2018 Guide to WAN Architecture and Design

Applying SDN and NFV at the WAN Edge

Executive Summary

By ***Dr. Jim Metzler, Ashton, Metzler & Associates***
Distinguished Research Fellow and Co-Founder
Webtorials Analyst Division

Steven Taylor, Webtorials
Publisher and Editor-in-Chief
Co-Founder, Webtorials Analyst Division

Platinum Sponsors:

apcela

CATO NETWORKS

cradlepoint

DELL

TALARI Networks

TELOIP®

TABLE OF CONTENTS

Introduction

One of the goals of the 2018 Guide to WAN Architecture and Design (The Guide) is to discuss the state of WAN architecture and design with an emphasis on the current SD-WAN solutions. Another goal of The Guide is to provide insight into the emergence of solutions that leverage the key concepts of SDN and NFV to support all components of the WAN edge.

A discussion of wide area networking is extremely timely for two reasons. One reason is that for most of the last fifteen years there has been little investment in the development of new WAN technologies and services. Hence, until the development of Software Defined WANs (SD-WANs) there hadn't been a fundamentally new WAN technology or service introduced into the marketplace since the turn of the century.

A discussion of the WAN edge is also very timely. One reason for that is the burgeoning use of the Internet of Things (IoT). For example, Gartner has forecasted that 8.4 billion connected things will be in use worldwide by the end of 2017, up 31% from 2016, and that there will be 20.4 billion connected things by 2020.

The Guide was published both in its entirety and in a serial fashion. The three serial publications were:

- Part 1: State of the WAN
  This section provides insight into the current state of the WAN, the status of SD-WAN adoption and the status of the branch office. It is based on surveys that were distributed in the March to August 2017 timeframe.

- Part 2: Key Considerations when Choosing new WAN and/or Branch Office Solutions
  This section discusses a range of considerations that network organizations need to keep in mind as they evaluate alternative SD-WAN and SD-Branch solutions. This discussion is intended to ensure that network organizations choose solutions that meet both their current and their future requirements and which are, to the maximum degree possible, future-proof.

- Part 3: The SD-WAN and the SD-Branch Office Ecosystem
  This section identifies the ecosystem of vendors who supply SD-WAN and/or SD-Branch Office solutions

State of the WAN

Concerns with WAN Services

Network organizations have concerns with all the available WAN services. Some of the primary concerns that they have with MPLS include cost, uptime and the time it takes to implement new circuits. The concerns that they have with the Internet include security, uptime and latency. Some of the limitations that are associated with cellular services include variable signal coverage, link setup latency and security.

Factors Impacting the WAN

One category of factors that has been impacting the WAN for a long period of time includes reducing cost, supporting real-time applications and providing better security. A category of factors that has only recently begun to impact enterprise WANs includes providing access to public cloud computing services, supporting mobile workers and supporting the IoT.

Satisfaction with the Current WAN Architecture

Two thirds of network organizations are at best only moderately satisfied with their current WAN architecture. This indicates that a large portion of the WAN marketplace would likely be receptive to alternative WAN architectures.

Plans for evaluating and Implementing SD-WANs

Slightly over a quarter of network organizations are actively analyzing vendors' SD-WAN strategies and offerings. Almost as many are currently analyzing the potential value that SD-WANs offer. In addition, year-over-year more organizations are running SD-WAN functionality in production and more expect to put it into production within the next year.

The Drivers of SD-WAN Adoption

Over the last two years the primary drivers of SD-WAN adoption have been to reduce OPEX and to increase flexibility. Over the last year increasing availability has become a more important driver and improving security has become a less important driver.

The Inhibitors to SD-WAN Adoption

Over the last two years the primary inhibitors to SD-WAN adoption have remained the same. Those inhibitors are that it would add complexity and that the current technologies are unproven and/or immature.

Preferred Location of WAN Functionality

In the emerging WAN architectures there are several places to host functionality such as orchestration, control and security. While there is interest in housing functionality in each of those places, the strongest interest is to house functionality in the cloud.

Choice of Implementation Options

When network organizations evaluate new WAN solutions they have a variety of implementation options to consider. This includes Do-it-Yourself (DIY) solutions, Network-as-a-Service (NaaS) solutions as well as the use of a managed service. While there is strong interest in DIY SD-WAN solutions, there is somewhat stronger interest in the other two options.

Choice of Vendors

A third of network organizations indicated that when choosing an SD-WAN solution that they would actively seek alternatives to their current vendor while only twenty percent of network organizations indicated that they would likely stick with their incumbent vendor.

Desired Functionality

When analyzing SD-WAN solutions roughly a third of network organizations are heavily focused on how the connectivity is provided. However, over half of network organizations are looking for SD-WAN solutions that in addition to connectivity provide optimization and security functionality.

Primary Deployment Issues

Relative to SD-WANs the most commonly mentioned deployment issue was that the implementation of the solution was more difficult than expected. The next tier of issues was:

- The solution created security challenges;
- Setting up and maintaining policy was more difficult than expected;
- The solution made operations more complex;
- Troubleshooting problems was more difficult than expected.

Current Deployment of Servers and Appliances

Roughly one third of companies have 3 or more servers in each of their mid-sized branch offices and a slightly higher percentage has 3 or more physical appliances in each of these offices. The extent of distributed IT hardware is an indication of the possible operational and financial gains that could be made through the virtualization and consolidation of branch office functionality.

Planning for the Evolution of the Branch

The fact that 16% of IT organizations have recently implemented a new approach to providing IT services to branch offices indicates that the movement to adopt a next generation branch office is roughly at the same point in the adoption curve as is SD-WANs.

Breadth of Branch Office Functionality

The primary classes of functionality included in the plans that organizations have for their branch offices are WAN connectivity, security, WiFi, WAN Optimization and voice.

Current and Intended Use of Virtualization

By the end of 2018, the vast majority of IT organizations will have virtualized at least some of the network and security functionality in their branch offices. One third of IT organizations expect that by the end of 2018 that they will have virtualized the majority of the network and security functionality in their mid-sized branch offices.

How Branch Office Virtualization will be Implemented

There is significant interest in using virtual CPE as the basis for implementing virtualized functionality in branch offices. However, there is still a lot of uncertainty about how IT organizations will implement virtualization in branch offices.

Key Considerations when Choosing new WAN and Branch Office Solutions

Software Defined

Because they potentially will benefit from the massive investments being made in the enabling technologies, network organizations should examine solutions that qualify as being software defined. A solution may contain multiple components that are each software defined; e.g., a combination of SD-WAN and Software Defined Perimeter (SDP) functionality.

Location of Key Functionality

The traditional approach to hosting WAN and branch office functionality onsite still has value. However, today there are many alternative places to host functionality. In some instances, organizations will find that the best solution is to locate functionality in multiple types of sites.

Application Delivery

When evaluating alternative solutions, network organizations must evaluate the solutions based on the ability of those solutions to ensure successful application delivery. This means that the solutions enable appropriate levels of performance and security and are easily managed.

Edge Computing

Network organizations have a strong interest in running functionality in the cloud. Running functionality at edge locations provides the same benefits as running it in the cloud. In addition, this approach eliminates some of the issues, such as latency, that are associated with the cloud.

Complexity

The implementation of any new solution always adds complexity, at least initially. On a going forward basis, IT organizations should only adopt solutions that once in production will reduce notably more complexity than is added during the adoption process.

Mobility and the Internet of Things (IoT)

It may well be that in the short term that the best option that a network organization has is to implement a WAN solution that just supports branch offices. However, before implementing a WAN solution with a narrow scope, network organizations should develop a WAN strategy that includes how they will effectively and efficiently support mobile workers and the IoT.

