

## SOLUTION BRIEF

# Netskope with VMware SD-WAN

Netskope with VMware SD-WAN enables optimized, scalable, and reliable connectivity along with data and threat protection for users accessing from anywhere.

### KEY USE CASES

- **Elastic, reliable connectivity to cloud applications:** With a cloud-delivered software-as-a-service (SaaS) approach, the solution provides optimized application and data delivery for any user and location.
- **Security without compromising performance:** Global cloud infrastructure enables real-time inline security defenses at scale, including secure web gateway (SWG), cloud access security broker (CASB), data loss prevention (DLP), Zero Trust Network Access (ZTNA), and more.
- **Perform investigations with detailed audit trails:** The combination of network and security services delivered as SaaS supports the rapid growth of users, applications, and data in the cloud.
- **Secure access service edge (SASE):** The combined solution enables a SASE architecture based on integrated best-of-breed SD-WAN and cloud-delivered security services.

### THE CHALLENGE

Enterprises are going through a digital transformation. Organizations are increasingly using new applications to manage business processes. These applications are hosted in more locations—not just in the corporate data center—but in multiple clouds. Additionally, the concept of a workplace perimeter is changing, as employees require more flexibility in where they work and on which devices they work. In addition to the need for reliable, high-performance connectivity, enterprises are also concerned with how to safely enable cloud and web applications across a rapidly growing and increasingly diverse set of users to protect these users and valuable data.

### NETSKOPE WITH VMWARE SD-WAN

VMware SD-WAN™ by VeloCloud® integrates with Netskope security to provide organizations with comprehensive cloud-enabled security in addition to optimized connectivity. VMware SD-WAN delivers high-performance, reliable branch access to cloud services, private data centers, and SaaS-based enterprise applications, while Netskope provides the complementary security services, such as a next-generation SWG, CASB with both API-enabled and inline protections, and DLP to supply advanced data and threat protection for users, applications, and data.

## CAPABILITIES

### SD-WAN FOR OPTIMAL BRANCH CONNECTIVITY

To support a cloud transition and deliver a quality user experience, enterprise network architects are re-evaluating the design of their WAN architectures by adopting SD-WAN to find ways to route internet traffic locally and take advantage of inexpensive broadband internet services. SD-WAN architectures address availability, performance, and cost challenges by dynamically utilizing multiple available connections (e.g., MPLS, broadband, LTE) to find the optimal delivery path for traffic across the entire network, shaping the bandwidth as needed to eliminate jitter and packet loss.

Using a lightweight IT footprint at branch offices, SD-WAN simplifies business connectivity by not requiring IT operations staff to configure and maintain complicated appliances at the branch. The cloud-delivered VMware SD-WAN with Dynamic Multi-Path Optimization (DMPO)

**VMware and Netskope offer organizations a high-performance, scalable, and secure environment to protect users and data inside and outside the traditional corporate perimeter.**

as its unique feature decides how traffic is steered on a per packet basis and performs real-time monitoring and remediation without the complexity and efforts of MPLS. VMware SD-WAN can identify and prioritize traffic among over 3,000 applications and with a distributed network of cloud gateways, offer closest on-ramp access to leading cloud service providers such as the Netskope security cloud.

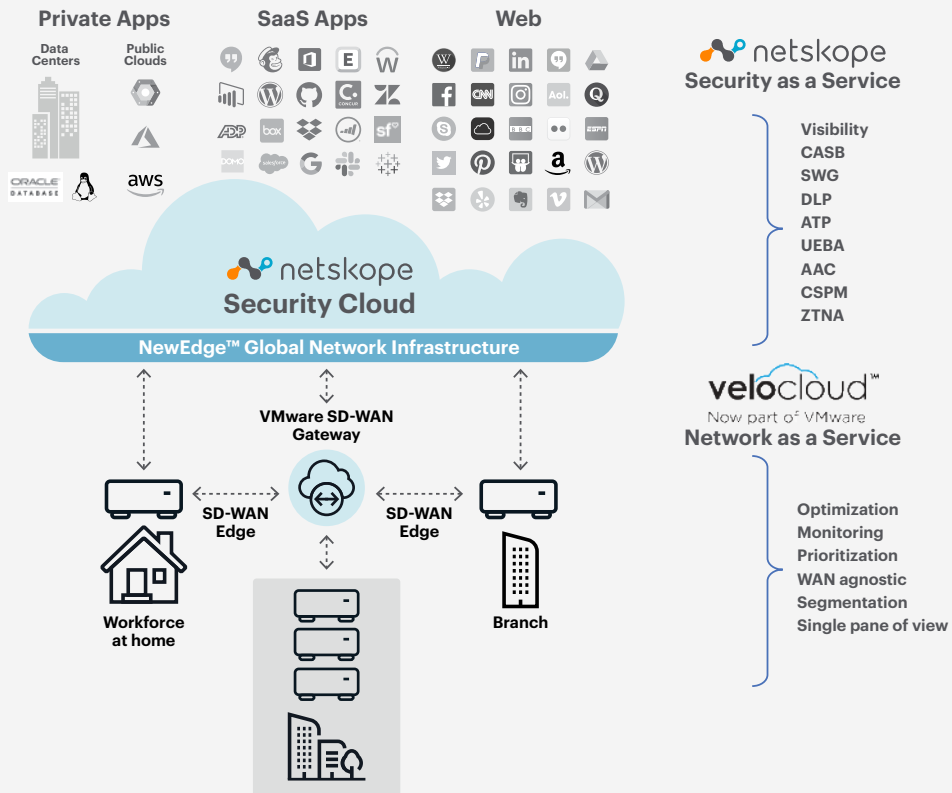


FIGURE 1: Netskope security cloud integration with VMware SD-WAN by VeloCloud.

