vmware®

GET STARTED

How SD-WAN Supports Digital Transformation in Healthcare

The Healthcare Industry is Evolving

Providing healthcare today is much more than making a diagnosis or prescribing a medication. The landscape for healthcare is evolving and there are many trends affecting the healthcare industry.

- Technology advances, such as CAT scans, imaging, and video are being used increasingly and carried over the network from central storage locations to the point where they are viewed.
- Hospitals were the sole owners of the data, now retail pharmacies and private equity are getting involved, which means more data is being shared with stakeholders.
- Healthcare systems are moving to rural locations, which are hard to serve effectively with existing network technology.
- Many organizations are going through a digital transformation. They need to support applications that are in the cloud.
- There is a need to provide greater access to information for patients and to provide improved performance for real time applications. Organizations need to support the growing use of mobile devices, yet also need to comply with regulations that require data protection and meet payment card standards.

Advancements in medicine, the increase in regulations to protect patient and doctor, and the digitization of the entire process requires a scalable, secure, uninterrupted and bandwidth-flexible healthcare IT network.

Healthcare IT Environments

The healthcare information technology (IT) environment is changing rapidly.

According to primary research of health organizations by research firm, ESG:

- **45%** of organizations are concerned with the increase in number and types of applications being used.
- **71%** of physicians are using telemedicine which puts pressure on the wide area network (WAN) links.
- **55%** of healthcare organizations are using virtual desktop infrastructure (VDI) which is bandwidth intensive and needs to work in real time.
- **43%** seeing higher data volumes due to increased application usage from telemedicine and VDI.
- **34%** increase in number and type of endpoint devices. Many organizations are supporting on-premises data centers and public cloud providers.
- **20%** reporting increase in number of remote/mobile workers.
- **100%** must comply with patient data protection regulations.

https://www.velocloud.com/sd-wan-resources/white-papers/positive-impact-of-sd-wan-on-healthcare

Critical Healthcare Use Cases

There are five main healthcare use cases where the network is critical.

Virtual Desktop Infrastructure

Clinicians are increasingly turning to VDI so that they can easily use technology at the point of care to access electronic medical records (EMRs). VDI supports multiple devices, such as smartphones and tablets, and it has robust security for the Health Insurance Portability and Accountability Act (HIPAA).

However, it also requires high levels of bandwidth, which is often not available in most clinics or branch offices. Patient files and records have shifted to digital forms—EMRs and electronic health records (EHRs)—and organizations increasingly leverage cloud-based storage and application delivery to enable care providers with constant access.

Telehealth/Telemedicine

Telehealth heavily utilizes video conferencing as a virtual connection point between a patient and a care provider. It also leverages cloud applications to deliver access to EMRs and the sharing of high-resolution medical images. This unified communications (UC) application requires a high level of reliable bandwidth.

Integrating EMR/EHR with cloud-based healthcare solutions gives an array of benefits such as effortless sharing of data and checking of e-prescriptions. EMRs are moving to cloud-based records systems, which facilitate the ability to do analytics on the data.

By having all data in the cloud, it becomes much easier to access records, bills, and health insurance plans. With the presence of cloud computing, the mobile health market becomes more accessible and automated.

Quality of service

When a patient requires over-the-phone care or physicians need to discuss patient cases for assessment and diagnosis, quality of service (QoS) is critical. Dropped calls or jitter-heavy connections are detrimental to providing high-quality care.

Pre- or post-treatment payment

Healthcare offices and clinics often require patients to render payment at the time care is provided. This requires that offices provide either a payment device or an ATM connected to the network. Not only must this highly sensitive data be segmented from regular office traffic, but it must also adhere to Payment Card Industry Data Security Standard (PCI DSS) Compliance regulations.

Remote branch offices, clinics, and pharmacies

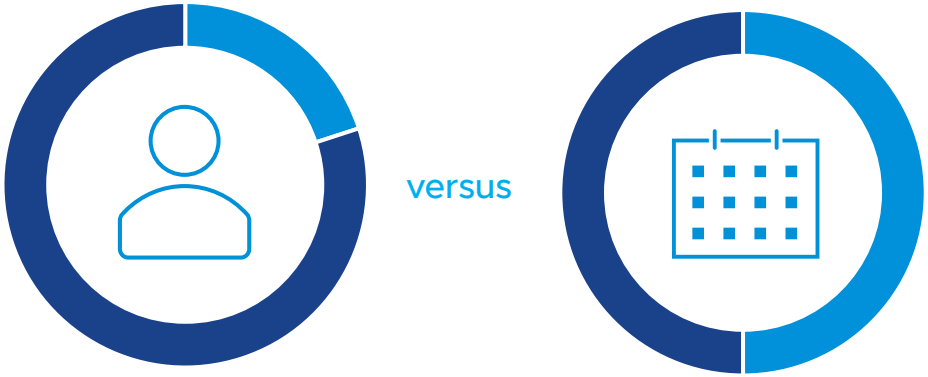
Healthcare systems are moving to rural areas which are hard to serve with existing network technology. Growth by merger and acquisition is a growing strategy for healthcare organizations, meaning that care is often shifted to small remote or regional branch offices.