The Role of Cellular

As the use of cellular evolves from being a backup service to where it is a primary service, network organizations need to include in their analysis of WAN and branch office solutions a focus on high-performing, effective cellular services.

5G

Within the next two years, 5G has the potential to fundamentally change networking. Network organizations evaluating new WAN and branch office solutions need to ensure that those solutions will aggressively and effectively support 5G.

Cloud Computing

Backhauling Internet traffic is no longer acceptable from either a financial or an application performance perspective. This has given rise for the need to deploy Direct Internet Access (DIA) at the branch, which fundamentally alters the prevailing security paradigm. This is one of the several factors driving the need to implement NFV somewhere at the edge of the WAN.

Security

Since branch offices are not the only class of WAN edge points, network organizations also need to ensure that their WAN architecture provides effective security to all the relevant WAN edge points, including mobile workers and the IoT.

Software Defined Perimeter (SDP)

As part of their adoption of new solutions to connect WAN edge points, IT organizations need to fundamentally rethink their approach to security in part to ensure that it isn't based on obsolete concepts such as the existence of a well-defined perimeter. For most IT organizations this will involve adopting at least some of the key concepts of an SDP.

WAN Optimization

In many instances adding WAN bandwidth eliminates application performance problems. However, in many other instances just adding bandwidth doesn't eliminate application performance problems and WAN optimization functionality of some type is required.

Network Functions Virtualization (NFV)

The transition that the IT industry is undergoing is a lot broader than just improving the functionality found in the WAN or in the branch office. At its core, the transition is about focusing broadly on supporting a wide and enlarging set of people, places and things. Distributed NFV is a key enabler of this transition.

*CPE

Two new forms of CPE are being deployed to support the WAN edge: uCPE and vCPE. Both forms of CPE provide value by hosting multiple network functions. However, it can be very challenging for solutions based on these types of CPE to provide sufficient WiFi support or to tightly integrate with branch office functionality such as Ethernet switching with PoE.

WAN Management

The deployment of new WAN solutions is an opportunity for network organizations to improve their ability to troubleshoot the WAN and hence improve their ability to support the company's critical business processes.

Machine Learning

Machine learning has the potential to fundamentally impact how IT functionality is operated and managed. As they analyze new WAN and branch office solutions, network organizations should spend time to understand the vendors' strategies relative to machine learning.

Ongoing Role of MPLS

While they are exploring alternative solutions, network organizations should make sure that they analyze solutions that enable them to aggressively reduce WAN transport costs.

Alternatives to a DIY Approach

When evaluating SD-WAN and SD-Branch solutions, network organizations need to ask themselves if they have the expertise to implement these solutions on a DIY basis and if they do, if that is the best use of their highly skilled resources. If that is not the case, then the organizations should evaluate NaaS and managed service offerings.

The SD-WAN and the SD-Branch Office Ecosystem

Do It Yourself (DIY) Solutions

In the case of DIY solutions, the network organization that consumes the solution is also the organization that is responsible for the lifecycle management of the solution. DIY solutions are provided by a range of vendors including start-ups and large established companies. These solutions are built around several different types of appliances and implementation options including:

- Traditional Routers;
- Special Purpose Appliances;
- Pure Play SD-WAN Software Routers;
- Converged SD-WAN Appliances;
- Cloud-Deployable Solutions.

3Rd Party Solutions

With this class of solution, an organization other than the network organization that consumes the solution is responsible for the lifecycle management of the solution. The vendors in this component of the ecosystem provide two primary classes of solutions:

- Network-as-a-Service (NaaS)
  A NaaS offering is typically built using a core network that interconnects a distributed set of Points of Presence (POPs). In addition to basic transport, a NaaS offering typically provides functionality such as security and optimization.

- Managed Solutions
  Managed Service Providers (MSPs) typically acquire and implement the same functionality that an enterprise network organization would in order for the MPSs to offer a managed SD-WAN or a managed SD-Branch Office.

Enabling Hardware

The vendors in this component of the ecosystem provide the hardware that is utilized in both DIY and 3rd party solutions. The type of hardware they provide is:

- Black Boxes
  A black box is a piece of purpose-built, proprietary hardware in which all the functionality provided by the CPE is implemented in physical hardware.

- White Boxes
  In this type of CPE, the appropriate functions are fully virtualized in software that is hosted on common off-the-shelf hardware, usually an X-86 appliance.

- Gray Boxes
  A Gray Box is a middle ground between a black box and a white box in that some of the functionality provided by the CPE is implemented in physical hardware.

Elements of a Successful Digital Transformation and the Role of SD-WAN

apcela

A network evolution is happening and at the heart are applications. Apps, once secured and accessed via enterprise data centers, are moving to the cloud at an accelerating pace and users have moved beyond enterprise firewalls, requiring remote access and mobility.

Enterprise IT is now distributed and apps are delivered across hybrid IT environments resulting in performance challenges and complexity. This fragmented landscape requires a new application delivery model – hybrid WAN – supporting an evolution in how applications are delivered, secured and managed to ensure optimal performance and end-user experience. However, to ensure speed, performance and security in this model, companies are turning to SD-WAN solutions to enhance and extend the key functions of their enterprise for a higher performing, next-generation, distributed IT infrastructure.

Hybrid IT at the Foundation

Hybrid IT, an enterprise approach that manages some IT resources in-house and uses cloud-based services for others is a reality. Previously, IT utilized public cloud computing for non-critical IT services such as development and test applications or for turnkey SaaS applications like web analytics. All of which could replace internal applications and enable access for a mobile workforce. Today, enterprises aggressively pursuing digital transformation are running behind cloud first mandates and deploying new applications as SaaS wherever practical. Additionally, public IaaS platforms are no longer the domain of development and test environments as enterprises re-factor and even re-architect legacy, mission-critical applications to run in public cloud environments.

To stay ahead of this accelerating transformation, network infrastructure must evolve as rapidly as the cloud environment. Unfortunately, many legacy enterprise network architectures cannot keep pace. Traditional enterprise network architectures are built around a hub-and-spoke, carrier MPLS network anchored on the legacy premises-based data center. These typically interconnect the business operations of the enterprise, including regional offices and branches - bringing all traffic back through the datacenter. Any users and traffic destined for the cloud, typically go through a centralized, security DMZ (demilitarized zone of firewalls and web gateways) in the datacenter. This worked in the past when applications were in the datacenter, but it's becoming obsolete. So, what is the solution?

Consider Hybrid WAN

Because the internet is critical to enterprise cloud connectivity, its performance is not consistent making it impossible to rely on for business and mission-critical applications. This is where hybrid WAN comes into play. Hybrid WAN leverages both internet and MPLS - meeting the requirements of broad and increasingly distributed application deployments. Hybrid WAN also keeps the MPLS network interconnected to the distributed enterprise operations and legacy applications in the enterprise datacenter and local internet connections. This allows direct transit to cloud-based applications and services without the latency and costs associated with bringing all traffic back through a centralized, security DMZ.

While a hybrid WAN architecture solves hybrid IT performance challenges, it poses security challenges. DMZs are centralized for easier management. This leaves enterprise IT managers with a potentially costly and complex alternative of deploying firewalls in front of every internet connection. This is why enterprises have turned to a software-defined WAN (SD-WAN), which in a hybrid WAN environment overcomes many of these challenges - with additional benefits. Most SD-WAN technologies include at least some basic firewall functionality such as packet filtering, while others include fully featured, next-generation firewalls.

