FREQUENTLY ASKED QUESTIONS

VMware SASE Platform

SASE General

Q.What is the VMware SASE Platform?

A. The VMware SASE Platform™ is the secure access service edge (SASE) platform that converges industry-leading cloud networking and cloud security to deliver flexibility, agility, security, and scale for enterprise of all sizes. The VMware SASE Platform is offered as-a-service, helping offload IT staff from deploying and maintaining WAN/security and saving enterprises operational costs.

Q. What are the components of the VMware SASE Platform, and what are available today?

A. There are four components of the VMware SASE Platform:

- VMware SD-WAN™
- VMware Secure Access™
- VMware Cloud Web Security™
- VMware NSX Cloud™ Firewall

VMware SD-WAN and VMware Secure Access are available today. At VMworld 2020, VMware announced Cloud Web Security with the availability date of Q2CY21.

Q. What are the benefits of the VMware SASE Platform?

- Cloud-First – Simplifies and provides cost-effective connectivity to SaaS-based applications
- Intrinsic Security – Unifies network and application security policies for branch and remote workers
- Application Quality Assurance – Ensures availability and performance of mission critical applications
- Operational Simplicity & ROI – Lowers operational expenses

Q. Will all VMware SASE components run inside the VMware SASE PoP™?

A. VMware runs SASE services inside its own worldwide points of presence (PoP). All component services: VMware SD-WAN, VMware Secure Access, VMware Cloud Web Security and VMware NSX Cloud Firewall will run inside the VMware SASE PoP.

Q. How are SASE services consumed?

A. Customers can purchase one or more components in the VMware SASE PoP. In order to take full advantage of the VMware SASE Platform, customers should deploy multiple SASE services.

Q. When will the VMware SASE Platform have a unified management system?

A. At launch, there will be separate management systems for VMware Secure Access. The following is planned:

- VMware Secure Access: Unified Endpoint Management (UEM) and VMware SD-WAN Orchestrator will be used separately at launch, with SSO-based cross-launch and other workflow on the integration roadmap.
- VMware Cloud Web Security and VMware NSX Cloud Firewall will be managed by VMware SD-WAN Orchestrator on day one.

Q. How do I order?

A. See the Pricing and Packaging section in this FAQ for more information on how to order the VMware SASE Platform. You can also find this information in the Ordering Guide.

SD-WAN

Q. How does VMware SD-WAN integrate with the VMware SASE Platform?

A. VMware SD-WAN provides branch office and remote users with the ability to:

- Prioritize business-critical traffic
- Mitigate network issues for best application performance
- Deliver traffic to a network of VMware SD-WAN Gateways for best SaaS, IaaS and data center applications

Once user traffic optimized with VMware SD-WAN arrives at the PoP, additional services from other components can be applied to that traffic for security checks.

Q. Do customers need VMware SD-WAN if they want to purchase additional services like Secure Web Gateway?

A. Traffic can come into the VMware SASE PoP in two ways: through VMware SD-WAN using a VMware SD-WAN Edge or through VMware Secure Access for remote/mobile users. Once the traffic is inside the PoP, it can be sent to VMware Cloud Web Security or VMware NSX Cloud Firewall for further inspection.

Q. How are the Work from Home bundles different from VMware Secure Access?

A. The Work from Home bundles are for home workers who want to deploy a VMware SD-WAN Edge. Home users behind this

Edge will have the same benefits as an office user: automatic application prioritization, link optimization with Dynamic Multipath Optimization^{TM} (DMPO), access to a network of gateways for optimized SaaS/IaaS applications, and more.

VMware Secure Access offers remote and mobile workers a way to securely connect to the VMware SASE PoP for optimal access to applications hosted in SaaS/IaaS/data center.

VMware Secure Access

Q. What is VMware Secure Access?

A. The VMware Secure Access solution provides users consistent, optimal and secure cloud application access through a network of worldwide, managed service nodes. The solution brings the best of both VMware SD-WAN and VMware Workspace ONE solutions into a single, cloud hosted offer that ensures a consistent application experience and verified access to corporate applications as users work at the office and remotely.

Q. How will VMware Secure Access benefit enterprises?

A. VMware Secure Access enables customers to deliver a branch-like experience to remote workers. As a hosted service, this means customers don't have to install and manage the Workspace ONE unified access gateway (UAG) component, delivering improved IT efficiency. Enterprises do not have to keep scaling VPN concentrators and buying additional Internet bandwidth associated with sending VPN traffic to the data center before sending it back out to the SaaS/IaaS cloud (hairpinning).

Q. What are the benefits of VMware Secure Access to enterprise users?

A. Remote users will enjoy an improved performance as they no longer have to access the VPN concentrator hosted in a few data centers. In addition, users can benefit from the ability to leverage global PoPs to eliminate hairpinning, and optimized traffic handling capabilities to help lower latency and drive better performance and resiliency in remote access.

Q. What are the major components of VMware Secure Access?

A. VMware Secure Access is comprised of:

- VMware hosted Workspace ONE UAG with stateful firewall and traffic steering, deployed in multi-region VMware SASE POPs.
- Workspace ONE license that provides access to tunnel services like Workspace ONE Advanced edition and above. Workspace ONE client support includes iOS, Android, Mac OS, Chrome OS, Windows OS, and more, ensuring support for BYO devices in enterprises.

