The Mobile Secure Workplace

Mobile, Secure Access to Applications and Data Across Devices and Locations

KEY BENEFITS

- Fast, policy-driven and location-aware access to data, applications and personalized desktops from a wide range of qualified devices
- Enhanced workplace mobility and support for BYOD and device diversity
- Centralized and streamlined desktop management reduces OpEx by up to 50 percent

A New Way to Work

Today's workforce is no longer tethered to traditional stationary desktops. New devices have proliferated companies of all sizes. Workers are increasingly mobile, and more than 60 percent of enterprise firms and 85 percent of SMB organizations are looking to initiate Bring Your Own Device (BYOD) programs. But while end users are embracing these trends, IT departments—faced with tight budgets—are struggling with how to best support and manage these new devices while protecting corporate data as it is accessed across networks and locations.

This is why finding a secure, streamlined and more cost-effective way to manage end users across devices and locations has become a top priority for so many customers today.

VMware has a solution. By virtualizing desktops and hosting them on VMware® vSphere®, a key component of VMware Horizon View™, and using a validated architectural design, organizations can now have unparalleled desktop and application access across devices and locations. With the VMware Horizon™ Mobile Secure Workplace, processes are automated and efficient, data is secure and the total cost of ownership is reduced by as much as 50 percent. And because this solution ties desktop environments to user identities instead of devices, end users are free to access their data and applications from any qualified device, whether in the office or halfway around the world.

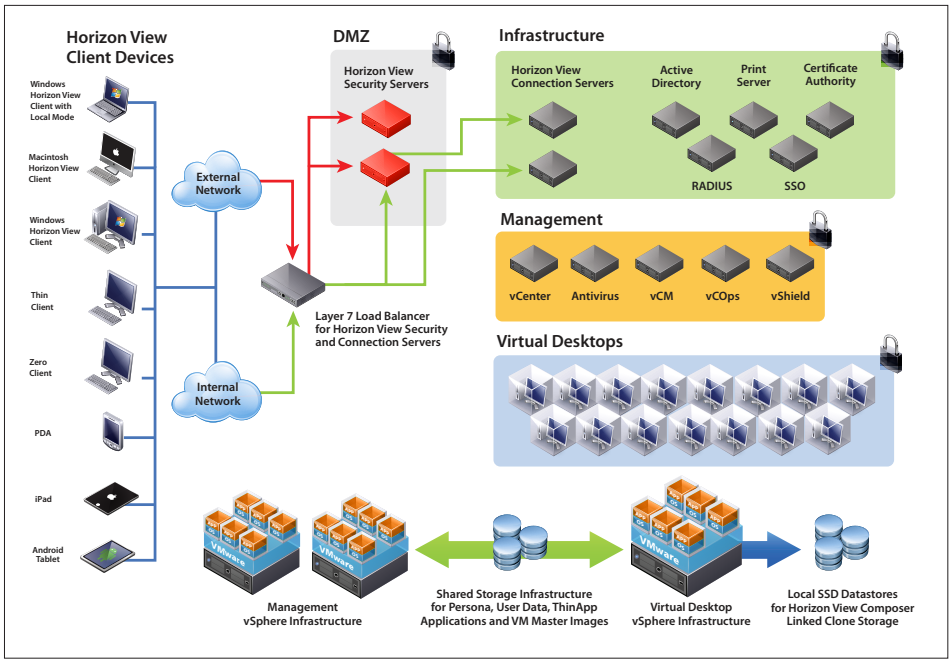

Figure 1: Mobile Secure Workplace Reference Architecture

The Mobile Secure Workplace Supports Device Diversity and BYOD Initiatives

This solution architecture provides an innovative way for IT to support device diversity and BYOD by improving user access and mobility, streamlining application updates, enhancing data security and delivering a high-quality user experience.

End-user access via two-factor authentication (RSA, RADIUS OTP tokens, and smart cards) ensures the connection from the Horizon View Client to the View Agent is fully encrypted. VMware vCloud® Networking and Security™ products, together with Horizon View and leading security vendor solutions, allow IT to offload AV to secure virtual machines and

"If you think about mobility today, it's really changed from just a few years ago. Wherever we are now is ubiquitous computing in a post-PC era. The PC and the Laptop used to be King of the Mountain and it really isn't anymore with the consumerization of IT and BYOD."

