White Paper

Multicloud Gateway: A New Paradigm for Agile Enterprise Cloud Networking

Sponsored by: Lumen Technologies

Jitesh Bhayani
December 2025

IDC OPINION

Modern distributed enterprise and digital platforms utilize a complex configuration of hybrid and proprietary cloud environments.

Digital transformation that includes the deployment of AI models and AI-enabled applications requires a modern approach to distributed networking. AI models operate across multiple interconnected datacenters, edge locations, and public cloud environments, which requires the flexibility and agility of a scalable, high-performance, and low-latency network infrastructure. Managing this complex environment in a hybrid and multicloud configuration has become the norm.

According to IDC research, most cloud buyers leverage 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.

There are many benefits to leveraging 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 leveraging best-of-breed services from multiple providers is crucial. Another key issue is the agility of edge computing. Deploying workloads closer to end users and points of consumption offers reduced latency and enhanced performance, ensures high availability, and delivers the agility of a scalable, future-ready, and flexible IT infrastructure.

Despite the multiple benefits of leveraging multicloud platforms, there are also many challenges. Public cloud providers prioritize intraplatform networking. Thus, a major challenge for many organizations is finding service providers that can facilitate efficient

December 2025, IDC #US53966725

multicloud networking capabilities. This includes implementing cost-effective routes that minimize cloud egress costs, delivering seamless interoperability, and simplifying the management of proprietary cloud environments.

Implementing a multicloud gateway (MCGW) or cloud routing solution can help address these challenges by reducing complexity. Additionally, optimized routing and performance that is secure and rationalizes costs can deliver a lower long-term total cost of ownership.

IN THIS WHITE PAPER

This white paper examines the key drivers behind implementing multicloud networking and the strategic challenges enterprises face in evolving their networks, leveraging complex AI-enabled distributed workloads, which include:

- The varying technologies and integration points lead to complexity in managing multicloud networks.
- The costs of the dedicated hardware, data center resources, and personnel expertise necessary for legacy and proprietary networking and cloud infrastructure are high.
- Inefficient routing between cloud platforms leads to performance limitations, including high latency and lag.
- Legacy networks require weeks or months to scale up and static financial commitments, which impact flexibility and scalability.
- Legacy networks require a physical presence in specific locations, leading to geographic limitations.

This white paper outlines how to overcome these challenges with the foundational components necessary for successful multicloud deployments and explores how efficient routing services can streamline connectivity, enhance agility, and unlock new innovation and growth opportunities.

SITUATION OVERVIEW

The use of multicloud configurations and networks has become mainstream. **Figure 1** shows the adoption of multicloud by enterprises in North America and Europe based on IDC's *2024 IaaS Network Services Survey*.

FIGURE 1

Multicloud deployment

*Q. Does your organization operate or is it in the process of deploying multicloud? **Multicloud refers to using IaaS cloud services from two or more cloud providers in a unified, coordinated architecture. Using multiple clouds for unrelated purposes does not qualify as multicloud usage.*

n = 1,003

Source: IDC's *2024 IaaS Network Services Survey*, September 2024

There are many issues with traditional approaches to linking disparate cloud environments:

- **Performance limitations/hairpinning:** This has evolved as a major source of complexity and cost for WAN and cloud networking. Most enterprises today rely on backhauling networking traffic from one site over the public internet to a central location, which may be a datacenter or cloud provider. Once security policy management has occurred, the traffic is routed back on a circuitous loop to the business site or another disparate location, affecting network latency and performance at every step along the way. Multiply this by hundreds or thousands of instances per day, and it becomes evident that network application performance and management complexity costs require a more efficient manner for traffic traversing between business sites and datacenters in a hybrid configuration and in a multicloud scenario.
- **Complexity of managing multiple public and private cloud platforms:** Each cloud provider has its own unique tools, interfaces, and processes, creating a complex and difficult-to-manage environment. Personnel expertise required for multiple cloud environments is an added cost burden of managing traffic across different cloud environments with different routing protocols and security policies. Routing algorithms, pricing models, and egress fees are all different. Consequently, it

is difficult to maintain a unified view of the overall cloud infrastructure to efficiently identify threats and monitor disruptions in a timely manner. Finding the talent with specialized skills to manage diverse networking protocols, APIs, data sets, and processes is an ongoing challenge.