## **COMPLEMENT THE NETWORK: THE NEED FOR SECURITY SERVICES**

In parallel to the need for reliable and optimized branch to HQ connectivity, enterprises also are challenged with how to safely enable cloud and web applications across an increasingly remote workforce. SaaS applications like Google G Suite, Office 365, Salesforce, Workday, Slack, and Zoom, combined with IaaS/public cloud services in AWS, Azure, and Google Cloud now make up the majority of network traffic rather than traditional web traffic. As users, applications, devices, and data are now in the cloud and outside of a traditional network perimeter, it's essential to protect these users and data no matter the device or location. Because legacy Next Gen Firewalls (NGFWs), secure web gateways (SWG), and cloud access security brokers (CASBs) are blind to the majority of this inline cloud traffic and cannot decode the API/JSON based communications that are the norm for cloud and web today, they put organizations at increased risk.

Collectively, VMware and Netskope fulfill and support the SASE design philosophy in which cloud-delivered network optimization services are combined with cloud-native security controls to offer organizations a highly scalable, optimized, and secure environment that protects users and data inside and outside the traditional corporate perimeter, no matter where they are.

## **SECURE WAN ACCESS WITH VMWARE AND NETSKOPE**

VMware SD-WAN Edges can be deployed as a physical appliance or a virtual machine at the customer site. These devices communicate via secure IPSec or encapsulated GRE traffic to the Netskope security cloud. When accessing public clouds like AWS or Azure, or SaaS applications like Office 365, the VMware SD-WAN Gateways hand off traffic to the Netskope security cloud, whereby granular security controls, plus advanced data and threat protection are applied. More specifically, this extends users' virtual access to the NewEdge global network infrastructure, which serves as the network foundation for the Netskope security cloud and provides high-capacity and low-latency access to cloud apps and websites for an optimized user experience.

VMware SD-WAN is built on three components:

- The VMware SD-WAN Edge sits at your branch office locations. It provides WAN connectivity and applies application policies to ensure application performance over the WAN link(s).
- The VMware SD-WAN Orchestrator is a cloud-hosted centralized management system. You don't have to install it—you just connect to it. VMware SD-WAN Edge devices are configured, monitored, and managed by the VMware SD-WAN Orchestrator.
- VMware SD-WAN Gateways are hosted in PoPs around the world. Traffic is sent to the VMware SD-WAN Gateways, which then hand off traffic to the closest application tenant location, which might be your data center or a cloud provider, like AWS or Azure.

## **NETSKOPE SECURITY CLOUD FOR COMPREHENSIVE SECURITY**

Based on application requirements, admins can choose to direct traffic to exit via VMware SD-WAN Gateways or via the Netskope security cloud before handing off the traffic to the application tenant location. Remote users outside of the VMware SD-WAN environment can connect directly to the Netskope security cloud via encrypted SSL/TLS communications whereby the aforementioned security controls are applied. Netskope and VMware tightly integrate security and SD-WAN features delivering network optimization services (e.g., acceleration, QoS, dejitter) along with cloud-native, converged single-pass security controls (e.g., CASB, SWG, DLP, ZTNA).

Remote workers using corporate or managed devices can use the lightweight Netskope client, which provides several key functions: it steers all traffic to the Netskope cloud, delivers consistent notifications to end users for coaching and guidance purposes when they violate a policy, and can provide the identity of the user with no additional setup needed by the

customer. Those remote workers in branch offices or using their own personal or unmanaged devices, such as in organizations supporting bring your own device (BYOD), would be directed to the Netskope security cloud via its reverse proxy functionality and the security controls would subsequently be applied. Also, Netskope can work with identity providers to forward traffic to Netskope for application access when the remote worker will not or cannot install the Netskope client.

## **ABOUT VELOCLOUD, NOW PART OF VMWARE**

VeloCloud, now part of VMware, simplifies branch WAN networking by automating deployment and improving performance over private, broadband Internet and LTE links for today's increasingly distributed enterprises. VMware SD-WAN by VeloCloud includes: a choice of public, private or hybrid cloud network for enterprise-grade connection to cloud and enterprise applications; branch office enterprise appliances and optional data center appliances; software-defined control and automation; and virtual services delivery. For more information, visit [www.velocloud.com](http://www.velocloud.com).



The Netskope security cloud provides unrivaled visibility and real-time data and threat protection when accessing cloud services, websites, and private apps from anywhere, on any device. Only Netskope understands the cloud and takes a data-centric approach that empowers security teams with the right balance of protection and speed they need to secure their digital transformation journey. Reimagine your perimeter with Netskope.