

# Magic WAN

Magic WAN은 무제한 연결로 SASE로 가는 경로를 간소화합니다

## 네트워크 아키텍처의 진화

### 새로운 기업 네트워크로서의 인터넷

하이브리드 근무가 새로운 기준이 되고 앱이 클라우드로 이동함에 따라 IT 팀에서는 다음 문제와 씨름하고 있습니다.

- **네트워크 복잡성:** MPLS 프로비저닝과 포인트 솔루션 조정에 너무 많은 시간이 소요됨
- **보안 격차:** 인터넷에 직접 연결하면 보안 및 이용 목적 제한 방침을 우회하고, 사용자와 데이터가 위험에 노출됩니다
- **높은 비용:** MPLS 링크와 보안 포인트 솔루션 이용으로 불필요한 지출이 발생함
- **열악한 사용자 경험:** 경계 보안 스택으로 트래픽을 백홀링하면 대기 시간이 발생합니다

Magic WAN에서는 분기 사이트, 멀티 클라우드 VPC, 데이터 센터와 [Cloudflare One](#) SASE 플랫폼의 네트워크 연결을 간소화하므로, 안전하고 성능이 뛰어나며 비용 효율적으로 연결하여 IT 팀의 하이브리드 근무 및 멀티 클라우드 과제를 해결할 수 있습니다.

유연성이 부족하고 비용이 많이 드는 [MPLS](#) 네트워킹이나 온프레미스 방화벽으로 구축된 복잡한 [SD-WAN](#) 배포와 달리, Magic WAN은 “가벼운 분기, 견고한 클라우드” 접근 방식을 사용하여 현재의 아키텍처를 개선/대체합니다. 배포가 간편하고 기본 제공되는 보안을 통해 다양한 비즈니스 요구 사항에 맞추어 규모를 조정할 수 있습니다.



Magic WAN은 물리적 또는 가상 네트워크 위치를 Cloudflare의 SASE 플랫폼에 연결합니다. 물리적 사이트의 예로는 지사, 공장의 여러 층, 리테일 지점, 본사, 데이터 센터가 있습니다. 가상 위치의 예로는 AWS, Azure, GCP, OCI 등의 퍼블릭 클라우드 서비스가 있습니다.



#### 개선된 운영 민첩성

하나의 관리 콘솔로 네트워크 보안 및 연결을 중앙에서 관리합니다. 제로 터치 구성으로 몇 분 만에 온램프(on-ramp) 트래픽을 처리할 수 있습니다.



#### 볼트온이 아닌 내장형 보안

클라우드 네이티브 DDoS 방어, 네트워크 방화벽, SSE 및 Zero Trust 기능 모두를 긴밀하게 통합된 서비스 형태로 제공받을 수 있습니다.



#### 네트워크 비용 절감

분기가 차지한 공간을 최소화하고 네트워크 기능을 클라우드로 전환하여 비용이 많이 드는 MPLS에 대한 의존도를 줄이고 SD-WAN으로부터 마이그레이션합니다.

## Magic WAN 주요 사용 사례

### 네트워크 연결 간소화

- **분기 연결성 단순화** — 짜깁기한 전용 회선과 네트워크 장비를 교체하여 지사와 데이터 센터 간 트래픽을 안전하게 라우팅합니다. Anycast IPsec을 이용하여 네트워크 위치 전반에 걸쳐 사이트 간 연결성을 실현합니다.
- **하이브리드 및 멀티 클라우드 연결성 단순화** — 조직에서는 다양한 공급자(예: AWS, GCP, Azure, Oracle, IBM)의 클라우드 인스턴스 및 온프레미스 데이터 센터에서 앱을 보유하고 있습니다. 이러한 다양한 환경 전반에 걸쳐 트래픽을 라우팅하고 보호하는 데 중앙화된 제어 기능을 사용합니다.

