SOLUTION BRIEF

Multi-Cloud Software-Defined Network

Enterprise Network Virtualization with VMware NSX* on Intel® Architecture

Network virtualization using VMware NSX* hosted on Intel® architecture-based servers provides a holistic environment that spans on-premises resources and multiple public clouds. Workloads can pass freely among these resources, with a consistent logical architecture and centralized control. Enterprises benefit from enhanced application performance and responsiveness, with greater agility, scalability, and security.

In the past several years, cloud computing has matured from being a market disruptor to become a mainstream foundation for digital enterprises. The benefits of cloud adoption are manifest in improvements to efficiency, agility, and cost for a broad range of workloads and usages. In fact, running workloads in a multi-cloud environment has become a strategic imperative, and a survey by Enterprise Management Associates indicates that more than 60 percent of enterprises reported using two or more public cloud providers[1].

Enterprise strategists are working to modernize their networks for multi-cloud environments to handle workloads of all types and sizes, including those running on bare metal, in virtual machines (VMs), and in containers. Seamless interoperation among all these modalities is vital, along with enabling IT organizations to flexibly manage, control, and automate all resources from a central point.

In addition to abstracting all these environments so workloads can pass freely among them, enterprises also need to choose resources where each workload should operate, according to the needed balance of price, speed, and capacity. In addition, considering the geographic location of workloads can also be vital for reasons of data sovereignty, because data is governed by the laws of the jurisdiction where it is located. This factor can have implications for issues such as regulatory compliance as well as the rights of specific governments to access the data.

VMware and Intel share a vision of virtualized networking that securely interconnects any workload, across any environment. The companies have been actively collaborating for several years to bring that vision about by co-engineering optimized solutions based on VMware NSX* running on Intel® architecture-based hosts. In addition to being optimized for typical network considerations such as performance, scalability, and security, the solution stack is designed to overcome challenges that are specific to multi-cloud networking, as shown in Figure 1.

The virtualized networking stack is built for operational consistency across the enterprise, from the data center to the cloud to branch and edge locations. It provides a coherent environment with a single set of processes and tools for management, security, and control. Hardware platforms range from relatively modest Intel Atom® processors to Intel® Xeon® D processors and Intel® Xeon® Scalable processors at the high end.

The solution provides built-in workload protection, applying security policy at the per workload level so that it travels with the workload as it migrates among hosts. Its design helps ensure that incongruent technologies such as otherwise incompatible file and VM formats, data structures, and applications are compatible with the whole environment, including across clouds.

Figure 1. Critical capabilities specific to multi-cloud networking.

Virtualizing Networks Across Deployment Models with VMware NSX*

VMware NSX is a comprehensive network virtualization and security platform that provisions and manages networks entirely in software, abstracted from the underlying hardware. The software-defined networks seamlessly span multiple environments and application domains, whether on-premises or multi-cloud, and provide centralized management, automation, and control. Multiple networks, each with specific purposes, can be spun up in seconds, simultaneously.

Programs and Reference Architectures to Accelerate Adoption

A range of programs and reference architectures help customers accelerate their time to production with full-stack software-defined networking deployments based on VMware and Intel® technologies.

- **Intel® Select Solutions** are verified solution configurations that streamline selection and deployment of network infrastructure.
- **Intel® Network Builders** is an ecosystem of software and equipment providers working to accelerate adoption of network functions virtualization (NFV) and software-defined networking (SDN).
- **Intel® Cloud Builders** provides detailed reference architectures developed jointly by Intel and leading systems and solution providers.

The virtualized networking environment operates over existing network hardware, with the NSX platform providing logical networking elements such as routing, switching, firewalling, and load balancing. The broader NSX portfolio, illustrated in Figure 2, tailors NSX to specific usages and provides complementary services and capabilities.

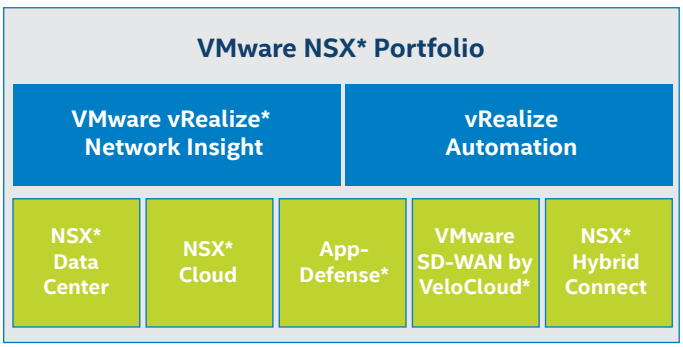

Figure 2. Building blocks in the VMware NSX* portfolio.

