White Paper

The Future of Enterprise Networking: Agile Connectivity for the Multicloud and AI Era

Sponsored by: Lumen

Courtney Munroe
March 2026

IDC OPINION

From the edge to the cloud, enterprises are significantly transforming their networking infrastructure. AI training and inferencing are driving exponential traffic growth across the entire networking fabric. Continued adoption of hybrid and multicloud networking demands agile, intelligent connectivity deployment that is secure, scalable, and, most importantly, meets demanding performance and resiliency requirements.

AI and data analytics, followed by security and cloud services, are dominating current enterprise IT spending. The corresponding network challenges are all related to these technologies. According to recent IDC research, the top 3 networking challenges for enterprises in 2025 are network security, network reliability and resiliency, and the alignment of network infrastructure to optimize AI application performance.

March 2026, IDC #US54428626

FIGURE 1

Top 3 networking challenges in 2025

n = 758

Source: IDC's 2025 Future Enterprise Connectivity Survey, August 2025

Enterprises are on a transformation journey, implementing digital infrastructure. Cloud environments are anchoring this, with the flexibility of scaling up or down. Aligning network resources to specific applications and performance is paramount.

IN THIS WHITE PAPER

In this paper, IDC explores the future of enterprise networking and the importance of connectivity as a critical element of enterprise IT infrastructure to enable successful business outcomes. This paper discusses the role of existing and emerging technologies, including VPNs, Ethernet, and high-capacity IP internet services, to meet the complex networking requirements of cloud and AI-driven workloads.

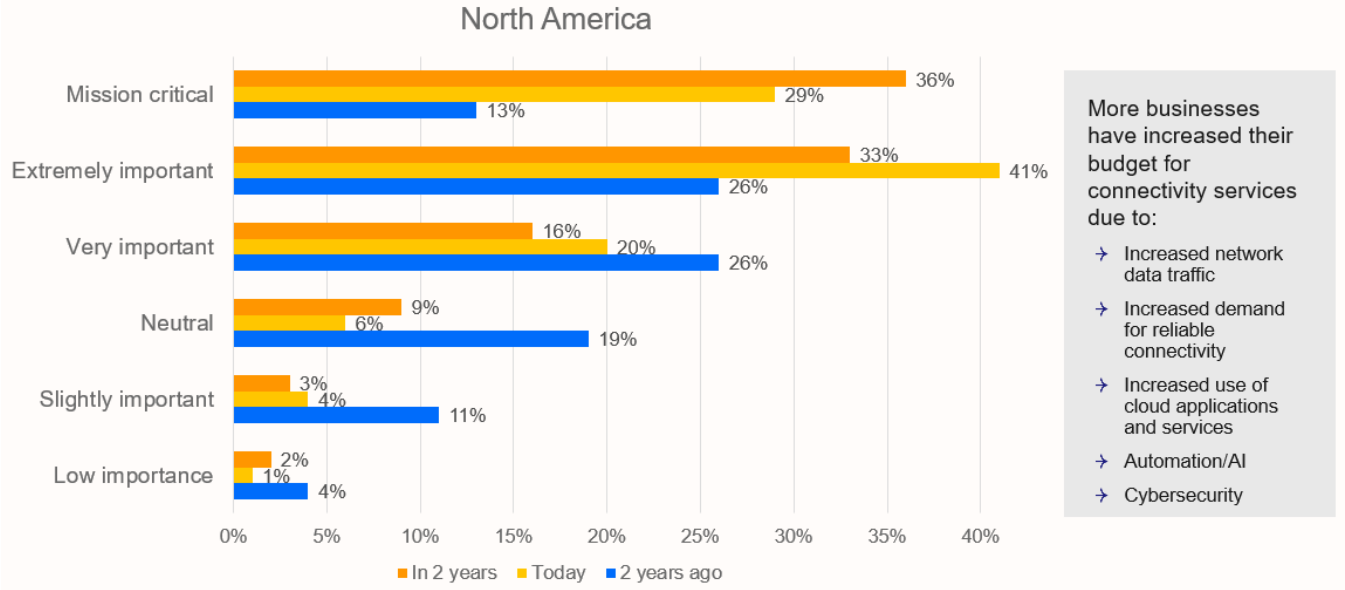
IDC also offers key considerations for selecting a connectivity service provider to facilitate a future-proof road map for scalable, reliable connectivity across the entire enterprise landscape, spanning datacenters, campuses, and remote environments.