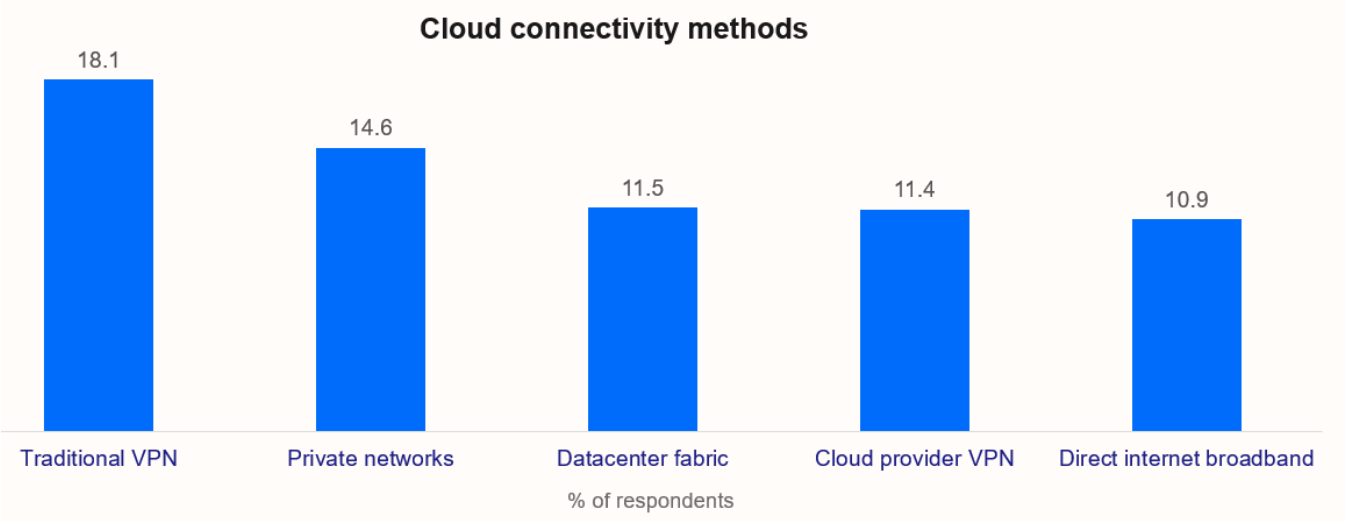
- **Public cloud egress costs:** Another element of intercloud routing that can be prohibitively expensive is the cost of traffic exiting each public cloud environment. Egress charges are incurred when data exits a cloud provider's network — such as transferring data to the public internet, another cloud environment, or an on-premises system. These fees often represent one of the most significant recurring costs in cloud networking. In addition to fees for traversing the public internet, cloud providers also charge for moving data between geographic cloud zones and regional cloud zones. Usage charges per gigabyte (GB) can be significant for companies moving as much as hundreds of terabytes monthly.

Figure 2 shows the main network connectivity methods for connecting to and across clouds.

FIGURE 2

Top 5 network connectivity methods for connecting to and across clouds

Q. Which of the following are your organization's most used network connectivity services when connecting to, within, or across clouds?



