Competitive Landscape: Private Cloud Connectivity Services

Published 26 July 2021 - ID G00740222 - 36 min read

By Analyst(s): Gaspar Valdivia, To Chee Eng

Initiatives: Communications Product Planning and Strategy

Enterprises continue to shift mission-critical workloads to cloud IT, accelerating and elevating the requirements on cloud interconnects. Product leaders of cloud connectivity can differentiate their offerings with cloud-like autonomous operation and high-performing cloud-to-cloud enablement.

Overview

Key Findings

- The more enterprises pivot to cloud-based IT for mission-critical workloads, the more they recognize the need for predictability and high performance in their connections to the cloud that internet-based interconnects cannot always guarantee.
- Choice of private connections to cloud services has multiplied over the last few years, with a variety of services and provider offerings, which yields greater ability for tailor-made approaches but also more complex decision making for enterprises.
- Growth in enterprise adoption of cloud-native software, often composed of microservices distributed in various clouds, makes dependable connectivity between these clouds become essential for the integrity and performance of these applications.

Recommendations

Product leaders at providers of cloud connectivity services responsible for product planning and strategy should:

- Gain customer trust by offering consultative and design services for tailored-made solutions that optimize performance, security and cost of cloud interconnects by combining public and private cloud connections on a per-use-case basis.

- Differentiate private cloud connectivity options by adding to high security and performance cloud-like attributes, including ecosystem and geographic breadth, service agility, commercial flexibility, self-management and service automation.
- Provide enhanced connectivity for cloud-to-cloud workloads by offering cloud networking capabilities inside and between clouds through clients' virtual routers that improve latency and reduce complexity for multicloud environments.

Strategic Planning Assumption

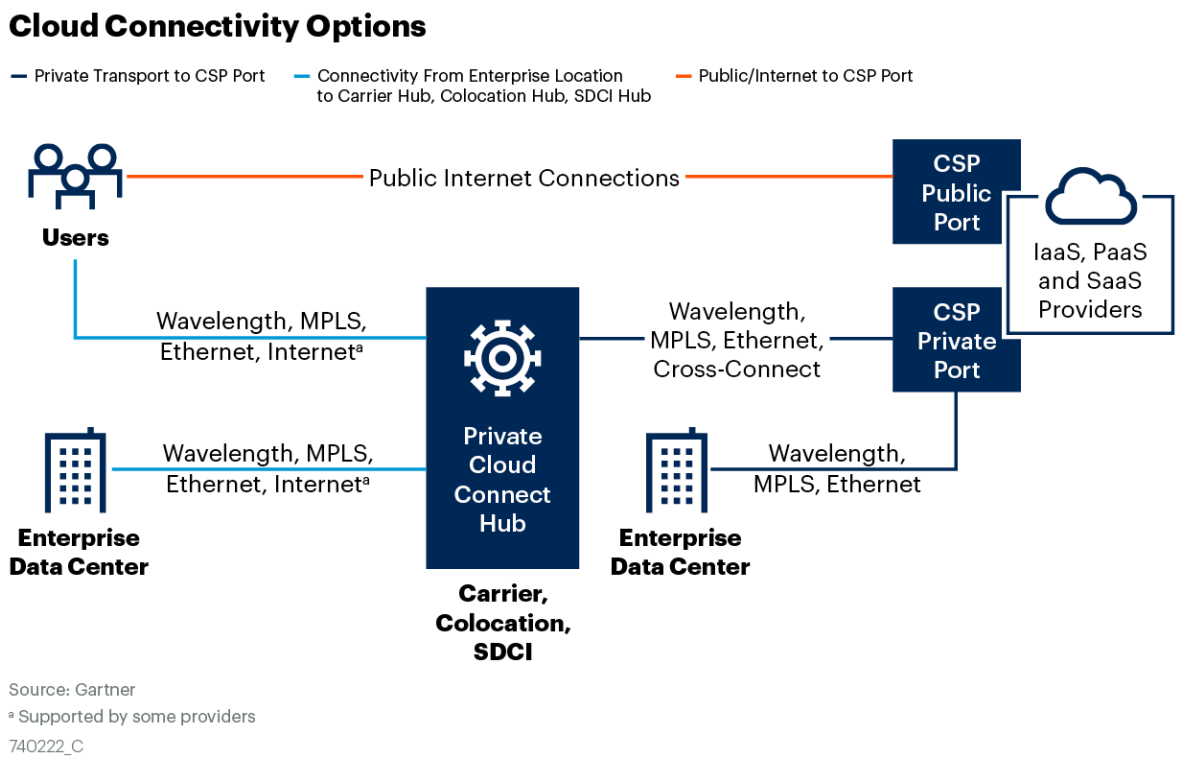
By the end of 2024, 30% of enterprises will employ software-defined cloud interconnect (SDCI) services to connect to public cloud service providers (CSPs), up from less than 10% in 2020.

Analysis

Private cloud connect services are Layer 2 and Layer 3 alternatives to internet services that enterprises can select to interconnect their wide-area networks (WANs) to public cloud services, either infrastructure as a service (IaaS), platform as a service (PaaS) or SaaS. In addition, these cloud connect services may or may not include the WAN connection from the enterprise site to the connectivity hub or colocation point, where the service provider establishes the private connection to one or more cloud providers.

The private cloud connect services market includes a range of vendor solutions, which enterprises can use individually or combine in tailored, mixed approaches (see Figure 1).

Figure 1: Cloud Connectivity Options



The private cloud connectivity architectural options include:

- **Point-to-point connections to private cloud ports** — Hyperscalers (e.g., Amazon Web Services [AWS], Microsoft Azure) and other public cloud providers offer private ports as entry points to their own cloud backbones. Enterprises can directly establish one-to-one connections from these private cloud ports to their private enterprise IP ports; for example, an enterprise data center, headquarters or major regional branch.
- **Colocation hubs** — Cross-connects in colocation hubs generally offered by data center and colocation providers, (e.g., Digital Realty, Equinix), for private, one-to-one, high-speed connections to the cloud providers.
- **Carrier-based interconnects** — Network service providers (e.g., AT&T, BT and Verizon) offer preprovisioned capacity to connect to either a cloud service provider (typically the largest in several discrete locations) or another private cloud connect service (e.g., colocation hubs [CH] or software-defined cloud interconnection [SDCI] hub). Different from other options, carrier-based interconnects (CBIs) include a private WAN from the customer edge location to the private cloud interconnection hub.

- **Software-defined cloud interconnects** — SDCIs offer a software-defined network (SDN) fabric of hubs that aggregate and intermediate connectivity between the enterprise site and a variety of cloud service providers as well as network and internet service providers. SDCIs support a multiple cloud approach and multicloud applications by interconnecting one CSP's offer with another's, without traversing the internet or employing Border Gateway Protocol (BGP).

