FULFILLING THE PROMISE OF THE DIGITAL WORKSPACE

Bringing workers, applications and devices together seamlessly
# Table of Contents

## Introduction

## Challenge

## The Future

## Audiences

- IT
- Line of Business
- End Users

## Benefits

- Identity management
- Unified endpoint management and security
- Delivering Windows as a Service
- Mobile productivity apps

## VMware Workspace ONE

### Portfolio

- Socialcast by VMware
- VMware AirWatch
- VMware AirWatch Content Locker
- VMware App Volumes
- VMware Boxer
- VMware Horizon 7
- VMware Horizon Air
- VMware Horizon Air Hybrid-Mode
- VMware Identity Manager
- VMware TrustPoint

### Industries

- Healthcare
- Retail
- Financial Services
- Manufacturing
- Government
- Education

### Editions

**Test Drive**
The varying demands on the digital world.

There’s no denying that today’s workforce is “mobile.” Inspired by the ease and simplicity of their own personal devices, today’s workforce relies on a variety of tools to accomplish their business tasks — desktops, smart phones, tablets, laptops or other connected devices — each with varying operating systems.

The specific tasks they need to accomplish? That depends on the person. But it’s safe to say remotely logging in and out of legacy, desktop, mobile, software-as-a-service (SaaS) and cloud applications is a given.

And the devices on which they work? They could be owned by the enterprise or the end user, with varying levels of company oversight, security and management. The result? An overabundance of “flexibility” that leads to fundamental IT challenges of security and manageability.

The global mobile workforce is set to increase from **1.32 billion** in 2014 to **1.75 billion** in 2020.¹

Consumer Simple and Enterprise Secure.

People are accustomed to easy-to-use devices, like the Samsung™ Android phone or the Apple® iPad®. They also routinely interact with applications like Netflix™ that are extremely simple to navigate. But often, their experience at work can be radically different. In the business world, companies take full advantage of software that is extremely secure, like SAP®, WorkDay™ and Salesforce. Yet these are not always easy to use — or access.

Given the trends of mobile workers and the state of innovation across the industry, the market requires a new model. One that:

- Defines how users leverage applications, information and resources across their portfolio of devices.

- Emphasizes how IT delivers, manages and secures these applications and services.

- Enables businesses to capitalize on new capabilities and styles of work to drive increased business results.
Consumer Simple and Enterprise Secure.

“Consumer simplicity has to make its way to the enterprise world. People expect a simple user experience. And when consumer simplicity meets enterprise security, you get magic. That’s what we’re trying to deliver in the digital workspace.”

— Sanjay Poonen, EVP and GM, End-User Computing, Head of Global Marketing and Communications, VMware
The digital workspace of the future.

Just as the desktop became the dominant, defining model for end-user computing during the client-server era, the digital workspace will be the model for end-user computing in the mobile-cloud era. But in order for the digital workspace to become a trusted infrastructure, it must truly meet the needs of mobile workers and their associated enterprises. It has to enhance the end-user experience and simplify IT management while preserving the reliability and security aspects required for business-critical applications and protection of sensitive corporate data.

It’s a rigorous balancing act that few companies can deliver, but one of critical importance to everyone involved. It’s a balancing act made possible by VMware® Workspace™ ONE™.

“I think that over time, the digital workspace will dominate how people think of computing.”

— Austin Park, principal consultant, Louisiana Children’s Medical Center
Who benefits from a digital workspace?

**VMware Workspace ONE** was created to help multiple audiences with multiple challenges to achieve multiple goals:

- **IT**
- **Line of Business**
- **End Users**
For IT.

Their goal? Simply and securely deliver technology, and safeguard data and applications across devices. Being able to centralize identity, maintain control and service their distributed workforces through a unified platform would certainly make their lives easier. And if they’re able to change the conversation with *lines of business*? All the better.