n = 1,003

Source: IDC's *2024 IaaS Network Services Survey*, September 2024

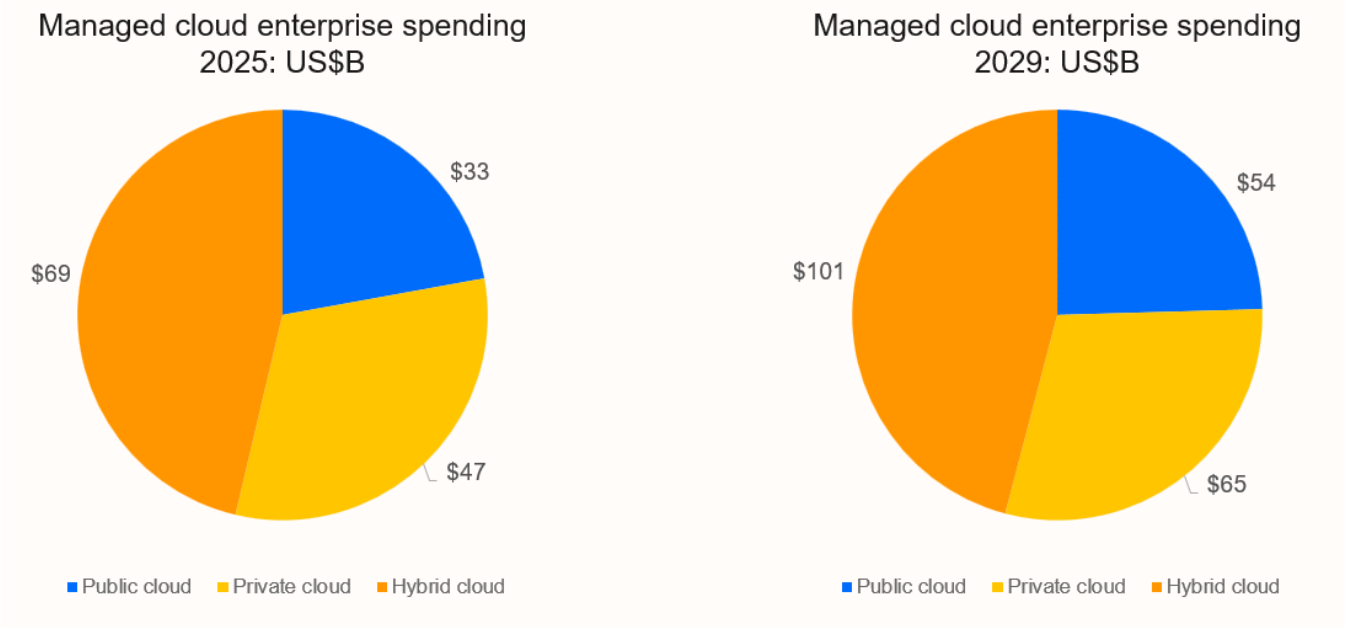
BENEFITS OF A MULTICLOUD GATEWAY

Key benefits of a multicloud gateway include:

- **Flexibility of leveraging multiple cloud platforms:** Integration is the top pain point in multicloud environments. Multicloud networking empowers organizations with greater flexibility, cost efficiency, and operational resilience to distribute workloads efficiently and easily across multiple cloud providers rather than relying on a single vendor. This approach helps avoid vendor lock-in, enables optimization for specific application performance and latency requirements, and reduces the risk of service disruption by eliminating single points of failure. It also eliminates delays in provisioning and scaling connectivity to meet business demand.
- **Solving security and compliance issues:** Multicloud networking enhances the support of disparate geographic and regional compliance, data sovereignty, and regulatory requirements by allowing workloads to reside in specific geographic regions aligned with specific corporate policies and compliance requirements.
- **Enhanced performance:** A traditional multicloud network that relies on routing traffic to multiple cloud platforms also requires scalable, low-latency, and high-performance connectivity. Telecommunications service providers such as Lumen are in the best position to bypass latency-inhibiting barriers and facilitate direct cloud-to-cloud connections with scalable private connectivity. Private connectivity avoids the complexity of carrier-neutral facilities, cross-connects, or traversing the public internet. This also offers reduced operational complexity, with optimal traffic routing for managing workloads across multiple clouds via a simplified unified portal.
- **Reduced egress costs:** One of the most important benefits of leveraging multicloud networking is the significant reduction in costs. Cloud providers charge up to $0.12 per GB in egress costs for moving data between clouds. For companies migrating terabytes of data per month, leveraging multiple cloud platforms, egress fees can be a major expense. A multicloud routing algorithm can dynamically route data between clouds via **low-cost private connectivity,** instead of costly egress paths. **Figure 3** illustrates worldwide enterprise spending on managed cloud services.

FIGURE 3

Worldwide enterprise spending on managed cloud services



Source: IDC's Worldwide Managed Cloud Services Forecast, 2025–2029, August 2025

FUTURE OUTLOOK AND CONSIDERATIONS

Key requirements for enterprises to consider include:

- **Scalable on-demand connectivity**: Deploying connectivity to a cloud provider can take hours to weeks, depending on the configuration. Leveraging a network service provider to deploy a multicloud gateway solution offers significant cost savings and enhanced efficiency. This can be deployed in minutes and can also scale with your business needs, allowing for future expansion to new clouds, regions, and edge environments without a full architecture overhaul.
- **Intuitive user interface**: A dynamic portal that offers multiservice capabilities (MPLS, Ethernet, internet), leveraging real-time dynamic bandwidth allocation and scalability, is important. The consumption-based pay-as-you-go model, which can facilitate flexible billing down to hourly or monthly usage, offers additional flexibility. This can reduce the complexity of network management and offer an appealing long-term ROI.
- **Performance:** Companies should carefully evaluate how a multicloud network solution meets application performance requirements such as latency, bandwidth capacity, and throughput.