Impact of IoT

Internet of Things (IoT) impacts the network because more devices are being connected that transmit data to a central location from remote offices. For many organizations, IoT initiatives have moved beyond early adoption and into mainstream adoption.

The increasing numbers of IoT devices will present a larger attack surface for hackers and drive additional data across the network. This brings on security concerns and the need to segment.

20%
Of organizations currently have an IoT initiative underway



versus

51%
Plan to deploy within 12-24 months

The increasing numbers of IoT devices will present a larger attack surface for hackers and drive additional data across the network.

https://www.velocloud.com/sd-wan-resources/white-papers/positive-impact-of-sd-wan-on-healthcare

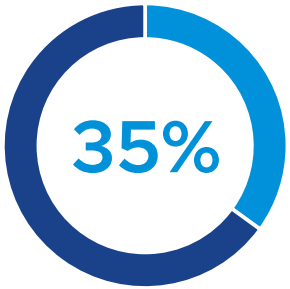
Buying Criteria for Healthcare IT

To meet evolving requirements, many healthcare organizations are embarking on digital transformation initiatives to deliver the appropriate workflows, policies, processes, and IT environments to provide a better experience for their stakeholders. Electronic medical records, access to cloud-based applications, and connected IoT devices are all enabling healthcare professionals to provide higher levels of services. Research from ESG indicates that 7 percent of healthcare organizations report having a mature digital transformation initiative, while 66 percent report they are either beginning or in process. The research also reveals that 89 percent of healthcare organizations currently use some form of public cloud service, whether software as a service (SaaS), infrastructure as a service (IaaS), or platform as a service (PaaS).

https://www.velocloud.com/sd-wan-resources/white-papers/positive-impact-of-sd-wan-on-healthcare

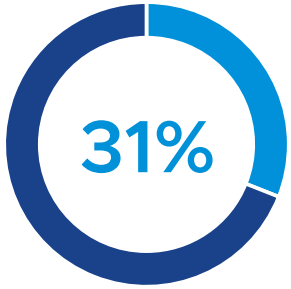
It is important to understand that IT transformation can determine the degree of success of the digital transformation program. The underlying IT environment is a key enabler, especially when connecting to cloud applications, centralizing medical records, and transmitting diagnostic imaging. ESG research also shows that the most important considerations for healthcare when justifying IT investments are improved customer satisfaction (35 percent), improved security (31 percent), and increased employee productivity (31 percent).

Provide a better patient experience



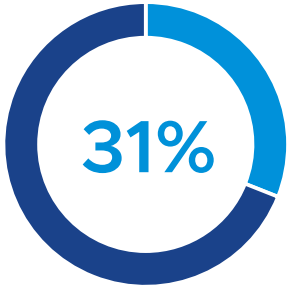
Improved customer satisfaction

Ensure secure communications



Improved security

Empower the caregivers



Increased employee productivity

Medical organizations want to differentiate the patient experience—this means adopting new technology for interacting with doctors and making payments easier. They also want to improve security and data protection and need to make sure that patient data is protected. In addition, they want to use new technology such as iPads and tablets, which are used for viewing patient records and doing remote consultations.

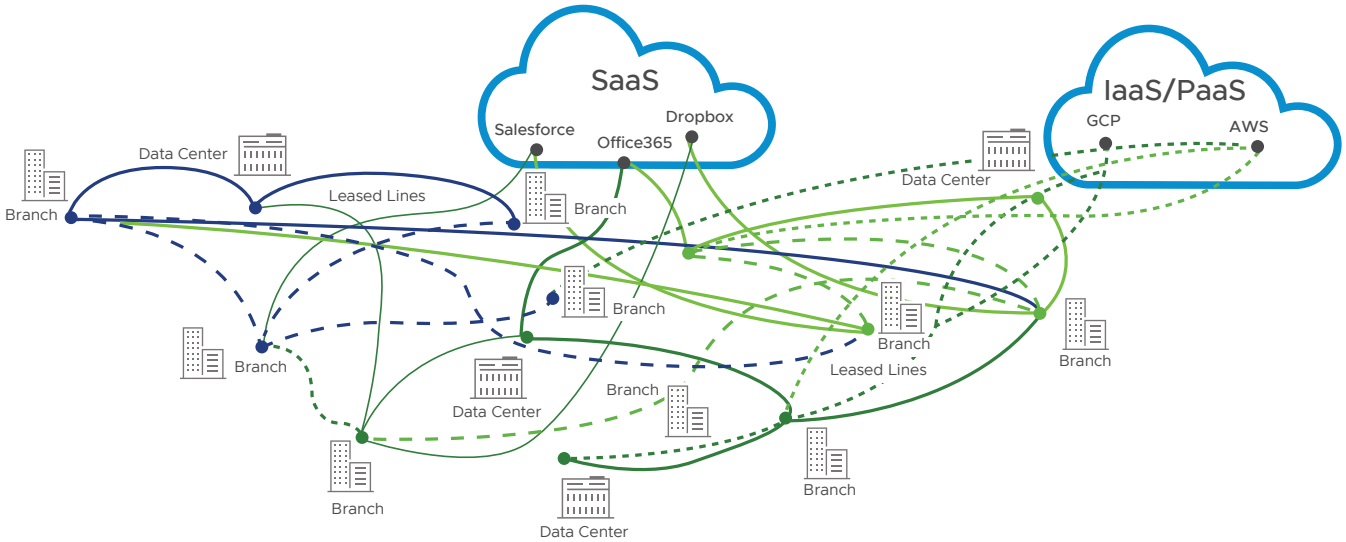
https://www.velocloud.com/sd-wan-resources/white-papers/positive-impact-of-sd-wan-on-healthcare