SITUATION OVERVIEW

Figure 2 illustrates the major trends transforming the way enterprise networks are designed and managed.

FIGURE 2

Seventy percent of North American businesses now see connectivity as a top priority



n = 758

Source: IDC's Future Enterprise Connectivity Infrastructure and Services Survey, August 2025

Shift to hybrid and multicloud architectures

Static legacy networking is no longer sufficient. According to IDC's research, most cloud buyers use more than one provider, and many are already combining the use of different cloud platforms. According to IDC's *1Q25 Cloud Pulse Survey* (June 2025), 90% of cloud buyers are deploying a hybrid cloud or are in the process of operating one, and 84% are already using multiple cloud providers.

Modern networks must seamlessly connect cloud, edge, branch, and datacenter environments. This requires the selective adoption of VPNs, Ethernet, and internet networks for always-on, mission-critical workloads.

There are many benefits to using multiple cloud platforms, including the avoidance of vendor lock-in, flexibility in managing egress costs, and assistance with regional compliance and data sovereignty issues. Additionally, the ability to optimize performance and implement resilience and innovation by using best-of-breed services from multiple providers is crucial. Please refer to the Lumen-sponsored IDC White paper *Multicloud Gateway: A New Paradigm for Agile Enterprise Cloud Networking* (IDC #US53966725, December 2025) for more information.

The impact of AI, edge computing, multicloud, and distributed environments

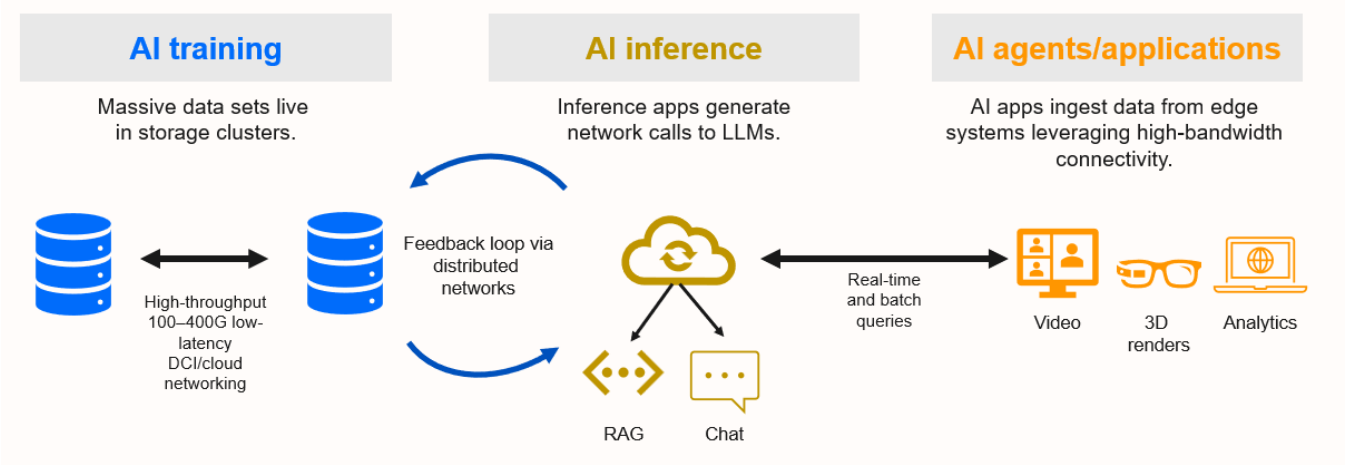
The proliferation of devices and data at the edge, combined with low-latency requirements, demands a network configuration capable of handling diverse and dynamic traffic flows. Edge devices can continuously produce large volumes of data (e.g., video streams, telemetry, and analytics). There is a higher aggregate bandwidth demand on local networks and backhaul links, especially for real-time applications such as video analytics or AR/VR. Applications such as autonomous driving, remote surgery, and industrial automation as well as AI agents require sub-millisecond latency, which means networks must support ultra-reliable, low-latency communication. Over the next few years, this trend will dramatically increase local bandwidth requirements and shift traffic patterns toward distributed architectures, with the corresponding demand for high-performance, low-latency connectivity. The integration of AI/ML model training and inference means enterprises must optimize traffic flows and performance while managing the costs and efficiency of networking across diverse cloud and premises environments.

