



## Equinix Network Edge: Laying the Path to Agile, Multicloud Networking

Sponsored by Equinix

*Powering clients to a future shaped by growth*

F R O S T & S U L L I V A N

<b>Introduction .....</b>	<b>3</b>
<b>The Business Value of Virtual Network Services to Enterprise WANs .....</b>	<b>4</b>
<b>Equinix's Network Edge—Bringing NFV Close to Enterprise Digital Partners .....</b>	<b>5</b>
<b>Why Should Businesses Care about Network Edge.....</b>	<b>6</b>
<i>Test New Markets and Quickly Expand Company's Global Presence.....</i>	<i>6</i>
<i>Seamlessly Connect Hybrid and Multicloud Deployments.....</i>	<i>6</i>
<i>Network Optimization to Support Mobility, Big Data, and IoT Trends .....</i>	<i>7</i>
<i>Provision-Enhanced Security Features in a Modular Fashion .....</i>	<i>7</i>
<i>Support Global SD-WAN Deployments.....</i>	<i>8</i>
<b>Significance of Network Edge to Other Stakeholders.....</b>	<b>8</b>
<i>Network Service Providers .....</i>	<i>8</i>
<i>Cloud Service Providers .....</i>	<i>9</i>
<b>Conclusion .....</b>	<b>9</b>

## INTRODUCTION


---

Cloud computing has completely changed the way enterprise IT deployments are planned today. IT resources are no longer confined to private data centers, with geographically distributed users trying to access enterprise applications in a hub-and-spoke model. Instead, enterprises are looking to deploy resources closer to the user to address speed and latency requirements while accessing critical applications. The COVID-19 pandemic has further highlighted the need to put data closer to the user as businesses across the globe have transitioned (wherever applicable) employees to a remote working environment. Deploying a traditional hardware-centric geographic presence is time consuming and expensive, and it is almost certain that post-COVID-19, businesses will re-evaluate their traditional branch office deployments with even more scrutiny.

In general, a business's "network edge" is increasingly located in carrier-neutral, co-location facilities or data center hubs operated by firms such as Equinix, as opposed to a company's physical location or branch site<sup>1</sup>. These data center hubs represent the "middle mile" in the enterprise's wide area network (WAN) infrastructure, with the co-location provider offering fully interconnected, low-latency, and reliable routes to major global metro centers. Businesses can establish a presence in the local data center and create virtual cross-connects to any other location on the co-location or data center hub provider's footprint. Equinix's Network Edge services enable businesses to quickly deploy virtual network services from multiple vendors, while globally interconnecting their partners, customers, suppliers, and employees. With data center hubs being a critical piece of the enterprise WAN infrastructure, the Network Edge service offering is a logical step for Equinix, as businesses increasingly embrace virtual network services.

While network service providers (NSPs) are focused on providing Software-Defined Networking (SDN) and Network Function Virtualization (NFV)-based virtual network services to enterprise branch locations, Equinix's Network Edge services put virtual network services in the middle mile, proximate to businesses' digital partners—cloud providers, internet service providers (ISPs), NSPs, content providers, and enterprises.

In this paper, we present an analysis of the business value of virtual network services, an overview of Equinix's Network Edge services, and its significance to enterprises.



**In general, a business's "network edge" is increasingly located in carrier-neutral, co-location facilities or data center hubs operated by firms such as Equinix, as opposed to a company's physical location or branch site<sup>1</sup>.**

---

<sup>1</sup> The network edge is the demarcation point where the enterprise network connects to an external service provider—be it an internet service provider (ISP), a network services provider (NSP), or a cloud service provider (CSP).

## THE BUSINESS VALUE OF VIRTUAL NETWORK SERVICES TO ENTERPRISE WANs

SDN is enabling the transformation of the WAN from a static, inflexible architecture to an agile and flexible software-centric one in which network resources can be pooled and consumed on demand. However, enterprise data centers (and branch locations) are still crowded with multiple hardware devices for separate network functions. For example, dedicated hardware is deployed for functions such as routing, firewall, and WAN optimization. The complexity and cost of deploying and managing multiple purpose-built hardware appliances in globally distributed branch locations exacerbate the traditional WAN problem.

NFV replaces proprietary network elements—hardware-based switches and routers usually contained within a NSP network—with industry-standard, centrally managed commodity servers. In the network, NFV allows routers, switches, firewalls, load balancers, content delivery systems, end-user devices, IP Multimedia Subsystem (IMS) nodes, and almost any other network function to run as software on virtual machines (VMs)—ultimately, on shared servers using shared storage. Using virtualized network functions (VNFs), enterprises can achieve enhanced control over their networking functions, with dramatically improved provisioning cycle times, and deploy new applications and services in a matter of hours or days. Enterprises realize a number of business benefits by deploying network functions as virtual network services compared to a traditional, hardware-centric approach. The following table presents a detailed comparison of the two.

