The future of IT security and hybrid work: Security without compromise

IT leaders no longer need to sacrifice security in the name of productivity or flexibility. See how smart IT will power the next evolution in hybrid and remote work.
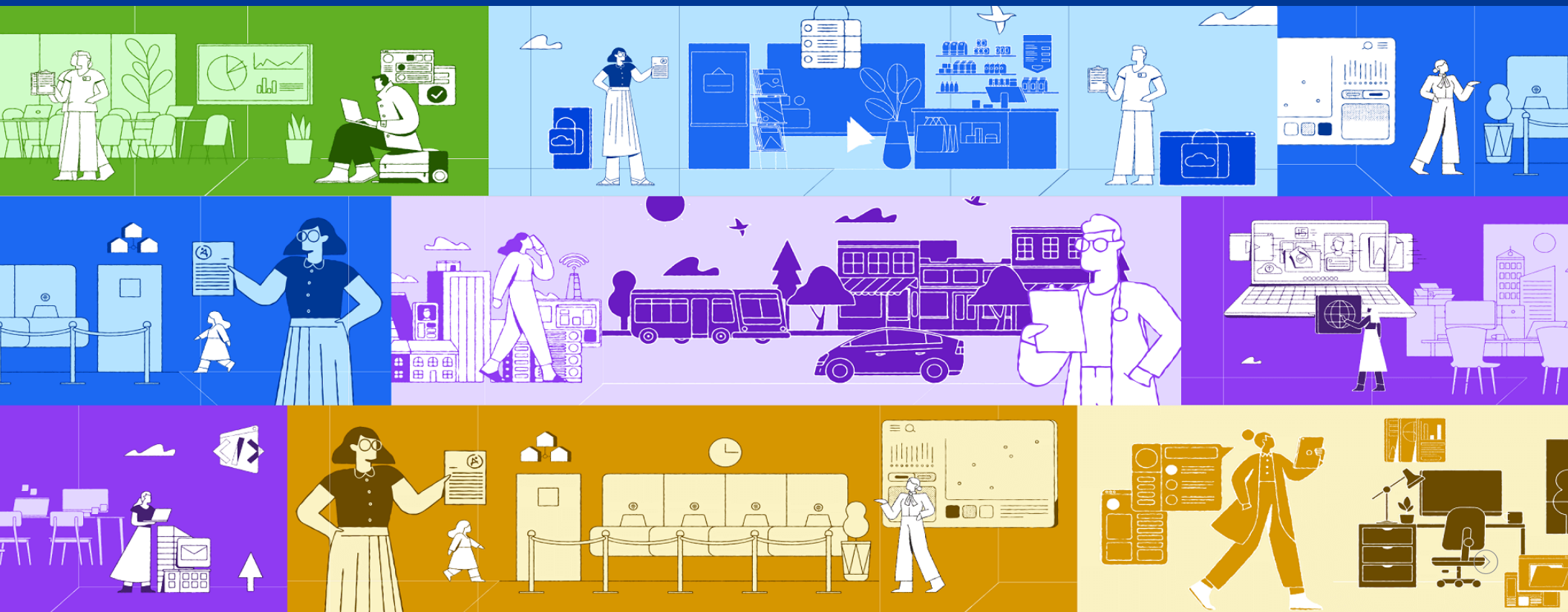
Table of contents

Let's start with the obvious: Hybrid is sticking around. In a [global survey of IT leaders](#) conducted recently by Fieldwork by Citrix and Pulse, 100% of respondents said their organization planned to implement a hybrid work model for the foreseeable future.

Nevertheless, IT teams are not always provided with the tools and systems they need to ensure enterprise flexibility and security. As opportunities multiply for cross-collaboration between teams and external partners, so too do an organization's challenges around security and systems integration. IT leaders understand that this new world requires them to work more efficiently, while also maintaining secure systems and platforms for distributed teams.

IT veterans recognize the contradiction at the heart of this moment. Historically, choosing flexibility meant compromising security. Bolstering security, meanwhile, often created a tedious, disjointed experience for the end user — and more than a handful of passwords scrawled in notebooks. Innovative tech solutions can help unleash an organization's true potential, but only when organizations implement them can they side-step these false choices.

When they do, IT leaders are freed to approach maintaining security and delivering a quality end-user experience as a "both/and" proposition, not an "either/or" one.

Compromise is a relic of the past. Here's how forward-thinking IT leaders can keep it there.

1. False compromise no. 1: Security vs. Employee experience

40%

of all remote access usage that will be served predominantly by ZTNA by 2024, up from less than 5% at the end of 2020 [1]

In the past, IT teams needed to balance maintaining security for their networks and providing employees with the tools they needed to do their jobs effectively. This was a simple solution when everyone sat behind the firewall; after all, VPN provided an effective solution when an employee was remote. New times, however, require new thinking.