Healthcare WAN is Complex

A major impediment to the transformation of healthcare is the network, which has become increasingly complex. Some of the issues include:

- The many connections to the hospital, remote offices and mobile devices.
- Lack of visibility into network traffic and performance.
- Security challenges with keeping patient data safe.
- Healthcare facilities have relied on private links from service providers using Multiprotocol Label Switching (MPLS) technology between sites and primary centers of data. MPLS is difficult to implement in every location, especially at smaller offices or clinics, due to its high cost and long provisioning times.

Healthcare is shifting away from MPLS and adopting software-defined wide area network (SD-WAN) either alongside it or as a substitute when MPLS contracts run out.



How SD-WAN Can Help

There are many ways that SD-WAN can help reduce network complexity. SD-WAN ensures application performance and reliability, enables agile rollouts, lowers costs and simplifies security.

Application Performance & Reliability

- Optimal customer experience
- Reliable uptime
- Cloud and legacy apps

Agile Rollouts

- Broadband & LTE
- Zero touch deployments
- Flexible configurations

Lower Cost

- Economical bandwidth
- Lower IT costs
- Efficient usage

Simplified Security

- Enables business
- Minimizes risk
- Reduced compliance efforts

Cloud Delivered VMware SD-WAN

VMware SD-WAN™ is a network service built on three components.

VMware SD-WAN Edge

Device that sits in your branch office locations that provides WAN connectivity.

VMware SD-WAN Orchestrator

Cloud-hosted centralized management system that requires no installation, only a connection to get started. The VMware SD-WAN Edge devices are configured by the VMware SD-WAN Orchestrator.

VMware SD-WAN Gateway

Hosted in point of presence (PoPs) around the world. Traffic is sent to the VMware SD-WAN Gateways from the VMware SD-WAN Edge and then routed to the destination, while providing optimization.

VMware SD-WAN simplifies WAN deployment with a cloud delivered model. The solution is an overlay on the existing network that is easy to deploy and manage. The solution components are delivered as a service for a subscription and hosted by VMware in the cloud.

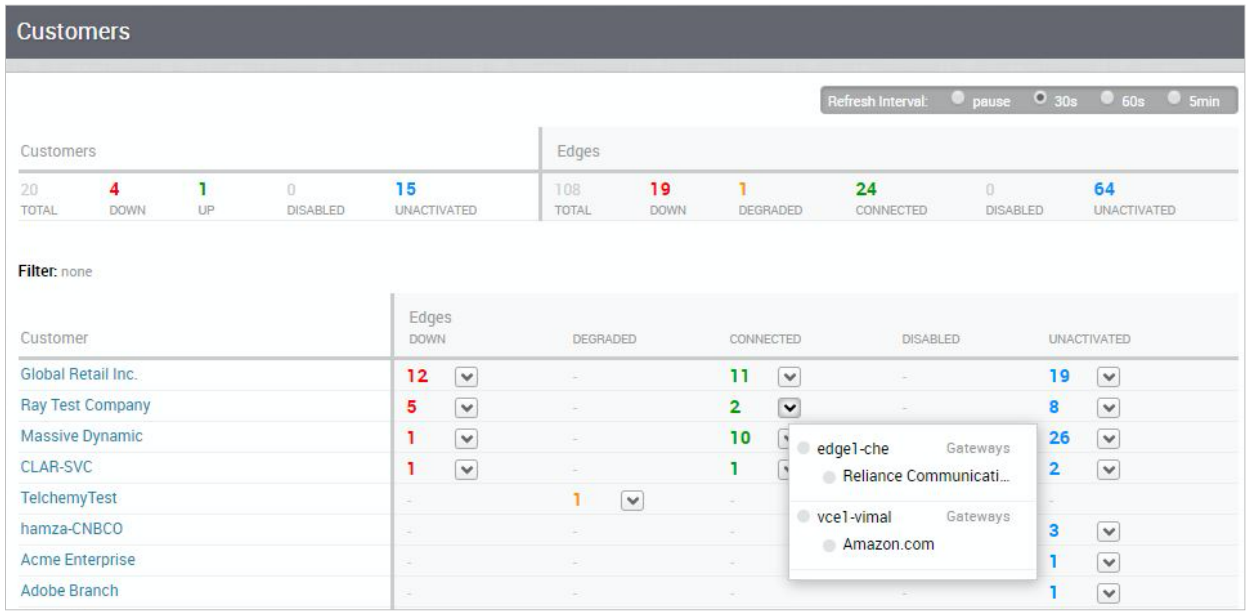
The important design of this SD-WAN model is that it is a transport independent overlay that can work across any combination of circuits deployed to connect any location to applications.

