WHITE PAPER

GO BEYOND MOBILE DEVICE MANAGEMENT WITH A DIGITAL WORKSPACE

vmware®

Table of Contents

MOBILE DEVICE MANAGEMENT WAS DESIGNED TO:

- Protect the corporate network
- Optimize the functionality and security of mobile devices
- Allow IT administrators to control, secure, and enforce policies on phones, tablets, and other endpoints

On Its Own, Mobile Device Management Can't Deliver on Modern Demands

Ten years ago, smart devices began taking over the workplace. Employees began using them at the office, at home, and on the go, to get work done anytime, anywhere. IT created BYOD policies and implemented mobile device management (MDM) to keep them under control. This approach was crucial in helping with software distribution, service configuration, policy, security, and inventory management. With MDM, IT organizations could be confident that data and information were being accessed securely, even outside the office or on non-corporate-owned devices.

MDM served a great purpose when the number and type of smart devices were limited—but in a fast-moving, app-focused digital landscape, it simply isn't enough anymore.

Two Challenges, Two Solutions

When MDM was introduced, everyone thought mobile apps would be the future of work. And while they are extremely important, desktops are also still vital, creating two separate tracks that IT is still largely managing separately.

To keep up, IT organizations are taking one of two approaches:

1. Move to Unified Endpoint Management (UEM) and support any device, anywhere

PC management hasn't changed much in 20 years, but the way employees work is completely different. They're using desktops and mobile devices. Working at an office and remotely. Moving to UEM is an approach that secures and controls desktops, laptops, and mobile devices from a single unified console.

It works with MDM solutions; for instance, Apple and Microsoft added MDM APIs to Mac and Windows as they witnessed the scale and speed of MDM on iOS and Android.

2. Evolve an existing Enterprise Mobility Management (EMM) strategy to enable anytime app access

Users not only want access to data and information on any device—they also want all their apps, including new SaaS services, internal web apps, native apps, and even Windows apps, to be available on all of those devices. Essentially, they want their desktops to be portable, going wherever they go, on whatever device they decide to bring with them.

But while internal client-server apps leverage Active Directory and Kerberos, SaaS apps have their own user directories and authentication schemes, and native apps require identity certificates for local authentication. But that complexity must be invisible to the modern worker. They want a consumer-simple experience that allows them to access all applications, anywhere, with a single sign-in.

Mobile Device Management Is Not a Complete Solution for Modern Workers

At a time when expectations are ramping up, applications are driving business, and threats are becoming more sophisticated, managing devices simply isn't enough on its own.

Traditional methods of deploying applications to an end-user environment and locking down mobile devices is both complex and extremely hard to manage. Yet for most IT organizations, complexity is the enemy. They're looking for ways to simplify day-to-day operations while strengthening security and improving the user experience.

MDM isn't extinct—but what will it look like in the future?

IT ORGANIZATIONS NEED TO CONSIDER MULTIPLE FACTORS:

- **End users expect consumer-like experiences.** The days of complex log-ins, separate passwords, and rigid device management are over. Workers need quick, simple access to applications and data so they can do their jobs more efficiently.
- **Diverse endpoints all require management.** There are more devices than ever—and IT must ensure that data and apps remain secure. They need to manage everything, while ensuring peak performance and allowing users to access information anytime, anywhere.
- **Silos impede the agility that modern business requires.** The silos in traditional data centers keep applications from moving seamlessly across environments. They also impede IT visibility, making it difficult to identify and stop security threats or other performance issues.

Times Are Changing

Thanks to digital transformation, workplace environments are more dynamic and unpredictable than ever before, as employees and businesses explore new ways to work and attract customers.

Driven by mobile and cloud technologies, consumer devices and application experiences are shaping how businesses grow. Employee expectations are changing, creating new application demands and providing opportunities to change outdated business processes.

Toward a Single, Integrated Platform

To handle all of these changes and expectations, IT organizations need a platform that collapses the traditional silos between mobile, desktop, and even line-of-business application management. With this approach, MDM becomes part of a larger digital workspace strategy designed to meet new requirements and accommodate future ones.