By implementing unified zero trust network access (ZTNA), it's possible to protect all users, apps, and data without creating silos or disruption. Deploying proper contextual access policies allows management to scale business propositions while still meeting today's toughest security standards, all without compromising employee productivity.

Furthermore, ZTNA can deliver adaptive access to corporate apps and protect against threats. A secure hybrid work environment also supports bring your own (BYO) and unmanaged devices, and provides access to IT-sanctioned apps, without inviting undue risk. ZTNA also grants secure access to IT-sanctioned apps and enhances security with adaptive authentication and single sign-on (SSO).

Key services

Citrix Secure Private Access uses ZTNA to help businesses scale and still meet today's modern security standards, without compromising the employee experience. Features include adaptive authentication and SSO to IT-sanctioned applications, helping prevent unauthorized access and threats from unmanaged and BYO devices.

1a. Use case: Financial services

Organizations in financial services need to balance their need for security — a paramount concern for any heavily regulated industry — and ensuring a quality employee experience. For example:

One brokerage house may offer VPN, which provides adequate but simplistic security and is prone to a slow, painful user experience.

The second brokerage relies on remote access to enabled apps via SSO only, which can present security vulnerabilities.
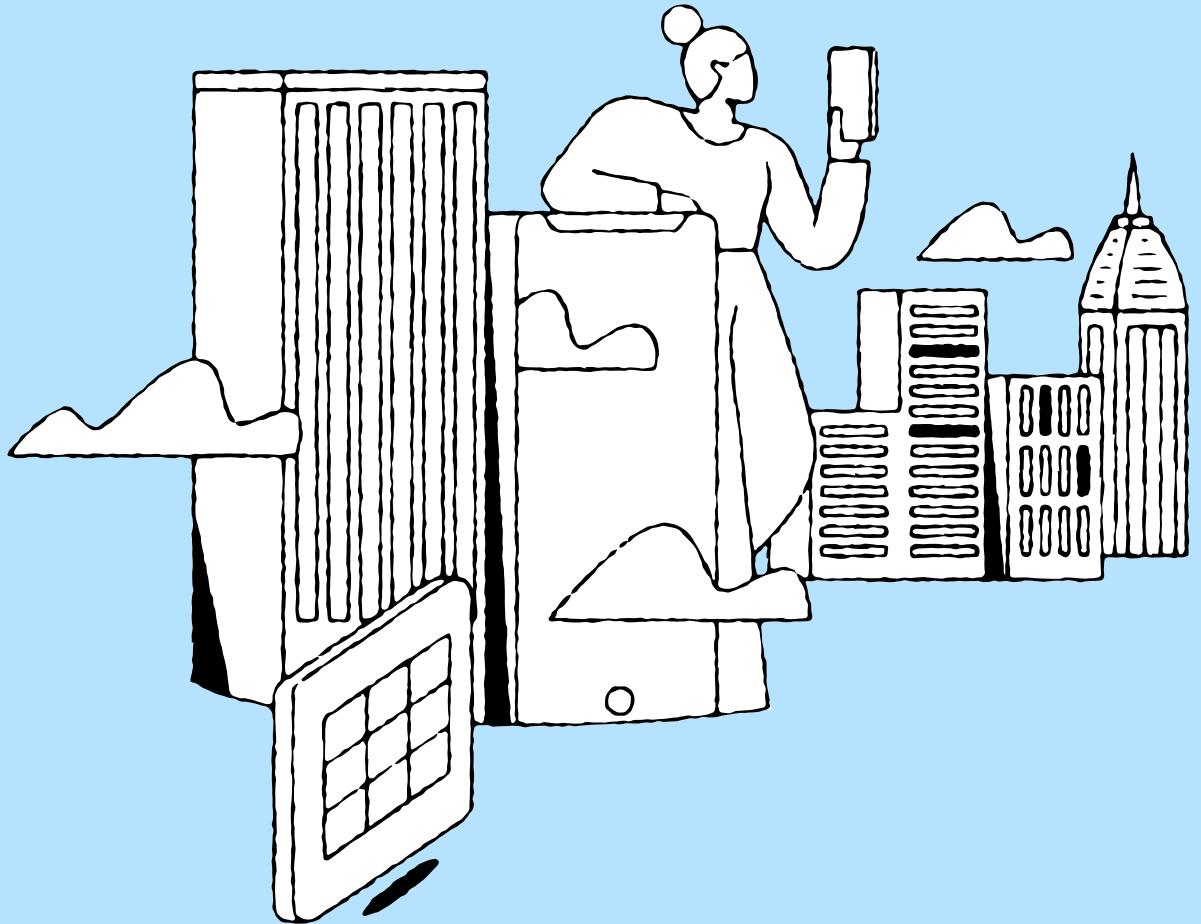
The no compromise solution

By tapping into IT and tech solutions such as DaaS that protect data — wherever work is taking place — companies, employees, and contractors can access more choice and flexibility in their workstreams, while maintaining a muscular security posture.