Competitive Situation and Trends

Now pervasive across all markets and regions, the enterprise's uptake of cloud IT continues to grow. Gartner's forecast for enterprise spend on public cloud services estimates a 22.4% compound average growth in the 2020-2025 period (see Forecast: Public Cloud Services, Worldwide, 2019-2025, 2Q21 Update). Sixty-nine percent of respondents to Gartner's 2020 Cloud End-User Buying Behavior Survey [1] indicated that their organization planned to increase their spend in cloud services following disruption caused by the pandemic. In most cases, these enterprises will use cloud services from multiple providers. Seventy-six percent of respondents to this study indicated that their organizations use multiple public cloud providers. In fact, Gartner estimates that enterprises using multiple cloud providers connect to more than 20 public cloud services on average. As demand for connectivity to the cloud grows, the market is becoming highly competitive.

Currently, the internet is the most popular way enterprises connect users to data and applications in the cloud. Cost efficiency, ubiquitous presence and cloud provider limitations for other types of connections (particularly by SaaS providers) have driven its popularity. Security requirements for these connections are often sufficiently met through VPN tunnels. A variety of measures can be used and combined to enhance internet connection performance, such as:

- Connecting to the closest ingress point in the CSP network for each enterprise site (see How to Interconnect With Azure, AWS and Google Backbones).
- Deploying software-defined, wide-area network (SD-WAN) gear, and leveraging cloud onramps offered by some of the vendors in this space (e.g., AYAKA, Cato Networks, VMware-VeloCloud).
- Leveraging solutions from emerging enhanced overlay internet routing providers, (e.g., Anapaya, Mode, Teridion).

However, the more enterprises rely on hybrid cloud and multicloud approaches for their IT, and the more these deployments support business-critical and performance-sensitive applications, the greater the need for dependable cloud connectivity. Customer relationship management (CRM), ERP, core banking systems (CBS) software and other business-operations-related IT systems are increasingly included in cloud migration strategies. Greater requirements on reliable, high-performing and secure connections to the cloud fuel demand for uncontended, high-speed and private connections to the cloud.

To balance operational requirements — in terms of high and/or predictable performance, flexibility, agility, security and service guarantees — with cost-efficiency, enterprises often select tailored mix approaches that combine internet-based with private IP-based cloud connections aligned with specific use cases. Enterprises have a growing choice of service types and service providers for private connections. Table 1 shows some representative examples of these service provider types categorized in three main segments: colocation hubs, carrier-based interconnects and SDCIs.

Table 1: Service Providers Offering Private Cloud Connections

Cross-Connects at Colocation Hubs	*Carrier-Based Interconnects*	*Software-Defined Cloud Interconnects*
Cologix CoreSite DE-CIX Digital Realty Equinix	AT&T BT Tata Communications NTT Communications Orange Business Services Verizon Vodafone	Epsilon InterCloud Megaport PacketFabric PCCW Global Unitas Global
Direct cross-connects in colocation facilities. Enterprises need to source independently a private WAN connection to the colocation hub	Dedicated point-to-point connections as well as virtual private connections over shared prebuilt links connecting the enterprise WAN to the CSP's private cloud port.	SDN fabrics enable virtual connections on-demand from one entry point to the fabric to several cloud services. Enterprises need to source independently a private WAN connection to the SDN fabric.

Source: Gartner (July 2021)

Cloud connectivity providers compete by offering services and tools that simplify establishing and managing connections for hybrid cloud and multicloud architectures through:

- **Point-to-point connections** from the enterprise location to the cloud service provider private port.
- **Prebuilt, high-speed Layer 2 and/or Layer 3 connections** in shared and colocation data centers and carrier hub exchanges.
- **Cloud onramps (private connections)** to many cloud providers from many locations. Typically, these onramps include all major hyperscale platforms, such as Alibaba Cloud, AWS, Google Cloud, Microsoft Azure, IBM Cloud, Oracle Cloud and numerous SaaS applications.
- **Software-defined network fabrics** that, through one physical connection to the SDN fabric, enable the enterprise to connect to multiple cloud providers through virtual local-area network (LAN) connections, which can be easily managed through the service web portal.

Some of the providers in Table 1 are capable of offering a complete end-to-end private link from the branch to the cloud; others offer private connections starting from their service points of presence (POPs). Partnerships between service providers across these categories for extending geographic coverage and service reach are also common. For some of the service providers in Table 1, enterprise access to these private cloud connectivity services require that they source other elements within their broader service catalogs, such as data centers, colocation, interconnection solutions or managed services. Network-as-a-service commercial options are emerging as a competitive claim in many service provider's offerings.

As enterprise demand for private cloud connect services grows, it also gets more sophisticated. Gartner sees provider offerings aligning to four main competitive trends:

- Guaranteed performance for mission-critical workloads in the cloud.
- On-demand consumption and enterprise operation autonomy.
- Enhanced support for cloud-to-cloud use cases.
- Augmented privacy, security and compliance.

Guaranteed Performance for Mission-Critical Workloads in the Cloud

Ensuring optimal performance for end-user access to mission-critical workloads is a leading driver for enterprises that shift from internet connections to private/dedicated cloud interconnections services. Other frequent drivers include privacy, security and compliance concerns.

To help overcome latency, packet loss and other internet middle-mile performance issues, private cloud interconnection providers use direct cross-connects in colocation hubs and/or privately owned and operated backbones. These solutions route the traffic in a controlled way to IaaS and SaaS provider's network entry ports. To offer end-to-end service performance guarantees, service providers also need the ability to monitor and control last-mile accesses from the customer edge location to its network POP.

Service providers continue to invest in differentiating their cloud interconnections offerings for reach, performance and advanced features in several ways:

- Breadth and depth of reachable cloud service partners beyond the big five hyperscalers, including a range of SaaS providers.
- Layer 2 and Layer 3 network backbones with high capacity and dozens (or hundreds) of POPs for global and/or dense regional coverage.
- Local partnerships for service extensions beyond own network reach and presence in hundreds of shared data centers and exchange hubs.
- Breadth and depth of cloud interconnect options, including high-speed options that can be customized and reach hundreds of Gpbs.
- Service reliability through high-quality connections, redundancy options, multihomed connections and service performance guarantees via stringent service-level agreements (SLAs).
- Directly provisioning last-mile connectivity or, alternatively, supporting it through agreements with third-party providers.
- Monitoring and near real-time view of data flows and application performance across networks and clouds that some service providers extend to user experiences.
- Quick failover and proactive assurance services leveraging data analytics, machine learning (ML) and artificial intelligence (AI) techniques.

