Software-Defined Everything: 5 Trends for 2018

By Kurt Marko

NOVEMBER 2017 | US$25 | S421117

Channel Partners™
Channel Futures™

Software-Defined Everything: 5 Trends for 2018

By Kurt Marko

NOVEMBER 2017 | US$25 | S421117

Channel Partners™
Channel Futures™

Table of Contents

Trend 1: Hybrid Clouds Bridge Public and Enterprise Data Centers With VPCs 5

Trend 2: Direct Connections Gain Favor for Big Cloud Users 6

Trend 3: Hybrid Container Environments Mature 6

Trend 4: SD-WAN Branches out to Enterprise Infrastructure Consolidation and Public Cloud . . 7

Trend 5: Big Data Analysis Meets Network Management 8

Market Stats Mean Channel Opportunities. 8

Summary & Recommendations 10

Channel Partners™

About the Author

linkedin.com/in/krmarko
@krmarko

KURT MARKO is an IT industry analyst, consultant and regular contributor to a number of technology publications, pursuing his passion for communications after a varied career that has spanned virtually the entire high-tech food chain from chips to systems. Upon graduating from Stanford University with bachelor's and master's degrees in electrical engineering, Marko spent several years as a semiconductor device physicist, doing process design, modeling and testing. He then joined AT&T Bell Laboratories as a memory chip designer and CAD and simulation developer. Moving to Hewlett-Packard, he started in the laser printer R&D lab doing electrophotography development, for which he earned a patent, but his love of computers eventually led him to join HP's nascent technical IT group. Marko spent 15 years as an IT engineer and was a lead architect for several enterprise-wide infrastructure projects at HP, including the Windows domain infrastructure, remote access service, Exchange email infrastructure and managed web services.

Software-Defined Everything: 5 Trends for 2018

SOFTWARE-DEFINED NETWORKING HASN'T DEVELOPED — AS A TECHNOLOGY OR A BUSINESS — QUITE

the way data center experts, investors, partner leads and IT prognosticators predicted when commercial products emerged earlier this decade. You may remember bold promises: SDN would upset the network equipment vendor apple cart, radically restructure data centers and lead to a glorious age of programmability. Gone would be the days of exorbitant prices, lock-in and manually rewiring connections and configuring network devices with arcane CLI commands. Take a few application servers — aka network controllers — and some inexpensive, interchangeable, programmable switches to execute application instructions and voila: Network services on demand.

Almost none of this ended up happening.

Sure, network programmability has improved, but that's thanks to advances in existing management platforms. And, with the notable exception of SD-WAN, the software-defined movement hasn't had a disruptive effect on customer networks. Most interest, investment and product development has targeted carriers and service providers as they grapple with exploding traffic from cloud services, mobile devices and online businesses.

Not to suggest the SDN market is sluggish. In fact, vibrancy has emerged in areas we never saw coming, and 2018 promises to accelerate that pace. We'll look at key trends creating turmoil for customers — and opportunity for service providers.

But first, let us assure you that investing effort and resources into SDN, and other software-enhanced network technologies, is imperative. We may get a little geeky here. The trickle down of this tech from carrier-class projects to the enterprise and midmarket is underway, and competitive advantage will go to partners that carpe the diem.

Trend 1: Hybrid Clouds Bridge Public and Enterprise Data Centers With VPCs

Although public clouds are shared utilities, providers like AWS and Azure take extensive measures to securely isolate customer workloads. A fundamental technique used by the dominant cloud providers to segregate network traffic is the virtual private cloud, or VPC.

VPCs provide a private virtual network with customer — or MSP — controlled CIDR block configuration, addressing and firewall-style ACLs that bundle in a virtual router, NAT for external communication and IPSec VPN termination.

VPC details vary by provider, but except for Google Cloud, which allows geographically distributed VPCs, and AWS under the right circumstances, most are confined to a single cloud region. That usually isn't a limitation, given the way most organizations design their cloud infrastructures. Customers typically partition a VPC into multiple subnets, one per application or security policy — for example, a subnet for databases, another for web hosts, a third for test and development systems — and use a virtual firewall/router to control traffic between VPC subnets and external networks.