> **"**
> VPN-less access with Citrix has added a great deal of value in making the employee experience better and our environment much more secure."

Gilliard Delmiro
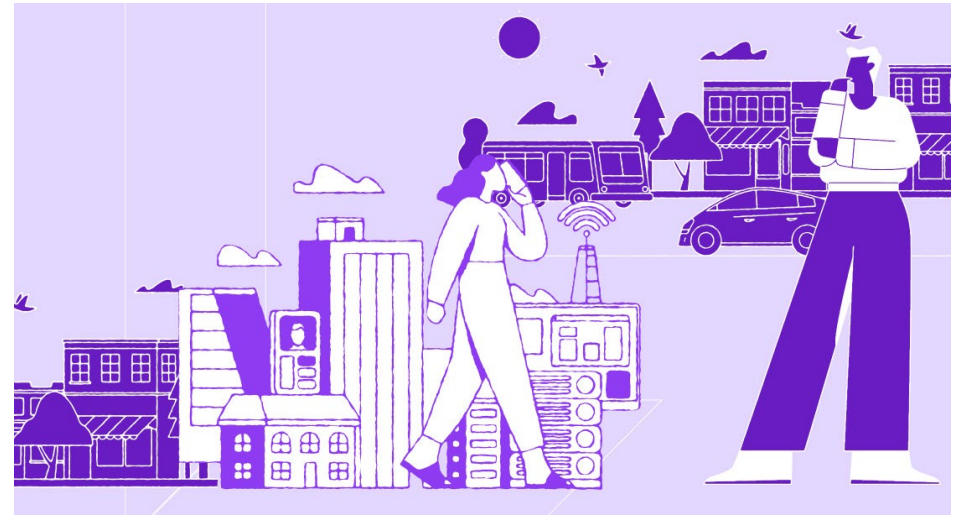Co-founder and CTO
HDI

Read customer story

1b. Use case: Defense

Multiple layers of security clearances make traditional methods of protecting data in the defense industry cumbersome for employees to navigate, especially in an on-the-go world where work may be performed from multiple locations and devices. For example:

The legacy systems of a traditional contractor require laborious effort from employees to protect data — whether they sit near the server closet or beyond the firewall.

In an effort to maximize work-from-anywhere flexibility for its employees, a defense startup may compromise its enterprise security as team members log in from multiple devices.

The no compromise solution

By using a service that offers secure ZTNA private access, both brokerages can ensure their people experience fast, seamless access to all their apps and data, while adding security layers beyond the initial point of access. The result? Robust data protection and a positive employee experience.
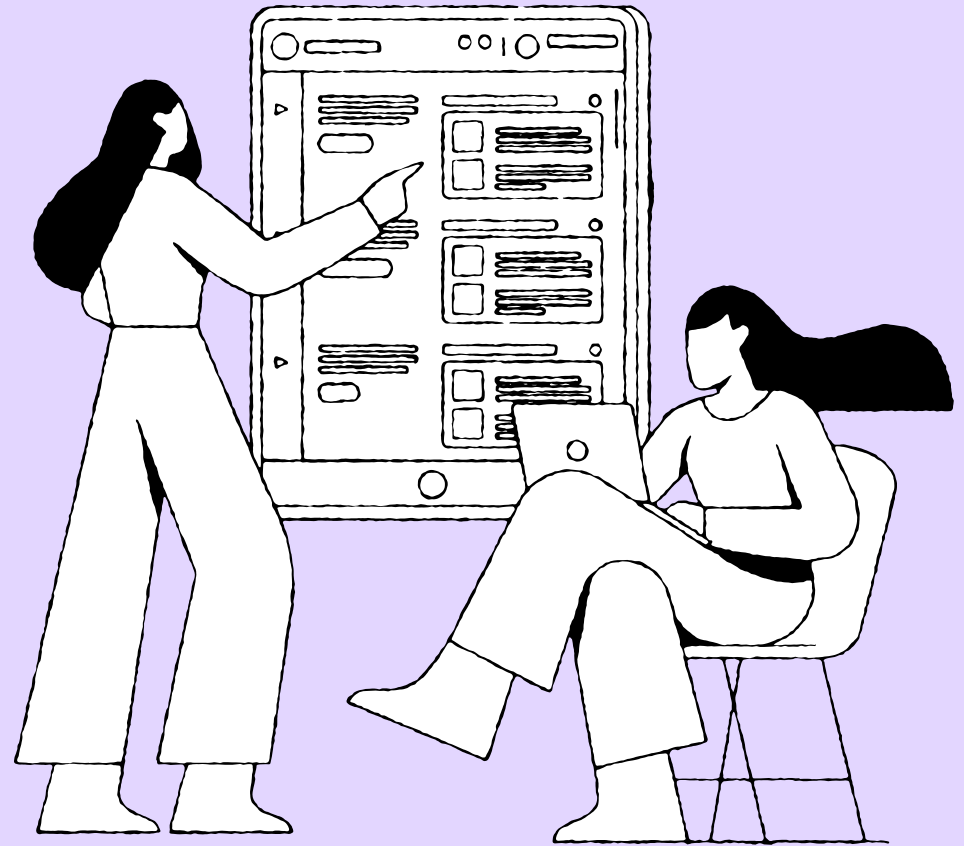
Customer story

