White Paper

Network Modernization — A Must for a Successful Cloud Strategy

Sponsored by: VMware

Brad Casemore Frank Della Rosa Deepak Mohan
October 2020

SITUATION OVERVIEW

More than ever, applications are both the face and the digital lifeblood of businesses. They have gained mission-critical importance to business outcomes and competitive advantage. Whereas traditional applications primarily addressed back-office and front-office requirements, modern cloud applications deliver digital experiences and direct engagement to customers, partners, employees, and other stakeholders.

Application workloads are more distributed than ever before, situated in a connected cloud architecture that resides across on-premises datacenters, public clouds (IaaS), private clouds, and edge locations and delivered as SaaS. Application architectures have changed and continue to evolve. Monolithic application architectures are being displaced by modern cloud-native architectures defined by containers and microservices, and serverless technology (function as a service) is quickly emerging to take full advantage of hybrid architectures.

While the primacy of these data-centric applications is undeniable and will only grow with the rise of AI, a failure to ensure modernization of underlying network infrastructure can compromise and constrain your organization's application-driven digital-first strategies.

A modern network should be abstracted and transparent to developers and lines of business, but it remains a foundational element in serving the needs of the business, which include agility, flexibility, openness, security, and elastic scale. The network's purpose has always been to support and deliver applications to users, but today the application engagement and experience are paramount. As result, network connectivity and services must be software defined and governed by SLOs predicated on application experience. While physical network infrastructure remains essential for fast forwarding of packets, software abstractions and declarative management ensure that the physical underlay can be standardized and software driven, unconstrained by hardware-defined architectures and complex management practices.

To understand the relevance of modern networks to developer needs and business outcomes, we first must consider how modern applications are evolving with respect to their distributed nature, how they're developed, where they reside, and how they are delivered. To do so, we look at the current state and future trajectory of SaaS applications and IaaS workloads and then show how modern network infrastructure should ideally support the needs of those applications and workloads by achieving closer proximity to applications, possessing insights into application context, and matching the inherent agility and flexibility of modern applications. In doing so, the network is capable of delivering tangible business and operational benefits to stakeholders outside the confines of traditional IT operations and networking.

NEW GENERATION OF SAAS AND CLOUD APPLICATIONS

SaaS (business applications) is the largest and most mature segment of cloud computing, forecast to reach $225 billion, or 40% of cloud revenue, by 2024. SaaS has democratized the business application buying decision and elevated the end user to the role of key influencer in the process. In organizations undergoing digital transformation, the roles of IT and procurement are to enable and empower users with solutions and services that help them efficiently do their jobs and achieve desired business outcomes. The exponential increase in remote workers caused by the crisis created a sense of urgency to deliver end-user experiences that are on par with or better than centralized in-office experiences. The as-a-service model liberates key stakeholders to choose alternatives that best suit their needs and deliver fast time to value. Conversely, customers, consumers, and partners that consume applications are concerned primarily with engagement and experience, whether in an online marketplace or in streaming digital content.

While there are clear advantages to this change, it often creates security and compliance challenges for IT. Over the past few years, a new breed of SaaS and cloud applications have emerged in response to growing enterprise demand for increased speed, portability, and faster access to new cloud-only features. Table 1 highlights the forces contributing to a new generation of SaaS. These cloud-native applications feature microservices and container architectures to take full advantage of well-connected cloud architectures. The current crisis has ushered the future of work ahead of schedule with more remote workers and decentralized processes. Enterprises responding to the current crisis need to be able to situate workloads and bring capability to where work is performed. Application workload portability continues to be a critical design consideration for modern cloud networks.

The forces contributing to this new generation of SaaS are described in Table 1.