It enables connectivity to both enterprise data centers and SaaS applications and IaaS in the cloud. It provides an orchestration layer for monitoring and configuration, as well as a controller for managing the control plane of the overlay network.

VMware SD-WAN Orchestrator

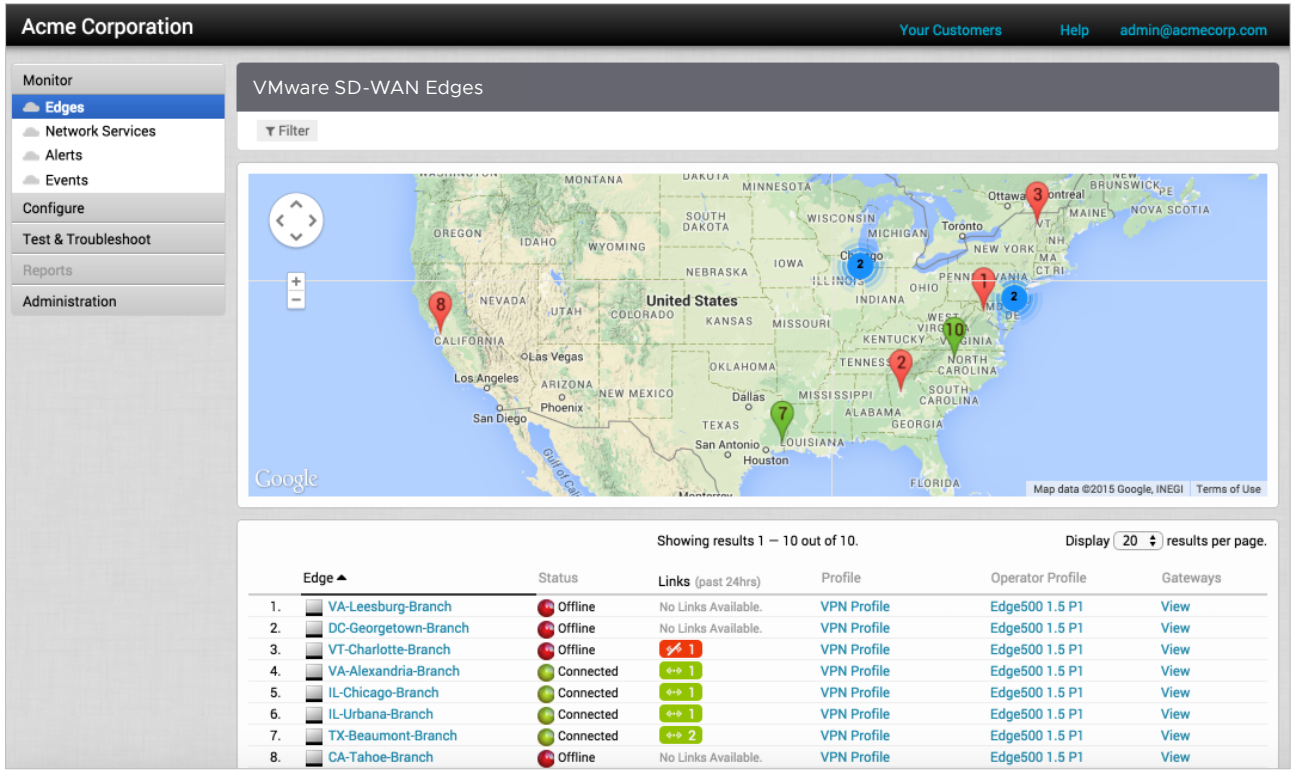
The VMware SD-WAN Orchestrator manages the provisioning of the VMware SD-WAN Edge devices, saving time in setting up new sites and in keeping devices configured correctly for the best performance. The VMware SD-WAN Orchestrator makes it easy to push out a predefined configuration and eliminates the need to access each device and configure line by line, like with routers. This means that the VMware SD-WAN Edge devices always handle application traffic efficiently. It also means that devices are always operating properly and if something happens to one, it can quickly be put right by resetting its configuration or troubleshooting the condition on the network.