The U.S. Defense Logistics Agency (DLA), which supports all branches of the Armed Forces as well as first responder personnel nationwide, had a data center infrastructure as massive as its mission.

To streamline operations while ensuring remote access to vital data, the DLA adopted a Zero Trust security model — which permitted BYOD access for remote DLA contractors — and a VDI environment to gain pinpoint control of end-user digital experiences.

The result? Savings from decreased power consumption, a smaller hardware footprint, and alleviated security issues.

Learn more

1c. Use case: Contact center

Contact centers can get caught between extending flexibility to employees around how they access networks, and maintaining security protocols at scale. For example:

A third-party contact center may need to scale tech solutions quickly based on the ever-changing needs of the multiple brands it supports, but frets about being locked into binding contracts.

A second center specializes in on-site support, but must adjust to the rapidly evolving needs of its distributed workforce.

The no compromise solution

With desktop as a service (DaaS) combined with ADC, all employees get a single, simple unified access point in and out of the office — as well as more autonomy and less reliance on IT — without lag or integration headaches.
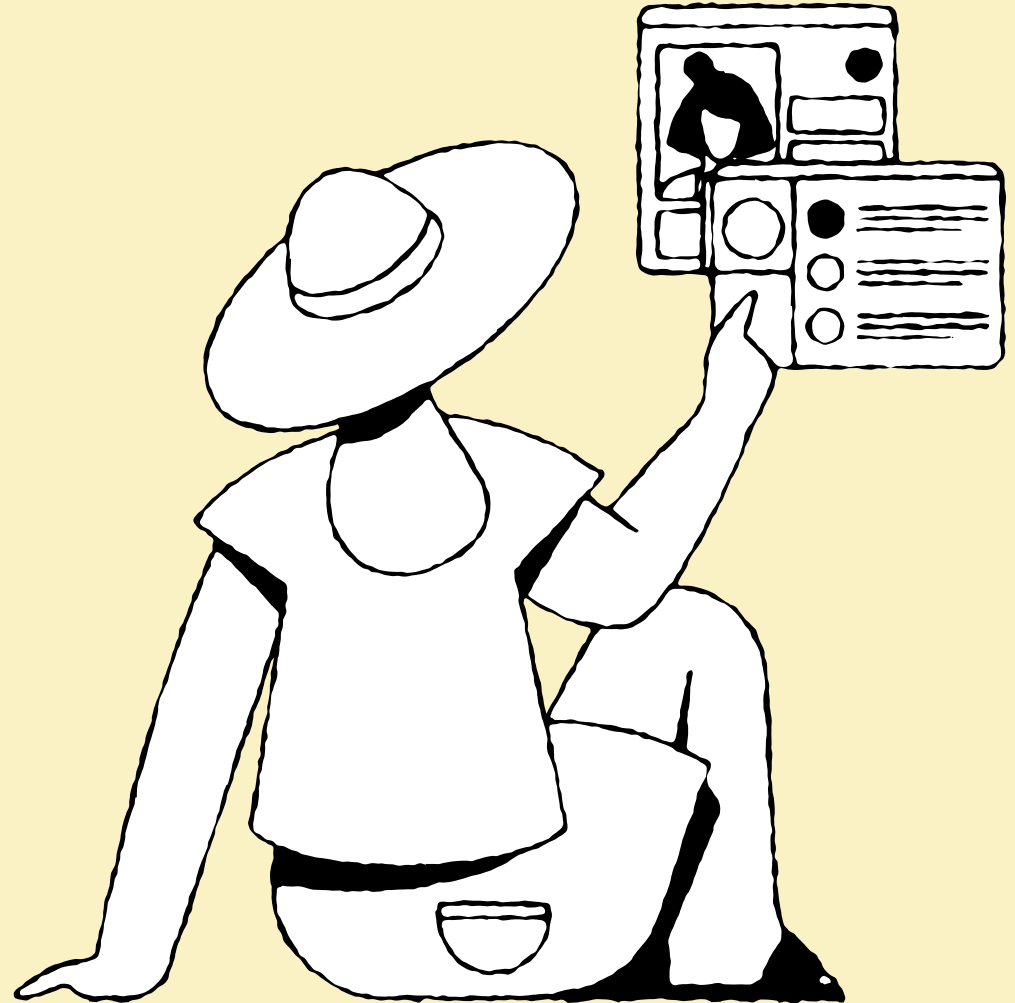
"

