White Paper

Achieving Network Modernization for the Decade Ahead

Sponsored by: VMware and Intel

Brad Casemore
May 2020

IDC OPINION

This year, more than those that preceded it, marks the beginning of new enterprise strategies and priorities. In response to COVID-19, organizations of all sizes are prioritizing the need to empower employees to work from home. With the rise of business continuity and resiliency challenges — including workforce connectivity, virtual desktop performance, and datacenter security — the need for network modernization is undeniable. Driven by the imperative of business resiliency, in conjunction with digital transformation, enterprises need to define or refine their cloud operational models amid the growing embrace of hybrid IT.

Well before it made its way to the network, virtualization had been essential to efficiency gains and consolidation efforts in the enterprise datacenter. The consolidation of compute resources on virtualized servers helped reduce capex, and it also lowered opex by simplifying and streamlining the management of datacenter resources.

A relative newcomer, network virtualization (which extends throughout the protocol stack and through all places in the network) is poised to play a valuable role in helping further modernize network infrastructure.

This White Paper examines how VMware and Intel have worked together to deliver network virtualization capabilities that leverage software and hardware innovation to provide a wide range of business and operational benefits to enterprises that need their networks to be every bit as agile, flexible, secure, and elastically scalable as their other infrastructure supporting the business resiliency, availability, and performance of increasingly valuable applications and workloads.

SITUATION OVERVIEW

Digital transformation is an overriding strategic imperative for enterprises worldwide. It's also a never-ending but hugely necessary and beneficial journey involving continuous iterative processes that increase business efficiencies, enhance the digital experiences of customers and other stakeholders, and deliver tangible business outcomes such as faster time to market, increased revenue, and greater competitive advantage. As volatility takes hold across all sectors, business resiliency will play an increasing role in digital transformation imperatives. Enterprises that modernize and embrace technologies such as cloud, software-defined networks (SDNs), and automation will be able to pivot faster.

Cloud — not just as a destination but as an operating model and a set of key technologies — is an integral means through which digital transformation is realized. For enterprises, the inherent agility and flexibility of cloud processes and technologies must extend throughout IT infrastructure and operations if digital transformation strategies are to achieve their objectives.

There's no question that applications and the IT infrastructure that support them are becoming increasingly distributed. IDC predicts that more than 90% of enterprises worldwide will rely on a mix of on premises and dedicated private clouds, several public clouds, and legacy platforms to meet their infrastructure needs through 2021 and that 60% of all enterprises' IT infrastructure spending will be on public cloud infrastructure services in 2025.

These shifts demand extensive modernization and transformation of IT infrastructure, including the network. IDC has found that enterprises that fail to properly appreciate the need for network infrastructure modernization invariably discover that the network becomes an inhibitor, rather than an enabler, of digital transformation.

Enterprise networks need to be designed end to end to extend from on-premises datacenter or cloud cores, where increasingly important applications reside, all the way to the edge, represented by branch offices and remote sites where digital business takes place, yielding both employee productivity and valuable engagements and transactions with customers and partners. Modernizing the network through virtualization transforms how networks are architected and operated and is vital to enabling the enterprise to innovate.

Enterprise Drivers for Network Modernization

Digital transformation is a key driver of network modernization. As applications become the digital lifeblood of the modern enterprise, end-to-end enterprise networks should be regarded as the digital nervous system. It should also be evident these networks must be comprehensively modernized, in lockstep with other components of IT infrastructure, if enterprises are to fulfill ambitious mandates for organizational digitization. If compute is modernized, for example, but the network is unchanged — remaining hardware defined, brittle, static, relatively unintelligent, and operated manually — digital transformation initiatives cannot help but fall short of their goals.

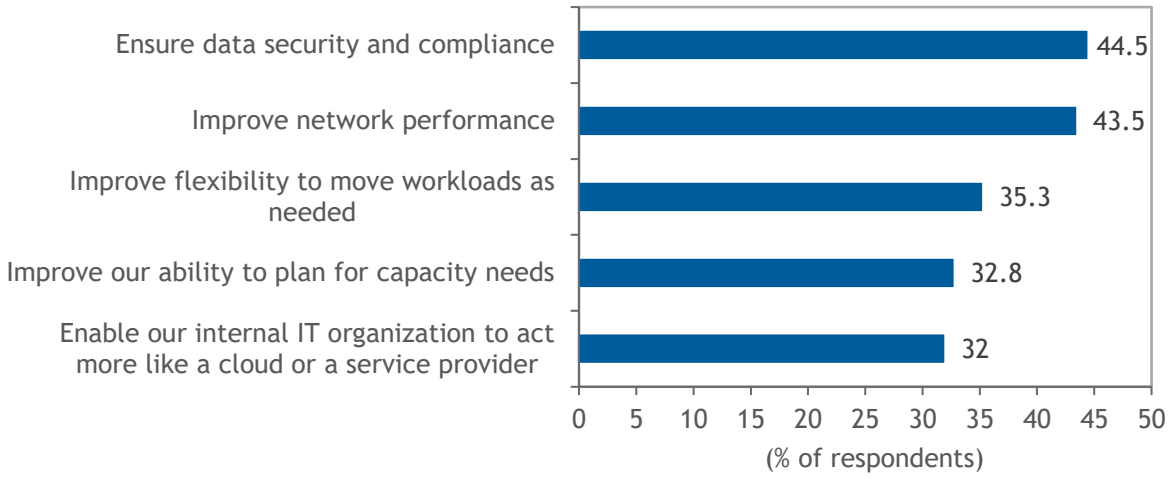
Furthermore, as enterprises grapple with volatility, modern networks that can be quickly added, updated, and removed (including security policies and telemetry data) — all via automation — solve many challenges for IT teams to quickly meet unpredictable needs. Business resiliency, a critical part of any IT strategy, has become even more salient, with the ability to connect, protect, elastically scale, and auto-remediate issues key for enterprise success.

