vmware®

Three Critical Digital Workspace Strategies for Financial Services

The shift to digital is transforming the way financial services institutions operate by unlocking new and innovative ways of working, letting employees work from anywhere, optimizing customer experiences, and improving operational efficiency and organizational performance.

Embracing a digital workspace is becoming one of the most important factors for financial services organizations to compete, grow, and obtain and retain top talent. According to a recent *global survey* of over 6,400 respondents across multiple industries, including financial services, digital transformation is shaping the way organizations compete, not only within their own market but also in acquiring the best talent. As digital needs continue to explode, the conversation is shifting from a traditional IT focus to one that brings IT, HR, and corporate leaders together to change the way the organization operates digitally.

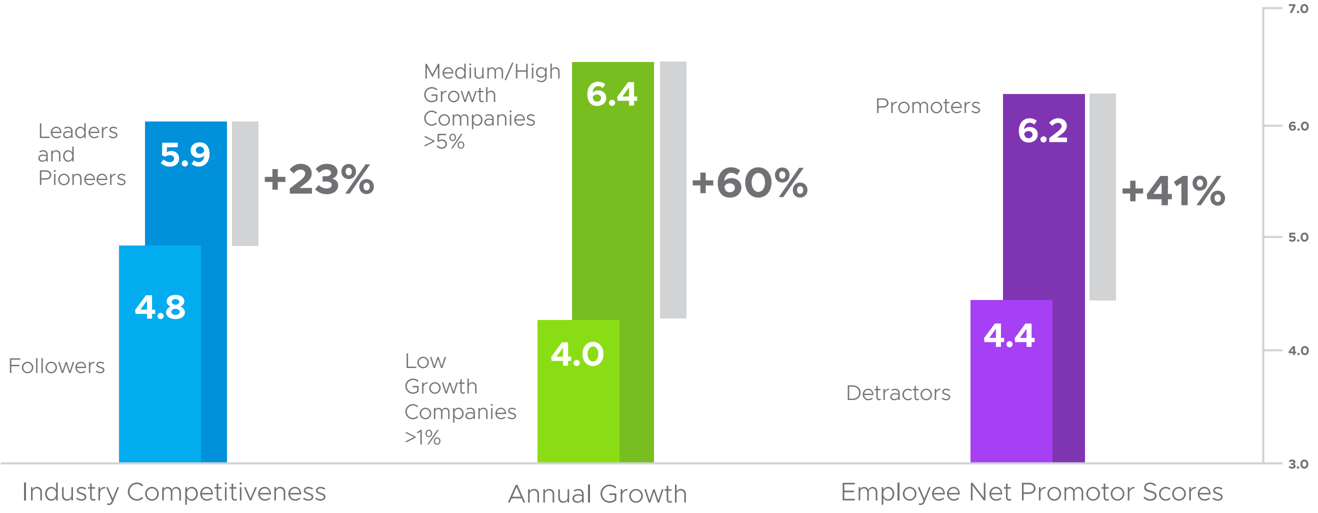


Figure 1: Research shows a strong correlation between digital employee experience and business performance. (Performance is based on composite employee experience scores.)

This brief explores the top-three digital workspace strategies for financial services organizations and how to deliver the foundation for a secure, engaging digital employee experience. It addresses the financial services trends and issues that shape:

Employee experience

Zero trust security

New ways of working

Elevate the Employee Experience

Traditional banks and other financial services institutions (FSI) are seeking easy ways to blend physical and digital channels to elevate customer experiences, but demand for personalized, anytime, anywhere digital services isn't limited to customers. To remain competitive and attract and retain top talent, organizations must also prioritize delivering a compelling employee experience.

Employee experience is a combination of culture, physical space, and technology, with technology heavily influencing both culture and physical space. A winning combination of technology boosts employee engagement, productivity, and enthusiasm toward the company, ultimately improving employees' customer interactions. Through VMware's digital workspace solutions, FSIs can capitalize on new opportunities to work and serve customers securely from anywhere, anytime, and often on the device that employees choose.

