Magic WAN

Simplify 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:** distributed users and personal devices increase risk for corporate data
- **High costs:** MPLS links and security point solutions create unnecessary spend
- **Poor user experience:** Backhauling traffic to enforce security 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 rigid, expensive MPLS networking or bloated SD-WAN deployments built on on-prem firewalls, Magic WAN takes a "light branch, heavy cloud" approach to augment or eventually replace your current architecture. It's easier to deploy, manage and consume 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 interface. 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 or SD-WAN deployments.

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 datacenters. Use centralized controls to route and secure traffic across these varied environments.

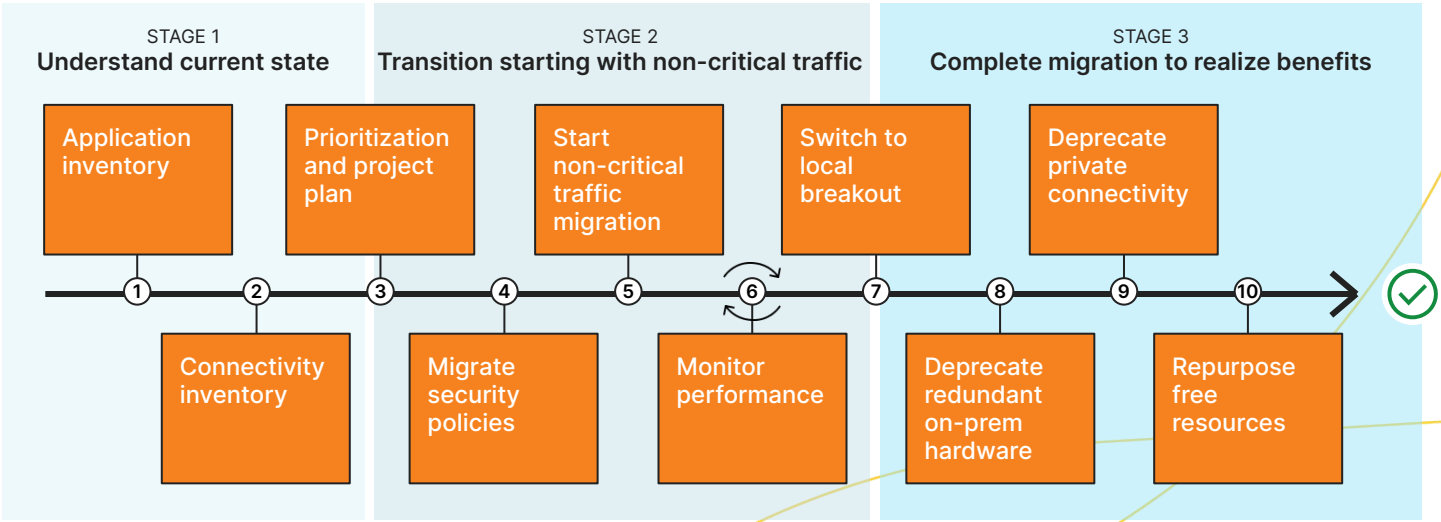
Boost security without sacrificing performance

- **Secure WAN connectivity** — Secure connections by applying filters and inspections for traffic between locations (branches, data centers, etc.) and to/from those locations in/out of the broader Internet by layering on firewalls and SWG controls to WAN.
- **Scale WAN performance** — MPLS deployments have been expensive to build and slow to scale. Removing MPLS and switching to cloud-delivered WAN offers more agile deployment and faster connections, with security built in.

Approaching Magic WAN deployment

Network transformation is a long-term process, with lots of small wins along the way

Magic WAN brings MPLS-like performance and reliability to the public Internet to provide a migration path from legacy network architectures. Start small with a non-critical traffic migration pilot and gradually offload more traffic 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 Internet-native architecture can deploy alongside existing SD-WAN implementations where needed or replace the need for new SD-WAN rollouts entirely.



