omnissa™

WHITE PAPER

The need for smarter, more efficient financial operations

How to balance operational efficiency with security and employee productivity

Table of contents

Transforming financial services through technology

Technology is reshaping the way customers interact with financial services, putting increasing pressure on the industry to innovate and modernize. Seamless digital experiences are no longer optional—they're expected. Modern consumers demand convenience, security, and a fast response. Financial institutions that fail to adapt are at risk of falling behind, as outdated systems, regulatory obligations, and operational inefficiencies create barriers to success.

While some financial organizations have embraced change in setting new benchmarks for digital interaction, many still rely on legacy systems that struggle to meet modern needs. These institutions face mounting pressure to not only comply with regulatory standards but also manage costs, safeguard data privacy, and maintain competitive operations. The solution? A holistic approach to modernization that balances operational efficiency, security, and innovative customer experiences.

The race to modernize core systems

For financial institutions, the clock is ticking. Consistent infrastructure management and the modernization of core banking systems aren't just priorities, they're necessities. Using outdated systems creates inefficiencies, drives up costs, and stifles innovation. To remain agile and competitive, your organization needs to adopt scalable and secure solutions that integrate seamlessly with your existing operations.

Essential components of modern financial services technology

An agile, tech-first foundation
Shift from legacy systems to modern, cloud-enabled platforms that foster scalability and innovation.

Unified endpoint management (UEM)
Centralize the management of devices to support consistent performance and security.

Virtual desktops & apps
Provide employees with secure, role-based access to apps and data, no matter where they work.

Security & compliance
Protect against threats targeting mobile devices and monitor risky behaviors and suspicious activities.

Digital employee experience (DEX)
Leverage data, analytics, AI, and automation to proactively solve problems.

Modernizing for a digital-first future

Today's banking customers demand a modern banking experience. Instant payments, personalized services, and intuitive platforms have become the standard, and it's up to your financial institution to deliver.

Simplifying device management, security policies, and communication tools not only reduces IT overhead, but also fosters agility across your organization. Minimizing downtime and enabling uninterrupted access to financial apps reinforces superior customer experiences without compromising operational efficiency.

Helping your organization thrive—today and tomorrow

By streamlining operations, leveraging cutting-edge analytics, and fostering a secure, flexible work environment, your financial organization can build a path toward success. But progress doesn't stop there. Collaboration, innovation, and a commitment to continuous improvement will help your organization turn challenges into opportunities.

Modernizing is about empowering your workforce, protecting your data, and delivering value to every stakeholder. With the right approach, your financial organization can drive growth, bolster resilience, and redefine what's possible.

Empowering financial brokers and bankers for success

Today, financial services professionals need the ability to access apps and data seamlessly across devices. Integrated, user-friendly workspaces streamline workflows and eliminate friction, enabling your employees to switch between devices without missing a beat. This consistent experience boosts efficiency and empowers your team to perform at their best—anytime, anywhere—while enhancing overall satisfaction.

The need for secure access to data and tools

By leveraging technology that enables real-time collaboration such as meeting platforms, secure messaging, and cloud-based document sharing, your employees can engage with clients regardless of location. These tools allow dispersed teams to innovate together and foster stronger client relationships by ensuring timely, consistent communication and support.

Enhancing agility and scalability

Agility and scalability are essential to succeed in the modern financial world. Whether you're opening new locations, integrating acquisitions, or scaling up during seasonal peaks, your financial organization needs to adapt quickly to stay ahead. But traditional infrastructure can hold you back, creating challenges with IT management, data security, and compliance. And trying to solve these issues with quick fixes can lead to higher costs and increased security risks. Thankfully, you can easily overcome these challenges by taking a modern approach with Omnissa.

Enhance data security and compliance

Virtualization centralizes data management, reducing the risk of breaches. Policy-based access controls and detailed audit trails augment regulatory compliance and help minimize violations.

