wipro | citrix

See beyond hybrid

Leading solutions for liberated workforces

Into the hybrid future: what's next for banking, financial services and insurance?

Many major retail and commercial banks, as well as other financial services firms and insurance providers, have long embraced some form of remote or hybrid working. Many more joined them during the pandemic in early 2020.

It has now become clear that hybrid is here to stay, with only 20% of US financial services employees believing a typical employee needs to be in the office any more than three days per week, according to PWC research. Globally, just 11% of companies expect to go back to full-time office working.

This is brilliant news for finance professionals, who have largely adopted the new 'work from wherever' culture, enjoying the autonomy, freedom of choice and flexibility it brings. But it has not been plain sailing for industry leaders, many of whom are concerned that this freedom might come at the cost of one of the industry's core principles: **security.**

For finance CTOs, turning temporary and partial digital measures implemented over the past few years into secure, permanent new ways of working is not easy. Those who took a piecemeal approach – adapting out of necessity rather than strategy – are using solutions that worked for them in the moment, but that are currently not fit for purpose.

So, what comes next?

Banking, financial services and insurance (BFSI) leaders have entered an age in which 'where' no longer matters. As such, they are looking to invest even more heavily in cloud-enabled services to deliver human-centric, secure and cost-efficient platforms – to support tomorrow's flexible, collaborative and energized workforce.

Free your future to find your best work

The big question is: how do organizations liberate their staff from stale, outdated working practices to create the future of work, without compromising the eternal quest for security? And how do organizations ensure employees have seamless user experiences, from any location, which enable them to lead productive, fulfilling working lives?

Achieving all of this while guaranteeing service delivery and real-time information exchange – vital in areas such as stock trading and retail banking – requires the harmonization of seemingly conflicting priorities. But it can be done when you're working with the right partners.

Wipro and Citrix's experience in this space means we understand that, in addition to this, organizations are facing operational challenges in the form of compliance issues, escalating cloud costs, below-par hybrid applications, recruitment headaches and competition from FinTechs.

Bringing together enhanced UX and robust security is possible. And in this concise guide, you will discover how embracing a centralized, managed services approach to the future of hybrid will support you to achieve your three key goals: **robust workspace security, always-on service delivery, and enhanced user experience and collaboration.**
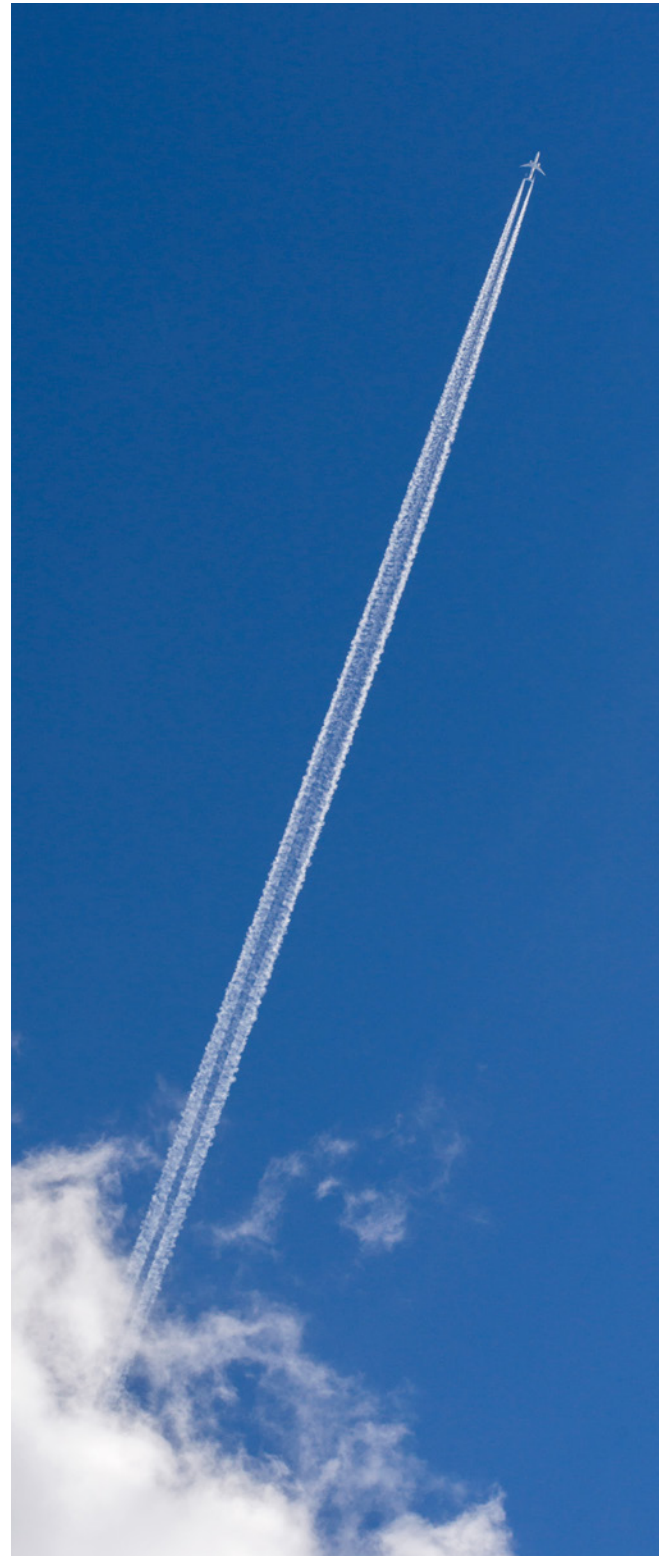
Can seamless hybrid work and robust security co-exist?