On-Demand Consumption and Enterprise Operation Autonomy

As the scale of in-production cloud IT in the enterprise grows, so does the need for agile and flexible cloud interconnections. CloudOps teams in enterprises deploy resources instantly in the cloud and increasingly use VPN components provided by CSPs, (e.g., AWS' virtual private clouds [VPCs], Microsoft's Azure Virtual Networks [VNets]) in a dynamic way. Infrastructure and operations (I&O) and CloudOps teams need to be able to deploy, configure, manage and change cloud connectivity easily and quickly. These requirements feed the demand for service automation and near-real-time instantiation of cloud connections and self-service options enabling technical and operational autonomy.

The requirements to address is to obtain cloud connectivity on demand, in an automated fashion and in near real time, and that can match the agility of cloud business. Customers want to rapidly provision new services globally and eliminate typical procurement headaches, such as pricing, long lead time and service performance visibility.

Three key components, in different levels of development across competitors, drive provider ability to meet this demand:

- **Software-defined network fabrics** provide a programmable framework that both enables agile establishment and configuration as well as expands the breadth of virtual private cloud connections atop prebuilt infrastructure through automation. Providers also differentiate their offerings through depth and breadth of other virtualized value-added services, such as monitoring, visibility, increased networking functionality, (e.g., SD-WAN) and security, (e.g., next-generation firewall as a service [NGFWaaS], Secure Sockets Layer [SSL]) that can be incorporated and orchestrated in software-defined service POPs (such as Orange Business Services' Next Gen Hubs). Further differentiation is achieved by enabling automation and orchestration of cloud connectivity via third-party provided underlays, (e.g., InterCloud) and cloud-to-cloud connections, (e.g., PacketFabric).

- **On-demand service web portals** enable, through an easy-to-use graphic interface, self-provision and management functionality, such as change and delete cloud connections to an ecosystem of public clouds and SaaS applications. Providers offer different options for authorized enterprise users to check and configure links, quality of service (QoS), domains and routing. Users can also view bandwidth allocation and utilization statistics, adjust bandwidth as needed and get self-service analytics with real-time visibility into application performance, SLAs and key performance indicators (KPIs). Some providers also compete by extending the capability to self-provision automated connections to other ecosystem partners, including carriers, internet exchanges, shared data centers, Internet of Things (IoT) networks or, in some nascent offerings, other customers, such as PCCW Global.
- **APIs** enabling integration of networking and cloud interconnection self-management functionality with the enterprise's own IT service management (ITSM) tools comprise service providers' recent capabilities. The ultimate objective is for the network (cloud interconnection fabric) to proactively respond to the needs of the business. Although this is still a development area for most leading cloud interconnection providers, several now offer open, representational state transfer (RESTful) APIs, allowing service discovery, ordering and cloud link provisioning.

Network function virtualization (NFV) is another element of competitive differentiation among providers. Virtual network function (VNF) hosting services in provider infrastructure enable on-demand integration of virtual appliances for networking and security solutions, such as SD-WAN controllers, intrusion detection system/intrusion prevention system (IDS/IPS) and next-generation firewalls in cloud connections.

Aligned with demand for high-performing, reliable connection and service automation, Gartner expects leading cloud connectivity providers to further leverage data analytics, ML and AI for more proactive service assurance, quick failover and enhanced customer experience.

Enhanced Support for Cloud-to-Cloud Use Cases

Enterprise continued growth in usage of IaaS, PaaS and SaaS fuels a growing demand for connections to the cloud, both over the internet and via private direct links to private cloud ports. Most enterprises adopt a hybrid architecture with a combination of private and multiple public cloud services. Yet, legacy applications, sometimes home-built, usually exploit local data and are typically difficult and expensive to migrate to the cloud. On the other hand, enterprise use of cloud-native software continues to grow. This software is often composed of aggregated microservices from multiple remote service providers that are distributed in various clouds. Connectivity between these clouds thus becomes crucial for the integrity and performance of these applications.

Multicloud approaches and distributed applications are already shaping the demand for those secure private cloud connectivity services that help simplify management of complex ecosystems and optimize performance for cloud-based applications and services. Accordingly, demand and competition in private cloud connectivity is shifting toward managing traffic flows within and between clouds, rather than just ensuring access to the cloud.

CSPs' own networking offerings have evolved to reduce complexity for traffic flows between workloads within their networks. However, enterprises increasingly have to deal with the continued growth of cloud destinations as well as the management of legacy applications, private clouds and on-premises infrastructures.

More advanced offerings include multicloud-specific support through:

- **Cloud networking** — Cloud traffic routing within the provider's network fabric that improves latency and reduces complexity for multicloud environments. Enterprises can use Layer 2 and Layer 3 private networks offered by the service provider to orchestrate and optimize traffic routing between regions within a single cloud provider or across multiple clouds and data centers. Some service providers (i.e., Megaport, PacketFabric) offer the possibility to deploy virtual routers so that enterprises can forgo using hardware or physical ports to control traffic at the IP level. Competitors strive to enhance the automation, operational visibility and control they offer for the creation and management of enterprise-class networks inside and between public clouds.

- **Closed user groups** — Setups by which enterprises can create their own private and dedicated virtual interconnection to other customers on the service provider's platform. Service providers such as PCCW Global offer users the ability to discover other users and businesses on the platform, and then communicate and privately connect their networks and applications. Service providers such as Equinix now leverage their large customer bases to target vertical-specific ecosystems and communities of interest (e.g.,financial services and global payments).
- **Support for edge computing** — Incorporated in numerous use cases, including augmented reality/virtual reality (AR/VR) and mixed reality (MR), autonomous vehicles, drone operation, real-time data analytics and others over the interconnection fabric. AT&T, Equinix and other providers recently launched services to support edge deployments and private edge connections over the network POPs and interconnection fabric (i.e., AT&T Network Edge and Equinix Metal).

Importance of Privacy, Security and Compliance

Increasing cloud design complexity with more mission-critical workloads in hybrid cloud and multicloud environments introduces new challenges and more demanding security requirements. Whereas the security challenge is widely acknowledged across providers and customers, competitive strategies and capabilities offered by service providers to ensure privacy and security for traffic to, from, within and between clouds vary significantly.

While partnering with specialized security vendors, (e.g., Check Point Software Technologies, Fortinet, Palo Alto Networks, Zscaler) is the most popular approach, some cloud connectivity providers have developed their own dedicated security services or made acquisitions for stronger differentiation.

Examples include:

- High-performing data encryption offered by Epsilon and InterCloud's hardware security module (HSM as a service) in its Cipher service.
- Traffic and network segmentation policies that enterprises can extend beyond cloud boundaries for consistent and centralized management of multicloud security domains by Epsilon and InterCloud.
- Dedicated fiber optic networks to ensure privacy and security of traffic flows, such as offered by Digital Realty following the acquisition of Ascenty in 2018.

