SPOTLIGHT
Sponsored by: Cloudflare

**As CIOs embrace multicloud, they should ensure that their network is modernized to support the agility, flexibility, elastic scale, and security required by distributed cloud services.**

# Network Modernization: Meeting the Need for Distributed and Secure Cloud Services

*September 2022*

**Written by:** Brad Casemore and Ghassan Abdo

## Introduction

Applications are the lifeblood of digital business and are increasingly distributed across cloud and edge environments. CIOs and CXOs face the challenge of ensuring simplified, consistent, extensible, highly automated network services that deliver robust security across a seemingly infinite distributed cloud landscape of applications and users. The question arises of how enterprises can achieve these objectives considering a challenging multicloud environment that requires modern approaches to networking to and across public clouds, on-premises datacenters, edge environments, and colocation facilities.

### AT A GLANCE

**KEY STATS**

In IDC's *CloudPulse Survey*, conducted in October 2021, only 24% of enterprise respondents indicated that they would focus on a single cloud environment within a two-year time frame, while the other 76% reported that they would pursue variations of a multicloud environment.

This paper explores how software-defined network architectures and cloud network services, which decouple software innovation and feature velocity from underlying hardware infrastructure, help enterprises achieve flexibility, agility, and performance in this new environment.

## Key Trends

Although the network, especially when it's doing its job, is invisible to users, it is imperative to the success of digital business. In fact, given the digital expectations of always-on applications and services, uninterrupted by performance degradation or outages, the network, extending everywhere that matters, is more important than ever. Applications and data depend, and succeed or fail, on the merits of the network.

Cloud has effectively redefined the architecture and infrastructure, as well as the operational model, associated with datacenter networking, and multicloud is driving a need for that transformation to extend across the WAN and edge environments. While it's true that networking has been software defined in the on-premises datacenter and even across the WAN (in the form of SD-WAN), the rise of hybrid and multicloud environments means that the need for intelligent, policy-based network automation, control, and security must become ubiquitous to meet cloud-era demands. In IDC's worldwide SD-WAN survey, respondents overwhelmingly indicated that SaaS and IaaS adoption, as well as their organizations' multicloud strategies, would be increasingly important to WAN technology choices.

In fact, as applications grow in business importance and become increasingly distributed across multiple clouds and edge environments, a business need has arisen for simplified, consistent, extensible, highly automated network services that deliver robust security across a seemingly infinite distributed cloud landscape of applications and users. In addition, enterprises face new requirements for routing traffic expeditiously, reliably, and securely, providing ingresses and convenient on-ramps to and from clouds to mitigate latency, improve availability, and enhance the digital experiences of users.

IDC finds that organizations on their cloud journeys are heavily adopting multicloud IT postures. In IDC's *CloudPulse Survey*, conducted in October 2021, only 24% of enterprise respondents indicated that they would focus on a single cloud environment within a two-year time frame, while the other 76% reported that they would pursue variations of a multicloud environment. Nearly 50% of respondents indicated they would have a multicloud environment that facilitated migration of workloads and data or one in which a single application could run seamlessly across different clouds. Furthermore, in IDC's *Future of Digital Infrastructure 2022 Global Sentiment Survey*, conducted in June 2022, 77% of enterprise respondents agreed that the need for interconnections between public clouds, colocation facilities, and edge/campus sites is changing network designs and compelling enterprises to work with new interconnection partners.

> Cloud has effectively redefined the architecture and infrastructure, as well as the operational model, associated with datacenter networking.

Amid this landscape, specific motivations for multicloud vary. Some organizations report that different applications or use cases are suited to different clouds, while others say they are expressly using multiple IaaS providers to mitigate the risk of lock-in. Still others report that they started their cloud journey with a single IaaS provider but expanded to others for architectural reasons. Sometimes, multicloud adoption is driven by a new application that requires capabilities that are available only at a different cloud provider, and sometimes different teams and departments, operating in parallel, independently select different IaaS providers. Further, some organizations adopt multicloud strategies to gain pricing and negotiation leverage with their primary IaaS provider.

