Magic WAN

Magic WAN simplifies the path to SASE with any-to-any connectivity

Evolution of network architectures

The Internet as the new corporate network

With hybrid work as the new normal and apps moving to the cloud, IT teams are grappling with:

- **Network complexity:** MPLS provisioning and adjusting point solutions takes too much time
- **Security gaps:** Direct to internet bypasses security and acceptable use policies, and puts users and data at risk
- **High costs:** MPLS links and security point solutions create unnecessary spend
- **Poor user experience:** Backhauling traffic to a perimeter security stack introduces latency

Magic WAN simplifies network connectivity from branch sites, multi-cloud VPCs, or data centers to the Cloudflare One SASE platform, enabling secure, performant, and cost-effective connectivity to solve hybrid work and multi-cloud challenges for IT teams.

Unlike inflexible, expensive MPLS networking or complex SD-WAN deployments built with on-prem firewalls, Magic WAN uses a "light branch, heavy cloud" approach to augment / replace your current architecture. It's easy to deploy and scales with your changing business requirements, with security built in.

Magic WAN connects physical or virtual network locations to Cloudflare's SASE platform. Examples of physical sites include branch offices, factory floors, retail locations, head offices, or data centers. Examples of virtual locations include public cloud services like AWS, Azure, GCP and OCI.

Better operational agility

Centrally manage network security and connectivity from one admin console. On-ramp traffic in minutes with zero-touch configuration.

Built-in, not bolt-on, security

Get cloud-native DDoS protection, network firewalling, SSE and Zero Trust functionality — all deeply integrated and delivered as-a-service.

Reduced network costs

Minimize your branch footprint and shift network functions to the cloud to reduce reliance on expensive MPLS and migrate off of SD-WAN.

Top use cases for Magic WAN

Streamline network connectivity

- **Simplify branch connectivity** — Replace a patchwork of proprietary circuits and network appliances to securely route traffic between branch offices and data centers. Facilitate site-to-site connectivity across locations with Anycast IPSec.
- **Simplify hybrid and multi-cloud connectivity** — Organizations have apps in cloud instances of different providers (e.g. AWS, GCP, Azure, Oracle, IBM) *and* on-prem data centers. Use centralized controls to route and secure traffic across these varied environments.

Boost security without sacrificing performance

- **Secure WAN connectivity** — Secure connections by enforcing network security policy between locations (branches, data centers, etc.) with cloud-delivered firewall and SWG controls.
- **Scale WAN performance** — MPLS deployments are expensive, inflexible and slow. Switching to Cloudflare enables lower cost, more agile deployment with security built in.

Approaching Magic WAN deployment

Network transformation is a journey

Magic WAN delivers performance and reliability over internet connectivity, and helps organizations migrate from legacy network architectures. Get started by deploying Magic WAN progressively by implementing a transition over time. Cloudflare's "light branch, heavy cloud" combination of last-mile connectivity and middle-mile performance, reliability, and security better helps connect and secure hybrid work. Our architecture supports deployment alongside existing infrastructure to migrate at your pace.

Comparing Cloudflare One to MPLS and SD-WAN

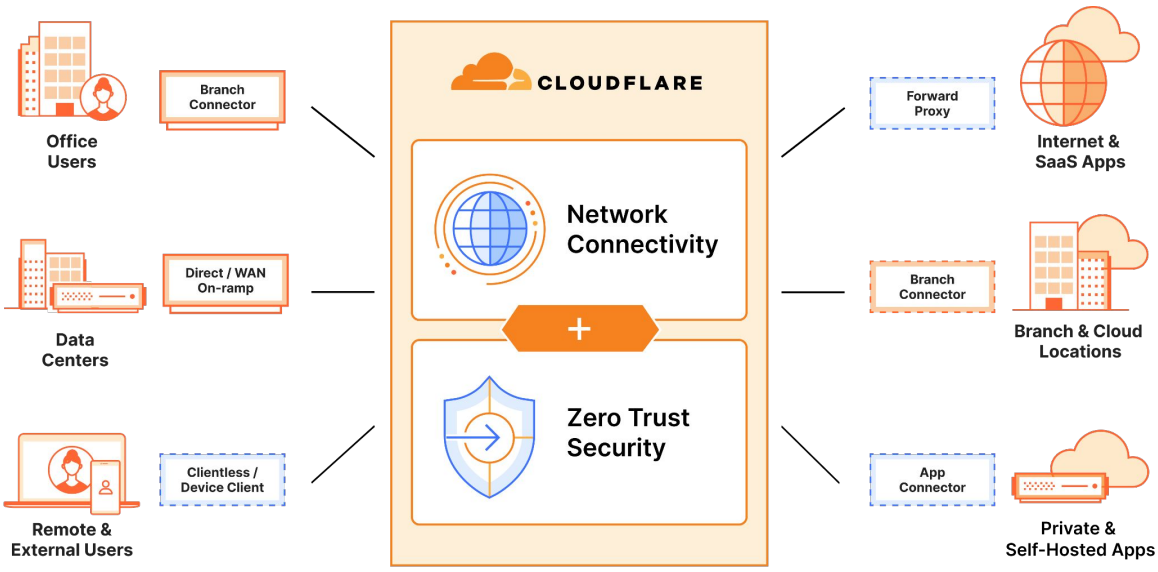
As applications have shifted to the cloud and organizations embrace hybrid work, traditional networking architectures face diminishing levels of performance and security. Backhauling traffic hurts performance and the user experience, while permitting local breakout hurts security consistency and efficacy. Neither scenario is desirable, and as a result, network designs make compromises which leave organizational and individual needs unfulfilled.