The VMware SD-WAN Orchestrator can save hours of time spent on device management because it can configure all devices from the central console using policies. The Orchestrator makes it easy to monitor devices and the performance of applications. It is used to set policies for prioritization of applications on the network to ensure that the most important applications get the top priority.



The VMware SD-WAN Orchestrator provides a dashboard to monitor performance of network connections and applications which directly show the benefits provided by VMware SD-WAN. The application monitoring features in the VMware SD-WAN Orchestrator allow troubleshooting of issues in much less time and prevent poor application performance, saving on application down time.

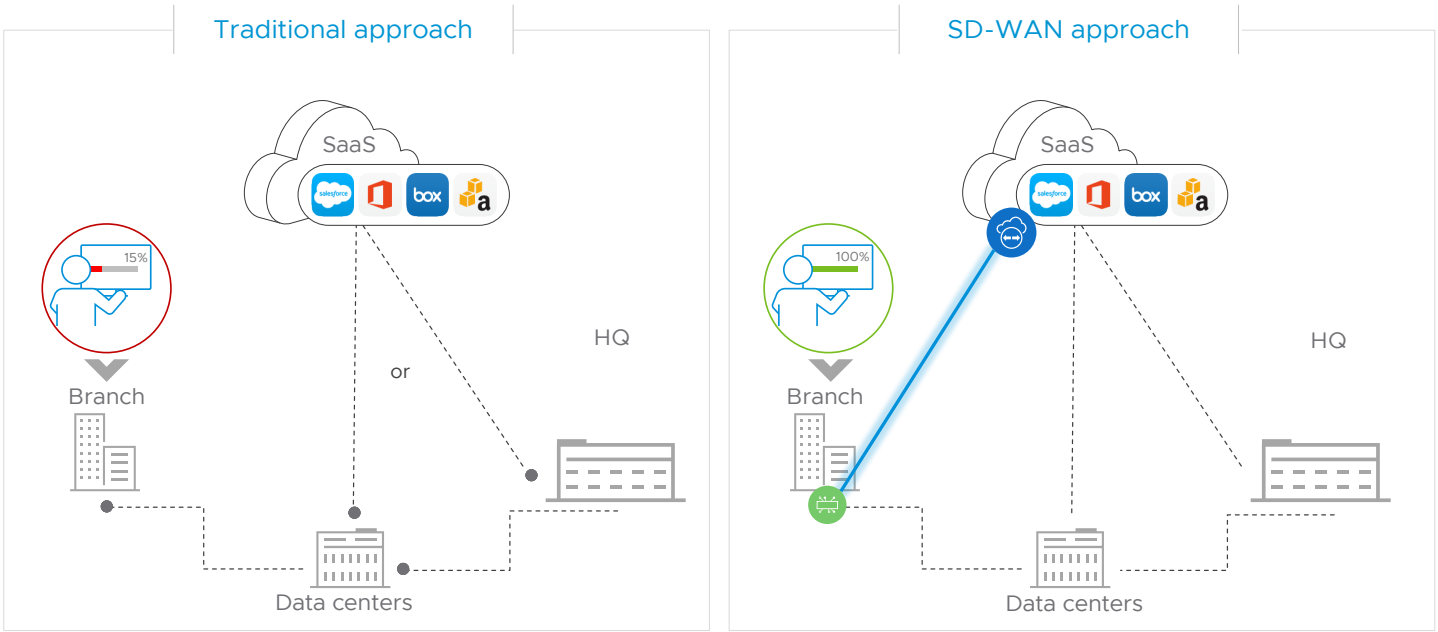
Healthcare IT teams now have visibility into the traffic flowing across the network and can ensure critical applications are prioritized over less-critical traffic. This is especially important in blackout/brownout situations, as SD-WAN can predict and remedy these situations, often repairing the lines to ensure connectivity stays consistent. VMware SD-WAN dynamically adjusts to the underlying network conditions and either steers or remediates the access and transport of these critical applications.



VMware SD-WAN Gateways

The VMware SD-WAN Gateways improve application performance by bringing users closer to the cloud. This is done by connecting office locations through the VMware SD-WAN Gateway that is hosted by VMware in a PoP close to the applications. Instead of the connection going back to the data center location and then going out to the hosted application, the connection goes directly to the application, over the Internet.

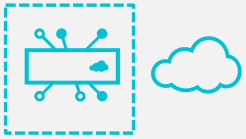
The VMware SD-WAN Gateway provides optimization between it and the VMware SD-WAN Edge device in the branch office location. So, no matter where applications reside, the performance is consistently good. The Gateways don't need to be owned or managed; they are all cloud hosted by VMware and provided as a service as part of a subscription.



