

# Work from Anywhere: A VMware SASE Solution

Secure and optimize your network connectivity while working remotely, with varied deployment options

vmware®

SASE™

To learn more about VMware WFH and WFA subscriptions, visit the [VMware Work from Anywhere Solution](#) web page.

Enterprises are going through a necessary digital transformation to support the distributed “anywhere” workforce and the proliferation of SaaS and cloud applications. Employees are now mobile, applications are being modernized, and cloud is being adopted at a rapid pace—all of which blur the enterprise edge. Companies must ensure employees working from anywhere are productive and efficient, while simplifying operations for IT teams and securing distributed users, applications, and devices.

To ensure a seamless work from home, or anywhere, experience, employees need a technical environment that closely replicates the experience they would have in the office. This means easy, seamless, and secure access to applications as well as consistent and always-on Internet availability. Inefficient network connectivity results in lack of bandwidth, broken and disrupted connections, and poor application performance. For remote users, secure access to the corporate network to utilize applications and protect these SaaS and web applications for day-to-day work is extremely important.

## Solving work-from-anywhere access issues with VMware SASE

For enterprises to provide employees with a better work from anywhere (WFA) or work from home (WFH) environment, VMware SASE™ combines industry-leading VMware SD-WAN™ with comprehensive security options embracing cloud and SaaS. VMware SASE delivers flexibility, agility, security, and scale for enterprises and enables WAN and edge transformation.

VMware’s unique approach includes SASE points of presence (PoPs) worldwide to serve as an on-ramp to SaaS and other cloud services. These PoPs, strategically located in IaaS and co-location data centers, deliver optimal performance because they are close to users and applications.

The VMware cloud-native SASE architecture combines VMware SD-WAN, VMware Secure Access™, VMware Cloud Web Security™, firewall as-a-service (FWaaS), and VMware Edge Network Intelligence™.

- **VMware SD-WAN** delivers excellent and optimized network connectivity, assured application performance along with security, providing the quality of service (QoS) users need. VMware SD-WAN also provides operational

### VMware work-from-home subscription options

- WFH Subscription
- WFH Pro Subscription

### VMware work-from-anywhere subscription options

- Secure Access
- Secure Access with Cloud Web Security *Standard*
- Secure Access with Cloud Web Security *Advanced*

simplicity by providing centralized monitoring, analytics, and control combined with artificial intelligence to simplify operations.

- **VMware Secure Access** provides remote and mobile users with consistent, optimal and secure cloud application access through a network of worldwide managed service nodes. This cloud-hosted solution is based on a zero-trust network access (ZTNA) architecture.
- **VMware Cloud Web Security** protects users and infrastructure accessing SaaS and internet applications from a changing threat landscape. This cloud-hosted solution leverages and integrates best-of-breed secure web gateway (SWG), cloud access security broker (CASB), data loss prevention (DLP), anti-virus protection, and URL filtering in the SASE PoP to provide secure, direct, and optimal access to SaaS and web applications and reduce surface of attack.
- **VMware Edge Network Intelligence** is a vendor-agnostic artificial intelligence for IT operations (AIOps) solution focused on the enterprise edge. VMware Edge Network Intelligence provides visibility not just into the SD-WAN network, but all the way to the LAN including Wi-Fi networks. It provides IT administrators with end-to-end network visibility to analyze and remediate any network issues.

## VMware WFH and WFA subscriptions for the enterprise

As the enterprises have a distributed workforce now, where the remote employees can either work from home or anywhere, be it a coffee shop or a remote site, it becomes imperative that they deploy new configurations. To help enterprises provide an optimized work environment and experience for remote employees, VMware offers two subscription options: VMware SD-WAN WFH and VMware SASE WFA that address the needs based on their usage and connectivity requirements.

### VMware SD-WAN subscriptions for WFH enterprise employees

VMware offers two subscriptions powered by VMware SD-WAN that enable users to get the best application performance while working from anywhere: WFH and WFH Pro.

Any VMware SD-WAN Edge can use either WFH subscription license type. The appropriate license type depends on end users' typical work tasks. Light users who use the network for regular emails and voice calls may use the WFH subscription license. Power users who need to download large files and attend video conferencing calls may need the WFH Pro subscription license. Both subscriptions include access to VMware Edge Network Intelligence.