A secondary driver of network modernization is multicloud, an extension of cloud that reflects the enterprise desires to ensure that applications and workloads are distributed effectively to run in environments that are best suited to their needs. While multicloud holds considerable potential benefits, enterprises understand that it also entails significant challenges. Among enterprise respondents to IDC's 2019 *Datacenter Operations Survey,* 43.5% cited the need for improved network performance as a top priority and challenge in a multicloud world, second only narrowly to ensuring data security and compliance. Interestingly, the third challenge identified, improving the flexibility to move workloads as needed, also has implication for the modernized enterprise network (see Figure 1).

FIGURE 1

Living in a Multicloud World

Q. Top priorities and challenges across traditional, private cloud, and public cloud datacenters



n = 400

Source: IDC's *Datacenter Operations Survey,* 2019

Unlike traditional enterprise networks, a modernized enterprise network for the cloud era must possess a range of essential capabilities that can extend end to end. Above all, it must be agile, a defining attribute of cloud, and that agility must extend across heterogeneous platforms and multicloud environments. To be clear, such agility can only be achieved through comprehensive network automation, not only for faster deployment and provisioning but also for ongoing day-to-day management, including faster troubleshooting and remediation of issues that threaten network availability and integrity. In that regard, software-defined networks, capable of policy-based microsegmentation, can provide levels of workload protection that were not available on traditional networks.

For network agility to be effective and sustained, however, automation must be fully invested with intelligence, which both informs declarative intent (policy) and enables a proactive approach to network operations. It is here that pervasive visibility, across places in the network and through all layers of the network stack, plays an invaluable role, validating and verifying policy and quickly identifying potential network events and issues before they result in disruptions and outages.

The Value of AI-Enabled Network Automation

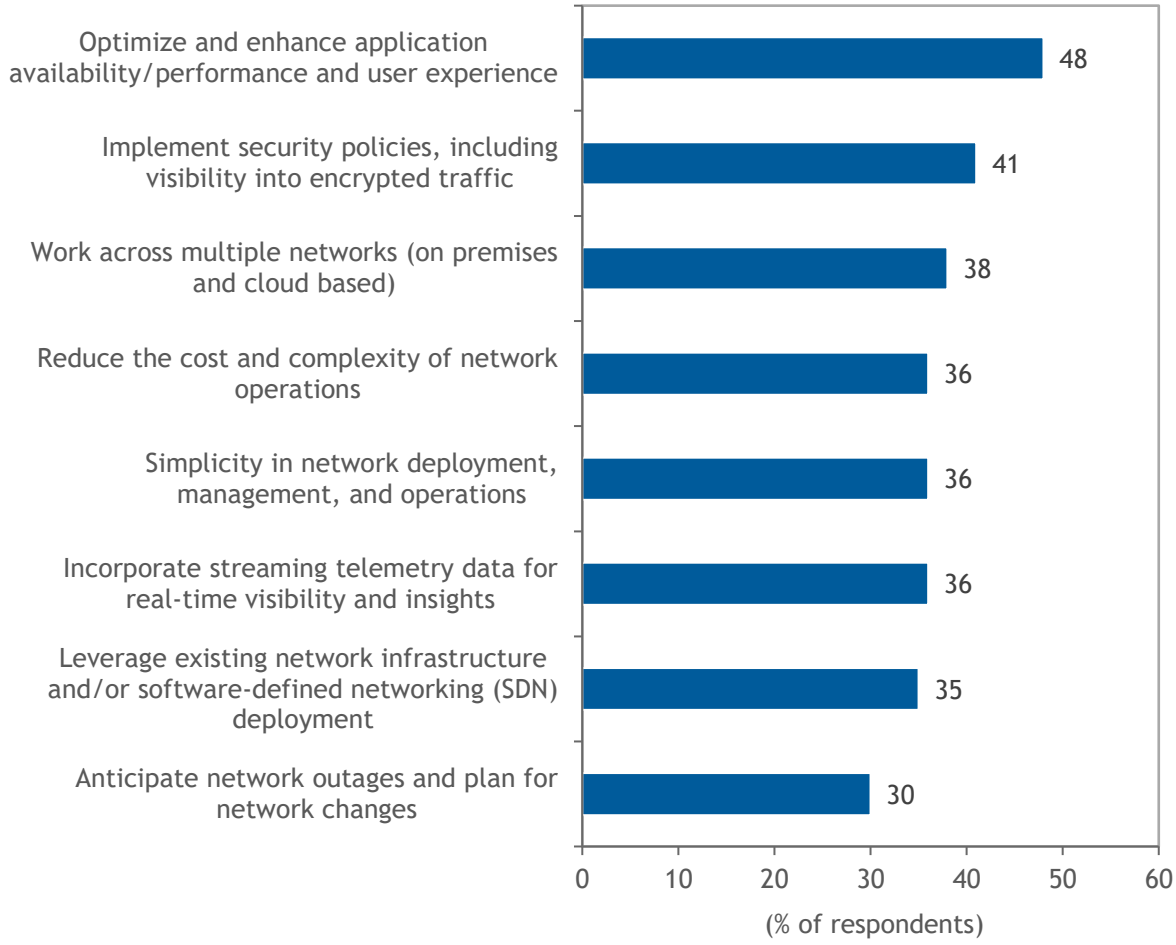
Enterprises recognize that AI and ML can be valuable enablers of intelligently autonomous networks. When asked to cite the most important aspects of AI-enabled network automation, respondents to IDC's *IT Strategy and AI Adoption Survey* highlighted the network's ability to "optimize and enhance application availability/performance and user experience" (48%). They also cited the ability to "implement security policies, including visibility into encrypted traffic" (41%), and the capacity to facilitate "work across multiple networks (on premises and cloud based)" (38%). Two other related points, both involving the need for greater simplicity in the traditionally complex practice of managing

networks, were also emphasized, namely the desire to "reduce the cost and complexity of network operations" (36%) and the need for "simplicity in network deployment, management, and operations" (36%) (see Figure 2).