Traffic can move in or out of a VPC through either an internet gateway service, for web-facing hosts or mobile app terminations, or a VPN to a private network. Fortunately, cloud VPN gateways use as their tunneling protocol IPSec, a technology most enterprises already use and support with existing on-site VPN gateways (appliances or embedded router software).

Once terminated internally, traffic from a VPC can be routed just like any subnet.

A small wrinkle comes when trying to integrate VPCs with on-premises virtual servers. Your larger and more technically sophisticated customers are moving their virtual server farms onto a virtual Layer 3 overlay network, for example by adding NSX to an existing vSphere environment or using Hyper-V Network Virtualization (HNV) on Windows Server. Combining VMs with a virtual network fabric improves application mobility across physical systems, while enabling a consistent security policy that can be tailored for and constrains particular applications or workload categories — so-called microsegmentation.

Virtual network policy can't translate to public cloud networks except when using the same virtualization platform in both places. Think VMware Cloud on AWS or Azure plus Azure Stack. Regardless, VPC traffic can terminate on a virtual network gateway such as NSX Edge or Nuage Network Services Gateway. Properly engineering the network and security policies for such terminations demands deep knowledge of the customer environment and understanding the technical and configuration nuances of both the private and virtual cloud network. This offers an opportunity for channel partners to provide valuable, differentiated network services that eliminate a technical hurdle for many organizations.

Trend 2: Direct Connections Gain Favor for Big Cloud Users

Although VPC VPNs work over any internet connection, as we detailed in a previous report, private, dedicated networks — direct connect circuits — are a better alternative for customers making heavy use of cloud, including SaaS such as Microsoft Office 365.

Offered by each of the three mega cloud providers along with most large carriers, these circuits provide a private network with dedicated bandwidth between data center LANs and the provider's facility. Again, the details of creating direct connect links are dependent on location, existing WAN carrier (if not using a co-location facility) and the provider's configuration requirements.

Direct connects also require customers use BGP as their external routing protocol (most large shops already do) to direct traffic between the two networks.

Since direct connects are physically distinct connections (kind of, they still traverse shared fiber, but have a dedicated optical channel), they don't need a VPN tunnel and can be managed like any other data center network, providing full control over routing and security policy.

Trend 3: Hybrid Container Environments Mature

Application containers are an increasingly popular alternative to VMs as a runtime environment and can accommodate a variety of application styles, whether large, monolithic legacy titles or new, container-native applications built using microservices. Because of the inherent modularity and portability of containers, the infrastructure can be readily scaled by adding nodes to a container cluster or adding clusters in another location. Cluster nodes and container workloads are managed by a container orchestration system such as Kubernetes, Mesos or Docker Swarm, which delivers control over an embedded virtual network within the cluster.

Containers share the host's kernel; however, the goal of containerization is application isolation, so you need a way to segregate network traffic using a shared host interface. Simple, single-server container implementations can enable cross-container communication using an internal virtual bridge, which is the default configuration for Docker. Things get more complicated, though, in the real-world case of routing traffic between nodes in a cluster.

Although there are a variety of approaches, most users have adopted the Kubernetes' style of assigning a unique, private virtual IP to every container, a process made possible by running a virtual switch on the container host. Still, there is no standard solution to the problem of cluster networking, and Kubernetes supports several alternative techniques, including open source projects like Open VSwitch and Contrail or commercial products like VMware NSX, Nuage Virtualized Cloud Services and Weaveworks. Indeed, the problem of cluster networking and cross-cluster routing is a subject of active development, spawning projects like Calico, Cilium and Romana.

For now, most enterprises are sticking with a commercial product for on-premises clusters or a cloud service like AWS ECS or Azure Container Service. But this is an area worth watching in 2018.

Integrating private and public container clusters into a hybrid design isn't a DIY project. In fact, it's been the subject of several interesting commercial partnerships between cloud and on-premises software vendors. Notably, VMware, via its Pivotal spinout and Google, introduced the Pivotal Container Service (PKS) that allows container workloads to effortlessly move between Kubernetes clusters running on vSphere and Google's Container Engine (GKE) using a single orchestration system. AWS and Red Hat are similarly cooperating to turn ECS and OpenShift into a hybrid container environment.

