Cloudflare Zero Trust

Cloudflare 솔루션 포트폴리오

CLOUDFLARE

Cloudflare Platform

1 Cloudflare One

Cloudflare Zero Trust Services

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

Cloudflare Network Services

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

Cloudflare Application Services

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

Cloudflare Developer Platform

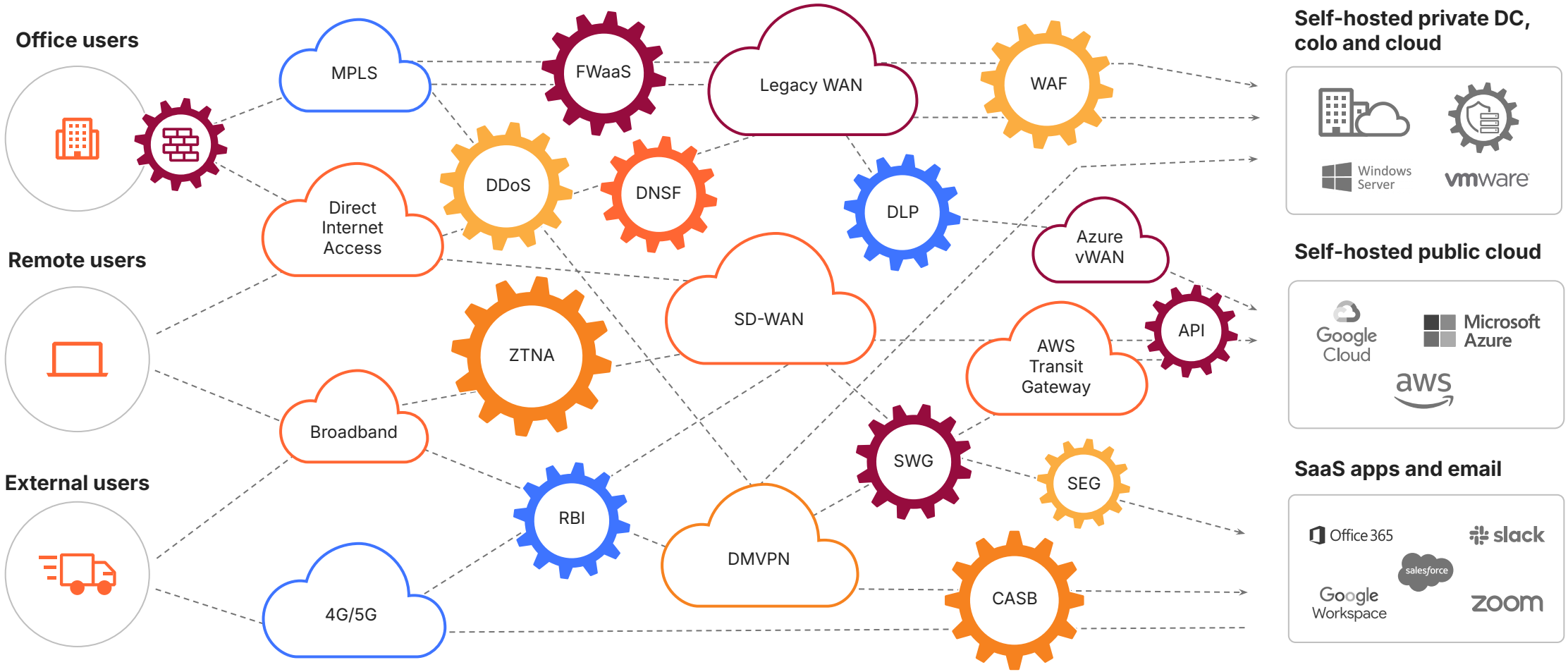
Workers | Pages | R2 | Workers KV | Durable Objects | Images | Stream

Cloudflare Global Network

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

CLOUDFLARE

다양한 장치와 사용자 위치에서 멀티 클라우드 및 **IaaS, DC, SaaS** 애플리케이션까지 다양한 서비스에 접근해야 합니다



CONNECTIVITY CLOUD

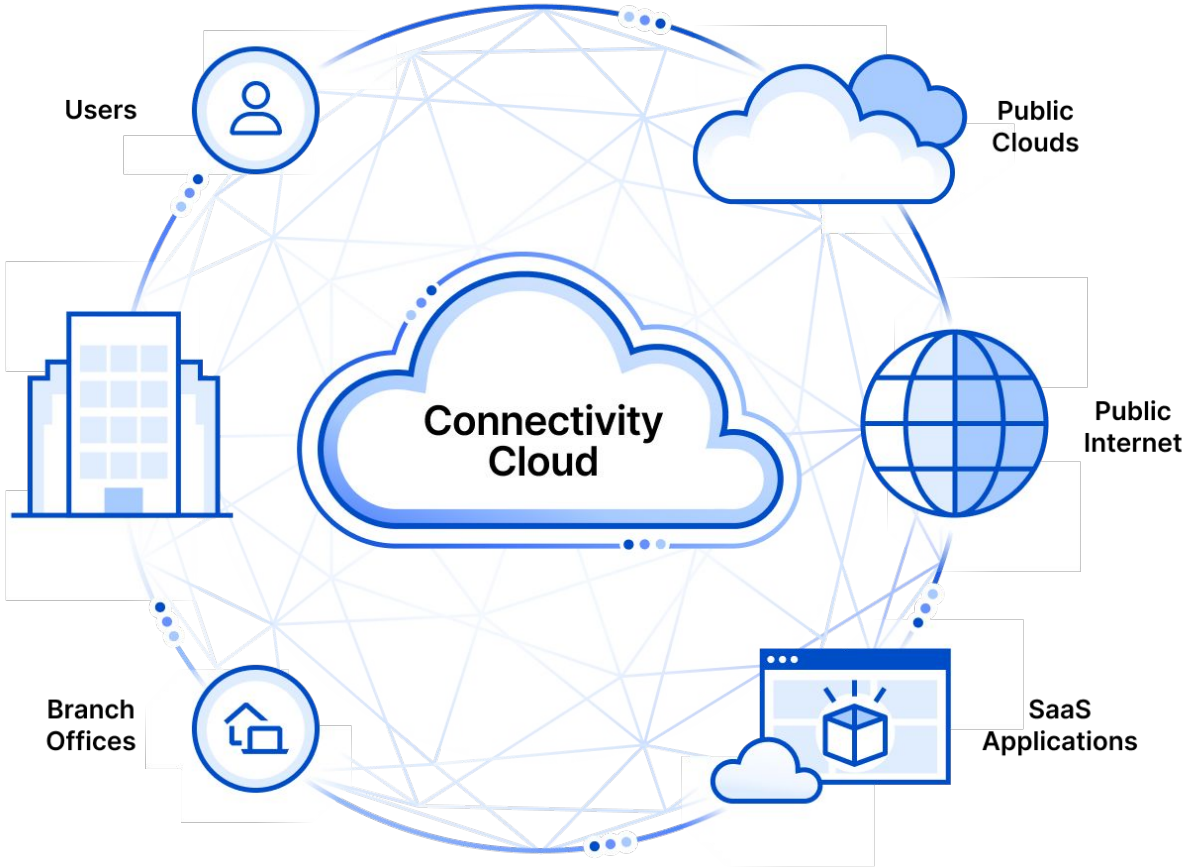
CLOUDFLARE

클라우드플레어의 커넥티비티 클라우드를 소개합니다
귀사의 비즈니스를 안전하게 연결, 보호 및 가속화하세요

모든 사용자와 모든 것을 어디서나 자유롭게 연결하면서도 완벽한 제어를 유지하세요

기업은 다음을 통해 경쟁 우위를 확보할 수 있습니다:

- **Any-to-Any 연결성** (유연한 네트워크 연결)
- **보안이 강화된 하이브리드 업무 환경**
- **멀티 클라우드 유연성**
- **인프라 통합 및 간소화**