Regardless of the reason, as enterprises execute on their cloud and multicloud strategy, they invariably find that IT infrastructure modernization is both acutely required and highly challenging. While compute and storage infrastructure have largely aligned with software-defined architectures and cloud services, the network too often lagged, not nearly as agile or service oriented as other infrastructure elements.

To an unprecedented degree, CIOs now understand the universal merits of software-defined network architectures and cloud network services, which decouple software innovation and feature velocity from underlying hardware infrastructure. Through this decoupling of hardware and software, organizations are able not only to provide agile network services but also to mitigate supply-chain constraints by gaining the flexibility of having multiple hardware options. This capability is exemplified by the case of virtualized or containerized functions that run on industry-standard hardware platforms and in the use of abstracted management and control planes that run above a standardized hardware-based, data-plane substrate and support the requirements associated with on-demand cloud services.

Nonetheless, IDC continues to find that many CIOs overlook or undervalue network modernization as a requirement in their adoption of multicloud, only to learn belatedly — and often at considerable cost — that network modernization is indispensable to multicloud success. Meanwhile, enterprises that have experienced these problems, or have given the matter greater advance consideration, recognize the need for ubiquitous network transformation.

The rise of cloud-native application architecture, predicated on containers and microservices, will accelerate the shift toward network modernization, exposing further limitations of hardware-defined, overprovisioned, and inflexible approaches to delivering vital network and security services. In cloud-native environments, the network must be just as cloud native as the applications it supports, providing for service choice and customization, elastic scale, extensive programmability, and API-based integrations with related tooling.

A cloud and multicloud network must be aligned closely with the needs of the application, moving at the speed of digital business. As more applications migrate to clouds, the network must adhere to cloud principles. The traditional architectures, infrastructure, and operational methods lack the agility, flexibility, and other cloud attributes that are essential to the cloud era — too brittle, too manual, too slow, and too prone to error to keep pace with continuous digital business. The architecture and infrastructure not only are outdated and complex, unable to support the need for speed demanded by digital business, but also fall short in providing the requisite security, with a fragmented mix of security infrastructure that spawns inefficient and incomplete enforcement chokepoints.

As the preceding points attest, the mandate for cloud-centric network modernization is clear and compelling. What's more, modernization offers a significant array of tangible benefits that impact service delivery and business success.

## Benefits

A multicloud network that is both well defined, through organizational collaboration, and well implemented can deliver a range of cloud-aligned capabilities:

- **On-demand performance.** Like the cloud, a multicloud network should be on demand — provisioned, deployed, and available as needed.
- **Elastic scale.** Just as cloud resources scale up and down automatically as needed, a multicloud network must similarly autoscale in alignment with the requirements of dynamic cloud workloads.
- **Agility and speed.** Traditional network infrastructures and the operational practices that accompany them have become notorious for their lack of agility. A multicloud network, which necessarily supports distributed cloud workloads, must be agile and capable of operating at the speed of digital business.
- **Flexibility and choice.** While always desirable attributes, flexibility and choice have become more important to enterprise IT buyers in the wake of the COVID-19 pandemic and ensuing supply-chain disruptions. Flexibility and choice give organizations the freedom to move quickly and innovate on their own terms, helping achieve business outcomes such as faster service delivery and continual service enhancements.
- **Zero trust cloud security.** Through comprehensive and ubiquitous zero trust security, enterprise IT can ensure that distributed applications and users are proactively protected from threats that endanger service availability and digital experience.
- **Pervasive, real-time observability for faster troubleshooting and remediation and proactive NetOps.** Enterprises pursuing multicloud often encounter a range of visibility challenges, including intermittent or partial visibility across clouds and a variety of blind spots. To speed the process of troubleshooting and remediation and to help IT operations achieve a more proactive approach to availability and performance, multicloud networks must possess pervasive, real-time visibility and observability. This also ensures that control is not sacrificed for agility.
- **Cost savings.** Intelligently automated and resilient, a modern cloud network ultimately ensures that disruptions and outages are minimized, that operations are more efficient and productive, that hardware costs are reduced, and that applications and services need not wait for network infrastructure and operators to get around to manually provisioning, configuring, and supporting traditional hardware-defined architectures and infrastructure.