From Many Solutions to One

A digital workspace reduces IT complexity with a unified approach that combines delivery models, centralizes management and security, and supports a wide variety of endpoint devices. It fulfills the promise of MDM, while allowing you to accomplish a whole lot more. With a digital workspace, you can:

ENABLE FLEXIBLE, CONSUMER-SIMPLE USER EXPERIENCES	PROVIDE CAPABILITIES THAT SUPPORT DIGITAL BUSINESS
Out-of-the-box enrollment. Users don't have to wait for an IT professional to set up their device or give them access to apps. They can start working within minutes.	**Enterprise-grade security.** Stay on top of existing and emerging security threats with granular protection that follows workloads everywhere.
Single sign-on. With just one username and password, workers can access all their applications. Different apps don't require complicated credentials that take away from important mobile moments.	**Compliance and automated remediation.** Ensure that apps stay in compliance, wherever they are, with embedded policies.
Self-service. When users need something, they can quickly access a portal and solve issues themselves without putting in a ticket or waiting for IT support.	**Intelligence and insight.** Get a clear view into application behavior, location, and activity.
BYOD. Workers can move from device to device without compromising security or performance.	**Automation.** Free up valuable time for IT by automating otherwise complex, manual processes.
Remote, nontraditional workers. Contractors, consultants, and partners can all have the same level of support without having to hire additional IT staff.	

How to Evaluate Digital Workspace Solutions

As you explore building a digital workspace for your organization, use these **5 key questions** to guide your evaluation process.

Does the solution put employees first?

Today, employees must be the focus of every business imperative. You can empower people, employees, teams, and lines of business to work when, where, and how they choose, with secure and seamless access to applications on any device. The digital workspace helps your employees work without restriction, so you can drive your business forward.

Does the solution support any application, anywhere?

Your IT organization needs the ability to simply and securely deliver and manage any app, on any device. This includes:

- All types of apps, including cloud, native, internal, Windows, and virtual
- Different identity stores, providers, and directories
- Leveraging existing investments that still have value

Does the solution enable modern management?

The ability to securely manage modern operating systems from the cloud is key to productivity and efficiency. Apple, Google, Microsoft, and Samsung all agree: It's the way every single device, regardless of ownership, will be managed in the future.

For devices currently managed by MDM, organizations must fill the gaps between OS MDM APIs and traditional PC management capabilities. Many enterprises won't unify management simply for the sake of unification because often, there isn't enough depth to support such an initiative. IT can't afford to lose any management capabilities.

Does the solution provide comprehensive insights?

You need insights to help you understand your employees' entire digital environment. Modern devices and apps can log thousands of points of data, so merely running a report or looking up logs isn't good enough. Artificial intelligence and machine learning tools are required to provide real insights on performance, security, risk, usage, and adoption.

Does the solution automate labor-intensive tasks?

While insights are critical, if the response to those findings requires manual intervention, your IT team will still be in reactive mode. A digital workspace must automate common, labor-intensive tasks like provisioning new apps or entire devices, but it must also auto-remediate conditions where devices become out of compliance or risk scores become too high. This doesn't mean you have to deny access—rather, it puts the employee in the driver's seat and avoids policies that leave workers without the tools they need to do their jobs.

The VMware Approach to the Digital Workspace

Your IT organization needs a partner that understands the challenges and benefits of the digital workspace—and is prepared to support you through all of them.

VMware helps you achieve the full benefits of consumer device and application innovation with a digital workspace that delivers both high-quality customer experiences and security. VMware Workspace ONE™ is a digital workspace platform powered by VMware AirWatch® that integrates access control, application management, and multi-platform endpoint management into one streamlined solution.

With Workspace ONE, you can securely and reliably deliver the apps and data that your employees need—on any device, at any time. It helps you put employees first, meeting rising expectations while securing data and information in a perimeter-free world. If you're ready to evolve your MDM solution to one that meets modern needs, VMware can help you make the journey.

GET STARTED

Learn more about Workspace ONE >

Try a Workspace ONE Hands-on Lab >

Join Us Online:

VMware, Inc. 3401 Hillview Avenue Palo Alto CA 94304 USA Tel 877-486-9273 Fax 650-427-5001 www.vmware.com
 Item No: EDW-0911_VM_Go-Beyond-Mobile-Device-Management-With-A-Digital-Workspace_WP_080318
8/18