FIGURE 2

Top Priorities for AI-Enabled Network Automation

Q. What do you see as the most important aspects of an AI-enabled network automation solution? (Pick three.)



Source: IDC's *IT Strategy and AI Adoption Survey,* February 2019

For obvious reasons, avoiding downtime is also a perennial concern. IDC estimates that the mean cost of enterprise downtime is $250,000 per hour. The number applies across all industries, organizational sizes, and geographies. Depending on the organization, the actual cost of downtime can vary widely. For example, large financial institutions that have heavy transaction loads can incur downtime losses measured in millions of dollars per hour.

The rise of cloud-native containers and microservices further accentuates the need for networking to be not only end to end but also full stack and software defined, with intelligent automation leveraging AI to perform

the automation of operational tasks and application layer visibility delivering unprecedented agility, flexibility, and workload protection for modern and traditional application environments. At the application layer, modernized networks must be able to deliver features such as thoroughgoing automation, including self-service provisioning for developers and DevOps teams. This automated functionality should extend to the provisioning and management of elastic North-South and East-West load balancing, traffic management for continuous integration and continuous deployment (CI/CD) processes, identical parallel "blue/green" production environments, and canary deployment scenarios (e.g., phased rollouts to subsets of users), all of which are increasingly important to digital enterprises across a range of industries.

Given all the criteria and challenges that must be met, modernizing end-to-end, full-stack network infrastructure can be a daunting proposition. From a resource perspective, enterprises often find it difficult to obtain the skills needed to work effectively across a software-defined landscape replete with APIs and automation rather than CLIs and manual processes. There is also a related challenge of optimizing IT processes and staff productivity. Further, there are the new challenges of implementing consistent security and access control policies across a hybrid IT and multicloud application landscape.

Requirements for Modernized Networks

The factors discussed previously collectively translate into a need for network infrastructure and architectures that are software driven and that reduce operational complexity, that provide flexibility and elastic scalability, and that are better aligned with business objectives and outcomes. This capability must extend across multiple platforms, clouds, and networks — from the inherently distributed multicloud datacenter to branch offices and remote sites, enhancing agility and flexibility at all places in 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, with management and orchestration and visibility that extends all the way up the network stack, from Layer 2 to Layer 7, including support for container-based microservices in the form of service meshes.

By now, there is no question that cloud, and its evolution to multicloud, has irrevocably changed the boundaries, traffic patterns, and requirements of core-to-edge enterprise networks. From a datacenter networking perspective, there are significant implications of the shift from having all applications reside on premises to having applications distributed across on-premises datacenters, colocation facilities, and emerging edge environments. In addition, the modern cloud era network must deliver an approach to business resiliency and disaster recovery that is equally agile, flexible, and resilient.

In this context, with applications and data increasingly distributed, latency has become a key consideration. Network architectures are being redrawn to reduce latency wherever possible, with edge computing environments, geosensing DNS-based global server load balancing (GSLB), and other technologies enlisted to ensure that the network meets exacting always-on application and data needs. Architecting edge-to-cloud and multicloud networks requires a deeper and broader knowledge base than in the past; to ensure success for both end-user experience and data management, network administrators must now understand not only application latencies, data locations, and usage patterns but also compliance and security requirements.