VMware SD-WAN work-from-home subscriptions	
WFH Subscription	WFH Pro Subscription
One business user Up to three (3) concurrent business devices	One business user Up to six (6) concurrent business devices
Up to 350 Mbps (or maximum device throughput)	Up to 1 Gbps (or maximum device throughput) for graphics and large file downloads
Improved app reliability and performance for audio/video conferencing, voice calls and emails	Improved app reliability and performance for audio/video conferencing, voice calls and emails
Includes direct SaaS and cloud VPN access	Includes direct SaaS and cloud VPN access
Delivers rich client experience with VMware Edge Network Intelligence	Delivers rich client experience with VMware Edge Network Intelligence
Unlimited home users and unlimited home devices	Unlimited home users and unlimited home devices

### Security

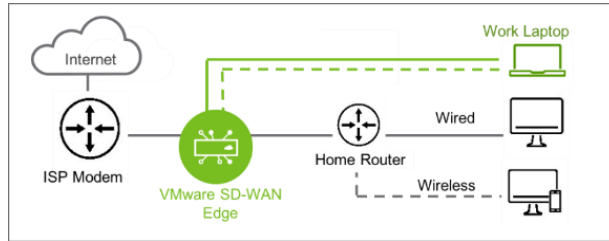
Customers should enable 802.1x authentication for all wired ports and wireless SSIDs (except for an SSID or wired port for home users). VMware SD-WAN Edge supports EAP-MD5 password-based authentication as well as Mac Authentication Bypass (MAB) for 802.1x authentication. Enabling 802.1x authentication ensures that only business users and devices can access the overlay and the enterprise network.

### Privacy

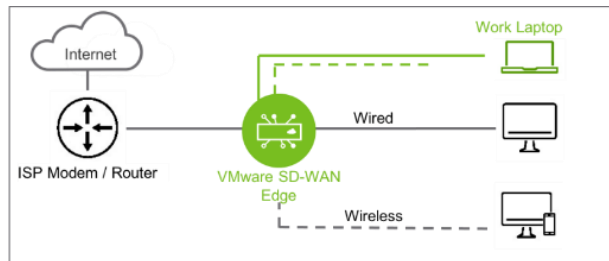
Home users and devices connected to the VMware SD-WAN Edge should be assigned to a VLAN that is configured as a private segment. Doing this ensures that traffic from these appliances will go directly to the internet via the underlay and ensures privacy for the home users' traffic (no flow data is collected or stored for private segments).

### Deployment options

VMware recommends two deployment options to obtain maximum benefit from SD-WAN. In both scenarios pictured below, all traffic is routed through the VMware SD-WAN Edge. It prioritizes work traffic and applies on-demand remediation when poor application performance is detected. This ensures better Quality of Service (QoS) and a better user experience.



Deployment with separate ISP modem and router



Deployment with integrated modem and router

## VMware SASE for work from anywhere subscription options

To help enterprises provide an optimized work environment and experience for their WFA employees, VMware offers three software subscriptions that enable users to get the best application performance and uncompromised security while working from anywhere: Secure Access, Secure Access with Cloud Web Security Standard, and Secure Access with Cloud Web Security Advanced.

All VMware SASE WFA subscriptions provide remote access to the corporate network and contextual access policy with device posture, identity, and user behavior through VMware Secure Access. The appropriate license type depends on the enterprise's desired level of control and ideal security posture.

VMware SASE work-from-anywhere subscriptions		
Secure Access	Secure Access with Cloud Web Security <i>Standard</i>	Secure Access with Cloud Web Security <i>Advanced</i>
One business user Up to five (5) concurrent business devices	One business user Up to five (5) concurrent business devices	One business user Up to five (5) concurrent business devices

Remote access solution to corporate network	Remote access solution to corporate network	Remote access solution to corporate network
Provides contextual access policy with device posture, identity and user behavior	Provides contextual access policy with device posture, identity and user behavior	Provides contextual access policy with device posture, identity and user behavior
	Protects against known and zero-day security threats accessing web apps	Protects against known and zero-day security threats accessing web apps
	Delivers visibility into SaaS apps	Delivers visibility into SaaS apps <b>and</b> provides control over user activities
No bandwidth limitation	No bandwidth limitation	No bandwidth limitation
Includes VMware Secure Access	Includes VMware Secure Access, VMware Cloud Web Security <i>Standard</i>	Includes VMware Secure Access, VMware Cloud Web Security <i>Advanced</i>

To learn more about VMware WFH and WFA subscriptions, visit the [VMware Work from Anywhere Solution](#) web page.