Core Network Virtualization

Three versions of NSX provide core network virtualization services, and each is tailored to a specific usage.

- **NSX* Data Center** is VMware's flagship networking product, an end-to-end network virtualization and security platform that reaches across software-defined data centers, clouds, branches, endpoints, and things. Applications pass freely among these environments, whether running on bare metal or in a VM or container.
- **NSX* Cloud** enables networking and secure connectivity with enhanced control for workloads that are native to public clouds such as Amazon Web Services (AWS)* and Microsoft Azure*. Because those clouds are built primarily if not entirely on Intel architecture, workloads hosted there benefit from the optimizations built into NSX by VMware and Intel.
- **VMware SD-WAN by VeloCloud*** helps meet increased requirements of capacity, security, and control to ensure application performance at branch and edge locations. It aggregates multiple network links such as leased lines, cable and DSL internet services, and 4G networks, abstracting them and managing them as a pooled connectivity resource.

Unified Management, Control, and Security

The core network virtualization services of NSX are complemented by a set of integrated tools that enhance management, control, and security across the multi-cloud environment.

- **VMware vRealize* Automation** streamlines and automates end-to-end delivery and management of infrastructure and applications. It controls IT operations using predefined policies and provides blueprints with definitions that allow new networks to be provisioned automatically.
- **NSX* Hybrid Connect*** extends the data center for seamless and secure connectivity, integration, and workload migration across sites, including those operating with different versions of VMware vSphere* and different network types. It also automates bulk migration between on-premises and public cloud infrastructure.
- **vRealize Network Insight** provides visibility across virtual and physical networks in multi-cloud environments to drive insights and discovery that optimize management and scaling of NSX deployments. These capabilities also help accelerate micro-segmentation planning and deployment.
- **AppDefense*** operates on data center endpoints to provide application-centric protection. Its primary mechanism is to perform deep application introspection as a means to understand each application's intended state and behavior, and then monitor for changes that could indicate a threat.

In addition to the building blocks shown in Figure 2, NSX Data Center and AppDefense provide built-in application security through adaptive micro-segmentation. Micro-segmentation is a well-established capability of NSX Data Center and NSX

Cloud that provides logical isolation of specific workloads across physical hosts, protecting east-west traffic within the network that is unseen by perimeter security measures. Adaptive micro-segmentation builds on that capability using AppDefense for deeper application intelligence, direct protection of application workloads, and adaptive policy that responds dynamically to application changes.

Building an Optimized Foundation with Intel® Architecture

Intel architecture building blocks provide end-to-end scalability and consistency, from the edge to the data center to the cloud. With a foundation based on Intel Xeon Scalable processors and Intel® Ethernet network adapters, a number of hardware and software technologies contribute to security and performance, as illustrated in Figures 3 and 4. Optimizations to the NSX platform, co-engineered by VMware and Intel, expose those technologies to workloads on the virtualized network, whether on-premises or in the cloud, running on bare metal, in a VM, or in a container.

Enterprise-Scale Compute Resources

Intel Xeon Scalable processors provide a consistent instruction set architecture across a broad set of SKU offerings that enable network operators to balance cost and performance requirements against factors such as core count and the robustness of individual cores. The platform accelerates network workloads and delivers up to 60 percent savings in total cost of ownership (TCO)[2] over predecessor platforms.

It features an entirely new core microarchitecture and low-latency cache hierarchy, as well as up to 28 cores per socket, supporting more VMs per server. Memory and PCI Express* improvements power up workloads that are bound by memory or I/O, including 1.5x the memory bandwidth of predecessors from six memory channels as well as increased PCI Express bandwidth. Intel® Advanced Vector Extensions 512 (Intel® AVX-512) instructions double the amount of data handled per clock cycle to speed up data-intensive enterprise applications.