Our Citrix digital technology allows us to support a sustainable hybrid work model that serves us well — now and into the future ... Now, we can conduct global searches and actually recruit, hire, train, and coach talent anywhere. We create new jobs in areas of the world in which economic downturn has caused high unemployment and fewer professional jobs to be available.

Jose Guereque
Executive Vice President of Infrastructure and Chief Information Officer, Teleperformance

Read customer story

2. False compromise no. 2: Security vs. Flexibility

79%

of respondents who indicated they believe alternative desktop delivery models such as VDI and DaaS are more secure than traditional desktop delivery models[2]

Traditionally, IT leaders needed to balance ensuring enterprise flexibility with creating secure environments for proprietary data. Thankfully, these leaders no longer have to compromise when it comes to how they provision, integrate, and deploy technology. By offering DaaS, organizations can power work from anywhere and gain IT simplicity and agility. DaaS also provides the flexibility for employees to thrive in their work, wherever they are, while IT teams maintain security protocols and standards.

These solutions work by reliably offloading infrastructure and maintenance while delivering cloud apps and desktops from a prove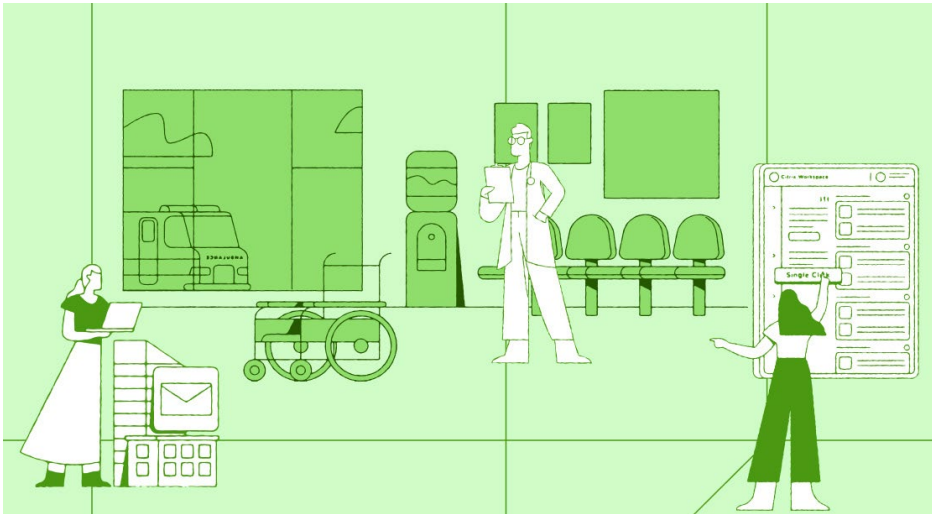n, secure provider. It's simple to migrate apps to and among clouds, and future-forward orgs will implement a best-in-class DaaS solution without locking in with a single vendor.
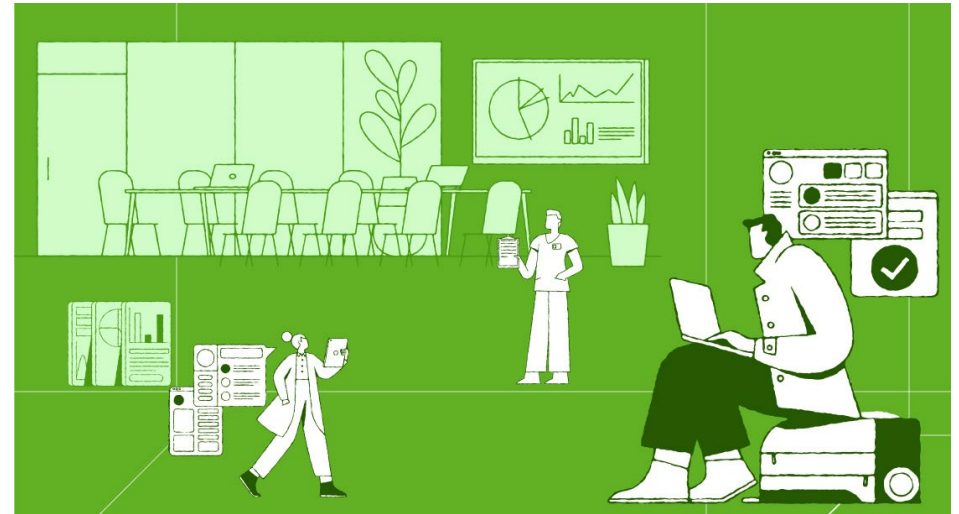
Key services

Citrix DaaS and VDI solutions allows companies to securely deliver apps and desktops to any device, over any network. These solutions empower companies to deploy secure remote apps and desktops to users at scale — while providing a great experience and simplifying IT management. No compromises necessary.