Reduce costs and simplify IT management

A centralized infrastructure simplifies patches, upgrades, and app rollouts. It cuts maintenance and storage costs, and enables IT teams to address cyberthreats quickly.

Boost operational agility

Rapidly adapt to changing market conditions, customer expectations, regulatory requirements, and tech demands. Deploy kiosks without heavy investment into physical infrastructure, quickly offer attractive deals to customers, and update security protocols when new data protection laws are introduced.

Embracing Omnissa solutions can improve both operational and strategic flexibility, leading to greater efficiencies for your organization.

What Omnissa can do for you

Streamline device management
Use Omnissa Workspace ONE® UEM to manage all devices across all operating systems, simplifying IT operations and reducing downtime.

Enhance DEX
Implement Workspace ONE Experience Management to measure, analyze, and remediate issues across apps and devices, reducing downtime and boosting productivity.

Strengthen security
Use Workspace ONE Mobile Threat Defense™ to detect and prevent phishing, malware, and zero-day attacks, and to reinforce secure access to financial data.

Efficiently deliver virtual desktops
Adopt Omnissa Horizon® 8 to deliver virtual desktops and apps fast, with secure access to resources, while maintaining low latency and high performance.

Boost desktop scalability
Leverage Omnissa Horizon Cloud Service™ to modernize virtual desktop and app delivery with next-gen DaaS that allows rapid scaling to meet your organization's needs.

Reduce risk to attract banking customers

Banks face increasing risks due to cyberthreats, compliance requirements, and operational inefficiencies. Omnissa offers integrated solutions that empower your bank to enhance security, compliance, and productivity.

Be a safe choice

Customers are more likely to choose a bank that guarantees secure transactions, fraud prevention, and uninterrupted access to their financial services. UEM helps enforce zero trust security, automate compliance, and protect customer data to help you build credibility, attract more customers, and increase retention.

What's more, a secure and frictionless customer experience means fewer disruptions, faster service, and higher satisfaction, leading to positive reputation and increased customer acquisition. In an era in which financial security is a top concern, embracing proactive security and compliance measures can help your bank stand out as a trusted, customer-first institution.

Key benefits

Enhance security and compliance
Centralize endpoint management and ensure all devices follow security policies. Keep sensitive data off local devices and reduce data breaches while ensuring compliance.

Mitigate cyberthreats
Provide secure, controlled access to apps and data while preventing unauthorized downloads or data exfiltration with strict authentication and monitoring.

Strengthen business continuity and resilience
Enable secure remote access and uninterrupted banking operations during crises. Automate patching and threat response to minimize downtime and vulnerabilities.

Balancing innovation with security and cost efficiency

The stakes have never been higher for financial organizations. Rising operational costs and evolving customer expectations demand bold action, but any advancements must prioritize safety and regulatory compliance.

Your organization needs to strike a fine balance between empowering employees with the tools they need for success and maintaining the highest levels of data protection. Investing in secure infrastructure and scalable solutions enables you to meet evolving industry challenges while future-proofing your operations.

Why it matters

- **Protecting financial stability** – Your bank manages vast amounts of money and data including deposits, loans, and investments. Poor risk management leads to financial losses, insolvency, or even collapse.
- **Optimizing regulatory compliance** – Failure to manage risk appropriately can result in heavy fines and legal actions from entities like the Federal Reserve, SEC, and international regulators.
- **Preventing fraud and cyberthreats** – A security failure can result in financial loss, legal consequences, and loss of customer confidence. Reducing risk through cybersecurity measures, fraud detection systems, and secure authentication methods is essential.
- **Safeguarding customer trust** – Customers expect their money and personal information to be secure. If your organization suffers a security breach, financial scandal, or liquidity crisis, it can damage your long-term viability.
- **Enhancing operational efficiency** – Strategies using UEM and VDI streamline operations and minimize human error, leading to cost savings and improved service delivery.
- **Strengthening market competitiveness** – Being able to manage risk attracts investors, secures better credit ratings, and bolsters financial resilience in the marketplace so you can expand services confidently.

