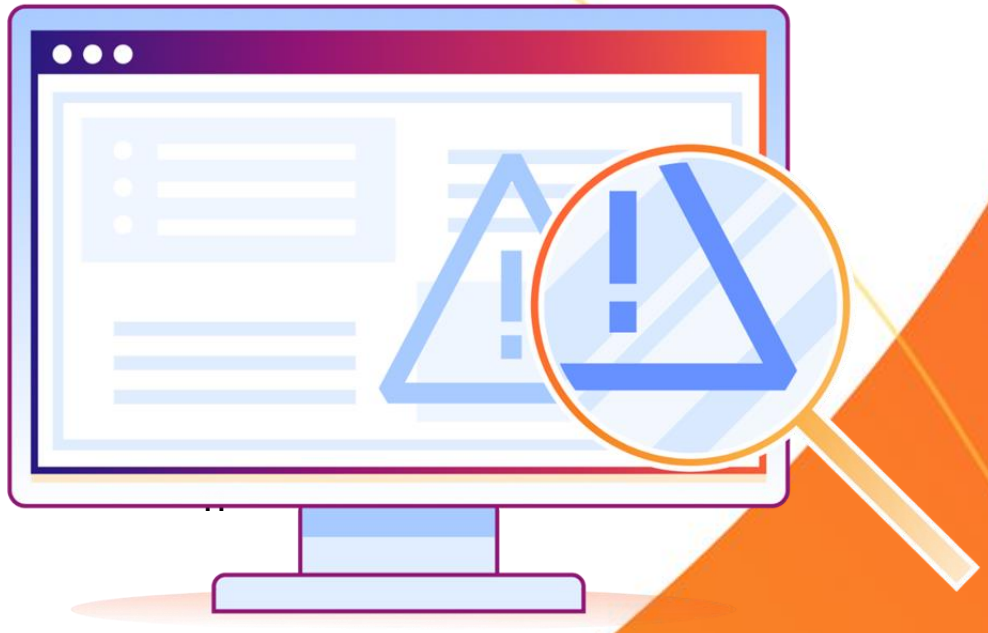
현재 제로 트러스트에 투자하고 있다고 밝혔으며, 51% 는 향후 12개월 이내에 투자할 계획이라고 밝혔습니다.

Source: *Cloudflare South korea Cybersecurity Readiness Survey 2024*

랜섬웨어에 대한 우려의 지속적인 증가

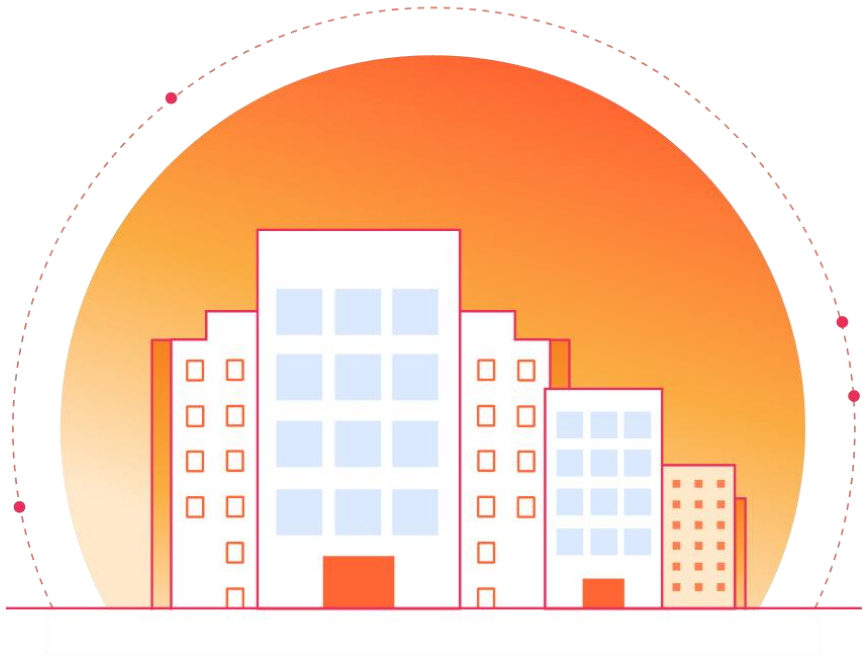
36%

응답자들은 랜섬웨어에 대해 우려하고 있었으며, 공격자는 가장 일반적인 진입 수단으로 웹 애플리케이션이나 서버(52%)의 패치되지 않은 취약점을 악용했습니다.



Source: *Cloudflare South Korea Cybersecurity Readiness Survey 2024*

사이버 보안은 계속해서 IT 지출에 있어 중요한 영역



77%

77%

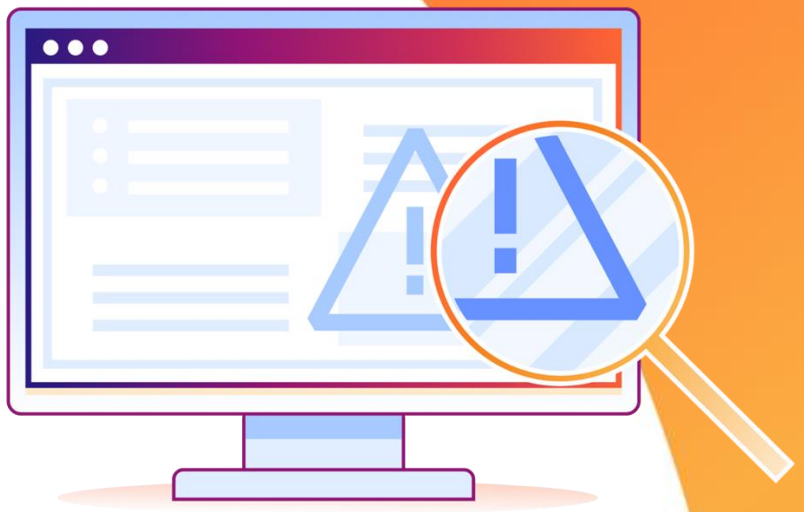
응답자들은 전체 IT 예산의

10%이상 이 사이버 보안에 쓰였다고 응답함

Source: *Cloudflare South korea Cybersecurity Readiness Survey 2024*

69%

데이터 유출을 방어할 준비가 되어 있다고 생각하는 비율



(Source: South Korea Cybersecurity Readiness Survey)

올바른 팀을 구성하는 것은 쉽지 않습니다.

35%

35%

의 응답자는 사이버 보안 준비를 강화하는 데 장애가 되는 요인으로 “인재 부족"을 꼽습니다.

Source: *Cloudflare South korea Cybersecurity Readiness Survey 2024*

클라우드플레어의 권장사항

Survey 결과, 고객 CISO를 위한 6가지 권장 사항

- 복잡성을 줄이기 위한 솔루션 간소화
- Chain에서 가장 약한 고리를 강화
- 랜섬웨어 공격자의 영향력을 제한, 침해에 대한 계획 수립
- 공격의 증가와 강화를 촉진하는 AI에 대비
- 투자를 자본에서 운영 지출로 전환
- 보안 로그를 좀 더 자세히 모니터링하는 습관

Source: *Cloudflare South korea Cybersecurity Readiness Survey 2024*

아시아태평양 지역의 다른 국가들과 한국의 Survey 비교

	한국	아시아태평양
향후 12개월 동안 제로 트러스트에 투자할 가능성이 더 높음	51%	40%
사이버 보안에 조직 IT 예산의 10% 이상을 지출할 가능성이 낮음	77%	84%
규제 요구 사항 및 인증에 보조를 맞추는 데 일주일 중 10% 이상을 소비할 가능성이 적음	19%	48%

Source: *Cloudflare South korea Cybersecurity Readiness Survey 2024*

Cloudflare 소개

Cloudflare at a Glance

CLOUDFLARE

Global company

35%
of Fortune 1000

Millions
of users, with
>2 million developers

Innovation

Founded 2010; IPO 2019
NYSE: **NET,** > $1B+ ARR

>250
patents and growing in Cloud, Security, AI, Networking

>900
companies building AI apps on Cloudflare

Market Leadership

App/API & Network Security and Performance
Developer services
SASE/SSE

Strategic partners: Accenture, Kyndryl

1,300
global channel partners

Cloud Network is our Differentiator

All services at all locations
One of the most interconnected networks with peering to over 12,500 networks.

330+
cities in network; with

~30
in China

120+
countries

160+
AI inference locations

L'ORÉAL BROADCOM GARMIN NCR VOYIX Carrefour JAPAN AIRLINES GPC

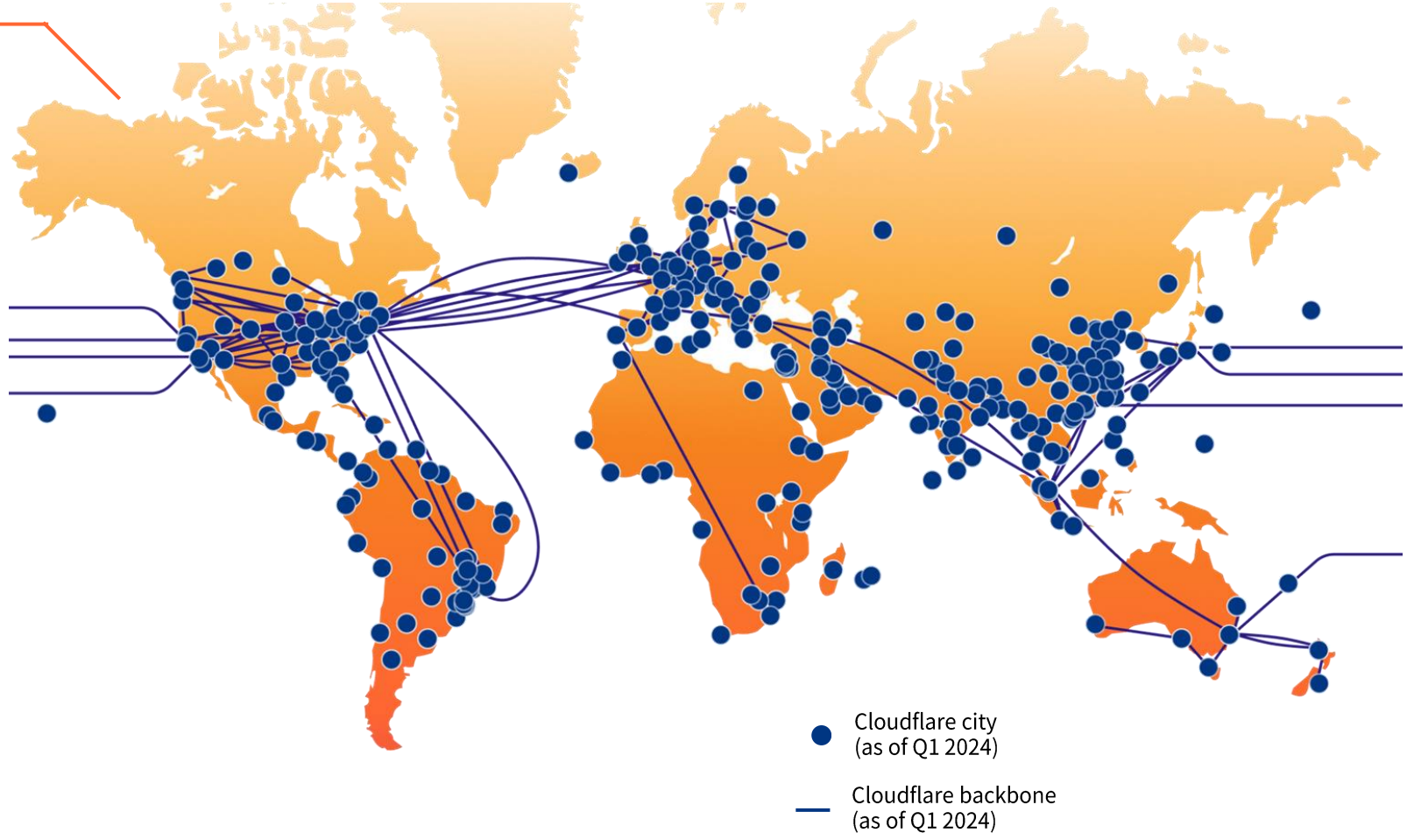
A single network that delivers local capabilities businesses need to accelerate — at scale