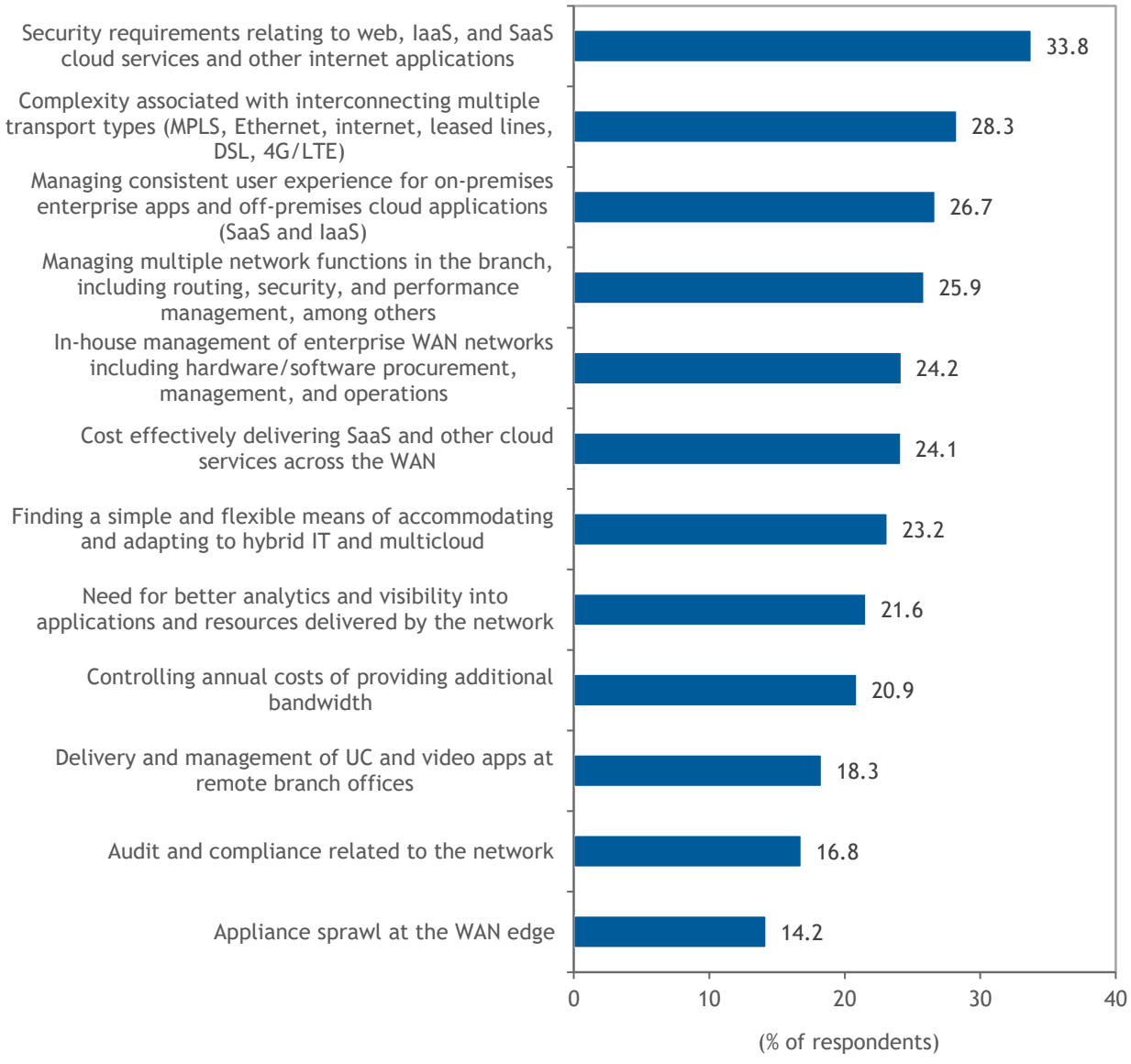
Similarly, the WAN also faces the need for transformation as branch offices and remote sites now must quickly, reliably, responsively, and securely connect to applications in SaaS and IaaS clouds as well as on-premises datacenters. Traffic patterns have changed profoundly, as have edge security requirements and WAN transport connectivity options, with broadband internet breakout increasingly preferable and viable relative to MPLS for many cloud applications and services. Indeed, in IDC's recent *Software-Defined WAN (SD-WAN) Survey,* enterprise respondents worldwide indicated that

their top 3 WAN challenges were addressing the security requirements of SaaS, IaaS, and other web-based services; mitigating the complexity associated with multiple transport types (i.e., MPLS, Ethernet, internet broadband, 5G/4G/LTE); and delivering a consistent user experience for on-premises and cloud apps (IaaS and SaaS). Many of the other WAN challenges they cited have similarly arisen as a consequence of the rise of distributed applications and a hybrid IT landscape (see Figure 3).

FIGURE 3

Cloud Security and Hybrid WAN Complexity Among Top WAN Challenges

Q. Please select the three most significant WAN challenges (from the following) that best relate to your company.



Source: IDC's *Software-Defined WAN (SD-WAN) Survey,* November 2019

Ideally, to further reduce complexity and increase agility and operational efficiency, enterprises pursuing a modernized, software-defined approach to end-to-end network infrastructure should place considerable emphasis on implementing an industry-standard hardware infrastructure that can support full-stack network virtualization across all infrastructure, including VMs and containers. This will provide operational simplicity and deliver operational efficiencies while also delivering the necessary performance, scale, and security.

IDC has witnessed this trend manifesting itself in the market, with the growth of datacenter SDN and SD-WAN and the increasing virtualization of network functions throughout the stack, overwhelmingly on Intel-based hardware platforms. SDN, including network virtualization overlays (NVOs) such as VMware NSX, is projected to sustain a CAGR of 17.7% from 2018 to 2023, when SDN datacenter software will generate approximately $2.8 billion in revenue. For its part, the worldwide market for SD-WAN infrastructure is forecast to record a CAGR of 30.8% topping $5.25 billion in 2023. Meanwhile, application delivery controllers (ADCs) increasingly are taking virtualized software form factors rather than hardware appliances. Revenue from software form factors of ADCs, including load balancing functions running in public clouds, surpassed revenue from ADC hardware appliances in 2019 and the gap will widen in subsequent years.

HOW VMWARE AND INTEL ADDRESS NETWORK MODERNIZATION

From digital transformation to business continuity, VMware and Intel have helped thousands of enterprises with network modernization for large and small environments. VMware and Intel co-engineered solutions leveraging industry-standard hardware infrastructure with network virtualization software that together deliver high performance, scale, resiliency, and efficiency for software-defined switching, routing, security, load balancing, analytics, and service mesh for datacenters, cloud, and edge. The joint integration enables enterprises to modernize and automate their infrastructure with the agility, resiliency, and efficiency they need for any market condition.

