VMware Secure Access

Secure, optimized and high-performance access for remote and mobile users

velocloud™
Now part of VMware

As enterprises move their business-critical applications to the cloud and their users become increasingly mobile, the traditional remote access model of deploying VPN concentrators at enterprise data centers is no longer efficient. In this model, remote and mobile user traffic has to traverse across the Internet to the data center before that traffic is subsequently sent back out to the Internet, introducing additional latency and negatively impacting the user experience. As employers adapt to a world in which a large majority of their employees are working outside of the office accessing all applications (on-premises, virtual, or SaaS), the traditional security models of protecting the network perimeter will become obsolete. Providing exceptional, secure user experiences and maintaining the supporting infrastructure for solving these problems requires resources, expertise, ongoing maintenance, and is often costly.

VMware solutions for a distributed workforce

VMware Workspace ONE allows enterprises to implement zero trust security models allowing only trusted devices and users to access applications hosted anywhere (on-premises or in the cloud). Each user is mapped to a per-application policy for both data center and SaaS/IaaS applications, regardless of whether the user is inside or outside the office, allowing IT personnel to maintain a single set of policies per user, reducing operating costs.

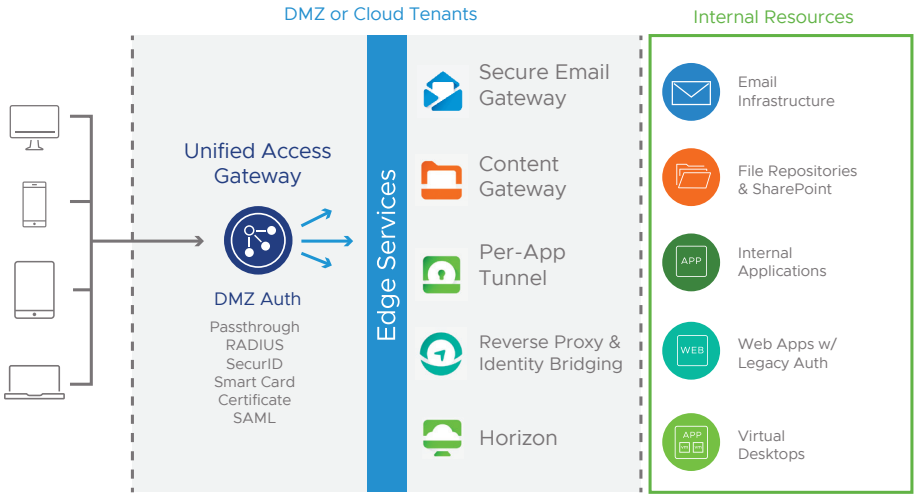

FIGURE 1: Workspace ONE architecture

vmware®

KEY TAKEAWAYS

- Bringing remote users into VMware SD-WAN fabric for a better and consistent experience
- Workspace One Tunnel Unifed Access Gateway (UAG) as-a-service for scalability and cost savings over legacy VPNs
- Cloud-hosted service simplifies Day 2 operations while ensuring consistent policy enforcement

VMware SD-WAN™ by VeloCloud® provides users inside the office with consistent, secure cloud application access across the Internet by optimizing applications through a network of VMware SD-WAN Gateways. Regardless of where the enterprise applications are hosted, either in the enterprise data center or in the IaaS/SaaS cloud, the user experience is greatly improved when accessing these applications through the Gateways.

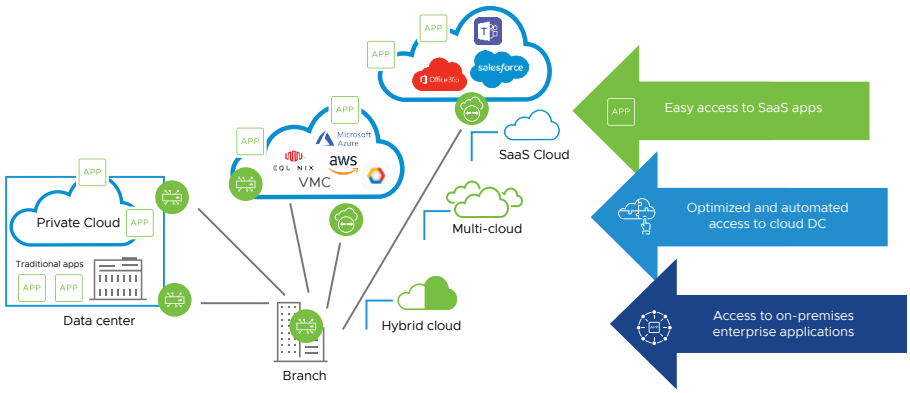

FIGURE 2: VMware SD-WAN architecture

The VMware Secure Access combines VMware Workspace ONE and VMware SD-WAN, bringing off-premises (remote and mobile) users into the enterprise VMware SD-WAN fabric. This enables all users to access cloud and data center hosted applications through a network of worldwide service nodes. Users can access these cloud resources without added latency and hairpinning, leveraging the security and benefits of a cloud-hosted solution, while easing IT deployment and maintenance of costly remote access services.

Challenges facing today's remote access solutions

Remote and mobile users today have a different experience accessing corporate applications compared to users inside a branch office. Traditional security models, including VPN, have employed the inside/outside trust model. In this model, once the remote user gets access to the network, that user can access any resource, including cloud applications that are outside the network. Enterprise IT has been deploying the Workspace ONE solution to replace VPN and implement Zero Trust security models to help address digital business transformation of any user accessing any application from anywhere.