- **Security and compliance:** Ensure the solution offers consistent security policies, such as identity and access management, and zero trust network access, across all clouds to meet compliance requirements.
- **Integration**: When evaluating solutions, it's critical to consider how easily they integrate into a multicloud environment. The best solution should provide API-driven automation, centralized policy control, and native backbone connectivity, including private IP and Ethernet. The solution should ultimately streamline architecture, consolidate ports, and lower costs, with multicloud neutrality to ensure seamless connections to AWS, Azure, Google, Oracle, and more — without vendor lock-in.

OPPORTUNITIES FOR MULTICLOUD GATEWAY DEPLOYMENT

An MCGW solution can enhance a traditional scenario of connecting workloads to different cloud providers.

Corporate edge to cloud without per-site cloud terminations

Over time, extending a corporate edge/LAN directly into the cloud — connecting premises and datacenters to cloud providers as if they were just another site — faces increased complexity in management and security, higher costs due to data transfer fees, and specialized tooling and performance issues, such as latency and bandwidth constraints between different cloud environments. MCGW solutions mitigate the requirement for multiple cloud-based devices and offer a centralized management framework and visibility, providing the routing intelligence to best route traffic to and from an organization's clouds. It offers significant performance enhancement by leveraging a single private connectivity fabric with a low-latency, direct route that avoids unnecessary latency-inhibiting hairpinning of traffic as it traverses from enterprise premises to and from clouds. This also avoids prohibitive egress costs that can balloon as data traffic exits public clouds in a hybrid or multicloud configuration.

Cloud-to-cloud interconnect for workload mobility and data synchronization

MCGW solutions seamlessly transfer workloads between leading public clouds using private connections — so there is no need to route traffic through an organization's datacenter. This direct approach helps reduce complexity, lowers costs, and enhances data protection while helping organizations accelerate performance. MCGW holistic private connectivity fabrics are cost-effective solutions that eliminate expensive egress costs, simplify network management, and reduce complexity. This architecture offers visibility and avoids the burden of managing disparate, multiple APs, routing, and security protocols, including the expense of maintaining experienced IT personnel for each cloud platform.

Leveraging scalable private connectivity for enhanced multicloud networking

Currently, many enterprises depend on public internet solutions by leveraging IPSec tunnels between clouds or SD-WAN to establish networking between corporate sites and multiple cloud environments. IPSec tunnels in multicloud deployments introduce significant operational and performance challenges. Each cloud VPC or VNet typically requires its own tunnel, leading to tunnel sprawl and increased complexity in large-scale environments, including limitations on throughput. Encryption overhead and bandwidth limitations further hinder performance, often without guaranteed SLAs. SD-WAN solutions, while offering centralized control, face their own set of multicloud integration hurdles with costly management overhead. The differing network architectures of AWS, Azure, and GCP require custom routing configurations, complicating deployment. Some SD-WAN architectures still rely on backhauling traffic through datacenter hubs, which increases latency and egress costs.

MCGW allows enterprises to implement high-performance private connectivity that can scale up to 100G virtual connections (VCs) for metro and inter-AS connectivity. This eliminates the need for IPSec tunnels or dedicated SD-WAN management expertise and offers a simplified solution with reduced costs, reliability, and SLAs.

CONSIDERING LUMEN TECHNOLOGIES

Lumen is redefining digital infrastructure. With one platform, one port and one bold strategy, they are fueling enterprise innovation at the speed of AI. Their extensive fiber backbone, cloud-based agility and simplified architecture don’t just support transformation—they power it.