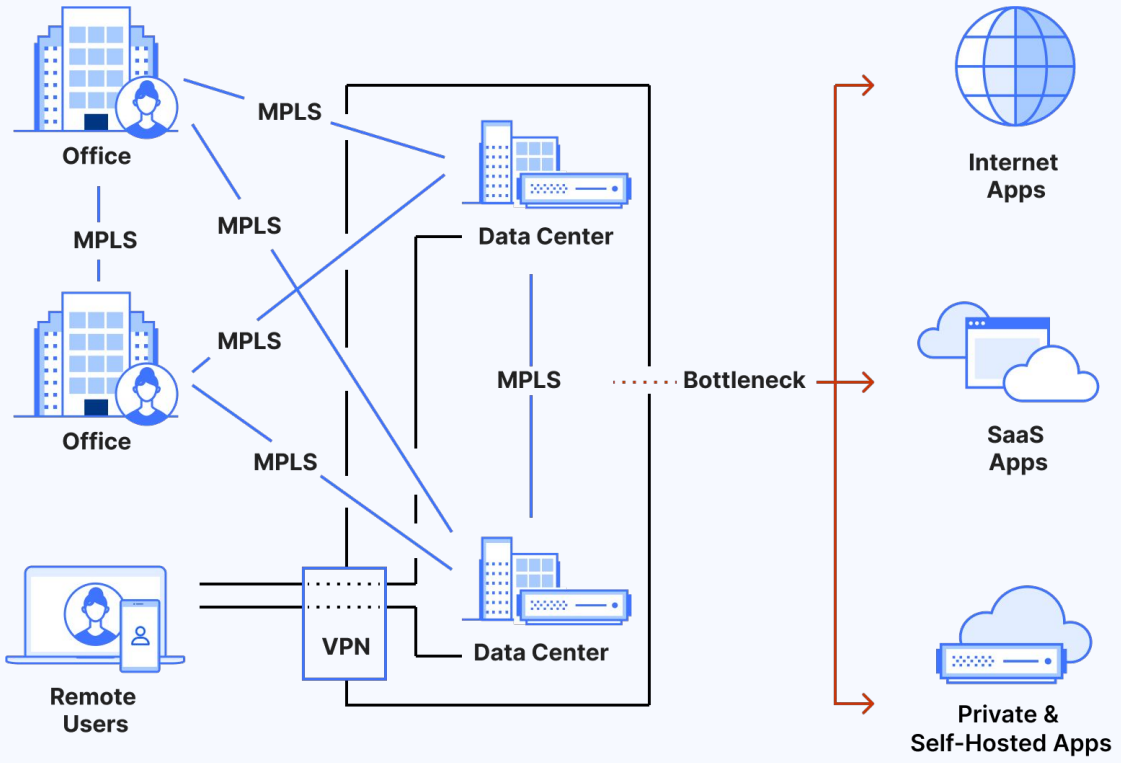


전 세계에 걸쳐 확장 가능한 글로벌 네트워크로 지원됩니다

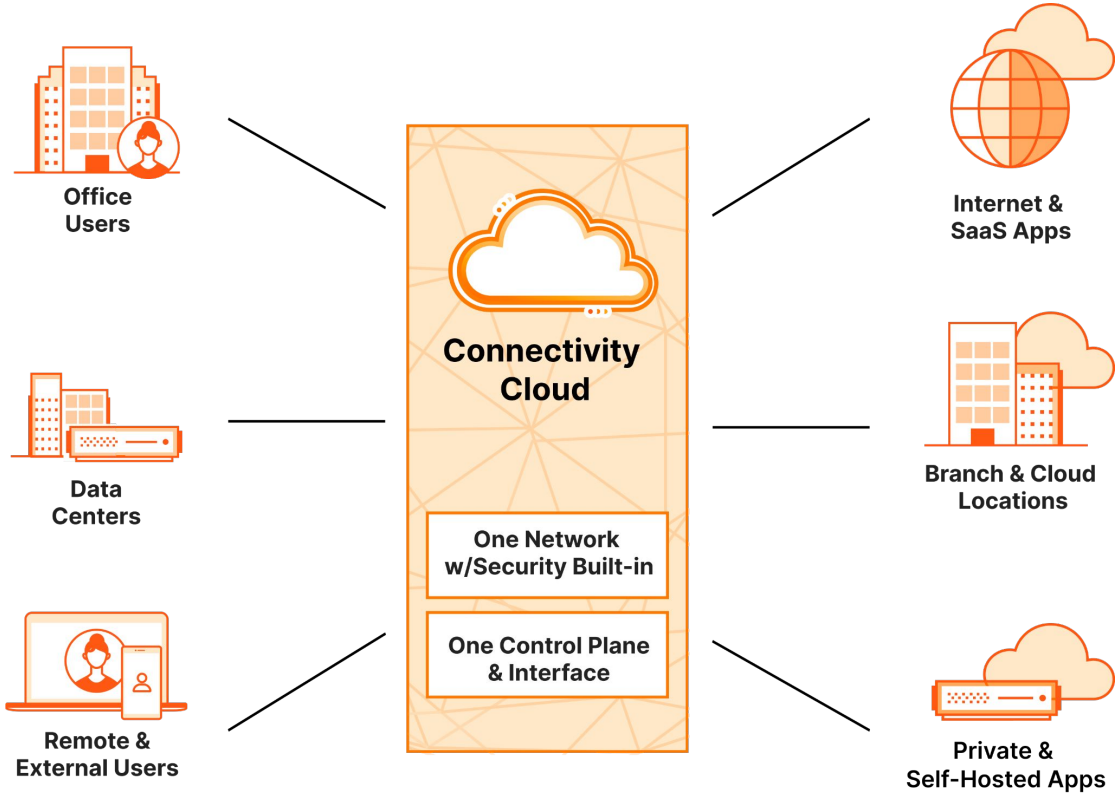
CLOUDFLARE

SASE는 **제로 트러스트**를 구현하기 위한 **아키텍처** 설계입니다

현재 기업 네트워크



모듈형(Composable) IT 인프라



Cloudflare One은 자체 Edge 플랫폼에서 모든 트래픽에 대한 접근 통제 & 위협 차단이 가능한 통합 보안 서비스입니다.

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

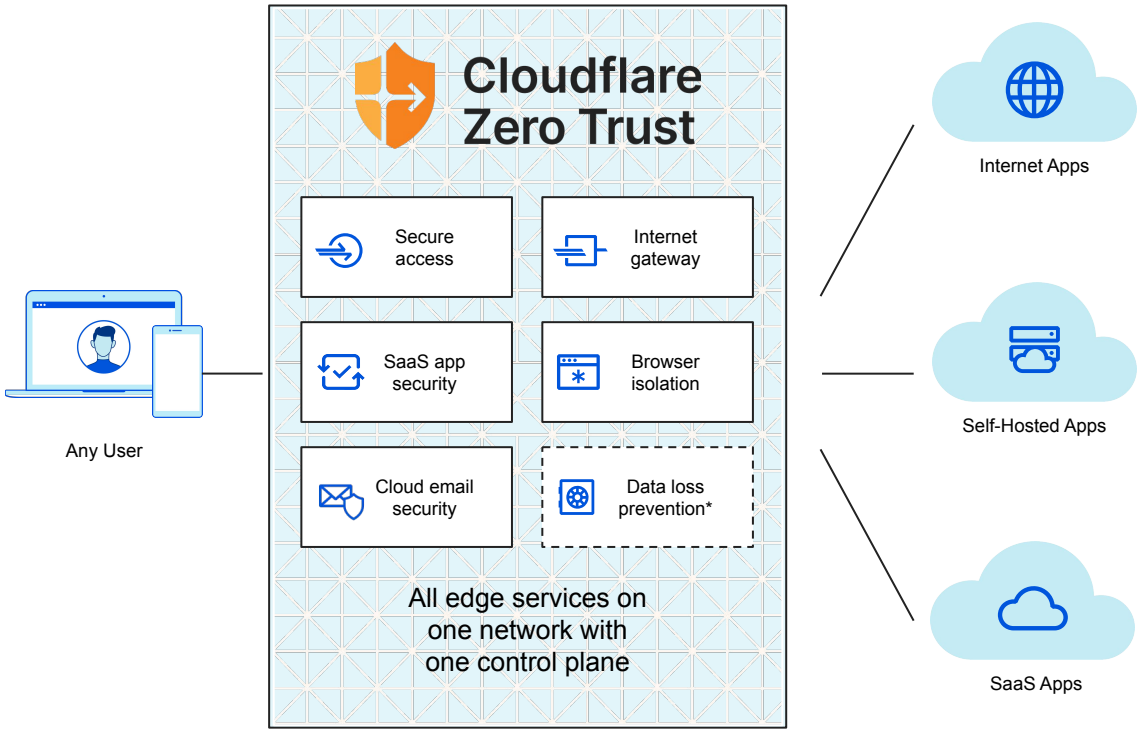
SWG(Secure Web Gateway)
인터넷 상의 멀웨어 감염 및 피싱등의 위협 방지 제공