### 성능 저하 없이 보안 향상

- **안전한 WAN 연결** — 클라우드 제공 방화벽 및 SWG 제어를 통해 위치(분기, 데이터센터 등) 간 네트워크 보안 정책을 적용하여 연결을 보호합니다.
- **WAN 성능 확장** — MPLS 배포는 비용이 많이 들고 유연성이 떨어지며 속도가 느립니다. Cloudflare로 전환하면 기본 제공 보안을 통해 보다 비용 효율적이고 민첩하게 배포할 수 있습니다.

## Magic WAN 배포 접근 방식

### 네트워크 변혁은 하나의 여정입니다

Magic WAN은 인터넷 연결을 통해 성능과 안정성을 제공하며 조직에서 레거시 네트워크 아키텍처로부터 마이그레이션할 수 있도록 지원합니다. 점진적으로 Magic WAN 배포를 시작하고 시간이 지남에 따라 원활하게 전환하세요. Cloudflare의 “가벼운 분기, 견고한 클라우드” 접근 방식은 라스트 마일 연결과 미들 마일 성능, 안정성, 보안을 결합하여 하이브리드 근무를 효과적으로 연결하고 보호합니다. Cloudflare의 아키텍처는 기존 인프라와 함께 배포를 지원하므로 원하는 속도로 마이그레이션할 수 있습니다.



## Cloudflare One과 MPLS 및 SD-WAN의 비교

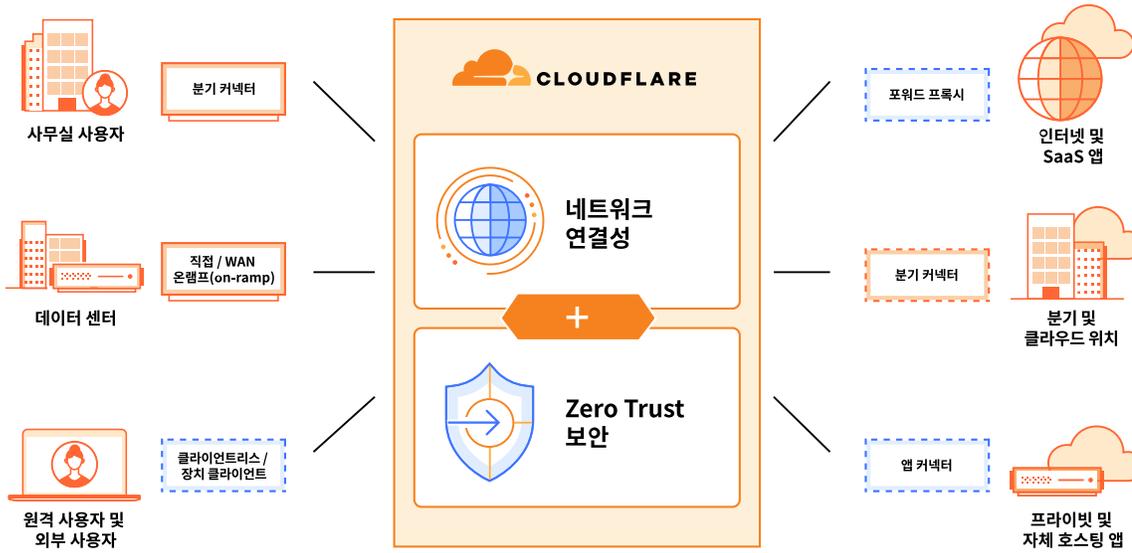
앱이 클라우드로 이동하고 조직에서 하이브리드 근무를 수용함에 따라 기존 네트워킹 아키텍처는 성능 및 보안 수준 저하라는 문제에 직면하고 있습니다. 트래픽을 백홀링하면 성능과 사용자 경험이 저하되고, 로컬 브레이크아웃을 허용하면 보안 일관성과 효율성이 저하됩니다. 두 경우 모두 바람직하지 않으며 결과적으로 조직과 개인의 요구 사항을 충족하지 못하는 네트워크 설계로 이어집니다.

