

Get High Performance for VMware Horizon Using VMware SD-WAN

vmware®

SD-WAN™

Key takeaway

When companies provide employees anytime, anywhere access to necessary applications, employees reported a 17% savings in time, ultimately freeing them to focus on more important tasks.

Digital workspace transformation needs WAN transformation

Enterprise organizations are accelerating their digital transformation as the modern workplace is evolving rapidly. Organizations are using best-of-breed applications from SaaS providers to manage business processes. Applications hosted in on-premises data centers are also moving to IaaS providers like Azure and AWS. The concept of a workplace perimeter is changing simultaneously, as employees require more flexibility in where they work and on which devices they work. Businesses are empowering employees to work from anywhere at any time, making a seamless user experience throughout the workday a non-negotiable requirement.

The digital workspace has emerged to address these evolving employee needs. It represents a fundamental shift in the way IT delivers end user services. In this model, IT delivers the apps and data employees need to work across any device, in any location. The digital workspace is made possible through an enterprise's transition to a software-defined infrastructure. Using cloud-based management technologies, digital workspace solutions deliver self-service, out of the box experiences that scale across platforms, locations, and device ownership models.

The benefits of moving to a digital workspace are well documented. A Forbes study found when companies provide employees anytime, anywhere access to necessary applications, employees reported a 17 percent savings in time, ultimately freeing them to focus on more important tasks, improving personal productivity and thus making their firm a more desirable place to work in the eyes of employees.¹

Studies confirm a significant return on investment (ROI) for application virtualization systems, with substantial time and cost savings, improved productivity, as well as benefits for both the business and IT. For example, a

¹ Forbes – Impact of Digital Workforce

“The four biggest challenges in adopting public cloud desktop as a service (DaaS) and application remoting as a service are cost (23.20%), trust (11.51%), creating a positive business case (11.34%) and performance (11.34%).”

VDI LIKE A PRO
END USER COMPUTING STATE OF THE
UNION - 2019

study by Forrester found that IT admins are expected to reduce work time required to deliver applications to users by 92 percent. Frontline support calls for security and management are expected to reduce 10 percent and tier 2 escalations by 46 percent.²

As part of the digital workspace, organizations are using virtualized applications and virtualized desktops to deliver applications more effectively to their employees. They are also using platforms to host and manage applications, such as VMware Workspace ONE. With virtualized delivery of applications, anytime and anywhere is the goal.

Supporting all applications—mobile, cloud-based, web-based, tasked-based, Windows legacy and so on—is a must. Making applications highly accessible is crucial in boosting employee performance and productivity. Employee experience is the heart of the digital workspace. IT must focus on providing an effective user experience across any device or location to ensure productivity does not suffer.

The digital workspace is delivered over the wide area network (WAN), which can impact performance due to congestion, limited bandwidth, poor security and a lack of visibility into conditions on the network. The question is, how do you deliver the best possible digital workspace to your employees without compromising on performance and security? The answer is VMware SD-WAN™.

How the WAN impacts performance for virtualized desktops

The benefits of application and desktop virtualization will be lost if poor application performance causes a poor user experience. This can happen when virtual applications and desktops are delivered across a WAN that suffers from limited bandwidth or poor connectivity performance.

VMware SD-WAN provides performance and reliability for virtualized applications and desktops by overcoming network impediments that affect the application performance across the WAN. VMware SD-WAN can overcome latency, packet loss, and bandwidth limitations that cause virtualized applications and desktops to perform poorly or become unreliable.

In the report “VDI Like a Pro—End User Computing State of the Union 2019” when asked what the biggest challenges were in adopting public cloud remote desktop and remote application services, respondents cited performance as one of the top four challenges. “The four biggest challenges in adopting public cloud desktop as a service (DaaS) and application remoting as a service are cost

² Forrester Total Economic Impact™ (TEI) Study: Workspace One Simplifies IT

(23.20 percent), trust (11.51 percent), creating a positive business case (11.34 percent) and performance (11.34 percent).”³

Issues with running virtual apps and desktops over the WAN

Network dependencies for VDI Blast Protocol

VMware Horizon Blast Protocol has a number of inherent capabilities to deliver an exceptional user experience, but it has no control over how the network handles protocol traffic in the presence of other traffic. For example, a virtual desktop infrastructure (VDI) client at a home office also has to deal with traffic such as Netflix, Xbox and web surfing. At branch locations the VDI clients have other traffic types that include voice, video, IoT and file transfer. Blast protocol’s ability to handle network issues requires IT admins to tune network parameters. This can increase operational complexity with large numbers of remote sites or with home users. The network type and network condition can significantly degrade the protocol performance and impact user productivity. For work at home users, there is a need to isolate office traffic from home traffic.