AI workloads are highly data intensive and place significant demands on networks across three dimensions:

- AI training involves moving massive data sets, often petabytes in size, from storage clusters to GPU farms. Distributed training across thousands of GPUs requires ultra-high-throughput, low-latency east–west traffic, prompting cloud providers to redesign backbone networks with faster fabrics (currently up to 400G and soon to expand to 800G and beyond). Larger models also drive more frequent data set refreshes and inter-regional transfers.
- AI inference generates sustained network traffic rather than short bursts. AI assistants and retrieval-augmented generation systems make frequent API calls to inference clusters, while real-time applications, such as translation, AI chatbots, computer vision, and autonomous operations, demand predictable low latency.
- AI-powered applications and agents ingest data from operational systems as well as devices such as edge sensors, cameras, and industrial assets, and often produce large outputs, such as real-time analytics, synthesized video, or 3D renderings, further amplifying bandwidth and connectivity requirements.

FIGURE 3

Impact of AI workloads on connectivity environments



Source: IDC, 2026

Adoption of consumption-based models (network as a service)

Enterprises are moving away from static and inflexible services to on-demand networking models. The shift to consumption-based connectivity, or network as a service (NaaS), marks a fundamental change in the delivery and consumption of networking. Instead of investing in fixed, hardware-centric infrastructure and subscription-oriented connectivity contracts, enterprises now access networking capabilities, such as bandwidth, security, and routing, through on-demand pay-as-you-go models. Driving this evolution are cloud adoption, distributed applications, and the need for agility, automation, and cost efficiency. NaaS leverages software-defined architectures and API-driven orchestration to provide elastic bandwidth, enabling rapid provisioning and dynamic scaling across hybrid and multicloud environments. By abstracting physical infrastructure into flexible virtual services, NaaS transforms networking into a cloud-like experience, aligning with modern digital business requirements.

Heightened focus on security, resilience, and observability

As networks become more distributed and dynamic, maintaining visibility and mitigating growing threat surfaces are critical priorities. Security, network redundancy, and observability have become the three foundational pillars shaping modern enterprise connectivity strategies. As applications and AI workloads migrate to the cloud, enterprises must embed security directly into the network fabric through zero trust, SASE, and

distributed enforcement points, ensuring consistent protection across all locations and paths.

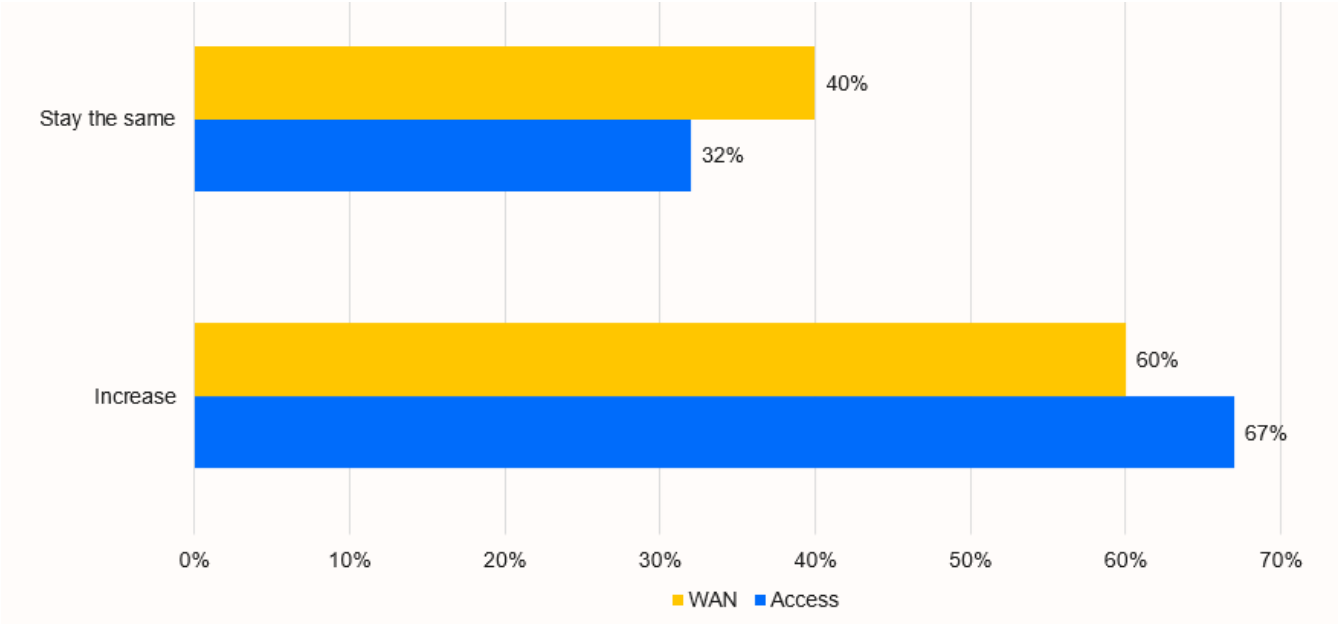
At the same time, redundancy is now essential for maintaining always-on access to mission-critical SaaS, cloud platforms, and AI inference services, driving the adoption of diverse access circuits, dual-cloud on-ramps, and active/active SD-WAN architectures. Finally, organizations require deep observability to monitor increasingly complex user-to-cloud traffic flows, enabling real-time performance insights, dynamic routing decisions, and faster root-cause identification across the internet, WAN, and cloud domains. Together, these elements push enterprises toward cloud-first, resilient, secure, and insight-driven connectivity architectures that deliver predictable performance and stronger business continuity.