For VPN deployments, a VPN concentrator is usually deployed inside an enterprise data center. The VPN concentrator terminates a mobile or remote user connection and directs all session traffic to the data center, regardless of the destination. With most of the applications moving out of the data center and into the cloud, VPN traffic is sent back out to the Internet and to a SaaS/IaaS, causing traffic hairpinning. This approach makes communication between the VPN endpoint and application server take a much longer path through the data center. The VPN traffic takes on additional latency and has to compete with other applications for data center Internet bandwidth, causing a poor user experience and lost productivity. SD-WAN network transformation and remote access integration address these new application traffic trends and work to reduce hairpinning, which has been a major challenge of VPN designs.

Using unified access gateways

Workspace One Unified Access Gateway (UAG) is used to easily secure and manage access to an organization's applications for all types of users and is often deployed in the demilitarized zone (DMZ) inside a data center. Enterprises need to install UAGs at multiple locations worldwide to provide mobile and remote users with access points closest to where the users are. In this way, traffic doesn't have to backhaul across the country or across continents, negatively impacting the user experience. Establishing a hosting presence to deploy UAGs in multiple regions is not trivial. Customers have to acquire a hosting presence in that region, deploy their own networking, compute, bandwidth and purchase maintenance contracts. All of this requires time, resources and expertise and increases costs for these enterprises.

VMware Secure Access

The VMware Secure Access provides Workspace ONE users with consistent, optimal and secure cloud application access through a network of worldwide service nodes. The solution brings together the best of both worlds: VMware SD-WAN and Workspace ONE are combined into a single, cloud hosted offer that ensures a consistent application experience for both remote/mobile and office users.

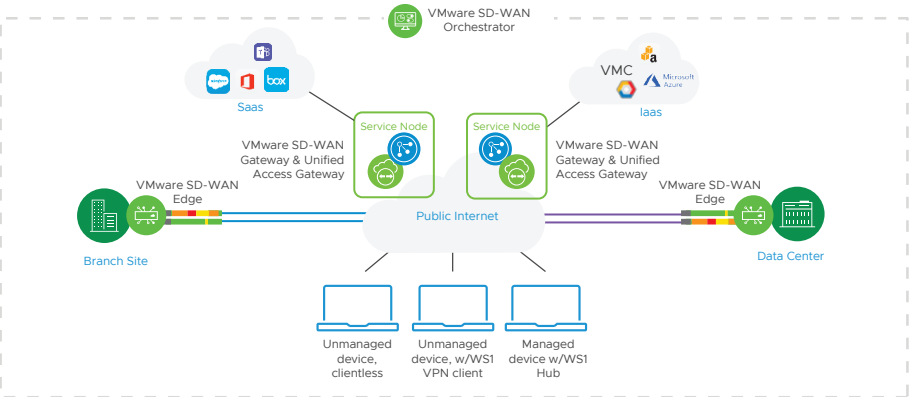

FIGURE 3: VMware Secure Access brings together SD-WAN and Workspace ONE for mobile users

Bringing off-premises users into SD-WAN fabric

VMware SD-WAN users today have access to a network of thousands of VMware SD-WAN Gateways deployed in more than 100 points of presence (POPs) worldwide. User traffic from branch offices is handed to the closest Gateway, to be routed to the application server hosted in either the enterprise data center, IaaS or SaaS cloud. Because the Gateways are deployed inside the same data center that hosts IaaS/SaaS, the destinations are milliseconds away from the Gateways, enabling a smooth application experience. If the traffic is destined for the data center, users' traffic is optimized by VMware SD-WAN Dynamic Multipath Optimization™ (DMPO), which can mitigate network issues such as latency, jitter and packet drops.

By hosting the UAG service in the same VMware POPs, remote and mobile users also have access to the same infrastructure as users in the branch offices. Remote users are connected to the closest service node, and the Gateway will send SaaS/IaaS/Internet traffic directly to their destination without the need for backhauling to the data center, while only data center traffic will be optimized by DMPO and sent there.

Because of this efficient architecture, application performance is greatly improved. With no additional latency, enterprises can save on the cost of additional bandwidth purchase in the data center because there is no need for backhauling. Lastly, traffic destined for the Internet never enters the enterprise's network, protecting the network from attacks and protecting user privacy within the enterprise.

Supports multi-region with distributed VMware Service Nodes

Remote workers who are not from the same region as the enterprise headquarters know full well that finding a VPN concentrator closest to the users' location is challenging. Enterprises often do not have the resources to deploy VPN concentrators across the world for employees' remote and mobile access. As a result, both remote and mobile workers find it challenging to connect to a concentrator across the country, and often, across continents, in order to access the applications needed. User experience is adversely impacted, and productivity will suffer due to added latency, extra hops and additional packet drops the users have to go through by not having a VPN concentrator close by.

VMware Secure Access supports multiple regions through its distributed Service Nodes. The solution is available in the US, Europe and Asia, with additional coverage in later phases.

Managed UAG-as-a-service

The VMware Secure Access is offered as-a-Service, with the built-in ability to scale up or down based on the enterprise's needs to support user demand and consumption. IT administrators no longer have to worry about deploying additional UAGs for availability and resiliency when the remote access demand arises, nor do they have to worry about deploying, monitoring and maintaining these UAGs.

Works with all types of infrastructure

Enterprises without existing VMware SD-WAN infrastructure today can also benefit from the VMware Secure Access. Managed UAG as-a-service allows customers to have a multi-region presence with distributed VMware Service Nodes, solving the hairpinning for SaaS/IaaS and Internet traffic problems and enhancing the remote and mobile user experience.

For more information about VMware SD-WAN, visit *www.velocloud.com*.