Add SD-WAN for Success

A fully functional hybrid WAN includes a range of architectural enhancements built for true cloud interoperability that includes a high-performance core network, carrier-neutral commercial data centers and extensive interconnection with both SaaS and IaaS cloud platforms. The combination of hybrid WAN and SD-WAN enables users and traffic destined for more critical cloud applications to reduce reliance on the unpredictable performance of the public internet and makes the interconnection with cloud applications directly to the user. Carrier-neutral commercial datacenters also serve as distributed security points and when combined with SD-WAN, enterprises can deploy a number of smaller distributed security DMZs. SD-WAN provides a comprehensive, distributed security approach providing access to policies across the network. Additionally, to further reduce network costs, SD-WAN:

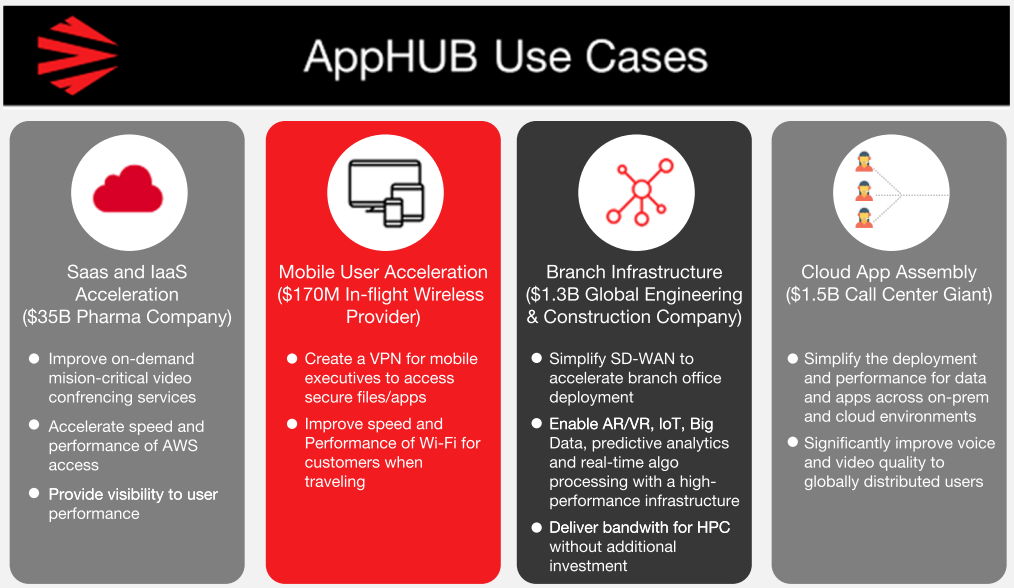
- Addresses latency and capacity issues;
- Provides an improved application performance – user location and application needs are not an issue;
- Creates an automated and simplified network connecting multiple locations with one overlay; and
- Offers telemetry that determines data traffic priorities.

Apcela, the high-performance application delivery company recognizes these three elements for a successful digital transformation. Apcela serves more than 100 of the Forbes Global 2000 including banks, exchanges, financial services and biopharma companies across 185 markets in 41 countries worldwide. Apcela enables enterprises to move to a cloud environment – keeping some of an organization's WAN and enhances and extends what companies already have with its AppHUB solution.

AppHUBs Enhance and Extend Key Functionalities with SD-WAN

AppHUBs are virtual datacenters deployed at network and cloud service provider-dense, carrier-neutral colocation facilities and datacenters. Built from colocation, network connectivity, hardware-optimized, virtualized network functions (VNFs) and hyper-converged compute and storage, each AppHUB is equipped with a complete network telemetry solution: AppMon. This ensures the underlay network and customer overlay networks meet SLAs. Additionally, AppHUBs' machine learning capabilities and run-over operating logs reduce the time-to-diagnosis for Apcela's NOC and in many cases, to the point where enterprises are unable to perceive an issue.

Enterprises can leverage computing capabilities with AppHUBs to eliminate bottlenecks in their networks, shorten the distance between edge locations and application hosting hubs, distribute security and improve overall performance of their WAN and application delivery platform. Apcela deploys SD router instances at each one of its AppHUBs to ingress- and egress-encrypted traffic to and from the AppHUB and network backbone. These instances are internet-connected, allowing enterprises to utilize Ethernet, DIA, broadband, or local access to securely connect to the WAN in the local AppHUB market. Additional AppHUB benefits include:



Distributed Security Extending across the Enterprise

AppHUB's suite of functions ensure security across its distributed system including:

- ***Distributed Endpoint and Cloud Security:*** Firewall, URL and file filtering, IDS/IPS, user Distributed Endpoint and Cloud Security: Firewall, URL and file filtering, IDS/IPS, user and application-based policies, malware detection and more.

- ***Improved Performance:*** By distributing firewalls closer to the edge, latency can reduced by more than 50%. VPNs can terminate closer to users and harness the low-latency backbone to move data across the WAN.

- ***Latency Optimized Internet Routing:*** AppHUBs include a network-based firewall with performance IP Internet. Performance IP leverages peering agreements with 6-12 ISPs and intelligently routes traffic to the ISP providing the best latency.

Network Connectivity for Best Performance

Carrier neutrality in an AppHUB facility ensures that WAN connectivity balances the best performance and best price. Carrier diversity ensures competition which drives carrier and path diversity as well as optimizes Apcela's opex for its underlay network infrastructure.

Cloud Gateways for Secure and Dedicated Connectivity

AppHUBs are Apcela's cloud gateways, offering secure and dedicated connectivity to the industry's leading cloud service providers like AWS, Google Cloud, Microsoft Azure and others. By leveraging the low-latency, core network connecting AppHUBs, along with Apcela's powerful telemetry tool AppMon, customer traffic can be routed to SaaS, IaaS and XaaS providers through the closest AppHUB location, lowering round-trip times and increasing application performance.

With innovation comes pitfalls. However, they can be avoided with these key elements: hybrid WAN, SD-WAN and with Apcela's AppHUB to ensure business and mission-critical applications function with the necessary speed and performance. No matter the location, company size, market or the amount of legacy infrastructure you have – AppHUB works to solve any issues you have moving to the cloud, while enabling growth for tomorrow.

The Future of SD-WAN. Today.

The WAN is Incompatible with Modern Enterprise

The migration to cloud applications and a mobile workforce is changing the shape of the business. The Wide Area Network (WAN) was built to connect and secure static, physical locations - not today's fluid and dynamic businesses. Enterprises pay the price of this incompatibility with expensive connectivity and convoluted topologies that are hard to manage and secure. Adding new locations, enabling secure internet access at remote locations and for mobile users, and optimizing network resources for cost and performance, all represent a growing challenge for most organizations. Traditional SD-WAN is offering flexible capacity and agility but persists the dependency on expensive MPLS connectivity and security appliance sprawl, and lacks optimized support for cloud resources and mobile users.

True WAN Transformation with Cato Networks

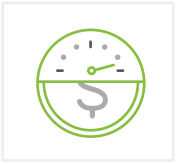
Cato Networks provides organizations with a global SD-WAN with SLA-backed backbone and built-in network security stack. The Cato Cloud reduces MPLS connectivity costs and branch office appliances footprint, provides direct secure internet access everywhere, and securely connects mobile users and cloud infrastructure into the enterprise network.

Secure And Optimized SD-WAN

Cato SD-WAN enables organizations to augment MPLS with affordable last mile services (Fiber, Broadband, 4G/LTE) and dynamically direct traffic based on applications needs and link quality. Unlike legacy SD-WAN solutions, Cato is uniquely capable to replace MPLS altogether with our global SLA-backed backbone.

Appliance Elimination

Cato eliminates branch office equipment such as UTMs, Firewalls and WAN optimization appliances. Cato protects all locations and users everywhere, without the need for unplanned hardware upgrades and resource-intensive software patches.



Affordable MPLS Alternative

Cato leverages cloud scalability, software-defined networking and smart utilization of a multi-carrier backbone to deliver a high performance and SLA-backed global WAN - at an affordable price.