Unifying heterogenous container networking environments remains an open and thorny problem; however, Vmware with PKS is the most comprehensive solution so far, largely thanks to its support for NSX across clouds.

As with cloud networking writ large, hybrid container networking is a work in progress and is an area where technically savvy partners can provide valuable differentiated services.

Trend 4: SD-WAN Branches out to Enterprise Infrastructure Consolidation and Public Cloud

SD-WAN has been perhaps the most prominent success story among SDN technologies because it allows organizations to aggregate multiple WAN circuits of any type, including non-traditional options such as business broadband and LTE, into a single enterprise-quality circuit. It's especially helpful for customers with far-flung branch and remote sites, as we discuss.

For 2018, expect an increasingly important symbiosis between SD-WAN and cloud services as organizations centralize applications and data analysis in corporate data centers or on cloud services, while simultaneously generating an exploding amount of data at the network edge via IoT devices, location-based customer tracking and employee mobile devices.

The nexus of cloud and edge data is fueling what some call a cloud-to-edge strategy to improve performance and interactivity for applications and data by putting processing nearer the user. While edge computing will likely see a resurgence, customers won't want to cede the benefits of centralization — namely consistency, control and security.

SD-WAN can provide centralized management over distributed networks, so customers can have their big data and secure it, too.

As mentioned, a significant driver of the cloud-to-edge use case is IoT. The proliferation of intelligent edge devices is leading to an explosion of data, with IDC predicting an order-of-magnitude increase in the amount of information generated annually by 2025.

While some of this data will be processed and consumed at the edge, much will be backhauled to the cloud, where each of the three mega-clouds offer IoT back-end platforms designed to aggregate and preprocess data streamed from intelligent devices. They then pass it along to a data warehouse for slicing and dicing or send it to machine learning and cognitive, AI services for advanced analytics or to train

AI models using the cloud's innate services. SD-WAN simplifies the networking design to allow widely distributed nodes to be part of a cloud-connected, centrally managed network fabric.

Trend 5: Big Data Analysis Meets Network Management

Just as data analytics are being applied to IoT, the same statistical and machine-learning models can improve network management by aggregating log data from network devices into a single repository. Partners can then analyze that information to produce descriptive and predictive statistics, package them up and provide in-depth reporting to customers.

This new generation of network intelligence software can:

- Monitor performance against calculated baseline (normal) behavior;
- Detect anomalies in application performance and activity;
- Flag suspicious behavior and potential security vulnerabilities;
- Correlate network activity across devices to aid in troubleshooting; and
- Create visual dashboards for various constituencies summarizing current network state, recommendations and remediation steps for detected problems.

For example, Cisco's Business Critical Services is a suite of products using statistical analytics and AI models to predict network failures, detect security anomalies and improve troubleshooting, while its Tetration product aggregates network telemetry and learns network topology to produce recommendations for security policies and network segmentation and to map application/device dependencies.

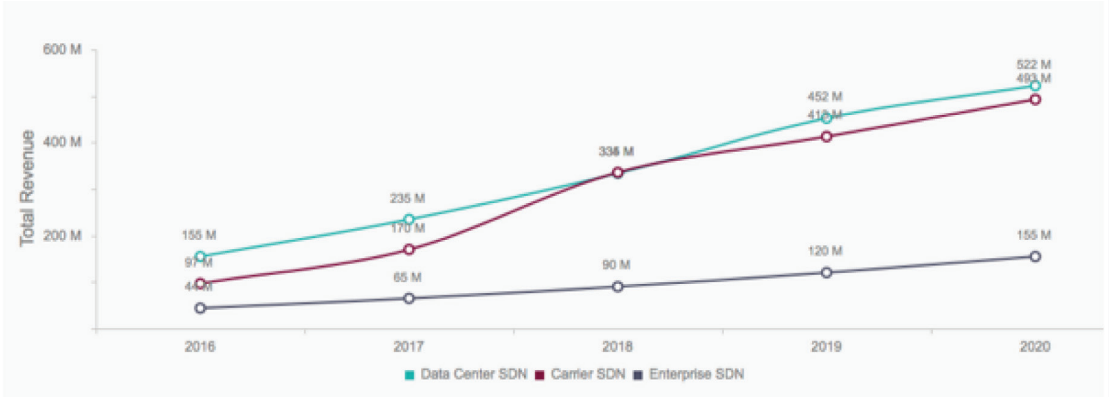
Similarly, startups such as Balbix and channel-focused ThousandEyes have taken a fresh approach to network and security analysis by using new models and sophisticated visualization to show network operations and correlate connected activity, by application, user or transaction, across an entire data center. They can then summarize the security exposure of various networks and applications, valuable insights for customers.