FUTURE OUTLOOK

Faster speeds, greater intelligence, and deeper integration with cloud and AI ecosystems are defining the future of network connectivity. Connectivity will evolve from a reactive, static transport layer into a dynamic fabric that enables predictive, autonomous and self-optimizing capabilities. This will enable flexible upgrades and personalization at scale by leveraging models trained on operational data to continuously improve network performance.

FIGURE 4

Q. How will overall network bandwidth (access and WAN) change over the next year?



n = 500

Source: IDC's 2025 Enterprise Communication Services Survey, November 2025

Enterprises will increasingly rely on cloud-native connectivity models such as SD-WAN, SASE, and private 5G to deliver secure, flexible access from anywhere, migrating from legacy WAN architectures. Edge computing will expand, bringing compute and inference closer to users and devices, which will reduce backhaul traffic and require dense fiber buildouts and high-capacity metro networks.

On the infrastructure side, operators will accelerate the adoption of 400G/800G transport, terabit-scale switching, and programmable optical networks to meet exponential bandwidth demand.

Connectivity requirements will shift toward outcome-based services: zero-downtime guarantees and integrated security performance offerings. The network will become more autonomous, self-healing, and application-aware, capable of adjusting to load, security threats, and performance requirements in real time. Connectivity will become **high speed, ubiquitous, intelligent, secure, and cloud integrated**, serving as the foundational platform enabling AI-driven enterprises, immersive experiences, automation, and the digital economy.

Enterprises will redefine how they measure network value. It is no longer about raw bandwidth; instead, it is about how the network enables business agility, supports remote and edge operations, and powers emerging AI workloads.

CHALLENGES/OPPORTUNITIES

- **Digital transformation complexity in the hybrid/multicloud era:** Managing a diverse range of legacy and modern connectivity protocols, devices, and requirements, including hybrid private and public cloud environments, is complex. Establishing a roadmap within a transparent, holistic ecosystem is difficult. The shift from centralized datacenters to distributed hybrid and multicloud workloads has disrupted traditional perimeter security models and complicated traffic routing, identity control, and policy enforcement. Multicloud adoption introduces inconsistent architectures, varied security controls, and fragmented connectivity models, making it difficult to deliver uniform performance and governance across different cloud environments.
- **Balancing legacy/modern connectivity infrastructure:** Many organizations still depend on static WANs with inflexible provisioning and therefore lack scalability and adaptability. However, emerging models, such as NaaS, with integrated wireless solutions for backup and redundancy, offer an alternative to gain cloud-like flexibility.
- **Capacity and performance demands of AI-driven workloads:** AI training and inferencing require significant networking capacity and high-performance access to cloud and datacenter environments, making them critical for successful business outcomes. AI inference traffic requires low-latency, high-reliability connectivity, while

distributed ML pipelines demand secure, high-bandwidth data transport across regions and clouds. Finally, enterprises struggle with cost control. Managing cloud egress fees, redundant circuits, security tools, and rising operational complexity can be addressed with a multicloud gateway solution. Together, these challenges force enterprises to rethink networking as an integrated, cloud-native, secure, and intelligence-driven fabric rather than a collection of isolated technologies.