Large communications service providers, such as AT&T, BT, Tata Communications, NTT Communications, Orange Business Services, Vodafone and Verizon Business, have adjacent **cybersecurity services portfolios** that enterprises can leverage to secure cloud connections. Typically, communications service providers offer the capability to insert next-generation firewalls as virtual instances in enterprise connections to the cloud. Broader security features, such as URL and application filtering, malware protection, IDS/IPS, DLP, and increasingly threat detection and response, can be sourced from communications service providers.

SSL inspection and authentication services have traditionally offered support for private remote access use cases. COVID-19 triggered a steep increase in demand for securing access to cloud workloads for remote workers, and enterprise interest for new tools that allow more selective, context-aware and identity-based secure access policies than VPN clients can. In response to this need, networking and security vendors are aligning their roadmaps to the secure access service edge (SASE) concept in parallel with market hype growth. Similarly, some providers of cloud connectivity have started to align their security capabilities, roadmaps and marketing approaches to the SASE framework. These providers leverage service POP architectures in their interconnection fabrics to offer SD-WAN gateways, cloud-based firewall as-a-service, secure web gateways, cloud access security brokerage and zero trust network access (ZTNA).

Table 2 summarizes how a set of representative service providers from diverse backgrounds compete across these trends.

Table 2: Examples of Private Cloud Connectivity Offerings

(Enlarged table in Appendix)

	Performance of Mission-Critical Workloads in the Cloud	*On-Demand Consumption and Enterprise Operation Autonomy*	*Support for Multicloud and Cloud-to-Cloud Use Cases*	*Privacy, Security and Compliance*
AT&T	Prebuilt, high-speed connectivity, 3M-100G+, into a majority of the largest data centers in the U.S. and a selection of others globally. Cloud-connect SLAs	Near-real-time, on-demand virtual network connections to CSPs through service portals. API-driven provisioning in certain CSPs.	Support for multicloud use cases through colocation ecosystem and Total Access Orchestration platform.	Secure, private connectivity to 1 5 CSPs (AT&T NetBond for Cloud).
	Broad portfolio of underlay connectivity solutions (e.g., MPLS, Ethernet, dedicated internet).	Integration of virtual networking and virtualized workloads in cloud connections (total access orchestration).	Enablement of edge computing use cases (AT&T Network Edge).	Options for virtual firewalls in cloud connections. Option for MSS, including IPS/IDS, SWG, TDR and CASB.
Digital Realty	Global data center footprint provides access to 280+ facilities in 45+ metros across 20+ countries on 6 continents.	On-demand private network connectivity to an ecosystem of cloud, network, partners and providers leveraging Digital Realty's cloud connectivity.	Support for multicloud use cases. One physical connection from a PlatformDIGITAL location to connect to various cloud providers through virtual LAN connections.	Private connections within their operating metros through a dedicated fiber-optic network for security and end-to-end control over data traffic.
	180+ onramps to the major 6 CSPs across PlatformDIGITAL in APAC, Europe and the Americas.			
Equinix	Global ecosystem of about 10,000 companies, provides customers access to 2,600+ cloud and IT services.	Software-defined interconnection to multiple cloud service providers as well as any other company's infrastructure on Platform Equinix.	Support for multicloud use cases. Software-defined network providing connections to multiple cloud providers colocated in Platform Equinix.	Direct cross-connects in colocation facilities.
	It also provides access to 1,800+ network services, 1,250+ financial services, 600+ content and digital media services, and 2,900+ enterprises.	Equinix Fabric integration into Network Edge and Equinix Metal support customers' own virtual workloads deployments.		
InterCloud	Network backbone is connected to several data centers and four major CSPs (AWS, Google, IBM and Microsoft).	SDCI, API-centric management platform.	Multicloud use cases enabled by its own fabric network as well as third-party provided underlays (e.g., Equinix, Megaport).	Direct cross-connects in colocation facilities.
	Routed access to the nearest InterCloud's Edge via a local loop and on-site equipment with end-to-end measurements and by default quality commitments in any interconnection, backed by SLAs.	CloudOps-oriented plugins (Terraform, Grafana).		Security resources on dedicated appliances (e.g., Palo Alto Networks or Fortinet firewalls) InterCloud's own dedicated security services (e.g., Cipher Service — HSM-as-a-Service).
Megaport	High-availability network backbone across 700+ enabled data centers (100+ data center operators) and 230+ cloud onramps in North America, Asia/Pacific (APAC) and Europe, SD-WAN providers, and over 360 service providers.	SDN integrated with leading cloud service providers for on-demand and automated provisioning of capacity to service endpoints via a portal and open API.	Virtual cloud routers (Megaport Cloud Router) are instantly provisioned through web-based portals in virtual points of presence to control traffic at the IP level and support cloud-to-cloud networking use cases.	Private cloud connectivity.
		On-demand NFV service that supports branch-to-cloud connectivity on SD-WAN platforms (Megaport Virtual Edge).		
PCCW Global	Service accessible from 450+ data centers across 50+ countries and fully integrated with hyperscale cloud providers to connect customers directly to over 150 cloud regional zones.	Self-provisioning, on-demand SDN platform for spinning up private connections and flex bandwidth to cloud providers and other partners through a web portal and APIs.	Support for hybrid and multicloud deployment and management by connecting multiple clouds from a single port, either in the same cloud region or global regions.	Private preintegrated connections to multiple clouds from a single port bypassing the public internet.
	Private, high-speed, uncontended, low-latency network with multiple grades of class of service (CoS)/QoS and backed by carrier-grade SLA.	App to discover and establish private connections to other user networks and applications.		
Unitas Global	Global SDN interconnects 900+ data centers in 1 23+ countries with over 560 networks and fiber access providers.	Global SDN for automated on-demand access to cloud locations.	One port, multiservice on-demand network provides options for distributed cloud, hybrid cloud, multicloud and private cloud.	Private-direct IP peering.
	Direct peering to 4,900 networks connects SaaS, content and broadband providers for reduced latency. SLAs guarantee the route and bandwidth.	Network service management APIs.	Access through local Ethernet connections (multiservice-Edge Link) supporting bandwidth split by service.	
Verizon	Diverse interconnections from MPLS backbone to CSPs in all major markets around the world for redundant, reliable service backed by a network SLA.	Automated, on-demand connections to CSPs through a service portal. Secure Cloud Interconnect (SCI) for bandwidth-based connections and Software-Defined Interconnection (SDI) leveraging platform Equinix for port-based connections.	Support for multicloud use cases through SCI to a cloud ecosystem of nine CSPs and through SDI to over 200 cloud providers colocated in Platform Equinix.	SCI and SDI: Private connections separated from public internet traffic.
	Broad portfolio of underlay connectivity solutions (e.g., MPLS, Ethernet, dedicated internet, mobile LTE). Support for multiple services on one access connection (multiservice access).	APIs for integration in customer's ITSM tools. Option for virtual network and security services on cloud connections.		Virtual SD-WAN, firewall and WAN optimization tools are provided as add-on services to cloud connectivity. Option for managed security services.

