White Paper

4 ways Citrix Endpoint Management beats VMware Workspace ONE

Let employees work how, when, and where they want with an endpoint enriched for secure productivity

A true digital workspace is there for people whenever and wherever they need it—any device, any place, any time. That makes unified endpoint management (UEM) an essential part of your workspace solution and your security strategy. Both Citrix Endpoint Management and VMware Workspace ONE offer capabilities to manage user endpoints, but to complete your workspace strategy, you need more than just administrative controls. With Citrix Endpoint Management, you can help people become more productive, allow more flexibility in device ownership, strengthen security, and make the full power of Citrix Workspace available any way people choose to work.

Here are four reasons Citrix Endpoint Management is your best choice for UEM:

1. Built for productivity

Citrix Endpoint Management takes mobile productivity seriously. Highly rated Citrix mobile productivity apps including Secure Mail, Secure Web, and Citrix Files, along with components like Citrix Workflows, Citrix ShareConnect, Citrix QuickEdit, and the Citrix Workspace app, help people get more done, more easily on any device they choose. Support for Samsung Dex lets users switch easily to a larger monitor any time they like. Mobile SSO across all productivity apps provides a fast, seamless, and convenient experience so people can get to work more quickly.

Secure Mail goes beyond personal apps by providing features designed for business productivity. Tabbed navigation, feeds, a prioritized inbox, and multi-swipe functions give employees efficient, intuitive ways to manage and navigate their email. iOS files integration and a better experience for attaching photos make it simpler to share content with colleagues. Users can overlay their personal calendar over their work calendar, or import/ export personal calendar events, to plan their time more easily and avoid inadvertent conflicts. Derived credentials support and one-touch reporting for phishing emails help improve security without adding friction to the user experience.

Secure Web provides a consumer-style web browsing experience with security for the enterprise. The built-for-business browser provides a secure and controlled alternative for personal browsers accessing internal web apps, and for launching allow-listed domains from links in SecureMail. IT can preload a corporate home page and bookmarks, and control the user interface, for a customized experience. For employees, Samsung Dex support and offline page viewing offer more flexible ways to work, while pop-up blocking keeps unwelcome intrusions out of the picture.

Citrix Files extends secure document sync, sharing, and co-editing to any device. Employees can access documents in Citrix Content Collaboration folders via any Citrix Endpoint Management app through single sign-on, and easily collaborate on files with users both inside and outside of their organization. An offline mode helps people stay productive even in limited network scenarios. To keep control over enterprise content, IT can set custom access permissions to files and folders for individual users, and can store specific files on premises, in the cloud, or in a hybrid environment.

Citrix Workflows makes it simple for employees to automate business processes without the need for mobile app development. A drag-and-drop form builder provides an intuitive way for individuals and lines of business to create their own mobile apps and workflows.

Citrix ShareConnect takes mobility even further by letting people securely access the folders and apps on their PCs from their tablets and phones. Citrix QuickEdit, an editing tool for mobile productivity apps, supports file types including Microsoft Word, Microsoft Excel, Microsoft PowerPoint, and image files so people can be fully productive on the go. And of course the Citrix Workspace app provides access to the user's Citrix Workspace—for the full power of Citrix solutions for virtual apps and desktops, content collaboration, and more.

VMware Workspace ONE defines UEM more narrowly. The tool offers only weak integration with enterprise file sync and sharing, limiting people's ability to work and collaborate with content on their mobile devices. Instead of enhancing the user experience, VMware Workspace ONE Content and Browser apps can be cumbersome and frustrating to use, hampering productivity. From IT's perspective, the fee charged for migration from on premises to cloud deployment, together with the lack of a wrapping-as-a-service offering, limit flexibility.

2. Better for BYOD

Citrix Endpoint Management is the industry's most comprehensive mobile application management (MAM) solution, giving IT the flexibility to keep business apps and data secure without compromising employee privacy. That makes it a great fit for any device ownership model, including bring your own (BYOD) or corporate owned, personally enabled (COPE). By isolating corporate apps from personal apps, IT can easily protect company data without touching employees' personal information. The ability to enforce effective security policies regardless of device ownership transforms BYOD from a security liability—and a source of anxiety for IT—to a safe, popular, and effective way to increase employee productivity and engagement.

As a leader in Platform MAM, Citrix Endpoint Management gives IT fine-grained control over apps from third-party app stores, with support for iOS Managed App Configurations, Android Enterprise, Samsung Knox, Windows Information Protection, and the AppConfig Community. To ensure tight security in BYO use cases, Citrix Endpoint Management provides a full set of technologies to protect data at rest and in motion, complemented by data loss prevention (DLP) policies. More than 60 out-of-the-box policies for high-security enterprise apps help speed deployment without putting business data at risk. Citrix microVPN technology provides additional protection for Secure Mail, Secure Web, and Citrix Files between the apps and the datacenter.