Hybrid Cloud Network Integration

Cato connects physical and cloud datacenters, across all providers and global regions, into a single, flat and secure network. Customers can seamlessly extend corporate access control and security policies to cloud resources, enabling easy and optimized access for mobile users and branch locations to all applications and data anywhere.

Secure Direct Internet Access

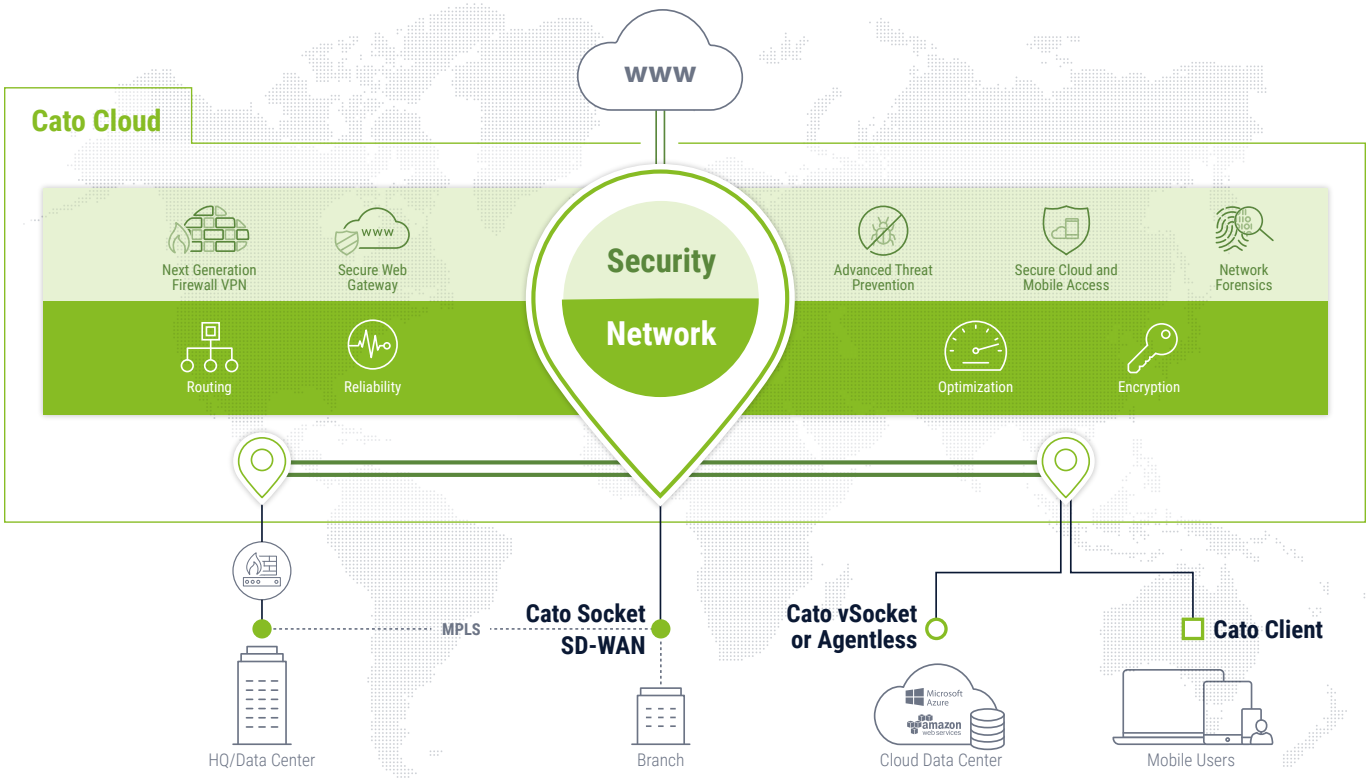
Cato connects all branch offices and remote locations to the Cato Cloud, providing enterprise-grade network security for any location without the need for dedicated appliances or traffic backhauling.

Mobile Workforce Secure Cloud Access

Cato connects every mobile user to the Cato Cloud and provides secure and optimized access to enterprise resources in physical and cloud datacenters, cloud applications and internet sites. Cato uses its global backbone to optimize routing and reduce latency to key applications like Office 365, and enforce application-aware security policies on all access.

Software-defined and Cloud-based Secure Enterprise Network

The Cato Cloud connects all locations, cloud resources and mobile users into an optimized and secure global SD-WAN. With both WAN and internet traffic, consolidated in the Cato Cloud, Cato applies a set of elastic and agile security services to protect access to enterprise applications and data, and protect users against Internet-borne threats.



Cato Cloud Network

A global, geographically distributed, SLA-backed network of PoPs, interconnected by multiple tier-1 carriers. Enterprises connect to Cato over optimized and secured tunnels using any last mile transport (MPLS, cable, xDSL, 4G/LTE).

Cato Security Services

A fully managed suite of enterprise-grade and agile network security services, directly built into the network. The services have no capacity constraints and are continuously updated to introduce new capabilities and adapt to emerging threats.

From the Creators of Network Security

Shlomo Kramer
Co-Founder and CEO

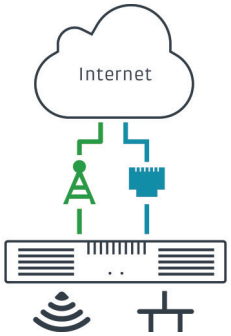
Gur Shatz
Co-Founder and CTO

Cato Networks was founded by Shlomo Kramer and Gur Shatz. Kramer is one of the founding fathers of network security and one of the leading cybersecurity innovators of our times. He is best known for introducing the first firewall to the market as a co-founder of Check Point Software, and later the first web application firewall as a founder and CEO of Imperva. Shatz has engineered the Imperva SecureSphere platform and built DDoS protection service company, Incapsula.

For more information, visit www.CatoNetworks.com

Elastic Edge: Pervasive Connectivity for People, Places & Things

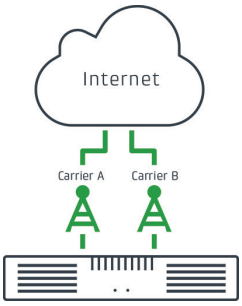
Software-Defined Branch



Cradlepoint's all-in-one branch network solutions are ideally suited for "Lean IT" organizations that demand business-critical 4G LTE connectivity. Powered by Cradlepoint NetCloud software and services, these solutions combine SD-WAN functionality with integrated WiFi, Ethernet switching with PoE support, advanced edge security, and multiple 4G LTE modems in a single platform. The entire branch network can be deployed, controlled and managed from a single of pane of glass in the cloud.

Feature Highlight: NetCloud SD-WAN functionality is optimized for LTE-dependent networks and utilizes a unique Active-Dynamic traffic steering algorithm that provides complete, policy-based control over hybrid WANs that include multiple 4G LTE connections. It can select the optimal path across any wired or wireless link based on a combination of signal strength, latency, jitter, service, carrier preference, and data plan consumption.

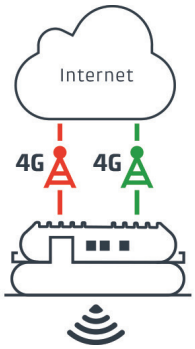
Cutting the Wire: LTE-Optimized SD-WAN



For highly distributed networks such as rural convenience stores and insurance offices, there are few options for reliable broadband. Even if wired options exist, building a nationwide network often requires stitching together more than 100 Internet Service Providers. In contrast, cellular networks provide pervasive, high-speed broadband data to cities and towns of all sizes, enabling a nationwide WAN with just a few providers. Cradlepoint leads the market in 4G LTE technology, from narrow-band IoT solutions to providing a pathway to gigabit LTE and 5G. Cradlepoint branch solutions have integrated software-defined modems supporting advanced capabilities offered by cellular providers.

