VMware Workspace ONE Tunnel Solution Overview

Key Takeaways

- **Security and Privacy:** flexibility to be deployed like a traditional VPN or as a per-app VPN that provides tighter Zero Trust controls around network and endpoint security.
- **Integration with Workspace ONE:** removes adoption barriers while providing a zero-touch, best of breed experience.
- **Cost:** included in Standard, Advanced and all Workspace ONE Essentials editions.

"60% of organizations will embrace Zero Trust as a starting point for security by 2025."

Gartner

Source: Gartner Unveils the Top Eight Cybersecurity Predictions for 2022-23

For years, hybrid and remote employees have accessed work resources from a corporate device via a virtual private network (VPN). As we move from general access to resources to a least-privileged, Zero Trust approach, the connections of remote users to enterprise networks deserves a review.

Today it's possible to replace legacy remote access VPNs with modern offerings that provide more segmented access to apps and resources and grant you the ability to better customize policies to respond to potential security risks in real time. This solution overview will tell you more about Workspace ONE Tunnel and the ways it can help modernize and better-secure remote access.

Replace Legacy VPN: Connect to Apps, Not Networks

Typically, a user launches their VPN app and is connected to much or even all of the company network. Remote access must move beyond this "one big pipe" approach. The one big pipe connecting in and out of corporate networks often results in lower throughput and higher latency due to the amount of the extra traffic being backhauled. This creates a poor employee experience and a higher total cost of ownership as organizations will require additional investments in infrastructure and bandwidth.

Moreover, this approach to app exposure also creates security weaknesses. Users have access to the wide area network, exposing them to more apps and services than are intended. VPNs places users' devices on the network, granting them local IP addresses and causing them to be routable from other devices in the network, further increasing the attack vectors to any enterprise data that lives on a user's machine.

Lastly, traditional VPNs only evaluate trust with the user at the beginning of a VPN session. This can expose your network to device-born threats that may arise during a VPN session, without any ability to revoke or restrict access until the session expires. As malicious actors become quicker with their methods, we need to be able to react quicker to these threats.

VMware Workspace ONE Tunnel

With Workspace ONE Tunnel, you can securely connect to apps, not whole networks – this includes apps you host in your own data centers or across any cloud. Tunnel improves traditional resource connectivity by (1) validating the security posture of users, and (2) refining connectivity to explicit apps and resources.

Workspace ONE Tunnel operates as an application proxy, adding an additional layer of protection by granting app access to internal resources based on your organization's policy. The solution consists of two components: the Tunnel client that lives on a user's device, and Tunnel service that is part of the VMware Unified Access Gateway, the hardened remote access gateway used by millions of users of Horizon and Workspace ONE. End-to-end, Tunnel uses strong TLS encryption and SSL pinning to secure access from users to the target resources. Tunnel is available for all major operating systems, as well as in an SDK form-factor on mobile for app developers.

Connections from Tunnel are routed to the destinations you define via the Unified Access Gateway (UAG), which serves as the session concentrator and provides the enforcement layer of device posture, user entitlement, and the least-privilege coupling of users to devices to apps to resources. UAG is typically hosted on-prem in any vSphere environment or cloud provider, or in the cloud as part of VMware's Secure Access Service Edge (SASE) offering.

All users are not equal, and some require more or different levels of access than others. One major way Tunnel enables advanced identity access management (IAM) and role-based access control (RBAC) is via per-app tunneling. Per-app tunnel is a mechanism to identify and isolate traffic from specific software and services running on an endpoint. This is unique in comparison to traditional VPNs that do not have the context of source app and cannot specify which apps on the device should be trusted. Tunnel uniquely provides this enhancement across platforms and can sculpt policies of software apps and what resources they can access, based on identity and device.

Workspace ONE Tunnel supports unmanaged devices and provides additional security controls for managed devices like network lockdown support for apps as well as device compliance for trust validation based on UEM signals. This helps relate risk and privacy with defined network policies per-app.

Zero Trust Alignment

While VPN has been a traditional and familiar way of providing access, Tunnel's architecture combined with the rich context from Workspace ONE combine to address these Zero Trust requirements.