Hybrid work is here to stay.

As mentioned above, only 20% of US finance workers believe they need to be in the office more than three days a week. In the Asia-Pacific region, IDC has found that more than 56% of employees want flexible work, with the option to work both in the office and remotely, showing that these changes are global.

Meanwhile, a recent Citrix survey of business leaders from the US, UK, Australia, France, Germany, Japan, Mexico and the Netherlands reported that **more than two-thirds (69%) of hybrid employees would recommend their employer as a place to work**, compared to 56% of office workers and 60% of remote workers.

But while hybrid work environments are now a prerequisite for retaining staff and attracting new talent, many global leaders in BFSI feel they are not prepared for what this looks like in the long-term. The security of systems across dispersed networks remains the primary concern, along with the need for employees to carry out all necessary functions – on any device – including tasks that were previously only possible on-site.

According to a recent BCI Cyber Resilience Report, three quarters of BFSI organizations have experienced a rise in cyber-crime over the past few years.

And two-fifths of respondents put this increase in attacks down to remote-working practices. The dilemma now is liberating workforces without compromising data security, as the BFSI sector is heavily regulated. Unfortunately, cyberattacks – such as ransomware and SQL injection attacks – are big business. Bad actors, who choose their targets based on maximum impact and profit, populate the internet. They're ready to exploit outdated security practices and pounce on the most valuable information – such as personally identifiable customer information and stock trading data.

And financial institutions are a prime target, not only because of the highly valuable data they store, but because their ongoing digital transformation efforts have been noticed and are creating greater opportunities for cybercriminals to access that data.

How does the industry allow the flexibility hybrid work affords, without compromising any further on productivity or security?

Allowing talent to thrive

With increased employee expectations around flexibility, the Great Resignation of 2021 and competition from FinTechs all affecting the search for new talent, the sector needs to be able to offer its employees a superior user experience that allows them to thrive in their roles, wherever they choose to fulfil them.

