

# DELIVER EXCEPTIONAL CUSTOMER EXPERIENCES

Empower Employees with a Digital Workspace for Financial Services to Increase Customer Wallet Share and Boost Workforce Productivity

## OVERVIEW

The consumerization of IT is forcing financial services organizations to reimagine how they deliver services. The VMware Secure Digital Workspace for Financial Services empowers employees to more effectively and efficiently engage customers through secure, remote access to resources and data across devices, locations, and applications.

## BENEFITS

- Simplify application and data access and management
- Enable digital bank services anytime, anywhere
- Reduce costs while modernizing call center infrastructure

## Embrace a Digital-First Mindset

Delivering mobile services is critical to customer engagement in the 21st century and is an integral component of digital transformation. Whether services are rendered in a brick and mortar branch or in a location outside the branch, financial services organizations must provide employees with secure access to resources and data to accelerate client response times and deliver excellent customer service.

The digital workspace is the defining model for end-user computing in the mobile cloud era, securely delivering anytime, anywhere access to any application on any device on any platform, including desktops, remote laptops, smartphones, and tablets. Financial services IT teams delivering the digital workspace enable users to gain the greatest benefit by providing them with access to increasingly diverse and heterogeneous applications from multiple devices. The digital workspace advances the early concepts of the client-server era desktop to give IT a more efficient, centralized, and simplified way of managing devices and applications while providing employees with a way to seamlessly access all their business resources across device types.

A key element of the digital workspace is that it takes inspiration from the advances in consumer technologies to enhance the end-user experience and simplify IT management while preserving the reliability and security aspects required to protect business-critical financial applications and sensitive customer data. The notion of consumer simple – enterprise secure is a central pillar of the digital workspace. Using the digital workspace, employees such as personal bankers, roaming branch staff, and loan agents can provide customer service while “on the move” by accessing a single aggregated workspace, securely delivered on any device, without compromising any sensitive customer information.

## Trends Point to the Need for Greater Personalization

Similar service offerings make it difficult for customers today to differentiate between banks and other financial services providers. Without digital customer engagement, many bank/customer relationships will be relegated to a commodity service relationship, based solely on price, with little room for brand or service quality. As banks compete to become the primary custodian of customers' wider financial relationships, a key strategy will be better digital banking capabilities. Payment Services Directive 2 (PSD2) in Europe will accelerate open banking and be a catalyst for innovation in the payment operations and services offered by banks. Although analysts anticipate slow initial adoption, many believe retail banking customers will experience some benefit.

### Simplify Application and Data Access and Management

Today, financial services organizations are leveraging VMware digital workspace solutions to provide employees with access to the resources and information they need to accelerate client response times. Because of VMware technology, employees can more effectively and efficiently serve customers through secure, remote access to resources and data across devices, locations, and applications. The Digital Workspace for Financial Services, powered by VMware Workspace ONE™, integrates identity, application, and enterprise mobility management (EMM) to securely deliver and manage any application on any device. It improves service delivery and competitive advantage by increasing employee productivity, morale, and retention. Support for single sign-on (SSO) ensures staff have fast, easy, self-service access to all the apps they need at once without having to log in to each one and remember a unique password. A wealth manager, for example, can install and view a variety of market-related apps without filing a help-desk ticket with IT.

A privately-owned investment management firm recently empowered employees to serve institutional clients, shareholders, and retirement plan participants anytime, anywhere with reassurance to all that always-on access did not mean compromising security. Since deploying the Digital Workspace for Financial Services, the firm has been providing frictionless and secure access to all the apps and data employees need to work, wherever, whenever, and from whatever device they choose. The VMware solution enabled the firm's IT staff to define identity and device-based policies to enforce access decisions based on authentication strength, data sensitivity, user location, and device compliance; automate security for the firm's bring-your-own device (BYOD) initiative with secure and conditional access to sensitive applications and data; and remove the friction of access security with one-touch convenience.