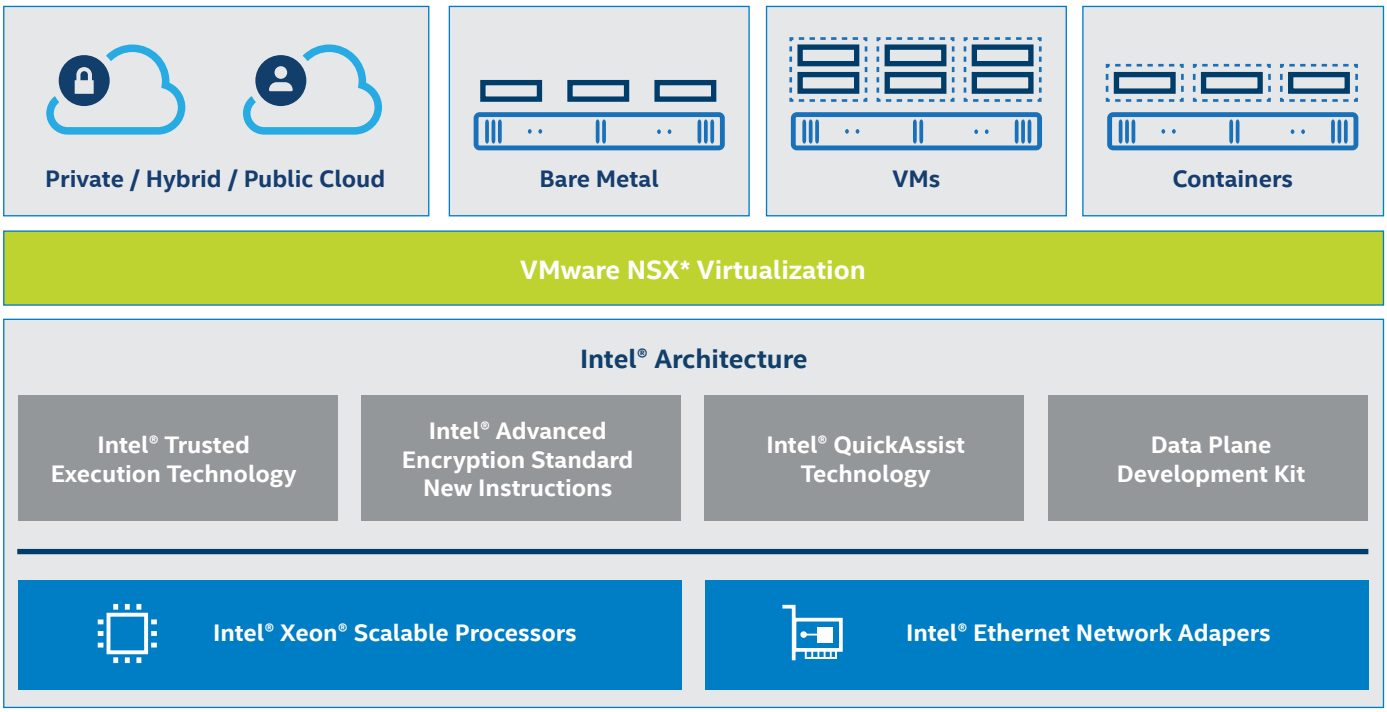

Figure 3. Intel® architecture building blocks in NSX* deployments.