VMware SD-WAN Edge

A VMware SD-WAN Edge device sits at each location, such as a branch office and data center. The VMware SD-WAN Edge device connects sites to the WAN and to the Internet and then to applications, in data centers or hosted in the cloud. The VMware Edge devices and the VMware SD-WAN Gateways communicate with each other to deliver optimization between them. These devices are auto configured so they're quick and easy to install. The cost to deploy these devices is much lower than with a typical router, that must be configured manually device-by-device.

VMware SD-WAN Edge devices support three models for deployment.

Option 1	Option 2	Option 3
Edge software pre-installed "bare metal" on VMware SD-WAN hardware	Virtual Edge installed on ESXi or KVM ESXi license not included	Virtual Edge installed in AWS or Azure On marketplace, BYOL IaaS fees not included
		
VMware SD-WAN Edge 510 to 2000	- Dell VEP4600 uCPE certified	

Simple and Quick Deployment: Pull Activation

VMware SD-WAN appliances automatically authenticate, connect, and receive configuration instructions once they are connected to the Internet in a zero touch deployment model. There is no need for a visit by IT staff, no need for pre-staging, nor any security risk if a device is lost, as it won't have any configuration on it. These devices auto detect the link type that they are connected to, so the installer doesn't need any site-by-site link knowledge. They don't require tracking by serial number and they're really easy to install.

1 Create config & send key

IT admin adds a new VMware SD-WAN Edge in the customer account.

IT admin generates an activation key and emails it to the installer.

2 Device ships

VMware SD-WAN Edge with factory default config is shipped to the remote site.

Office admin powers up the device and connects it to the internet.

3 Install, authenticate & pull config

Office admin plugs in the device and connects to the Internet through VMware SD-WAN Edge WLAN/LAN

Office admin clicks on activation link in the email. Edge is activated.

Assured Application Performance Over Any Link

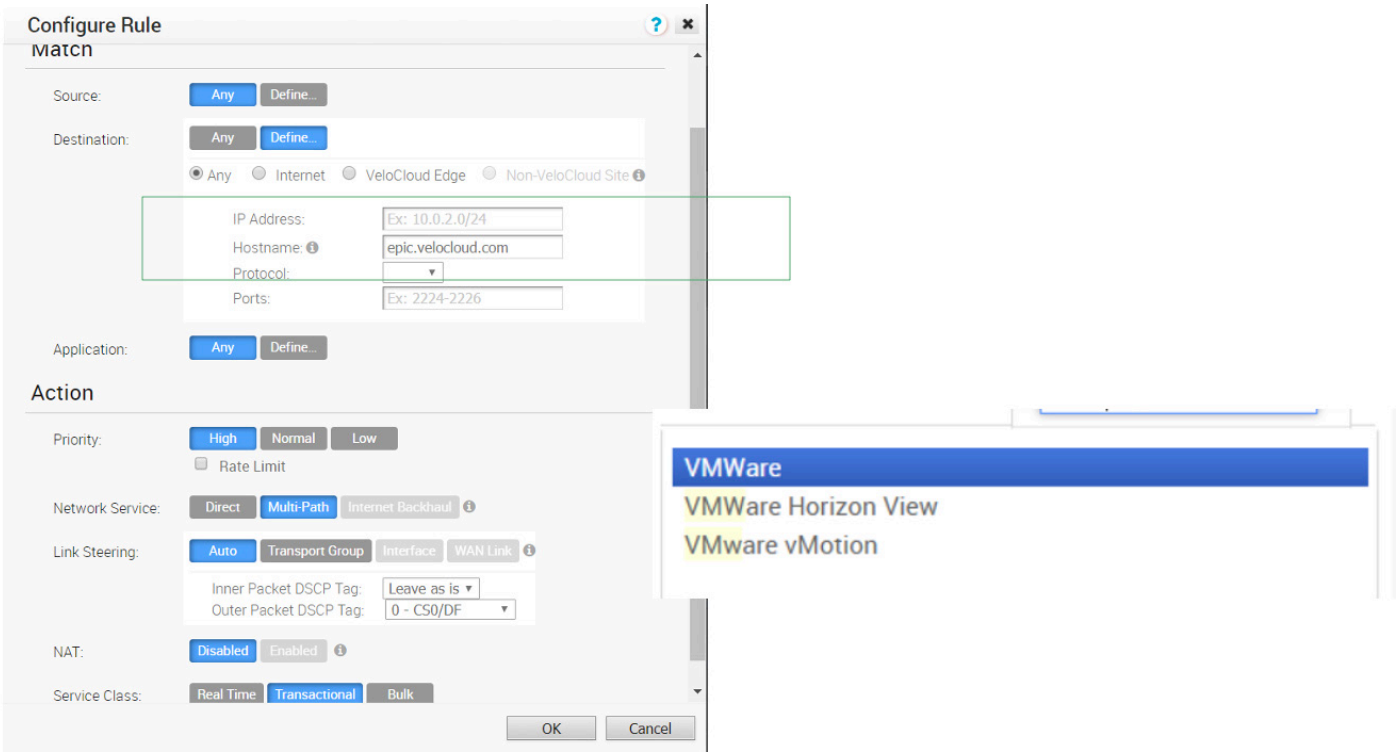
VMware SD-WAN increases the performance of applications over the WAN with real time remediation and traffic steering. The VMware SD-WAN Edge bonds multiple links and virtualizes them to act as one. If an existing link doesn't have enough throughput, easily get a second link and increase bandwidth without changing anything about the network. Combine links of many types, for example, add cheaper broadband to an MPLS link.