According to a Hays Financial Markets Salary Guide 2022 survey of 267 financial service employers, **more than four fifths (83%) of banks suffered a skills shortage in 2021.** Offering the most attractive working environment – with superior technology tools as well as competitive salaries – is the key to attracting and retaining the best possible talent at all levels. Also, offering a superior user experience is key to maintaining robust security and enhancing the overall productivity of the business.
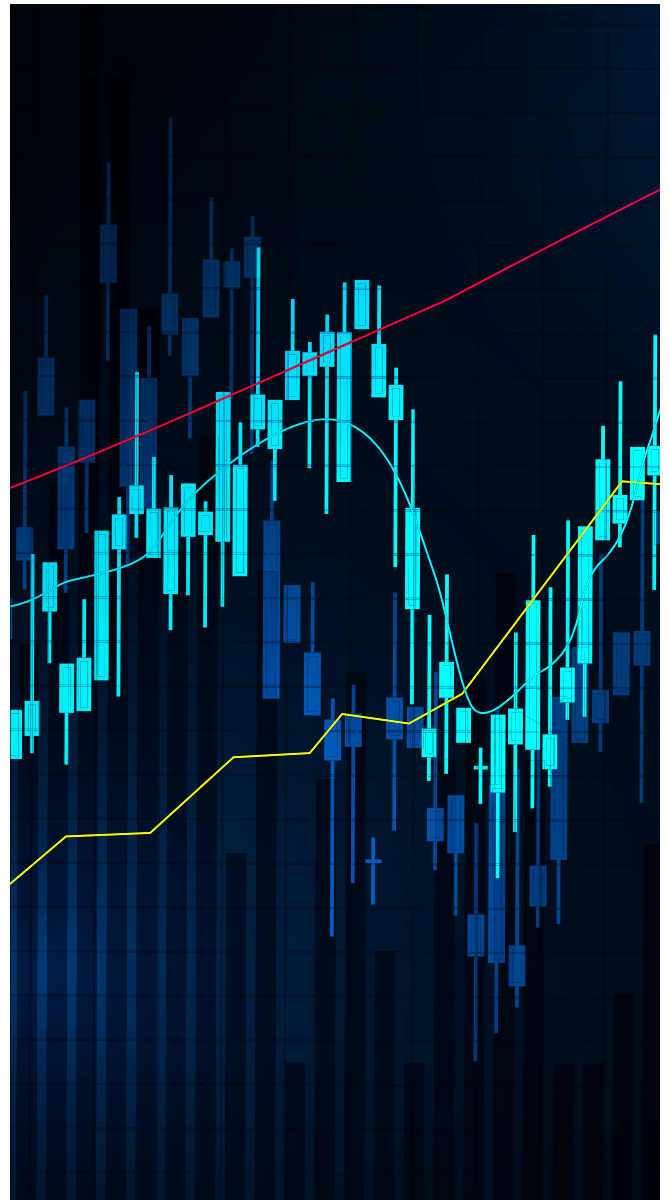
Adapting to the practical realities of hybrid working

Aside from getting to grips with who works on what, where and when, industry leaders must also get to grips with prioritizing solutions that empower employees with connectivity and security. The aim should be to allow simple and seamless scalability in response to rapidly shifting hybrid trends, and ever-changing regulatory and data privacy mandates.

Today's hybrid bank teller, for instance, must be on hand to remotely deliver new products, such as loans or credit cards, from whatever device they're working from, and from outside the traditional layers of on-premises security.

When a finance employee uses their own device – without appropriate endpoint security – IT has no way of tracking whether the machine is properly patched, has visited a fraudulent site, or has a virus. This expands an organization's cyber-attack surface and puts highly confidential data at risk.

Indeed, Citrix's 'State of Security in a Hybrid Work Environment' 2021 report revealed that almost three quarters (73%) of survey respondents said the volume of data they had to process and number of security events had increased significantly over the past year – introducing an imperative for robust security and constant vigilance over connectivity between dispersed teams.

The need for border-spanning communications and transactions, and the importance of delivering data security with global visibility, has seen banking leaders increase their reliance

on the IT network over the past few years – specifically their reliance on cloud, with many recognizing the benefits of hybrid cloud solutions.

A recent International Chamber of Commerce Global Trade Survey suggests more than half (54%) of banks identified blockchain, digital trade, and online trade platforms as their near-term strategic development priorities, which will further escalate reliance on cloud and hybrid cloud solutions.

But as cloud hosting becomes more prevalent, cloud data breaches grow bigger and more disruptive.

According to the 'Thales Cloud Security Report, 2022' almost half (45%) of global businesses experienced a cloud-based data breach, or failed an audit in the past 12 months, up 5% from 2021. What's more, a third (32%) have had to notify the government, customers, partners and employees of a data breach.