Feature Highlight: Cradlepoint branch routers accommodate two LTE modems and up to four carrier SIMs. NetCloud Manager lets customers centrally configure Smart WAN Selection and perform zero-touch deployments.

SD-WAN on Wheels

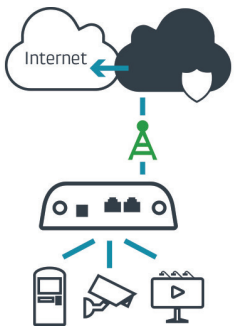


Many organizations—first responders, disaster response teams, mass transit, school districts, and more—rely on in-vehicle networks to serve their customers or the public. These mobile networks require a wireless WAN that delivers high availability, advanced security, and optimal application performance on the move.

Cradlepoint delivers the SD-WAN capabilities of its NetCloud platform in a ruggedized mobile router that combines multiple 4G LTE modems, WiFi, advanced edge security, GPS tracking, and telemetry integration—keeping vehicles, and the people and things in them, connected and protected.

Feature Highlight: Cradlepoint is the only SD-WAN mobile router that supports FirstNet, the private 4G LTE network for first responders. Policy-based Active-Dynamic traffic steering delivers persistent application sessions during cellular disruptions, and can intelligently steer applications between FirstNet and commercial LTE.

Connected & Protected IoT Devices



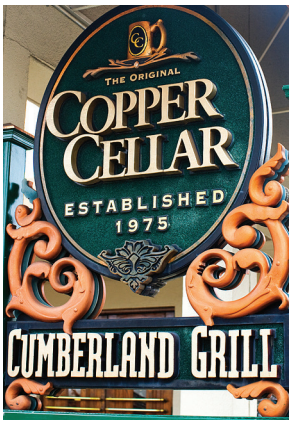
The news of Reaper and Mirai botnet attacks affecting millions of IoT devices illustrates the ever-increasing WAN vulnerabilities of IoT deployments. Cradlepoint, a global leader in 4G LTE routers for M2M/IoT networks, is the only vendor to integrate Software-defined Perimeter (SD-P) technology to provide perimeter security, a private IP overlay for Internet and enterprise WAN isolation, and micro-segmentation. Enterprises use NetCloud to orchestrate and deploy—in minutes—secure overlays for M2M/IoT devices anywhere, with no configuration or Internet-routable IP addressing required.

Feature Highlight: Cradlepoint's NetCloud Perimeter (NCP) feature is available on M2M and branch routers, enabling SD-P overlays that connect and protect M2/IoT devices in the branch or in the field. The NCP Client extends SD-P functionality to remote workforces that require secure access to Intranet and public cloud applications from laptops, tablets, or smartphones.

Stories of Software-Defined Networking in the Branch & Beyond

Stores Optimize Connectivity With SD-WAN

For its rapidly expanding restaurant chain, The Copper Cellar needed more flexibility, less hardware, better WAN uptime, and the ability to manage everything through the cloud.



The Copper Cellar streamlined its branches with Cradlepoint's SD-WAN solution, including a dual-modem router with wired broadband set up as the primary link and 4G LTE for failover.

Cradlepoint's NetCloud platform provides zero-touch deployment, single-pane-of-glass management, and SD-WAN services for optimized path selection. The IT team easily sets up business-based policies that seamlessly move traffic such as voice and video to the best-performing link.

Remote Sites Use LTE as Primary WAN

Professional Contract Services Inc. (PCSI) needed connectivity for its offices located in areas without access to wired WAN. With Cradlepoint's NetCloud Manager (NCM) and routers, PCSI's small IT team provides connectivity quickly and cost-effectively – with limited man-hours and simplified configuration, deployment, and remote management.

The IT team configures its routers at headquarters through NCM's single-pane-of-glass platform, then later can push out firmware upgrades, security patches, and other updates instantly.

"I was overwhelmingly impressed with how simple, quick, and easy it was to deploy Cradlepoint solutions," said Nathan Matarazzo, systems analyst at PCSI.

Cities Use SD-WAN in Police Vehicles

In major U.S. cities, police departments often face unreliable connectivity and insufficient bandwidth for their high-tech cruisers. With Cradlepoint's cloud-managed in-vehicle routers and extensibility docks with SD-WAN capabilities, officers are always connected to critical information and applications in the field.

This dual-modem SD-WAN solution enables cellular-to-cellular failover when a connection drops and dynamic traffic steering when it deteriorates. IT teams also can push out updates through the cloud rather than bringing each vehicle to headquarters.

Additionally, four-nines uptime enables officers to file report from anywhere instead of at the office, which improves incident response times.

Stores Protect IoT With Secure Perimeter

Many large retail and restaurant chains are installing video surveillance cameras to monitor employee and guest activity. However, without cloud access to their DVR systems, these enterprises lack PCI-compliant options for real-time monitoring.

IT teams address their IoT connectivity and security needs with cloud-managed Cradlepoint routers and NetCloud Perimeter (NCP), which enables a Virtual Cloud Network to be created in minutes. With NCP running on every router and on each manager's mobile device, a Software-defined Perimeter is established. With its own cloud-based network attached to a devoted VLAN, end-to-end encryption keeps data protected.

LEARN MORE ABOUT NEXT-GENERATION ELASTIC WAN CONNECTIVITY: **CRADLEPOINT.COM/ELASTIC-WAN**

cradlepoint

SD-WAN Solutions

We're Ready When You Are

Dell EMC is ready to provide turn-key hardware and software solutions designed to simplify and accelerate production-ready SD-WAN deployments and services, with a choice of SD-WAN software from Versa Networks, Silver Peak, or VeloCloud.

Introducing Dell EMC SD-WAN Ready Nodes

At Dell EMC, we view SD-WAN as a critical and necessary component for Digital Transformation. For Service Providers, SD-WAN represents an opportunity for creating new services, accelerating time-to-revenue and increasing service agility. For enterprises large and small, SD-WAN represents an opportunity to lower cloud connectivity costs, while also optimizing WAN traffic patterns and usage. Dell EMC has double down on strategy of open and verified solution choices, to build SD-WAN for production, by offering validated product options for SD-WAN services, that is built upon the industry's foremost virtualization infrastructure, and hardware platforms.

We're meeting this need with a family of Ready Node offerings, designed for Service Providers and Enterprises alike intended to simplify and accelerate SD-WAN adoption. At the heart of our Ready Nodes are validated, pre-tested solutions comprising of Dell EMC compute platforms and industry leading SD-WAN software offerings from Silver Peak, Versa Networks, and VeloCloud. Included in the Ready Node offerings are Bill of Materials (BOM), partner software SKUs for the appropriate use-cases, pre-installed drivers and firmware settings.

The choice of multiple ready node hardware platforms provides maximum deployment flexibility for large, medium or small environments. Moreover, multiple SD-WAN partners furthers that flexibility by supporting many use cases.