2a. Use case: Healthcare

Medical organizations of all sizes can have sprawling technical infrastructures with legacy tools and systems. Furthermore, patient privacy laws require specific types of security protocols that can be onerous to implement and enforce. For example:
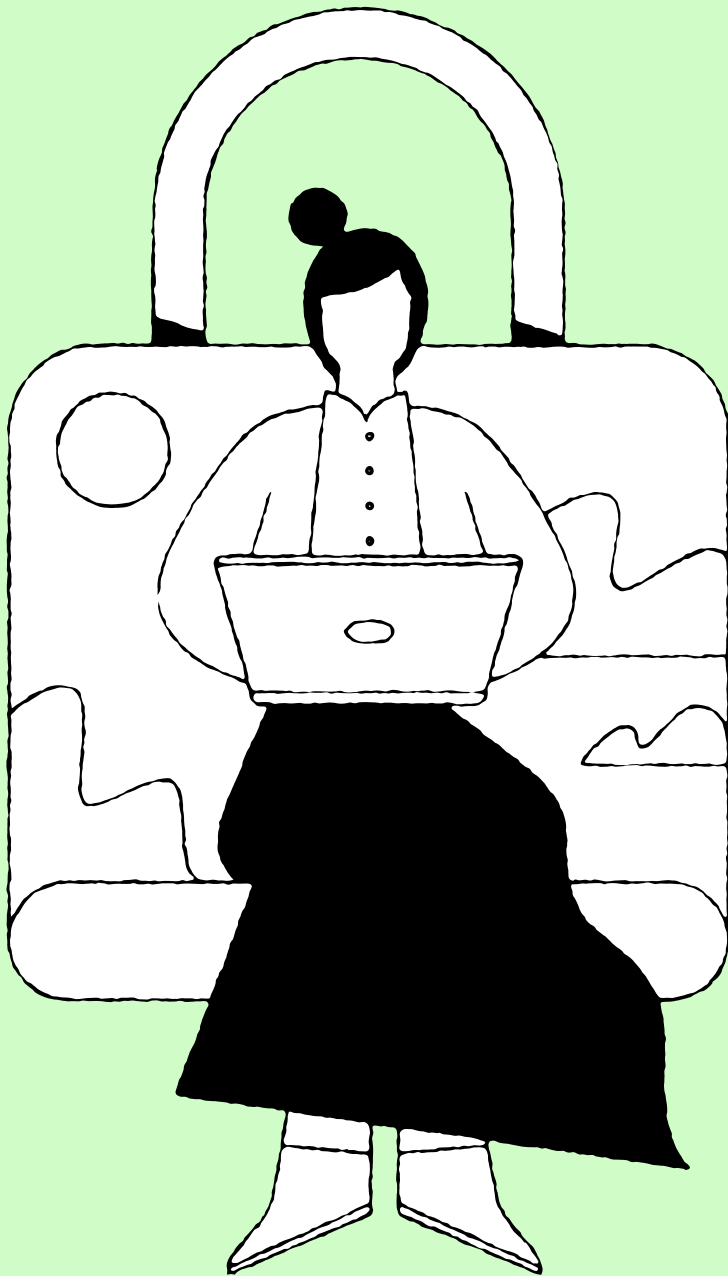

One large hospital group boasts a computer network housed across a sprawling geographical area, all running on legacy hardware and software.

Another is struggling to ensure compliance with patient privacy laws that require specific types of security protocols, which can be difficult and time-consuming to implement and enforce.

The no compromise solution

Tech-agonistic platforms don't lock a business into a single provider, integrating flawlessly with existing tech solutions via Microsoft and Google partnerships. This helps manage IT transformation projects incrementally, without wholly replacing existing systems or disrupting business. Services like DaaS make an environment that powers work-from-anywhere and IT simplicity, while allowing a company to quickly ramp up office staff in a world of hybrid work.