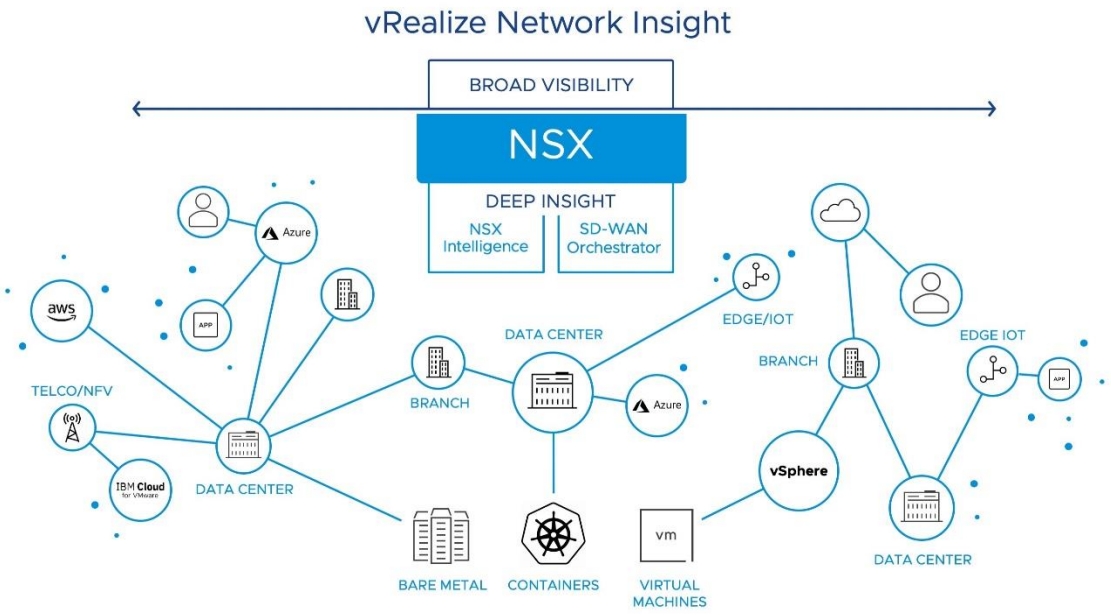
VMware introduced Virtual Cloud Network (VCN) in 2018, which has now been adopted by thousands of customers worldwide including 89 of the Fortune 100 and 8 of the top 10 largest telcos. Defined entirely in software and built on a complete L2–L7 networking and security platform, the Virtual Cloud Network is VMware's end-to-end vision for connecting and securing applications, independent of the underlying physical network infrastructure. Powered by VMware NSX and VMware SD-WAN by VelcoCloud technologies, the Virtual Cloud Network encompasses a growing portfolio of network virtualization solutions that form a unified platform to bring a consistent networking and security policy for VMs, containers, and bare metal workloads from cloud to datacenters to edge.

When combined with the industry-standard Intel Architecture (IA), Virtual Cloud Network helps enterprises enhance business and operational agility, achieve greater operational efficiencies, and support the scalability, reliability, and security required for critical applications in a world increasingly defined by cloud principles and technologies.

VMware's Virtual Cloud Network benefits from an array of Intel optimizations, discussed in this section, to address not only current requirements but also emerging and future needs relating to evolving network architectures, operations, and infrastructure, all of which must respond to the increasingly distributed applications and data that are driving the digital transformation initiatives of organizations worldwide (see Figure 4).

FIGURE 4

Network Modernization with Virtual Cloud Network



Source: VMware, 2020

VMware Virtual Cloud Network (see Figure 5) is designed to provide a seamless, secure, software-defined networking layer from datacenter to cloud to edge. It simplifies hybrid operations with an all-in-one cloud model that extends intrinsic security and end-to-end policy consistency across an increasingly distributed environment. The Virtual Cloud Network can be leveraged for a unified L2-L7 stack to replace purpose-built appliances. Through VCN, enterprises can achieve integrated management and security, consistent policies across clouds, and end-to-end analytics and troubleshooting. VMware's software-defined networking portfolio, which runs on optimized Intel-based hardware, comprises the following:

- **VMware NSX,** which offers a full-stack networking functions all-in software, supports Intel-based hardware platforms to provide connectivity and network security for VMs, containers, and bare metal workloads running on premises and extending out to public clouds. As a software-defined approach to networking, NSX helps enterprises accelerate network automation with a single API to improve network agility while providing zero-trust security through workload protection offered by microsegmentation, distributed firewall, and IDS/IPS and addressing the multicloud challenge of ensuring consistent network and security polices across hybrid environments.

  In addition, capex and opex cost savings can result from the consolidation of virtualized network functions on Intel-based hardware. NSX Cloud, which uses the same management and control plane as NSX Data Center, ensures application and enforcement of consistent network and security policies for workloads in public clouds such as AWS, Microsoft Azure,

IBM Cloud, Oracle Cloud, and Google Cloud. As a result, NSX can support network and security for many use cases such as traditional monolithic apps and microservices, network automation, cloud-based application continuity, disaster recovery, and workload migration.

With NSX-T 3.0 now publicly available, Intel QuickAssist Technology (QAT) Support for VPN Bulk Encryption is now supported to offload VPN bulk encryption on Bare Metal Edge.