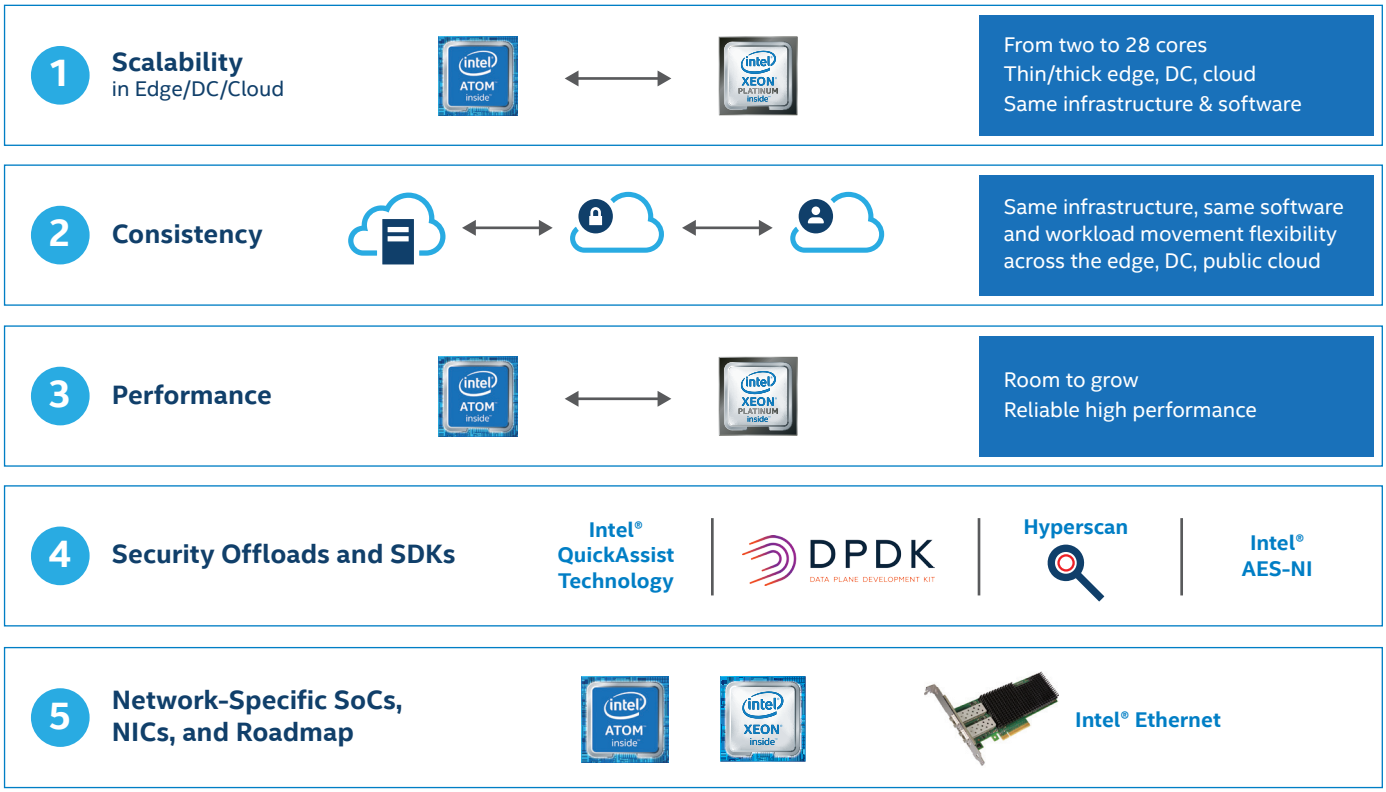

Figure 4. Intel® architecture benefits and advantages from the edge to the data center to the cloud.

In addition to these features oriented toward cost-effectiveness, performance, and scalability, Intel Xeon Scalable processors also incorporate hardware-based security features that complement the robust software measures built into NSX. Some key features that are especially relevant in this context include the following:

- **Intel® Trusted Execution Technology (Intel® TXT)** measures the launch environment to verify that software components such as the BIOS and hypervisor have not been tampered with. This creates a hardware-based root of trust that can be attested and discovered by VMware management software.
- **Intel® Advanced Encryption Standard New Instructions (Intel® AES-NI)** accelerates key parts of the AES algorithm in hardware, dramatically reducing the associated performance overhead. This acceleration helps make it viable for NSX to protect data by encrypting it pervasively across virtual networks.
- **Intel® QuickAssist Technology (Intel® QAT)** accelerates the data operations that underlie functionality such as encryption, authentication, digital signatures, and lossless compression. Intel QAT helps boost application throughput, increase network efficiency, and reduce overall data size.

Advanced Networking Technologies

Intel Ethernet network adapters deliver high networking performance through sophisticated packet processing, intelligent offloads, and high-quality open-source drivers. VMware NSX is highly optimized for this network hardware, including the use of poll mode drivers (PMDs) that eliminate the overhead of context switching due to the network interface sending a processor interrupt each time a packet arrives. Instead, a core is assigned to poll the network interface, making the interrupts unnecessary. This enhancement specifically targets the large numbers of small packets that are associated with network functions virtualization (NFV).

In addition, the NSX-managed virtual distributed switch (N-VDS) is performance-optimized using the Data Plane Development Kit (DPDK), providing a 4x throughput enhancement[3]. The DPDK optimizes packet processing by means of data plane libraries and network interface controller drivers, isolating control plane and data plane workloads. Traffic-handling performance of the N-VDS scales linearly with the addition of logical cores for PMD operation.