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



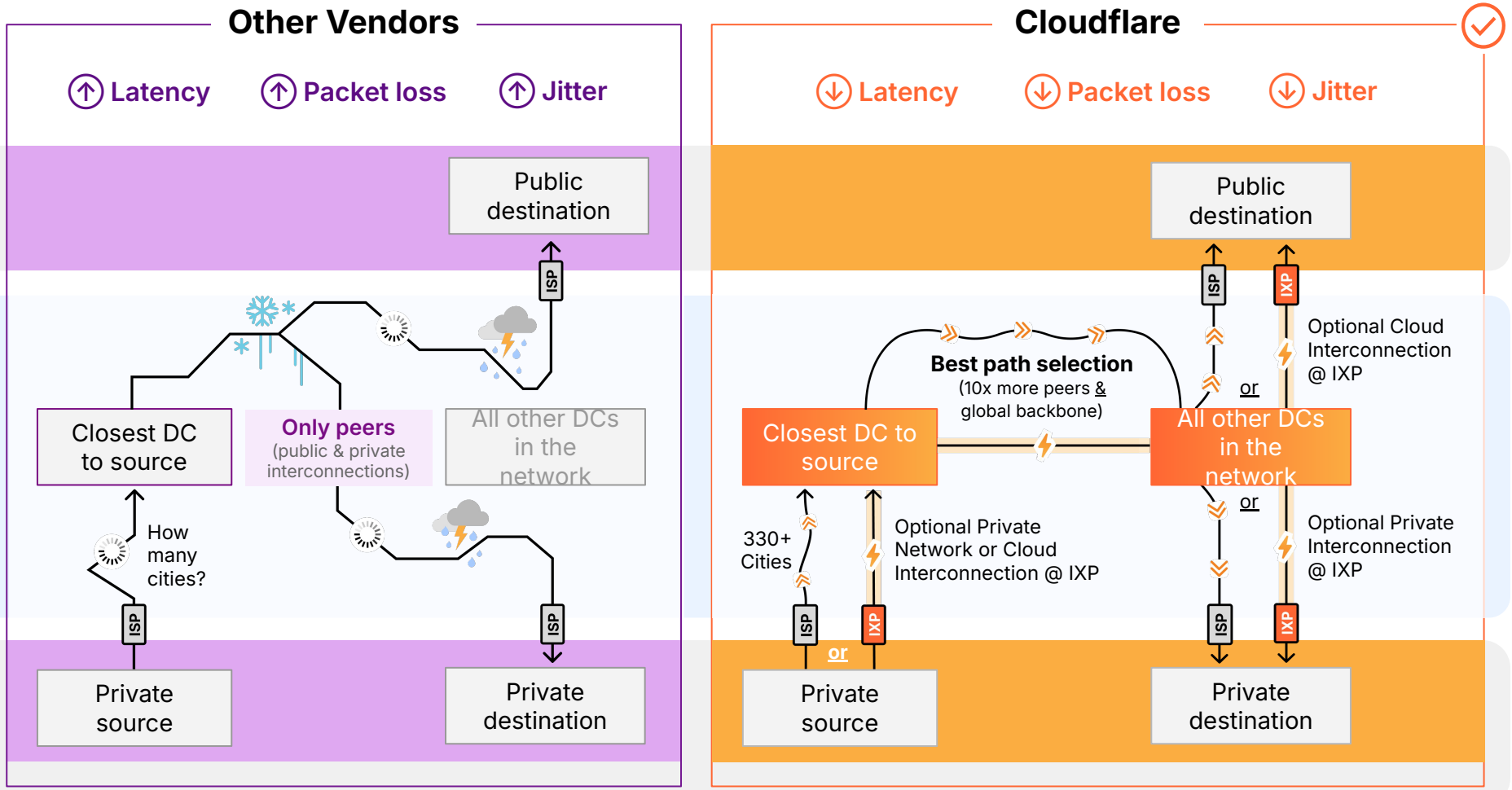
CLOUDFLARE

글로벌 백본은 **프라이빗 및 퍼블릭 트래픽 전송**에 있어 중요한 역할을 합니다.

벤더 전용 커넥터를 사용하는 **퍼블릭 네트워크/클라우드**

공용 인터넷을 통한 **미들 마일(Middle Mile)**은 기본적으로 **탄력적이지 않으며 성능이 보장되지 않습니다.**

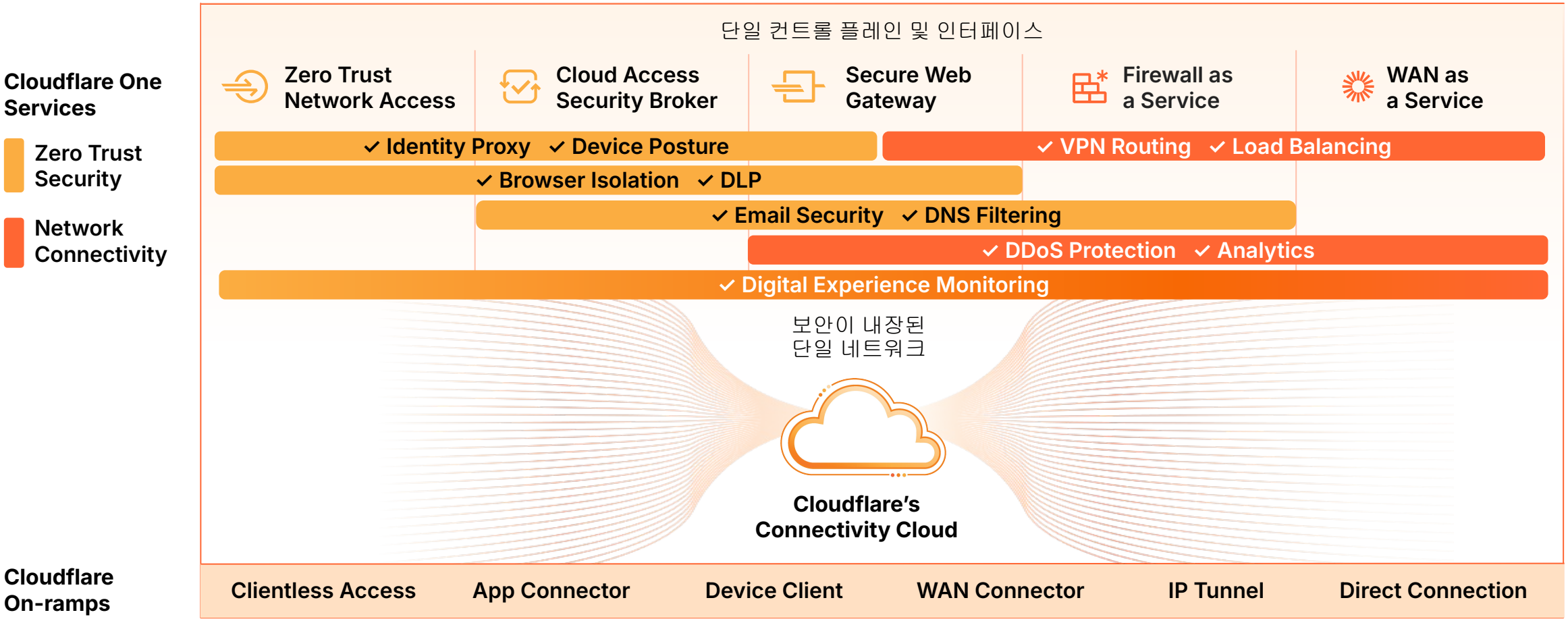
벤더의 **클라이언트리스, 클라이언트, 애플리케이션 또는 WAN 커넥터**를 활용한 **프라이빗 네트워크/클라우드**