- **VMware Service-Defined Firewall,** built into the infrastructure providing intrinsic security, detects and mitigates threats on East-West traffic within the datacenter perimeter. From its position inside the hypervisor, the Service-Defined Firewall provides visibility into both network traffic and application behavior to provide workload protection. With advanced microsegmentation and software-based IDS/IPS, the Service-Defined Firewall minimizes attack surface and reduces false positives by attaching curated signatures to applications that move as applications migrate with vMotion across networks. Optimized on Intel Architecture, the Service-Defined Firewall can reduce capex and opex compared with custom firewall appliances that use proprietary hardware and can be costly to maintain.
- **VMware NSX Advanced Load Balancer,** a virtualized ADC platform formerly by Avi Networks, provides elastic load balancing and performs SSL termination in software. It leverages advances in Intel's second-generation Intel Xeon Scalable processor family to provide high capacity and scalability. In this area, Intel has added enhancements such as Advanced Encryption Standard New Instruction (AES-NI) to further offload cryptographic workloads onto dedicated rather than general-purpose processing.

  As Intel moves forward with subsequent generations of processor technology, NSX Advanced Load Balancer performance will continue to improve.

  With an integrated web application firewall (WAF) and analytics, NSX Advanced Load Balancer offers centralized policy management, programmability, and end-to-end application insights into performance, end-user experience, and application security.

  The operational and business benefits of using VMware NSX Advanced Load Balancer on Intel-based hardware include greater operational agility and efficiency, the ability to better align with the needs of applications and developers (through self-service provisioning and other means), and cloudlike elastic scalability, as opposed to having to overprovision as is the case with hardware ADC appliances. These benefits extend to cloud-native application environments compromising containers and microservices. Indeed, both VMware NSX Data Center and VMware Advanced Load Balancer provide virtualized networking and security services spanning containers, VMs, and bare metal, including capabilities such as microsegmentation, distributed firewalls, egress/ingress policies for each container/VM, and IDS/IPS capabilities.

- **VMware SD-WAN by VeloCloud** is designed to deliver a rich user experience for enterprise SaaS and legacy applications delivered from any cloud. The VMware SD-WAN solution consists of three main components, starting with the VMware SD-WAN Edge by VeloCloud deployed at the customer's branch office, in datacenters, or in customers' public cloud instances. The VMware SD-WAN Edge is available as an Intel Architecture–powered appliance or as a software or virtual appliance that can be run on Intel Architecture–based servers. The VMware SD-WAN Edge by VeloCloud combines application, network, and threat intelligence to deliver applications securely based on link conditions, business policies, and application requirements.

  The VMware SD-WAN Edge leverages both the Intel Architecture with Data Plane Development Kit (DPDK) and QuickAssist Accelerator (QAT) to deliver fast data plane performance for SD-WAN, security, and other network functions, helping enterprises reduce the costs associated

with procuring and maintaining multiple hardware appliances, increase WAN operational efficiencies, and improve the security posture at the branch. The ability to innovate and add features through updates to the VeloCloud software running on Intel-based hardware helps continually meet evolving branch needs for application performance and reliability.

The second component, VMware SD-WAN Gateway by VeloCloud, is a distributed multitenant gateway that optimizes access from any facility across the globe to public cloud, private cloud, and SaaS cloud services with simple on-ramp capabilities. The VMware SD-WAN Gateway ensures scalability, redundancy, and on-demand flexibility.

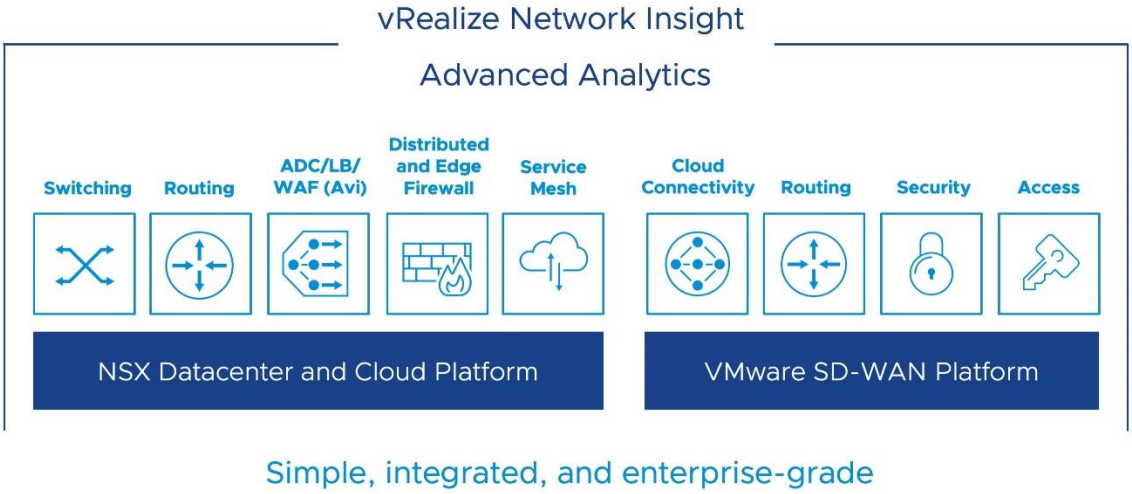
The third component of the solution is the VMware SD-WAN Orchestrator by VeloCloud, which facilitates service deployment, management, and teardown — including service activation and virtual appliance or virtual network function (VNF) software installation, configuration, and real-time monitoring. The orchestrator can be deployed either in the cloud or on premises in a datacenter and reports key performance metrics and end-to-end quality of service. The VMware SD-WAN Orchestrator is both multitier and multitenant.

- **vRealize Network Insight (vRNI)** provides end-to-end visibility and analytics across datacenters, cloud, and edge to help enterprises monitor and troubleshoot network issues. vRNI provides visibility for hybrid and multiclouds such as VMware Cloud on AWS and Microsoft Azure as well as underlay and overlay networks and SD-WAN. With ML-based application discovery, Kubernetes pod visibility, network path visibility for clouds and hop-by-hop latency metrics, vRNI is a comprehensive system for network operations to reduce MTTR, optimize application performance, and troubleshoot virtual and physical networks.