TABLE 1

Forces Contributing to a New Generation of SaaS

Force	Description
Volume and velocity of data	Exponential increase in the velocity and volume of data necessitates new sophisticated capabilities to analyze and act on insights.
Changing user expectations	The workplace is increasingly becoming digital and will continue in this direction as demographics change and millennials with considerably different attitudes and preferences become a greater presence.
Cognitive technologies	IDC expects that, by 2022, 50% of application workflows will be automated by AI, requiring most new applications to be AI enabled.
Unbundling of the monolith	There will be a transition over time to an agile and composable microservice architecture connected with APIs and orchestrated with Kubernetes.

Source: IDC, 2020

There are SaaS solutions for every vertical and functional market. To differentiate, some ISVs specialize in niche markets that are too small for the largest SaaS providers. These vertically tuned applications deliver greater business value for the customer and increased margins and customer retention for the ISV.

Modern SaaS applications are infused with autonomous capabilities, providing ready access to technologies like AI and machine learning for analyzing large volumes of data and freeing workers from mundane, repetitive tasks; increasing productivity; and improving the user experience. Intelligent applications are increasingly run on powerful platforms that help simplify data and application integration through APIs and provide a common framework and set of tools for extending or building new services. SaaS platforms enable businesses to rapidly build and deploy applications comprising best fit commercial and custom services.

EVOLUTION OF IAAS

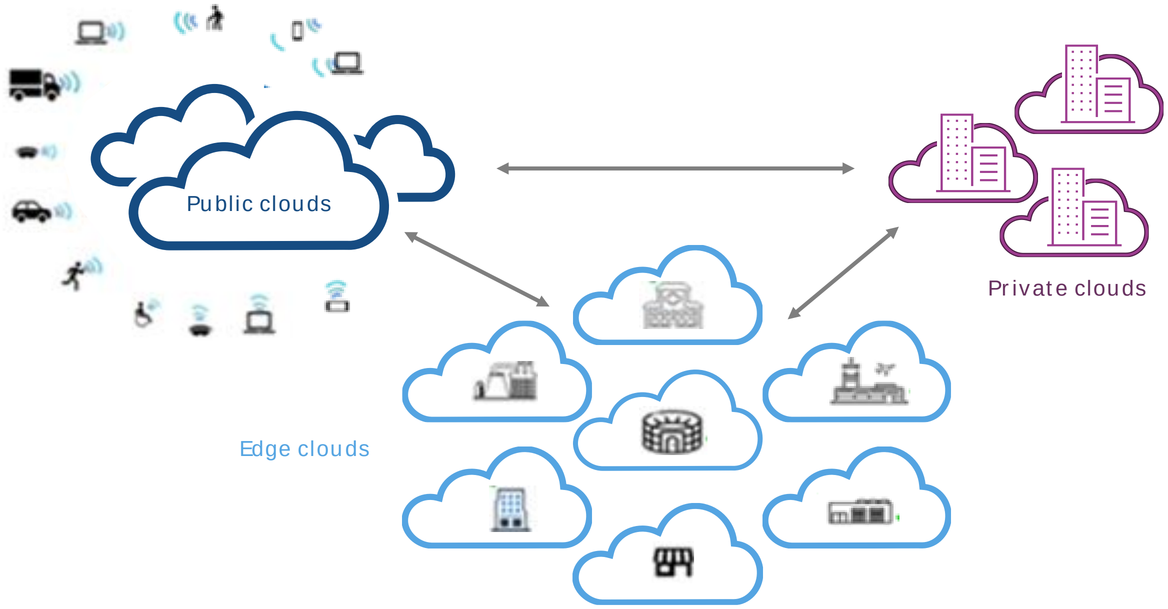
IaaS and Cloud Services Become Ubiquitous

IaaS has emerged as a competitive (and even preferred) infrastructure option for nearly all types of enterprise IT workloads. IaaS brings to workloads and enterprises the flexibility, agility, and access to new technologies, all of which are critical to business success and business survival in today's economy. This is evidenced by the 38% growth in the IaaS market seen in 2019 and the strong resilience seen in cloud services spending in 2Q20.