Almost half of today's leading organizations are planning to invest in cyber-security technologies as a priority over the next 12-18 months, according to the report, highlighting a willingness to adapt to the new realities of working.

Guaranteeing service delivery and performance in a new era

There is often a disparity between network and application performance for hybrid/remote employees and for on-site employees. This can have a huge impact on the ability of employees to thrive in their work, and also on service delivery on a broader scale.

On-site employees have their tech powered by hard-wired network connections and protected by in-house security protocols and firewalls. Remote employees, on the other hand, are often accessing applications and internal systems while relying on fluctuating network conditions, leading them to expose security weaknesses. For example, employees may collaborate insecurely, using common tools such as MS Teams, WebEx and Zoom.

Workers' increased reliance on these tools can also constrain computer memory and result in sluggish, low-performing desktops and applications.

This, in turn, can lead to people taking digital shortcuts to stay on schedule or budget. An example of this is sharing data on an insecure sharing platform, which then has broader implications for compliance and security, not to mention the financial cost to the organization.

All of this has been aggravated by the challenges faced by IT support in troubleshooting problems remotely, too. There is a real need for hybrid solutions that support seamless and consistent workflows across all locations, ultimately contributing to always-on service delivery. This is vital for activities such as FOREX, consumer banking and insurance reporting.

The challenge of dispersed teams

For leaders across the BFSI sector, it's crucial to optimize the user experience in order to empower dispersed teams to have greater accessibility and means of collaboration.

But how does a company unify and secure those connections? How does it bring about joined-up, cloud-enabled services, superior UX and next-level security? How does a company keep their employees engaged and collaborative?

Industry leaders need to provide secure, remote working and superior user experiences, and find solutions that enable them to successfully monitor and manage user experience across hybrid teams.

Predictive monitoring is key, as well as a holistic, end-to-end hybrid working solution with security and superior functionality built into its DNA. This might be software that enables IT teams to judge app performance or to monitor network/application utilization, ensuring that productivity and value are enhanced on an ongoing basis.

Six ways the BFSI sector can rise to today's challenges

1. By transforming its legacy systems into the future-fit systems of today

Traditional legacy systems need to be strategically phased out. Choosing a digital solution that brings siloed technologies together into one centralized platform, delivering an end-to-end virtual desktop service with single sign on, will give organizations:

- **Simplified, streamlined operations**
- **End-to-end visibility** across all systems and data, which in turn will give teams access to valuable data that can drive business decisions and better outcomes
- **Enhanced collaboration capabilities** to drive improved performance and CX
- **Robust security**

2. By creating secure end-to-end virtual environments

Managing applications in the cloud has many advantages for BFSI companies. By facilitating a seamless but secure flow of information and data, organizations can save time and money, boost operational efficiency and expand the scope of business possibility.

However, this can also open them up to potential new cybersecurity vulnerabilities, such as ransomware attacks. To tackle this as part of a holistic security strategy, businesses need to:

- **Conduct an in-depth assessment of the organization's infrastructure and risk:** This should be done to identify network, device and user weaknesses, and should include reviewing where devices are on the network and who has access to them. Such reviews should also assess whether networks are set up to proactively monitor for attacks, and if hacker attempts can be isolated and stopped quickly. Additionally, users, apps, data and more should be analyzed to identify vulnerabilities and ensure business continuity. Finally, the infrastructure should be reviewed to find out if it is flexible enough to allow remote access and optimal signal strength from any endpoint, anywhere.

2. By creating secure end-to-end virtual environments (cont.)

- **Secure hosting agreements and requirements:**
  To future-proof company infrastructure, IT and business decision makers need to decide upon a technology solution that is capable of hosting current requirements. These technology solutions should be agile enough to enable seamless upgrades and tighten security.

- **Implement proactive monitoring:**
  Logging and monitoring of cybersecurity threats is crucial in making sure an organization can react quickly to security incidents. Robust governance and real-time risk analysis are vital to maintain trust in sector institutions.