**Figure 1: Traditional Hardware-Centric Approach vs. Virtual Network Services**

Description	Hardware-Centric Approach	Virtual Network Services
Appliance	Every network function runs on proprietary hardware appliances that need to be physically deployed and separately maintained. For multisite enterprise locations, this quickly adds up to hundreds or thousands of boxes to purchase and manage in the network.	VNFs can be deployed on a premises-based x86 white box or in the cloud, thus reducing the amount of hardware equipment in the enterprise WAN, which means less hardware cost, fewer moving parts, fewer things that could go wrong, and lower maintenance burden for the IT team.
Flexibility	With the hardware-centric approach, businesses need to commit to hardware and the vendor due to the CAPEX involved. As businesses emerge out of the COVID-19 pandemic and re-evaluate their branch office strategy, the hardware-centric approach offers limited flexibility.	Virtual network services offer immense flexibility for businesses to test new markets and new vendor solutions without long-term contracts. Virtual network services are typically sold as monthly or yearly subscriptions that businesses can pay using OPEX budgets.
Maintenance Costs & Time	Changes to the network functions require that a technician be sent on-site to carry out the re-configuration on the equipment.	In the case of VNFs, the network administrators can simply rip and rebuild that software-based function remotely. The VNF download and storage configuration can be up and running in a matter of minutes, as opposed to days with the hardware-centric approach.
Security	Traditional WAN security involves proprietary solutions from vendors, which can be expensive to deploy and manage.	Virtual solutions make it easier to deploy additional security measures in near real time, as functionality is in the virtual machines. Enterprise IT departments can choose to deploy modular security solutions by spinning up VMs to combine security solutions from multiple vendors.
Total Cost of Ownership (TCO)	High TCO, as enterprises need to invest capital to buy dedicated hardware for each network function. It also means vendor lock-in, with any changes requiring expensive overhaul.	Reduced TCO, as enterprises can use OPEX dollars to procure VNFs on demand, in an as-a-service model, and pay for them in a monthly, recurring charge model.

Source: Frost & Sullivan

## EQUINIX'S NETWORK EDGE—BRINGING NFV CLOSE TO ENTERPRISE DIGITAL PARTNERS

Equinix's Network Edge services allow businesses to deploy VNFs (for example, virtual router or virtual firewall) closer to the enterprise's network edge using the company's large global footprint of data centers. This enables businesses to efficiently connect partners, suppliers, and employees to their IT resources that are increasingly distributed among private data centers, co-location/hosting data centers, and multiple clouds.

The Network Edge offering is tightly integrated with the global interconnection platform, Equinix Fabric™, which is architected for the easy consumption of digital capabilities. Equinix Fabric™ includes network service providers, cloud providers, financial services companies, enterprises, and content providers, thus providing customers seamless access to Equinix's digital marketplace. Equinix offers one of the broadest data center footprints and portfolio of interconnection services in the market, with a digital ecosystem that includes: 1,800+ network providers, 2,900+ cloud and IT services providers, and nearly 3,000 global enterprises.

The Network Edge offering currently supports the following VNFs:

- Cisco® Cloud Services Router 1000v
- Juniper® vSRX Virtual Firewall
- Palo Alto Networks® VM-Series Firewall
- Cisco SD-WAN
- CloudGenix Virtual ION SD-WAN
- Fortinet FortiGate VM Series
- Fortinet Secure SD-WAN
- SilverPeak Unity EdgeConnect SD-WAN
- Versa FlexVNF™ SD-WAN
- VMware SD-WAN Edge



Businesses can order a virtual device, provision the VNF, and connect to Equinix Fabric™, or any other partner on Platform Equinix, in a matter of minutes. Network Edge services are available in a subscription model from Equinix, and customers can choose to bring their own license for virtual functions.

Network Edge is currently available in 11 Equinix data centers: Silicon Valley, Ashburn, Amsterdam, London, Singapore, Sydney, Chicago, Dallas, Frankfurt, Seattle, and Toronto, and there are plans to expand to several more locations in 2021, including Madrid, Tokyo, Sao Paulo, and Hong Kong.

## WHY SHOULD BUSINESSES CARE ABOUT NETWORK EDGE

---

Equinix's Network Edge offering aligns well with the market trends to help organizations speed up their digital strategies.

