CLOUDFLARE

PRODUCT BRIEF

Magic WAN

Connectivity, security, and performance — delivered as a service to simplify the path to SASE

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.

Figure 1: Magic WAN provides customers on-ramps to connect their physical or virtual network locations to Cloudflare One. 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.

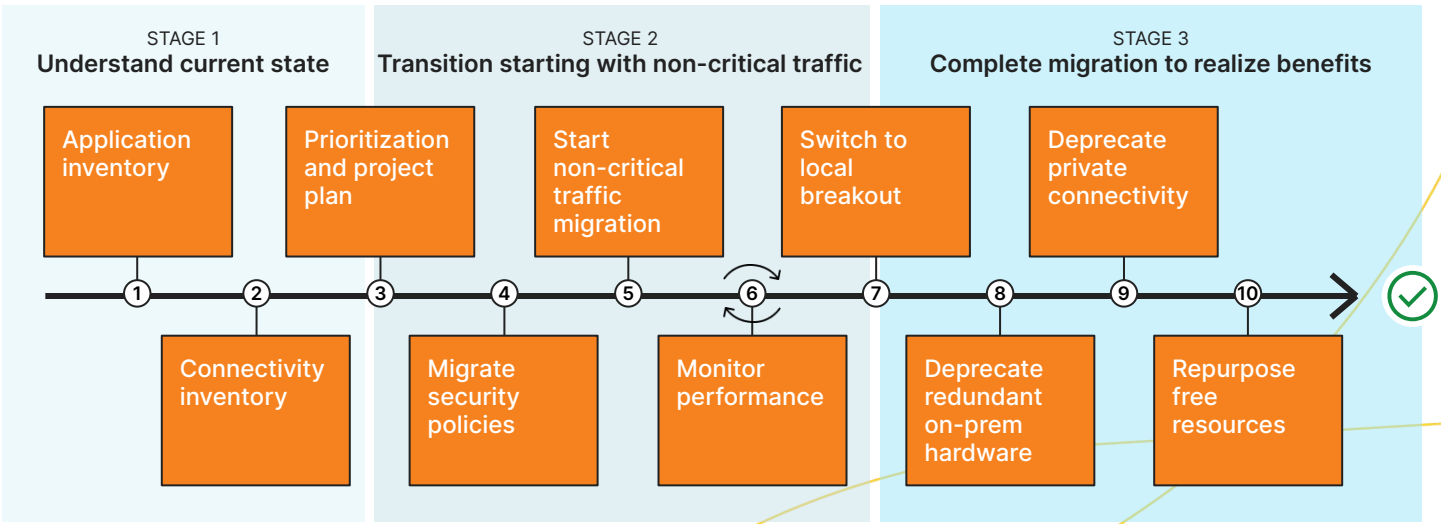
Boost security without sacrificing performance

- **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.



On-ramping traffic to Cloudflare One

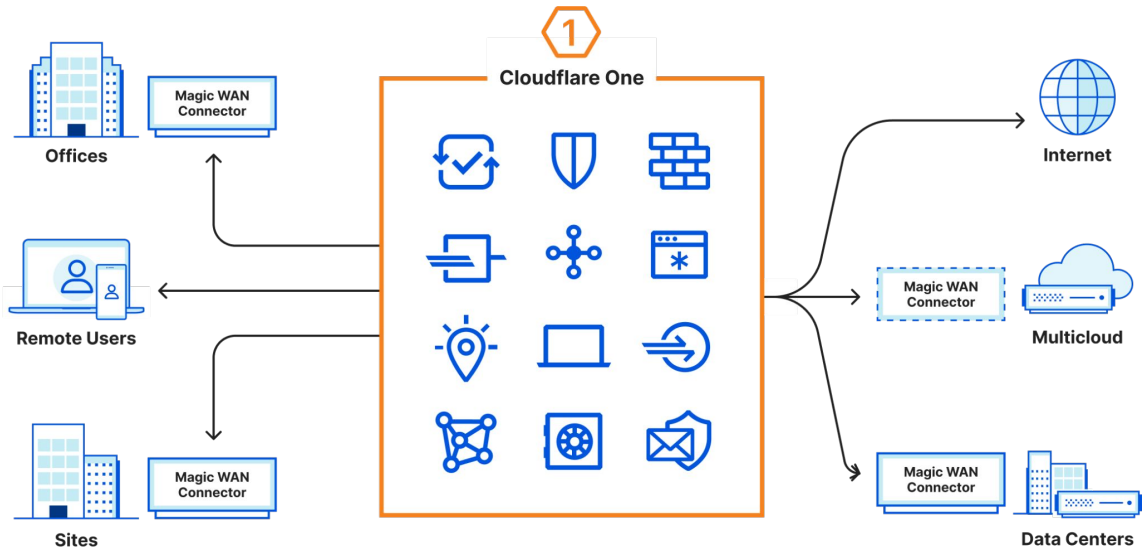
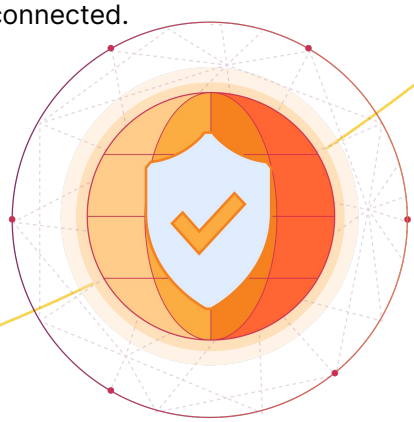