Network congestion

Packet loss is often a big contributor to poor performance of virtual applications and desktops over the WAN. Packet loss can occur on shared network infrastructures, such as MPLS links and IP VPNs, due to network congestion or out-of-order delivery, as packets are routed on different paths.

Research by VMware found that packet loss in traditional enterprise WANs varied up to 12.5 percent over 24 hours. The performance impact of packet loss is high: During a file transfer with 0.5 percent packet loss, TCP throughput drops from 10 Mbps to 1 Mbps. For real time traffic, the mean opinion score (MOS) drops from 4.5 to 2.5. (MOS scores range from 1 [unacceptable] to 5 [excellent].)

When loss occurs, packets must be retransmitted across the WAN, which can add considerable latency. For example, packet loss can turn a 200-millisecond round trip into a 1-second delay. To end users, the virtual application or desktop seems unresponsive when packets are lost and subsequently retransmitted. They start to hit the keys again on their client machine, which compounds the problem by sending even more data across an already congested WAN.

High latency

Some WAN links will have higher latency than others due to less optimal routing over more hops. There are also times when a low-latency path gets routed over longer physical network segments due to underlying infrastructure changes. It

³ VDI Like a Pro – End User Computing State of the Union 2019

Key takeaway

Packet loss impacts end user experience as the virtual application or desktop seems unresponsive.

Tests show that VMware SD-WAN can remediate packet loss nearing 15% on a single WAN link to deliver exceptional user experience for real-time applications like VDI.

is critical to detect link performance in real-time and steer traffic to the better performing links.

Insufficient bandwidth

WAN bandwidth limitations can negatively impact the performance of a virtual application or desktop. If WAN links cannot provide the bandwidth for a VDI environment, application performance will suffer and the user experience will be poor. Although virtualized applications are efficient with bandwidth, GPU-based engineering applications, high-definition videos, large file transfers and print jobs can consume significant WAN bandwidth. To compound matters, many branch and remote offices are linked to the data center and the cloud over low-bandwidth private lines. To address bandwidth constraint, organizations are looking for ways to utilize bandwidth-rich Internet while ensuring performance and security.

Network link failure

With virtualization, the connection between a branch office and the data center is essential for providing streamlined access to the application. If that connection is lost, productivity will suffer as access to the applications will end. Enterprises generally minimize this risk by using expensive private circuits such as MPLS, with service level agreements (SLAs), and often pay for backup connections. But MPLS connections can fail or degrade and SLAs don't cover the cost of downtime. During such failures traffic gets re-routed on a backup link, disrupting real time sessions and forcing a session reset, resulting in a poor user experience and calls to the support desk.

Improve VMware Horizon performance over the WAN

Organizations that use VMware Horizon services should be especially interested in VMware SD-WAN, because it provides significant benefits to virtualized applications and desktops.

In their report, "VDI and DaaS Demand the Enterprise Architects Rethink Their Network Architectures", Gartner says that "Customers deploying VDI and DaaS should consider deploying SD-WAN to increase useful capacity and resilience."⁴ Gartner specifically calls out the WAN as a key part in virtual application delivery, but it also matters to voice quality, video quality, and other applications. Real time applications such as voice, video and VDI are the ones that are most affected by WAN quality and require a low-latency, low-loss connection.

VMware Horizon is one of the 3,000+ applications that the VMware SD-WAN deep application recognition feature can recognize. It recognizes VMware Horizon traffic and applies a specific policy to it, such as priority, network service link steering, and service class. The benefit of this feature is that

⁴ VDI and DaaS Demand that Enterprise Architects Rethink Their Network Architectures

VMware SD-WAN can ensure always-on availability of the VMware Horizon application, for the best possible end user experience. It can also provide insights into the delivery of the application across the WAN, which will help with network visibility and troubleshooting.