As enterprises increase and expand the use of IaaS, the focus has expanded from just a single public cloud provider to multiple premises across multiple public cloud providers. This includes patterns of infrastructure usage like hybrid cloud and hybrid IT. IDC's 2019 *IaaSView Survey* reveals that over 52% of enterprises are already using some form of hybrid cloud architecture for their infrastructure needs. This is up from 36% in 2018, highlighting the rate at which a hybrid cloud pattern is gaining prevalence. Moreover, the scope of cloud integration continues to expand – from a single cloud provider and platform to multiple cloud providers and hybrid IT to additional infrastructure footprints in multiple fragmented customer edge locations. Figure 1 captures the expanding boundary of the emerging multicloud landscape.

FIGURE 1

The Evolving Multicloud Landscape



Source: IDC, 2020

New Cloud Infrastructure Services Usage Patterns Create New Connectivity and Consistency Needs

With the growth in edge data, enterprise IT infrastructure footprints will increasingly see investments and application assets deployed in edge locations.

Modern enterprise IT applications will increasingly be distributed across premises, with components deployed based on best-of-breed technology availability and optimized location choices. These will be built in increasingly higher levels of abstraction to maximize agility and developer productivity (use of containers, serverless abstractions, CI/CD pipelines, etc.), enabling rapid development and deployment, supported by cloud-native compute and data services.

To support the productivity and agility of this new environment, developers will demand an equally abstracted and capable networking layer across their cloud footprints — to maximize the agility benefits of the cloud services being used for their applications across these IT locations. Developers invariably do not wish to directly interact with or manage network infrastructure, but they notice when it doesn't perform to expectations, and they benefit from the ability of the network to support abstracted application availability, workload portability, resilience, seamless service insertion, and workload protection. Capabilities such as a unified private networking address space, policies that can span physical footprints, and automated routing rule propagation can greatly assist in enabling this abstraction of developer experience from the underlying network layer fragmentation.

WHY THE MODERN NETWORK MATTERS

Many networks deployed today are not suited to the needs of modern SaaS and IaaS applications or PaaS environments. Traditional networks were designed and built in response to the requirements of the client/server era, predicated on hardware-defined architectures, manual provisioning processes, and laborious CLI-based management. The result is a less-than-agile model that is poorly suited to the needs of cloud applications and the CI/CD processes of DevOps and developers.

The networking implications of the cloud era are often underappreciated, but they are profound. All previous networks were built on the assumption that applications would be hosted in on-premises environments, resulting in network architectures and operational models that are no longer useful. This is as true in the datacenter or core — now dispersed and distributed among clouds — as it is at the edge, in branch offices and remote sites, where a growing percentage of the applications consumed actually reside in SaaS or IaaS public clouds rather than in traditional on-premises datacenters. This same philosophy carries over into the natively available network layers in the public clouds, which are designed to deliver security, governance, and automation, all within a single cloud provider's service.

At the same time, enterprises are demanding greater agility and speed throughout their digital processes, including the workflows involved in the creation, deployment, and management of applications. While developers and DevOps teams have moved to CI/CD processes and other agile means to expedite development workflows, they are often inhibited by a reliance on their organizations' slower-moving, hardware-defined network infrastructure. Responsiveness and quick turnarounds are required for resource requests, but the reality of network provisioning is another matter. Cumbersome provisioning processes consume too much time, hobbling developers and constraining the applications at the forefront of digital business. The ultimate result is a drag on business agility.

Unfortunately, many enterprises often aren't fully cognizant of their networks' cloud deficiencies and limitations until they experience them firsthand. By then, the network's inability to accommodate new requirements would have compromised enterprise realization of its multicloud strategy. In fact, IDC has found that enterprises frequently overlook or undervalue network modernization as a requirement for cloud and multicloud, only to learn belatedly and at high cost that a modern network is absolutely critical to success.