- **VMware Tanzu Service Mesh** operates at the application layer providing discovery, connectivity, observability, control, and security for microservices. Tanzu Service Mesh leverages an open source project, Istio, with enhanced enterprise services across multiple Kubernetes clusters, and extends visibility to users, data, and services. Tanzu Service Mesh is designed to provide support for multiple application platforms, public clouds, and runtime environments and supports federation across multiple clusters.

FIGURE 5

Foundation for the Virtual Cloud Network



Note: VMware offers a full stack of L2-L7 networking and security services.

Source: VMware, 2020

Capabilities and Features of the Intel Architecture

The Intel Architecture provides a foundational industry-standard hardware infrastructure that supports extensible virtualized networking and security functions for VMs and containers. In that vein, Intel and VMware have co-engineered optimizations that leverage the Intel developer tool set, including the following (see Figures 6 and 7):

- **The second-generation Intel Xeon Scalable processor data-centric platform** incorporates advanced compute cores, a new memory hierarchy, connectivity, and acceleration designed to provide high performance and infrastructure efficiency across a wide range of network-intensive workloads. Intel claims the new processor platform delivers up to 1.58x performance improvement over the previous generation of Intel Xeon Scalable processors for network workloads. Intel also notes that the platform supports up to twice the number of subscribers for the virtualized SD-WAN services and up to five times more virtual network function capacity when complemented with Intel QuickAssist Technology and the Intel Ethernet 800 Series Ethernet controllers.
- **The Data Plane Development Kit** is a library of open standard software drivers originally developed by Intel that boost packet processing performance by routing network packets around the Linux kernel. DPDK enables NSX Edge to increase packet performance to the North-South off-ramp traffic flows, while the DPDK-enabled Enhanced Datapath mode supports high-performance packet processing for East-West traffic in NSX.
- **Intel QuickAssist Technology** provides a software-enabled foundation for security, authentication, and compression, increasing performance and efficiency.

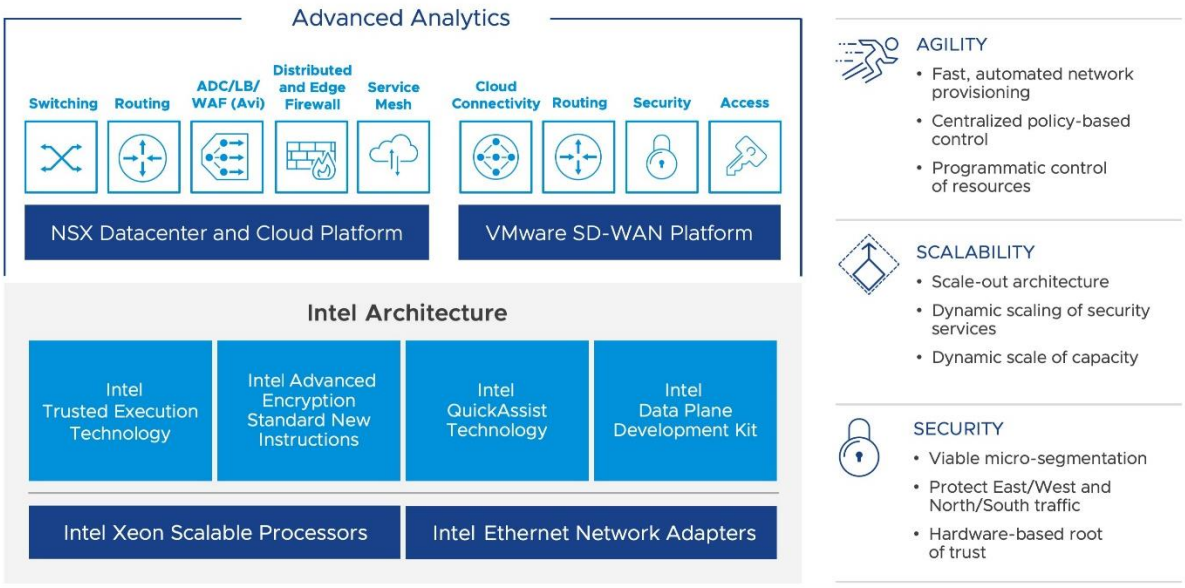
- **Intel Advanced Encryption Standard New Instructions (Intel AES-NI)** accelerates key parts of the encryption algorithm in hardware, making pervasive end-to-end encryption possible without degrading performance. NSX also benefits from Intel AES-NI to accelerate processor-intensive encryption and decryption routines in hardware, helping maintain pervasive encryption as workloads and topologies scale.
- **Intel Trusted Execution Technology (Intel TXT)** moves the root of trust from software to hardware, checking the execution environment against a known good image at start-up to verify that no unauthorized changes have been made that could jeopardize the security of application workloads.

  An underlying function at the heart of most security applications, pattern matching is supported by Hyperscan, Intel's software pattern matching library, capable of matching large groups of regular expressions against data blocks or streams. This is useful for network and security applications that need to scan large amounts of data at high speed, such as NSX IDS/IPS optimization.

  The NSX network virtualization platform runs on second-generation Intel Xeon Scalable processors and 10/40Gb Intel Ethernet Network Adapters. The Intel processors (Intel C620 Series Chipsets) reduce overhead for near-native I/O performance with SR-IOV.
- **10/40Gb Intel Ethernet Network Adapters** enable logical networks that allow VMs to communicate across subnets while reducing configuration and management requirements and increasing network responsiveness and flexibility.