Figure 2: The Magic WAN Connector makes it easy to connect your network locations to Cloudflare. Install the software on physical or virtual Linux appliances that you manage, or purchase it pre-installed and configured on a hardware appliance for the lowest-friction path to SASE connectivity.

Part of a growing family of flexible on-ramps

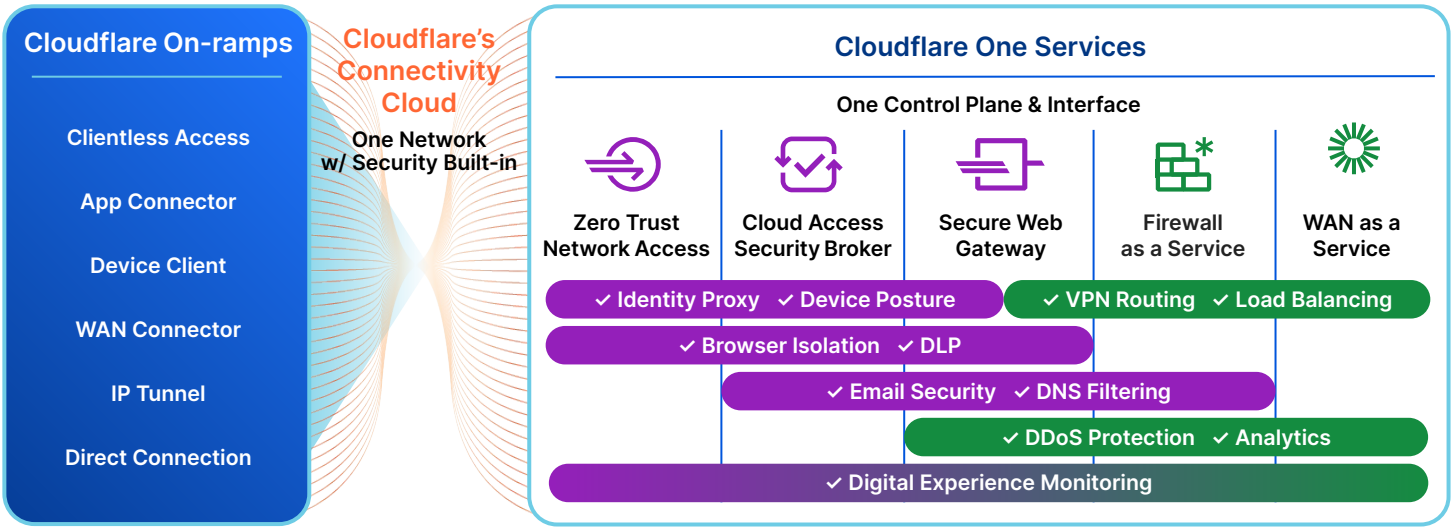
The first step to adopting SASE is getting connected—establishing a secure path from your existing network to the closest location where Zero Trust security policies can be applied. Cloudflare offers a broad set of "on-ramps" to enable this connectivity, including client-based and clientless access options 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.



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.



Zero Trust services: **PURPLE** Network services: **GREEN**

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.

If you're looking to discuss your Zero Trust or SASE roadmap further, **contact us here**.