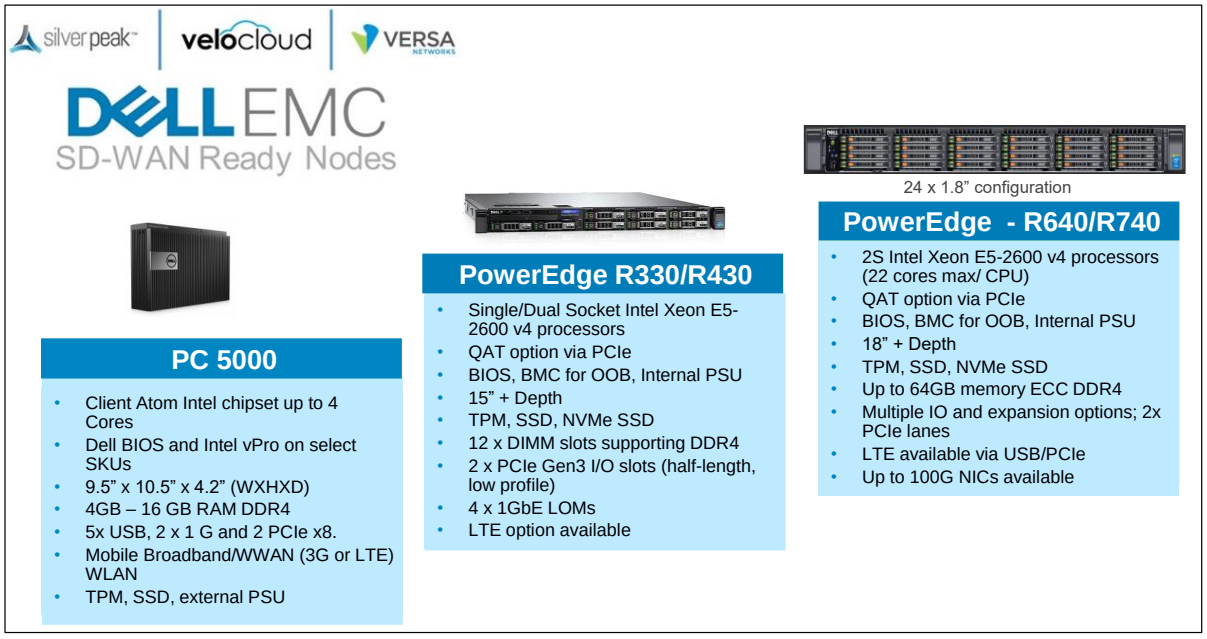


Figure 1. Dell EMC SD-WAN Ready Nodes

SD-WAN Ready Node use-cases

Service Providers can add new profitable managed services (e.g., cloud-managed SD-WAN or SD-Security service), and reduce their time-to-revenue for these new services. Communications Service Providers, for example, can improve their competitive advantage by offering a hybrid WAN allowing current customers to add managed internet bandwidth to their branches, particularly for less critical traffic flows. Managed Service Providers can generate new revenue streams by adding Managed SD-WAN services; and can further benefit in productivity improvements with features such as zero touch provisioning.

Enterprises can choose to deploy a do-it-youself on-premise SD-WAN, using the Dell EMC SD-WAN Ready Nodes. Enterprises can benefit with lower capital and operating costs, by leveraging lower-cost broadband connections and improving application performance, through intelligent route selection.

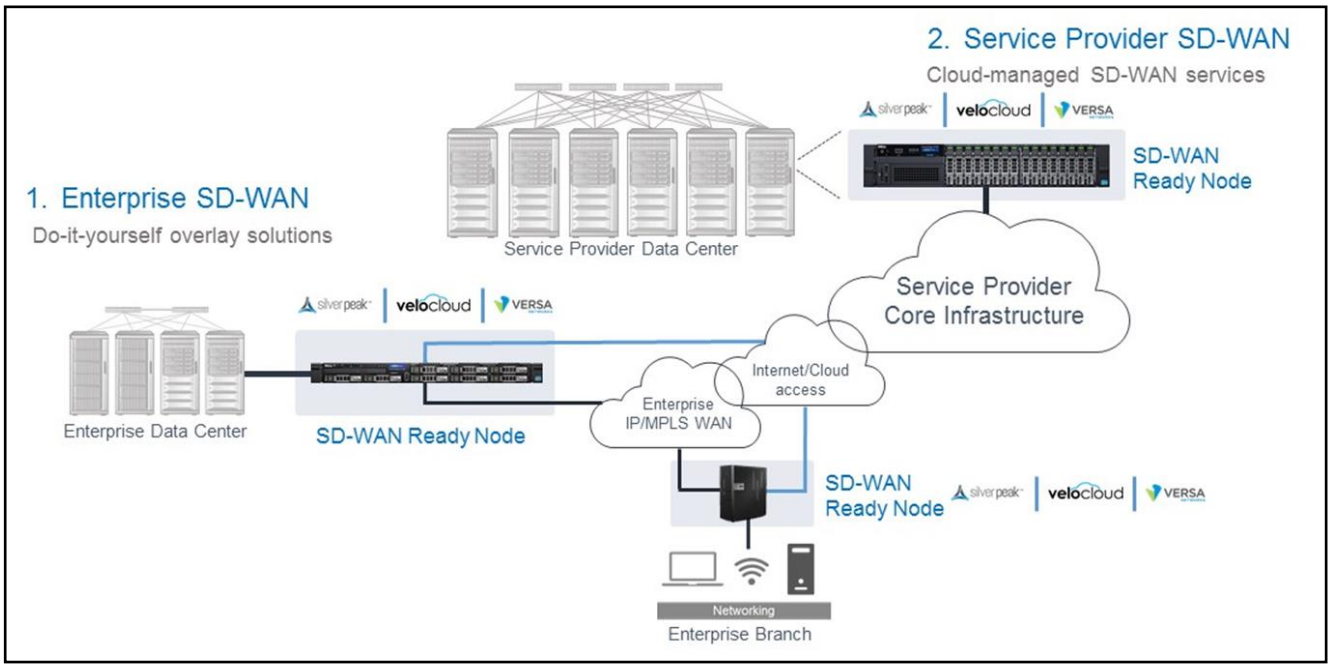


Figure 2. Dell EMC SD-WAN Ready Node use-cases

Take the next step

Contact your Dell EMC, Silver Peak, VeloCloud or Versa Networks representative to learn more about SD-WAN Read Nodes from Dell EMC.

Learn more about Dell EMC SD-WAN Solutions

Contact a Dell EMC Expert

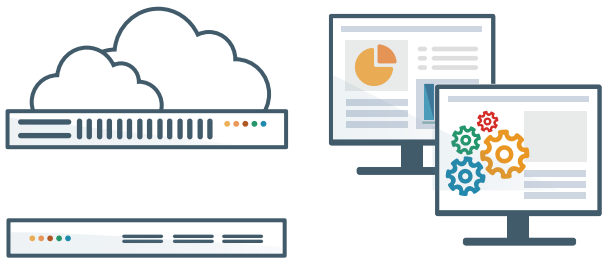
TALARI Networks™

SD-WAN SOLUTION OVERVIEW

Talari Networks, SD-WAN technology innovator, is engineering the internet and branch for maximum business impact by delivering a Failsafe Software Defined WAN (SD-WAN) solution that offers increased capacity, improved reliability, higher quality of experience while lowering costs. Talari's solution also enables a secure and consolidated branch infrastructure which delivers application and service deployment flexibility, without sacrificing availability or performance.

With the explosive growth in real time applications, distributed workforces and cloud computing, a company's productivity and customer responsiveness have never been more dependent on the WAN infrastructure. Because of this, organizations are turning their focus to their wide areas networks (WANs) and cloud access networks, knowing that having enough bandwidth to support the increased demand and predictable reliability to ensure continuous application availability are keys to their success.

The cloud is rapidly changing demands on enterprise IT legacy resources. The traditional WAN deployment of the last decade - MPLS circuits and enabling devices, often augmented by separate WAN-Op and firewall equipment - no longer offer enterprise IT the necessary requirements for cost savings, flexibility, bandwidth, manageability and streamlined cloud connectivity. Talari's failsafe WAN offers organizations the unique combination of availability, performance and reliability, yielding a highly resilient remote site with platinum application Quality of Experience.



Talari Solution Components

A Talari Networks Software Defined WAN, built on a comprehensive physical and virtual appliances portfolio, engineers the internet and branch for application reliability and unparalleled resiliency. Customers have great flexibility in determining how a Talari SD-WAN solution is deployed at the physical edge, the virtual edge, or in the cloud through the use of Talari's Controller, a full suite of appliances and centralized orchestration and analytics platform.