Market Stats Mean Channel Opportunities

Looking first at SDN infrastructure, IDC expects the SDN market, including physical hardware, control software, SDN applications and, most importantly for channel partners, professional services, to grow by more than 50 percent annually through 2020, hitting $12.5 billion.

Grand View Research predicts similar exponential growth in SDN integration, deployment, maintenance, training and management services through 2024. A vendor-sponsored estimate from Plexxi is, unsurprisingly, even more rosy, predicting 88 percent annual growth to a total market size of $35.6 billion next year.

Carrier SDN vs. Data Center SDN vs. Enterprise SDN



This chart displays the total revenue within the Carrier SDN, Data Center SDN, Enterprise SDN and other markets worldwide between the years 2016 to 2020. In the last period, 2020, the largest presented point is Data Cetner SDN with total revenue of 522M. The fastest growing participant in our report is Carrier SDN with 409.57% growth in total revenue over 5 years between 2016 to 2020. The

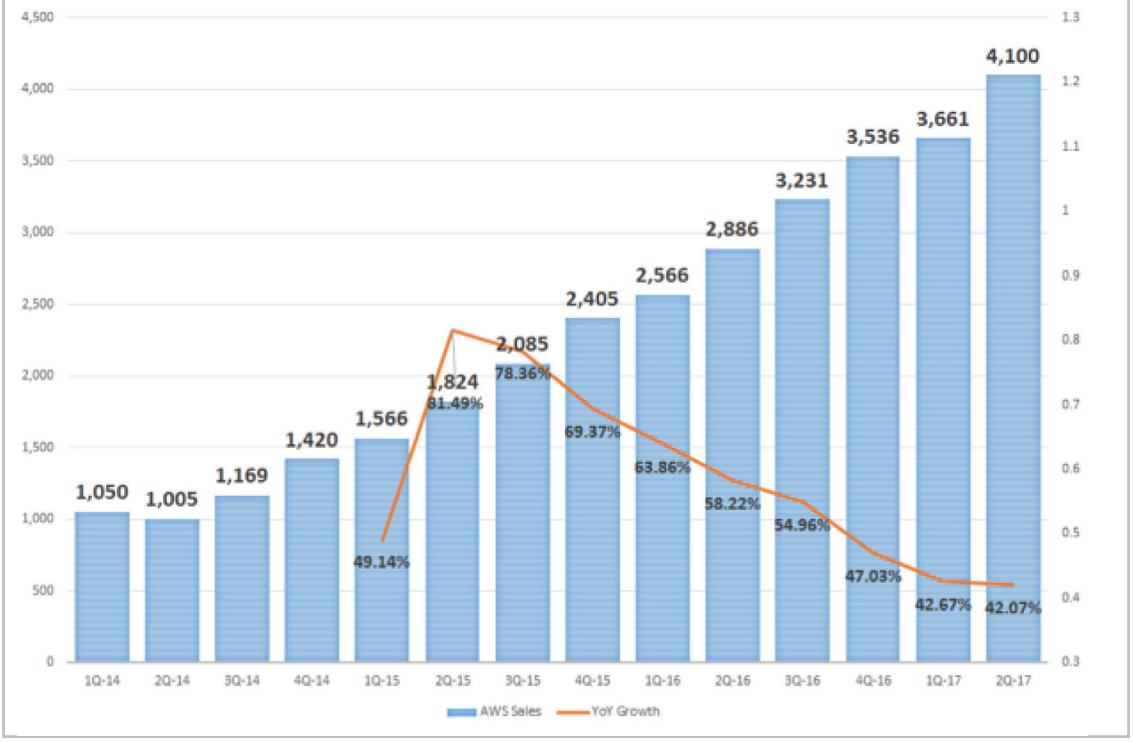
While carriers and service providers are driving the spending, enterprises are embracing SDN through software overlays like VMware NSX, Nuage VCS or OpenStack Astara that overlay on existing Ethernet fabrics.