If there are two links, one MPLS and Broadband, connecting a branch site to a data center and there is a problem on one link, the VMware SD-WAN Edge device immediately steers traffic to the other link. This ensures good performance, even if the links are of varying quality. With this arrangement you can increase throughput while reducing the cost per unit and still maintain the reliability of connections.

VMware SD-WAN Dynamic Multipath Optimization™ (DMPO) is the feature responsible for traffic steering and continuous monitoring. As it detects congestion, DMPO moves traffic to the best link. It performs steering packet-by-packet over both of the links at the same time, without having to wait for a total link failure to facilitate the switch over. As the connection degrades, DMPO activates traffic steering. Unlike with routers used in a hybrid network, with DMPO, there is no waiting for routes to reconverge. If both links are experiencing congestion, the system will send duplicate packets in real time over both links to ensure they get through. This translates to a high-quality user experience, even with sub-optimal link conditions. Unlike redundant links on a router that are active/passive, with VMware SD-WAN, all links are utilized active/active, which is most cost efficient and offers the best performance, where transitions are seamless.

Prioritize Epic, VDI

VMware SD-WAN recognizes over 2000 applications. You can establish application priority using pre-installed templates. VMware provides support for virtual desktop applications, including VMware Horizon, and Citrix VDI. Application policies are simple to configure with the graphical interface. Setting up a policy will ensure high performance for medical applications such as EPIC that run on VDI.



PCI DSS 3.2 Certified SD-WAN

VMware SD-WAN is certified for PCI DSS 3.2. This ensures Payment Card Industry (PCI) compliance in a simple, efficient, and cost-effective manner. Organizations benefit from a PCI Attestation of Compliance (AOC) to help pass and simplify the PCI audit and know that solution components are PCI compliant.

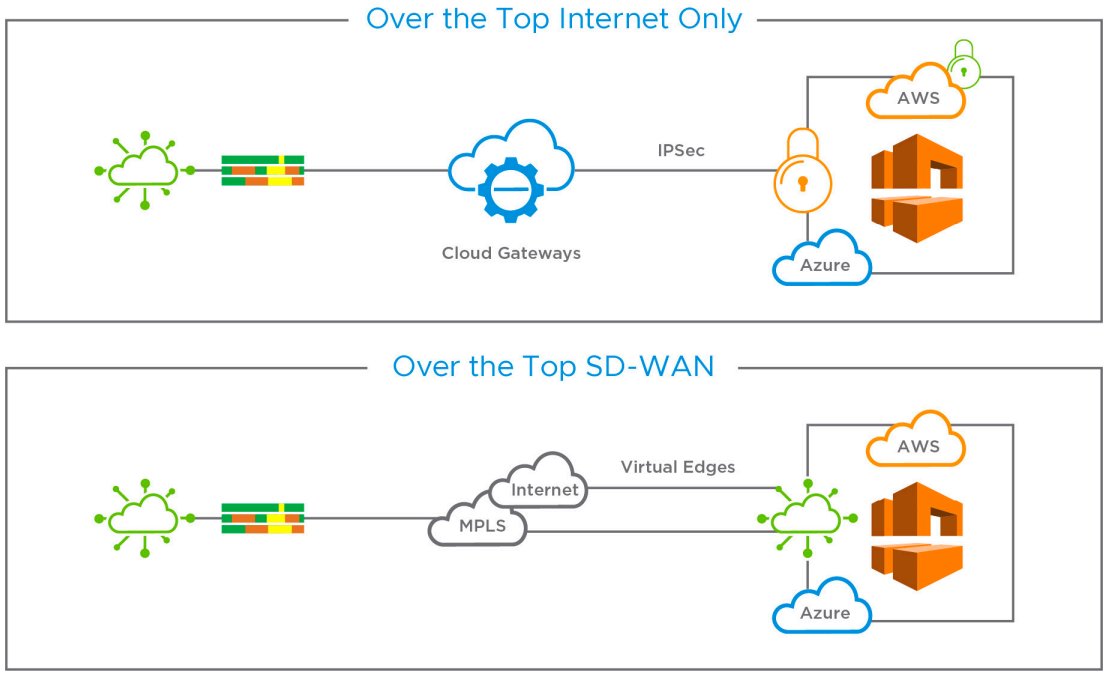
The VMware SD-WAN solution is validated by the PCI Security Standards Council and Coalfire, an industry certification organization. This means that you can use VMware SD-WAN with confidence in your PCI environment.