A single-vendor approach using VMware SD-WAN with VMware Horizon delivers an exceptional user experience by improving performance and problem resolution through dynamic remediation. By using VMware SD-WAN with VMware Horizon, organizations can expect the following benefits:

- Reliable, secure and efficient access to the virtualized app/desktops delivered from the cloud or on-prem data center using optimization capabilities during failure or dim-outs on WAN links that include loss, latency and jitter, all done dynamically without any operator intervention.
- Rich user experience delivered by prioritizing real-time Horizon VDI client traffic over lower priority applications like web browsing, for highest quality user experience.
- Auto-selection of low latency and optimal path to connect Horizon clients to VDI applications in the cloud leveraging cloud hosted VMware edge points of presence (VMware Edge PoP™).
- Application-aware visibility to indicate an application's quality of experience delivered for a period of time at any site. This helps troubleshoot poor user experience at any remote location and analyze historical trends.
- Aggregate bandwidth consumption taking into account all available WAN links at branch sites to access virtualized applications and virtual desktops eliminating wasted bandwidth from active-standby WAN architectures.
- Secure segmentation of user traffic within SD-WAN enables VDI client and non-VDI clients from a branch location to access applications unique to their business such that application data are isolated from each other.
- Flexible security via a built-in firewall or using third party security services as a Virtual Network Function (VNF) on the SD-WAN Edge or directing applications to third-party security service in the cloud.

The VMware SD-WAN solution

VMware SD-WAN Edge

A VMware SD-WAN deployment starts with placing a VMware SD-WAN Edge device at each location, such as a branch or home office, on-prem data center and optionally in an organizations' IaaS cloud instance. The VMware SD-WAN Edge connects branch or home office sites to the WAN, the Internet, and applications hosted in data centers or in the cloud.

The VMware SD-WAN Edge devices work in conjunction with VMware Edge PoPs to optimize delivery of traffic between them. The SD-WAN Edge performs

policy enforcement using Dynamic Multipath Optimization™ (DMPO) to ensure consistent application traffic delivery. A VMware SD-WAN Edge automatically joins the SD-WAN fabric once powered on and connected to the internet. The SD-WAN Edge devices are auto-configured so they're quick and easy to install with no IT visits to the branch or home location.

VMware Edge Cloud Orchestrator

The VMware Edge Cloud Orchestrator is a secure and scalable web-based central management tool that provides simplified configuration, provisioning, monitoring, fault management, logging, and reporting. The Orchestrator also offers a single pane of glass for real time insights into network and application performance. It is used to set business policies for prioritization of applications on the network to make sure that the most important applications get the top priority. It pushes these policies to thousands of Edge devices with a single click.

VMware Edge PoPs

A key differentiator in the VMware SD-WAN solution are VMware Edge PoPs. These PoPs are highly available and hosted strategically at SaaS/IaaS locations such as Microsoft 365, Azure, AWS, Zoom and Salesforce. The proximity of SD-WAN Gateways, located worldwide, offer branch and home office users low-latency access to all cloud applications. This approach also avoids backhauling SaaS application traffic from the branch to a data center before routing to the cloud. The VMware Edge PoPs optimize DMPO traffic to the VMware SD-WAN Edge device in the branch office location for exceptional user experience to the cloud applications.

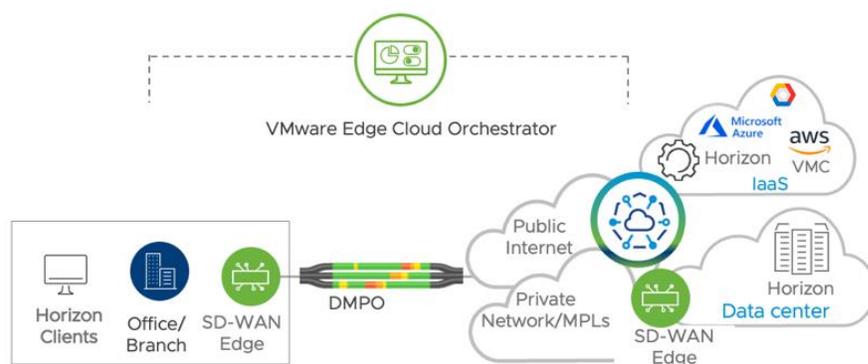


Figure 1: VMware SD-WAN with VMware Horizon VDI deployment

Benefits of using VMware SD-WAN with VMware Horizon

Assured performance

VMware SD-WAN is constantly monitoring the state of WAN links to ensure that a VDI session is always steered over a low latency path. VMware SD-WAN

classifies and prioritizes real-time applications like Horizon VDI over other applications during network congestion or dim-outs. Business policy is defined on the VMware Edge Cloud Orchestrator to handle Blast Protocol traffic as real-time with the traffic priority set to High as shown in Figure 2. This policy is automatically pushed to all the Edge devices at branch sites or home office soon after the Edge device is powered on. Pushing policies from the centralized Orchestrator ensures that the users at the SD-WAN Edges get the same consistent experience at different branch locations or at home without any IT visits to the remote sites.