More recently, SD-WAN added overlays to manage traffic in hopes of offering an alternative to MPLS. However, SD-WAN largely depends on edge devices to implement security, leaving teams to stitch together a patchwork of hardware, virtualized, and cloud-based tools. As a consequence, the added complexity offsets many of the intended benefits.

Cloudflare's SASE platform converges security and networking in our connectivity cloud and allows organizations to use our network as an extension of their own. Simplified management, reliable performance, modern Zero Trust security, and reduced total cost of ownership are only simultaneously possible with a truly reinvented approach to SASE.

Criteria	MPLS/VPN Service	SD-WAN	SASE with Cloudflare One
Configuration New site setup, configuration & management	By MSP through service request	Simplified orchestration and management via centralized controller	Automated orchestration via SaaS portal; centralized dashboard
Last mile traffic control Traffic balancing, QoS, & failover	Covered by MPLS SLAs	Best Path selection available in SD-WAN appliance	Minimal on-prem deployment to control local decision making
Middle mile traffic control Traffic steering around middle mile congestion	Covered by MPLS SLAs	"Tunnel spaghetti" and no control over middle mile	Integrated traffic management & private backbone controls in same interface
Cloud integration Connectivity for cloud migration	Centralized breakout	Decentralized breakout	Native connectivity with Cloud Network Interconnect
Security Filter in & outbound Internet traffic for malware	Patchwork of hardware controls	Patchwork of hardware and/or software controls	Native integration with user, data, application & network security tools
Cost Maximize ROI for network investments	High cost for hardware and connectivity	Optimized connectivity costs at the expense of increased hardware and software costs	Decreased hardware and connectivity costs for maximized ROI

Steering traffic to Cloudflare's SASE platform



The Magic WAN Connector makes it easy to connect your network locations to Cloudflare. Use the branch connector software pre-installed and configured on a Cloudflare-certified hardware appliance for simplified deployment, or deploy the software on physical or virtual Linux appliances within your environment.

Part of a growing family of flexible on-ramps

The first step to embracing SASE is getting connected - establishing a secure path from your existing network to the closest location where Zero Trust security policies can be applied. Cloudflare offers a broad set of "on-ramps" to enable this connectivity, including client-based and clientless access options for hybrid work users, application-layer tunnels established by deploying lightweight software connectors, network-layer connectivity with Anycast-enabled GRE or IPsec tunnels, and physical or virtual interconnection for both private data centers and public clouds.

To make SASE adoption even easier, the Magic WAN Connector can be deployed in any physical or cloud network location to provide automatic connectivity to the optimal Cloudflare data center, leveraging your existing last mile Internet connectivity and removing the requirement for IT teams to manually configure network gear to get connected.