## Considering Cloudflare

Cloudflare has responded to the need for modern cloud and multicloud networking with a growing array of network, application, and security services that are extending both its use case applicability and its geographic ubiquity.

Cloudflare's network spans 275 cities globally and directly peers with 11,000 other networks, including major internet service providers, cloud services, and enterprises, enabling the company to leverage real-time data across its network and enhance performance for its customers. Its network delivers 155Tbps of edge network capacity, designed to prevent large volumetric DDoS attacks, and delivers responses in 50ms or less for 95% of the global internet population.

Cloudflare's commercial services can be categorized into four main buckets: application services, network services, developer services, and zero trust security services, all underpinned by Cloudflare's network infrastructure and developer products.

Cloudflare's performance and security application services include the following:

- **Application performance:** Caching/CDN, (Anycast) DNS, load balancing, video streaming and delivery (Cloudflare Stream), web content optimization (e.g., image resizing, HTTP/2 prioritization, and full-page optimizations), mobile optimization (mobile SDK), and WAN optimization
- **Application security:** DNSSEC; Layer 3 (L3)/L4 DDoS protection; SSL/TLS; bot management; L7 DDoS protection; web application firewall; IoT security, rate limiting, and perimeter security; DNS firewall; and API/page shield (launched in 2021)

Cloudflare One is Cloudflare's latest platform that supports a unified SASE architecture. Cloudflare One comprises:

- Composable SSE platform that supports secure access, SaaS security, email security, internet gateway, browser isolation, and data loss prevention
- Network-as-a-service offering that consists of Magic WAN, Magic Firewall, and Magic Transit

Cloudflare's network services include firewall as a service (FaaS), reverse proxy-based L3 and L4 DDoS protection, WAN as a service (WANaaS), and Network Interconnect, enabling both public and private IP connectivity between datacenters, branch offices, and partner sites.

Cloudflare's performance, security, and network services are underpinned by the company's Argo Smart routing solution. Argo Smart routing intelligently routes the traffic around the network with reduced latency and increased reliability. Smart Tiered Cache, also part of Argo, leverages the same performance and routing data to dynamically search upper-tier datacenters for an origin.

Cloudflare's Workers platform, based on isolated serverless architecture, is the vendor's flagship developer suite. With Cloudflare Workers, developers can build serverless applications that scale without needing to spend time and effort on infrastructure or operations.

The company provides services that range from implementation and integration to support and consultation. It has global 24 x 7 "follow the sun" support centers in the following locations: San Francisco, Austin, Kirkland, London, Lisbon, Munich, Singapore, and Japan. Self-service portal customers receive support via email (Free, Pro, and Business plans) and chat (Business plan only). Feedback surveys, sent after support tickets are closed, are used to measure customer satisfaction.

Cloudflare's go-to-market model is mostly client direct, although the company also sells through partners where it makes sense. It typically segments its customers by strategic, field, midmarket, and SMB and aligns sales/go-to-market resources with the unique delivery, security, and IT infrastructure needs of those segments. Cloudflare's bandwidth alliance initiative showcases the company's approach to collaborating with other cloud providers to grow the Cloudflare customer base. Cloudflare is very much focused on expanding its OEM partnerships, such as those it has with IBM, Rackspace, and Acquia. The vendor works with major cloud providers, colocation providers, and global carriers (of which the majority are in the Americas) to expand its capacity and improve interconnectivity for its customers. The vendor is committed to sustainability initiatives such as building a green internet and reducing emissions, although no tangible goals are currently available.