This table showcases examples of different types of service providers in terms of market reach or competitive differentiation. Inclusion in the list does not imply Gartner's opinion on the quality of the service rendered by the service provider compared to others, either included or not in the table.

Source: Gartner (July 2021)

Competitive Profiles

Below we provide brief competitive profiles highlighting varied competitive strategies from a few service providers from diverse backgrounds. The list is not comprehensive for all options from service providers delivering private cloud connect services to enterprises. A selection has been made to showcase relevant examples from different types of service providers in terms of market reach or competitive differentiation. Inclusion in the list does not imply Gartner's opinion on the quality of the service rendered by the service provider compared to that of others not included. Profiles are provided in alphabetical order.

AT&T

Product or Portfolio Overview

AT&T is a global communications service provider that offers private cloud connectivity services to small and midsize businesses (SMBs) and enterprises through its AT&T Business division. AT&T addresses business demand with cloud onramps with prebuilt capacity for internet, Ethernet and MPLS services, and with integration between AT&T's private MPLS services and several cloud service providers (AT&T NetBond for Cloud). The provider extends its offering to support enterprises' private and public edge cloud use cases with low-latency connectivity (AT&T Network Edge) to shared data centers within a metro as well as major cloud service providers respectively.

How AT&T Competes

AT&T leverages its extensive network and service assets as a leading domestic telco in the U.S. and global carrier, and focuses to compete by offering comprehensive end-to-end solutions from last-mile accesses to the cloud connections and security as well as multiple other ancillary services. AT&T delivers a set of collective capabilities that together establish an on-demand, software-defined network platform.

AT&T has invested in private cloud connectivity onramps with prebuilt, high-speed connectivity, 2M-100G+, into a majority of the largest, most active shared data centers in the U.S. and other locations globally. Reach is extended through partner exchanges — such as Equinix Fabric, Digital Realty Service Exchange and Megaport — to offer private cloud access to a colocation ecosystem. This includes seven different providers featured in 595+ data centers across five continents and 24 countries. AT&T continues to invest in network capacity enhancements (with plans to enable 400G ultra-high-speed connectivity between U.S. shared data centers in 2021) and local peering expansion with global partners, enabling private connectivity to shared data centers and the cloud.

AT&T NetBond for Cloud offers an on-demand service portal and APIs by which customers can add/delete/change their virtual network connections (VNCs) between AT&T VPN service (MPLS VPN) and an ecosystem of IaaS, PaaS and SaaS providers. They can also change the bandwidth of these connections on demand. AT&T also includes orchestration capabilities that enable customers to insert VNFs into the network to support functions, such as IDS/IPS, next-generation firewall, high-speed routing and SD-WAN, with choice of vendors.

Gartner expects the service provider to further invest in expanding the reach and capacity of its cloud interconnection network and add enhanced support capabilities for edge computing use cases. An example of this would be wireline and 5G low-latency options for connecting enterprise endpoints to edge computing zones in shared data centers and the cloud. Other expected enhancements include LTE and 5G network APIs for applications to invoke network requirements for performance assurance based upon real-time network telemetry.

Digital Realty

Product or Portfolio Overview

Digital Realty is a global data center provider with presence in five geographic regions. It operates 280+ facilities in 45+ metros across 20+ countries. Its Interconnection Services are SDN-enabled and available on demand to enterprise customers. Customers can set up direct private network connections to cloud providers hosted in Digital Realty's facilities. In addition, they have access to connected data communities globally, for connecting private infrastructure to cloud and other service providers supporting hybrid IT environments.

How Digital Realty Competes

Digital Realty differentiates on its global coverage, with strong presence in three main geographic regions, including Europe, the Americas and Asia/Pacific. It focuses on key metros, where most large enterprises are headquartered. It is beginning to expand its presence in South America and Africa in anticipation of future demand.

Digital Realty competes with global reach, data center quality and operating experience, which has allowed the provider to draw in both enterprises and service providers, including both CSPs and network providers. Major CSPs hosting in Digital Realty include AWS, Microsoft Azure, Google Cloud Platform, IBM Cloud and Alibaba Cloud.

Digital Realty's Service Exchange product provides on-demand private network connectivity to an ecosystem of providers and partners to enable hybrid-cloud, multiple clouds and cloud-to-cloud use cases. Digital Realty's direct cloud connection service is delivered through a single Layer 2 physical network connection. Customers can set up virtual LAN connections to multiple cloud providers as well as network service providers, other customers and partners hosted in Digital Realty. The service offers redundancy options, with up to 99.999% availability.

In addition, Digital Realty provides access to 180 onramps located in major geographic regions. PlatformDIGITAL enables enterprise deployments of any size to have direct access to cloud providers in its facilities and third-party data centers.

Equinix

Product or Portfolio Overview

Equinix is a global data center provider offering enterprise customers private cloud connectivity to all the cloud providers as well as any other company's infrastructure hosted in its facilities. The service, Equinix Fabric, is a software-defined interconnection service available on demand, with flexible bandwidth and 99.999% availability guarantee for dual access ports configuration. Currently, Equinix Fabric supports approximately 31,100 customer connections.

How Equinix Competes

Equinix's primary strength is its global footprint, with more than 220 data centers in more than 60 markets across five continents. It has connected its data centers with a private software-defined network, enabling its enterprise customers to connect to all cloud providers, CSPs and enterprises hosted in Equinix's facilities, which it positions as a global infrastructure platform. Equinix's network value proposition (Equinix Fabric) enables its enterprises customers to connect their private infrastructure with cloud providers across a single network for hybrid cloud requirement

It has an early lead in drawing major cloud providers into its data centers, attracted by its highly distributed geographic coverage, strong enterprise customer base and proven data center experience. Among the cloud providers hosting with Equinix are AWS, Microsoft Azure, Google Cloud Platform, IBM, Oracle Cloud Platform, Cisco and Zoom.

Equinix is investing aggressively in new data centers with strong investment partners. Labeled XScale, the data centers are specifically built for hyperscalers targeting new or growth markets. By drawing hyperscalers deeper into its infrastructure, Equinix will attract more enterprises to colocate their private infrastructure with Equinix.

Further, Equinix offers Network Edge, an NFV platform where enterprises can host virtual workloads, such as SD-WAN and security services, for connecting brand sites to the cloud and Equinix Metal, an automated, on-demand bare metal service. Equinix Fabric is integrated into both allowing a single interconnection approach to connect enterprise physical and virtual devices located within International Business Exchange (IBX) data centers and the Platform Equinix digital ecosystem.