ARCHITECT

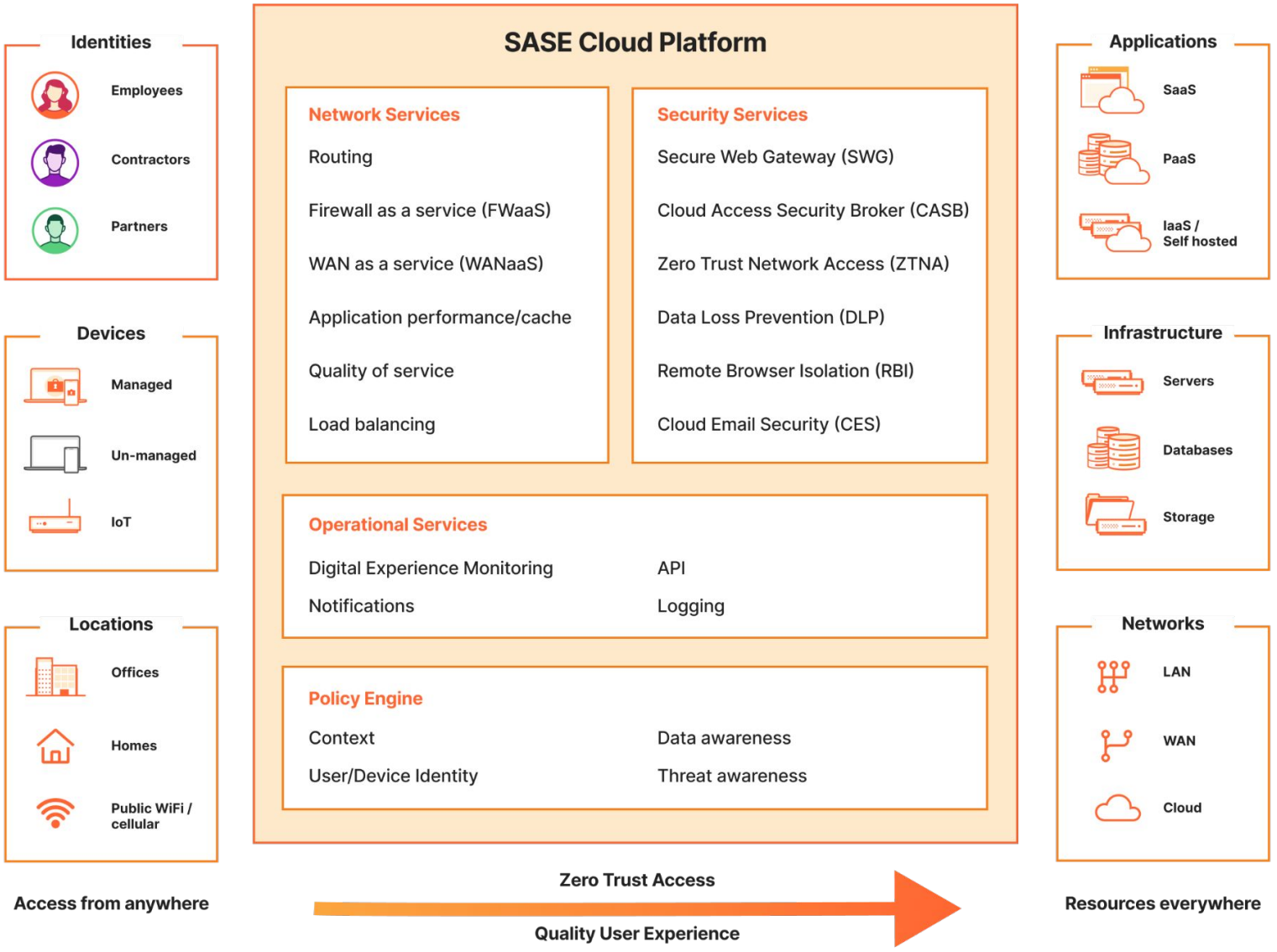
CLOUDFLARE

제로 트러스트 보안 **통합** 및 **SASE** 기반 네트워크 현대화



CLOUDFLARE'S SASE ARCHITECTURE

CLOUDFLARE



One

새로운 기능 개발과 보안 정책 적용이 가능한 프로그래머블 단일 네트워크 및 컨트롤 플레인

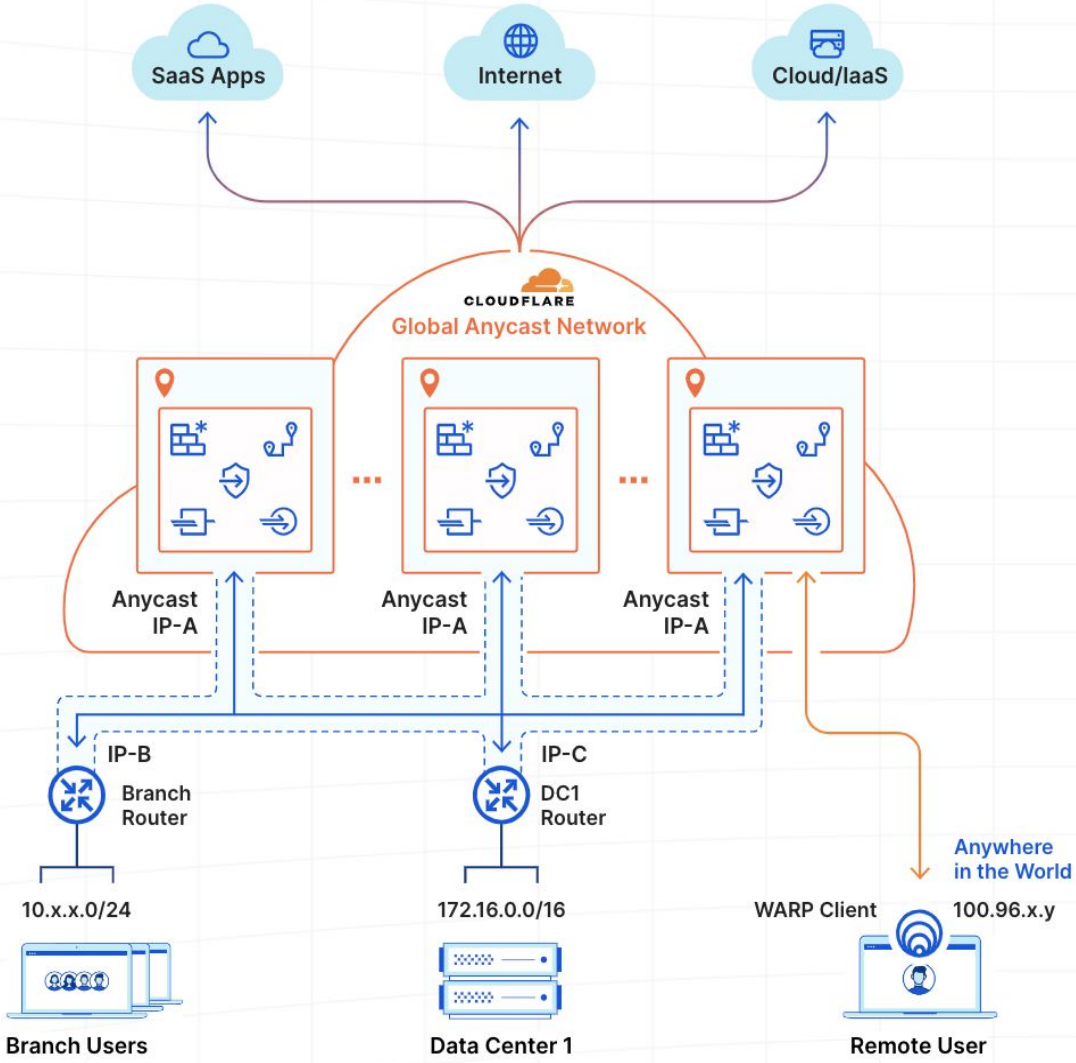
SLA 100%

오직 **Anycast** 기반 아키텍처만이 제공할 수 있는 유료 플랜 대상 **100%** 가동 시간 **(SLA)** 보장

All

모든 서비스가 모든 **Cloudflare** 네트워크 위치에서 실행되도록 설계되어, 모든 트래픽을 소스와 가장 가까운 위치에서 검사하여 일관된 속도와 확장성을 제공

WAN routing + Web Access with Magic tunnel and WARP on-ramp



Each data center in Cloudflare's global anycast network delivers all Cloudflare services, including Magic WAN, Magic Firewall, Zero Trust and DDoS services

Anycast IPsec/GRE Tunnels between customer site routers and Cloudflare global anycast network