MPLS and SD-WAN Comparison

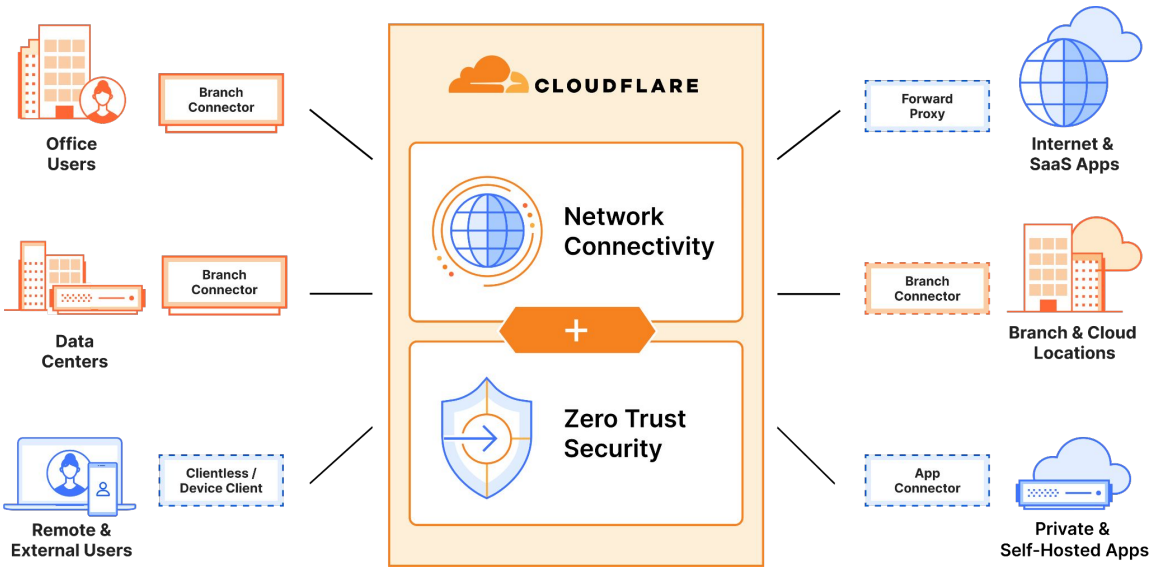
Historically, private MPLS circuits may have provided adequate performance for their time, but configuration is far too cumbersome relying on MSPs, and control requires central breakouts and backhauling all traffic through a patchwork of security appliances. Especially as their cost scales for larger deployments, MPLS can't efficiently serve modern connectivity needs.

More recently, SD-WAN helped improve orchestration pain with intuitive, centralized web interfaces, and smart routing features were implemented locally to make better instant decisions for steering and shaping traffic in the last mile. However, SD-WAN appliances still don't generally have embedded security controls, leaving teams to stitch together a patchwork of hardware, virtualized, and cloud-based tools for coverage. While costs were supposed to decrease with the promise of ending MPLS contracts, organizations typically haven't achieved this either due to new hardware, license, or maintenance costs, or not being able to replace MPLS after all due to SD-WAN's security and reliability shortcomings.

Cloudflare's SASE platform converges security and networking in our connectivity cloud to serve all traffic through a "light branch, heavy cloud" approach, allowing organizations to migrate away from legacy private circuits and 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—which the SASE design architecture aims to be for organizations undergoing digital modernization.

Aspect	Example	MPLS/VPN Service	SD-WAN	SASE with Cloudflare One
Configuration	New site setup, configuration and 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, and 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 still 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

On-ramping traffic to Cloudflare's SASE platform



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

Part of a growing family of flexible on-ramps

The first step to adopting 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 a lightweight software daemon, 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 this first step to SASE even easier, the Magic WAN Connector can be deployed in any physical or cloud network location to provide automatic connectivity to the closest Cloudflare network location, leveraging your existing last mile Internet connectivity and removing the requirement for IT teams to manually configure network gear to get connected.