### Challenges

Although Cloudflare has been on a strong growth path since its IPO, it faces several challenges:

- It needs to improve and enlarge the breadth of media delivery services. Considering the ever-increasing impact of video traffic on the internet, Cloudflare will want to be better positioned in this segment with advanced media delivery services, including content protection such as DRM.
- Cloudflare has successfully grown its network and capacity in past years, but it needs to create more awareness of how this has bolstered performance and reliability of its video streaming services and how it intends to continue this investment focus going forward.
- The company can benefit from expanding its channel business to complement its direct sales effort. A programmatic approach to partner management will drive further growth opportunities for Cloudflare.
- Cloudflare is growing its business at a rapid pace. It needs to invest in the right quality and quantity of resources to keep up with its success and maintain momentum.

## Conclusion

Properly understood, digital transformation has yielded an increased emphasis on digital business. Applications, especially those that facilitate meaningful engagement with users, are the lifeblood of digital business. That said, applications depend on a digital nervous system that takes the form of a modern network, capable of delivering robust and scalable network and security services across an increasingly complex and distributed landscape.

For the reasons explored in this paper, enterprises across industries and geographies increasingly recognize that networks cannot be left unchanged amid transformations of digital infrastructure. Provided that Cloudflare can continue to develop its portfolio in lockstep with evolving customer requirements, IDC believes the company can play a valuable role in helping enterprises modernize their network architectures, infrastructure, and operational models to meet the needs for digital agility, flexibility, performance, reliability, scale, and pervasive security.

# About the Analysts

| | |
|---|---|
| | ***Brad Casemore,*** *Research Vice President, Datacenter and Multicloud Networks*<br>Brad Casemore is IDC's Research Vice President, Datacenter and Multicloud Networks. He covers datacenter network hardware, software, IaaS cloud-delivered network services, and related technologies, including hybrid and multicloud networking software, services, and transit networks. Mr. Casemore also works closely with IDC's Enterprise Networking, Server, Storage, Cloud, and Security research analysts to assess the impact of emerging IT and converged and hyperconverged infrastructure. |
| | ***Ghassan Abdo,*** *Research Vice President, Worldwide Telecom, Virtualization, and CDN*<br>Mr. Abdo, Research Vice President in the Telecommunications group, covers the evolution of the telco cloud ecosystem as well as the emerging virtualized enterprise networking services. His primary focus areas include service provider SD-WAN and managed services and emerging NFV-based virtual networking services as well as other managed WAN services. |

## MESSAGE FROM THE SPONSOR

### More About Cloudflare

Cloudflare has built a global cloud platform that delivers a broad range of services — making organizations more secure, enhancing the performance of their applications, and eliminating the cost and complexity of managing individual network hardware. This platform serves as a scalable, easy-to-use, unified control plane to deliver security, performance, and reliability across on-premises, hybrid, cloud, and software-as-a-service (SaaS) applications.

Crucially, every data center in Cloudflare's 275+ city global network can deliver every one of these services, reducing the latency that can complicate cloud implementations. Streamline your network stack, accelerate transformation, and arm your network for what comes next.

Learn more at www.cloudflare.com/cloudflare-one/

IDC Custom Solutions

The content in this paper was adapted from existing IDC research published on www.idc.com.

**IDC Research, Inc.**
140 Kendrick Street
Building B
Needham, MA 02494, USA
T 508.872.8200
F 508.935.4015
Twitter @IDC
idc-insights-community.com
www.idc.com

**This publication was produced by IDC Custom Solutions.** The opinion, analysis, and research results presented herein are drawn from more detailed research and analysis independently conducted and published by IDC, unless specific vendor sponsorship is noted. IDC Custom Solutions makes IDC content available in a wide range of formats for distribution by various companies. A license to distribute IDC content does not imply endorsement of or opinion about the licensee.

External Publication of IDC Information and Data — Any IDC information that is to be used in advertising, press releases, or promotional materials requires prior written approval from the appropriate IDC Vice President or Country Manager. A draft of the proposed document should accompany any such request. IDC reserves the right to deny approval of external usage for any reason.