Lumen Multi-Cloud Gateway and Lumen Ethernet Fabric Connect are designed to meet the need for agile cloud networking. Together, they provide an integrated, high-performance networking solution that unifies connectivity across multiple cloud providers, enterprise datacenters, and edge sites via a single digital platform. By leveraging direct cloud on-ramps and Lumen Connectivity Fabric, the Lumen Multi-Cloud Gateway allows enterprises to consolidate disparate connections onto a streamlined digital platform enabling connectivity services on one port. This architecture significantly lowers capital and operating expenses (fewer ports and cross-connects) and eliminates redundant backhaul while improving security by isolating public and private traffic. In short, the Lumen solution offers fast, secure, and effortless multicloud networking that is ready for the demands of AI-driven workloads and digital business initiatives. Key outcomes include:

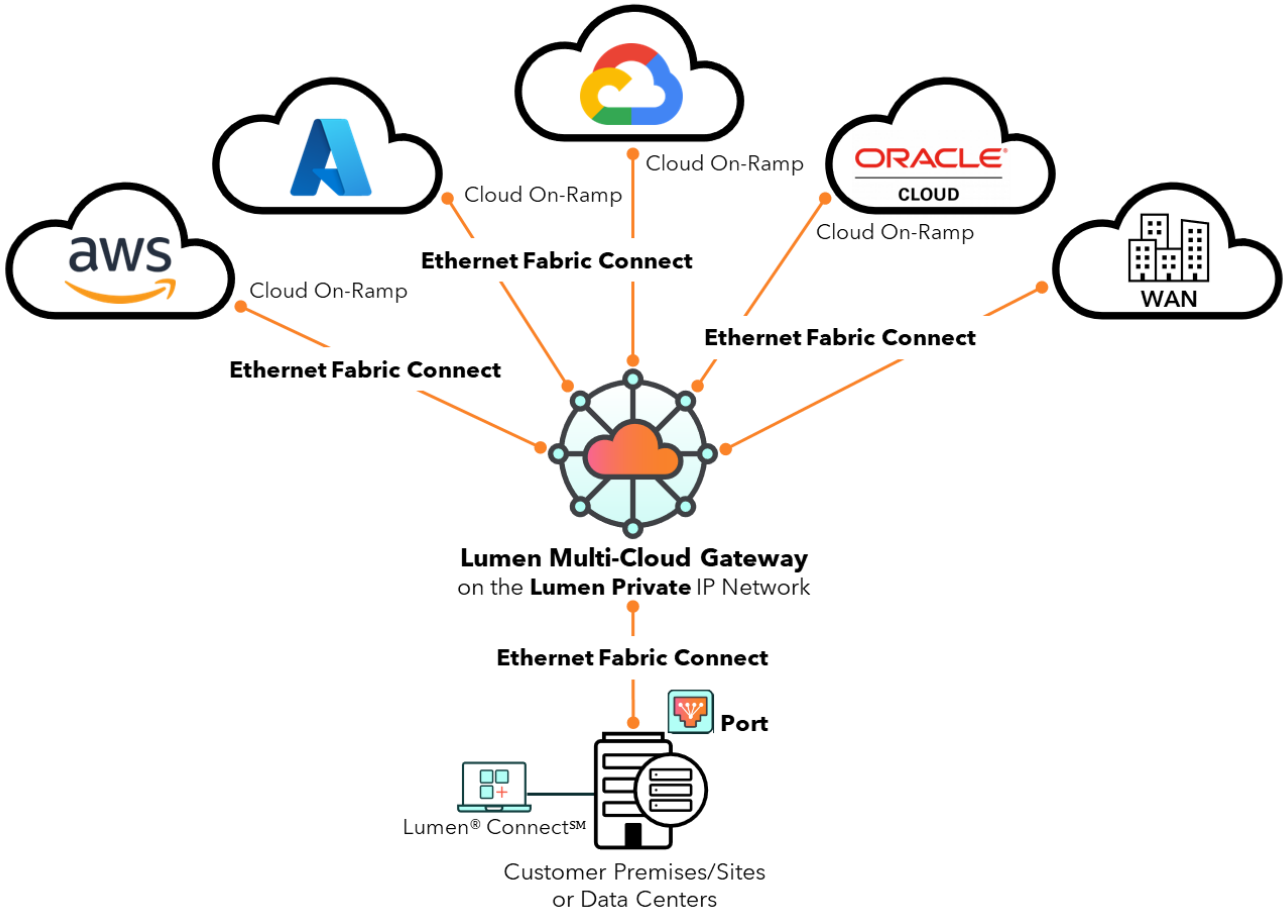
- Simplified operations with integrated, centralized, cloud-like network management and automated provisioning. One platform to unify cloud-to-cloud and cloud-to-site routing, reducing complexity and operational overhead.

