



| citrix.

Grow beyond hybrid

Leading solutions
for liberating
your workforce



Into the hybrid future: what's next for healthcare?

The healthcare and life sciences sector has shown remarkable innovation and agility in keeping pace with the turbulent global and technological changes of the past few years. During this time, the industry fast-tracked its already-strong focus on digital transformation, adapted to the remote and hybrid work climate, and subsequently achieved some ground-breaking wins – the development and speed to market of the Oxford/ AstraZeneca Covid-19 vaccine being one striking example.

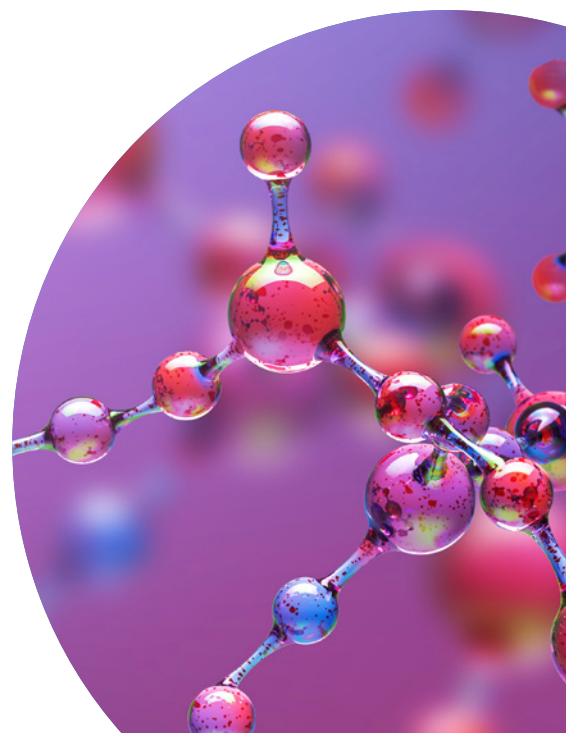
And yet, during this shift to hybrid work, cyberattack surfaces expanded as businesses moved work systems to dispersed networks – where employees lacked the protection of company firewalls and security protocols. This was a result of many hybrid strategies being built rapidly to address specific and immediate remote working challenges – rather than as part of an overarching future-ready digital strategy.

In the time that's followed, many organizations have still not updated these protocols, even though hybrid work is clearly here to stay.

These security gaps mean organizations are now prey to cybercriminals looking to steal

billions of dollars'-worth of valuable intellectual property. Customer-driven healthcare companies are the perfect target for hackers as they have more data accessible through patient and healthcare provider portals.

The most prolific cybercriminals have started targeting these companies to distribute ransomware designed to freeze their operations, and interrupt or steal research and development – such as molecule development for new drugs.



Along with these additional security challenges, the way remote and virtual clinical research teams collaborate has changed. For instance, they're now using communication technologies – such as video conferencing, cloud-based file sharing and telehealth – along with electronic informed consent (eConsent) and remote monitoring. All of which demand a reliable, high-performance network to deliver media-rich experiences.

The onus is now on healthcare and life sciences leaders to review and optimize their hybrid working strategies. This will mean implementing the necessary infrastructure, virtual collaborative tools and security measures to meet diverse hybrid working needs – urgently.

Speaking to our current customers in this space, we understand the major operational challenges of this altered landscape are:

- Conflicting c-suite views on hybrid working
- Increased cybersecurity risks
- Compliance issues
- Escalating cloud costs
- Below-par hybrid applications resulting in bad user experiences and impeding collaboration
- Recruitment pressures



As the workplace evolves, the healthcare and life sciences sector will need a proactive and future-proof strategy to deal with change. And in this concise guide, you'll discover how embracing a leading-edge, centralized hybrid platform will support your organization in these four key areas:

- 1 Workspace security
- 2 Hybrid cloud and service delivery
- 3 User experience
- 4 Collaboration

Hybrid work is here to stay

As healthcare companies made progress towards 'getting back to normal', they redefined what that 'normal' working model would look like, with many switching to a permanent hybrid model. This model, which supports employees working both on-site and remotely, liberates workforces from stale practices, inviting more flexibility and making careers in healthcare more accessible and sustainable.