- Continuous Authorization: frequently reviewing device posture and adjusting or revoking access based on changes in posture.
- Access Segmentation: defining explicit connection paths and availability of software apps to reach specific network destinations.

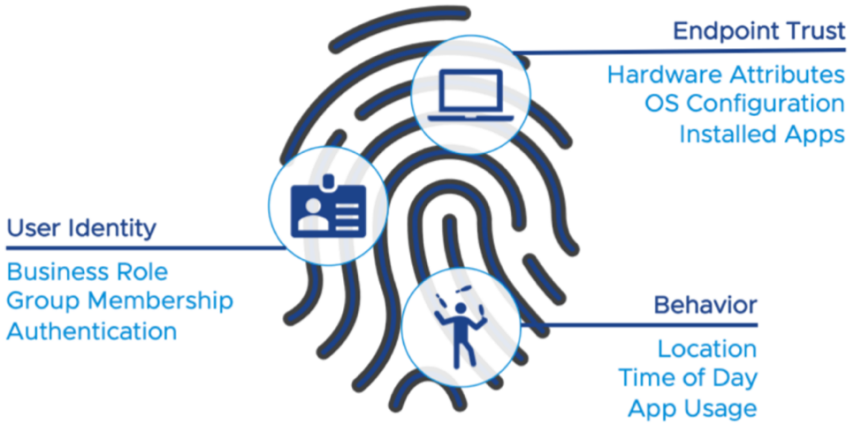

Figure 1: Key identity factors to verify before providing application access.

Continuous Authorization

IT admins using Workspace ONE can grant access to apps with high confidence. Tunnel integration with the Workspace ONE platform means that vital data – including device health, identity, and behavior – can inform the decision to grant access to resources. If something changes related to a user, their device or other attributes of their app session, access may be quickly revoked.

For example, if a user jailbreaks their device or installs an unapproved app, Tunnel can respond by interrupting the session. Folding in identity controls for conditional access, Tunnel can provide even greater integration of multi-factor authentication (MFA), risk policies, and variable authentication requirements.

Access Segmentation

Workspace ONE Tunnel is unique relative to other remote access solutions because of its architecture. While Tunnel complies with cryptographic standards like FIPS 140-2, it breaks the mold of traditional VPNs by preventing routability back to the device – your devices cannot be "connected to" by other devices or services in your network.

Tunnel can be deployed in either a per-app mode (for the mature Zero Trust integrator) or in full-device mode, for organizations that require it or are looking to safely implement app tunneling over time.

In either deployment mode, Tunnel's awareness of software apps enables it to monitor and manage the network events of individual pieces of software, enabling your organization to have visibility into software behavior and updates, be it from internally developed apps or third-party apps. Admins can then curate policy to ensure that apps stay in compliance with any DLP or regulatory policies your organization has. Flexibly, Tunnel enables you to gain insights directly via our core data platform, Workspace ONE Intelligence, or from any security information and event management (SIEM) tool.

Compliance and Privacy

Improving workspace security shouldn't come at the expense of employee experience. The tug of war between user experience, security, and privacy has come to a head in recent years with new laws like Europe's General Data Privacy Regulation (GDPR) and California's Consumer Privacy Act (CCPA).

Tunnel helps organizations meet these needs by enabling granular policies for users and separating work and personal information. The Tunnel app also informs the user of the privacy policy and understanding which apps have been configured by the enterprise.

Integration with Workspace ONE

The Workspace ONE portfolio provides turnkey deployments for admins and a seamless experience for user productivity – enabling users to access any combination of SaaS, virtual, native, web, or internal apps. All of these apps can be automatically deployed to devices and launched via the Workspace ONE Intelligent Hub app, enabling all types of user personas to help keep their businesses moving forward.

Workspace ONE Tunnel can help you along your Zero Trust journey wherever you are, layering in conditional access and MFA, supporting mixed-modes of workers' device types, or transitioning from traditional VPN deployments to segmented, least-privilege access.

Get Started

Visit Test Drive to see Workspace ONE Tunnel in action or contact your sales representative for more information.