330+ cities
in 120+ countries, including mainland China

w/180+ cities
for AI inference powered by GPUs

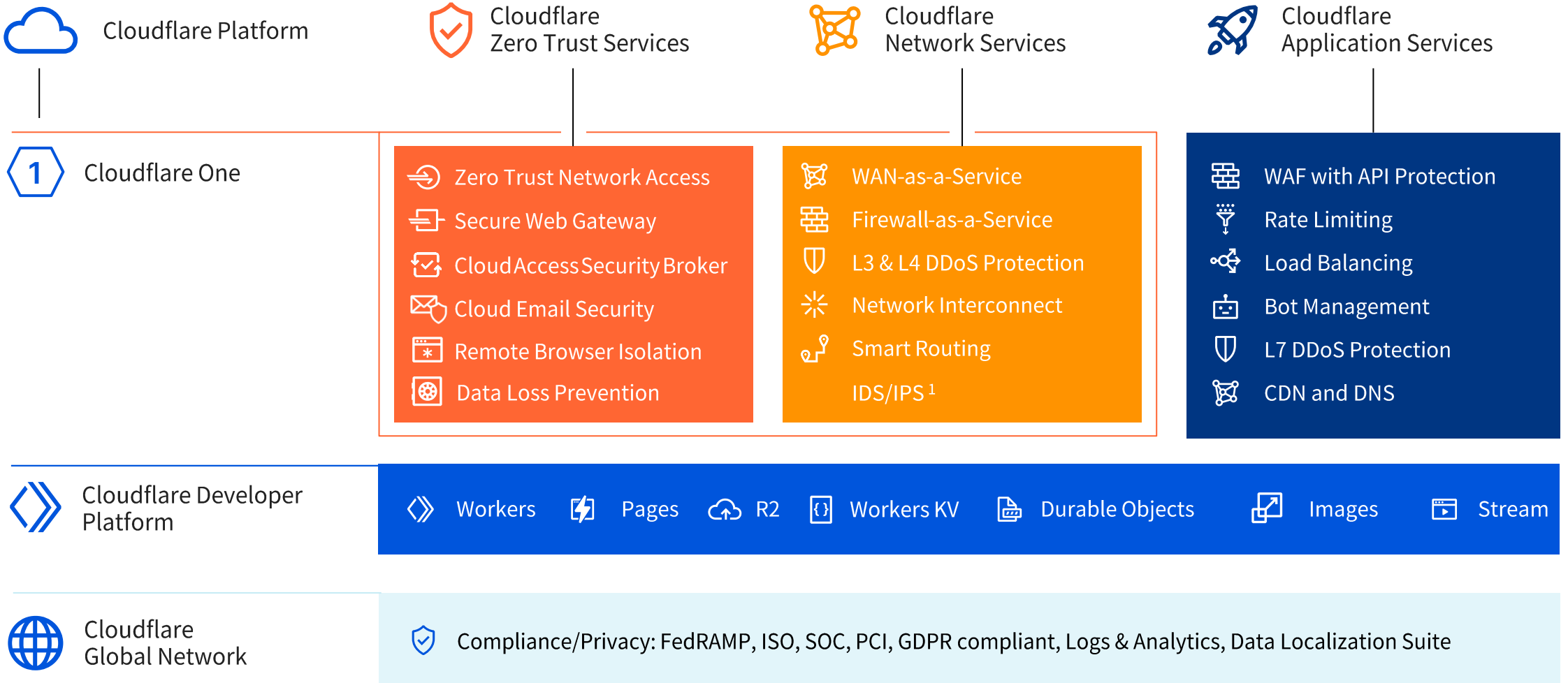
~13,000 networks
directly connect to Cloudflare, including ISPs, cloud providers, and large enterprises