FIGURE 6

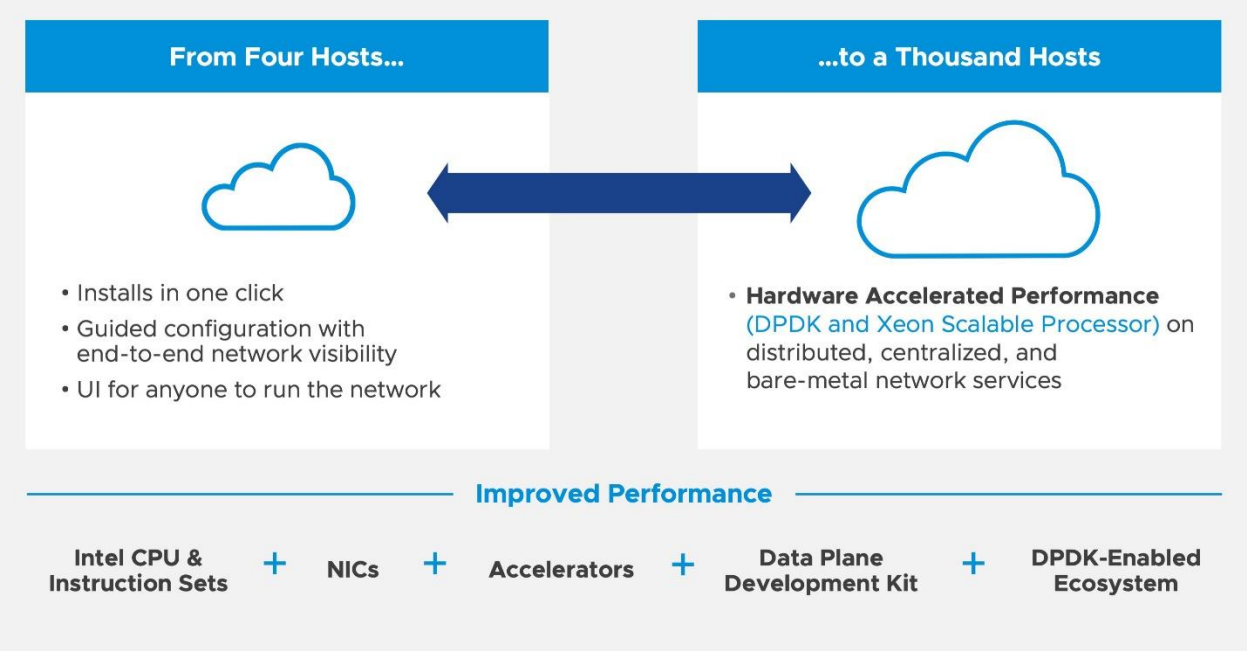
VMware and Intel Joint Networking Solutions



Source: VMware and Intel, 2020

FIGURE 7

VMware Cloud-Scale Platform — "Intel Accelerated" for Anyone



Source: VMware and Intel, 2020

CHALLENGES/OPPORTUNITIES

The biggest challenge for enterprises and for the vendors serving them, such as VMware and Intel, is represented by a paradox. On one hand, enterprises often fail to recognize the salience of network modernization to their digital transformation initiatives. That said, even when they do acknowledge the need to modernize their network infrastructure, they are sometimes flummoxed by the seeming enormity of the challenge, especially in the context of preexisting investments, processes, resources, and skills relating to their legacy network infrastructure. As such, the need for network modernization is either underappreciated or perceived as too daunting.

Nonetheless, VMware and Intel are well placed to help enterprises acknowledge the need for end-to-end network modernization and to enact it in a way amenable to any given enterprise's IT culture, previous network investments, existing operational processes, and current skill sets. The key for the enterprise and its suppliers is an emphasis on simplicity and the benefits that accrue from it, which are aligned with digital transformation and help establish network infrastructure, and those who operate it, as a meaningful contributor to business outcomes rather than a cost center and inhibitor to business agility.

Enterprises that overcome these hurdles, as well as the vendors that help them do so, stand to benefit significantly from a compelling array of benefits, both operationally and from an overall business perspective.

CONCLUSION

2020 started with volatility and uncertainty that spread globally. While digital transformation will continue to inexorably drive enterprise infrastructure automation, business resiliency is now also a paramount consideration for network planning. Modernization and automation are critical as enterprises increase their adoption of cloud, modern applications, AI, and analytics.

The cloud is more than a destination for workloads. As an integral tool in service to digital transformation, it is also an operational model and a set of software-driven and -defined technologies that are increasingly essential to business outcomes and operational efficiencies.

For enterprises and their IT departments, there is an acute need for infrastructure to be better aligned with the requirements of an increasingly digitized business. From a networking perspective, that translates into a demand for networks that are as agile and flexible as they are reliable and scalable, delivering unprecedented availability, resilience, and software-defined, AI-driven programmability and visibility. In addition, modern networks must possess full-stack integrity for security and workload protection, and they must be simple to provision and to manage on a day-to-day basis.

To achieve these results, enterprises require a blend of software-based agility, flexibility, and innovation predicated on a robust, reliable, and scalable hardware foundation. The partnership between VMware and Intel was designed to meet that mandate, and the two companies now have more than a decade of joint history in collaborative engineering and technology integrations. Presuming the two vendors continue to work closely together to satisfy the evolving needs of hybrid enterprises, they will be well placed to assist enterprises with the network modernization initiatives that are integral to their 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