Successful onboarding

The role of technology in employee experience begins before an employee accepts the job offer. According to the 2019 VMware Global Survey on Digital Employee Experience, 73 percent across all generations of workers agree that the flexibility of tools that a company offers, such as technology, apps, and devices, influences the decision to apply or accept a position.

While flexibility of tools is imperative, it is important to continuously support employee access to tools, from initial onboarding to retirement. Day one is a new hire's first impression of working life at a company, offering a glimpse into its structure and culture. FSIs can spur excitement and build loyalty by providing both new and established employees seamless access to company resources, teammates, and the required training and documentation.

Delivering exceptional customer and employee experiences with mobility

With the availability of new service and engagement models, FSIs are empowering employees to work beyond the confines of a traditional office. Financial and wealth management advisors are spending more time meeting face-to-face with customers, requiring secure real-time access to personal information at the customer's home, office, or other convenient meeting location. Letting advisors use the device and operating system with which they are the most confident helps them work more smoothly and competently, and subsequently, deliver the best possible experience to the customer. Implementing multifactor authentication security mechanisms and single sign-on access to the different financial systems that might be required when meeting with customers facilitates an efficient use of time and lays the foundation for a great advisor-client relationship.

The digital transformation is also enhancing the branch experience. Digital ambassadors, equipped with mobile devices, are delivering new customer-centric experiences with the ability to provide customers who are entering the branch individualized information on financial products and services. With similar initiatives being adopted by mortgage lenders and call center staff, mobility is transforming the way financial services are being delivered.

Implement Zero Trust

The financial services industry is one of the most targeted industries for cyberattacks. According to a report by the Boston Consulting Group, it is estimated that financial services firms are 300 times as likely over other companies to be targeted by a cyberattack. The report also states that cyberattacks and the aftermath carry a significantly higher cost for banks and wealth managers than for any other sector. Protecting your organization and clients' assets and upholding credibility and integrity demands maximum security across all fronts.

Moving toward a digital workspace requires new security models that reach beyond traditional perimeters to provide the comprehensive threat protection, detection, and remediation that today's enterprise requires. The following trends in the financial services industry pose security vulnerabilities in this world without perimeters.