321 Tbps
of network capacity and growing



Cloudflare 솔루션

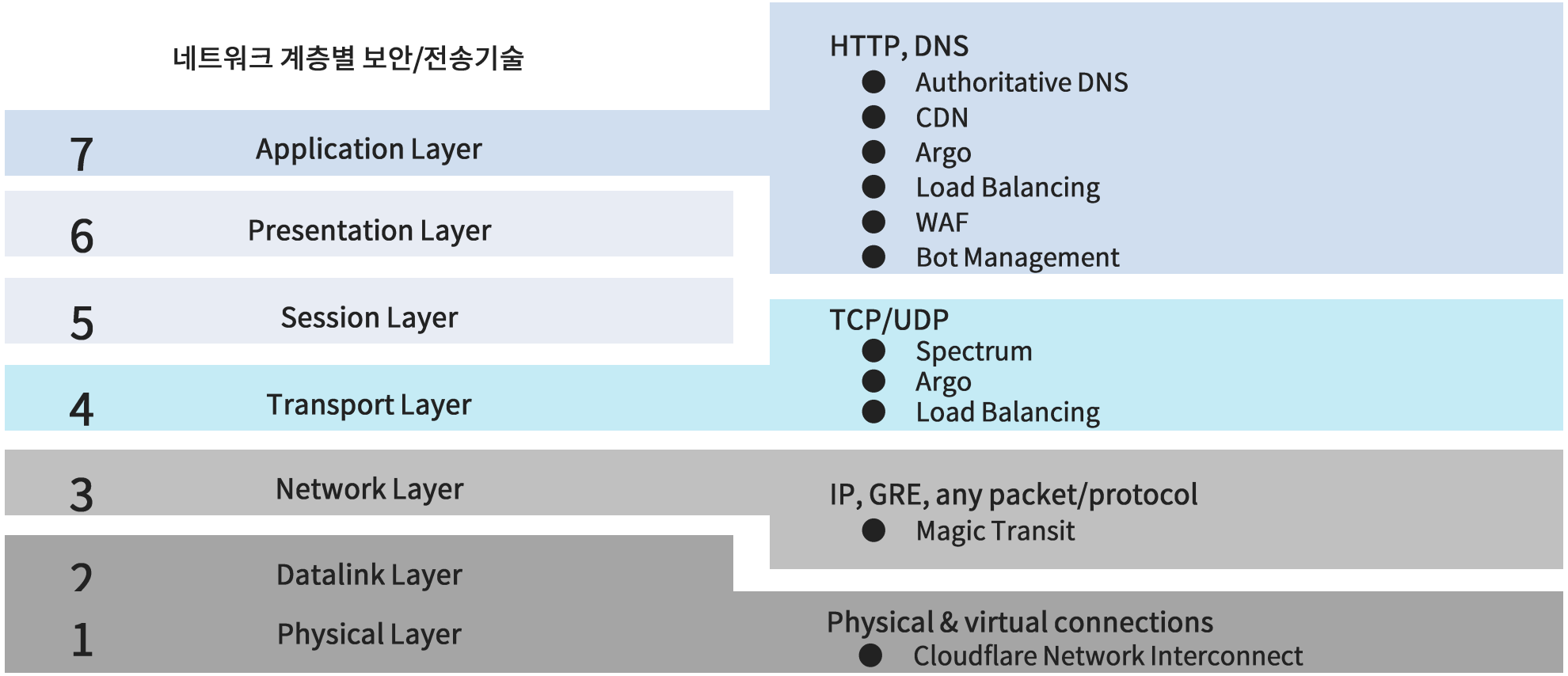
Cloudflare Services Portfolio



Cloudflare Service Introduction

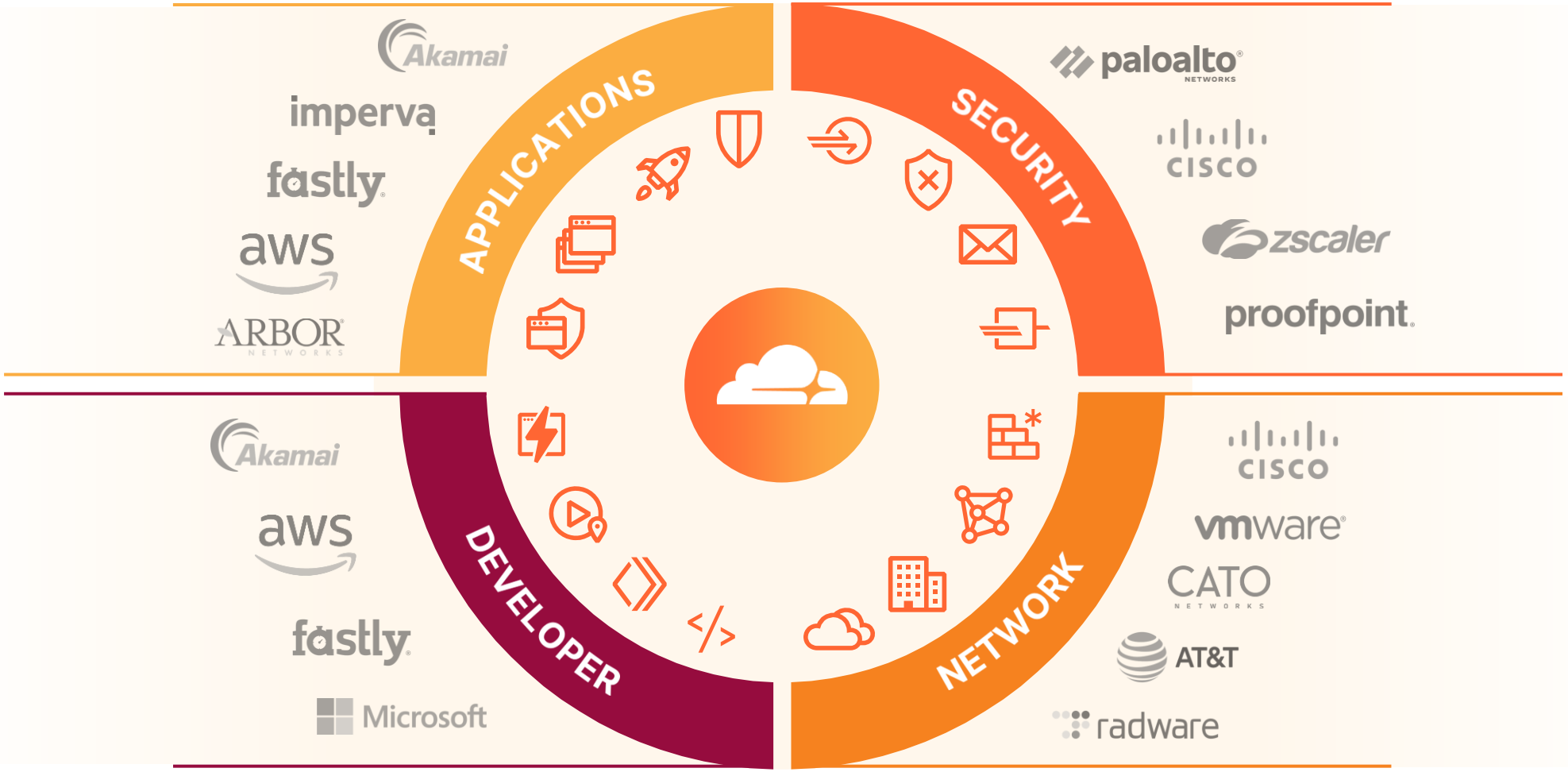
CLOUDFLARE

네트워크 계층별 각기 적용 가능한 보안/전송 솔루션 보유



CLOUDFLARE

Cloudflare fits in everywhere your organization needs



Cloudflare's AI

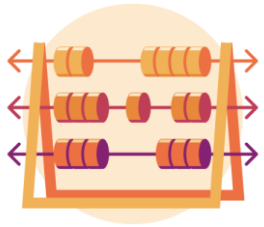
클라우드플레어 AI Product

Workers AI

Serverless inference at a global scale

AI Gateway

Control, monitor, and optimize AI applications



Vectorize

Simple vector storage to power RAG applications

클라우드플레어 AI Product

Workers AI

Serverless inference at a global scale

- 전세계 어디서나 사용자와 가까운 위치에서 AI 추론을 실행할 수 있는 가장 쉬운 플랫폼, 현재 전 세계 180개 이상의 도시에 GPU를 설치, 이러한 GPU 네트워크를 통해 AI 플랫폼 중 가장 큰 글로벌 범위를 보유, 사용자와 최대한 가까운 위치에서 AI 추론을 실행하고 고객 데이터를 더 가까운 곳에 보관할 수 있도록 설계
- 개발자들이 클라우드플레어의 글로벌 네트워크에서 AI 모델을 손쉽게 실행할 수 있도록 지원하는 서버리스 AI 추론 플랫폼
- 서버리스 AI 추론: 개발자는 Workers, Pages, 또는 클라우드플레어 API를 통해 직접 AI 모델을 실행할 수 있으며, 이를 위해 별도의 서버 관리가 필요 없습니다.
- 광범위한 모델 지원: Llama, Stable Diffusion, Mistral 등 최신 AI 모델을 지원하여 다양한 애플리케이션 개발에 활용할 수 있습니다.
- 글로벌 GPU 네트워크: 전 세계 180개 이상의 도시에 GPU를 배치하여, 사용자와 가까운 곳에서 AI 추론을 실행 함으로써 지연 시간을 줄이고 성능을 향상시킵니다.
- 활용 사례:
  - 실시간 데이터 분석: 사용자와 가까운 위치에서 AI 모델 실행, 실시간 데이터 분석, 빠른 의사결정을 지원
  - 개인화된 사용자 경험 제공: 사용자 행동 기반으로 맞춤형 콘텐츠나 추천 제공, 향상된 사용자 경험을 제공
  - 보안 강화: AI를 활용하여 비정상적인 활동을 감지하고, 잠재적인 위협을 신속하게 차단

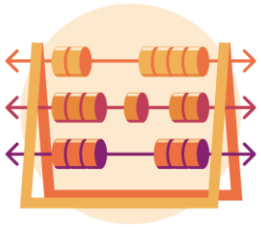
클라우드플레어 AI Product

AI Gateway

Control, monitor, and optimize AI applications

- 클라우드플레어의 **AI 게이트웨이(AI Gateway)**는 AI 애플리케이션의 안정성, 관찰 가능성, 확장성을 높이기 위해 설계된 플랫폼입니다. 이 게이트웨이는 애플리케이션과 AI API(예: OpenAI) 사이에 위치하여 다양한 기능을 제공합니다.
- 주요 기능
  - 응답 캐싱: 자주 사용되는 응답을 저장하여 반복적인 요청 시 원본 API 호출을 줄이고, 응답 속도 향상
  - 요청 속도 제한(Rate Limiting): 과도한 요청을 방지하여 시스템의 안정성을 유지하고, 비용을 관리
  - 요청 재시도 및 모델 폴백(Fallback): 요청 실패 시 자동으로 재시도하거나, 사전에 정의된 대체 모델로 요청을 전환하여 서비스의 연속성을 보장합
  - 사용량 모니터링 및 분석: 프롬프트, AI API 호출, 오류, 토큰 사용량, 비용 등에 대한 가시성을 확보하여 애플리케이션의 성능을 분석하고 최적화할 수 있습니다.
- 주요 특징:
  - 간편한 통합: 코드 한 줄만으로 AI 게이트웨이에 애플리케이션을 연결할 수 있어, 개발자는 빌드에 집중할 수 있습니다.
  - 다양한 AI 공급자 지원: OpenAI, Hugging Face, Anthropic 등 주요 AI 공급자와의 통합을 지원하여, AI 애플리케이션에 대한 포괄적인 가시성을 제공합니다.
  - AI 게이트웨이는 이러한 기능들을 통해 AI 애플리케이션의 안정성, 확장성, 생산성을 보장하며, 개발자가 효율적으로 AI 애플리케이션을 구축하고 관리할 수 있도록 지원합니다.

클라우드플레어 AI Product



Vectorize

Simple vector storage to power RAG applications

- 클라우드플레어의 Vectorize는 전 세계적으로 분산된 벡터 데이터베이스로, 개발자들이 AI 기반 애플리케이션을 효율적으로 구축하고 운영할 수 있도록 지원합니다. 이를 통해 시맨틱 검색, 추천, 분류, 이상 감지 등 다양한 머신러닝 작업을 수행할 수 있으며, 대규모 언어 모델(LLM)에도 컨텍스트를 제공할 수 있습니다.
- 주요 기능
  - 임베딩 저장 및 검색: 텍스트, 이미지, 오디오 등 다양한 데이터의 임베딩을 저장하고, 유사도 검색을 통해 관련 정보를 빠르게 찾을 수 있습니다.
  - 글로벌 분산 아키텍처: 클라우드플레어의 전 세계 네트워크를 활용하여 낮은 지연 시간과 높은 가용성을 제공
  - 다양한 데이터 소스 통합: Workers KV, R2, D1 등과 통합되어 다양한 데이터 소스의 임베딩을 관리할 수 있습니다.
- 활용 사례:
  - 시맨틱 검색: 사용자 쿼리와 유사한 콘텐츠를 빠르게 찾아 정확한 검색 결과를 제공합니다
  - 추천 시스템: 사용자 선호도에 기반한 맞춤형 추천을 통해 개인화된 경험을 제공합니다.
  - 이상 감지: 비정상적인 패턴이나 활동을 신속하게 식별하여 보안 및 운영 효율성을 향상시킵니다.
  - Vectorize는 클라우드플레어의 Workers AI와 함께 사용하여 AI 애플리케이션의 성능을 극대화할 수 있으며, 개발자들은 별도의 인프라 관리 없이도 강력한 AI 기능을 구현할 수 있습니다.

클라우드플레어 AI 활용 원칙

- 내부 직원과 외부 고객이 AI의 혁신적인 잠재력을 책임감 있게 활용할 수 있도록 지원
- 우리는 AI 시스템의 안전성, 신뢰성, 견고성에 대한 우 의 헌신을 강조하는 명확한 원칙을 설정
- 머신러닝("ML")과 생성형 AI("GenAI") 관련 모든 프 젝트에 적용되어야 합니다.

=> 내부 IT, 마케팅, 법무팀, 연구개발팀, Support 대부분의 내부 팀이 참여하는 AI Community 를 통해 명확한 가이드와 원칙 하에 AI 시스템을 활용

AI Audit

CLOUDFLARE

폭발적인 AI 서비스의 증가

ChatGPT had 1 million users within the first five days of being available

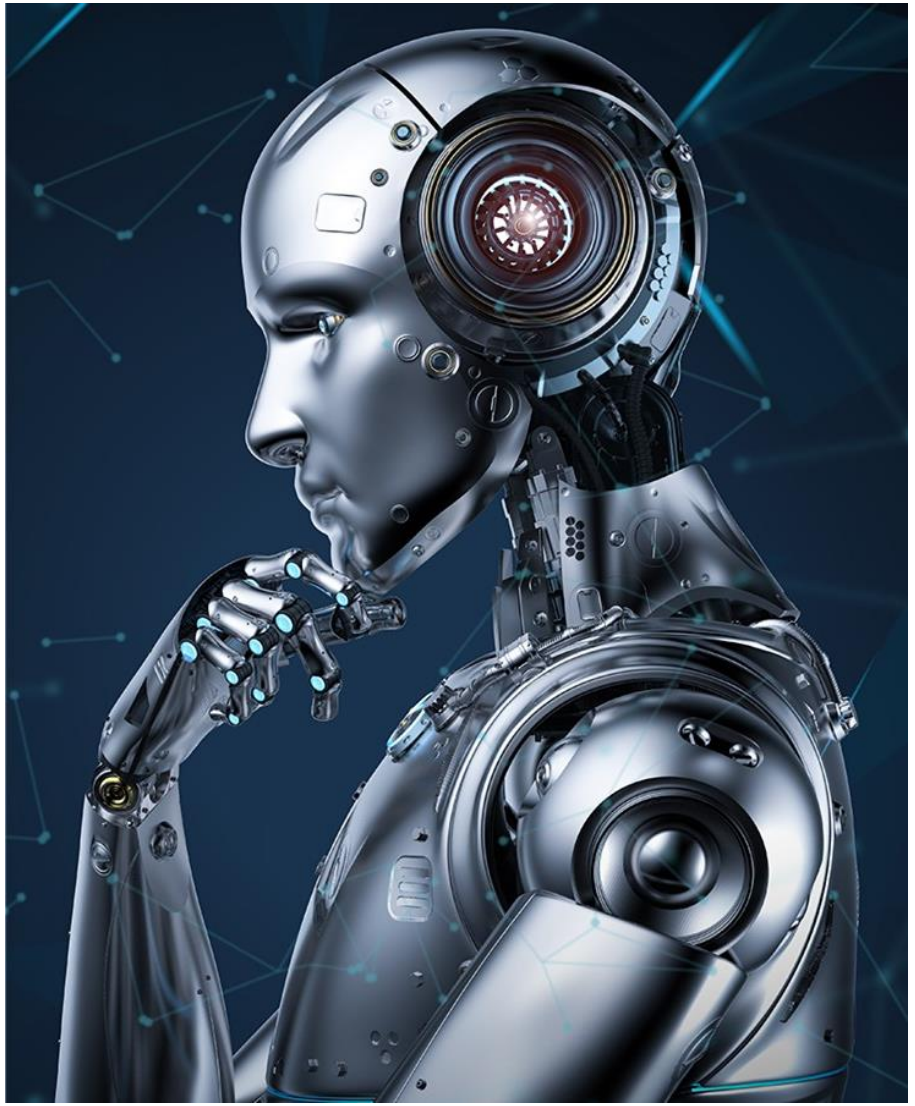
ChatGPT's remarkable adoption rate is evident as it garnered 1 million users within the first five days of its release.[2]