One thing is for certain, hybrid work is here to stay.

69% percent of hybrid employees would recommend their employer as a place to work, compared to 56% of on-site workers and 60% of remote workers

The needs of the workplace are technological and practical: leaders must provide an effective hybrid work environment that attracts and retains staff, but that calls for the provision of the right advanced technology. They need leading-edge solutions which will keep the business cyber-secure while fuelling innovation, communication, and boosting UX and CX to drive growth.

20-50% of healthcare companies indicated that healthcare professionals interactions are expected to be digital in future.

Allowing talent to thrive

Meeting employees' experience expectations is important, especially when the healthcare industry has not shown itself to be immune to 'the great resignation' – the current voluntary quitting and job shifting trend that has touched many industries. In this challenging attraction-and-retention landscape, business leaders must balance heightened employee expectations of flexibility with business needs.

The past few years have seen:

- An increase in employee burnout leading to higher staff turnover
- A growth in demand for hybrid working
- Increased pressure for leaders to recruit digital natives



Digitally skilled new recruits in the industry – inherently aware of their market value and with salary demands to match – are often choosing to work for companies offering the best work-life balance.

In fact, according to [McKinsey](#), four-fifths (80%) of healthcare professionals believe the future of their industry is an agile one. Leaders must meet the demand or lose out to the competition in the race to attract top talent.

Four-fifths (80%) of healthcare and life sciences professionals believe companies are likely to fully embrace agile ways of working – with more than two-thirds (70%) feeling healthcare organizational structures will be radically simplified.

Opening up versus locking down

To remain relevant, attract talent, reduce churn, and continue driving the best business and health outcomes, healthcare companies must rapidly accelerate remote working programs. These are essential to empower employees to deliver life-saving treatment and vital R&D, without sacrificing on security, user experience or delivery.

But there's friction between business leaders who want to offer employees this flexibility and IT decision makers (ITDMs) who need to prevent the expansion of the attack surface.

This is because when working remotely, many employees are connected to unsecured networks, without the protection of the usual office security protocols.

The ITDMs are right to be cautious.

In fact, healthcare and life sciences organizations suffer more breaches than those in any other industry, with more than half ([53%](#)) of those resulting from malicious activity. Attacks specifically targeted at the sector include credential theft, invoice phishing and business email compromise attacks.

Bad actors notoriously target sectors they believe are vulnerable and less prepared to fight off attacks. Healthcare is high up on their list for two reasons. First, many organizations haven't invested enough in cybersecurity. Second, many are susceptible to supply chain attacks because of the way they operate with other businesses in those chains.

Leaders in the field need to understand that, even if their organization isn't on a cyber-attack hitlist right now, it may well be in future. Which is why being proactive – establishing strategies and implementing flexible, hybrid working and cloud solutions, with next-level security built-in – is crucial right now.

Adapting to the practical realities of hybrid working

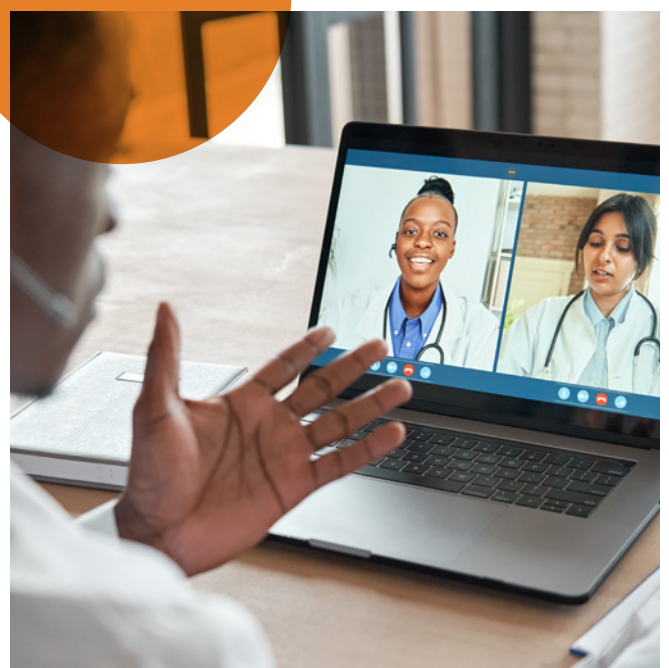
A hybrid working model is more complicated than a fully remote one, which puts all kinds of traditional working practices to the test.