Nearly **70%** of global technology security decision-makers place a high or critical priority on enabling employee productivity with improved mobile security capabilities and services.²

²Forrester Research, Data Wrapping Promises Strong Mobile Data Security and a Positive User Experience, January 2015
For the lines of business.

Their goal? **End users** that are productive, engaged and collaborative. In order to make that happen, their team members need easy, consistent access to the SaaS and corporate applications that make them effective — from apps run centrally and displayed on a browser-based device to third-party or on-premises business critical applications such as Salesforce or SAP.
For end users.

Their goal? The applications they need, when they need them, on the devices they choose to carry. And if they can't get what they want on a corporate-deployed device, they'll use their own. After all, being successful for them is all about getting their job done quickly and well.

69% of employees admit to using their own mobile devices for work.\(^3\)
How people, places and productivity meld.

Because every business is different, the benefits of the digital workspace are different for every business. But there are some things almost every business needs, such as:

- **Identity management**
- **Unified endpoint management and security**
- **Delivering Windows as a Service**
- **Mobile productivity apps**
Are you who you say you are?

In the past, when individual PCs operated independently of a network, a simple password was the standard for end users to prove who they were. Today, because of mobile-cloud emergence, the number of users, accounts and access points to the network have exploded. Systems are no longer tied to a single device or network, so authenticating who has access to what is of critical importance. IT is no longer tasked with solely tracking a domain login for full access, as every service may require individual authentication. In fact, IT is finding it is no longer the only gatekeeper. Because network access happens through remote devices that are often user-owned, IT is challenged to manage access to resources when the resource itself isn’t managed by IT.

Enter identity management. Because it is practically impossible for IT to source all of the needs of so many disparate systems, identity management enables users to prove they are who they say they are — through methods that are easily and automatically verified as part of the process. Traditionally, identity management occurred in silos with policies tied to a single directory. With the digital workspace approach, each app has its own directory, so identity functions across all systems.
Deliver any application.

As soon as a user is authenticated through VMware Workspace ONE, they can immediately access their personalized enterprise app catalog and subscribe to virtually any mobile, Cloud or Windows app, including:

- Internal web apps through a secured browser and seamless VPN tunnel
- SaaS apps with SAML-based SSO and provisioning framework
- Native public mobile apps through brokerage of public app stores
- Internally developed mobile apps secured through the AirWatch SDK
- Modern Windows apps through the Windows Business Store
- Legacy Windows apps through MSI package delivery or real-time delivery with App Volumes
Additionally, users can isolate problematic Windows apps through App Volumes isolation mode (ThinApp), secure sensitive systems of record apps, and deliver complete virtualized managed desktops and data centers by hosting with VMware Horizon Air (either in the data center or in the cloud).

**Conditional access.**

For starters, there’s policy enforcement that combines identity and mobility management to mobile, web, and Windows apps on a per-application basis — all configured through VMware Identity Manager. Companies can impose authentication strength and restrict user access via either network scope or through device restrictions (rooted devices, using app blacklists, geolocation and others) implemented by AirWatch.

**Self-service app catalog.**

Change the way you handle employee onboarding with a complete, self-service enterprise app catalog that can be effortlessly adapted and branded for your business.
Single Sign On.

With the built-in VMware Identity Manager, Single-Sign On authentication is already recognized on employees’ devices, putting access to applications just a click away. You’ll be able to eliminate the need for convoluted logins by creating trust between users and devices. You can also upgrade to unified biometric or other multi-factor authentication methods for more vital applications.

One-touch access.

When an employee unlocks a registered, unique device using local PIN or biometric services, they only need to touch an app to keep it open for as long as the authentication window is set.

Authentication brokerage.

This feature leverages existing and new methods of third-party authentication, supporting services such as Radius, Symantec, RSA SecureID, Imprivata Touch and Go, and others.
Adaptive enrollment.