### Enable Digital Bank Services Anytime, Anywhere

Banks can increase engagement by connecting both customers and workforces to resources on the devices that they prefer (e.g., Android, iOS, QNX, Tizen, Windows CE, and Windows 10). An identity-defined app catalog enables seamless access to any app—from mobile cloud apps to new and traditional Windows apps—across mobile devices. Contextual access management protects data with identity and device-based policies that enforce access decisions based on authentication strength, data sensitivity, user location, device compliance, and more. Two-factor authentication is enabled via smart cards, derived credentials, biometrics, and more. IT can protect against data leakage with an automated compliance engine that solves for rooted or jailbroken devices, restricts access based on the location of the device, and prevents copy/paste and sharing of data across apps. Policy automation improves security and eliminates time-consuming, resource-intensive tasks. For example, IT can enforce access and data policies across all apps, devices, and locations in one place, or provision a new laptop, out of the box, in minutes.

For example, Australia and New Zealand Banking Group (ANZ Bank) takes banking mobile with dozens of apps created for customers and employees. ANZ Bank deployed an internal app store for employees that scales and provisions apps quickly to employees. ANZ Bank has specific requirements about keeping customer data and corporate data secure, including requirements from regulators, making VMware's enterprise security model a must-have capability. At ANZ Bank, mobility provides simple, intuitive transactions at a kiosk inside the bank branch or with an employee outside of the branch.

Across mobile devices, laptops, workstations and PCs, virtual desktop infrastructure (VDI) enables employees with a secure, consistent, high-performance (e.g., 2D and 3D graphics), highly available, and highly reliable computing environment across desktop PCs and mobile devices while ensuring IT maintains centralized control over application and data access. VMware Horizon® not only reduces IT operational expenses, but it also speeds desktop delivery, reduces computing and storage costs, ensures painless application packaging and installation, improves the consistency of operations, and strengthens data loss prevention.

ABN-AMRO Bank N.V. Singapore, for example, enabled workforce mobility with VDI, securing virtual desktops with a virtual DMZ that allows bank employees to work on the go. Now advisors can securely and seamlessly access market feeds, client portfolio details, and account information on any device, from any location, without compromising client data. VDI helps ensure financial advisors have what they need to stay connected to their clients and always be productive.

### Support Call Center Modernization

With VMware solutions, financial services IT teams can completely transform application delivery—updating legacy teller and call center desktops to modern experiences. At the same time, IT can support bring-your-own device (BYOD) and choose-your-own device (CYOD) models, managing mobile devices and users from a single platform with VMware AirWatch®.

The transformation of application and endpoint management—including Windows 10—happens with VMware AirWatch Unified Endpoint Management which delivers virtualized Windows apps and full desktops across networks and non-Windows devices. Built on industry-leading AirWatch technology, Unified Endpoint Management innovates traditional PC lifecycle management by adopting EMM as the standard management tool for any device running Windows 10. IT can manage, monitor, and support all desktops and devices in a single, secure solution. They can configure accounts, deploy security patches, install software, and distribute classic desktop and modern apps over-the-air.

Financial institutions are leveraging both VDI and VMware App Volumes® to modernize call centers, improving app access and reducing management, delivery, upgrade, and maintenance costs throughout app lifecycles. VMware App Volumes transforms application delivery and management with a just-in-time application delivery and lifecycle management model that disaggregates IT-managed applications and user-installed applications from the operating system. This dynamic delivery of apps in seconds' results in increased engagement and enhanced security. Moreover, VMware solutions reduce storage capacity requirements by 70 percent without impacting network and compute resources, and reduce the number of images being managed by up to 95 percent by simplifying application delivery and management.

The addition of VMware Mirage® further enables financial institutions to automate backup and recovery and ease Windows management by providing next-generation desktop image management for physical desktops across distributed environments.

Greater visibility into and management of virtualized operations as well as real-time application lifecycle management and personalized user management enables IT to monitor, provision, and personalize applications to help ensure remote employees' success on the job. At one global financial institution, call center staff are now leveraging virtual desktops to work remotely while having the same access to apps, phone systems, and resources. By reducing the number of call centers managed, the firm reduces costs—in this case by more than \$500,000 (USD) a year—and diverts those critical funds to further support the entire business.

### [Learn More about VMware Secure Digital Workspace Solutions for Financial Services](#)

VMware solutions bridge past to future, deepening engagement and growing profits by providing access to data and information customers and employees anytime, anywhere, on any device. VMware's always-available infrastructure supports every endpoint—from the data center to the device. With VMware, financial services organizations can deploy a digital-first vision to achieve business outcomes.

Visit <http://www.vmware.com/solutions/industry/financial-services.html>.