But Millennials and Generation Z workers, aged between 18 and 40, currently make up most of the global workforce. By 2035, these [digital natives](#) will be at the helm of many leadership teams, so understanding and investing in this cohort is critical to future business success. Implementing future-fit digital solutions can help leaders create a hybrid environment that enables both in-person and digital activity, and offers healthcare professionals real flexibility within their busy schedules.

But, as we've seen, maintaining secure working practices across hybrid workforces is a complex yet essential concern. For example, how can a company ensure that only the right person can access a specific work laptop? Also, how do companies prevent personal patient data or images, or new product information being taken from someone's virtual desktop?

According to Citrix's ['State of Security in a Hybrid Work Environment'](#) 2021 report, 73% of survey respondents said the volume of security events and data to process had increased significantly over the past year.

The industry is calling for technology that can deliver next-level user experiences and service delivery for its people and customers – underpinned by robust security – in one integrated solution.



Can seamless hybrid working co-exist with robust security?

The need for border-spanning communications and access to secure data with global visibility has seen the healthcare industry increase its reliance on the IT network and cloud technology over the past few years.

But as cloud hosting becomes more prevalent, industry leaders must exercise caution with regards to the security of valuable and confidential data stored on those networks.

According to [McKinsey](#), three quarters (75%) of experts across the industry consider cyber risk to be a top concern. Now that the pandemic has permanently altered the functioning of our socioeconomic systems, cyber attackers will continue to exploit our fears and our digital vulnerabilities. To remain vigilant and effective, CISOs will need new tactics, particularly in two areas: securing work-from-home arrangements at scale, and supporting high levels of consumer-facing network traffic.

Meanwhile, as reported by an [Hippa Journal's article](#), between January 1, 2022, and June 30, 2022, 347 healthcare data breaches of 500 or more records were reported to the Department of Health and Human Services' Office for Civil Rights (OCR) – the same number of data breaches reported in 2H, 2021.

Also, The war in Ukraine has been accompanied by talk of a growing cybersecurity threat. Electronic Health Records (EHRs), data sharing, telehealth and ICT have become common in healthcare, making the field more

interdependent, and hackers have increasingly targeted healthcare organisations.

According to the latest [Thales Cloud Security report](#), almost half of today's leading organizations are planning to invest in cybersecurity technologies as a priority over the next 12-18 months.



45% of global businesses experienced a cloud-based data breach in 2021

Guaranteeing service delivery and performance in a new era

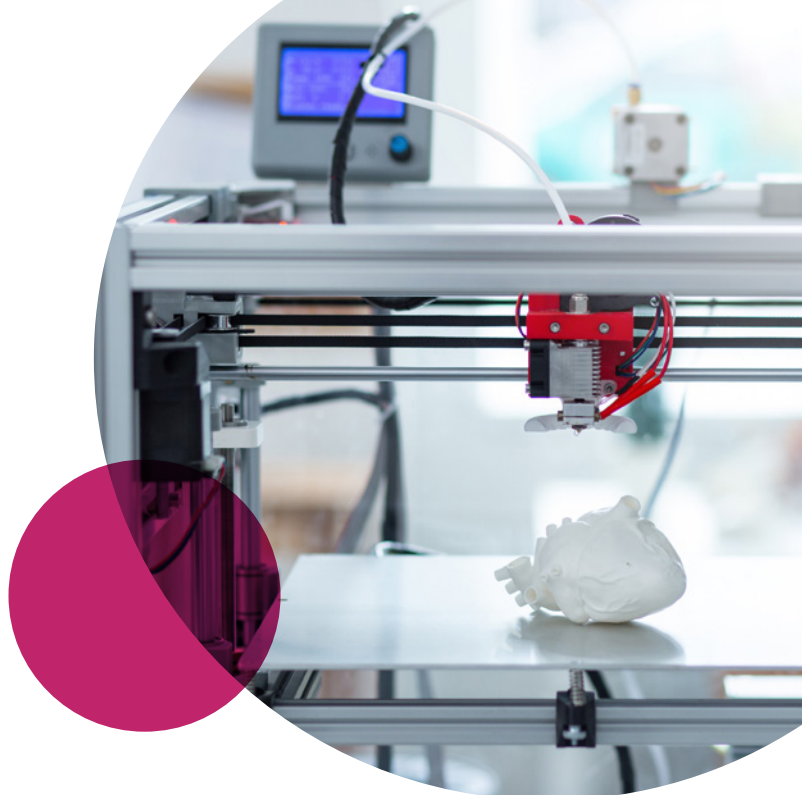
Most industry leaders believe hybrid work environments are key to attracting the industry's top talent, and keeping their companies ahead of the curve. Yet, there is also widespread concern about a disconnect between the network and application performance of technology for on-site workers versus for remote/hybrid workers.