WARP connections between remote users and Cloudflare global anycast network

- **On-ramp to Cloudflare Magic WAN**
  - Customer sites with IPsec/GRE tunnel-capable routers on-ramp to Cloudflare Magic WAN via Anycast IPsec/GRE tunnels
  - Remote users on-ramp to Cloudflare Magic WAN via WARP client on their devices
- **Full-mesh Magic WAN** network connectivity (RFC 1918 address space) between all sites and users over Magic WAN
- **Web access** with Zero Trust control from all sites and users via Magic WAN + Cloudflare Zero Trust services
- **Fine-grain security and control**
  - Magic Firewall
  - Cloudflare Zero Trust

CLOUDFLARE

VPN을 ZTNA(Zero Trust Network Access)로 대체하세요

CLOUDFLARE

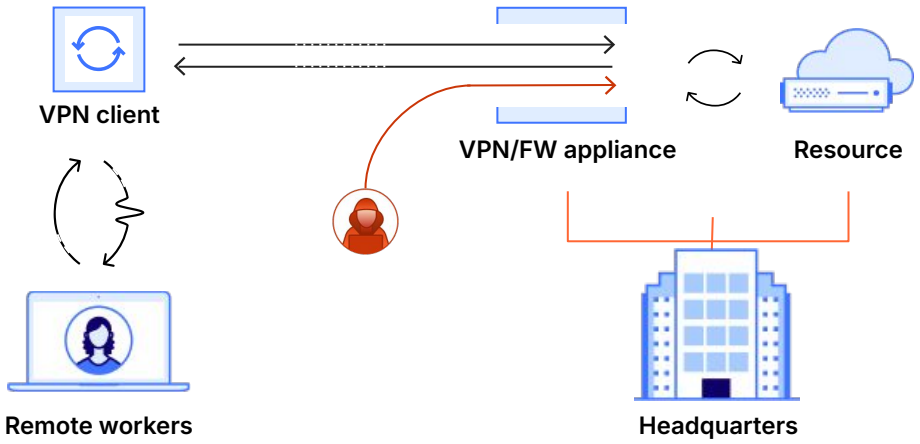
VPN vs. ZTNA

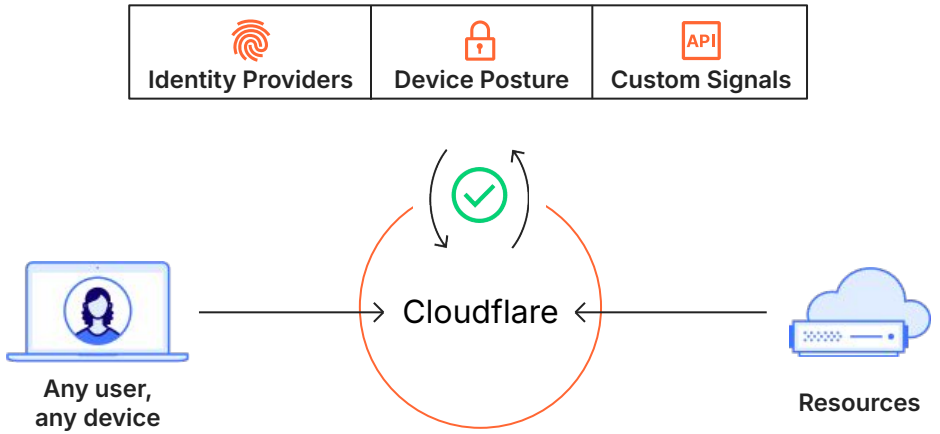
현대적인 하이브리드 업무 환경을 위한 **혁신적인 원격 액세스 솔루션**

Problem:
기존 VPN 클라이언트는 **과도한 신뢰를 부여합니다**

Solution:
ZTNA는 세분화된 컨텍스트 기반 접근 제어를 제공합니다

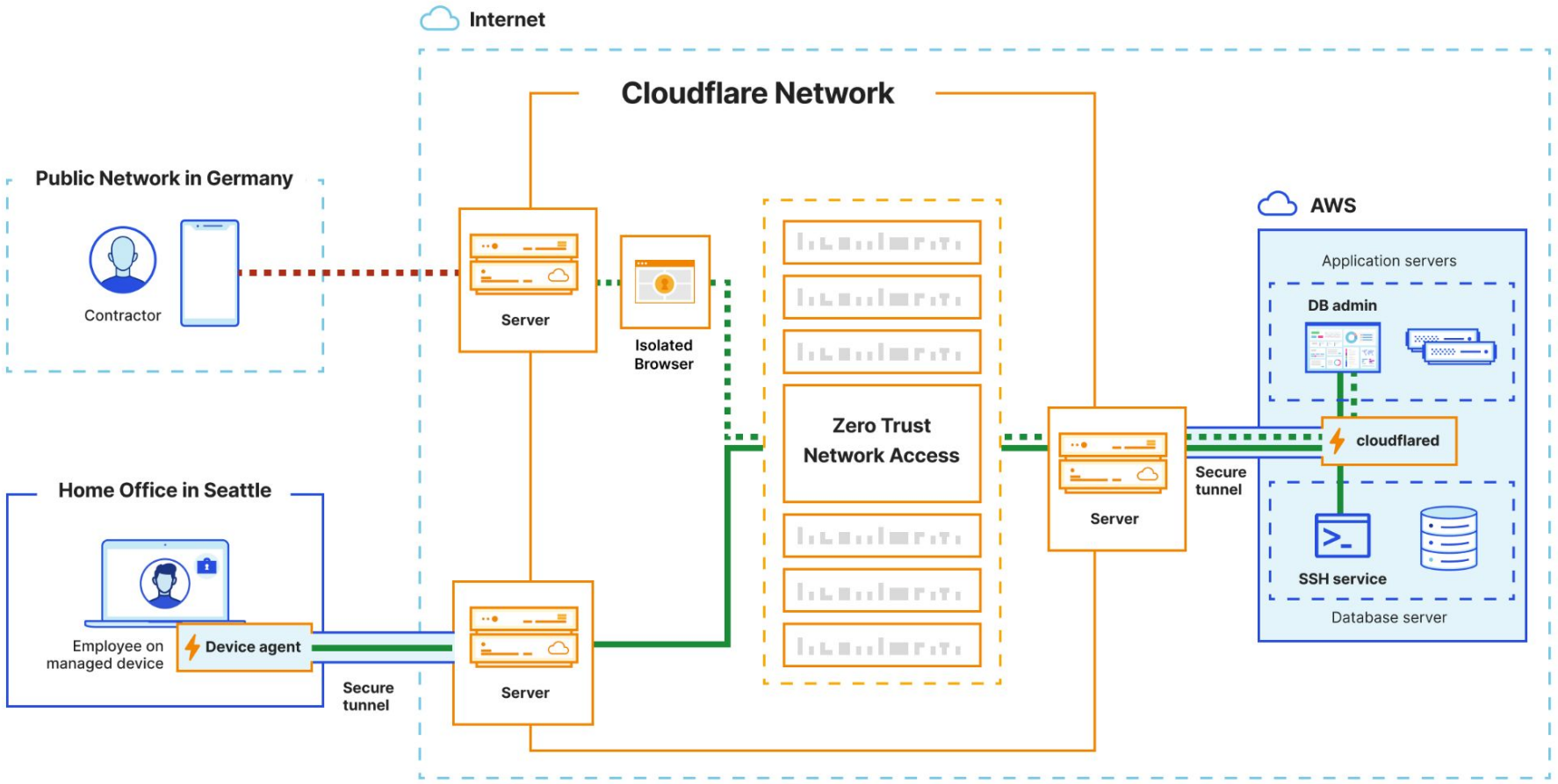
	VPN	Cloudflare
확장성 / 처리량(Throughput)	수동 / 제한적 (Manual / Limited)	즉시 적용 / 무제한 (Instant / Unlimited)
아키텍처 / 라우팅	중앙 집중식 위치에서의 사이트 간 연결 (Site-to-Site)	Anycast는 전 세계 335개 이상의 위치에 걸쳐 운영
정책 엔진 (Policy Engine)	일반적 (Generic)	세분화 (Granular)
사용자 및 디바이스 신뢰	기본적으로 허용됨 (Granted by Default)	아이덴티티 및 컨텍스트 기반 접근 제어
실시간 모니터링 (Real-Time Monitoring)	제한적 (Limited)	포괄적 (Comprehensive)