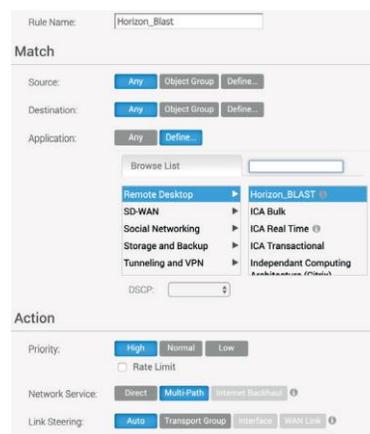


Figure 2: Business policy set in Orchestrator for VDI traffic

Self-healing

VMware SD-WAN performs dynamic remediation during dim-outs and connectivity loss on WAN links. The solution addresses packet loss with real time forward error correction (FEC). Each packet can be duplicated over two WAN links using FEC, with VMware SD-WAN Edge or Gateway at the far end ensuring proper packet order. FEC also works on single WAN link connectivity use cases such as work-from-home users. Remediation takes effect for both ends of SD-WAN, at the Edge and the Gateway.

In a test conducted with Horizon VDI hosted on Azure, home users with a single WAN link connectivity and accessing a 4K training video over the internet suffered from a choppy experience with a 5% packet loss on the legacy WAN infrastructure. The same content viewed by users on VMware SD-WAN infrastructure experienced choppiness in the video when the packet loss approaches 15% over the WAN infrastructure.

Similar observations were made with 1080p video where the quality suffered at 10% packet loss for legacy WAN when compared to the quality impact when the packet loss gets closer to 20%.

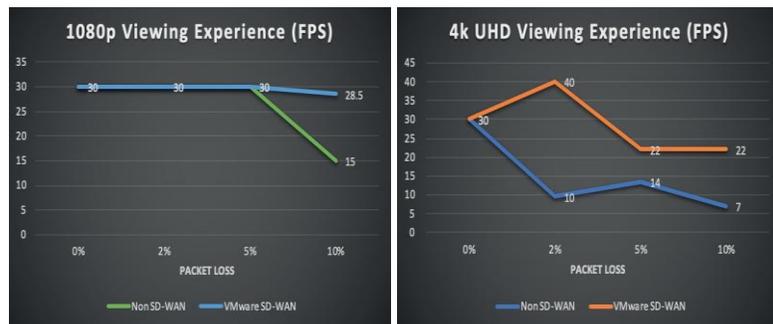


Figure 3: Better quality user experience during packet loss with VMware SD-WAN

The pronounced difference in user experience is due to the dynamic remediation capabilities of the VMware SD-WAN solution where the SD-WAN Edge is constantly checking link status, recognizing Blast Protocol traffic related to VDI sessions and sending FEC notifications to the SD-WAN Gateway. The Gateway applies FEC to ensure packets are replicated and sent towards the affected SD-WAN Edge.

The rate of replication goes up as the packet loss increases in real time and mid-flow while the user continues to experience good quality video reception. The Edge device reassembles the packet in the right order before it is sent to the VDI client. On the server side, Horizon VDI is relieved from the task of replicating packets and regains some cycles. The tests showed about three times the amount of packet replication is eliminated with the solution.

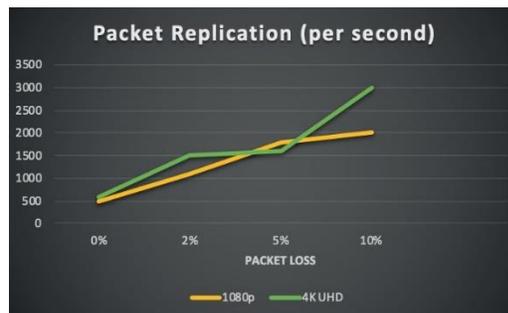


Figure 4: SD-WAN packet replication increases with packet loss

Path optimization

The advantages of path optimization offered by SD-WAN Gateways for SaaS applications can be seen from the following example. A Horizon pod deployed in the Azure cloud in the East US region have VDI clients accessing this pod from the west coast of San Francisco. The VDI client traffic is routed via the SD-WAN Gateway located at the peering point in the West region connecting to Microsoft's backbone and getting dropped at the cloud data center in the East region as seen in Figure 5. This capability to auto-detect the nearest entry point to the IaaS provider for shortest path to Horizon VDI is a major advantage for VDI clients.

The second example is for Zoom conferencing session. A Zoom thin client plugin installed on VDI clients helps break out Zoom traffic within VDI. This helps the VMware SD-WAN solution identify Zoom traffic, apply the optimization needed and ensure the traffic is routed via the Gateway closest to the Zoom tenant instead of carrying the traffic back to the Horizon pod before it is routed to Zoom, avoiding backhaul and a sub-optimal user experience.