Conversely, enterprises that have experienced these problems, or have given the matter a greater degree of advance consideration, recognize the need for network transformation. Indeed, in IDC's 2019 *Datacenter Operational Survey,* enterprise respondents identified "ensure data security and compliance" and "improve network performance" as their top 2 priorities and challenges in hybrid IT and multicloud. Similarly, in IDC's latest *Cloud Pulse Survey,* 59% of enterprise respondents indicated that "integrated network processes across cloud providers" will be an important area for cloud investments for the next two years.

Meeting the Requirements of Cloud Apps

SaaS and IaaS present common networking challenges and also some that are unique to each realm. For SaaS, networks must be capable of ensuring that applications are delivered reliably and securely to employees and other stakeholders across a distributed enterprise landscape. The wide area network (WAN) plays a critical role here, and it has been modernized, in the form of SD-WAN, to address the needs of modern SaaS applications, which have network requirements that include adequate bandwidth, low latency (especially for collaborative apps), packet loss and packet reordering, and jitter.

In IDC's 2019 *Software-Defined Wide Area Networking (SD-WAN) Survey,* 73% of enterprise respondents indicated that SaaS and cloud services were currently important to their WAN technology choices, with that percentage rising to more than 78% when they were asked to consider how the situation might change in 12-24 months.

The reasons are clear. The traditional WAN is deficient when it comes to supporting SaaS. That's because the traditional WAN came of age in the client/server era, when applications resided exclusively behind the firewall in enterprise datacenters. WANs were designed and constructed to support branch-to-datacenter and branch-to-branch traffic, not to support increasingly critical branch-to-cloud application traffic. Further, the traditional WAN is poorly suited to the security requirements associated with cloud applications.

Meanwhile, PaaS environment requirements need network support for elastic scaling of Kubernetes environments, including multicluster and multicloud capabilities; advanced container networking, from the north-south ingress controller through to the east-west service mesh; and application layer network and security services, including load balancing and per-app workload protection.

For IaaS applications, many of the same challenges that relate to SaaS are present, but others are evident too. One challenge is the need for the traditional datacenter network to be both modernized and extended to serve as a distributed connected cloud datacenter network that supports all applications and workloads. This modern cloud network must be simple to consume, deploy, manage, and optimize. This simplicity derives from using software-defined application policy to abstract the otherwise inherent management complexity, which is compounded by the fact that the cloud-era datacenter is necessarily distributed and no longer a fixed geographic entity on enterprise real estate. The network must abstract complexity and bring simplicity to challenges associated with defining and enforcing consistent policies governing connectivity and security (including compliance requirements) for applications and workloads potentially scattered in disparate IaaS clouds, each of which has different connectivity models and API-based network services.

Another challenge is the fragmentation between the networking frameworks and capabilities that customers can use, as they transcend cloud provider and premises boundaries. While most providers now enable some level of integrated private level 3 networks for customer deployments that extend beyond their boundaries, the higher-layer optimizations on the network no longer function effectively in this fragmented yet integrated networking environment. Cloud services such as policy enforcement, routing rules, audit, and oversight capabilities, while comprehensive from a functional perspective, are not designed to function over an IaaS footprint that is fragmented across cloud providers and premises. And today, this is a growing need as customers look at best-of-fit services across the IaaS landscape to meet their functional, compliance, and integration needs for specific use cases.

This is further compounded by the growing prevalence of cloud-native containers and microservices, which further accentuates the need for networking to be not only end to end but also full stack and software defined. At the cloud-native application layer, modernized networks must be able to deliver automated self-service provisioning for developers and DevOps teams. The ability to set and enforce global governance mechanisms in such a rapidly evolving distributed application landscape is critical to ensure compliant and error-free operations at scale.

It is here that the network's capacity to enable and support workload portability comes into play. Through network virtualization, the network can provide an extensible fabric that ensures the definition and application of consistent network and security policies regardless of workload placement. This allows application owners to place workloads where they belong at any point in time, with the flexibility to move them as needed and to create redundant virtual networks to support application continuity and business resilience.