The success story of public cloud services is nothing new. However, all three mega-providers — Amazon AWS, Microsoft Azure and Google Cloud — see the enterprise as critical to their next stages of growth. Although off from the torrid triple-digit increases it once registered, AWS continues growing at more than 40 percent annually and will soon be a $20 billion business. Although from a smaller base, Azure is growing even faster, 90 percent annually, with Microsoft's Intelligent Cloud segment (which includes server software, Azure and related professional services) generating over $28 billion in revenue over the past year.

However, most organizations don't want to lift-and-shift existing applications and data to a cloud provider. They're either developing or in dire need of a multicloud strategy. That requires integrating enterprise data center LANs, remote office WANs and public cloud services into a cohesive, secure network fabric, creating another software-defined stress fracture in today's legacy networks. This is possibly *the* services play of 2018.

SD-WAN is the market most benefitting from the nexus of SDN technology and public cloud services. Not only does SD-WAN allow substituting lower cost broadband circuits for traditional enterprise WAN services, but it provides a controlled way to integrate remote sites with public cloud services, whether IaaS or SaaS, without backhauling traffic to a central data center. Consequently, the SD-WAN market is seeing vigorous growth. As we detailed in previous SD-WAN reports (see related links) IDC estimates the SD-WAN market will grow at almost 70 percent annually through 2021, reaching an $8 billion market, with Gartner projecting that the number of SD-WAN deployments, while still small, will double each year resulting in 30 percent of enterprises using SD-WAN by 2020.

Amazon Web Services Revenue (USD Millions)



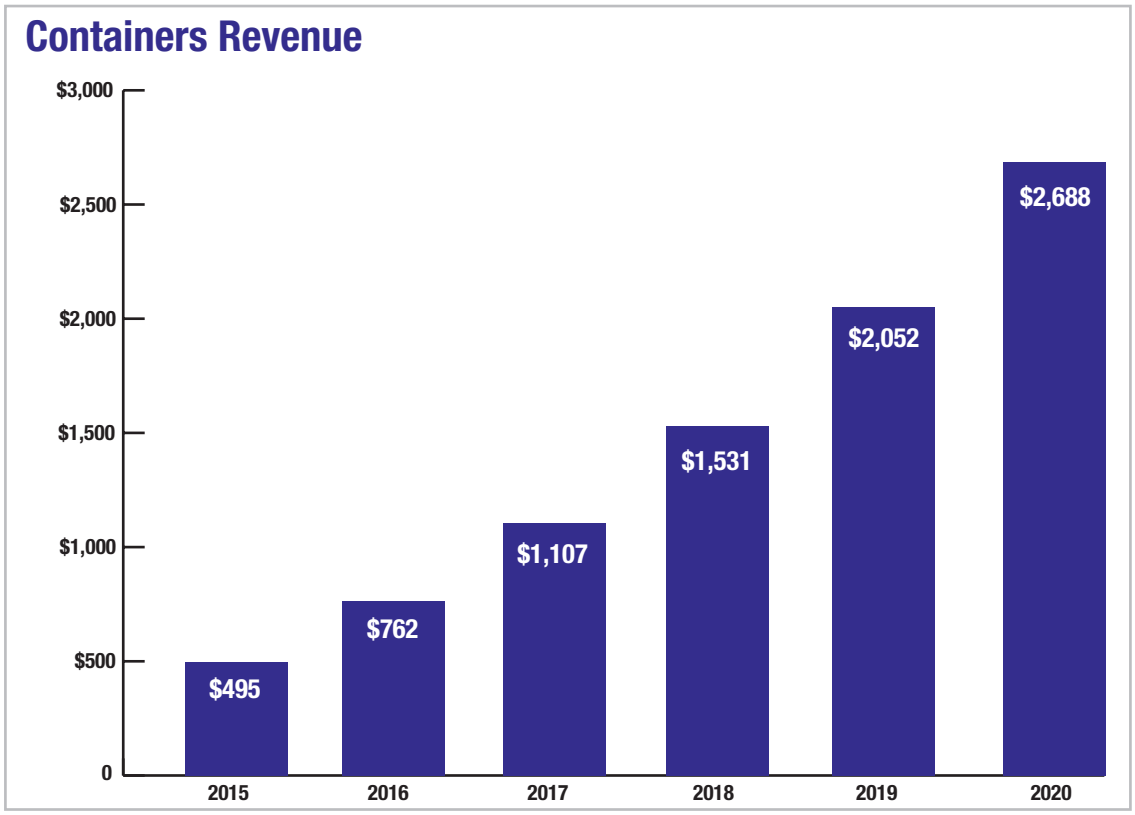
Containerization is an increasingly popular application deployment model that is affecting enterprise network plans on two fronts. First, due to the need to integrate the internal virtual network and switch created by the container runtime engine with physical and virtual data center networks and also because application containers are often deployed across both internal container clusters and public cloud container services and thus need the same transparent access to cloud networks as traditional applications.