InterCloud

Product or Portfolio Overview

InterCloud is a provider of SDCI that offers secured, end-to-end managed interconnection services. Its managed services portfolio spans private connectivity to cloud services providers, connectivity hubs and internet exchanges peering.

How InterCloud Competes

InterCloud has developed a product offering based on service components (Connectors and Links) that customers can flexibly combine and scale to build and deploy solutions tailored to their use cases. These include hybrid and multiple clouds, and cloud-to-cloud connections for distributed workloads. The Connectors expose what each cloud provider offers in terms of capacity and functionality. InterCloud partners with the major IaaS and SaaS providers, including AWS, Microsoft Azure, IBM, Google Cloud, Salesforce and ServiceNow, among others. InterCloud also offers Connectors for on-premises and private clouds. Links provide routing between Connectors by leveraging the InterCloud network fabric, or underlays from partners, including Megaport and Equinix. Enterprises can access the InterCloud's network fabric through colocation cross-connects, private local loops with on-site equipment as well as secured public accesses (such as IPsec VPNs), enabled by InterCloud's Edge Doorway capabilities.

All InterCloud services are fully managed with a range of several service levels for different degrees of customer's autonomy, pricing, support and quality commitments (SLAs). It also offers design and consultancy services. Enterprises can also leverage NFV capabilities in InterCloud's connectivity hubs to accommodate additional networking features, such as security, monitoring, optimization and, currently in roadmap, SD-WAN gateways and controllers. In addition to third-party vendor firewalls (such as Fortinet and Palo Alto Networks), the service provider has developed its own InterCloud's Cipher Service, an HSM-as-a-Service that adds data encryption on the Links.

For customers that demand greater control and autonomy, InterCloud offers SDCI platform management via APIs as well as CloudOps-oriented plugins, including Terraform and Grafana. Gartner expects InterCloud to further develop its security offering associated with the cloud interconnection capability with firewalling-as-a-service, cloud agents in major clouds for application segregation and ZTNA (in addition to performance measures). The provider is also investing in automating cloud connectivity over InterCloud-managed, third-party-provided underlays to offer its customers a choice of underlays based on SLA, performance, security, regulatory and pricing criteria.

Megaport

Product or Portfolio Overview

Megaport provides cloud connectivity, data center interconnect and internet exchange peering services on its SDN platform. Its cloud connect services portfolio includes virtual cross connects (VXC), virtual cloud routers (MCR) and virtual edges (MVE). VXCs are private point-to-point Ethernet connections between an enterprise port and a private port from a cloud service provider. MCRs are virtual routers that customers can instantly deploy on virtual POPs in Megaport's fabric through a web-based portal to control cloud traffic at the IP level and enable cloud-to-cloud use cases. MVE is an on-demand NFV service that supports branch-to-cloud connectivity on SD-WAN platforms.

How Megaport Competes

Megaport proposes agile networking capabilities that reduce operating costs and increase speed to market compared to traditional networking solutions. It leverages its own software-defined network platform which is available in 700+ enabled data centers and 230+ cloud onramps in North America, Asia/Pacific and Europe. Megaport offers connectivity to all the major cloud providers, 100+ data center operators, leading SD-WAN providers, as well as over 360 service providers that include managed services firms and leading system integrators.

Megaport offers on-demand delivery of private virtual cloud connections on its network fabric that enterprises can order and provision in minutes from an easy-to-use web portal or by leveraging Megaport's open APIs. The provider claims enterprises using its private cloud connectivity can drastically reduce egress fees and network charges compared to VPN tunneling over the public internet. Performance (controlled routing and latency optimization) and security together with simplified network management of multicloud setups are other key selling points.

Gartner expects the service provider roadmap to focus on footprint expansion to new markets and capacity enlargement for its virtual cross-connects to more than the current maximum of 10 Gbps speeds. Other roadmap enhancements will reinforce the Megaport Virtual Edge offering with a new ability to host load balancers and firewalls as well as SD-WAN software from a greater choice of technology vendors. The ability to deliver security from Megaport's network will be reinforced with network address translation (NAT) functionality over the onramps to clouds and data centers.

PCCW Global

Product or Portfolio Overview

PCCW Global is a global CSP that provides connectivity to more than 3,000 cities in 160+ countries worldwide. Its Console Connect service is a software-defined interconnection platform that can connect enterprises directly to multiple cloud services, including AWS, Microsoft Azure, Google Cloud, IBM Cloud, Oracle Cloud, Alibaba Cloud and Tencent Cloud, in over 150 cloud regional zones. The Console Connect service is available on demand at 450+ data centers across 50+ countries via a self-service portal.

How PCCW Global Competes

PCCW Global's Console Connect platform rides on the global carrier network infrastructure of PCCW Global, which enables uncontended service across its network fabric with assured quality of service, and the ability to scale and flex high-speed connectivity on demand. The services are backed up with a carrier-grade SLA.

The platform enables enterprises to connect in minutes, avoiding lengthy provisioning times and long-term contracts. Customers can provision dedicated circuits for durations from as little as one day. Pricing is simple, transparent and competitive, helping customers reduce network and connectivity costs, only pay for what they use and flex bandwidth needs on demand in seconds.

The intuitive UI makes it easy for enterprises to connect to public cloud resources. The platform is fully integrated with all major cloud providers, and helps businesses simplify hybrid and multicloud deployment and management. They can connect multiple clouds from a single port and can take advantage of its extensive onramps to preintegrated cloud and SaaS partners. Enterprises can also interconnect with the platform via API and activate and manage network connections directly from their own applications.

Console Connect is integrated with a broad global digital ecosystem, enabling customers to reach beyond cloud providers to connect to any other Console Connect customer or partners within its growing community of businesses and IaaS, PaaS and SaaS providers. The platform is self-service and provides all the tools needed to manage and monitor multiple secure direct connections.

Unitas Global

Product or Portfolio Overview

Unitas Global is a managed network service provider that offers direct connections to the most popular IaaS and PaaS providers (AWS, Azure, Google Cloud, IBM Cloud and Oracle Cloud). It has its own global software-defined network, featuring key interconnects with multiple other networks and fiber access providers in 133 countries, including over 900 carrier-neutral data centers. Unitas offers one-hop onramps to highly demanded SaaS providers, such as Microsoft 365, Salesforce and Zoom, and local access to its SDN through multiservice Ethernet connections. Its management and monitoring platform provides visibility into the health and performance of both cloud and network infrastructure.

