Cloud Infrastructure

VMware SD-WAN by VeloCloud provides services for reliability, resiliency, and security

velocloud™
Now part of VMware

"VMware SD-WAN incorporates a distributed network of service gateways and VMware SD-WAN Orchestrators deployed at top-tier cloud data centers around the world, providing scalability, redundancy, and on-demand flexibility."

DANIEL SIMMS
HEAD OF IT OPERATIONS
ADDLESHAW GODDARD

SD-WAN and cloud networking technologies simplify branch office orchestration and connectivity. VMware SD-WAN™ by VeloCloud® is a cloud-delivered solution that is easy to deploy and manage. WIth VMware you can implement a flexible business-class WAN to every branch office with SD-WAN technology and cloud-delivered WAN services, including traffic steering, path selection, zero-touch deployment, single-point orchestration, business and security policy setting, and cloud-VPN. The VMware SD-WAN Gateway by VeloCloud and the VMware SD-WAN Orchestrator by VeloCloud enable optimized data paths for all applications, branches, and data centers, along with the ability to deliver network services from the cloud. Eliminate data center backhaul penalties with a cloud-ready network to provide an efficient, direct path to public and private enterprise clouds. Enterprises get unmatched flexibility to decide which services to deploy and manage, and when to upgrade and adhere to network operation policies.

VMware SD-WAN was built for reliability, resiliency and security. Here are some of the capabilities and specifications of the VMware cloud-delivered SD-WAN solution.

Availability and uptime

- 99.99 percent uptime service-level agreement, with 24x7 automated failure detection
- Global infrastructure of data centers for optimal selection and redundancy
- VMware SD-WAN Orchestrator is not in the data path nor required for ongoing flow control
- Management continuity is provided with failover VMware SD-WAN Orchestrators and regular backups
- Active-active VMware SD-WAN Gateways provide sub-second resiliency for VPN traffic
- Software-as-a-service (SaaS) traffic can also failover to bypass gateways
- Scheduled maintenance windows are advertised 72 hours in advance, and VMware SD-WAN Edge by VeloCloud upgrade windows are deferrable with times requested by the account holder
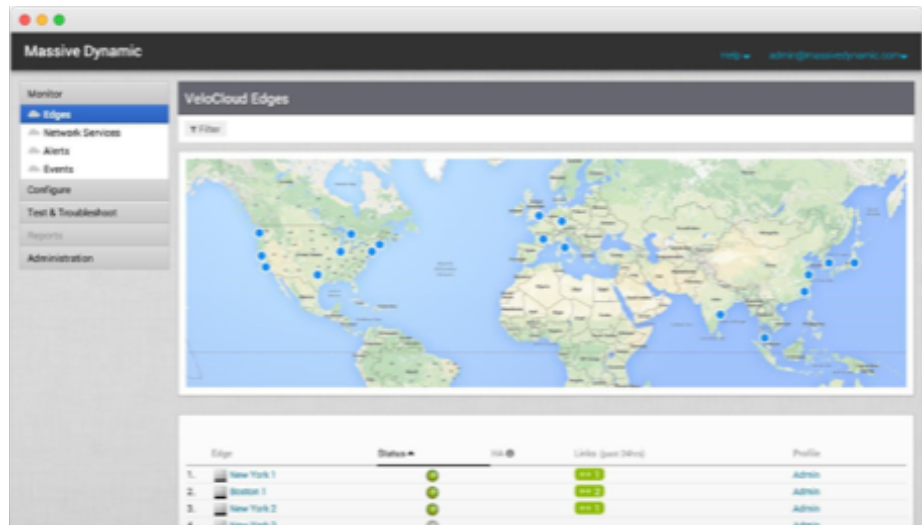- Cloud connectivity does not impact customer network operations

vmware®

FIGURE 1: Geographically separated VMware SD-WAN Edges.

Cloud data centers

• Co-located in Tier IV SSAE 16 Type II certified data centers

• ISAE 3402 (SAS 70/SSAE 16 replacement) certified facilities and providers deliver reliable failover design to ensure uninterrupted service in the event of a catastrophe

• Multiple providers and multiple locations service each data center

• Each data center meets the requirements of international privacy controls and is compliant with European safe harbor type policies

Redundancy and disaster recovery

• Replicates customer network data (system and configuration data) across multiple data centers with regular backups

• Provides well-documented, rapid-response operation teams across multiple locations

• Services all data centers with multiple top-tier carriers

• Provides rapid failover to the backup system in the event of hardware failure or an external factor

Robust physical infrastructure

• Controlled physical access with onsite 24x7 security, CCTV coverage, and biometric access controls with mantraps

• N+1 uninterruptible power supply (UPS) system with a minimum of 5 minutes of reserve power at full data center load; N+1 redundant generators with onsite fuel for a minimum of 36 hours

• Blended transit with a minimum of 10Gbps capacity, and facilities are selected to be near or at IX locations with dense participation

• Precision cooling system providing temperature, airflow, and humidity controls

• Early fire detection with isolated and fast suppression response

Network infrastructure and security

- Secure account separation for multitenant VMware SD-WAN Controllers and VMware SD-WAN Gateways

- Strong firewall policies to deny access for malicious traffic from public networks

- Proactive monitoring, regular vulnerability scans, and penetration tests performed by a reputable service provider, and automated notifications

- Management network communications protected by industry-standard encryption algorithms and security protocols

- Multifactor authentication for administrative remote access

- Configuration change monitoring and access audits for production network

Account protection and privacy

- Accounts are password protected and accessed via Transport Layer Security (TLS)

- Granular user, role-based access controls and policy framework help to manage third-party access

- Monitoring and incident response procedures are provided in all locations with 24x7 standby teams

- No data traffic is captured or stored unless enabled by the customer with the packet capture feature

- User and host machine information is only available to administrators selected by the account holder

A better WAN solution

The WAN is in transition as enterprises seek to improve agility and economics, and adapt to the shift of applications to the cloud. VMware SD-WAN offers a cloud-delivered solution for enterprise-grade performance, security, visibility, and control over both public Internet and private networks. VMware dramatically simplifies the WAN with zero-touch deployment, one-click business policy and services insertion, and cloud-based network as a service. The result is a better performing WAN with increased reliability and lower cost of ownership.

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