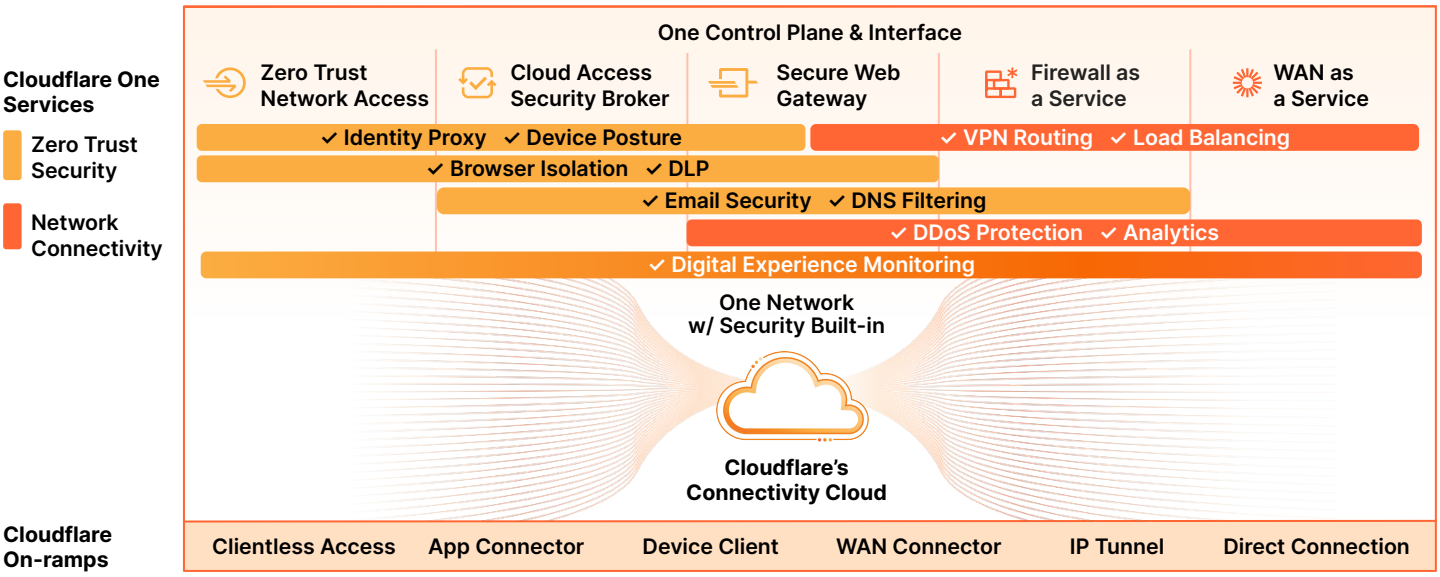
Software capabilities and hardware specifications

Magic WAN software capabilities[1]	
WAN Connector setup	Plug-and-play, zero-touch provisioned CPE device(s) that are centrally managed via Cloudflare dashboard/API. Automatically set up IPsec tunnels and routes to direct traffic to Cloudflare network for connectivity and security functions. Automatic software upgrades (within customer-defined service window).
WAN Connector site configuration	WAN/LAN support for static IP or DHCP configurations. Support for VLANs and local network segmentation.
"Light branch, heavy cloud" approach	High availability lightweight WAN Connector with load balancing and failover across multiple WAN circuits based on health checks. Security services such as firewall and Zero Trust SSE capabilities delivered from Cloudflare's connectivity cloud.
Third-party integration	Configure Anycast IPsec or GRE tunnel endpoints with your existing cloud VPCs like Amazon AWS Transit Gateway or customer-premises equipment such as SD-WAN, firewall, and router devices. Configure static routes with ECMP packet forwarding to the Cloudflare network.
Security built in	Built-in L3 firewall and intrusion detection; seamless integration with other SSE/security capabilities and on-ramps like L4-7 secure web gateway, device client, app connector, etc.
Visibility and control	App-based traffic detection and routing. Bandwidth control. Visibility/analytics for tunnel, traffic and device metrics available via dashboard, API, logs, or GraphQL. Manage using Cloudflare dashboard, API or Terraform.
Magic WAN Connector hardware option specifications[2]	
Device specs	• **Ports:** (6× 1G Copper RJ45) + (2× 10G SFP+) + (2x USB 3.0 Type A) • **Dimensions:** 8.1×7.9×2.0 inches; 1.5RU; **Weight:** 2.87 lbs • **Mounting options:** desktop placement, wall mount, or rack mount (w/ tray) • **TPM:** 2.0, worldwide except China • **CPU:** Denverton 4 Core C3558 • **Drive:** M.2 120 SSD with 16G eMMC Flash • **RAM:** 8 GB DDR4 • **WiFi & Bluetooth:** 802.11ac, 2×2 MIMO, max. phy rate: 866.7 Mbps • **Fan:** One

[1] All Magic WAN feature-level documentation found in Cloudflare Docs
[2] Cloudflare-certified hardware with Magic WAN software pre-installed: Dell VEP 1425 sold through partner (comes w/ rack mount)

Network connectivity and the path to SASE

Cloudflare's connectivity cloud provides the deployment simplicity, network resiliency, and innovation velocity needed to stay ahead as you consolidate point products and converge on a unified IT strategy.



Cloudflare One is enabling organizations of all sizes to make the transition to SASE: connecting any traffic source and destination to a secure, fast, reliable global network where all security functions are enforced and traffic is optimized on the way to its destination, both within a private network or on the public Internet.

Whether your organization is offloading traffic from mature MPLS or SD-WAN deployments or approaching network modernization for the first time, Magic WAN can help simplify the process. Cloudflare One provides both Zero Trust security and WAN-as-a-service to achieve single-vendor SASE, but can also complement a multi-vendor strategy to assist with your SASE journey.

Let's discuss network connectivity for your organization

Request a workshop

CLOUDFLARE

Learn more about Cloudflare's SASE platform