97% of business owners believe ChatGPT will help their business

According to Forbes Advisor, a staggering 97% of business owners believe that ChatGPT will benefit their businesses. One in three businesses plan to use ChatGPT to create website content, while 44% aim to generate content in multiple languages.[3]

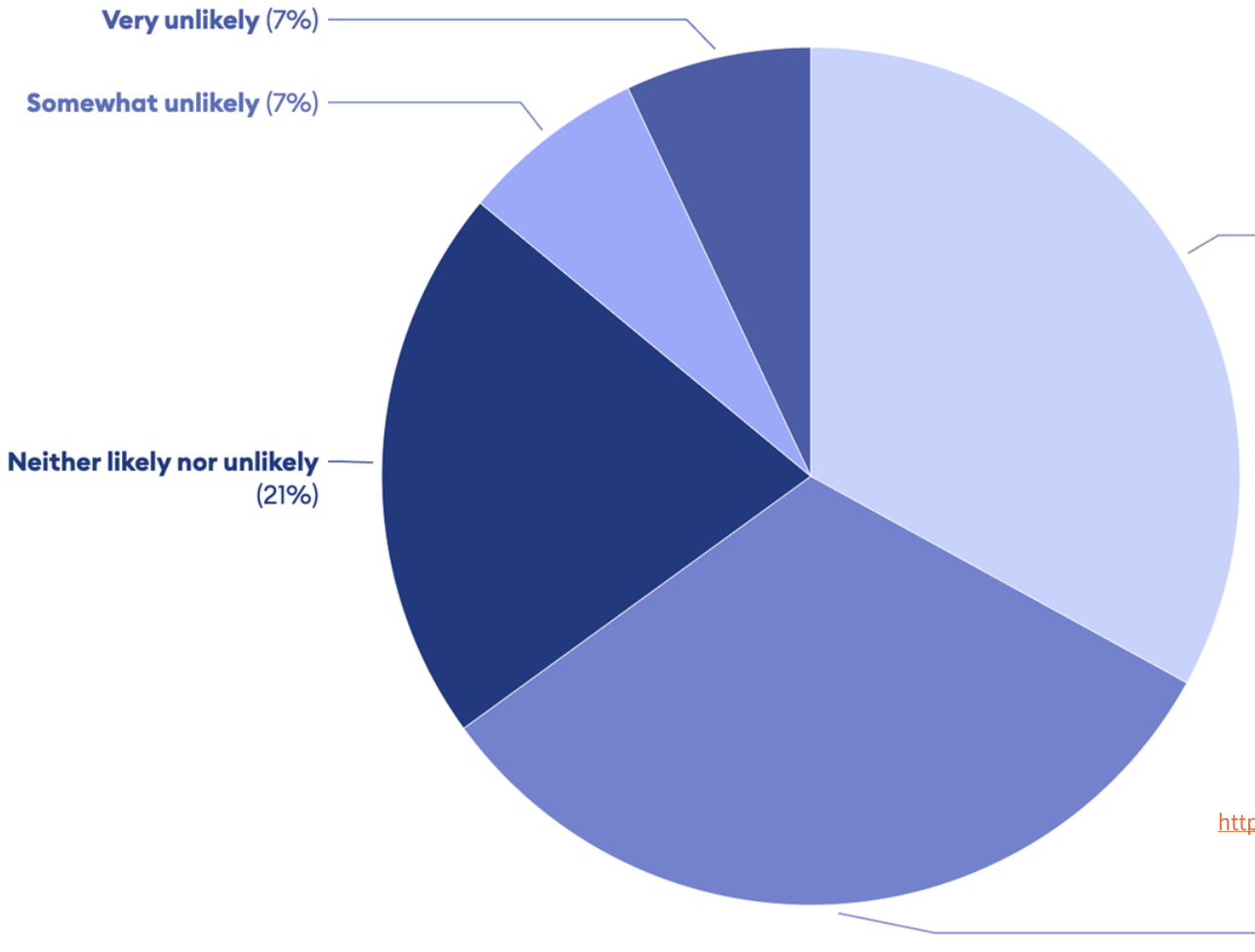
64% of businesses expect AI to increase productivity

A significant 64% of businesses believe that artificial intelligence will help increase their overall productivity, as revealed in a Forbes Advisor survey. This demonstrates the growing confidence in AI's potential to transform business operations. [3]



CLOUDFLARE

How likely are you to trust a business that uses artificial intelligence?



사용자가 AI를 비즈니스에 활용되는것을 자연스럽게 받아드리고 있음

65% 긍정적

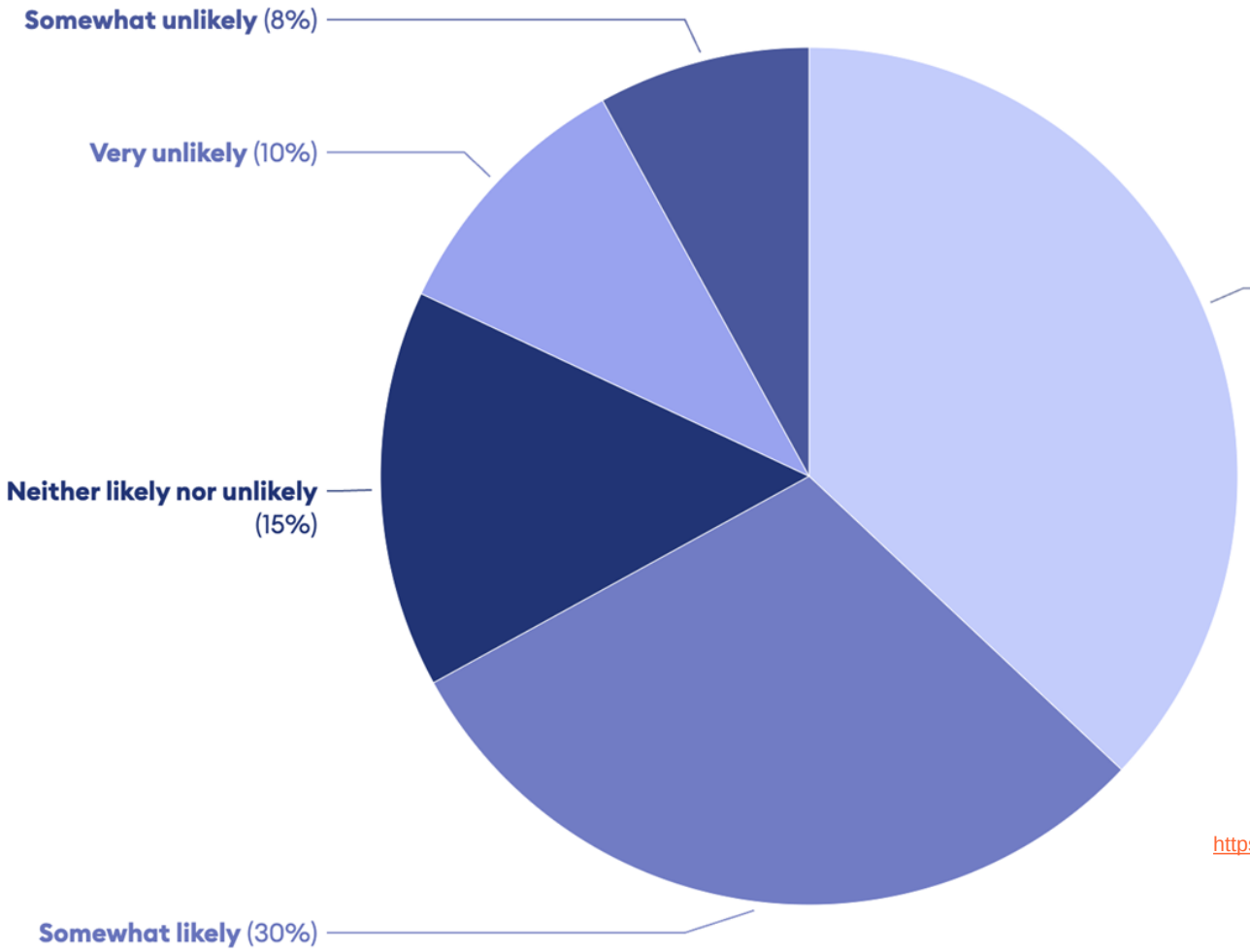
https://www.forbes.com/advisor/business/ai-statistics/

Source: Forbes Advisor • Embed

Forbes ADVISOR

CLOUDFLARE

Would you use ChatGPT instead of Google?