Conclusion

IT organizations must build next-generation networks that enable workloads to pass freely among different on-premises and cloud environments, running on bare metal, in VMs, or in containers. Network virtualization solutions based on NSX and Intel architecture provide integrated solution stacks that optimize performance, scalability, and security across workloads. In addition, those resources and workloads can be centrally controlled and managed, wherever they are.

NSX provides robust network virtualization and security that meets these goals, modernizing the environment with a high degree of optimization for Intel platforms and Intel Ethernet network adapters. Intel architecture provides a consistent, scalable foundation across the networking environment, with hardware that can be easily tailored to specific needs. The combined hardware and software stack improves agility and decreases total cost of ownership (TCO) by delivering resources as a service and scaling on demand. It automates management with rapid, unified, enterprise-wide configuration, deployment, update, and decommissioning.

Network virtualization solutions based on VMware and Intel® technologies are the key to a highly tuned, software-defined enterprise that lowers the barriers to successfully getting the full value out of today's multi-cloud reality.

Learn More about VMware and Intel Co-Engineering:

www.intel.com/vmware

www.vmware.com/partners/strategic-technology-partners/intel.html

Solution provided by:

[1] Source Tech Target: https://searchcloudcomputing.techtarget.com/definition/multi-cloud-strategy. Of enterprises surveyed, 35 percent use four or more public clouds, 10 percent use three public clouds, and 16 percent use two public clouds. Therefore, more than 60 percent use two or more public clouds.

[2] Configuration details: Up to 60 percent TCO savings with Intel® Xeon® Scalable processor compared to 5-year old system. Example based on estimates as of June 2018 of equivalent rack performance over 4-year operation on integer throughput workload (estimate based on SPECrate2017_int_base on Intel internal platforms) running VMware vSphere* Enterprise Plus on Red Hat Enterprise Linux* Server and comparing 20 installed 2-socket servers with Intel® Xeon® processor E5-2690 at a total cost of $737,460 [per server cost $36.8K: acquisition=12,5K, infrastructure and utility=4.5K, os & software=10.2K, maintenance=9.7K] vs. 5 new Intel® Xeon® Platinum 8180 at a total cost of $294,540 [per server cost $58.9K: acquisition=12,5K, infrastructure and utility=10.1K, OS and software=10.1K, maintenance=9.7K]. Assumptions based on https://xeonprocessoradvisor.intel.com, assumptions as of June 6, 2018. For more complete information visit www.intel.com/benchmarks.

[3] Source of performance claim: Gerben Menting, NFV Strategist, VMware. VMware vCloud NFV 3.0 showcasing N-VDS benefits with Intel processors tuned for Telco Networks versus VMware vCloud NFV 2.0. Packet size 64 = 4.33x, packet size 128 = 4.2x, packet size 512 = 3.x https://www.telecomtv.com/content/demo-zone/vmware-vcloud-nfv-3-0-showcasing-n-vds-benefits-with-intel-processors-tuned-for-telco-networks-31443/?utm_content=bufferd1a4d&utm_medium=social&utm_source=twitter.com&utm_campaign=buffer.

Software and workloads used in performance tests may have been optimized for performance only on Intel microprocessors. Performance tests, such as SYSmark and MobileMark, are measured using specific computer systems, components, software, operations and functions. Any change to any of those factors may cause the results to vary. You should consult other information and performance tests to assist you in fully evaluating your contemplated purchases, including the performance of that product when combined with other products. For more complete information visit http://www.intel.com/benchmarks.

Performance results are based on testing as of December 2018 and may not reflect all publicly available security updates. See configuration disclosure for details. No product can be absolutely secure. This document may contain product features that are currently under development. This overview of new technology represents no commitment from VMware to deliver these features in any generally available product. Features are subject to change, and must not be included in contracts, purchase orders, or sales agreements of any kind. Technical feasibility and market demand will affect final delivery. Pricing and packaging for any new technologies or features discussed or presented have not been determined.

Intel technologies' features and benefits depend on system configuration and may require enabled hardware, software or service activation. Performance varies depending on system configuration. No computer system can be absolutely secure. Check with your system manufacturer or retailer or learn more at intel.com.