– Doug Cadell
CIO, Foley and Lardner

provide high levels of isolation between resource pools and networks. This allows IT to apply policies across virtual machines and pools of users.

vCenter™ Operations Manager™ for View provides analytic dashboards and end-to-end monitoring of desktops, users and network to help IT troubleshoot, trend and proactively address potential issues across the end-user environment in order to maximize uptime and compliance.

Mobile Secure Workplace with PCoIP™ additionally delivers end users a seamless experience across devices, networks and locations—and supports end users who may need applications, printing, unified communications and 3D graphics as part of their daily workspace.

And by leveraging desktops with persona management, the Mobile Secure Workplace ensures end users can carry their persona with them across sessions and devices for a more personalized desktop experience.

Solution Elements

The Mobile Secure Workplace is a validated solution architecture offered by VMware and VMware Ready Partners. It is specifically built to meet the needs of organizations looking to securely support end users across devices and locations. It combines VMware and ecosystem products and services to meet the necessary requirements for supporting security, rapid and automated provisioning and mobile access across devices. Key solution elements include:

VMware Horizon View
The cornerstone of the Mobile Secure Workplace solution, Horizon View modernizes desktops and applications by moving them into the cloud and delivering them as a managed service. With Horizon View and VMware ThinApp®, IT has the ability to grant or restrict access to desktops, data and applications based on endpoint device configuration, network location and user identity.

From the end user's perspective, Horizon View with Persona Management makes it possible to work from virtually any location using any qualified device to access their personal desktops—including corporate and personally owned PCs, thin clients, zero clients, iPads and other tablets. The user's familiar desktop appears across devices and locations with everything in the right place; with all authorized applications, files, and data available; and with everything functioning as expected.

vCenter Operations Manager for Horizon View
vCenter Operations Manager for Horizon View allows IT administrators to have broad insight into desktop performance, quickly pinpoint and troubleshoot issues, optimize resource utilization and proactively manage their desktop environment.

vCloud Networking and Security (vCNS) Platform
The vCNS suite of products, including vShield App™ and vShield Edge™, allow IT to effectively firewall virtual machines and partition networks and resource pools. With vShield App, IT can apply rules to virtual machines based on IP addresses as well as business or application requirements. vShield Edge allows for segmentation of resource pools and allows IT to provide a common set of services to virtual machines that reside within a defined perimeter.

Included in Horizon View, vShield Endpoint™ provides the intermediary for anti-malware and deep packet inspection. This allows IT to enhance endpoint performance across the desktop environment by offloading virus scanning to secure virtual machines—effectively eliminating the need to install complex antivirus agents inside each individual virtual machine.

Summary

The Mobile Secure Workplace from VMware is a managed solution that integrates technology from VMware and our partner ecosystem. The solution leverages mobile, wireless and wired networks, vCNS security services, and monitoring components—to better protect data and monitor IT infrastructure across locations.

This solution is optimized for organizations looking to drive higher levels of productivity by improving end-user access across devices and locations, reduce costs by streamlining desktop management, and enhance security and compliance.

Learn More about the Mobile Secure Workplace

For additional information about how the Mobile Secure Workplace solution is built and validated, read the Mobile Secure Workplace Reference Validation document at vmware.com.

Or call VMware for an assessment today. Our experts will help you determine the opportunity for your organization—and chart your course to mobile, secure desktop access. For more information or to purchase VMware products, call 1-877-4VMWARE (outside of North America dial +1-650-427-5000), or visit www.vmware.com/products, or search online for an authorized reseller.

vmware®

VMware, Inc. 3401 Hillview Avenue Palo Alto CA 94304 USA Tel 877-486-9273 Fax 650-427-5001 www.vmware.com
Copyright © 2013 VMware, Inc. All rights reserved. This product is protected by U.S. and international copyright and intellectual property laws. VMware products are covered by one or more patents listed at http://www.vmware.com/go/patents. VMware is a registered trademark or trademark of VMware, Inc. in the United States and/or other jurisdictions. All other marks and names mentioned herein may be trademarks of their respective companies. Item No: VMW-SB-MOBILESECWKPL-20130403-WEB