How Unitas Global Competes

Unitas Global operates Unitas Reach, a Layer 2 software-defined Ethernet transport network that uses several transit providers for diverse and redundant connections between the network POPs and interconnects with multiple private and public cloud providers. Enterprises can use a one port, multiservice connection to reach Unitas Global's SDN POPs, and use its marketplace platform to establish on-demand network connections to multiple cloud providers. Unitas Global leverages a suite of tools to provide management, proactive monitoring and ticketing for multivendor network and cloud infrastructure in a single-pane-of-glass view.

Private direct IP peering to over 4,900 networks, including onramps to SaaS providers, is another key element in Unitas Global's competitive differentiation claim. Unitas Global uses this architecture to deliver more direct paths for application data, resulting in reduced latency and packet loss. Also, direct peering allows Unitas Global to have better control of the underlay connection and offer SLAs that guarantee the route and available bandwidth.

Further, with Unitas Nexus, the provider offers partners and enterprises a marketplace that enables them to automate design, pricing and ordering of IP and Ethernet services from millions of edge locations to public and private cloud destinations. Unitas Nexus uses a proprietary multisource database that analyzes in real-time multiple connectivity options based on clients requests, such as performance, cost or specific points of presence to interconnect. The database includes over 560 Ethernet, IP and wireless providers worldwide. The provider roadmap includes expanding Unitas Nexus API functionality to include self-service orchestration.

Verizon

Product or Portfolio Overview

Verizon is a global communication services provider that offers private cloud connectivity services to SMBs and enterprises through its Verizon Business division. Verizon's Secure Cloud Interconnect offers preprovisioned private bandwidth for both Layer 2 and Layer 3 connections to most popular cloud service providers. Verizon provides customers with the option to integrate SD-WAN, firewalling and WAN optimization add-on services to cloud connectivity. Verizon Software Defined Interconnect, delivered in partnership with Equinix, is a port-based service that connects enterprise's MPLS networks to over 200 cloud service providers within Equinix facilities.

How Verizon Competes

Verizon offers a comprehensive set of network, security and other ancillary services that leverage its global network, service capabilities and partnerships to deliver end-to-end connectivity to enterprises from last-mile access (Ethernet. broadband, 5G/LTE fixed wireless access [FWA]) to cloud interconnections.

Verizon offers two distinct cloud interconnect services — SCI and SDI. SCI provides preprovisioned private Layer 3 bandwidth to nine CSPs (Alibaba, AWS, DXC Technology, Google, IBM, Microsoft, Oracle, Salesforce and SAP) in 166 countries and territories through 230+ network-to-network interfaces (NNIs) in 10 countries.

SDI delivers private port MPLS and Ethernet connections (dedicated and switched E-Line and switched E-LAN) into 133 Equinix data centers in 18 metro areas (10 markets in U.S. and four in APAC — Hong Kong, Singapore, Sydney and Tokyo — and Europe — Amsterdam, Frankfurt, London/Manchester and Paris). The service allows end-to-end automation and on-demand bandwidth scalability up to 10 Gbps (depending on the market), using APIs for ordering, provisioning, billing and support for cloud interconnections to 200+ cloud providers globally colocated in Equinix data centers.

Verizon can turn up cloud connectivity with same-day activation for both SCI and SDI products. Virtual network services, including SD-WAN, firewalls and WAN optimization, can be provisioned on demand and service-chained in Verizon's network nodes to the SCI and SDI connections into the cloud.

Gartner expects Verizon to continue to extend its support for cloud connectivity with further expansion of network reach and capacity for cloud interconnections and innovative pricing options. Verizon supports enterprise adoption of edge computing use cases with VNS Application Edge, a new service that allows customers to deploy and manage their own containerized applications (Kubernetes) on the Verizon-provided, universal customer premises equipment (uCPE). Enterprises can manage those, together with Kubernetes clusters, in public and private clouds (e.g., AWS) from a single-pane-of-glass management portal.

References and Methodology

Gartner secured information for this report from multiple sources, including vendor surveys and briefings, primary research, analyst consultation and peer reviews.

Evidence

[1] **2020 Gartner Cloud End-User Buying Behavior Survey.** This survey was conducted to understand how technology leaders approach buying, renewing and using cloud technology.

The research was conducted online from July through August 2020, among 850 respondents from midsize and larger ($100 million or more in revenue) organizations in the U.S., Canada, U.K., Germany, Australia and India. Industries surveyed include energy, financial services, government, healthcare, insurance, manufacturing, retail, and utilities. All organizations were required to currently have cloud deployed. Respondents are involved, either as a decision maker or decision advisor, in new purchases, contract renewals or contract reviews for one of the following cloud types in the past three years: public cloud infrastructure (IaaS), public cloud platform (PaaS), public cloud software (SaaS), private cloud infrastructure, hybrid cloud infrastructure or multicloud infrastructure. Respondents were also required to work in IT-focused roles, with a small subset of procurement respondents.

The study was developed collaboratively by Gartner analysts and the Primary Research team.

Results of this study do not represent global findings or the market as a whole but reflect the sentiment of the respondents and companies surveyed.

Recommended by the Authors

Some documents may not be available as part of your current Gartner subscription.

How to Optimize Network Connectivity Into Public Cloud Providers

Innovation Insight for Software-Defined Cloud Interconnection

Market Opportunity Map: Enterprise Network Services, Worldwide

Forecast Analysis: Enterprise Networking Connectivity Growth Trends, Worldwide

Market Trends: SD-WAN and NFV Enable Shift to Internet and Cloud-Centric Enterprise Networks

Market Trends: 5 Key Enterprise Communication Services That Offer Opportunities for CSPs

---

Table 1: Service Providers Offering Private Cloud Connections

Cross-Connects at Colocation Hubs	*Carrier-Based Interconnects*	*Software-Defined Cloud Interconnects*
Cologix CoreSite DE-CIX Digital Realty Equinix	AT&T BT Tata Communications NTT Communications Orange Business Services Verizon Vodafone	Epsilon InterCloud Megaport PacketFabric PCCW Global Unitas Global
Direct cross-connects in colocation facilities. Enterprises need to source independently a private WAN connection to the colocation hub	Dedicated point-to-point connections as well as virtual private connections over shared prebuilt links connecting the enterprise WAN to the CSP's private cloud port.	SDN fabrics enable virtual connections on-demand from one entry point to the fabric to several cloud services. Enterprises need to source independently a private WAN connection to the SDN fabric.