Professionals on-site and in the lab have their tech powered by hardwired network connections, and protected by in-house security protocols and firewalls. Yet, remote employees are often accessing applications and internal systems from home – or other remote locations – and so relying on slower, less secure broadband connections.

In healthcare – where 3D and graphic-heavy workloads are common – IT leaders must provide powerful tech solutions. They also have to optimize their audio-video collaboration capabilities. And they have to do all of that while maintaining the most robust security posture possible for both on-site and remote workers. There are other pitfalls to relying on outdated or unsecured tech. If an organization doesn't have a secure platform for sharing and collaboration as part of its internal infrastructure, for example, employees might take reckless shortcuts to get things done faster. And that might lead them to share highly sensitive information across external or unsecured collaboration platforms. That sort of activity has wider implications for compliance and security, potentially leading to punitive financial costs.

Empowering dispersed teams with next-level tech

For leaders across the healthcare sector, optimizing the user experience to give dispersed teams greater accessibility and scope for collaboration is crucial. You only need to look at the collaboration between the dispersed teams of the University of Oxford and AstraZeneca – who created together a lifesaving Covid-19 vaccine – to see the power and potential of hybrid working, as enabled by leading-edge tech.



Putting in place the foundations to maximize data

Predictive analytics – the machine-learning process of crunching big data to help predict and prepare for future outcomes – has become increasingly important in the life sciences sector.

For healthcare companies to crunch their data securely, efficiently, and effectively, as part of an overarching digital strategy, it's imperative they're supported by cutting-edge technology.

An advanced, centralized solution with proven network reliability and bandwidth – and the capacity to deliver agile, high-performance virtual desktops for hybrid workers – is an essential building block in the race to harness the power of predictive analytics.

In today's fast-paced business environment, data-driven insights on everything from patient experience to competitor performance are crucial to delivering results. To succeed, you need technology that's at the very leading edge.

Five ways to rise to the challenges of the new hybrid world

1. By transforming legacy systems into future-fit systems

Equipping employees with the most secure technology to support communication, collaboration and innovation is the way forward. They also need full visibility into workflows, data and assets.

However, for many healthcare businesses, IT departments may have implemented digital products in a piecemeal fashion to meet immediate demand, rather than as part of an overarching strategy. As such, these siloed, incompatible technologies are an obstacle to digital success.

What life sciences and healthcare companies need is:

- **The right, flexible yet secure hybrid cloud infrastructure** that can scale with their needs, and provide visibility into workloads and data across distributed environments
- A solution that offers the **protection of on-site-level security for sensitive information** – with the rapid, scalable properties of public cloud
- **Visibility of data across the network** and cloud architecture to simplify operations and offer a view of end-to-end workflows
- **A solution that offers multiple types of virtual desktops**, specifically tailored to meet the performance, security and flexibility of individual employees – while creating increased capacity for secure and seamless collaboration
- A solution that ensures **rich, high-definition experiences on any device** for enhanced user experience



2. By creating secure end-to-end virtual environments using cloud-enabled tech

Managing applications in the cloud has many advantages for healthcare and life sciences companies. By facilitating a seamless yet secure flow of information and data, it can save time and money, boost operational efficiency and expand the scope of business possibilities.