최근에는 MPLS의 대안을 제공하기 위해 트래픽 관리를 위한 오버레이를 SD-WAN에 추가했습니다. 하지만 SD-WAN은 주로 에지 장치에 의존하여 보안을 구현하므로 팀에서는 하드웨어, 가상화, 클라우드 기반 도구를 짜깁기하여 조합해야 합니다. 복잡성이 증가하면 결과적으로 의도한 많은 이점이 상쇄되고 맙니다.

Cloudflare에서 제공하는 SASE 플랫폼은 클라우드 연결성에 보안과 네트워킹을 통합하여 조직에서 자체 네트워크의 확장으로 활용할 수 있도록 지원합니다. SASE를 향한 진정한 혁신적 접근 방식을 통해서만 간소화된 관리, 안정적인 성능, 최신 Zero Trust 보안, 총소유비용 절감을 모두 동시에 실현할 수 있습니다.

기준	MPLS/VPN 서비스	SD-WAN	SASE 및 Cloudflare One
<b>구성</b> 새로운 사이트 설정, 구성, 관리	서비스 요청으로 MSP에서 제공	중앙화된 컨트롤러를 통한 오케스트레이션 및 관리 간소화	SaaS 포털을 통한 오케스트레이션 자동화, 중앙화된 대시보드
<b>라스트 마일 트래픽 제어</b> 트래픽 밸런싱, QoS, 장애 조치	MPLS SLA에서 보장됨	SD-WAN 장비에서 최적 경로 선택 가능	최소한의 온프레미스 배포로 로컬 의사 결정 제어
<b>미들 마일 트래픽 제어</b> 미들 마일 정체 시 트래픽 조정	MPLS SLA에서 보장됨	“터널 스파게티”와 미들 마일에 대한 제어 불가	동일한 인터페이스에서 트래픽 관리 및 비공개 백본 제어 통합
<b>클라우드 통합</b> 클라우드 마이그레이션을 위한 연결	중앙화된 브레이크아웃	탈중앙화된 브레이크아웃	클라우드 네트워크 상호 연결로 네이티브 연결
<b>보안</b> 맬웨어 검사를 위한 인/아웃바운드 인터넷 트래픽 필터링	짜깁기 형태의 하드웨어 제어	짜깁기 형태의 하드웨어 및/또는 소프트웨어 제어	사용자, 데이터, 애플리케이션, 네트워크 보안 도구와 네이티브 통합
<b>비용</b> 네트워크 투자에 대한 ROI 극대화	하드웨어 및 연결에 대한 높은 비용	하드웨어와 소프트웨어 비용 부담을 덜고 연결 비용 최적화	하드웨어 및 연결 비용 절감으로 ROI 극대화

## Cloudflare의 SASE 플랫폼을 향한 트래픽 유도



Magic WAN Connector를 사용하면 네트워크 위치를 Cloudflare에 쉽게 연결할 수 있습니다. 간단하게 배포하기 위해 Cloudflare에서 인증한 하드웨어 장비에 미리 설치되고 구성된 분기 커넥터 소프트웨어를 사용하거나, 귀사의 환경 내에 있는 물리적 또는 가상의 리눅스 장비에 해당 소프트웨어를 배포합니다.

### 증가하고 있는 유연한 온램프(on-ramp) 제품군의 일부

SASE를 수용하기 위한 첫 번째 단계는 Zero Trust 보안 정책을 적용할 수 있는 가장 가까운 위치까지 귀사의 기존 네트워크를 안전하게 연결하는 것입니다. Cloudflare에서는 이러한 연결을 사용하기 위해 광범위한 “온램프(on-ramp)” 세트를 제공합니다. 여기에는 하이브리드 근무 사용자를 위한 클라이언트 기반 및 클라이언트리스 액세스 옵션, 경량 소프트웨어 커넥터를 배포하여 설정한 애플리케이션 계층 터널, Anycast를 이용한 GRE 또는 IPsec 터널을 통한 네트워크 계층 연결, 비공개 데이터 센터 및 퍼블릭 클라우드를 위한 물리적 또는 가상 상호 연결이 포함됩니다.