Designed to maximize usage for even the most security-sensitive companies. VMware Workspace ONE permits employees to adopt BYOD programs by putting control in their hands. They can decide what level of access and corresponding management they need.

Shrink-wrapped device provisioning.

Allows users to self-configure their laptops, tablets and smartphones for instant enterprise use by leveraging OS management interfaces. It leaves configuration and app management to IT, while allowing devices to receive OS patches directly from the vendor for the quickest response to vulnerabilities.

“Mobile is going to be a huge differentiator for us as we strive to be the best we possibly can be at customer service. The interconnected world that we live in is going to continue to drive new ways of interacting with our customers and we have to be ready for that.”

— Mike Guhl, VP store and credit systems, Home Depot
Out of reach, but not out of control.

As differences between desktops, laptops and mobile devices blur, companies need to look at the bigger picture. To truly be future ready, instead of focusing on form factor, they are designing ubiquitous mobile platforms with enterprise and ability management APIs that can manage anything within an operating system stack.

As a result, IT now has to find a centralized way to maintain policy and management based on varying levels of potential risk. What types of information or applications can be accessed? Where is the user? What type of device do they have? What other security measures are necessary?
Device management and compliance.

After that, there’s automated device compliance to protect against data leakage, including protection against rooted or jailbroken devices, whitelist and blacklist apps, open-in app restrictions, cut/copy/paste restrictions, geofencing, network configuration and a range of advanced restrictions and policies — all enforced through the AirWatch policy engine.

App and device analytics.

You can also monitor systems in real time by recording application, device and console events, viewing logs in the console, or exporting pre-defined reports.
Intelligent network.

Finally, you can now further segregate traffic from applications to specific workloads in the data center through the added capability of VMware NSX with AirWatch tunnel. This considerably decreases the possibility of attacks by viruses or malware which could do major damage to an organization.

“...

We want to be able to say ‘We can enable you on any device, anywhere, any time’ to our employees and AirWatch provides the user experience that allows us to do that.

— Al Mackay, global IT mobility lead, AstraZeneca

“...”
Windows apps and desktops, reimagined.

As recently as two or three years ago, any new application developed would be written for the web. All you needed was a browser and you could access any application. But with the advent of mobile devices that cache and store information internally, everything changed. Native applications have become the requirement again, providing immediate access and usage even when not connected to a network. But with the resulting lack of centralized control, having IT be the app gatekeeper can be problematic.

The success of an application partly depends on the success of the underlying operating system. When PCs were the only devices, having a single version of Windows simplified application development, delivery and management. But as platforms and device types diversified, developers faced a choice of competing platforms. APIs were not unified across mobile, desktop and embedded versions of Windows. And, despite the emergence of web and mobile proliferation, legacy apps still need to be managed and assets still need to be delivered to all applications across operating systems and devices.

The beauty of desktop virtualization? Customers can seamlessly make that transition, as well as providing new apps.
Legacy apps.

Despite the emergence of web and mobile proliferation, people still need to manage legacy apps. Businesses need to get assets to all applications across operating systems and devices. The beauty of desktop virtualization is that customers can seamlessly make that transition, as well as provide new apps. And with VMware Workspace ONE, that also includes mobile apps.

Efficient desktop management.

Virtual desktops and apps that allow Windows to be delivered as a service ensure that IT can now easily support end users, maximize productivity and keep costs under control. What’s more, organizations now have the flexibility and freedom to take advantage of desktop and application on-premises, as a cloud service, or via a hybrid deployment model. Organizations can simply choose the model that best meets their budgets and use cases.
Seamless desktop and application virtualization.

When done well, unified application and user management can improve employee productivity and streamline day-to-day management. A simplified application lifecycle management approach can relieve IT of unnecessary steps in the app delivery, update, and retirement process. Additionally, providing contextual profile and policy management alongside application management ensures that end users have a consistently great experience across a range of devices and locations. And finally, proactive application and desktop monitoring can further reduce support costs and improve user experience.
How efficiently can you work from there?