Source: Forbes Advisor • Embed

Forbes ADVISOR

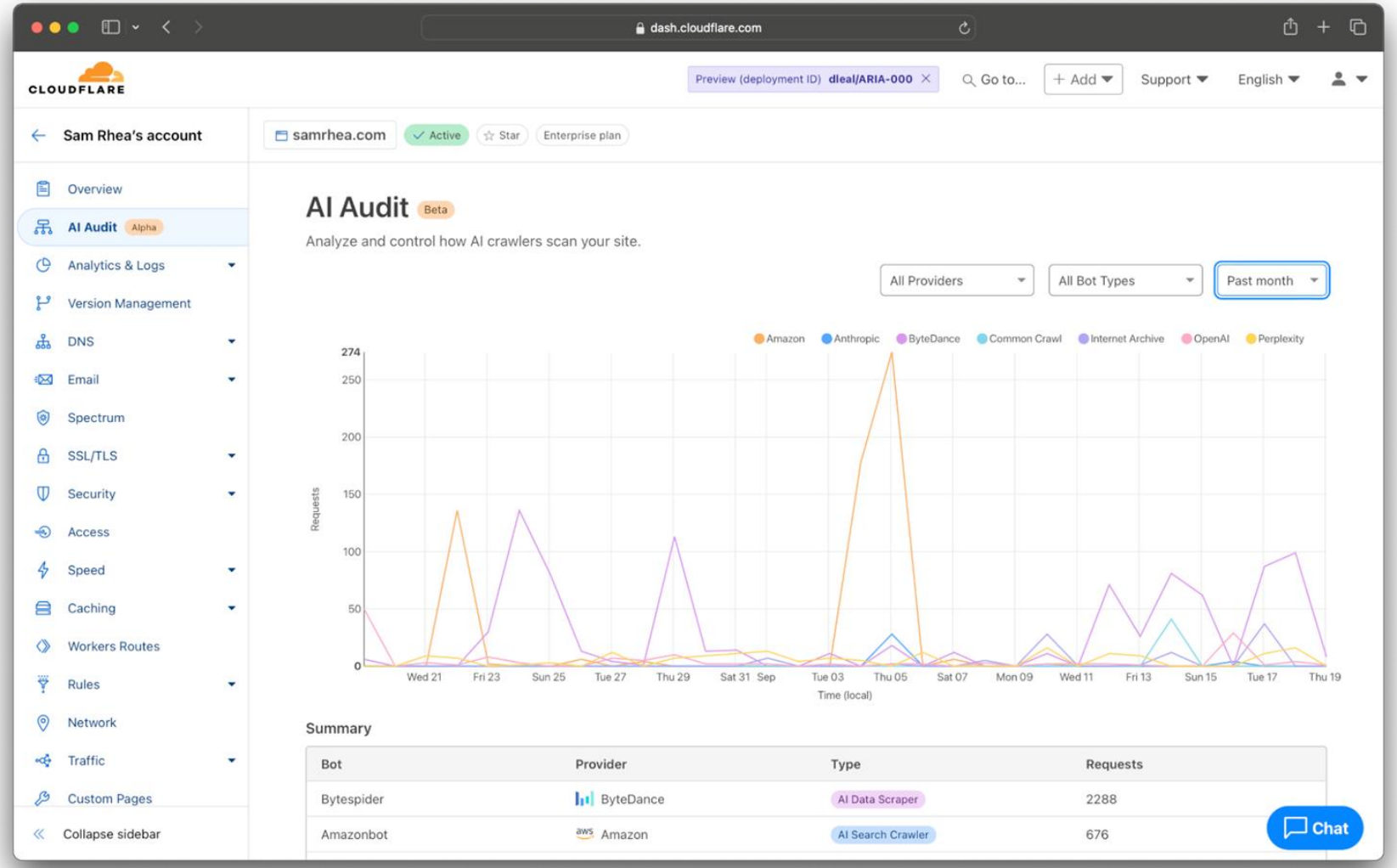
AI model이 검색엔진을 대체하고 있음

67% 긍정적

https://www.forbes.com/advisor/business/ai-statistics/

CLOUDFLARE

증가하는 AI crawling bot과 문제점

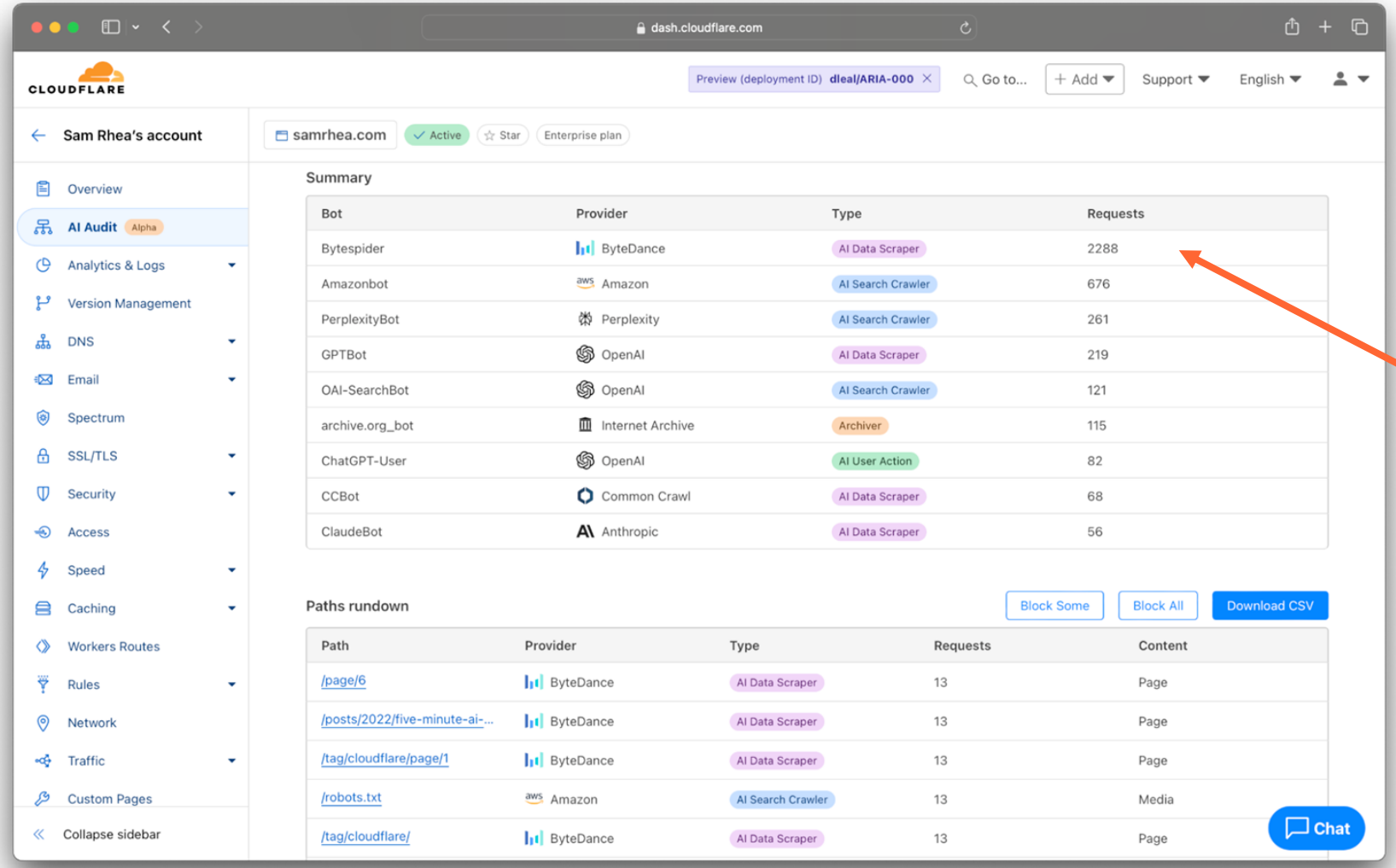


AI 삯없읙 밝젅곽 합껙
긱학귮숙젂윽록 즞각학늕 AI crawling bot곽 trafflc

Content 샞삱작엑겍 돍악각직 몼학늕 숙읶

작싡읙 컩텞측각 AI굑윢엑 쓱익늕직 목륵늕 겾욱각 댁북붅

AI crawling의 가시성 확보

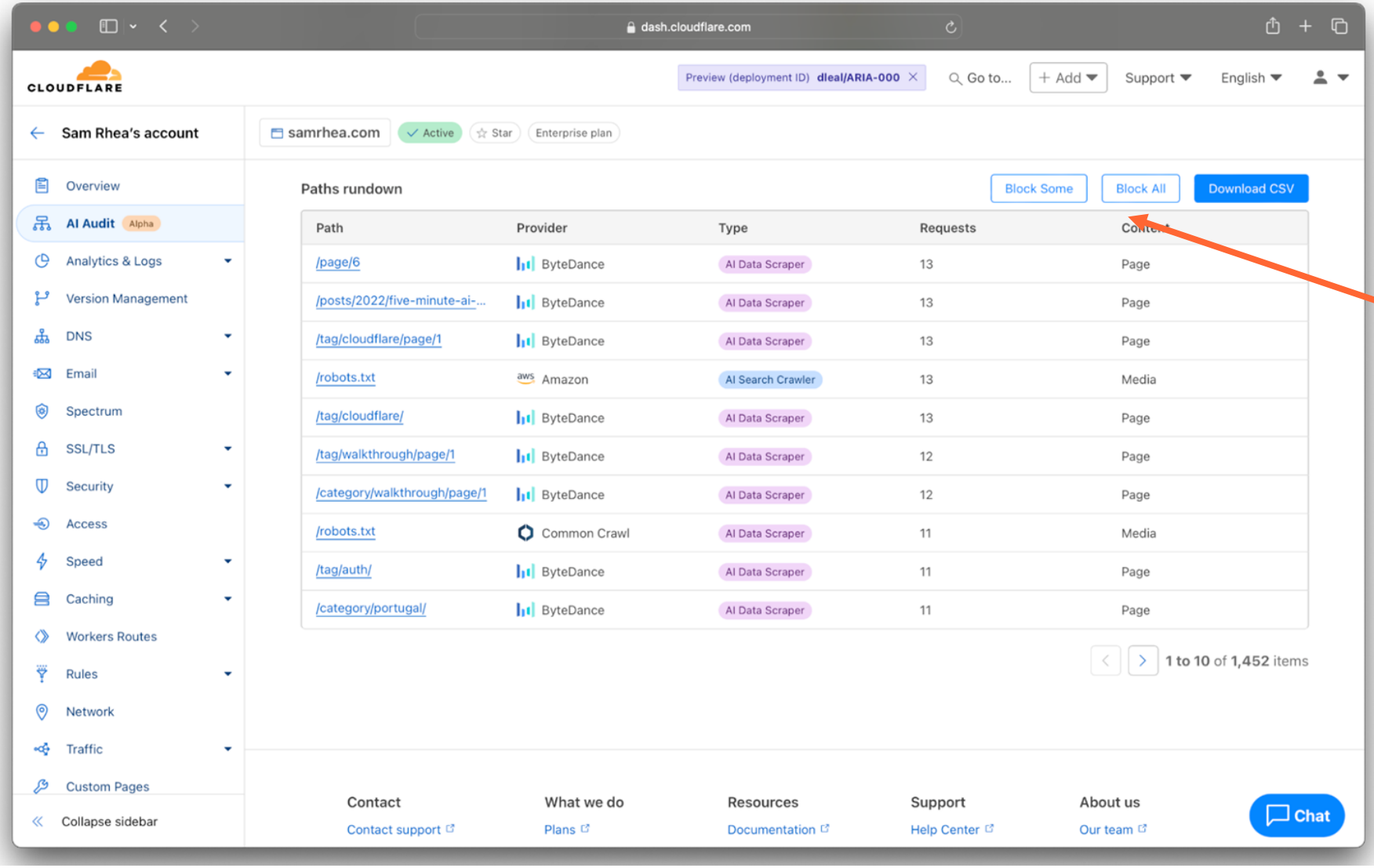


어떤 AI bot이
- 언제
- 어떤 데이터

를 가져갔는지 가시성을 확보할 수 있음

CLOUDFLARE

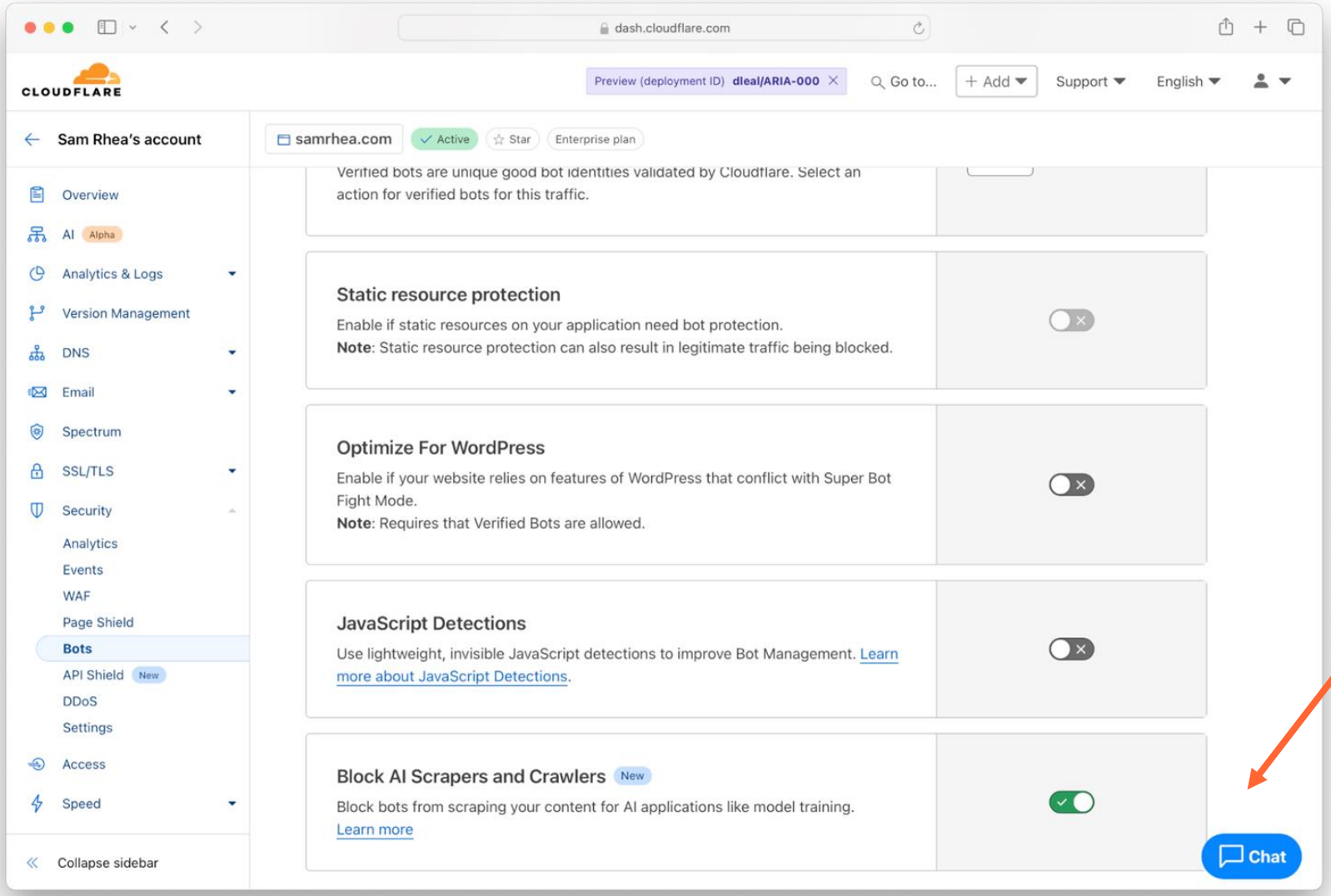
AI crawling의 가시성 확보



데이터를 기반하여 현재의 우리 비즈니스를 분석하고 AI 봇에 대한 대응책을 생각해 볼 수 있음

CLOUDFLARE

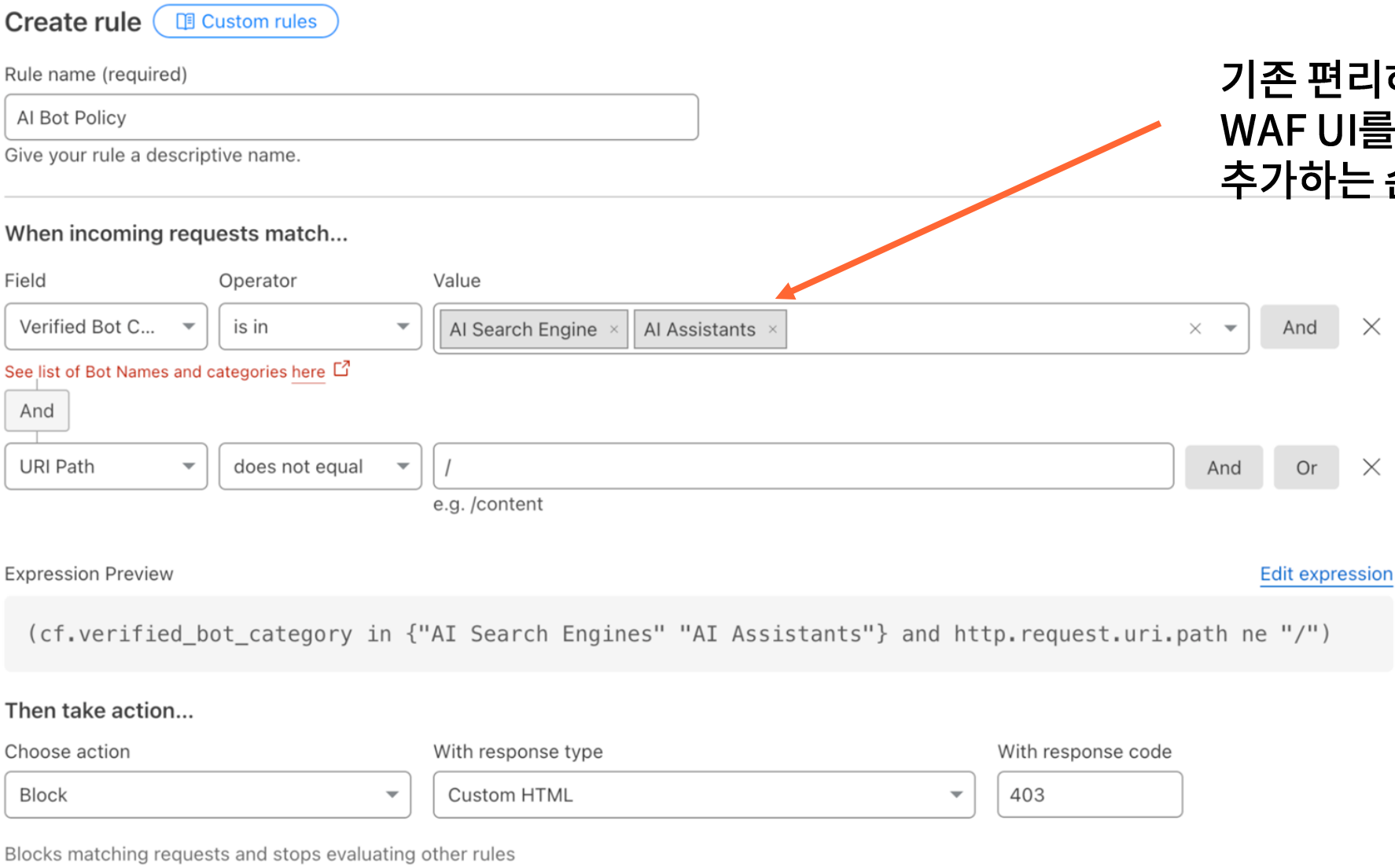
AI crawling 대응



원클릭으로 실행 가능한 간단하면서 쉬운 UI

CLOUDFLARE

AI crawling 대응

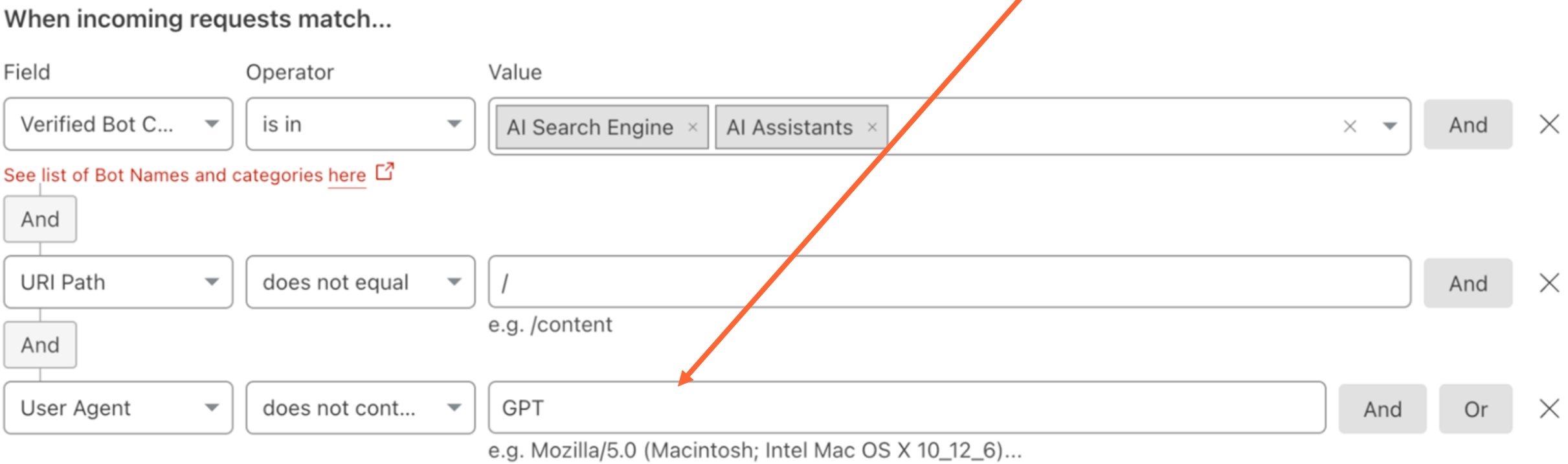


기존 편리하고 쉬운 Cloudflare WAF UI를 그대로 하나의 룰로 추가하는 손쉬운 방어 모드

CLOUDFLARE

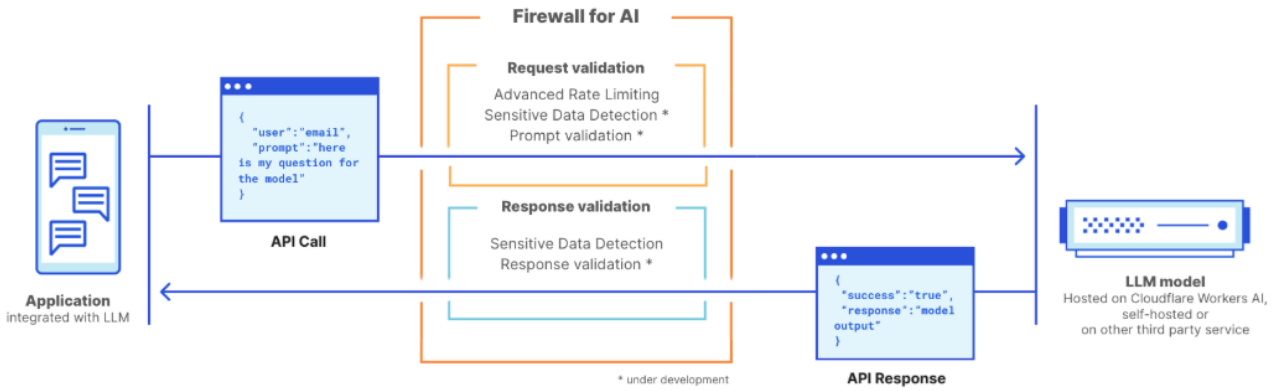
AI crawling 대응

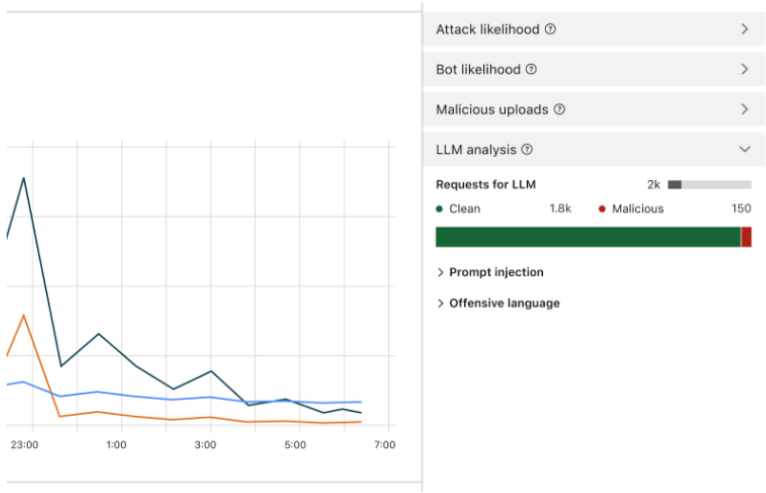
선별적으로 특정 Bot만 통과도 가능



Firewall for AI