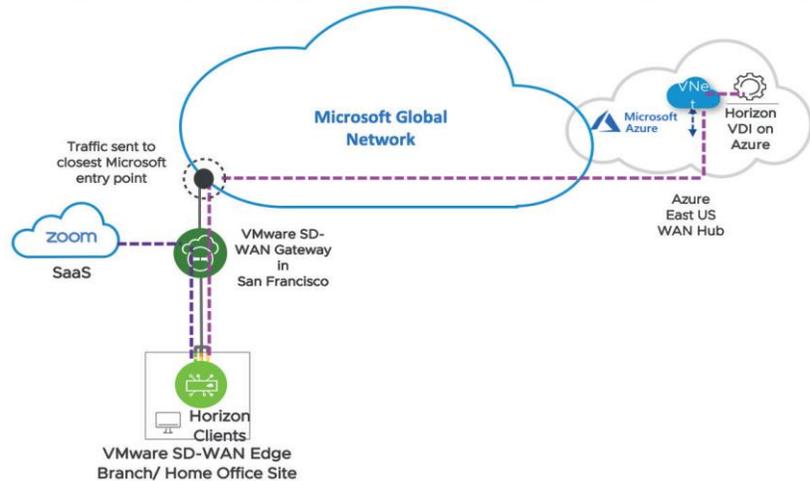


Figure 5: SD-WAN path optimization for Horizon VDI on Azure and Zoom traffic

Simplified operations

VMware SD-WAN provides visibility to application performance, which will help with setting policies and troubleshooting application delivery issues. A major benefit of the VMware SD-WAN architecture is global visibility into network performance and issues. The VMware Edge Cloud Orchestrator makes it easy to monitor devices and the performance of applications on the network. The application monitoring features in the Orchestrator ease the task of troubleshooting issues and can prevent poor application performance and application downtime. Using the Orchestrator, you can view overall health of a remote site, quickly assess link quality, and drill down on application usage to see what applications are using your bandwidth.

Intrinsic security

VMware SD-WAN provides security via its built-in firewall, third-party NGFW options, and policy-based traffic steering. For a smaller location, you can use the built-in firewall on the VMware SD-WAN Edge device. For midsize locations, the VMware SD-WAN Edge device provides a hosting capability to run an NGFW from 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 (VNF) infrastructure. Policy-based traffic steering can also be used to send traffic to security services that are hosted in the cloud.

Learn more

- VMware SD-WAN, sase.vmware.com/sd-wan
- VMware SASE, sase.vmware.com
- VMware Horizon, www.vmware.com/products/horizon

VMware SD-WAN with VMware Horizon on public cloud

Organizations are looking at cloud-only, multi-cloud or hybrid cloud solutions to rapidly scale VMware Horizon desktops and applications. Many organizations are doing this with VMware Cloud on AWS or Horizon Cloud on Azure.

While there are many benefits of hosting VMware Horizon in the cloud, it is important to transform the rigid WAN infrastructure to simplify operations. VMware SD-WAN accelerates this transformation and offers multiple on-ramp options to connect VDI clients to virtual desktops and applications in the cloud and in the data center.

One option is to use the VMware SD-WAN Gateways to connect to IaaS and SaaS Providers worldwide. This option helps you take advantage of the DMPO tunnel from the Edge to the Gateway. Another option is to deploy a VMware SD-WAN virtual Edge instance on AWS and Azure. The virtual Edge software is available on the AWS and Azure marketplaces. The virtual Edge helps customers extend DMPO into the public cloud and apply business policies to handle VDI Blast Protocol traffic from the virtual Edge to all branches.

Better virtual apps and desktops for healthcare providers

Clinicians are increasingly turning to VDI, such as VMware Horizon, to 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).

Healthcare applications require high levels of bandwidth, which is often not available in most clinics or branch offices. Patient files and records are now in digital formats, EMRs and electronic health records (EHRs), and organizations increasingly use cloud-based storage and application delivery to give care providers constant access to applications and data.

VMware SD-WAN can help with the ability to bond multiple links to act as one and steer traffic over the best available link, as well as reserve bandwidth based on application policies. With the ability to use any link type, adding bandwidth to remote sites is much easier.

VMware SD-WAN accelerates cloud adoption of virtual app and desktop

Using desktop virtualization systems like VMware Horizon provides cost savings, control and security benefits compared to running applications locally on the client. However, performance over the WAN can be a limitation. VMware SD-WAN can overcome these limitations by ensuring bandwidth availability and mitigating congestion, while providing security over the WAN.