SASE 도입을 더 쉽게 수행할 수 있도록 Magic WAN Connector를 모든 물리적 또는 클라우드 네트워크 위치에 배포하여 최적의 Cloudflare 네트워크 데이터 센터에 자동으로 연결할 수 있습니다. 따라서 기존 라스트 마일 인터넷 연결을 활용할 수 있고 IT 팀에서 연결을 위해 네트워크 장비를 수동으로 구성할 필요가 없습니다.

## 소프트웨어 기능 및 하드웨어 사양

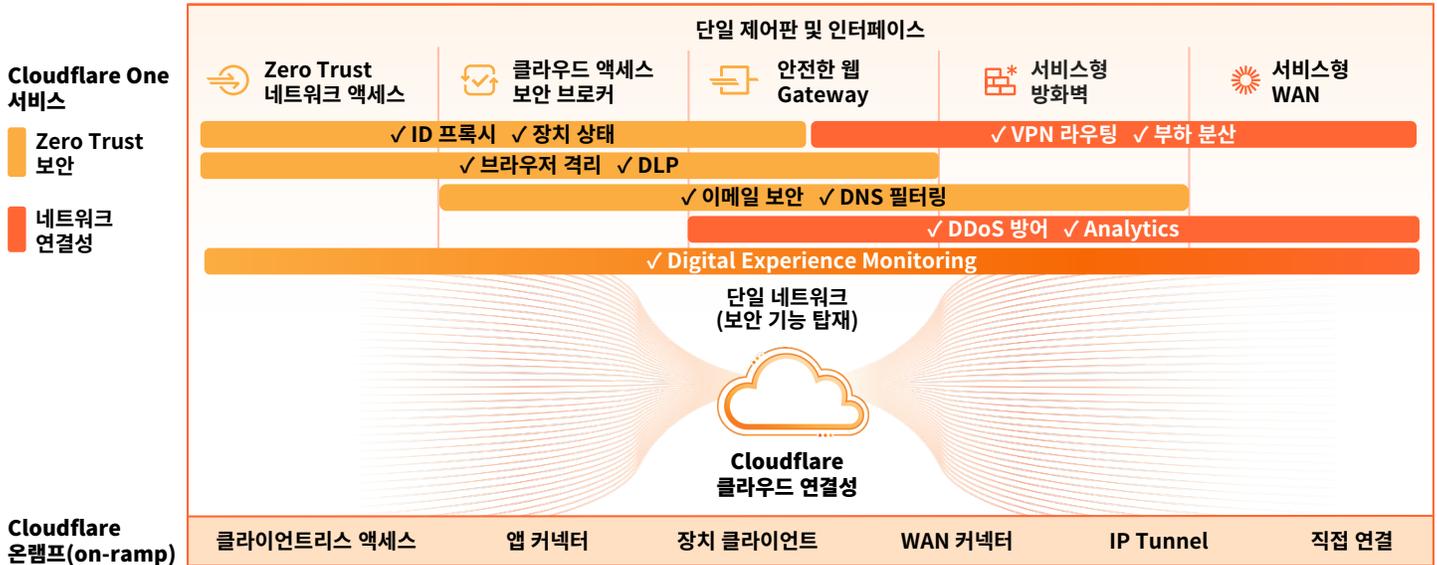
Magic WAN 소프트웨어 기능 <sup>1</sup>	
WAN 커넥터 설정	Cloudflare 대시보드/API를 통해 중앙에서 관리되는 플러그 앤 플레이, 제로 터치 방식 CPE 장치. IPsec 터널과 경로를 자동으로 설정하고 트래픽을 Cloudflare 네트워크로 이동시켜 연결 및 보안 기능을 이용할 수 있습니다. 소프트웨어 자동 업그레이드(고객이 정의한 서비스 기간 내).
WAN 커넥터 사이트 구성	정적 IP 또는 DHCP 구성을 위한 WAN/LAN 지원. VLAN 및 로컬 네트워크 세분화를 위한 지원.
“가벼운 분기, 견고한 클라우드” 접근 방식	상태 점검 기반으로 여러 WAN 회선 전반에 걸친 부하 분산 및 장애 조치 기능을 갖춘 고가용성 경량 WAN 커넥터. Cloudflare의 클라우드 연결성을 통해 제공되는 방화벽 및 Zero Trust SSE 기능 등의 보안 서비스.
타사 통합	Amazon AWS Transit Gateway와 같은 기존 클라우드 VPC 또는 고객 온프레미스 장비(SD-WAN, 방화벽, 라우터 장치 등)로 Anycast IPsec 또는 GRE 터널 엔드포인트를 구성합니다. ECMP 패킷 포워딩을 사용하여 Cloudflare 네트워크로 향하는 정적 경로를 구성합니다.
기본 제공 보안 기능	L3 방화벽 및 침입 감지 기본 제공. L4~7 보안 웹 게이트웨이, 장치 클라이언트, 앱 커넥터 등 온램프(on-ramp) 및 기타 SSE/보안 기능과의 원활한 통합 제공.
가시성 및 제어	앱 기반 트래픽 감지 및 라우팅. 대역폭 제어. 대시보드, API, 로그 또는 GraphQL을 통한 터널, 트래픽 및 장치 메트릭에 대한 가시성/분석. Cloudflare 대시보드, API, Terraform을 통한 관리.
Magic WAN Connector 하드웨어 옵션 사양 <sup>2</sup>	
장치 사양	<ul style="list-style-type: none"> <li>● 포트: (6x 1G Copper RJ45) + (2x 10G SFP+) + (2x USB 3.0 타입 A)</li> <li>● 치수: 8.1x7.9x2.0인치, 1.5RU, 무게: 2.87파운드</li> <li>● 장착 옵션: 데스크톱 배치, 벽면 장착 또는 랙 장착(트레이 포함)</li> <li>● TPM: 2.0, 중국을 제외한 전 세계</li> <li>● CPU: Denverton 4코어 C3558</li> <li>● 드라이브: M.2 120 SSD 및 16G eMMC 플래시</li> <li>● 램: 8GB DDR4</li> <li>● Wi-Fi 및 블루투스: 802.11ac, 2x2 MIMO, 최대 phy 비율: 866.7Mbps</li> <li>● 팬: 1개</li> </ul>