> "
> **With Citrix cloud services, we were able to double our capacity, from 600 to 1,200 users, overnight. There's no way we could have scaled so quickly if we hadn't already been on cloud.**
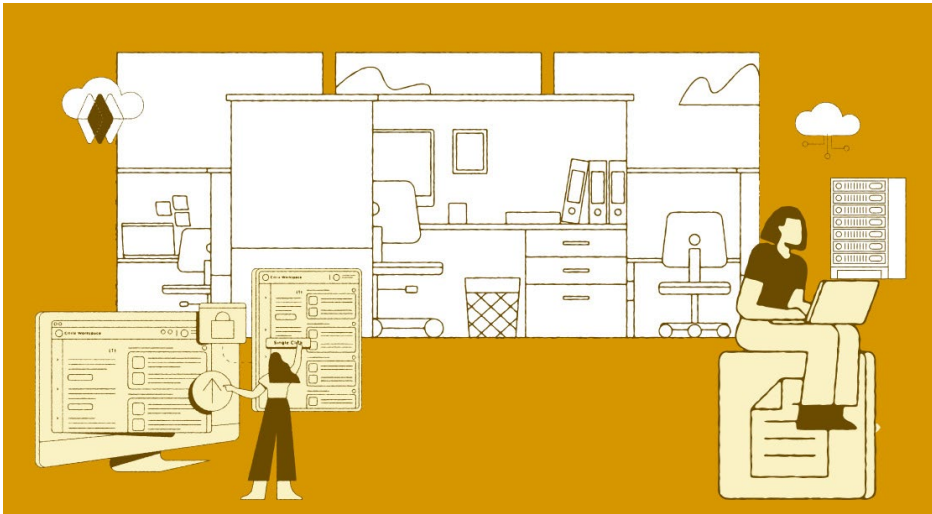
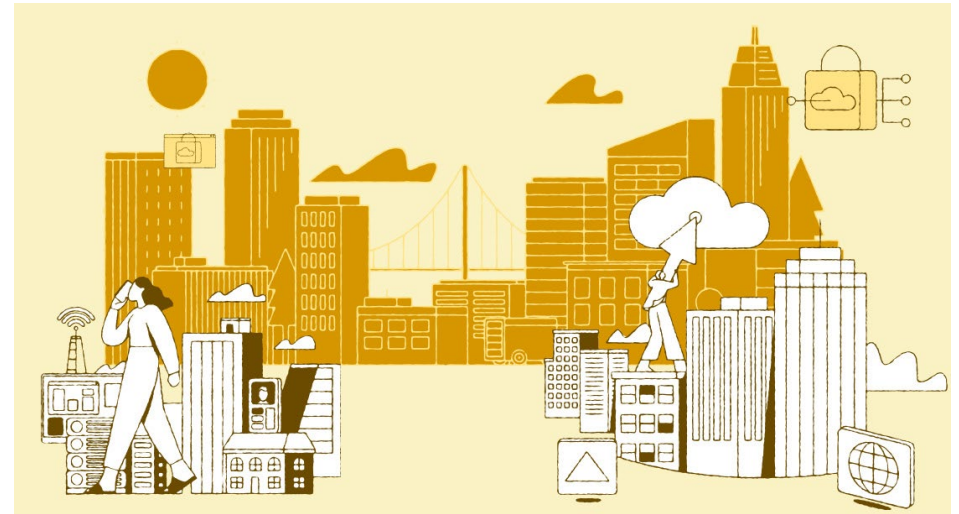**Justin Beardsmore**
CTO
Lewisham and Greenwich NHS Trust

Read customer story

2b. Use case: Financial services

Security rules and regulations governing the financial services sector can be onerous for employees to navigate —
even for the regulators themselves. For example:

One financial industry regulator is considering moving to a cloud-based VDI solution, but is concerned about security.

A second regulator conducts its work more traditionally, via a full-service solution, but lacks the simplicity of the cloud.

The no compromise solution

Services such as VDI and DaaS can be deployed in both environments, delivering the best of both worlds and eliminating the need to choose between flexibility and efficiency. Organizations that employ these services empower their people to be productive in any working situation, while quickly and securely moving from task to task or device to device.