Firewall for AI





- 오늘 클라우드플레어는 대형 언어 모델(LLM) 앞에 배치하여 악용 사례를 모델에 도달하기 전에 식별할 수 있는 보호 계층인 "AI용 방화벽 (Firewall for AI)" 출시(Beta Version)
- AI 모델, 특히 LLM이 급증하는 가운데, 고객들은 자체 LLM을 확보하기 위한 최선의 전략이 무엇인지 고민하고 있으며 인터넷에 연결된 앱의 일부로 LLM을 사용하면 악의적인 행위자가 악용할 수 있는 새로운 취약점이 생깁니다.
- 삽입, 데이터 유출 등 기존 웹 및 API 앱에 영향을 미치는 취약점 중 일부는 LLM 세계에도 적용되지만 LLM의 작동 방식 때문에 새로운 위협 등장
- AI용 방화벽은 고급웹 앱 방화벽(WAF)으로, LLM을 사용하는 앱에 특별히 맞춤화, 앱 앞에 배포할 수 있는 도구 세트로 구성되어 취약점을 감지하고 모델 소유자에게 가시성을 제공합니다.
- 이 새로운 검증 방식으로 최종 사용자가 제출한 프롬프트를 분석하여 모델을 악용하여 데이터를 추출하려는 시도 및 기타 악용 시도가 식별되며 AI용 방화벽은 Cloudflare 네트워크의 규모를 활용, 사용자와 최대한 가까운 곳에서 실행되어 공격 조기에 식별, 남용 및 공격으로부터 최종 사용자와 모델을 모두 보호할 수 있음

Cloudflare 소개(Cont'd)

Web Security

Service Introduction - Security

CLOUDFLARE

DDos공격과 기타 웹 위협들이 Origin 서버를 공격하기전에 미리 앞단에서 고객의 웹을 보호

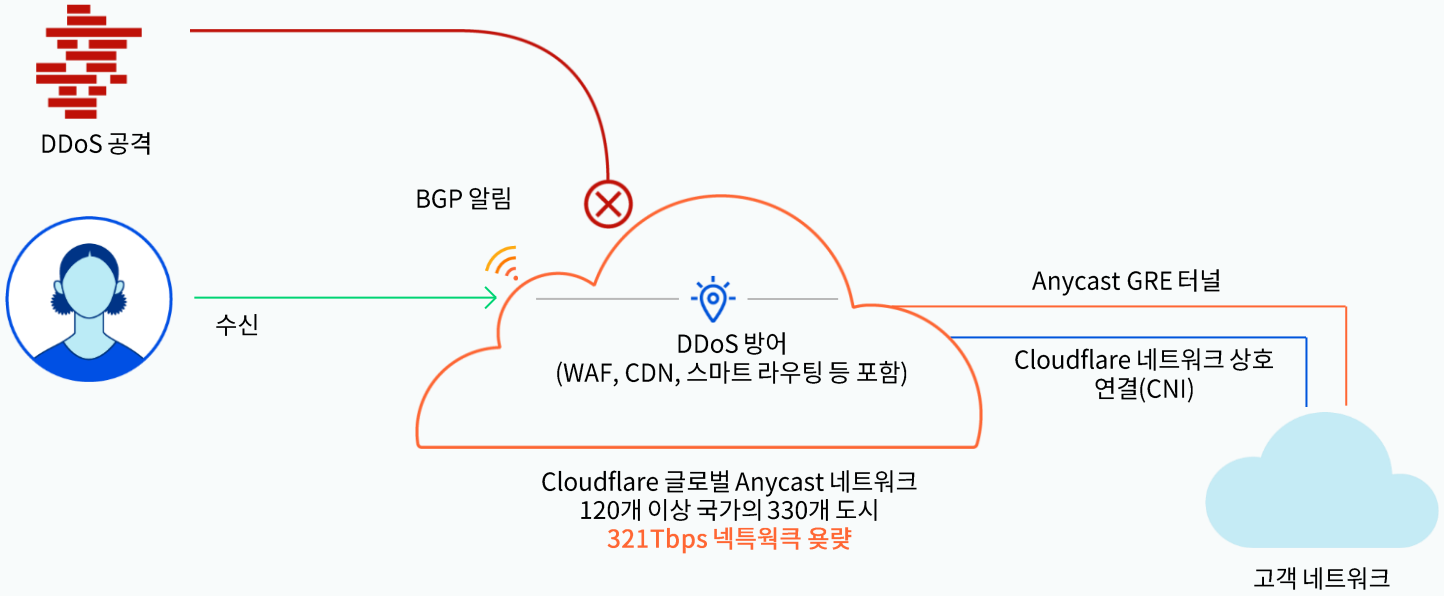
- 향상된 DDos방어 : Cloud flare 각 데이터센터에 장착된 서비스는 UDP및 ICMP 프로토콜, SYN/ACK, DNS증폭, 교묘한 Layer 3,4,7 공격등을 완화할수 있습니다(296Tbps 방어 Capacity)