<sup>1</sup> 모든 Magic WAN 기능 수준 문서 참조: [Cloudflare Docs](#)

<sup>2</sup> Magic WAN 소프트웨어가 사전 설치된 Cloudflare 인증 하드웨어: [Dell VEP 1425](#), 파트너를 통해 판매됨(랙 장착 포함)

## 네트워크 연결성 및 SASE 경로

Cloudflare의 클라우드 연결성에서는 포인트 제품을 통합하고 통합 IT 전략으로 융합할 때 앞서 나가는 데 필요한 배포 단순성, 네트워크 복원력, 혁신 속도를 제공합니다.



Cloudflare One을 사용하면 모든 규모의 조직에서 [SASE 전환](#)을 수행할 수 있습니다. 이를 통해 사설 네트워크 또는 공용 인터넷에서 모든 보안 기능이 적용되어 있고 목적지로 향하는 트래픽이 최적화되어 있는 안전하고 빠르고 안정적인 전역 네트워크에 모든 트래픽 소스와 목적지를 연결합니다.

조직에서 성숙한 MPLS 또는 SD-WAN 배포에서 트래픽을 오프로드하거나 처음으로 네트워크 최신화에 접근하는 경우, Magic WAN은 프로세스 간소화에 도움이 될 수 있습니다. Cloudflare One은 Zero Trust 보안과 서비스형 WAN을 모두 제공하여 단일 벤더 SASE를 달성할 수 있지만, 멀티 벤더 전략을 보완하여 귀사의 SASE 여정을 지원할 수도 있습니다.

조직을 위한 네트워크 연결성에 대해 논의할 수 있습니다

워크숍 요청하기



[Cloudflare의 SASE 플랫폼](#)에 대해 자세히 알아보세요