> "
>
> **Citrix has provided us at Indiabulls a stable platform that has centralized management of all our end-user machines, which has brought significant efficiencies around the key parameters of security and user experience while reducing cost and improving response times."**
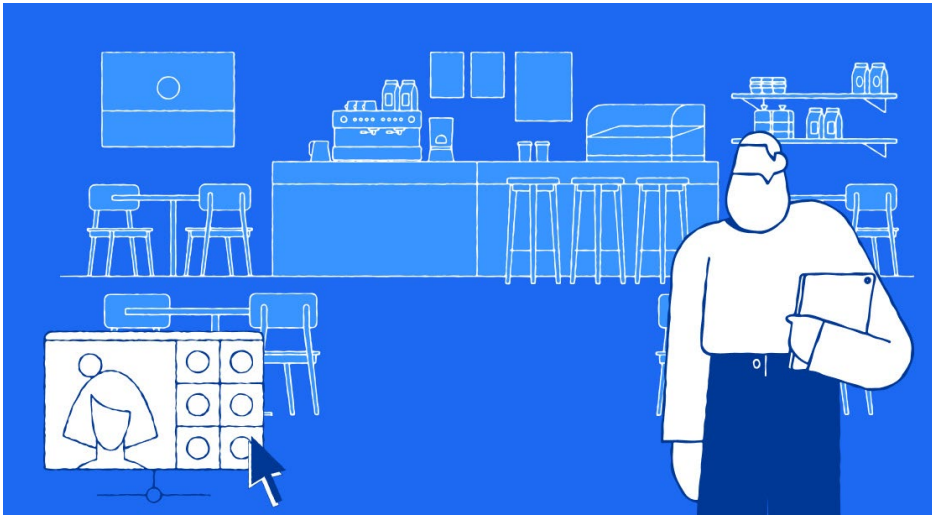
Ravi Verma
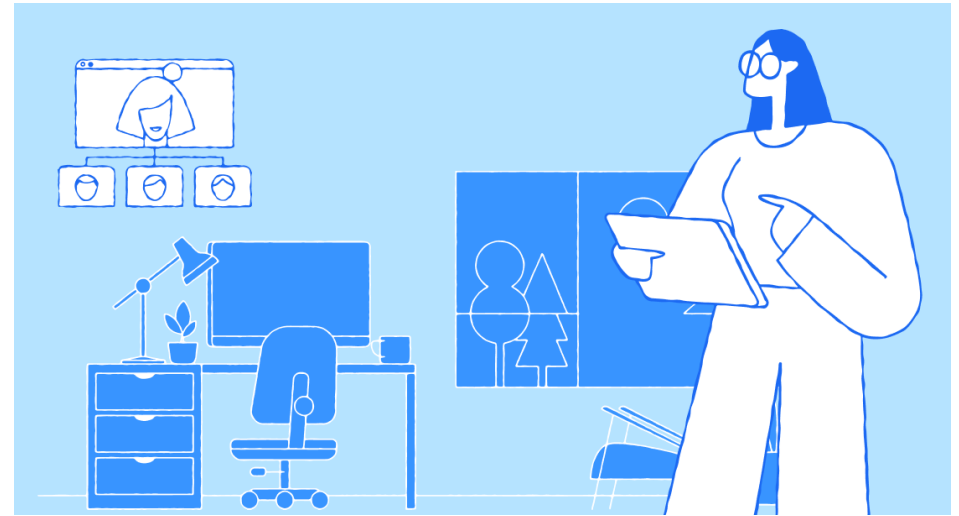Indiabulls

Read customer story

2c. Use case: Education

Given the range of technology requirements from faculty, students, staff, and other users, IT needs vary widely across different types of educational institutions. For example:

A university system has a large physical and technical footprint across multiple cities, creating a massive perimeter — and potential attack surface — that must be secured.

A community college relies on traditional static resources such as powerful workstation PCs or advanced software installed on a limited number of desktops, which fails to meet teaching and learning needs in a post-pandemic world.

The no compromise solution

With DaaS, it's possible to deliver a powerful and familiar desktop experience to students and staff, on campus or off. By leveraging cloud services, educational institutions can provide a trusted, innovative solution that offers an exceptional user experience for everyone who logs on.

> **"**
>
> **Citrix was our first choice because of the flexibility, scalability, and manageability it offers."**

Alan Blakely
Client Software Manager
Northumbria University

Read customer story

Enabling a 'no compromise' world of work

When it comes to ensuring security while delivering the highest-quality employee experience possible, the choice is clear: There's no need to choose. Gone are the days when a company's IT team was forced to compromise between flexibility and efficiency, or security and employee experience.

Solutions such as ZTNA, DaaS, and VDI can help organizations deploy secure solutions that set employees up for success. These assets and systems allow workers to thrive in hybrid work situations while also empowering cross-team as well as intra- and inter-organization collaboration. And by avoiding contracts tied to single providers, the solutions can scale up and down efficiency on an as-needed basis — saving time, effort, and money.

See how Citrix and [Partner name] can help you support your flexible workforce fast with secure, easy-to-manage cloud desktops and apps. Learn more at: (URL goes here)

1   https://www.gartner.com/en/newsroom/press-releases/2021-06-22-gartner-forecasts-51-percent-of-global-knowledge-workers-will-be-remote-by-2021
2   https://www.citrix.com/products/citrix-daas/resources/content/dam/citrix/en_us/documents/analyst-report/esg-are-desktops-doomed.pdf

ICT NETWORK SYSTEMS INC.

This area can be used for a partner-specific message. Lorem ipsum dolor sit amet, consectetur adipiscing elit, sed do eisumod tempor incididunt ut labore et dolore magna aliqua. Quisipsum suspendisse.