VMware Secure Access

Frequently Asked Questions

Last updated June 2021

Q. What is VMware Secure Access?

A. VMware Secure Access™ is a remote access solution that is based on the Zero Trust Network Access (ZTNA) framework. The solution offers multiple benefits over the traditional VPN access method, including:

- Cloud-native: Cloud-hosted remote access solution
- User-centric: Access granted based on the user identity and end device posture, with access to only the applications the user needs
- Location-independent: Consistent policy regardless of where the user access from

The solution offers both remote and mobile users a consistent, optimal and secure cloud application access through a network of worldwide managed service nodes.

Q. How will this benefit the enterprise?

A. This solution enables enterprises to deliver a branch-like experience to remote workers. The solution is a hosted service, meaning customers will not have to install and manage the remote access solution. IT will also be able to scale the solution up or down based on their needs without having to invest heavily in the on-premises architecture, delivering improved IT efficiency. The zero trust benefits of Secure Access also help improve security by granting user access to only the applications users need.

Q. What are the benefits to the end user?

A. Remote users will enjoy improved performance as they access applications hosted in any cloud. Users can connect to the VMware SASE™ network of global points of presence (PoPs), and the SASE PoP will route traffic to the destination without hairpinning traffic to the data center for better latency, packet drops and jitter.

Q. What are the major components of Secure Access?

A. VMware Secure Access is comprised of:

1. VMware hosted remote access solution deployed in multi-region POPs.
2. VMware Secure Access comes with the VMware Workspace ONE client with tunnel connections to the PoPs. Customers who want to manage their endpoints using Workspace ONE in addition to tunnels can optionally purchase the Workspace ONE Advanced license.
3. Management console. At the time of release, Workspace ONE user management continues to be through Unified Endpoint Management (UEM), and traffic steering is performed on the VMware SD-WAN Orchestrator.

Q. My customer has another MDM besides Workspace ONE. Can they still use Secure Access?

A. Yes. Secure Access can work with any third-party mobile device management (MDM) solution. The Workspace ONE client can also be downloaded and installed by the users themselves.

Q. My customer already has Workspace ONE. Can they use this client to connect to Secure Access?

A. Yes. Secure Access solution comes with a Workspace ONE client that supports only the tunnel service. Customers who have Workspace ONE Advanced license and up have access to both tunnel service and UEM management, and they can use this client with Secure Access.

Q. What is per-app VPN?

A. Per-app VPN allows the IT administrator to specify which desktop application can access which cloud application through tunnels. An example policy would be that users can access www.cnn.com using Chrome web browser, and users would be denied www.gambling.com through Firefox.

Q. What is full device VPN?

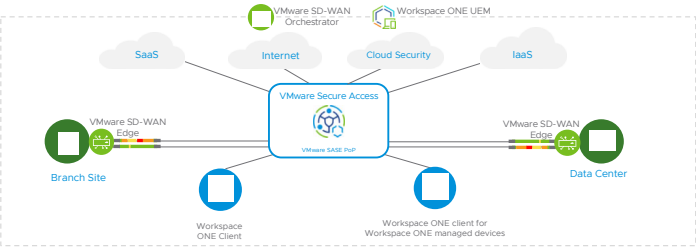
A. Full device VPN permits/denies all traffic originating from the device. All UDP/TCP traffic will be able to generate traffic. Depending on the destination, that traffic can either be blocked or allowed through the tunnels.

Q. Do customers need SD-WAN infrastructure in place for this solution to work?

A. Secure Access can be deployed without VMware SD-WAN™. With VMware SD-WAN deployed together with Secure Access, customers get an additional benefit of Dynamic Multipath Optimization™ (DMPO) for applications between the

POP and data center/branches. Benefits of deploying these two solutions together include:

- Consistent QoS policies across WAN
- Integrated and consistent WAN firewall policies
- Resilient (DMPO) access to data center-hosted applications
- Dynamic tunneling to sites and data center for lower latency and contention



Q. Can customers connect their existing VPN solution to the VMware SASE Platform instead of going through Secure Access?

A. Not directly. Customers must connect their VPN head-end to a VMware SD-WAN Edge, then connect the Edge to the VMware SASE Platform. While technically possible, this may introduce additional latency for certain traffic destination. As for clients, the VMware Secure Access solution uses VMware Workspace ONE client to connect to Secure Access, therefore customers cannot use their existing VPN client to access Secure Access.

Q. Can customers choose their POP locations?

A. Yes. Each enterprise will be able to choose up to five POPs to connect to. If additional PoP locations are needed, they will have to open a case with VMware support.

Q. Can customers purchase Secure Access without SD-WAN or VMware Cloud Web Security?

A. Yes. Secure Access, as part of VMware SASE, can be purchased as a standalone solution. VMware Cloud Web Security™ can also be added to protect remote and mobile users from web threats.

Q. What are the SLAs for this offer?

A. All components are deployed with redundancy in mind. Secure Access servers are deployed in a redundant mode and the solution is deployed in POPs across multiple regions for PoP redundancy as well.

Pricing, Packaging and Ordering

Q. Can I order Secure Access through VMware paper and VeloCloud paper?

A. Customers and partners can order VMware Secure Access from both VeloCloud paper and VMware paper.

If the customer wants to manage endpoints using Workspace ONE UEM in addition to Secure Access, a Workspace ONE Advanced license is needed. Workspace ONE is only available on VMware paper.

Q. What are the sample SKUs for Secure Access?

A. Here is a sample SKU for Secure Access on VMware paper, with 1-year subscription, prepaid. Prices listed are for illustration purposes only.

Sample SKU	Description	List (/user/month)
SA-HD-T-12P-C	VMware Secure Access, Per User, Subscription for 1-year, Prepaid	$5

Here is a sample SKU for Secure Access plus an optional Workspace ONE Advanced license for UEM device management.

SKUs	Description	List (/user/month)
WMU-ADWOAP-12PT0-C1S	VMware Workspace ONE Advanced 12 month, Prepaid	$10.90
NB-VC-AD-HRA-12P-C	VMware Secure Access Add-On for Workspace ONE; Per User; Requires Workspace ONE Subscription with access to tunnel service; Subscription for 1 year, Prepaid	$5

Prices listed are for illustration purposes only.

Q. What are the add-on charges for LATAM and APJ?

A. There is a per-user add-on charge for customers utilizing LATAM and APJ POPs. However, if customers are physically located in LATAM or APJ but the remote workers only access the POPs in North America or Europe, they will not have to pay for these add-ons.

Q. What happened to the minimum user and bandwidth consumption limitations introduced earlier?

A. The 700-user minimum, 5GB/user/month limitations introduced at Secure Access launch in September 2020 are lifted at the Release 4.4 launch. The bandwidth consumption per user is now unlimited with no user minimum requirement.

Q. What is the Non-SD-WAN Destination (NSD) add-on?

A. Secure Access customers are entitled to 5 NSD licenses per enterprise, enabling 5 PoP-Cloud connections from the PoP to any five destinations including Cloud Security, Data Center, or IaaS. Additional NSD licenses can be purchased when needed.

Q. Where can I find more information?

A. You can find more VMware Secure Access information on the VMware SASE web page, sase.vmware.com.