Take, for example, email. There’s no denying that it’s a driver for business productivity. And while end-user devices are fully capable of providing email availability and accessibility, the level of functionality they enable is dramatically below that of a true business experience. These apps do not provide a consumer simple, enterprise secure experience because they were never designed for business.

Consider the amount of email required to schedule a meeting. True mobile collaboration would allow a recipient to see any incoming messages regarding the meeting, then immediately propose a date with the full capabilities — as if they were seated in front of a desktop running Outlook. This increased functionality might also allow a user to swipe across a message and take action through enterprise integrations — without having to jump through four links and loads, not to mention numerous sign-ins.

"We wanted to create a digital workspace in a way that was easy and natural for everyone, whether our employees had previous digital experience or not. Workspace ONE has helped us make that happen."

— Per Brantsing Karlsson, CIO, Akademiska Hus

Next >
Consumer simple email app.

Designed for business but still a hit with consumers, our faster, smarter email app supports Gmail, Outlook, Exchange, Hotmail, Yahoo, iCloud, Office 365, IMAP and POP3 mail accounts. Featuring secure integrations with services like Dropbox, Box and Evernote, it’s simpler than ever to stay structured.

Integrated calendar.

By integrating their email app with their calendar, end users won’t have to leave their email to respond to a meeting invitation. With just a couple of clicks, they can review and reply to any meeting request without having to jump between apps.

Advanced email attachment security.

Now users can also enforce enterprise encryption and reduce data outflow with the AirWatch Secure Email Gateway.

Content management app.

The latest, most up-to-date information will be at employees’ fingertips with AirWatch Content Locker. Files get delivered straight to devices across a range of internal repositories and external cloud storage providers.
Enterprise chat and social.

Increase employee engagement through Socialcast, the secure enterprise chat platform that bridges systems of record by integrating into existing enterprise applications while offering the ability to personalize mobile-first chat and notification experience.

“When you think about where we’re going from a Horizon Desktop standpoint, where I would have had an army of field technicians taking care of those desktops, now it’s basically eight guys that will be managing that environment. Our mission statement is very simple, and that is to ‘help people get better.’ Sprint believes that mobile connectivity is the most powerful enabler in the world today.”

— Joe Hamblin, Director of Emerging Platforms, Sprint

For today’s digital workspace to truly enable mobile workers, it has to combine all devices, applications and services required by users — securely managed and unified by common access and identity. It’s a tall order for IT and for end users. But it’s one delivered by VMware Workspace ONE.
The integration of application and device.

VMware Workspace ONE is the simple and secure enterprise platform that delivers and manages any app on any smartphone, tablet or laptop. Redefining mobile productivity and collaboration, it gives end users a secure, unified consumer experience on any device. So they can focus on the work to be done, not the technology in their hands. It also gives IT the means to control access, increase security and automate employee onboarding and offboarding in a way that is scalable, manageable and therefore cost efficient.

By integrating identity management, real-time application delivery and enterprise mobility management, VMWare Workspace ONE not only engages digital employees, it reduces the threat of data leakage and modernizes traditional IT operations. Tightly integrating all these competencies, VMware Workspace ONE helps organizations embrace the mobile-cloud era and drive business mobility with a truly digital workspace that meets the needs of their business.
When you think about a business making the shift to a digital workspace, consider all that it involves:

- Becoming more digital.
- Making manual processes more automated.
- Making paper processes more mobile-driven.

It’s digital transformation, and it’s all part of VMware’s digital workspace proposition. See how we helped the American Red Cross.
A comprehensive portfolio to be proud of.