- Cost savings through port consolidation, usage-based pricing, eliminating unnecessary infrastructure/equipment to manage, lower egress fees, and centralized BGP policy control.
- Improved performance via direct, low-latency routing between clouds and enterprise locations.
- Enhanced agility and faster time to value with rapid provisioning via APIs and portals, reducing setup from weeks to minutes.
- Enhanced security and governance with private, segmented connectivity to keep traffic off the public internet and enforce consistent policies across environments.
- A 400GB backbone for scalability and support for AI and data growth, with tiered bandwidth options and backbone integration to support high-volume traffic and future expansion.

By achieving these outcomes — simpler operations, greater agility, easier scalability, lower costs, better performance, stronger security, and higher resiliency — enterprises put themselves in a position to fully leverage multicloud and digital transformation. They can launch new services faster, respond to market changes, protect data, and ensure that their IT backbone is not a bottleneck but rather a business enabler.

FIGURE 4

Lumen Multi-Cloud Gateway



Source: Lumen

Challenges

As organizations increasingly adopt multicloud platforms to enhance flexibility, resilience, and performance, they face a range of operational, security, and financial challenges. Successfully implementing multicloud routing requires navigating these complexities to ensure consistent performance, security, and cost efficiency.

Operational complexity: Managing multiple cloud environments introduces significant overhead due to differing interfaces, APIs, and billing models. Visibility is often fragmented, making it difficult to monitor system health and performance holistically. A lack of standardization hinders integration across platforms, requiring custom solutions to ensure interoperability.

Security and compliance risks: Leveraging multiple cloud environments expands the statistical probability of failure and complicates the enforcement of consistent security and compliance policies. Data protection becomes more challenging, especially when sensitive information moves across jurisdictions. Managing identity and access across disparate systems further increases the risk of misconfiguration and unauthorized access.

Performance and cost management: Some connectivity solutions from cloud providers could introduce performance degradations. Latency can increase as data traverses between cloud providers, impacting real-time applications. Egress costs can increase exponentially depending on the level of traffic migration. Performance tuning is more complex in distributed environments, and cost optimization is difficult due to varying pricing models. Additionally, there is a shortage of skilled professionals with the expertise to manage diverse cloud environments.

IDC GUIDANCE

Key considerations & benefits

While many companies offer OTT multicloud networking solutions, enterprises should seek a partner that can provide end-to-end assets, including secure, high-capacity 100G VCs, from edge to cloud and between clouds.

Cloud networking is changing how enterprises configure their WANs. AI workloads that leverage inferencing are driving an exponential growth in enterprise data consumption and network traffic. The ability to leverage network as a service to scale up demand with unlimited capacity reduces complexity and prohibitive networking costs.

Robust security and simplified management across multiple clouds avoids vendor lock-in and provides diversity for business continuity, which facilitates significant ROI and reduced costs for infrastructure and IT operations, including personnel.

CONCLUSION

Selecting the right multicloud networking solution is critical to long-term business agility, reliability, and security. Legacy solutions are complex and not conducive to simplified, cost-effective intercloud networking. Multiple recent cloud outages demonstrate that vendor lock-in can be extremely damaging, both financially and for brand perception.

A multicloud solution offers the benefits of reduced costs and complexity, simplified orchestration of intercloud traffic, and a future-proof infrastructure with enhanced performance that is scalable and secure.

ABOUT IDC

International Data Corporation (IDC) is the premier global provider of market intelligence, advisory services, and events 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, IT benchmarking and sourcing, and industry opportunities and trends in over 110 countries. IDC's analysis and insight helps IT professionals, business executives, and the investment community to make fact-based technology decisions and to achieve their key business objectives. Founded in 1964, IDC is a wholly owned subsidiary of International Data Group (IDG, Inc.).

Global Headquarters

140 Kendrick Street
Building B
Needham, MA 02494
USA
508.872.8200
Twitter: @IDC
blogs.idc.com
www.idc.com