- Dynamic WAF: Cloudflare의 WAF는 기본적으로 OWASP ModSecurity Core 규칙집합과 Cloudflare 규칙집합을 실행하여 SQL삽입(SQL Injection), XSS(Cross site Scripting), 응용프로그램별 공격(Application Specific Attacks)으로부터 고객을 보호합니다. 또한 고객은 필요로하는 맞춤형 자체 WAF 작성 및 적용이 가능하며 그외 개발자들의 규칙집합들도 추가할수 있습니다.
- Rate Limiting: 특정 IP, Pattern에 대한 일정 기간 접속 중지 등의 기능 수행
- Bot Management: Machine Learning, Fingerprint등 최신 기술을 이용한 효율적인 Bot 공격 차단
- 간편한 SSL 적용 : 자체 기사용중인 SSL 인증을 사용할수도 있고 또는 Cloudflare에서 발급해주는 새로운 SSL인증을 사용할수도 있습니다
- 글로벌 네트워크의 학습효과 : Cloudflare의 네트워크는 2천 6백만개가 넘는 웹사이트를 지원하고 있습니다. 매달 20억개가 넘는 IP에 대한 동적 평판 평가(Dynamic Reputation Scoring)을 제공하는 Cloudflare는 실시간으로 공격을 확인하며, 학습한 내용을 즉시 배포하여 고객을 보호할수 있습니다
- 실시간 Online Report : Cloudflare는 검색엔진 크롤러, 봇(bots) 그리고 나쁜 평판을 가진 방문자들이 고객 웹사이트에 접속하는 것을 중지시키고 이에 대한 상세를 정보를 제공합니다.

CLOUDFLARE

DDoS 방어

Layer 3 방어-Magic Transit

DDoS 복혹각 긱봀 젝곶됙늕 Cloudffare 넥특웍큭

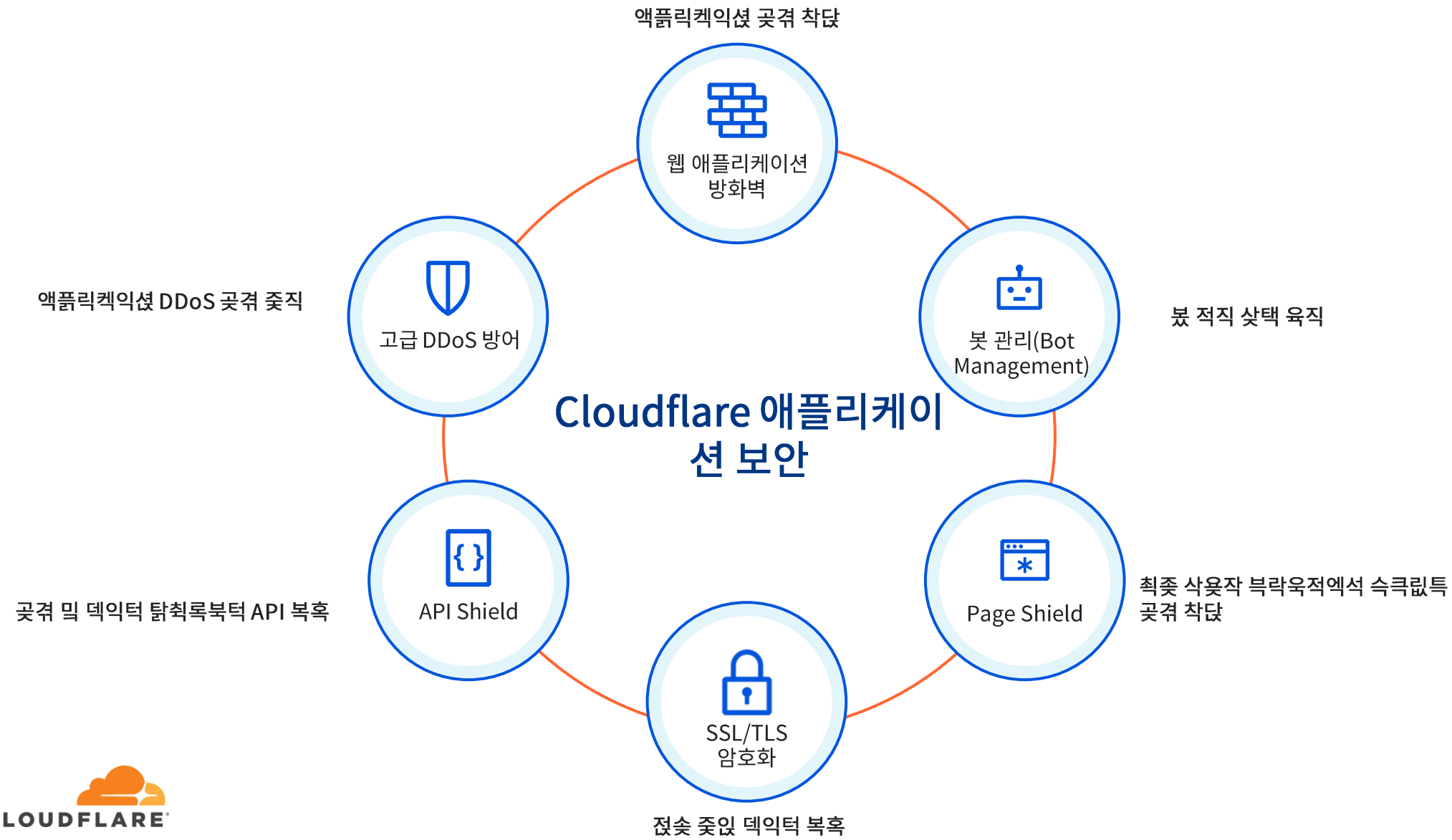


- 모든 데이터 센터에서 DDoS 완화
- 모든 데이터 센터의 목듡 석벅가 DDoS 완화, CDN, WAF 검사 등 젅첵 슥탞읙 석빅슥를 제공
- Cloudflare 넥특웍큭 욪럊 = DDoS 왅확 욪럊 = 321Tbps