In the midst of making such a complex network environment simpler to operate, the modern network must also provide ubiquitous visibility. An old adage says that one cannot manage what one can't see. As one might surmise, visibility into cloud application flows over the modern network is essential to fast troubleshooting and remediation of issues that could cause serious application outages. Any modern network must offer real-time, application-centric visibility that can contribute to rapid root cause identification and resolution of issues, providing actionable insights not only into the source and location of the problem but also into how it can be promptly rectified. The fragmentation of infrastructure footprint discussed here makes holistic visibility an ever-increasing challenge today.

Supporting Business Outcomes with a Modern Network

These factors collectively translate into a need for network infrastructure and architectures that are software driven, reduce operational complexity, provide flexibility and elastic scalability, and are better aligned with business objectives and outcomes. This capability must extend across multiple platforms, clouds, and networks — from the now distributed multicloud datacenter to branch offices and remote sites, enhancing agility and flexibility in all places of the network.

As noted, the functionality should also extend across mixed application environments and infrastructure, not just on-premises and cloud applications but also applications running on bare metal, VMs, and containers. The network must be able to span and comprehensively support all these environments, including support for container-based microservices in the form of service meshes and API management.

BUSINESS BENEFITS

The business benefits that accrue from having network infrastructure that is truly responsive to the needs of cloud applications and their owners are compelling. They include the following:

- **Greater agility, flexibility, security, and resilience in support of cloud application delivery and integrity.**
- **The ability of the network to align with and facilitate business outcomes, including the release of new applications, product launches, and new customer-facing services.** This benefit directly aligns with the purpose of digital transformation. Indeed, a modern network can contribute materially to business outcomes such as faster delivery of applications and digital services, quicker product launches, and enhanced customer engagement and richer digital experiences.
- **Optimized application access and user experience, including the ability to deliver this benefit anywhere in the world.** The result is a uniformly engaging user experience that derives from optimized performance, security, and cloud-centric elastic scale.
- **Emphasis on what the business needs strategically from the network instead of on what network elements demand from the business.** Network infrastructure has historically been alienated from the needs of the business. The network has been widely seen as a collection of siloed devices that are complex and costly to manage, incapable of responding at speed to the dynamic needs of the business. Modern networks can change that perception, resulting in a new reality in which the network responds in seamless, smooth alignment with other infrastructure and the dynamics of the business.
- **Networking alignment with DevOps and CI/CD processes.** An alignment of automated network infrastructure and operational workflows with those belonging to other forms of infrastructure and DevOps and CI/CD processes results in expedited application-oriented workflows.
- **The capacity of the network to support workload portability and enhance hybrid IT and multicloud strategies.** A modern network can satisfy its rightful multicloud mandate as the digital nervous system for the cloud era. A device-based, manually operated approach to managing a multicloud network is destined to failure. Conversely, a modern network serves as a flexible foundation for a successful multicloud strategy that includes being able to place each workload where it belongs to achieve optimal business outcomes at any given point in time.
- **Global visibility and governance over a distributed IaaS footprint.** Network connectivity is the foundation on which the distributed architectures and deployments of the digital era are built. Failures, gaps, or errors in the networking or access control rules can result in issues ranging from poor customer experience to catastrophic data exposure. The ability to set and enforce networking policies, and have holistic enforcement and oversight, is a critical requirement for success in the digital era. This is critical at both early-stage cloud adopters, where the application owners and the developers own and execute the governance required, and mature cloud environments, where dedicated networking security teams ensure a holistic security posture.

Finally, as the world slowly recovers from the COVID-19 pandemic and the economic hardship that has followed in its wake, IDC has noted that business resilience and continuity have been cited as long-term enterprise IT priorities.

IDC strongly believes that the pandemic has driven a long-term requirement for software-driven network automation and multicloud networking. Indeed, network automation was cited as the top area for network investments in IDC's June 2020 *Future Proofing Enterprise Networking Survey.* Both network automation and multicloud networking can help organizations keep the lights on and keep businesses running, even in the event of another major crisis that prevents personnel from getting into on-premises facilities.