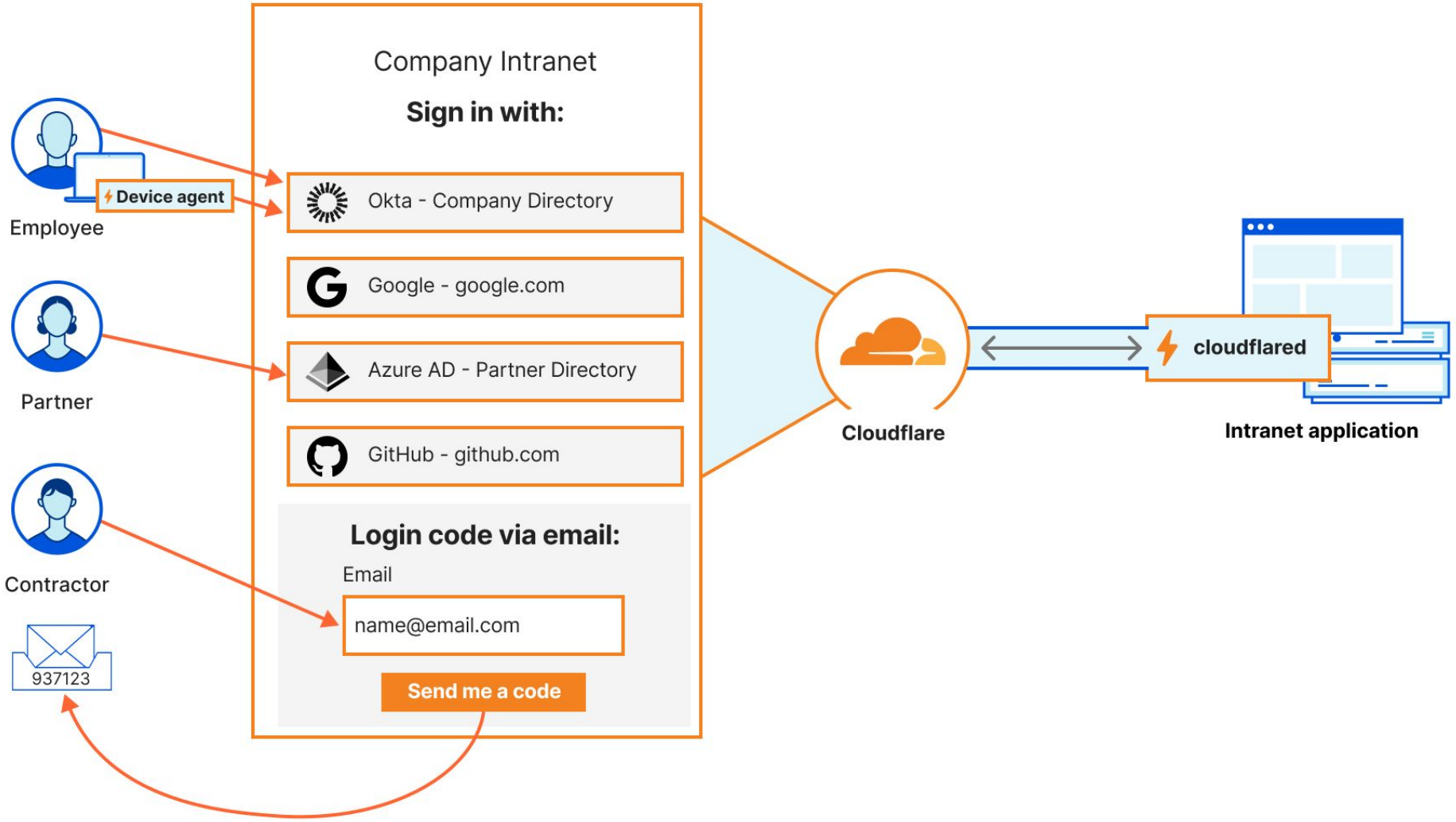
CLOUDFLARE

High Level Architecture



CLOUDFLARE

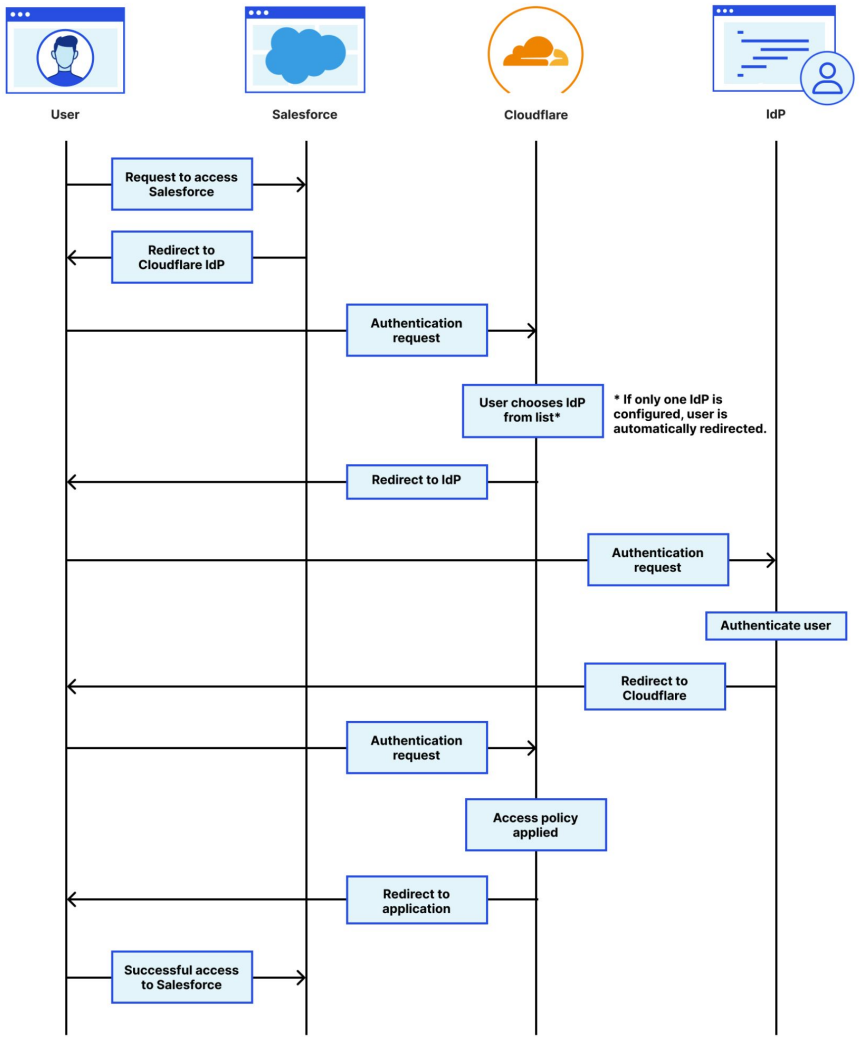
아이덴티티 제공자(Identity Providers) 통합



CLOUDFLARE

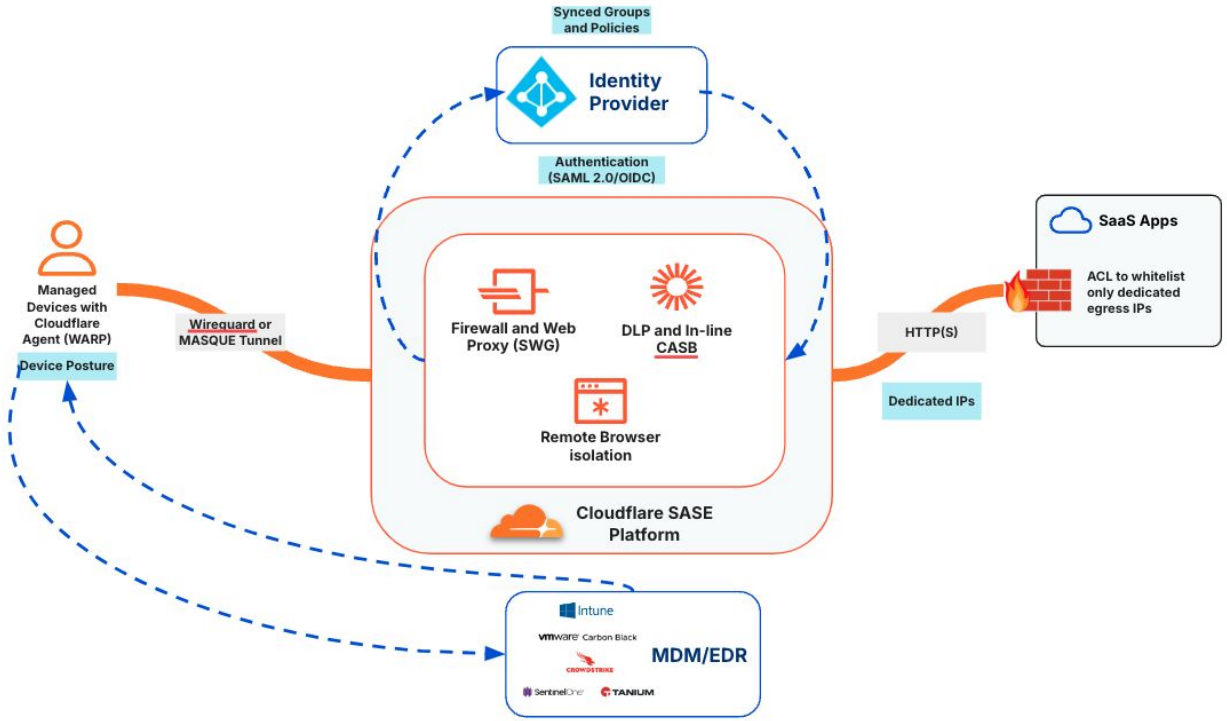
SaaS 접근 방식: SSO 프록시 (옵션 1)

- **Zero Trust** 원칙에 맞춘 보안 접근 방식
- 아이덴티티 기반 접근 제어
- 디바이스 상태(**Posture**) 평가
- 네트워크 경로 정책 적용
- 다중 아이덴티티 제공자(**IdPs**) 지원
