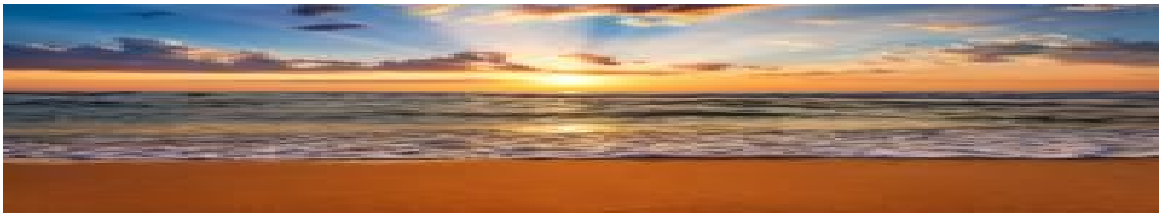

VMware VeloCloud's Cloud Delivered SD-WAN was one of the first SD-WAN offerings and the earliest proponents of delivering SD-WAN from the cloud. VeloCloud virtual or physical appliances connect company locations with broadband Internet access or MPLS into a virtual overlay. Cloud offerings are available for bringing private clouds, specifically AWS, and SaaS applications, such as Office 365, into the overlay.

nlike other OTT vendors, however, VeloCloud also maintains a global network of PoPs (points of presence). Within region, SD-WAN nodes connect to one another through those PoPs. Between regions, SD-WAN traffic would need to travel via the company's own MPLS service or the Internet.

Description

VeloCloud's solution is made up of four basic components: the gateway, the edge, the orchestrator and the controller.

VeloCloud's collection of service gateways deliver network services from the cloud and provide optimized data paths from the underlying transport system to data centers, branches, and web applications.

The edge component is an enterprise-class zero-touch appliance which provides connectivity to applications, performs QoS, and hosts VNF services.

VeloCloud's orchestrator centralizes enterprise-wide SD-WAN installation, monitoring, and configuration, and orchestrates the network's data flow.

Skilled-Nursing Company Taps Fortinet's Secure SD-Branch for Converged Networking and Security

"If I log into a FortiGate, it will notify me if there are updates available for our switches and access points as well. We can use FortiManager to push out patches and updates to all our buildings from a central location. Having that centralized management is a key reason to go with Fortinet."

Diversicare operates 61 skilled nursing centers across the United States. Making sure core systems are highly reliable and patient information remains secure is critical. Its network and security solutions landscape, however, involved too many vendors and was too complex to manage. When a wireless LAN project involving Fortinet deployed to improve connectivity for Internet of Medical Things (IoMT) devices, staff application use, and patient and visitor use, that quickly expanded into a consolidation of the organization's security and networking solutions.

Fortinet partner Liquid Networx deployed a software-defined branch (SD-Branch) solution offering single pane of glass visibility and management across Fortinet Secure SD-WAN (software-defined wide-area network) and Forti Switch and Fortas (access point) devices at the LAN edge. FortiNAC further added network access control capabilities. Divers care benefits from seamless integration and unified management of the solution driven by FortiManager and FortiAnalyzer. Configuration changes, compliance, and scaling to new locations are all executed more effectively and efficiently. Ultimately, better and more secure connectivity benefits patients.

Read about Diversicare's networking and security infrastructure transformation via Fortinet SD-Branch in this case study.

Business Impact

Defense

Improved security for patient information and other vital data, as next-generation firewalls (NGFWs) leverage real-time security services to prevent known and unknown threats from entering the corporate network

Compliance

Strengthened compliance with federal regulations around patient care and data security

Connectivity

Functional and secure software-defined wide-area networking (SD-WAN) connectivity

Time

40% reduction each week in staff time spent managing network and security infrastructure

Platform support

Improved ability of IT staff to fill in for one another when needed

Scalable

Streamlined corporate expansion through easier rollout of standard technologies to new skilled-nursing centers