HOW VMWARE MODERN NETWORKS SERVE DEV/BUSINESS NEEDS

Addressing the evolving needs of digital transformation and cloud applications, VMware offers a software-driven network modernization portfolio to address the cloud-defined networking requirements of enterprise customers of all sizes.

VMware's conception of the Virtual Cloud Network (VCN), first introduced in 2018, was designed with cloud applications in mind. Defined entirely by software, built to provide a comprehensive L2–L7 network and security platform, the Virtual Cloud Network represents VMware's end-to-end vision for connecting and securing modern cloud applications, independent of underlying physical network infrastructure. Powered by VMware NSX and VMware SD-WAN (VeloCloud) technologies, the Virtual Cloud Network includes network virtualization capabilities that constitute a unified platform for consistent networking and security policies across VMs, containers, and bare metal workloads residing in any cloud environment.

Network virtualization, popularized by VMware through its acquisition of Nicira in 2012, invested network infrastructure with the same software-driven agility and flexibility, in addition to associated cost benefits, that compute infrastructure had previously derived from server virtualization. Through subsequent acquisitions and organic development within VMware, the company has assembled an end-to-end, full-stack network portfolio designed to address the architectural and operational requirements of cloud applications, both IaaS and SaaS.

Additions to the portfolio include NSX Advanced Load Balancer (formerly Avi Networks' Avi Vantage), which includes ingress controller functionality for Kubernetes environments and global server load balancing (GSLB) for global traffic management across availability zones, geographic regions, and clouds, and full life-cycle analytics, observability, and actionable network insights for network self-healing from vRealize Network Insight (vRNI) and NSX Intelligence, which have been further augmented by acquisitions of Veriflow (network simulation and verification), Nyansa, and Lastline.

As a result, the portfolio has evolved to align with and support the business imperatives and operational models of cloud applications and workflow processes.

In 2H20, VMware introduced the modern network architectural framework, which articulates the attributes of the network necessary to support hyper distributed, modern application environments. The Virtual Cloud Network enables customers to realize the modern network principles and future-proof their networking and security investments.

CONCLUSION

Fundamentally, the modern network must resolve a cloud-era paradox. On one hand, the network is arguably more important than ever, providing the digital nervous system for the growing tide of modern SaaS and cloud applications and data that are increasingly paramount to the success of organizations worldwide. At the same time, the network must become invisible to developers, lines of business, and application users while providing the agile operation and simple management required by network professionals, ITOps, cloud architects, platform teams, and SREs. At the end of the day, the network must do its job, simply and effectively, while staying out of the way.

Just because one can't see the modern network, however, doesn't mean that it isn't there, providing essential connectivity and network-related application services that enhance the availability, integrity, reliability, responsiveness, and digital experiences associated with cloud applications.

Software-defined networks and network virtualization provide enterprises with the network infrastructure that they require for a cloud era that features SaaS, IaaS, and multicloud applications. These software-based networks, leveraging application policy and abstractions that enable agility and simplicity, allow the network to seamlessly and unobtrusively extend from endpoints to clouds, helping businesses and developers achieve their objectives without having to concern themselves with the architectural and operational details of the underlying infrastructure.

If the network can achieve this goal, through software definitions and models, it will have solved the cloud-era paradox, invisibly delivering and supporting SaaS and IaaS cloud applications with the agility, consistency, and reliability that are essential to the realization of digital transformation strategies.

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. IDC helps IT professionals, business executives, and the investment community make fact-based decisions on technology purchases and business strategy. More than 1,100 IDC analysts provide global, regional, and local expertise on technology and industry opportunities and trends in over 110 countries worldwide. For 50 years, IDC has provided strategic insights to help our clients achieve their key business objectives. IDC is a subsidiary of IDG, the world's leading technology media, research, and events company.

Global Headquarters

5 Speen Street
Framingham, MA 01701
USA
508.872.8200
Twitter: @IDC
idc-community.com
www.idc.com