

Connect and Secure the Distributed Edge with VMware SD-WAN



SD-WAN™

VMware SD-WAN brings compute and networking together for enterprise application transformation while delivering security and ubiquitous access for the distributed workforce.

Organizations are re-evaluating their network and security strategy as they increase adoption of cloud infrastructure and services, remote work, and new business applications at edge locations. These transformational trends bring opportunities but also challenges for legacy network infrastructures.

Legacy solutions send traffic to central data centers for routing and security checks before passing it on to cloud providers. This increases latency and frustrates users who are now working everywhere—branch offices, homes, airports, and cafes.

An entire new set of business applications is emerging to convert local intelligence gathered from IoT and other edge devices into smarter decisions and new customer experiences. These applications use local compute and require fast, reliable, and self-healing connectivity to the cloud.

A distributed cloud-based architecture is needed to deliver dispersed applications securely and reliably to users everywhere with speed.

VMware SD-WAN cloud-based architecture

VMware SD-WAN™ is architected based on the concept that “the cloud is the network.” VMware and its partners have over 200 PoPs around the world to put branches and users within milliseconds of major cloud infrastructure and SaaS providers.

Ensuring a reliable user experience requires understanding the network and adapting to network issues in real time. Beyond simple error correction, Dynamic Multipath Optimization™ (DMPO) ensures high bandwidth, reliable connectivity, and lower latency for business-critical application traffic.

Network operations are simplified with smart defaults and artificial intelligence. VMware Edge Network Intelligence™ (included in most SD-WAN editions) can help companies take remedial action to resolve network issues, greatly reducing operational time and effort.

Cloud and SaaS access

VMware SD-WAN includes thousands of gateways deployed at cloud provider on-ramps for maximum performance. It supports a wide range of services including AWS Cloud WAN, Azure Virtual WAN, and Google Cloud Network Connectivity Center.

Remote and hybrid workers

In addition to providing secure, reliable, and optimal connectivity for branch locations, VMware SD-WAN also extends these capabilities to the remote user through a unique client solution for endpoints and mobile devices and incorporates AIOps to provide a self-healing network.

Business applications at the edge

VMware SD-WAN is integrated with VMware Edge Compute Stack, a full-featured integrated IT and OT edge platform, offering the flexibility and consistency to operate current and future modern, edge-native applications on containers at the edge of your network.

Hardened security

VMware has engineered the cloud-delivered solution to meet the strictest security standards. VMware SD-WAN is certified for SOC2 Type 2 and ICSA, and is the only FedRAMP High certified SD-WAN solution. It allows customizable security policies across the network and protects, prioritizes, and isolates traffic via zero trust end-to-end segmentation. With hardened security built-in, our customers can feel confident about the integrity of VMware SD-WAN to secure their networks.

Secure remote access for branches and workers anywhere

Multiple access options fit your organization's connectivity needs and support your zero-trust journey. VMware SD-WAN Edge appliances deployed at branches or at homes provide optimized connectivity and secure VPN. The new VMware SD-WAN Client supports users anywhere on laptops or mobiles with remote access that offers better security and ease of use than traditional VPN solutions.

For organizations that also need a unified endpoint management solution or are further along on a zero-trust implementation, VMware Secure Access™ provides extensive device and user posture management as part of a zero-trust network access (ZTNA) solution.

Flexible VMware SASE architecture

SD-WAN is crucial to deliver applications and security to dispersed branches and users in a secure access service edge (SASE) framework. VMware provides flexibility and choice of cloud security controls through VMware or third parties. VMware SASE™ offers cloud security services that include secure remote access, cloud access security broker (CASB), secure web gateway, or available deep integrations with major third-party security providers.

Learn more

- VMware SD-WAN, sase.vmware.com/sd-wan
- VMware SASE, sase.vmware.com
- VMware Secure Access, sase.vmware.com/products/vmware-secure-access
- VMware Cloud Web Security, sase.vmware.com/products/cloud-web-security
- VMware Edge Network Intelligence, sase.vmware.com/products/edge-network-intelligence



Figure 1: VMware SD-WAN securely connects users anywhere to applications anywhere and is a crucial part of a SASE framework.

Do more with VMware SD-WAN

VMware SD-WAN helps transform your business to embrace the advantages of the cloud, hybrid work, and new edge applications.

- **Ready for multi-cloud:** Connect users and branches securely to the cloud, through the cloud, and with the cloud without consuming data center resources
- **Work anywhere:** Empower enterprise employees to work remotely, securely, easily, and productively from any device, anywhere
- **Take on new use cases:** Embrace new applications at the edge with an SD-WAN platform designed for digital transformation
- **Integrated AIOps:** Reduce operational complexity by harnessing the power of AIOps to rapidly identify root causes and remedial actions associated with poor application performance
- **Flexibility and choice:** VMware SD-WAN supports many popular secure service edge (SSE) providers and virtual network function (VNF) applications, allowing you to choose how and when you will transition to SASE