- **API CASB** 스캐닝 구성 지원



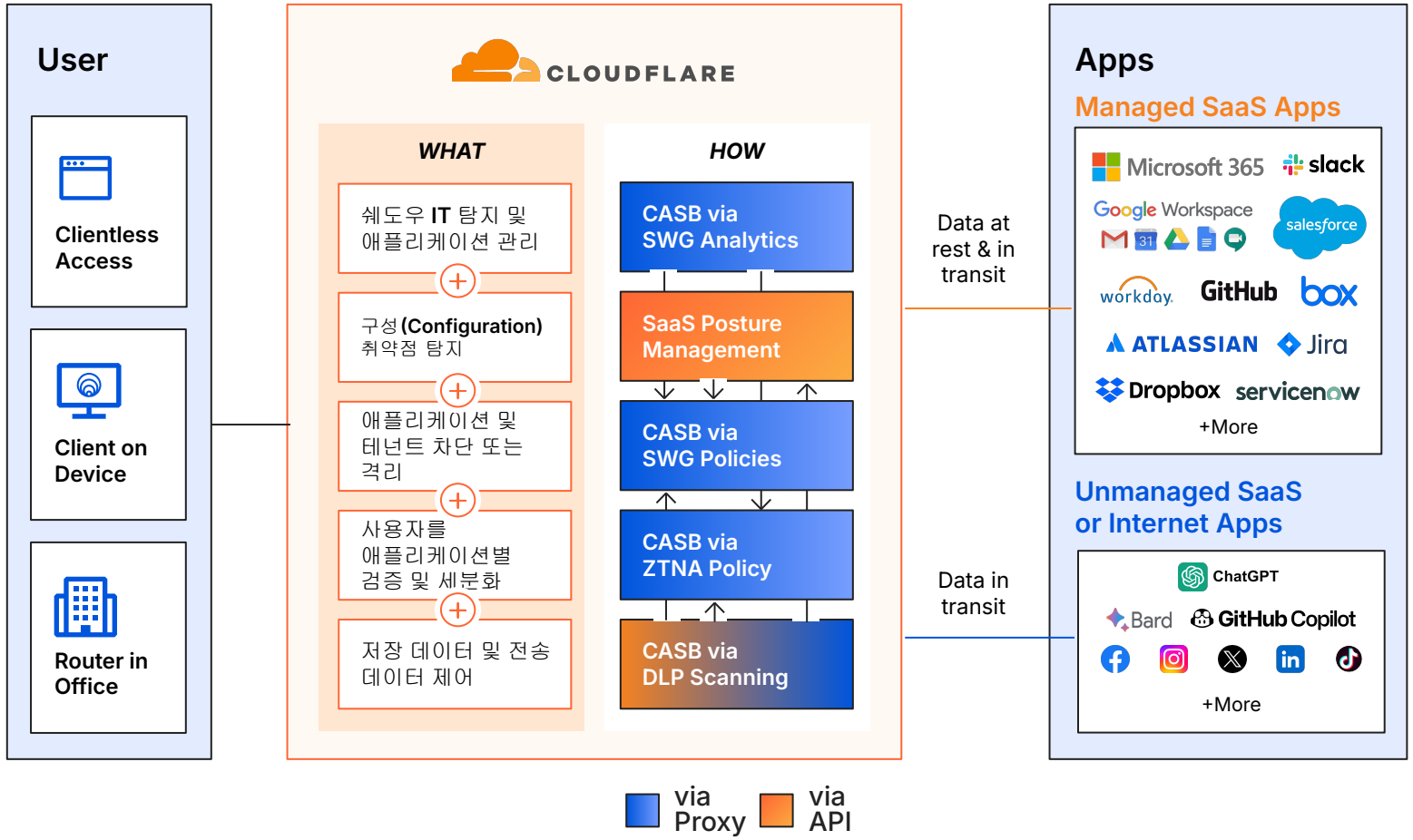
SaaS 접근 방식: 전용 IP + 화이트리스트 (옵션 2)

- 네트워크 기반 접근 제어 방식 적용
- **Cloudflare**에서 사전 할당된 전용 **IP** 사용
- 정책 기반 구성 가능
- 디바이스 상태**(Posture)** 평가 지원
- **IdP** 구성 변경 없이 적용 가능
- **SaaS** 화이트리스트 기능 필요



CLOUDFLARE

데이터 보호 (Data Protection)



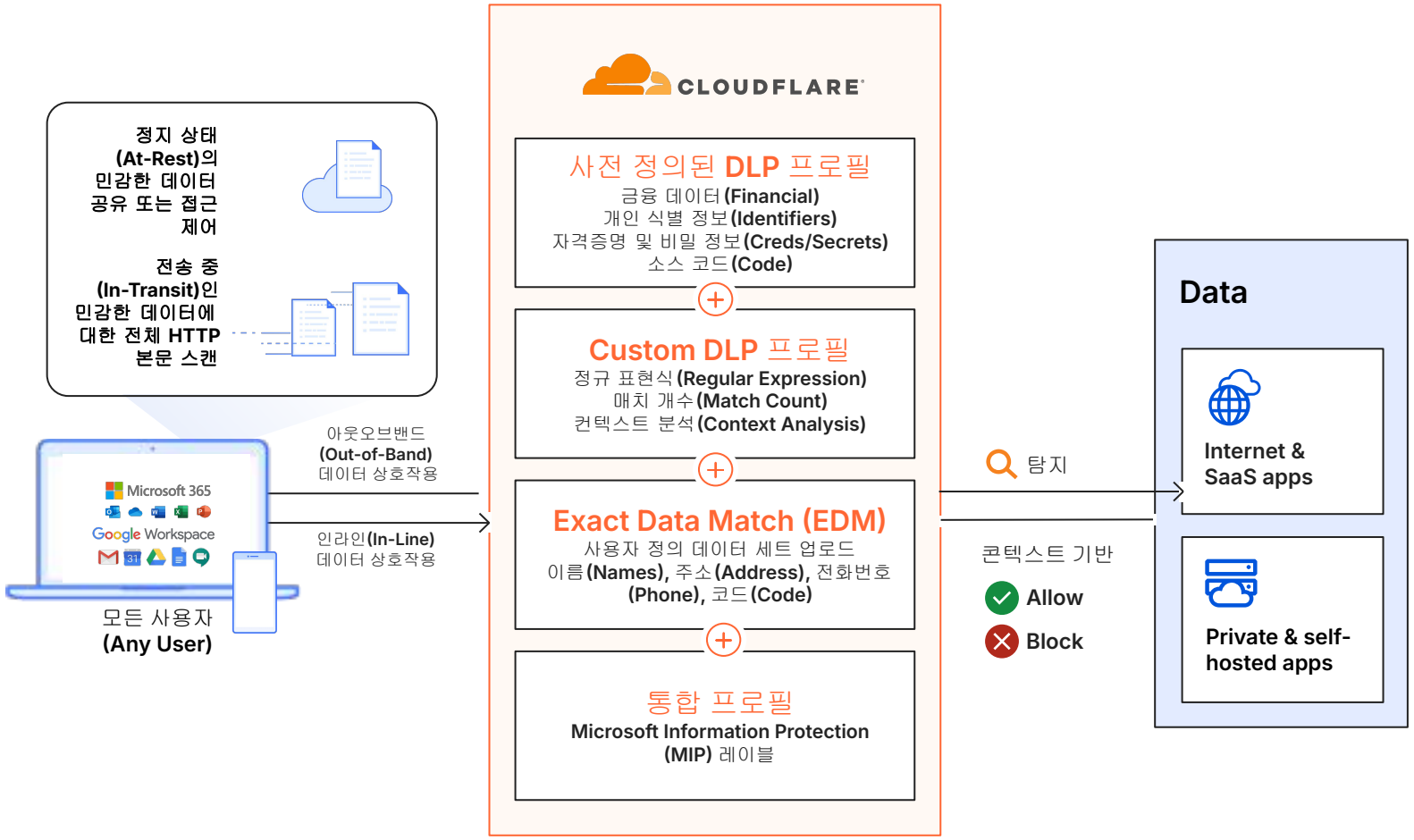
Cloud Access Security Broker (Multimode)