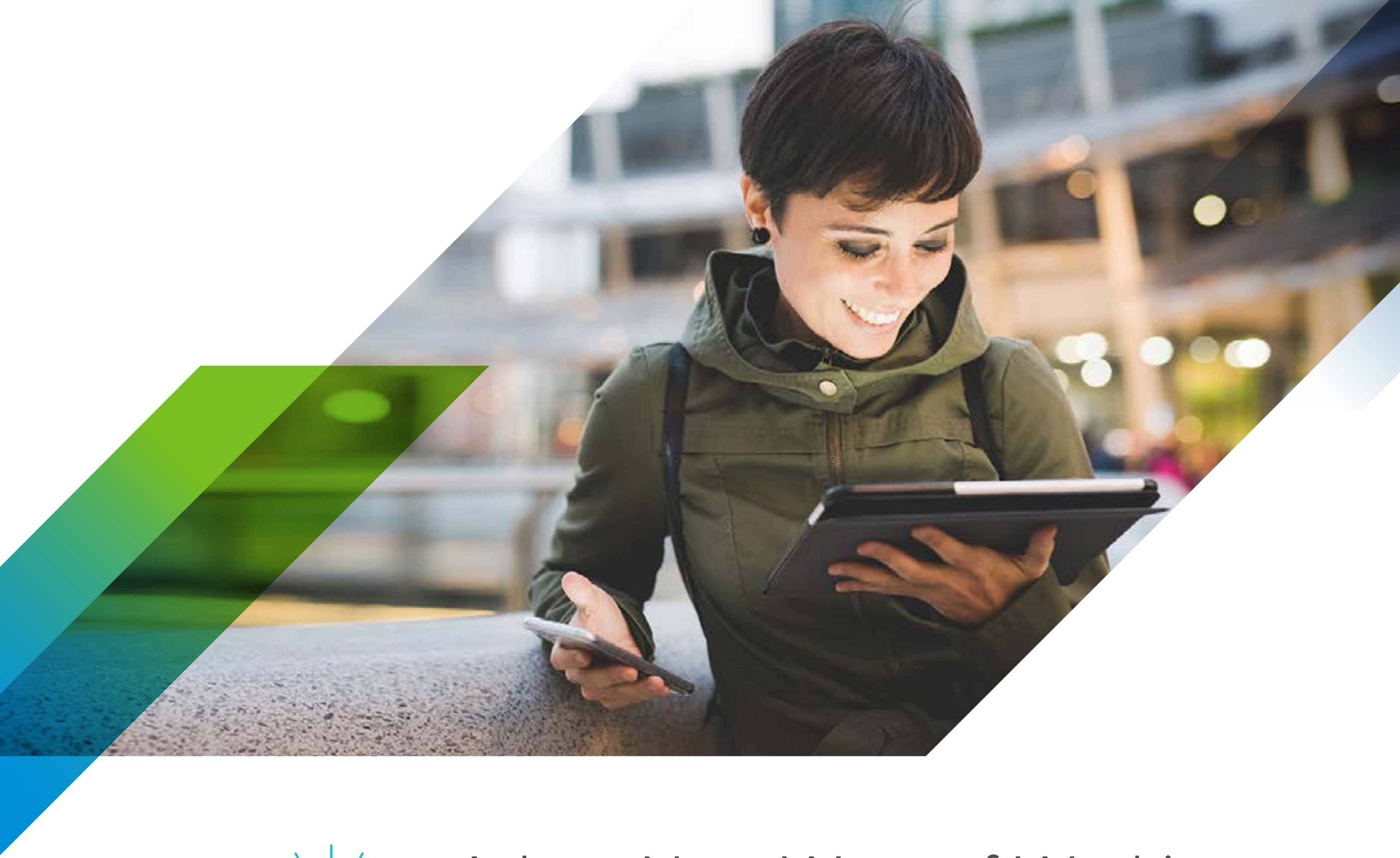
Choice of endpoints – Providing internal staff the freedom to use any preferred device: desktop, laptop, tablet, smartphone, and more.

Flexible work styles for bankers and staff – Giving access to financial accounts and customer data whenever and wherever banking takes place: in the branch, over the phone, or in the field.

Applications everywhere – In an increasingly app-centric world, supporting all types of apps—web, native, or virtual—running on-premises and in cloud environments.

To maintain convenience, accessibility, and security, FSIs are shifting from existing security silos to modern security frameworks, such as zero trust. Zero trust is based on the concept of continuous verification of trust. Compared to traditional security approaches that focus on securing the perimeter while trusting every resource inside, the zero trust model does away with the concept of implicit trust and considers all resources external. Zero trust relies on continuous verification of devices, users, and apps before granting access to enterprise resources.

By combining zero trust security with industry-leading modern management, such as granting each user the least amount of privilege and access to get their work done and nothing more, IT departments in financial services organizations can intelligently and proactively secure the digital workspace, reduce IT complexity, and protect the firm's reputation and brand.



Adopt New Ways of Working

Today's employees expect their work digital experiences to mirror the seamless digital experiences in their personal lives. Increasingly, employees prefer to use their own tools for work, putting pressure on IT to enable different ways of working and better support remote employees and bring-your-own-device (BYOD) programs. Organizations must also consider emerging work styles, such as hot desking. Over the past decade, BYOD has evolved in terms of technology and user perspective. BYOD programs let employees work from anywhere without the burden of carrying multiple devices, and they are an important pillar of crafting a modern experience for employees.

Technology innovations, such as iOS 13 User Enrollment, advancements in Android for Enterprise, Windows 10, mobile application management, and full mobile device management, help the financial services industry meet different use cases across the organization. Modern digital workspace platforms make it easy for firms to deploy various BYOD management approaches to meet a myriad of employee requirements instead of enforcing a one-size-fits-all program—all while safeguarding sensitive business data.