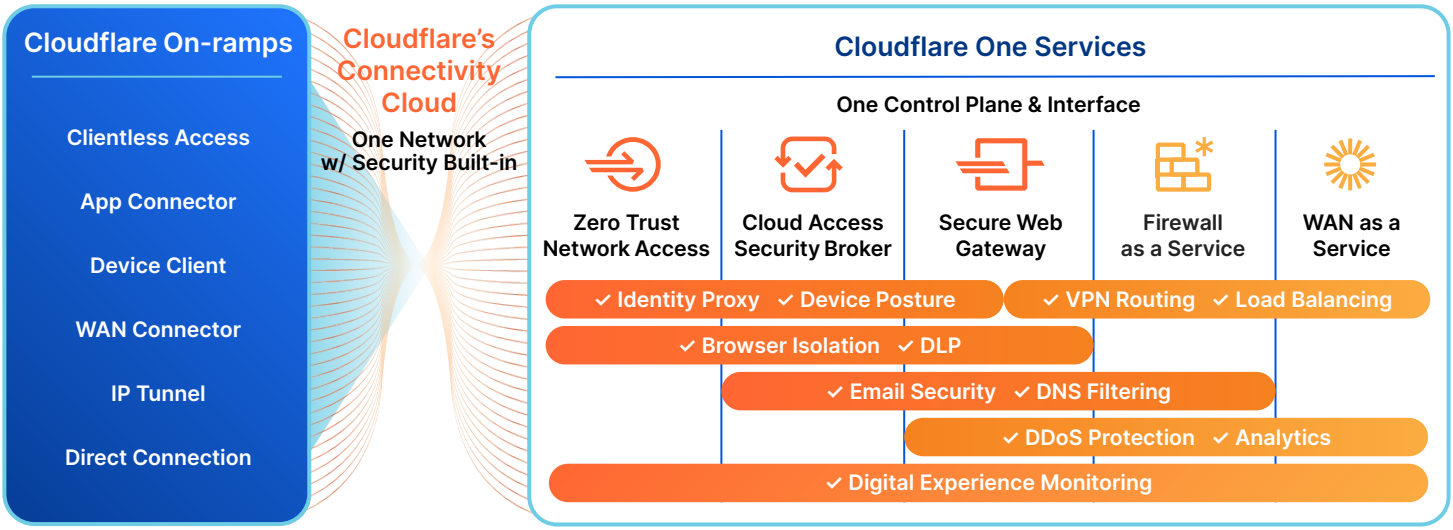
Magic WAN capabilities/specifications

Software capabilities: Magic WAN[1]	
Simple 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 over time.
Site configuration	WAN/LAN support for static IP or DHCP configurations that exist at each site. Support for VLANs and local network segmentation.
"Light branch, heavy cloud" approach	On-prem load balancing and failover across multiple WAN circuits based on health checks. Most resource intensive firewall and SSE capabilities delivered from Cloudflare's connectivity cloud in the middle mile.
Security built in	Built-in firewall and intrusion detection; seamless integration with other SSE/security capabilities and on-ramps like Secure Web Gateway, device client, app connector, etc.
Visibility and control	Control via Cloudflare dashboard, API or Terraform. Visibility/analytics for traffic and device metrics available via dashboard, API, or logs.
Hardware specifications: Magic WAN Connector[2]	
Device specs	• **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 • **Ports:** (6× 1G Copper RJ45) + (2× 10G SFP+) + (2x USB 3.0 Type A) • **Fan:** One • **TPM:** 2.0, worldwide except China • **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)

[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 transformation for the first time, Magic WAN can help you modernize. 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 through its component parts to meet you where you're at in your SASE journey.

Let's discuss network connectivity for your organization

Request a workshop

CLOUDFLARE

Not quite ready for a live conversation?

Keep learning more about Cloudflare's SASE platform