For organizations using Microsoft Office 365 apps, Citrix Endpoint Management offers extended features to enhance security and management regardless of who owns the device being used. Admins can use the Citrix Endpoint Management console to manage Office 365 via Graph API integration, and use the Citrix control plane to configure Microsoft Endpoint Manager App Protection policies. IT can also manage apps with Microsoft Endpoint Manager App Protection while using Citrix microVPN technology for secure app-specific connectivity. For devices managed using Microsoft Endpoint Manager MDM, Secure Mail can be deployed in the same container as Office 365 apps to enable seamless productivity.

VMware Workspace ONE lags far behind on BYOD. With fewer than half as many MAM policies, the tool allows much less control over business apps and content on personal devices. With microVPN unavailable in MAM-only mode, organizations are unable to provide this high level of protection without using MDM to fully manage the employee's device, a highly unpopular and intrusive approach to BYOD. Workspace ONE provides only limited app provisioning and MAM control over VMware and line-of-business-enabled apps; more advanced features require MDM—again, an unappealing option. Providing only a light SDK and no online service for wrapping apps, the tool allows less flexibility and integration than Citrix Endpoint Management.

Workspace ONE also fails to extend and enhance the utility of Microsoft Endpoint Manager. VMware does not provide either apps that work with Microsoft Endpoint Manager App Protection, or a mail app compatible with Microsoft Endpoint Manager MDM devices. And unlike Citrix Endpoint Management, Workspace ONE requires a bridge app for cut/copy/paste across managed apps. Add it up, and Workspace ONE makes for a less flexible, more intrusive approach to BYOD.

3. Secure by design

Citrix Endpoint Management gives organizations a high level of protection and control over mobile apps and data with Citrix microVPN technology. Clientless configuration and management is driven entirely through Citrix ADC configuration, with no need for MDM enrollment or device-side VPN policy or client. Employees gain seamless access without having to input settings manually on either iOS or Android. Provided on-demand, per-app microVPNs are activated only when they're needed, simplifying security while lowering data transfer costs and allowing better performance.

VMware Workspace ONE relies on a Unified Access Gateway per-app tunnel for connectivity. This approach requires MDM enrollment as well as a device-side VPN policy or client, increasing IT's administrative overhead and limiting the tool's suitability for BYOD. IT must also install a VPN client (VMware Tunnel) and VMware UAG with Tunnel component in the DMZ, adding further work and complexity for IT.

4. Integrated with the top digital workspace solution

Citrix Endpoint Management is designed with the understanding that UEM should be about much more than security and control. Closely integrated with Citrix Workspace, the top digital workplace solution, Citrix Endpoint Management gives employees ready access to all the apps and content they need to be productive, on any device, using a single identity and sign-on to get to work quickly and easily. Auto-discovery and an automated enrollment workflow for the Citrix Workspace app make it simple to get up and running.

Citrix Virtual Apps and Desktops provides all the same functionality on mobile devices as on desktop computers, with conditional access to virtual apps and desktops to ensure security in any scenario. Integrated troubleshooting tools help users diagnose and resolve any problems that arise with apps and sessions.

Citrix Content Collaboration integration with Citrix Endpoint Management includes secure access and editing for files and data, easy content sharing, and integrated workflows to help teams collaborate effectively using any device, anywhere.

Citrix ADC delivers a great experience with reliable performance wherever people work, for apps hosted anywhere, over any type of connection.

Citrix Analytics for Security strengthens protection for mobile users by providing insights into potential security breaches, risks to intellectual property, and other threats.

Security features	VMware	Citrix
Market leader in Content Collaboration and EFSS (enterprise file share and sync)		●
Using own encryption vault instead of leveraging device key chain		●
Appliance-only microVPN for enhanced sercurity with no app required on the device		●
microVPN tunnel for MAM only (no MDM)		●
Over 60+ MAM-only policies (no MDM)		●
Shared apps (not shared devices)		●
Derived credentials-based enrollment without domain password or MDM OTP		●
S/MIME support for the email client	●	●
Ability to co-author Office files directly from the EFSS web application		●

Conclusion

Your digital workspace solution is only as strong as its weakest component. To help employees do their best work using any device they choose, make sure the UEM solution you choose goes the extra mile for productivity and security. With capabilities VMware Workspace ONE can't match, Citrix Endpoint Management is the clear choice for the modern workforce.

To learn more about Citrix Workspace, go to citrix.com/workspace.

Enterprise Sales
North America | 800-424-8749
Worldwide | +1 408-790-8000

Locations
Corporate Headquarters | 851 Cypress Creek Road, Fort Lauderdale, FL 33309, United States
Silicon Valley | 4988 Great America Parkway, Santa Clara, CA 95054, United States