Failsafe Software Defined WAN

A Talari SD-WAN solution delivers a resilient network that ensures application availability while lowering cost. The following are some of the leading capabilities and benefits of this solution:

Secure Cloud Access with Visibility

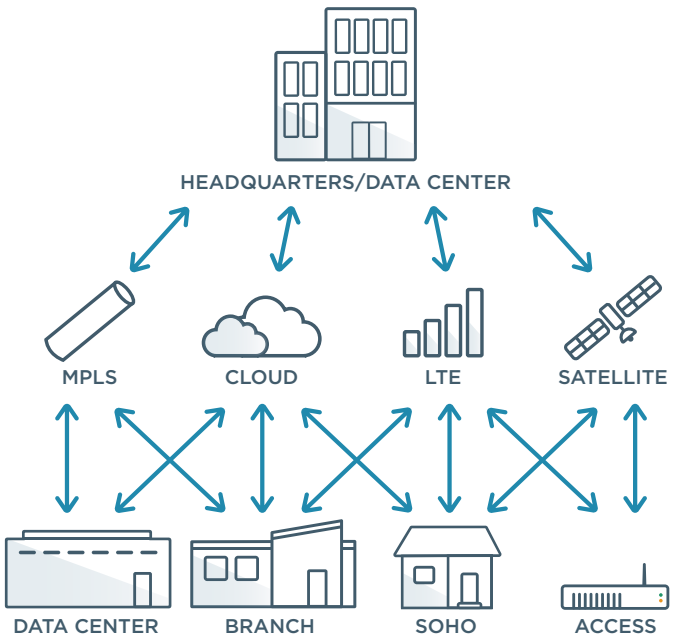
Talari extends the reach of the corporate WAN into the cloud by delivering an encrypted infrastructure with the performance, reporting and control capabilities a company requires to ensure a successful deployment.

Increased Application Quality of Experience

Talari ensures that applications work without interruption, even in the case of link failure or network impairments such as high jitter, delay, or packet loss.

Change WAN Economics with a Hybrid WAN

Companies can now modify their MPLS WAN infrastructure to incorporate low-cost, high-bandwidth broadband links that Talari technology converts into a business-class network.



SD-WAN Resiliency Benefits

- Continuous per-packet, unidirectional performance analytics that factor in packet loss, latency, jitter, and bandwidth between all paths and aggregated links
- Adaptive, deterministic per-packet optimal WAN-path decisions, and in particular sub-second response to degrading network issues such as link/device failures and/or congestion-based disruption or outages
- Enabling "liquid" application flows that are not impeded even when heavy loss/jitter occurs, let alone link failure
- Enabling single priority flows across multiple links; using all m/x/n paths between location pairs
- Ability to leverage all available bandwidth across multiple links, even for a single high-bandwidth flow
- Customizable by bandwidth availability: highly efficient bandwidth utilization
- Replication of flows and packets across disparate links, especially real-time apps like VOIP that require platinum QoS support
- Enables unmatched support for real-time and highly interactive apps
- Extremely scalable (thousands of WAN links with continuous, real-time path measurement) to accommodate QoE standards set by cloud service access providers and edge-network co-location facilities (carrier agnostic)
- Superior inbound congestion avoidance; that is, "bandwidth reservation and control" that enables business-quality app predictability

TALARI'S LEADING IT BENEFITS

- Gain resiliency, reliability and superior QoE
- Maintain high availability and uptime of business-critical apps
- Leverage bandwidth aggregation with commodity Internet services to reduce WAN legacy costs

DAYTON SUPERIOR

"Talari gives us the quality of service and guaranteed bandwidth we need to meet our service-level agreements for VDI and business applications." **- Dayton Superior**

Taft/

"I bought Talari to make the network more reliable, and it did exactly what it promised."
- Taft, Stettinius & Hollister, LLP

Driscoll's ONLY THE FINEST BERRIES

"After we implemented Talari...we went from paying $600 per Mbps to $100 per Mbps for bandwidth for our distribution centers. We scaled up the WAN bandwidth without scaling up the pricing." **- Driscoll Strawberry Associates**

Bremer Bank

"We can leverage Talari's capabilities to negotiate the highest bandwidth at the lowest cost without compromising reliability/availability in preparation for more rich content, video and streaming applications in the future." **- Bremer Bank**

Maricopa Region 911

"If a WAN link goes down, the call-takers are unaware. The peace of mind and visibility we get with Talari is invaluable." **- Maricopa 911**

United FEDERAL CREDIT UNION

"Talari provides the bandwidth we need to sustain our growth in an efficient and reliable platform."
- United Federal Credit Union

TO LEARN MORE OR REQUEST A DEMO, VISIT TALARI.COM

TALARI Networks

Talari Networks, Inc.
1 Almaden Blvd, Suite 200
San Jose Ca, 95113

Phone: +1 408.689.0400
info@talari.com
www.talari.com

SOLUTION-OVERVIEW-201707-007

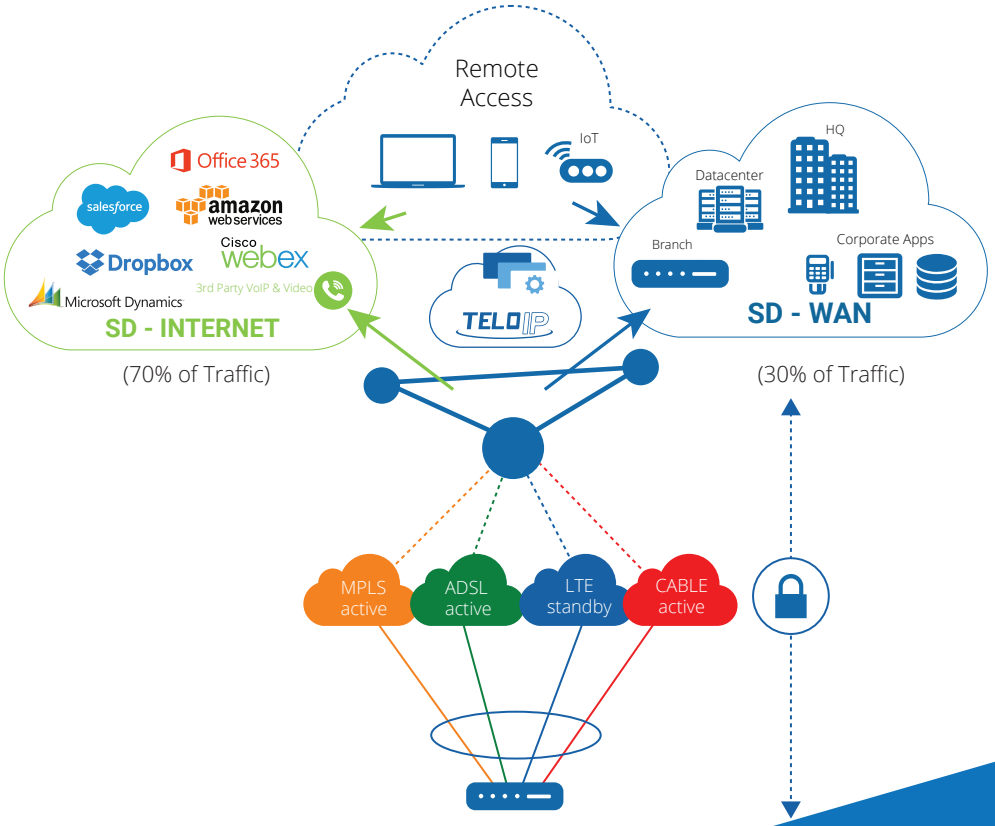
RISK FREE SD-WAN

Experience

For over 15 years, TELoIP has been managing converged voice, video and data solutions that deliver the promise of the internet for business customers.