자주 사용하는 애플리케이션과 통합 다음과 같은 보안 이슈 탐지:

- 잘못된 구성 (Misconfigurations)
- 데이터 노출 (Data Exposure)
- 비정상적 접근 (Out-of-Band Access)
- 비관리형 애플리케이션 접근 제어
- 위험한 행동 차단을 위한 정책 설정
- 데이터가 테넌트 밖으로 유출되는 것 방지

CLOUDFLARE

데이터 보호 (Data Protection)

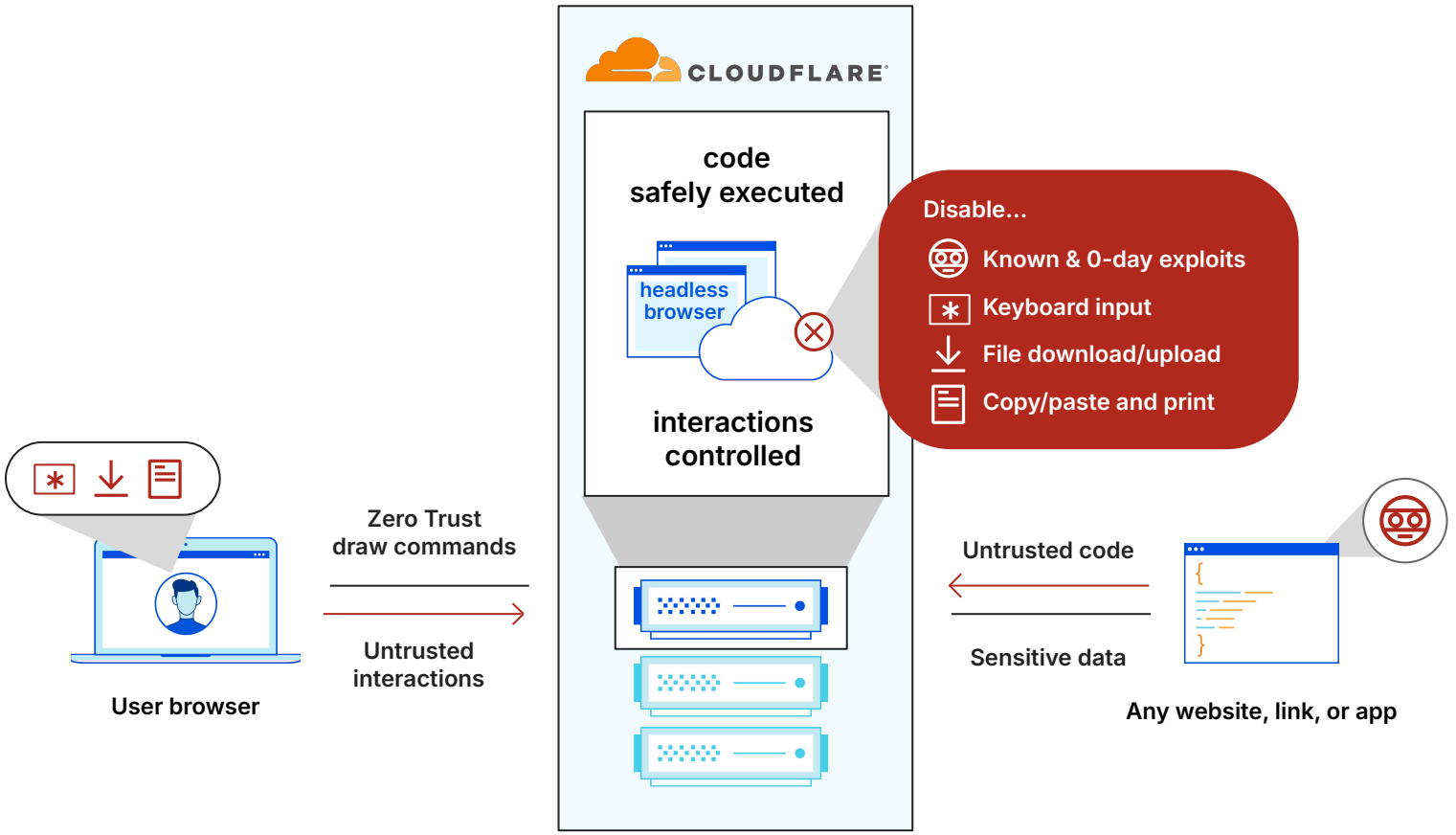


DLP 통합 데이터 유출 방지 (Integrated Data Loss Prevention)

- 규제 준수 간소화 및 자동화
- 데이터 유출 및 보안 침해 위험 최소화
- 데이터, 사용자, 애플리케이션에 대한 인라인 모니터링 강화 **(Data Exposure)**

CLOUDFLARE

제로데이 공격 원천 차단



RBI 원격 브라우저 격리 (Remote Browser Isolation)

- 제로 트러스트 기반 웹 브라우징 및 이메일 링크 보호
- 사용 중인 데이터 **(Data-in-Use)** 보호
- 고속 사용자 경험**(UX)** 제공
- 모든 브라우저와 호환 가능

CLOUDFLARE

Cloudflare One은 기업이 **보안, 성능, 연결성을 동시에 강화할 수 있는 최적의 솔루션**을 제공합니다

🚀 **주요 강점**

1️⃣ 제로 트러스트 보안(Zero Trust Security)

- 사용자 및 기기 신뢰 기반 접근 제어
- 네트워크, 애플리케이션, 데이터 보호

2️⃣ 통합 SASE 아키텍처(SASE Integration)

- 네트워크 보안(SWG, CASB, DLP) 및 제어 기능 통합
- 글로벌 Anycast 네트워크 기반

3️⃣ 빠르고 안정적인 연결(Fast & Reliable Connectivity)

- 전 세계 335개 이상 PoP에서 제공
- 퍼블릭/프라이빗 네트워크 트래픽 최적화

4️⃣ 원격 브라우저 격리(Remote Browser Isolation)

- 피싱 및 악성 링크 차단
- 인라인 데이터 보호 및 보안 강화

5️⃣ 보안과 네트워크 가시성(Security & Network Visibility)

- 실시간 모니터링 및 위협 탐지
- AI 기반 정책 자동화 및 위협 대응

6️⃣ 데이터 보호(Data Loss Prevention & Compliance)

- 사전 정의 및 커스텀 DLP 정책 지원
- 민감한 데이터 보호 및 규제 준수 강화

7️⃣ 쉬운 배포 및 관리(Simple Deployment & Management)

- 모든 클라우드 및 온프레미스 환경에서 유연한 적용
- API 및 자동화를 통한 간편한 운영

Thank you