- **Manage identities and permissions:**
  Zero-trust is a security architecture that applies not only to networking, but across the organization in users, devices, networks, applications. It trusts no one by default. In a zero-trust model, anyone trying to access a company network is treated as a bad actor as a first step and must be continuously verified via mechanisms like multi-factor authentication (MFA) and adaptive authentication.

- **Choose a solution that supports the journey from legacy to modernization:**
  Many of today's major organizations are in a state of flux between the two. This requires a next-generation technology that is flexible enough to cater to both. Using a managed Desktop as a Service (Daas) enables this flexibility.

3. By implementing leading-edge preconfigured delivery models to enhance service delivery and user experience

As has already been outlined, BFSI firms need to be able to virtualize, manage, stream and remotely display applications – and securely deliver remote and secure desktops.

Traditionally, leaders have been hesitant to implement such changes, believing it will result in downtime, outages, and impact negatively on employee service level agreements and customer experience.

Today's plug-and-play, preconfigured delivery models improve time to market of new products, and enhance service delivery, performance and scalability of hybrid cloud environments. Leaders can support IT teams that lack the in-house resources or time required to set everything up themselves. Service delivery and managed services models, which provide regular support and guidance on how to improve infrastructure and protocols, can ensure any solutions are implemented in line with business objectives.

4. Apply end-to-end performance optimization through predictive monitoring

Leveraging the leading tech solutions discussed above empowers team leaders to monitor systems for the purpose of identifying areas that require performance optimization across dispersed networks.

BFSI companies need solutions that can monitor application use, network performance and outages, and allow for deep insight into user analytics. This is not about 'keeping tabs' on or spying on remote employees: **it is about ensuring that frequently-used apps are supported appropriately.** Predictive monitoring uses the data gained from this monitoring to identify common issues, improve processes and prevent future incidents.

5. By leveraging advanced security analytics and risk indexing to better manage cloud security

Security analytics and risk indexing translate into better managed security in the cloud. By deploying a combination of Desktop as a Service (DaaS) and adjacent security solutions, organizations can enable their hybrid workforces to gain secure access to applications without needing users to log in. This feature also ensures user workflows are deeply incorporated into the solution, which results in a better user experience while maintaining a strong security posture.

## 6. By improving user experience and customer experience

For the hybrid workforce, user experience is central.

Today's hybrid finance professionals are often required to perform the highly confidential and complex tasks they once carried out on site – everything from mortgage assessments to insurance policies – on their laptops, tablets and smart phones.

These employees expect to be able to do this easily and seamlessly, with minimal disruption. The key for employees, wherever they are working, is to feel they can collaborate with colleagues as effectively as if they were sitting next to them.

Customers must also feel they are being supported just as well virtually as they would be in person.

By deploying the highest quality audio and video tools, underpinned by robust security, BFSI companies can facilitate seamless collaboration and communication that drives greater customer and employee experiences.
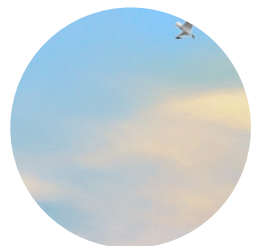
Citrix and Wipro:
Your best work is waiting for you

By leveraging and combining leading cloud and hyper-converged infrastructure (HCI) – such as Wipro virtuadesk™, Citrix DaaS, Citrix Secure Access and HDX Technology – the Wipro and Citrix partnership offers your organization a single solution which will empower you to realize your key business ambitions.

This partnership's solution harmonizes seemingly conflicting capabilities to deliver superior cybersecurity, user experience and service delivery. It removes the barriers to successful transformation and enables a human-centric approach to the future of banking, financial services and insurance.

Our cutting-edge alliance is responsible for leading most of the high-volume deployments in the BFSI industry. Our partnership is successful because while Citrix offers the advanced security solutions, Wipro complements it by bringing next-generation systems integration, management and consultancy to the mix. All of this is delivered in a managed services approach, ensuring long-term support for your hybrid future.