Dynamic security to protect critical data

Implementing zero trust and contextual security models is essential to control access to sensitive data. Zero trust adheres to least-privilege principles, ensuring that users and devices are granted only the minimum level of access necessary for their specific roles. This significantly reduces the risk of unauthorized data exposure.

Beyond zero trust

A zero-trust approach is complemented by contextual security measures, which dynamically adapt security protocols based on device in use, user identity, and geographic location. This adaptability allows for more granular control and real-time adjustments to security measures, ensuring that access remains secure and appropriate under varying conditions.

Managing secure access to apps and devices is crucial for maintaining robust data protection in financial institutions. Multi-factor authentication grants access only after multiple layers of verification have been completed, and single sign-on provides a user-friendly experience by streamlining the login process across apps.

The need for dynamic security

The financial sector is a prime target for cyberthreats, given the sensitive data it manages.

Complex regulations like GDPR and CCPA add further pressure, requiring robust protection measures, regular audits, and a commitment to ongoing compliance.

An integrated data security approach

With Omnissa, you can provide your employees with secure access and allow them to quickly assist customers—whether from a branch, call center, or remote location—without delays caused by security roadblocks or IT issues. Role-based access control (RBAC) ensures that customer service reps and financial advisors have access to the right apps and data, enabling faster response times and personalized customer interactions.

Secure every transaction

Encrypted transactions protect sensitive financial data and build customer trust while maintaining industry regulations. By minimizing IT downtime and preventing fraud, your bank can offer consistent, secure, and high-quality customer experiences leading to stronger customer relationships and increased loyalty.

Protecting data on both managed and unmanaged devices mitigates breach risks. Simplifying and automating onboarding and offboarding strengthens security by ensuring that access rights are promptly adjusted, reducing the likelihood of unauthorized access and streamlining administrative tasks. This approach to access management balances security with operational efficiency, safeguarding critical data while facilitating a consistent user experience.

Start with these two areas

Proactive threat mitigation and compliance

Enforce security policies across all endpoints and centralize data to prevent breaches. Create a seamless, secure user experience and reduce human errors that lead to vulnerabilities while maintaining compliance.

Enhanced visibility and automated response

Provide real-time monitoring of devices, isolate bank applications from endpoint threats, and leverage analytics to detect anomalies, enabling automated threat response and minimizing attack impact.

Strategies for a comprehensive solution

Combining virtualization with cutting-edge cybersecurity and a unified technology strategy delivers a powerful advantage for financial services organizations. Centralized data and apps enable simplified security management and consistent protection across every access point. At the same time, prioritizing cybersecurity infrastructure and promoting a culture of compliance among employees fortifies your organization against emerging threats. By adopting innovative solutions, you can achieve heightened security, improved operational flexibility, and the efficiency your organization needs to thrive in a constantly evolving market.

Taking the first step

The path to a fully integrated solution starts with a clear digital transformation roadmap tailored to your goals and industry standards. Selecting the right tech partners is critical—focus on their ability to integrate seamlessly with existing systems, scale with future growth, and demonstrate a proven track record for delivering secure, high-impact solutions.

What's next

After choosing your solutions, driving adoption across the organization is key to success. Engage stakeholders early, establish a reliable support system, and foster a collaborative culture focused on continuous improvement. By managing change strategically, financial institutions can design a smooth transition, maximize ROI, and unlock the full potential of their tech investments.

By taking these steps, your organization will move closer to a future of unparalleled security, agility, and innovation. Are you ready to elevate your operations and transform your technology strategy? The time to act is now.

Get started

Learn more about how Omnissa can help your financial services organization increase operational efficiency, security, and employee productivity. Visit our financial services **web page** or **contact** an Omnissa representative today.

omnissa™