Lumen® SASE with VMware FAQ

Lumen and VMware partner to provide a comprehensive cloud-based network and security management experience offering the agility and reach to deliver high-performance, secure access to your business applications from virtually anywhere, on any device.

Lumen SASE Solutions

Q What is Lumen SASE Solutions?

Lumen SASE Solutions is a cloud-based network and security experience designed for today's distributed enterprise that is centrally controlled, fully integrated and flexibly managed.

Lumen SASE unites the purchase, deployment, orchestration, and management of software-defined network infrastructure and information security to simplify the delivery of applications wherever the business needs them.

Q What are the benefits offered by Lumen SASE Solutions?

Lumen SASE Solutions combines our expansive network and cloud platform availability with leading software management partners designed to deliver improved control, visibility, and simplified management of network and security for cloud-based application delivery anywhere, on any device.

Lumen SASE is an integrated solution – High performance, secure delivery of cloud applications wherever your business needs them. Lumen SASE Solutions offer optimal application performance and availability through:

- **End-to-end control and visibility -** 2,200 connected public and private data centers and one of the most highly peered IP backbones.
- **Low latency application performance and closer threat analysis** - 50+ edge locations in major metros connected to high-capacity fiber.
- **Full integration of network and security management** – Centralized policy control and performance visibility for branch locations and remote workforce.

Lumen SASE is a secure solution – Secure application delivery from the cloud, across the network, to any device, on virtually any network.

- **The right solution for your business** offering your choice of leading SD-WAN and security partners.
- **Monitoring threats around the clock and across the globe** with Black Lotus Labs® offering customer visibility and support across nine Security Operations Centers.
- **Secure application access policy by location, device, and user** using Zero Trust Network Access (ZTNA) and to local Secure Web Gateways (SWG) to analyze threats sooner.

Lumen SASE Solutions is flexible – Flexible control, delivery, updates, and management of network and security using a unified online experience for all your locations and users.

- **Simplified network and security deployment and management** that moves from dedicated hardware to flexible software that you purchase and configure online.
- **Simplified addition and automated update** of network and security features and services.
- **Flexible management options** that fit your current business needs with the ability to easily add deeper levels of Lumen management as needed.

Q How Is the service provided via the Lumen® Platform?

Lumen SASE offers the convergence of networking and security functions in a cloud first unified solution with a focus on the digital experience and built on the world class Lumen Platform.

VMware SASE General

Q What is the VMware SASE Platform?

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 designed to save enterprises operational costs.

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

There are four components of the VMware SASE Platform:

- VMware SD-WAN™
- VMware Secure Access™
- VMware Cloud Web Security
- VMware Firewall-as-a-Service (FWaaS)

SD-WAN, Secure Access, and Cloud Web Security are available with our initial offering. FWaaS availability is targeted for late 2022. Cloud Web Security inspects traffic going to the web/SaaS cloud while FWaaS is deployed to inspect traffic going to the Enterprise Data Center.

Q What are the benefits of the VMware SASE Platform?

Benefits include:

- **Comprehensive Distributed Workforce Solution.** The VMware SASE offering helps ensure the availability, security, and performance of mission critical applications from the branch, home, or away and for users on company-owned or BYO devices.
- **Mature Global Cloud Platform.** VMware SASE is field proven, multi-tenanted platform with points of presence to help ensure application performance.
- **Single Comprehensive Management Platform.** Simplifies operations and minimizes support complexities by unifying networking and security.
- **Broad Ecosystem and Open Architecture.** VMware SASE has a broad ecosystem of partners, allowing enterprises to control their migration to SASE.

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

Benefits include:

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 FWaaS will run inside the VMware SASE PoP.

Q How are SASE services consumed?

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

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

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

How do I order?

VMware SASE services can be ordered using the Lumen SASE Solutions marketplace and Lumen SASE Manager experience. Services can always be purchased by contacting our Lumen sales team.

SD-WAN

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

VMware SD-WAN provides branch office and remote users behind an edge device 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 access to SaaS, IaaS and data center applications.

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

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

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 FWaaS for further inspection.

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

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 (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

What is VMware Secure Access?

The VMware Secure Access solution provides remote access users a 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 helps ensure a consistent application experience and verified access to corporate applications as users work at the office and remotely.

How will VMware Secure Access benefit enterprises?

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 remote access concentrators, delivering enhanced IT efficiency. Enterprises do not have to keep scaling remote access 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).

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

Remote users will enjoy an enhanced performance as they no longer must access the VPN concentrator hosted in a few data centers. In addition, users can benefit from the Zero Trust Network Access (ZTNA), 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. Cloud Web Security service can be applied to the remote user traffic protecting users from internal and external threats.

What are the major components of VMware Secure Access?

VMware Secure Access is comprised of:

- VMware-hosted Workspace ONE Tunnel Service, stateful firewall and traffic steering, deployed in multi-region VMware SASE POPs.
- Client options (see below).

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

Users have multiple options:

- **Managed client:** Workspace ONE is used 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.
- **Stand-alone:** Third-party MDM can be optionally used to install VMware Workspace ONE VPN client to the devices, or the endpoint can download and install this VPN client directly. The Workspace ONE VPN client can then connect to the VMware SASE PoP.

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

Workspace ONE can be used behind a VMware SD-WAN Edge. Depends on the Enterprise policy, Workspace ONE can be configured to 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.

Cloud Web Security

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

- Integrated Service Delivery with security administered on the optimal path between user and the application. Single stop processing that brings remote access, branch and campus traffic on an efficient path to SASE PoP and combines packet decryption, inspection, encryption and hand off to SaaS and Internet destinations. This approach is designed to reduce latency and increase productivity.
- Single management plane with VMware SD-WAN Orchestrator to configure, monitor and manage network services and security services. Using the VCO IT admins can configure the security policies for user and user groups and assign it to network segments without any policy mismatch. NetOps and SecOps can use a centralized portal to get visibility, control and view of the user experience, security posture and determine opportunities to tighten the surface exposed to attack.
- Local presence with security delivered as a cloud hosted service at each SASE PoP globally using the industry proven deployment architecture and experience. This helps with faster service activation and accelerates move to cloud. The platform uses readily available contextual information about the user, user group, user location and destinations sought to determine the security action.
- Pervasive security for anywhere workforce with consistent policy implementation whether the employee is working from home, office or on the move. The solution offers comprehensive security coverage for the entire spectrum of users ranging from power users to light users working from virtually anywhere.

Is there a common admin interface?

Cloud Web Security is offered using the centralized portal for managing security and networking policies. This is made possible using the VMware SD-WAN Orchestrator. For example, security policy can be configured in the Orchestrator UI and applied to the network segment as a single workflow. This approach eliminates any mismatch between security and networking policies. NetOps, SecOps, CSO, CIO and Compliance teams can get common view of network performance and security posture.

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

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?

VMware Cloud Web Security will include the following functionalities that will be delivered in phases:

- Secure web gateway (SWG): URL filtering, advanced antimalware with file hash check, cloud sand box, SSL inspection.
- Cloud Access Security Broker (CASB) visibility and control.
- Data loss prevention (DLP) visibility and control.
- Remote browser isolation (RBI).

Discover more about Lumen SASE Solutions with VMware by visiting lumen.com/SASE solutions
www.lumen/sase.com