However, as we've seen, this can also open organizations up to potential new cybersecurity vulnerabilities. To tackle this as part of a holistic security strategy, businesses need to:

- **Conduct an in-depth assessment** of their organization's infrastructure and risk by identifying network, device and user weaknesses. It should include a review of where devices are on the network and who has access to them; whether they need to be patched; how well the network is set up to proactively monitor for suspicious activity and attacks; and whether, in the event of an attack, hacker attempts can be isolated and stopped quickly. Additionally, risk should be analyzed by looking at users, apps, data and more 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.
- **Agree hosting requirements:** To future-proof company infrastructure, IT and business decision makers need to decide upon a technology solution that's capable of hosting current requirements, while being agile enough to enable seamless upgrades and tighten security.
- **Proactive monitoring:** Implementing logging and monitoring of cybersecurity threats is also crucial in making sure an organization can react quickly to security incidents. On average it takes a healthcare organization [257 days](#) to identify and contain a breach. With the sector so visible and present in the public's consciousness, robust governance and real-time risk analysis is vital to maintaining trust in sector institutions. [Zero Trust](#) is a strategy that applies not only to networking, but across the organization in users, devices, networks and applications. Zero trust is a security architecture that, by default, trusts no one. In a zero-trust model, anyone trying to access a company network is treated as a bad actor and must be continuously verified via mechanisms like multi-factor authentication (MFA) and adaptive authentication.
- **Managing identities and permissions:** It's essential for businesses to do this when using Virtual Desktop Infrastructure (the delivery of secure virtual desktops to endpoint devices, enabling users to access their work desktops from anywhere) – especially as the sector focuses on how information is shared and on what is made available to whom.

Other urgent considerations include establishing an enterprise-wide security policy, creating a Disaster Recovery plan, encrypting data, and implementing advanced authentication.

Worldwide end-user spending on public cloud services is forecast to grow 20.4% in 2022 to total \$494.7 billion.

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

The user demands of today's hybrid workforce are different from a pure remote working model. A hybrid environment is much more flexible and has different network, virtualization, streaming, access, display, desktop virtualization and security demands which need to be scaled both up and down according to need, quickly.

Once the need for scaling services has been established, many leaders worry about how long it will take to establish extra support, and whether it will result in downtime that affects employees and customers, and causes disruption to existing systems.

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

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


Leading-edge tech solutions empower team leaders to monitor systems and identify areas for performance optimization across dispersed networks.

Leaders can use advanced predictive monitoring to continually improve service delivery by enhancing the performance and utilization of different applications.

To do this, healthcare companies need solutions that can monitor application use, network performance and outages, and provide deep insights into user analytics. This is not about 'keeping tabs' or spying on remote employees; it's more about ensuring that frequently used app use is supported appropriately. Predictive monitoring uses the data to identify common issues, improve processes and prevent future incidents.

As the age-old study from [Gartner](#) set out, using a predictive monitoring platform can avoid a significant cost implication (around 300,000 dollars per hour).






5. Leveraging high resolution, real-time, mobile, secure working environments to enhance the collaborative team experience

The hybrid world can often require healthcare professionals to collaborate and deliver on highly confidential and complex R&D tasks on both mobile and desktop devices. To empower employees to do this, IT decision makers need to break down user experience and network barriers that prevent users from viewing high-definition graphics with clarity.

Real-time access and collaboration can also be provided through apps which are deployed quickly and managed on a single platform, with single sign on for devices, for increased accessibility.



Fortunately, UX software, virtual desktop platforms and managed services can assure a rich, high-definition user experience on any device, enabling reliable service delivery on a hybrid cloud platform. Solutions which allow for 3D graphics cards to be present on a few servers, where users can access them from shared sessions, help to provide visually rich images from any mobile device. This optimal user experience and flexibility, coupled with robust security, also enables agile collaboration between dispersed teams, streamlining the communication of crucial project information.