**VMware Workspace ONE** combines identity and mobility management to provide frictionless and secure access to all the apps and data employees need to work, addressing the broadest set of challenges your organization faces — not just today but in the future. Enable your digital workspace via:

- **Socialcast by VMware**
- **VMware AirWatch**
- **VMware AirWatch Content Locker**
- **VMware App Volumes**
- **VMware Boxer**
- **VMware Horizon 7**
- **VMWare Horizon Air**
- **VMWare Horizon Air Hybrid-Mode**
- **VMware Identity Manager**
- **VMware TrustPoint**
Socialcast by VMware

A new means of enterprise collaboration, Socialcast frees end users from the old device-centric computing era and unites people, applications and data in real-time — whether behind a firewall or in the cloud. Socialcast enables instant secure collaboration across business systems and regular communication channels.
VMware AirWatch

Allows **IT** to administer the entire lifecycle of any endpoint, across all major operating systems, in a single management console. This enterprise mobility platform provides superior access to business apps with integral security for employee productivity – and covers everything from enterprise email, calendar and contacts to browsers, content and social networking.
VMware AirWatch Content Locker

Integrated and protected access safeguards sensitive content in a corporate container and provides users with a central application to securely access, store, update and distribute documents from their mobile devices.
VMware App Volumes

Removes the stress of application packaging with application and user management solutions that can lower storage and operational expenditures. App Volumes’ proactive monitoring reduces IT costs by up to 70% — all the while offering your users a personalized, reliable and consistent experience.
VMware Boxer

Access corporate email in an intuitive, secure container. Boxer is a mail, calendar and contacts app that provides both a stellar user experience as well as enterprise-grade security and management.
VMware Horizon 7

Brings the virtues of the mobile cloud to virtual desktops and apps, with greater speed, performance and security than ever before. Horizon 7 uses Instant Clone Technology to rapidly generate new desktops for users that retain their original customizations from session to session, even while the previous desktop is destroyed every time the user logs out.
VMware Horizon Air

A cloud service that permits end users to access their desktops and apps from any device or browser securely — and allows IT to manage the deployment using existing skills and tools. It’s a rich desktop experience that provides instant, secure access to corporate data and applications from any device, anywhere.
VMware Horizon Air Hybrid-Mode

Our current solution combining Horizon 7 and Horizon Air also provides for the delivery of desktops from both on-premises and the cloud to a user via a single client. This is a unique attribute of the solution because it allows users to easily work on desktops that can be delivered from multiple locations and potentially by different providers.
VMware Identity Manager

Provides application provisioning, self-service catalog, conditional access controls and Single Sign-On (SSO) for SaaS, web, cloud and native mobile applications. Establish trust between users, devices and the hybrid cloud for a seamless user experience and powerful conditional access controls.
VMware TrustPoint

Provides complete endpoint visibility and control with next-generation threat detection and remediation at unparalleled speed and scalability.
The Digital Workspace in Action

Other teams across many industries have implemented the digital workspace to improve their data security, identity, end-user mobility and Windows app. See for yourself how it has been done in:

- Healthcare
- Retail
- Financial Services
- Manufacturing
- Government
- Education
Healthcare

- **Goal:** Improve patient outcomes by enabling secure access to health records.

- **Challenge:** Reliable mobile access to patient care applications and information can have life-or-death consequences.

- **Traditional IT outcome:** Slow logins, poor images and sluggish application performance negatively impacts a clinician’s ability to rapidly respond to changing care conditions.

- **Digital workspace outcome:** The digital workspace delivers secure, rapid access to critical information and applications (including EHRs) on any device. Through centralized and secure desktop and application management, IT can improve care team collaboration and response time while simultaneously protecting data.
Retail

- **Goal:** Drive customer engagement through improved associate productivity.

- **Challenge:** Associates represent the brand. When consumers experience slow and impersonal service, they feel the company is inefficient; when they experience rapid inventory checks and don’t have to wait in long checkout lines, they think just the opposite.

- **Traditional IT outcome:** Traditional workflows — from paper-based inventory reporting to cash-register lines — negatively impact retail associate efficiency.