The container market is one of the hottest in IT with 451 Research expecting it to see the fastest growth of any so-called cloud-enabling technology through the rest of the decade. The firm estimates 40 percent annual growth in container technology reaching nearly $2.7 billion in revenue by 2020. IDC estimates there will be about 1 billion container instances in use by then, five-times the number of VMs.

Together, these markets are changing the way organizations design enterprise networks and external interconnects and present significant opportunities to create and enhance network services, strategically engage with existing customers and win new business.

Summary & Recommendations

The term “software-defined network” has taken on a much more expansive meaning since its initial use to describe the disaggregation of network switching into data-forwarding appliances and centralized flow controllers. In fact, software is defining the network in myriad ways. Think software gateways that can connect on-premises



In Millions
Source: 451 Research Market Monitor: Cloud Enabling Technologies, Q3 2016

virtual networks to cloud infrastructure and container clusters, WAN controllers that can aggregate multiple consumer-grade circuits into a virtual enterprise link, data-fueled machine learning to improve network management and security, and more.

Customers need hybrid infrastructures to support next-generation cloud and IoT applications. For channel partners, the software-defined trends we've discussed present opportunities for value-added network service differentiation and lucrative consulting engagements.

Related Reports

Channel Guide to Intent-Based Networking

Don't get bogged down in semantics: Customers don't care which supplier has "true" intent-based networking or who did what first. What they do care about are business benefits and knowing that their trusted advisers are up-to-date on the next big trend. In this Report, we'll explain the reasoning and technology behind intent-based networking — and how it benefits you and your customers.

Cisco, Verizon, Versa: SDN in the Real World

Do you struggle to explain the importance of software-defined networking (SDN) to internal and customer stakeholders? In this Report we delve into real-life projects undertaken by Cisco partner Trace3, Verizon and Versa in tandem with VergX.

SD-WAN: A Branch Office, Remote Site Savior

Got clients that want to transition to SD-WAN but see remote site connectivity as a roadblock? That's where you come in. This Report explains how a hybrid WAN can bundle multiple connection types and provide customers with business-class features, security and connectivity to locations where traditional circuits would be prohibitively expensive.

SDN & Security: The Future Is Now

The move to SDN/NFV will not be limited to a few functions or services — it is a ground-up shift from on-premises legacy systems and operations to more cloud, agile/microservices development and delivery approaches, and DevOps organizational structures. Helping customers successfully navigate this transformation will require the right skills and partnerships — but growth is off the charts.