Citrix and Wipro: your best work is waiting for you

The Wipro and Citrix partnership offers your organization a single solution which will empower you to achieve your key business ambitions. Wipro virtuaDesk™ combines the power of cloud, hyper-converged infrastructure (HCI) and Wipro's intellectual property and delivery model with Citrix capabilities like Secure Access, HDX Technology and Citrix Cloud Services.

This partnership's solution harmonizes seemingly conflicting capabilities to deliver superior cybersecurity, user experience and service delivery. Doing so removes the barriers to successful transformation and enables a human-centric approach to the future of life sciences and healthcare.

Our cutting-edge alliance is responsible for leading most of the high-volume deployments in the healthcare industry. Our partnership is successful because, on the one hand, Citrix offers advanced security solutions to provide a superior user experience. Meanwhile, on the other hand, Wipro brings next-generation systems integration and management, as well as consultancy. All of this is delivered in a managed services approach, meaning that it's not just a solution, it's long-term support for your hybrid future.

In partnership with you, we'll support you in delivering a secure, hybrid workforce, with next-generation service delivery and user experience.



DaaS platform

Improved
service
delivery

Superior
user
experience

Secure
foundation
support

Expert
hosted
service

Hybrid
multi-cloud

Case Study:

Global Healthcare company

Scenario:

Our client was required to show innovation and flexibility during the early stages of Covid-19. The global shift in working practices had placed a strain on business continuity, employee productivity and collaboration, and the security issues arising from a newly hybrid workforce.

The main challenges included:

- Ensuring critical IT systems remained secure
- Enabling seamless access to client applications and corporate networks for always-on service delivery
- Enhancing user experiences in remote working environments

With the client providing invaluable support to global efforts to tackle the pandemic, it was vital that they were able to realize their ambitions of a secure, productive hybrid team. Initially, Wipro and Citrix, along with Microsoft, worked with the client to onboard 500 employees within two weeks. However, as events unfolded, we extended our partnership to a year, with the goal of onboarding a further 1,500 employees.

Solutions:

- **Wipro virtuadesk™** – An appliance-based desktop-as-a-service solution focused on creating and enhancing virtual workplaces. Delivered by Wipro, it combines Citrix and Microsoft capabilities to implement, deliver and run the client's enterprise virtual environment.
- **Citrix DaaS** – Delivering secure, future-proofed desktop virtualization which provides a superior user experience, enabling the client's teams to maintain collaboration and productivity from anywhere.
- **Microsoft Windows Virtual Desktop** – Windows 10 multi-session desktop experience, Azure-hosted virtual desktop infrastructure (VDI) capabilities with performance analytics, and extended support for Win 7 VDI.

The client was able to achieve rapid and secure virtual desktop infrastructure deployment, readily scalable for a future in which where no longer matters. The solutions implemented helped the client to instil simplicity, flexibility and agility, and increase mobility. Crucially, the client was able to enhance service delivery, and business analytics and monitoring. Meanwhile employees could thrive together with a superior user experience, enabling them to work anywhere, safely and securely.



Benefits:

- **Secure and optimized workforce collaboration** screenshare and document sharing with watermarking for restricted audio/ video session recording/ playback and auditing.
- **Frictionless service** and exceptional, secure user experiences in an enterprise-grade hyperscale VDI.
- **Seamless data management** between on-premise and cloud with a hybrid cloud model.
- **End-to-end, 24/7 support** for licensing and service for global client users.
- **A single management control plane** for cloud and on-premise VDI management.
- **Monitoring and predictive analytics** to identify issues and respond without downtime.



Ready to give your people the future?

Harnessing 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.

