

VMware SD-WAN and SSE Integrations

vmware®

SD-WAN™

At VMware, our focus on customer success means not only building great solutions for our customers, but also ensuring that our solutions add value to a customer's existing environment. This approach is very helpful for enterprises that are in the middle of digital transformation that affects every aspect of their network infrastructure. Applications are now spread across data centers, cloud, SaaS, and the edge, and end users are everywhere. IT teams are burdened with the difficult task of managing all these moving parts. Networking and security are moving to cloud-delivered services that align with distributed applications and users—a key part of this transformation.

To address these changes, the industry has responded with a architecture called Secure Access Service Edge (SASE) that is comprised of SD-WAN and Secure Service Edge (SSE).

VMware has responded to this emerging industry architecture by delivering a complete SASE solution that provides cloud delivered networking for branch and remote site connectivity based on Zero Trust, cloud-delivered security to protect users and infrastructure against external threats, and integrated AIOps to simplify Day 2 operations for IT teams. The return on investment and the benefits of this comprehensive VMware SASE™ solution is evident in a recent Forrester Total Economic Impact report that shows ROI based on customer data.¹

In addition to offering a full SASE solution, VMware recognizes that customers want flexibility in choosing solutions across networking and security to help them in their transformation journey. Customers can choose an integrated solution that includes VMware SD-WAN™ to address their networking needs and VMware SSE partners for security enforcement. VMware SD-WAN is the predominant cloud networking solution used by thousands of customers worldwide in many verticals and consistently recognized as a leader by major industry analysts.

¹ [The Total Economic Impact™ Of VMware SASE Cost Savings and Business Benefits Enabled By SASE](#)

VMware’s SSE partnerships are growing with solutions from leading cloud security providers. Customers gain immediate benefits with the integrated solution and sets them on an accelerated path to SASE led transformation.

Note that this dual-vendor approach to networking and security works well for customers who have distinct teams focusing on each area. Small to medium-sized organizations may have resource constraints and cannot afford such functional boundaries.

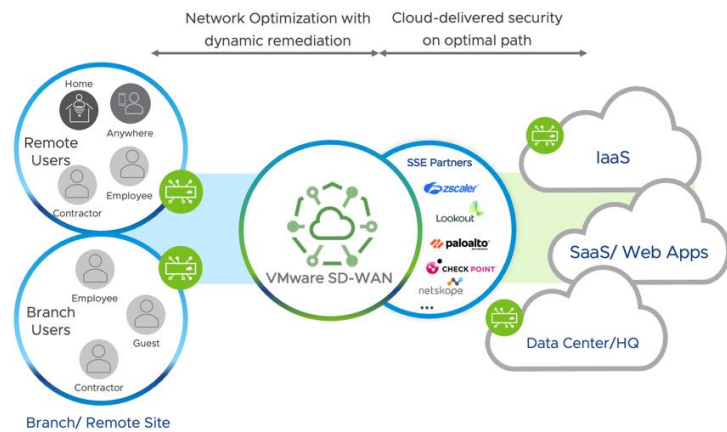


Figure 1: VMware SD-WAN and our SSE Partners deliver comprehensive SASE solution

The benefits of a dual-vendor SSE solution from VMware and our SSE partners include:

Sustained and rich user experience

IT must ensure users get a consistent and rich experience when they access applications, whether these workloads are in the data center or in the cloud. Network performance can vary from branch to branch depending on local conditions like packet loss. VMware SD-WAN dynamically remediates network conditions at each branch without operator intervention. This helps deliver a consistent and sustained experience without placing undue burden on IT.

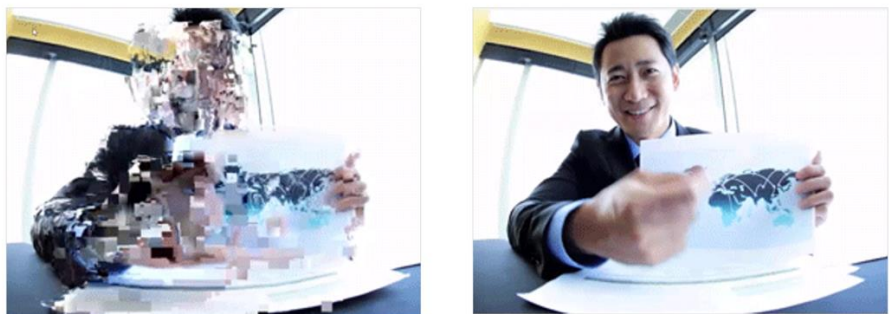


Figure 2: VMware SD-WAN dynamically remediates connections for a consistently rich end-user experience

Learn more

- VMware SSE partners, sase.vmware.com/partners/sse
- VMware SD-WAN, sase.vmware.com/sd-wan
- VMware SASE, sase.vmware.com

Uncompromised security

Enterprises don't have to choose between network performance and keeping the infrastructure safe. VMware solutions place user traffic on the optimal path to app destinations. Cloud security solutions from partner SSE providers enforce security along this optimal path. This approach eliminates unwanted latency that arises when traffic must be sent to a central location for security enforcement. The security capabilities include Secure Web Gateway (SWG), Cloud Access Security Broker (CASB) and Data Loss Prevention (DLP) capabilities to protect against a changing threat landscape.

Customers that need to protect branch and remote sites can deploy a Firewall using enhanced security services on VMware SD-WAN Edge devices. These edge devices also support Virtual Network Function (VNF), giving enterprises the flexibility to choose firewall solutions from other vendors.

Ease of deployment

VMware SD-WAN makes it easy for IT to connect their branch locations without site visits. The solution uses a cloud-hosted central orchestrator where all the branch configurations and policies are defined. The SD-WAN Edge device deployed at the branch location uses zero-touch provisioning to speed up deployment. Customers have provisioned thousands of branch locations within a week using VMware SD-WAN. Adding new branch locations or modifying policies becomes easy to manage.

Simplified operations

VMware SD-WAN provides visual evidence into the Quality of Experience for each class of application at every branch location. The solution leverages AIOps to provide action-oriented insights into end-user and IoT device experience when these devices access applications. The solution simplifies Day 2 Operations for IT and puts time back on their clock.

Conclusion

Integrating VMware SD-WAN with SSE solutions from our security partners gives customers the choice and flexibility to transform their infrastructure and accelerate SASE adoption. This integration helps IT protect against the changing threat landscape without compromising employee productivity. The solution simplifies deployment and management of branch and remote site connectivity to the security enforcement points, and reduces the burden of dealing with multiple disparate tools and services that are common in legacy deployments.