- **Security and compliance:** Distributed architectures expand the attack surface, reduce visibility, and expose enterprises to new threat vectors as security threats grow more sophisticated. As connectivity becomes more distributed, network-level security plays a foundational role by embedding protection directly into the connectivity layer, enabling faster threat detection and response across the digital infrastructure, reducing complexity, delivering cleaner traffic, and strengthening overall resilience by working to stop threats before they reach customer environments. On top of this foundation, Zero trust mandates continuous identity verification, encryption, segmentation, and deep visibility into user behavior, requirements that place new burdens on network design and operations. Integrating SASE/SSE platforms with existing SD-WAN and cloud environments proves challenging due to overlapping functions, vendor sprawl, and operational skills gaps. Ensuring consistent policy enforcement across remote workers, branch offices, cloud workloads, and edge locations remains difficult. Meanwhile, distributed application flows reduce visibility, making observability tools essential yet often underutilized. A managed solution from a competent partner can help mitigate these challenges.
- **Skills gaps:** Networking teams require expertise in automation, software-driven networking, and cloud integration — skills that are increasingly difficult to manage — and look to connectivity partners for expertise, a future-proof road map, and easier-to-use offerings.
- **Cost pressures:** As companies seek to increase the ROI of networking investments within their IT budget constraints, NaaS is a viable option. Unfortunately, many organizations are not familiar with the cost benefits of NaaS, which is relevant for on-demand networking in the AI era. The ebb and flow of AI workloads brings a degree of unpredictability as companies scale up and reduce resources as necessary for AI networking. However, while this flexibility offers optimized efficiency for bandwidth utilization, it is different and unfamiliar compared to the static and predictable subscription model of legacy networking architectures. NaaS and multicloud-optimized networking solutions reduce the complexity and costs of legacy networking and the inefficient and costly routing between public cloud environments.

CONCLUSION

Modern digital enterprise infrastructure requires secure, high-capacity bandwidth and connectivity that can be rapidly deployed and scaled as needed. AI workloads have introduced the need for reliable, low-latency connectivity in core and edge environments. Most companies rely on multiple cloud environments, and hybrid multicloud networking is an essential aspect of enterprise networking.

Distributed networking across disparate sites also adds to the complexity, and choosing the right networking partner that offers a diverse range of solutions is essential. Ideally, enterprises require a partner that can offer simplified multiservice capabilities on a single multiservice port, with a secure, scalable, and redundant platform.

ABOUT LUMEN

Lumen connectivity customer solution area (CSA) offers high-performance, scalable services that connect locations, datacenters, and clouds quickly and reliably. The company designed its platform for next-gen agility across its physical infrastructure, North America's largest ultra-low-loss intercity fiber network. With several connectivity services backed by a 99.99% service availability SLA, you can confidently support modern apps and continuity.

Lumen offers a broad range of meshed and point-to-point networking services, including Ethernet and IP networking services and IP VPNs. As companies increasingly use multicloud infrastructure, Lumen's Multi-Cloud Gateway portfolio offers significant benefits to optimize networking resources while reducing the complexity of management. Lumen's ubiquitous up-to-400G-enabled backbone network offers on-demand networking capabilities for rapid deployment. This includes scalable capacity based on its national fiber and broadband infrastructure, which includes a service provider colocation network of over 2,200 datacenters and 125+ cloud on-ramps.

Lumen's solutions support various types of challenges.

Scenario: managing the complexity of modern enterprise networking

- **Challenge:** Organizations need to overcome the complexity of managing an enterprise networking infrastructure that meets the diverse secure connectivity requirements for corporate datacenters, campus environments, and remote locations.
- **Solution:** Lumen IP VPN, IP VPN On-Demand, Ethernet, and Ethernet On-Demand deliver high-speed, low-latency connectivity between datacenters, public and private cloud platforms, and enterprise locations. These services can be available via multiservice ports provisioned via a next-generation network architecture that enables the creation of secure, high-performance network meshes with full control over

endpoints and participants. It spans multiple connectivity configurations (e.g., Ethernet and IP networking) while providing dynamic management of bandwidth, latency, load balancing, and redundancy. Powered by APIs and advanced routing protocols, Lumen Connectivity Fabric delivers programmable, resilient connectivity tailored for modern digital ecosystems.