### Test New Markets and Quickly Expand Company's Global Presence

As organizations look to expand globally and bring new local sites online quickly, it may not always be evident which global regions make business sense without testing the markets. With Equinix Network Edge, businesses can test new markets in an inexpensive way as the service comes without any long-term contract, and it allows organizations to use OPEX dollars. For locations confirmed for expansion, Equinix Network Edge enables businesses to deploy a virtual presence on Platform Equinix™ to instantly and seamlessly deploy direct and secure virtual connections to cloud providers.

The COVID-19 pandemic has further highlighted the limitations of hardware-centric, hub-and-spoke branch architectures. The fact that most of the workforce (wherever applicable) had to transition to a remote working environment, almost overnight, has escalated the challenges of shipping, deploying, configuring, and managing physical network appliances. As businesses embrace long-term remote working trends, optimizing and securing user connectivity to cloud-based applications requires local presence. Businesses can use Network Edge services to establish their presence in local markets in close proximity to users to enable seamless access to cloud-based applications.

### Seamlessly Connect Hybrid and Multicloud Deployments

In the 2020 Frost & Sullivan Global Cloud Survey, over half of the respondents indicated "improving business efficiency & quality" as the most important strategic goal while evaluating cloud services for their organization. In the same survey, 42% of the respondents (up from 37% in 2019) indicated that they currently use a hybrid cloud, and another 43% indicated that they plan to use a hybrid cloud in the next two years. Additionally, it is common for enterprises to use a multicloud deployment for various workloads. Frost & Sullivan's cloud survey results indicate that 43% of the enterprises use three or more clouds, and they expect usage to increase significantly (more than 50%) in the next two years.

Equinix's Network Edge pre-integration with Equinix Fabric™ dramatically simplifies the process of establishing private connectivity for multicloud deployments. Equinix Fabric™ allows customers to use a single port to establish separate virtual circuits to a cloud provider's network. This is accomplished by cloud vendors locating their edge equipment at Equinix data centers, with connections to their cloud data centers through private networks. The edge equipment from multiple vendors is further interconnected within the Equinix Fabric™, enabling enterprises to seamlessly move workloads among their own servers and multiple vendor clouds.

Using Network Edge, businesses can deploy a virtual router to route traffic between multiple clouds. This eliminates the network costs associated with multiple networks connecting to different

cloud providers. It also addresses low latency requirements of certain enterprise applications hosted in the cloud, such as big data analytics, virtual desktop, and unified communications.

### Network Optimization to Support Mobility, Big Data, and IoT Trends

The current business environment is experiencing an influx of new technology trends—including mobility and Internet of Things (IoT)—requiring WAN managers to connect geographically dispersed teams and nodes. Mobile users are using their own smartphones and tablets to access corporate resources. Additionally, big data and IoT applications distributed across cloud and on-premises data centers are putting immense pressure on WAN bandwidth, making network optimization a key priority for network and IT managers.

The traditional WAN architecture—with traffic passing from remote sites into central data centers, and back via private networks (for example, MPLS)—does not work well for distributed deployments. This is particularly true in the case of IoT applications where the number of connected nodes can be extreme, making the use of private networks cost prohibitive. Furthermore, data from IoT nodes is typically sent to the cloud for storage and analysis.

Businesses can establish a local cloud presence closer to the edge (i.e., IoT nodes or remote employees) using Equinix Fabric™ and Network Edge to deploy a virtual router to route the traffic from the local cloud to a remote cloud or a private data center for analysis. The pre-integration of Network Edge with Equinix Fabric™ means businesses can build point-to-point connections between any two metro areas on the Equinix Fabric™.

### Provision Enhanced Security Features in a Modular Fashion

Admittedly, the migration of applications to cloud comes with its own set of challenges. Security, reliability, and application performance concerns continue to top the list of restraints every year. Cloud providers have been addressing some of these concerns by enhancing their services with core or optional security elements and offering better service-level agreements for availability.

For their part, enterprises have been adopting private connectivity to access cloud-based applications, as a way to leverage the security features already embedded in their WANs, to

**Security, reliability, and application performance concerns continue to top the list of restraints every year.**

<sup>2</sup> Frost & Sullivan defines hybrid cloud as any combination of cloud, hosting, and private data center resources that are managed and controlled as a single pool of resources to run a workload.

<sup>3</sup> Frost & Sullivan defines multicloud as an environment that combines services and resources from more than one cloud service provider. Multicloud deployments may involve workload or platform integration via APIs.

minimize the risks of distributed denial of service (DDoS) or other threats presented in the public internet. However, there will always be public-facing apps, like a company's website, which most users will access via the public internet. To reduce the security risks associated with traffic coming from public internet, businesses can choose to deploy virtual security using the Network Edge platform between the cloud apps and users.