Hardened Infrastructure

TELoIP Cloud network is carrier-class SD-WAN-as-a-Service infrastructure providing both high-availability and high-performance plus a long haul WAN transport network for the lowest overall cost.



SIMPLIFYING CLOUD ACCESS
WITH SOFTWARE DEFINED NETWORKS

VINO SD-WAN

CLOUD CONNECTIVITY

We eliminate barriers to SD-WAN adoption by leveraging a turnkey, multi-tenant cloud (the TELoIP Cloud) with nine points of entry in North America. We located each point of entry in carrier-neutral facilities, allowing us to take advantage of a plethora of blended transit services co-located in these sites.

COST-EFFECTIVE

VINO SD-WAN allows enterprises to take advantage of broadband pricing and carrier diversity to create a non-stop network ensuring virtual private network reliability and performance at 'best effort' price points.

CLOUD MANAGED

The TELoIP Cloud creates a Virtual Intelligent Network Overlay (VINO) that unifies all branch traffic into a single cloud-managed SD-WAN overlay connection.

WHY IS TELOIP DIFFERENT

TELoIP has long held that the battleground is on the network edge, where our patented ANA/IPDE/MPDS technologies provide a measureable performance advantage over any other SD-WAN competitor — especially with poor underlays or under congested busy hour conditions..

TELoIP's VINO architecture provides a patented Virtual Network Function (VNF) Control Plane that builds a full mesh topology between points of entry. The multi-patented Data Plane provides comprehensive underlay management and Virtual Network Functions (VNF) for IPQoS, Firewall, Link Aggregation, Failover and Routing. The VINO Portal offers complete Management Plane with service orchestration, move, add, change delete support and performance visualization.

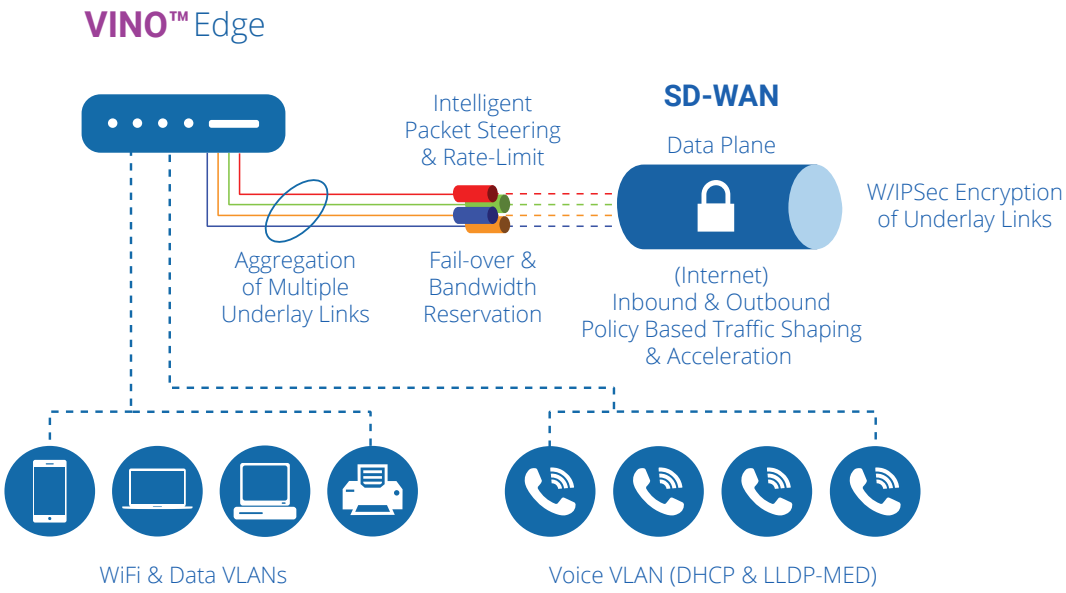
TELoIP offers substantial differentiation, with patented technology in each of the data plane, control plane and management plane that delivers higher aggregated speeds and better quality of experience than competitive solutions when tested using the same underlay links and test scenarios. We believe that TELoIP is well-positioned in the SD-WAN market because:

- Only TELoIP provides both WAN and Internet optimization
- TELoIP enables high-quality voice and video calls with no drops
- We address the need to connect remote and mobile users securely
- We can address scalable security requirements for IoT ecosystems
- VINO SD-WAN aligns network services to user, application and business requirements

TELoIP Inc. | 1-5430 Timberlea Blvd., MIssissauga, ON L4W 2T7 | TEL: +1 416 203 7838 | www.teloip.com | info@teloip.com

VINO SD-WAN DELIVERS

- VoIP Quality-of-Experience
- 'Hitless' VoIP/Video Fail-over
- Increased Performance
- Software Defined Perimeter
- Cloud Managed Network
- Centralized Orchestration
- Secure Remote Access Solutions
- Cloud Agility
- Lower WAN Costs



WHY VINO SD-WAN

INNOVATION

Deploy knowing TELoIP has the deepest intellectual property portfolio in the SD-WAN business. We turn business challenges into technology solutions, with award-winning technology that has been awarded 21 patents and counting

EASY TO BUY & DEPLOY

We ensure customer success by combining all the VINO SD-WAN components into a simple, predictable license fee that includes professional design, installation and ongoing 24/7/365 support.

NON-STOP BROADBAND

We build unbreakable cloud tethers backed with impeccable network engineering and support services. Working with our partners we ensure that you have a risk-free experience.

KEY CHALLENGES WE ADDRESS

- Network Reliability & Uptime
- VoIP & UCaaS Performance Issues
- Multi-Cloud Reliability & Performance
- End-User Productivity
- Network Capacity/Bandwidth
- Branch Office Security
- Branch Office Complexity
- Network Visibility and Control
- Remote/Mobile/IoT Device Access
- Support of Digital Transformation Efforts
- IT Budget Pressure

CONTACT

SMB or Enterprises – Call us for SD-WAN consultations from Network Design to ROI Calculation and Price Quotes at info@teloip.com

About the Webtorials® Editorial/Analyst Division

The Webtorials® Editorial/Analyst Division, a joint venture of industry veterans Steven Taylor and Jim Metzler, is devoted to performing in-depth analysis and research in focused areas such as Metro Ethernet and MPLS, as well as in areas that cross the traditional functional boundaries of IT, such as Unified Communications and Application Delivery. The Editorial/Analyst Division's focus is on providing actionable insight through custom research with a forward looking viewpoint. Through reports that examine industry dynamics from both a demand and a supply perspective, the firm educates the marketplace both on emerging trends and the role that IT products, services and processes play in responding to those trends.

Jim Metzler has a broad background in the IT industry. This includes being a software engineer, an engineering manager for high-speed data services for a major network service provider, a product manager for network hardware, a network manager at two Fortune 500 companies, and the principal of a consulting organization. In addition, he has created software tools for designing customer networks for a major network service provider and directed and performed market research at a major industry analyst firm. Jim's current interests include cloud networking and application delivery.

For more information and for additional Webtorials® Editorial/Analyst Division products, please contact Jim Metzler or Steven Taylor.

Published by Webtorials Editorial/Analyst Division
www.Webtorials.com

Division Cofounders:
Jim Metzler
jim@webtorials.com
Steven Taylor
taylor@webtorials.com

Professional Opinions Disclaimer

All information presented and opinions expressed in this publication represent the current opinions of the author(s) based on professional judgment and best available information at the time of the presentation. Consequently, the information is subject to change, and no liability for advice presented is assumed. Ultimate responsibility for choice of appropriate solutions remains with the reader.