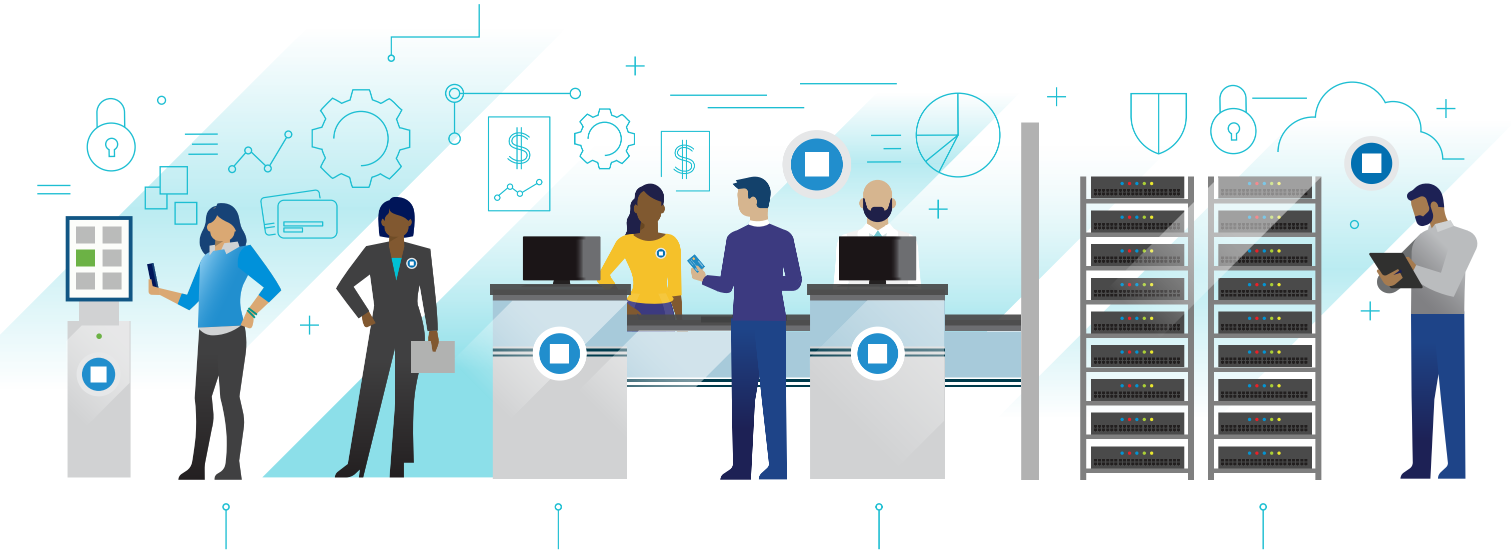
Employee privacy, especially in BYOD deployments, is also an important consideration when building a digital workspace strategy. The separation of work and personal content on BYO devices, along with transparent communication around device control and data collection, gives employees peace of mind. An effective digital workspace platform enables IT teams to collect data to control corporate access while complying with privacy laws that promote trust and transparency with employees.

VMware Workspace ONE Digital Workspace

Consistently ranked as a leader by industry analysts across the board, VMware Workspace ONE® delivers best-in-class device management, access control, zero trust security, intelligence and analytics, and application and desktop virtualization.

With the Workspace ONE solution, financial services institutions can

Provide employees with the digital tools to work from wherever financial services transactions take place



Offer customers a more personalized, convenient branch experience on tablets, IoT devices, and kiosks to enable bank staff to focus on delivering high-value services to customers

Increase employee satisfaction and retention by delivering engaging digital experiences

Protect company and client information and reputation through a zero trust security model that uses risk-based conditional access integrated with user, device, and network intelligence

Secure, manage, and scale IoT infrastructure at the branch to improve operational inefficiencies and customer banking experiences

Change isn't always easy, but with the right strategies in place, the shift in the way financial services institutions operate digitally can transform the experiences of both employees and customers. By leveraging the strategies outlined in this brief and through the implementation of a modern digital workspace platform, like VMware Workspace ONE, financial services institutions can make this digital transformation a reality—all without compromising security.

VMware, Inc. 3401 Hillview Avenue Palo Alto CA 94304 USA Tel 877-486-9273 Fax 650-427-5001 www.vmware.com