We support you in delivering a secure, hybrid workforce, with next-generation service delivery and user experience.
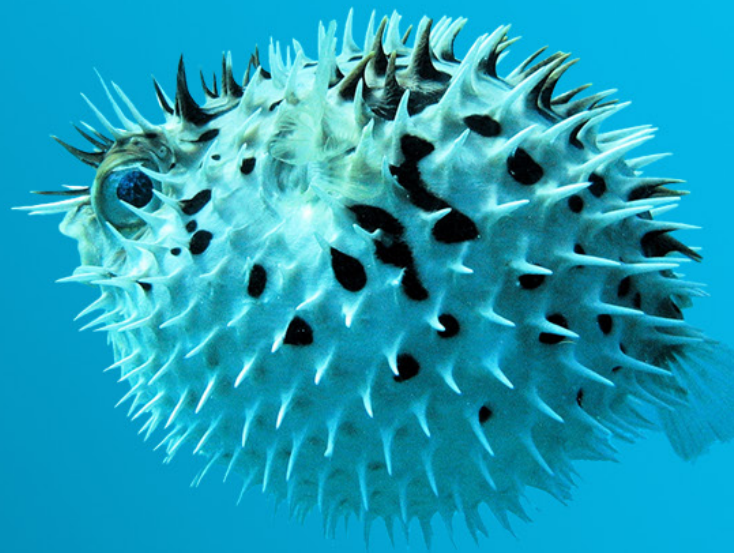
Case study:
Leading European bank

Scenario:

A multinational investment bank needed a scalable and secure virtual desktop solution for third party and internal developers that offered the same access and functionality to remote and external workforces as its internal and office-based staff.

The bank required a next-generation workplace to realize its ambitions, going beyond simple hybrid working to deliver scalability, flexibility and superior user experience for its employees, and guaranteeing compliance with the 60+ regulatory bodies it is answerable to.

The main challenges included:

• Meeting financial compliance and security requirements

• Ensuring desktop application performance and compatibility

Solutions:

The solutions implemented included:

• **Wipro virtuadesk™** – An appliance-based Desktop-as-a-Service solution focused on creating and enhancing virtual workplaces, that combines Microsoft Azure Virtual Desktop and Citrix Cloud Services

• **Citrix DaaS** – Enabled enterprise-grade Hybrid Workspaces and analytics to ensure secure, remote work from anywhere, and to drive seamless productivity

• **Microsoft Windows Virtual Desktop –** Windows 10 multi-session desktop experience, Azure-hosted VDI capabilities with performance analytics, and extended support for Win 7 VDI

Benefits:

The bank will now be able to rely on a solution that sits in harmony between the twin challenges of compliance and user experience. Banking staff will benefit from a frictionless service in an enterprise-grade VDI that can be customized to their needs. This will result in a consistent user experience for employees, irrespective of their location or device.

The bank will be able to monitor, manage and analyze their staff from a single management control plane. Other benefits include:

• **The ability to deal more effectively with business disruption**

• **Seamless data management between on-premises and cloud with a hybrid cloud model**

• **Increased flexibility with built-in auto-scaling functionality**

Ready to give your people the future?

Leveraging the power of advanced technologies to lead your organization into a successful future is not difficult. Our smarter, more secure and seamless solutions can support you in going beyond your existing, traditional approaches.

Our future-fit desktop virtualization solution supports organizations in protecting highly sensitive data and intellectual property. It delivers a complete ecosystem – with governance, security, and accessibility – to teams across the globe, while holding data in compliance with the latest regulations.

It facilitates greater hybrid team collaboration and innovation by offering the same level of accessibility and visibility to hybrid and on-site employees, while being user-friendly and seamless to implement.

Our partnership has a proven track record of delivering outstanding success for organizations across the globe – and we are proud to be considered a trusted partner by many leading firms.

We would love to help you realize your ambitions through hybrid today. Whatever your priorities, **Wipro and Citrix have you covered.**

Let us show you what we can do for you.

For more information get in touch with us at **virtuadesk.marketing@wipro.com**

Join us online: in 🐦

wipro | citrix

DaaS platform

- Improved service delivery
- Superior user experience
- Secure foundation support
- Expert hosted service
- Hybrid multi-cloud

wipro | Ambitions Realized.