PCI DSS Requirement	Description of Requirement	Compliant to PCI DSS Requirements *(Select One)*	
		YES	NO
1	Install and maintain a firewall configuration to protect cardholder data	☒	☐
2	Do not use vendor-supplied defaults for system passwords and other security parameters	☒	☐
3	Protect stored cardholder data	☒	☐
4	Encrypt transmission of cardholder data across open, public networks	☒	☐
5	Protect all systems against malware and regularly update anti-virus software or programs	☒	☐
6	Develop and maintain secure systems and applications	☒	☐
7	Restrict access to cardholder data by business need to know	☒	☐
8	Identify and authenticate access to system components	☒	☐
9	Restrict physical access to cardholder data	☒	☐
10	Track and monitor all access to network resources and cardholder data	☒	☐
11	Regularly test security systems and processes	☒	☐
12	Maintain a policy that addresses information security for all personnel	☒	☐
Appendix A1	Additional PCI DSS Requirements for Shared Hosting Providers	☒	☐
Appendix A2	Additional PCI DSS Requirements for Entities using SSL/early TLS	☒	☐

Connectivity to IaaS

Many organizations are using cloud IaaS. With so many applications being hosted in the cloud, easy access with high performance is a necessary part of an SD-WAN solution. Set up an optimized connection using SD-WAN and connect with a virtual edge in the cloud.

An important part of the VMware SD-WAN infrastructure is the cloud hosted VMware SD-WAN Gateways that provide access to SaaS applications. These gateways terminate connections from the VMware SD-WAN Edge devices and direct traffic over high-speed links to applications. The VMware SD-WAN Gateways are hosted close to the applications for the best performance and are multitenant, so that they can serve many customers. VMware SD-WAN partners with the top cloud providers such as Amazon Web Services (AWS), Azure and Google Cloud for this service and is a built-in part of the solution.



Distributed Services Insertion

An important part of a security plan is to be able to use outside services. Many security services are provided as a service from the cloud. VMware SD-WAN make this easy with a service chaining capability where you can direct traffic to cloud hosted security services, such as web firewalls and URL filtering services.

VMware SD-WAN provides a simple, policy-based service chaining capability to direct traffic flows to cloud services. Using VMware SD-WAN, you can:

- Direct different applications to different destinations depending on the need.
- Service chain through the firewall or apply a virtual private network (VPN) or URL filtering.
- Set up services with policies and customize as needed.

The process is easy with one-click application aware services insertion. Automated service chaining reduces branch complexity and enables implementation of services. With this capability, you can ensure the security of traffic going over the Internet.

Virtual Services Delivery

An important part of your business is your data and it needs to be protected. VMware SD-WAN provides for security services in several ways.

- For a **smaller location** you can use the built-in firewall on the VMware SD-WAN Edge.
- For a **medium sized location**, the VMware SD-WAN Edge device provides a hosting capability where you can run a next-generation firewall (NGFW) from one of the popular vendors for this type of service.
- For a **larger branch office** that needs to deploy many virtual machines (VMs) for multiple network services, you can use the virtual network function infrastructure.

Objectives for Remote Field Clinics

VMware SD-WAN offers a number of advantages for remote field clinics.

Fast activation of remote sites over any connection type.

Instant onboarding for new networks and sites.

Consistent security posture for remote locations.

Improved unified communications.

Reserved bandwidth and best link selection to support telemedicine and large image file transfers.

Protected medical data through network segmentation.

Case study: Saber Healthcare Group

Who:

Saber Healthcare group

Objective:

Managing care and health of 10,000 residents, growth by acquisition

Before VMware SD-WAN:

- Limited bandwidth to support their many high throughput applications, including telemedicine and remote doctor visits.
- It took a long time to bring new locations onboard due to the limited connectivity options from legacy service providers.

With VMware SD-WAN:

- Increased network visibility and can troubleshoot applications faster.
- Reduce the number of in-person visits with the doctor by using video.
- Save money by using lower cost circuits over the Internet instead of private lines.

VMware SD-WAN Advantages for Healthcare

The benefits of VMware SD-WAN include:

- Simple to install and manage VMware SD-WAN Edge device that can replace your router.
- Centralized management of devices using templates and policies.
- Application traffic steering over any link type, including less expensive broadband, and ensured reliability and performance.
- Direct access to SaaS, IaaS and cloud services, with performance, reliability and security.
- Enables organizations' transition to the cloud.

For more information see, https://sdwan.vmware.com/.

Join us online:

vmware®

VMware, Inc. 3401 Hillview Avenue Palo Alto CA 94304 USA Tel 877-486-9273 Fax 650-427-5001 www.vmware.com Item No: sdwan-904-dig-trans-healthcare-eb-0720 5/19