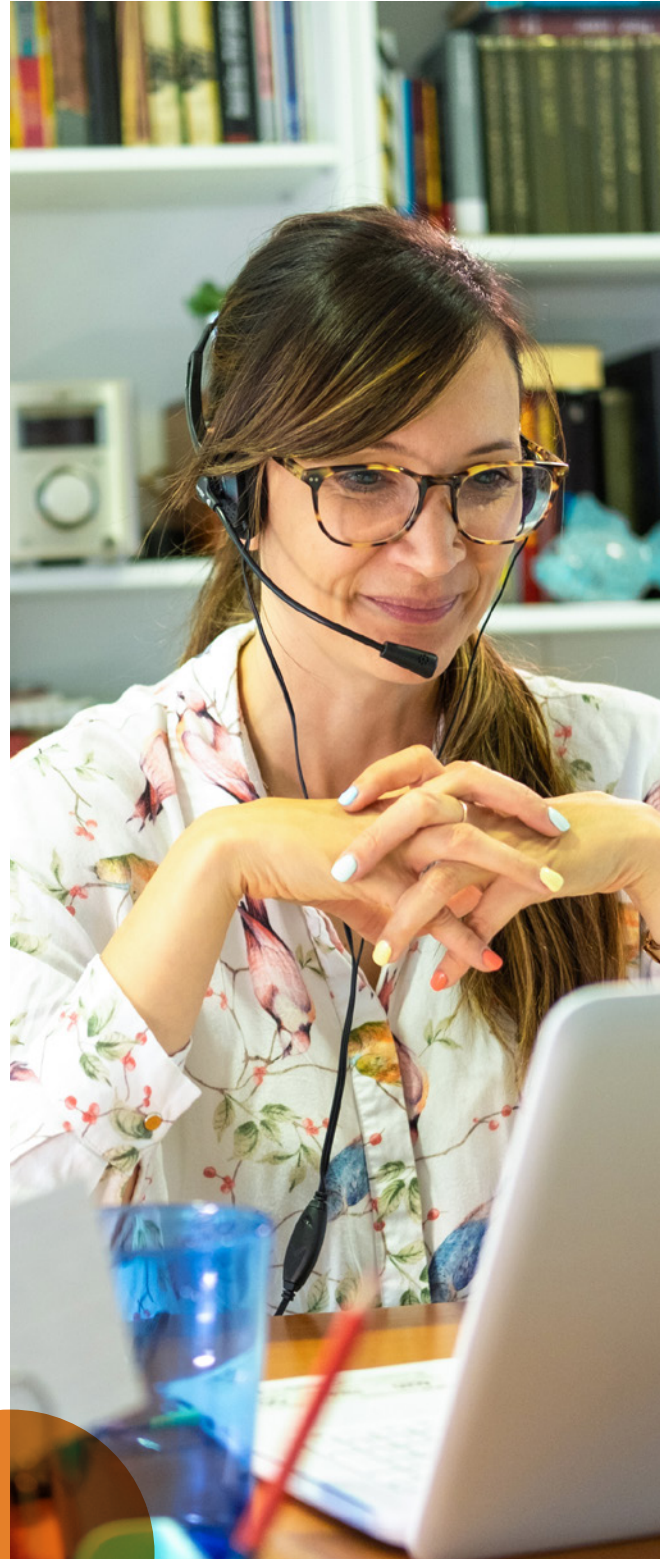
Our future-fit desktop virtualization solution supports organizations in protecting highly sensitive data and intellectual property. It delivers a complete ecosystem – with governance, security and accessibility – to teams across the globe, while holding data in compliance with the latest regulations.

It facilitates greater hybrid team collaboration and innovation by offering the same level of accessibility and visibility to hybrid and on-site employees, while also 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're proud to be considered a trusted partner by many leading healthcare and life sciences firms.

Ensure that security and technology teams within your business are aligned on your hybrid working approach.

Wipro and Citrix can make this happen.





Ambitions Realized.

Wipro Limited
Doddakannelli
Sarjapur Road
Bengaluru – 560 035
India

Tel: +91 (80) 2844 0011
Fax: +91 (80) 2844 0256
wipro.com

Wipro Limited (NYSE: WIT, BSE: 507685, NSE: WIPRO) is a leading technology services and consulting company focused on building innovative solutions that address clients' most complex digital transformation needs. Leveraging our holistic portfolio of capabilities in consulting, design, engineering and operations, we help clients realize their boldest ambitions

and build future-ready, sustainable businesses. With over 250,000 employees and business partners across 66 countries, we deliver on the promise of helping our customers, colleagues and communities thrive in an ever-changing world.

For more information,
please write to us at info@wipro.com