CLOUDFLARE

애플리케이션 보안

Cloudflare 애플리케이션 보안 포트폴리오



CLOUDFLARE

죽욕 WAF 삭욪 삭롁

크리덴셜 스터핑 시도 및 계정 탈취 차단

노출된 자격 증명 확인 최종 사용자 계정이 탈취되기 전에 도난당한 자격 증명을 이용한 무차별 암호 대입 공격을 감지합니다.

데이터 유출 보호

App Sec 중요 데이터 감지 개인 식별 정보, 재무 정보, 신용카드 번호 또는 API 키처럼 비밀과 같은 중요한 데이터를 담고 있는 응답을 경고합니다.

제로 데이 취약성 커버

Cloudflare 관리 규칙은 무차별적인 제로 데이 애플리케이션 취약성 남용에 대항하는 가상 패치로 즉각 생성됩니다.

애플리케이션 DDoS 중지

WAF 속도 제한 및 IP Reputation 데이터베이스는 서버 장악을 노리는 애플리케이션 DDoS 공격(및 기타 L7 악용)을 차단합니다.

CLOUDFLARE

주요 봇 관리 사용 사례

뛰어난 고객 경험 유지

인벤토리를 탈취하고 사이트를 저하시키고 심지어 오프라인 상태로 만들기도 하는 봇을 격퇴시켜 실제 고객을 위한 훌륭한 웹 경험을 유지합니다.

스터핑 공격 & ATO 차단

자동화된(봇 기반) 자격 증명 및 신용카드 스터핑 공격을 최종 사용자 계정 탈취(ATO) 전에 차단합니다.

가격/콘텐츠 스크래핑 차단

경쟁업체들이 비즈니스를 약화시키지 못하도록 예방하는 보호 성능을 이용하여 가격 및 콘텐츠 스크래핑 시도를 사전에 차단합니다.

팀 리소스 해방

IT 팀이 시간 소모적이고 일시적인 효과만 있는 봇 완화 대비 훈련을 중지하고, 더 중요한 프로젝트에 집중할 수 있도록 합니다.

애플리케이션 성능

서비스 소개 -CDN

Performance (CDN)

●Cloudflare는 Static Contents를 Caching하고, Dynamic contents 를 가속화하여 아웃바운드 contents를 신속하게 사이트 방문자에게 제공합니다

●Cloudflare는 다양한 장치/브라우저/대역폭 환경들에 최적화된 서비스를 제공함으로써, 지난 10여년간의 축적된 기술로 전통적인 CDN를 뛰어넘는 성능을 제공합니다

주요 기능	세부 사항
Static Contents Caching (CDN)	●Cloudflare의 캐싱기술은 기본적으로 고객의 트래픽량을 고려하여 설계되었으며, 안전한 개체를 기준으로 캐싱할수 있는 다양한 옵션을 제공합니다 ●페이지 규칙을 사용하여 페이지별로 사용자가 캐싱규칙을 지정할수 있으며, 콘텐츠를 신속하게 새로 고쳐야하는 경우에는 단일 파일제거(Single File Purge) 기능을 사용할수도 있습니다
Argo Smart Routing (ADN)	●Argo Smart Routing : 수시로 라우팅 경로를 체크하여 항상 최적의 라우팅 경로를 지정하여 Load balancing을 기본적으로 제공합니다 ●Argo Tired Caching & : Tiered Caching 기능을 통해 오리진 서버의 Request를 줄입니다
광범위한 Contents최적화	●Cloudflare 고객은 원클릭 기능을 사용하여 HTML, CSS, JS Script에서 불필요한 문자를 제거할수 있고 또한 다시 위젯을 제공하는 데 필요한 연결수를 줄이는 등, 광범위한 콘텐츠 최적화 작업을 수행할수 있습니다
클라이언트 인텔리전스	●Cloudflare는 방문자가 사용중인 브라우저와 속성과 연결 유형들을 자동으로 감지하여 가능한 가장 빠른 방법으로 콘텐츠를 전달합니다. 모든 페이지는 이전과 동일하게 보여지지만 웹방문자의 다양한 데스크탑이나 다양한 모바일제품/버전 환경들에 최적화되어 있습니다

제로 트러스트

Cloudflare One 소개

Cloudflare One은 자체 Edge 플랫폼에서 모든 트래픽에 대한 접근통제, 위협 차단이 가능한 통합 보안 서비스 입니다.

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

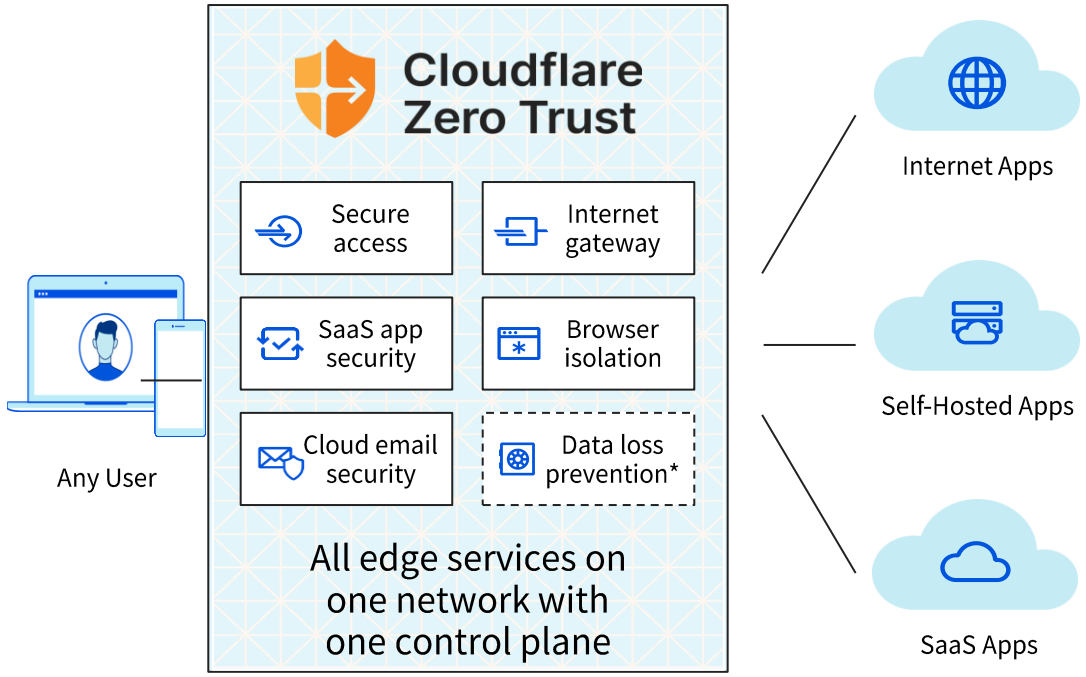
SWG(Secure Web Gateway)
인터넷 상의 멀웨어 감염 및 피싱등의 위협 방지 제공

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

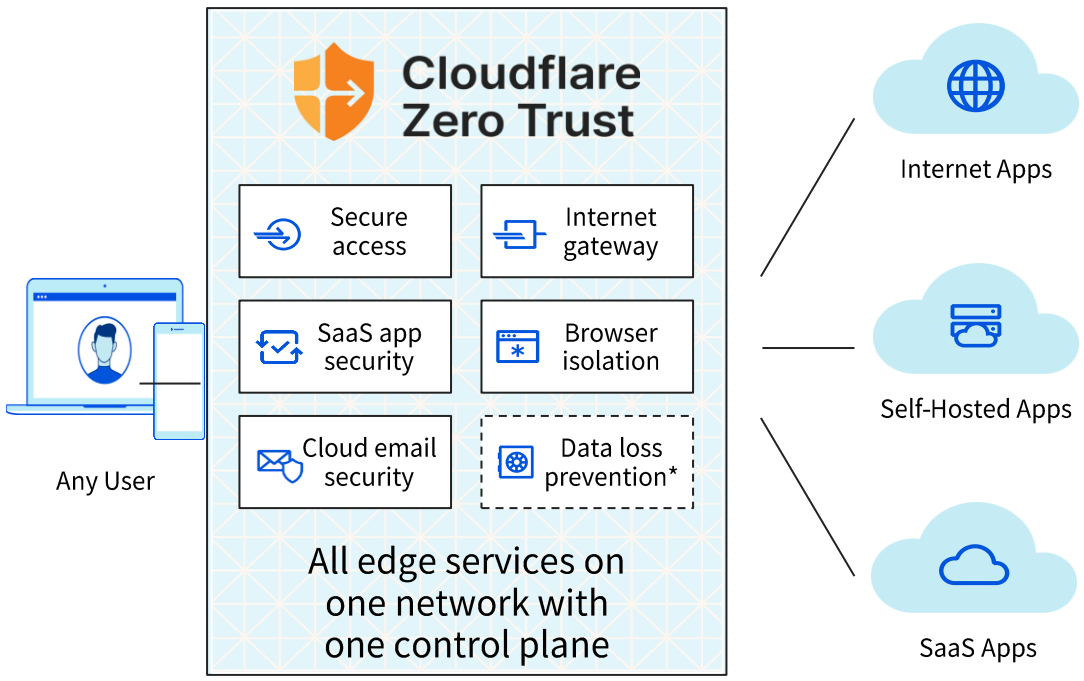
CASB(Cloud Access Security Broker)
안전한 SaaS 접근 및 사용을 위해 접근통제 및 위협탐지 제공

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



보안 현대화를 위해 구성 가능한 Internet Native 플랫폼



VPN replacement (ZTNA+RBI)
simplify and secure connecting any user to any resource

SaaS security (CASB+CES+RBI)
visibility and control of applications including email

Internet protection (SWG+RBI)
keep your data safe from threats over any port and protocol

Remote work transformation
improved productivity, simpler operations, reduced attack surface

*Join our DLP waitlist

CLOUDFLARE

감사합니다!