NFV-based solutions make it easier to deploy additional security measures in near real time. IT administrators can choose to deploy modular security solutions by spinning up VMs to combine security solutions from multiple vendors. In the event of a DDoS attack on the VM or a VNF, the affected VM can be quickly detected, isolated, shut down, quarantined, and replaced by another dynamically instantiated VM. The threat can then be quickly resolved by applying security patches to fix the code vulnerability.

### Support Global SD-WAN Deployments

Global SD-WAN market revenue crossed the \$1 billion mark in 2019, with revenue and customer sites growing more than 100% from 2018 to 2019. Across industries, businesses are embracing these services as an integral part of their WAN transformation strategy, largely to gain cost and operational efficiencies.

Cost-effective branch site connectivity, fast deployment times, centralized network management, and optimized cloud connectivity are some of the drivers for managed SD-WAN adoption. As enterprise applications get distributed across multiple clouds, SD-WAN enables enterprise IT to predefine business policies through the SD-WAN controller to specify which cloud applications are suitably accessed directly through the internet versus backhauled to a hub site. With Equinix's Network Edge, which is a marketplace of virtual network devices, businesses can deploy virtual instances of SD-WAN closer to their branch sites in different metro centers to build interconnection hubs at Equinix locations, thereby optimizing branch internetworking and branch-to-cloud connectivity.

## SIGNIFICANCE OF NETWORK EDGE TO OTHER STAKEHOLDERS

---

While the Network Edge offering is most significant to enterprises, other digital partners in the Equinix ecosystem also stand to benefit.

### Network Service Providers

By establishing a presence at Equinix, NSPs drive incremental revenue for themselves by selling connectivity to Equinix Fabric™ (i.e., more bandwidth and services, new termination destinations). The pre-integration of Network Edge with Equinix Fabric™ will drive demand for bandwidth, as related network functions can be deployed quickly via the network connectivity. NSPs connected to the Equinix Fabric™ were able to extend connectivity to their customers with great speed and efficiency during the COVID-19 pandemic.

Additionally, as NSPs look to scale their virtual network services offering, Network Edge can help them expand into new metro areas by deploying virtual devices at hub locations, solving latency and reliability issues for distributed branch locations.

## Cloud Service Providers

Equinix Fabric™ enables CSPs to reach the large base of enterprises that are already co-located at Equinix data centers. Network Edge pre-integration with the Equinix Fabric™ will drive enhanced demand for cloud services, as enterprises can deploy cloud instances on the go and procure related network functions to route traffic from one cloud to another. The ability to deploy a virtual firewall in minutes means CSPs can also attract enterprise customers that otherwise may be reluctant to adopt cloud, fearing the security risks and performance inconsistencies of the public internet.

## CONCLUSION

---

Equinix has built a trusted global platform that enables organizations to interconnect and bring together the foundational digital infrastructure that businesses need to be successful in today's market. As companies look to become increasingly agile and accelerate digital transformation initiatives, virtual on-demand services are essential to achieving these business goals. Equinix continues to evolve its platform with this top-of-mind awareness: bridging physical and virtual deployments with Equinix Fabric™, enabling network modernization with [Network Edge](#), and providing companies with the ability to easily consume infrastructure when and where they need it with [Equinix Metal](#).

Network Edge services build on and complement the co-location and interconnection services the company offers, while bridging the gap in NFV-based services in the middle mile.

As private data centers give way to shared and cloud-based models, enterprises are looking to evolve their WANs to be more agile by utilizing SDN and NFV technologies. The combination of Equinix Fabric™ and Network Edge services allows businesses to do exactly that—quickly and reliably move traffic from branch to cloud and cloud-to-cloud by deploying virtual network functions 'on the go.'

Roopa Honnachari

Industry Director – Business Communication Services Strategist | Frost & Sullivan

[roopashree@frost.com](mailto:roopashree@frost.com)



## AUTHOR

---

Roopa Honnachari, Industry Director

## FROST & SULLIVAN

---

Frost & Sullivan, the Growth Partnership Company, works in collaboration with clients to leverage visionary innovation that addresses the global challenges and related growth opportunities that will make or break today's market participants. For more than 50 years, we have been developing growth strategies for the Global 1000, emerging businesses, the public sector and the investment community. Is your organization prepared for the next profound wave of industry convergence, disruptive technologies, increasing competitive intensity, Mega Trends, breakthrough best practices, changing customer dynamics and emerging economies?