Q. What are the options for client access into VMware Secure Access?

A. Users can access VMware Secure Access by using Workspace ONE as a mobile device management (MDM) to manage endpoints such as laptops, smartphones, tablets in an enterprise. The Workspace ONE client is used to connect to the VMware SASE PoP.

Q. Can I use the Workspace ONE client when I am behind a VMware SD-WAN Edge?

A. Workspace ONE can be used behind a VMware SD-WAN Edge. Workspace ONE will pause the tunnel to the VMware SASE PoP while the client is on the enterprise network; traffic will be sent over the tunnel between the Edge and the PoP.

Q. How do customers raise technical support requests for VMware Secure Access

A. Customers should raise their support request to the Workspace One team using the external *KB (2151511) article*.

Cloud Web Security

Q. Who are you partnering with for Cloud Web Security services?

A. We are integrating SWG technology from Menlo Security to form the basis of the VMware-branded Cloud Web Security (CWS). Menlo services will be running in VMware SASE PoPs, along with other VMware SASE services.

Q. Do you plan to continue supporting other third-party security providers with your SD-WAN deployment?

A. Our SD-WAN architecture is built to provide flexibility for customers to choose the cloud security provider. We are expanding our existing relationship with Zscaler for large enterprises with broad security requirements. We will support third-party vendors like Check Point, Palo Alto and Fortinet for VNF FW function deployed on the VMware SD-WAN Edge.

Q. What is the benefit of offering Cloud Web Security as a service of the VMware SASE Platform?

A. Benefits include:

- Alignment of business policies with security policies, via the VMware SD-WAN Orchestrator, to address a changing threat landscape. As an example, a security policy may say that all YouTube traffic can bypass VMware Cloud Web Security, and that will be interpreted as a business policy to place YouTube traffic directly on the Internet instead of sending it to the nearest VMware SASE PoP over the DMPO tunnel.
- Single management plane with VMware SD-WAN Orchestrator to configure, monitor and manage network services, security services and remote access. This will help

users located in the branch, at home or on the move access enterprise applications, internet applications, and SaaS applications. The SASE platform will take advantage of shared intelligence between these services for adaptive integration of policies. As an example, a business policy to allow users to access social networking sites during non-office hours will be interpreted to activate CASB function for social networking applications during that period.

- Improved user application experience and reduced latency with secure handoff to SaaS applications at the nearest exit using a global network of VMware SASE PoPs. The solution helps eliminate unwanted hairpinning or backhauling of traffic to the data center to administer security before sending it to cloud destinations.
- Ensure consistent business policy implementation across the distributed workplace to protect user and infrastructure from internal and external threats. The enterprise security posture remains consistent, no matter from which location users are trying to access any application.

Q. Will VMware Cloud Web Security require a hardware upgrade at the VMware SD-WAN Edge?

A. The introduction of VMware Cloud Web Security will not require any hardware upgrades to existing VMware SD-WAN Edge deployments.

Q. What functions will VMware Cloud Web Security support?

A. VMware Cloud Web Security will include the following functionalities:

- Secure web gateway (SWG)
- Cloud access service broker (CASB)
- Data loss prevention
- Sandbox
- Remote browser isolation (RBI)

Pricing

Q. How is the VMware SASE Platform priced?

A. The VMware SASE Platform is priced per component. Customers can consume one or multiple components. Here is the summary:

- VMware SD-WAN: licensed per bandwidth tier
- VMware Secure Access: licensed per user
- VMware Cloud Web Security: licensed per user and per bandwidth, depending on use case

Q. How is VMware Secure Access priced?

A. VMware Secure Access is licensed per user. For managed clients, customers need two types of licenses:

- Workspace ONE Advanced and above license: Existing Workspace ONE Advanced and above customers do not need to purchase additional Workspace ONE licenses.
- Hosted Remote Access license: This is VMware's UAG hosting in the VMware SASE POPs around the world. The SKU for this hosted remote access license is:
  - VC-AD-HRA-[subscription term][payment]
  - Subscription term: 12-, 36- and 60-months
  - Payment: Prepaid, Monthly, Annually
  - For example, the SKU for 36-month, prepaid would be VC-AD-HRA-36P

Q. How is VMware Cloud Web Security priced?

A. VMware Cloud Web Security is licensed per user (remote access use case) and per bandwidth (branch use case).

Partners

Q. What are the offers partners can provide to their end customers?

A. Partners, including value-added reseller (VAR), managed services provider (MSP) and service provider can continue to resell VMware SD-WAN, in addition to the new services in the VMware SASE PoP, including VMware Secure Access, VMware Cloud Web Security and VMware NSX Cloud Firewall.

Q. Can Telecom service provider partners implement the VMware SASE Platform in their own PoPs?

A. Telecom service providers can resell the VMware SASE Platform (SD-WAN, Secure Access and Cloud Web Security) through the over the top (OTT) model. Hosting VMware SASE in the SP PoPs is planned for a later date.

Q. Where can I find more information?

A. You can find more SASE information on the *VMware SASE Platform* page.

VMware, Inc. 3401 Hillview Avenue Palo Alto CA 94304 USA Tel 877-486-9273 Fax 650-427-5001 vmware.com