Scenario: facilitating AI workloads

- **Challenge:** Transporting massive amounts of data for AI model training and inferencing is critical for enterprise business success, but it requires costly, low-latency, high-bandwidth capacity.
- **Solution:** Lumen offers high-speed, scalable Ethernet and internet services on a single port, enabling AI readiness by providing dynamic bandwidth allocation and seamless integration with major cloud providers. Lumen's 340,000–route mile network with direct access to 163,000 buildings, and over 2,200 third-party datacenters with a capacity of over 350Tbps, delivers these services. The network currently has over 100,000 miles of up-to-400G-enabled route miles, with 1.26 petabytes of capacity at over 300 locations across 25 metro markets, including 70+ datacenters.

Scenario: hybrid multicloud networking

- **Challenge:** Traditional multicloud networking depends on a hodgepodge of proprietary cloud infrastructure with diverse policies, inefficient and expensive routing, and the use of risky public internet circuits.
- **Solution:** Lumen’s Multi-Cloud Gateway provides a unified, virtual routing service that enables **quick, secure, and effortless connections** between multiple clouds and enterprise sites. It delivers cloud-like agility for the network, such as provisioning in minutes, scaling on demand, and integrating with cloud provider networks, all on a private, high-performance fabric. This allows organizations to focus on innovation and growth instead of managing complex network plumbing.

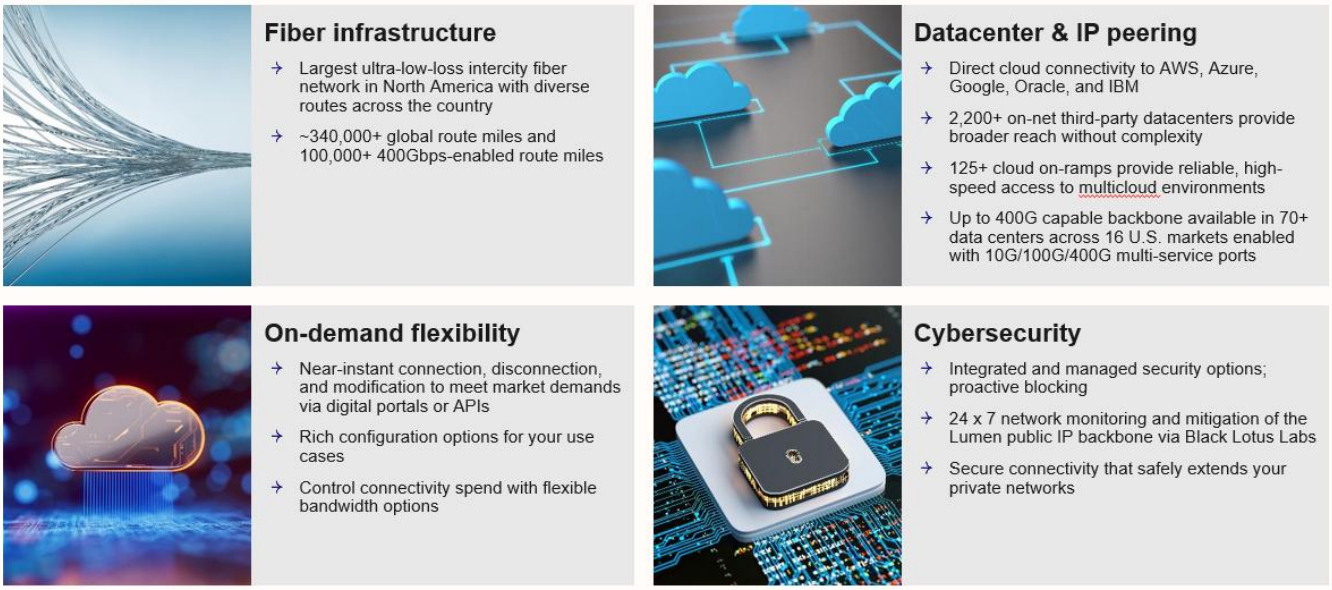
FIGURE 5

Lumen connectivity portfolio

Source: IDC, 2026

FIGURE 6

Why Lumen?



Source: Lumen

ABOUT IDC

International Data Corporation (IDC) is the premier global market intelligence, data, and events provider for the information technology, telecommunications, and consumer technology markets. With more than 1,300 analysts worldwide, IDC offers global, regional, and local expertise on technology and industry opportunities and trends in over 110 countries. IDC's analysis and insight help IT professionals, business executives, and the investment community make fact-based technology decisions and achieve their key business objectives.

Global headquarters

One Beacon Street
Suite 33100
Boston, MA 02108
USA
508.872.8200
X: @IDC
blogs.idc.com
www.idc.com