Source: Gartner (July 2021)

Table 2: Examples of Private Cloud Connectivity Offerings

	Performance of Mission-Critical Workloads in the Cloud	*On-Demand Consumption and Enterprise Operation Autonomy*	*Support for Multicloud and Cloud-to-Cloud Use Cases*	*Privacy, Security and Compliance*
AT&T	Prebuilt, high-speed connectivity, 2M-100G+, into a majority of the largest data centers in the U.S. and a selection of others globally. Cloud-connect SLAs.	Near-real-time, on-demand virtual network connections to CSPs through service portals. API-driven provisioning in certain CSPs.	Support for multicloud use cases through colocation ecosystem and Total Access Orchestration platform.	Secure, private connectivity to 15 CSPs (AT&T NetBond for Cloud).
	Broad portfolio of underlay connectivity solutions (e.g., MPLS, Ethernet, dedicated internet).	Integration of virtual networking and virtualized workloads in cloud connections (total access orchestration).	Enablement of edge computing use cases (AT&T Network Edge).	Options for virtual firewalls in cloud connections. Option for MSS, including IPS/IDS, SWG, TDR and CASB.
Digital Realty	Global data center footprint provides access to 280+ facilities in 45+ metros across 20+ countries on 6 continents.	On-demand private network connectivity to an ecosystem of cloud, network, partners and providers leveraging Digital Realty's cloud connectivity.	Support for multicloud use cases. One physical connection from a PlatformDIGITAL location to connect to various cloud providers through virtual LAN connections.	Private connections within their operating metros through a dedicated fiber optic network for security and end-to-end control over data traffic.

	Performance of Mission-Critical Workloads in the Cloud	*On-Demand Consumption and Enterprise Operation Autonomy*	*Support for Multicloud and Cloud-to-Cloud Use Cases*	*Privacy, Security and Compliance*
	180+ onramps to the major 6 CSPs across PlatformDIGITAL in APAC, Europe and the Americas.			
Equinix	Global ecosystem of about 10,000 companies, provides customers access to 2,900+ cloud and IT services.	Software-defined interconnection to multiple cloud service providers as well as any other company's infrastructure on Platform Equinix.	Support for multicloud use cases. Software-defined network providing connections to multiple cloud providers colocated in Platform Equinix.	Direct cross-connects in colocation facilities.
	It also provides access to 1,800+ network services, 1,250+ financial services, 600+ content and digital media services, and 2,900+ enterprises.	Equinix Fabric integration into Network Edge and Equinix Metal support customers' own virtual workloads deployments.		

	Performance of Mission-Critical Workloads in the Cloud	*On-Demand Consumption and Enterprise Operation Autonomy*	*Support for Multicloud and Cloud-to-Cloud Use Cases*	*Privacy, Security and Compliance*
InterCloud	Network backbone is connected to several data centers and four major CSPs (AWS, Google, IBM and Microsoft).	SDCI, API-centric management platform.	Multicloud use cases enabled by its own fabric network as well as third-party provided underlays (e.g., Equinix, Megaport).	Direct cross-connects in colocation facilities.
	Routed access to the nearest InterCloud's Edge via a local loop and on-site equipment with end-to-end measurements and by default quality commitments in any interconnection, backed by SLAs.	CloudOps-oriented plugins (Terraform, Grafana).		Security resources on dedicated appliances (e.g., Palo Alto Networks or Fortinet firewalls). InterCloud's own dedicated security services (e.g., Cipher Service — HSM-as-a-Service).

	Performance of Mission-Critical Workloads in the Cloud	*On-Demand Consumption and Enterprise Operation Autonomy*	*Support for Multicloud and Cloud-to-Cloud Use Cases*	*Privacy, Security and Compliance*
Megaport	High availability network backbone across 700+ enabled data centers (100+ data center operators) and 230+ cloud onramps in North America, Asia/Pacific (APAC) and Europe, SD-WAN providers, and over 360 service providers.	SDN integrated with leading cloud service providers for on-demand and automated provisioning of capacity to service endpoints via a portal and open API.	Virtual cloud routers (Megaport Cloud Router) are instantly provisioned through web-based portals in virtual points of presence to control traffic at the IP level and support cloud-to-cloud networking use cases.	Private cloud connectivity.
		On-demand NFV service that supports branch-to-cloud connectivity on SD-WAN platforms (Megaport Virtual Edge).		
PCCW Global	Service accessible from 450+ data centers across 50+ countries and fully integrated with hyperscale cloud providers to connect customers directly to over 150 cloud regional zones.	Self-provisioning, on-demand SDN platform for spinning up private connections and flex bandwidth to cloud providers and other partners through a web portal and APIs.	Support for hybrid and multicloud deployment and management by connecting multiple clouds from a single port, either in the same cloud region or global regions.	Private preintegrated connections to multiple clouds from a single port bypassing the public internet.

	Performance of Mission-Critical Workloads in the Cloud	*On-Demand Consumption and Enterprise Operation Autonomy*	*Support for Multicloud and Cloud-to-Cloud Use Cases*	*Privacy, Security and Compliance*
	Private, high-speed, uncontended, low-latency network with multiple grades of class of service (CoS)/QoS and backed by carrier-grade SLA.	App to discover and establish private connections to other user networks and applications.		
Unitas Global	Global SDN interconnects 900+ data centers in 133+ countries with over 560 networks and fiber access providers.	Global SDN for automated on-demand access to cloud locations.	One port, multiservice on-demand network provides options for distributed cloud, hybrid cloud, multicloud and private cloud.	Private-direct IP peering.
	Direct peering to 4,900 networks connects SaaS, content and broadband providers for reduced latency. SLAs guarantee the route and bandwidth.	Network service management APIs.	Access through local Ethernet connections (multiservice Edge Link) supporting bandwidth split by service.	

	Performance of Mission-Critical Workloads in the Cloud	*On-Demand Consumption and Enterprise Operation Autonomy*	*Support for Multicloud and Cloud-to-Cloud Use Cases*	*Privacy, Security and Compliance*
Verizon	Diverse interconnections from MPLS backbone to CSPs in all major markets around the world for redundant, reliable service backed by a network SLA.	Automated, on-demand connections to CSPs through a service portal. Secure Cloud Interconnect (SCI) for bandwidth-based connections and Software-Defined Interconnection (SDI) leveraging platform Equinix for port-based connections.	Support for multicloud use cases through SCI to a cloud ecosystem of nine CSPs and through SDI to over 200 cloud providers colocated in Platform Equinix.	SCI and SDI: Private connections separated from public internet traffic.
	Broad portfolio of underlay connectivity solutions (e.g., MPLS, Ethernet, dedicated internet, mobile/LTE). Support for multiple services on one access connection (multiservice access).	APIs for integration in customer's ITSM tools. Option for virtual network and security services on cloud connections.		Virtual SD-WAN, firewall and WAN optimization tools are provided as add-on services to cloud connectivity. Option for managed security services.

This table showcases examples of different types of service providers in terms of market reach or competitive differentiation. Inclusion in the list does not imply Gartner's opinion on the quality of the service rendered by the service provider compared to others, either included or not in the table.

Source: Gartner (July 2021)