- **Digital workspace outcome:** For associates whose workspace is primarily outside an office, the digital workspace solution enables secure remote access to the full suite of applications. This, in turn, delivers new levels of user productivity, efficiency and service delivery. Increased associate engagement leads to improved customer service, which reduces costs and drives profitability.
Financial services

- **Goal**: Ensure that security and compliance meet industry requirements.

- **Challenge**: Financial institutions face increasing internal and external threats to data security across networks, applications and mobile devices, including cyberattacks, malware infection and theft of customer information.

- **Traditional IT outcome**: Without proper protection on users’ desktops and mobile devices, financial services organizations can’t prevent sophisticated data breaches and theft. With so many applications, devices and user types operating within a complex computing landscape, firms are discovering that they need to adopt more advanced data security measures.

- **Digital workspace outcome**: Identity, EMM and VDI solutions radically harden data security across applications and devices. Centralized management, streamlined application patching and updates, automated compliance checks, role-based access controls, remote device wipe, multifactor authentication and smart card support are among the advanced security features the digital workspace offers.
Manufacturing

- **Goal:** Continuity of operations.

- **Challenge:** Manufacturing operations stall in the face of natural disasters, power outages and cybersecurity breaches.

- **Traditional IT outcome:** In cases of unplanned downtime or emergency, traditional desktop infrastructure inhibits access to data and applications. For some organizations, a computing environment disruption can seriously affect safety, while for others, an office closure causes significant losses in workforce productivity.

- **Digital workspace outcome:** By eliminating dependencies on physical systems, the digital workspace supports continuity of operations and disaster recovery goals by giving employees full access to mission-critical data and applications outside the office.
Government

- **Goal:** Improve first response.

- **Challenge:** Every second counts for first responders. When apps are used to notify mobile users of event details in real-time, incident planning and resolution are greatly improved.

- **Traditional IT outcome:** Without mobile access to real-time event details, first responders lack contextual information that can greatly affect outcomes. For desk-bound dispatchers, sluggish legacy desktop systems reduce efficiency and performance while increasing latency. For IT, elevated data security concerns from unpatched systems, as well as higher system equipment and maintenance costs, leave little time for innovation.

- **Digital workspace outcome:** First responders gain real-time mobile access to mission-critical applications, including Windows and legacy applications, computer-aided dispatch and 3D geographical information systems, along with increasing situational awareness and more efficient resource allocation. Responders can also capture and send data, photos and videos from incident sites securely while maintaining compliance with criminal justice information services.
Education

• **Goal:** Enable limitless learning through bring your own (BYO) anything policies.

• **Challenge:** Students and educators now rely on a variety of computing devices to support their learning and teaching requirements.

• **Traditional IT outcome:** Traditional desktop infrastructure inhibits any time, anywhere learning, providing inconsistent learning environments across locations and negatively impacting digital equality.

• **Digital workspace outcome:** By removing dependencies on physical systems, the digital workspace provides full access based on user identity to all of the educational resources required.
No matter your goal, **VMware Workspace ONE** has an edition that works for you.

VMware Workspace ONE is available in three different end-user versions:

1. **VMware Workspace ONE Standard.** It’s all about the application delivery. Regardless of which device you’re using, you need a consistent way of getting to your applications, and VMware Workspace ONE Standard gives you the confidence of knowing that every email and chat is secure.

2. **VMware Workspace ONE Advanced.** For when you need to oversee the compliance of the device. Whether for security reasons or because you’re going to manage your device inside your organization, the management interface of VMware Workspace ONE Advanced gives you the control you need.

3. **VMware Workspace ONE Enterprise.** This is where you can layer on all the virtual apps and desktops you require. VMware Workspace ONE Enterprise assures you ultimate security and operational control, regardless of which device type you choose to employ.
Test drive VMware Workspace ONE now

See how easy it can be to bring workers, applications and devices together seamlessly. There’s never been a better time!

Workspace ONE Hands-on Labs